SPRAWOZDANIE Z DZIAŁALNOŚCI PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH W ROKU 2020

SPRAWOZDANIE Z DZIAŁALNOŚCI
PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
w ROKU 2020

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 2020 r. do 31 grudnia 2020 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 2020. 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 2020 r. minął drugi, pełny rok kalendarzowy bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych w polskim porządku prawnym. Przyszedł czas na refleksje i podsumowania, 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 2020, 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 2020, 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 w maju 2018 r., nastąpiła także zmiana instytucjonalna. Na podstawie art. 167 ust. 1 ustawy o ochronie danych osobowych Biuro Generalnego Inspektora Ochrony Danych Osobowych stało się

[14] Ustawa z 10 maja 2018 r. o ochronie danych osobowych, t.j. Dz. U. z 2019 r. poz. 1781.

Urzędem Ochrony Danych Osobowych (UODO). W 2020 r. w strukturach Urzędu powstały nowe Departamenty, a w ich ramach Wydziały odpowiadające za realizację zadań wynikających z przepisów o ochronie danych osobowych dotyczących określonych sektorów.

Statutowe komórki organizacyjne Urzędu Ochrony Danych Osobowych noszą następujące nazwy: Departament Orzecznictwa i Legislacji (DOL), Departament Współpracy Międzynarodowej i Edukacji (DWME), Departament Kontroli i Naruszeń (DKN), Departament Komunikacji Społecznej (DKS), Departament Skarg (DS), Departament Kar i Egzekucji (DKE), Departament Informatyki (DIF), Departament Organizacyjny (DO), Departament Administracyjny (DA), Dział Finansowy, Dział Audytu i Kontroli Wewnętrznej, Dział Kadr, Zespół Radców Prawnych, Samodzielne Stanowisko Inspektora Ochrony Danych oraz Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych.

W trzech departamentach wyodrębnione zostały **wydziały**, które zajmują się sprawami z określonych sektorów. I tak, w Departamencie Orzecznictwa i Legislacji powstały trzy wydziały: Wydział Legislacji, Wydział Współpracy z Inspektorami Ochrony Danych oraz Wydział 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.

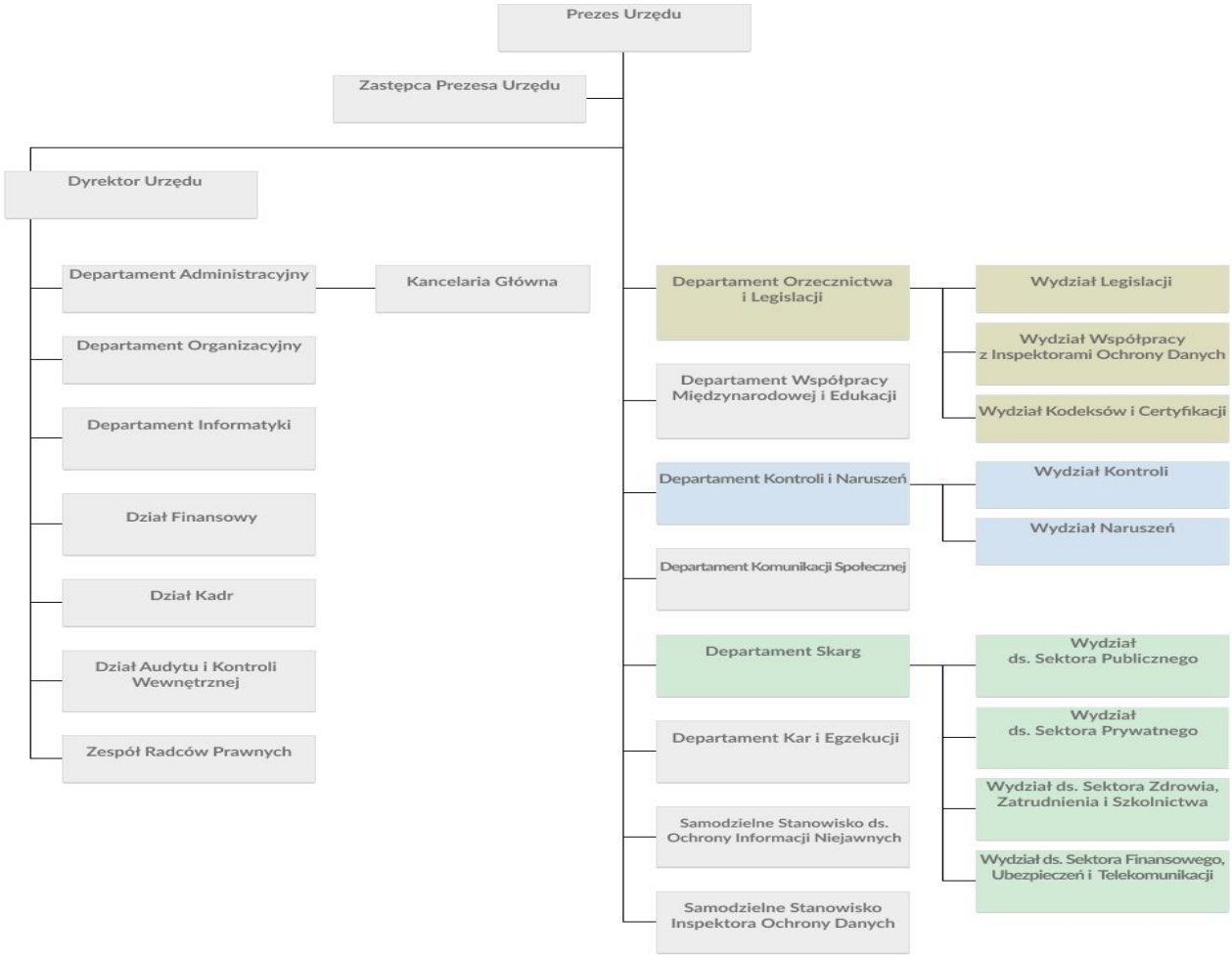
Wdrożone zmiany pozwoliły reagować na naruszenia ochrony danych osobowych bez uszczerbku dla realizowanych innych zadań organu oraz usprawniły działania Urzędu, co przełożyło się na lepszą ochronę danych osobowych obywateli.

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 Urzędu Ochrony Danych Osobowych z 6 listopada 2019 r. w sprawie nadania statutu Urzędowi Ochrony Danych Osobowych[15].

[15] https://uodo.gov.pl/pl/p/regulamin-urzedu



Wykres 1. **Struktura organizacyjna Urzędu Ochrony Danych Osobowych.**

2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2020 r. w przeliczeniu na pełne etaty wynosił 244,05 etatu (tj. 247 osób). Natomiast zatrudnienie w UODO na dzień 31 grudnia 2020 r. wynosiło 272,55 etatu (tj. 277 osób). Na koniec 2020 r. na stanowiskach merytorycznych zatrudnionych było 245 osób, a na stanowiskach pomocniczych 30 osób. Wyższe wykształcenie posiadało 246 pracowników, w tym 148 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2020 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 – 30 osób (30 etatów), w tym:
   - Wydział Legislacji – 10 osób (10 etatów),
   - Wydział Współpracy z Inspektorami Ochrony Danych – 4 osoby (4 etaty),
   - Wydział Kodeksów i Certyfikacji – 5 osób (5 etatów),
5) Departament Współpracy Międzynarodowej i Edukacji – 14 osób (13,3 etatu),
6) Departament Kontroli i Naruszeń – 47 osób (46,4 etatu) w tym:
   - Wydział Kontroli – 18 osób (18 etatów),
   - Wydział Naruszeń – 22 osoby (22 etaty),
7) Departament Komunikacji Społecznej – 15 osób (14,8 etatu),
8) Departament Skarg – 97 osób (96,5 etatu), w tym:
   - Wydział ds. Sektora Publicznego – 17 osób (17 etatów),
   - Wydział ds. Sektora Prywatnego – 29 osób (29 etatów),
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 18 osób (17,5 etatu),
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 11 osób (11 etatów),
9) Departament Kar i Egzekucji – 9 osób (9 etatów),
10) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 1 osoba (1 etat),
11) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba (1 etat),
12) Departament Administracyjny – 25 osób (24 etaty),
13) Departament Organizacyjny – 9 osób (9 etatów),
14) Departament Informatyki – 11 osób (10,42 etatu),
15) Dział Finansowy – 5 osób (5 etatów),
16) Dział Kadr – 4 osoby (4 etaty),
17) Dział Audytu i Kontroli Wewnętrznej – 1 osoba (0,5 etatu),
18) Zespół Radców Prawnych – 3 osoby (3 etaty),
19) Radca – 2 osoby (1,3 etatu).

2.3. Budżet Urzędu Ochrony Danych Osobowych za 2020 r.

Budżet UODO ustalony w ustawie budżetowej na 2020 r. wynosił: 36 707 tys. zł, w tym:

- wynagrodzenia 24 585 tys. zł
- pochodne od wynagrodzeń 4 451 tys. zł
- wydatki majątkowe 1 262 tys. zł
- pozostałe wydatki 6 409 tys. zł

Budżet UODO po zmianach wprowadzonych na podstawie przepisów art. 31 ust. 2 i 3 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[16] oraz w związku z decyzją Prezesa Rady Ministrów z dnia 26 listopada 2020 r. w sprawie blokowania na rok 2020 wydatków budżetu państwa[17], **wyniósł 35 228 tys. zł,** w tym:

- wynagrodzenia 23 163 tys. zł
- pochodne od wynagrodzeń 4 302 tys. zł
- wydatki majątkowe 992 tys. zł
- pozostałe wydatki 6 771 tys. zł

Wydatki zrealizowane przez UODO w 2020 r. w kwocie 34 898 tys. zł, w tym:

- wynagrodzenia 23 064 tys. zł
- pochodne od wynagrodzeń 4 298 tys. zł
- wydatki majątkowe 988 tys. zł
- pozostałe wydatki 6 548 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

[16] Dz. U. z 2020 r. poz. 374.
[17] Rozporządzenie Rady Ministrów z dnia 26 listopada 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, Dz. U. z 2020 r. poz. 2091.

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[18].
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**).

[18] 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.

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

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

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

Należy podkreślić, że RODO nie powstało w próżni normatywnej. Ponad 20 lat doświadczeń w stosowaniu dyrektywy 95/46/WE – zarówno przez administratorów danych, jak i podmioty danych, ale także niezależne organy nadzorcze – stało się 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, finansowego, ubezpieczeń i telekomunikacji), 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.

Departament Kontroli i Naruszeń prowadzi działania kontrolne w oparciu o przygotowane wcześniej projekty planów kontroli. 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, nakładane były administracyjne kary pieniężne.

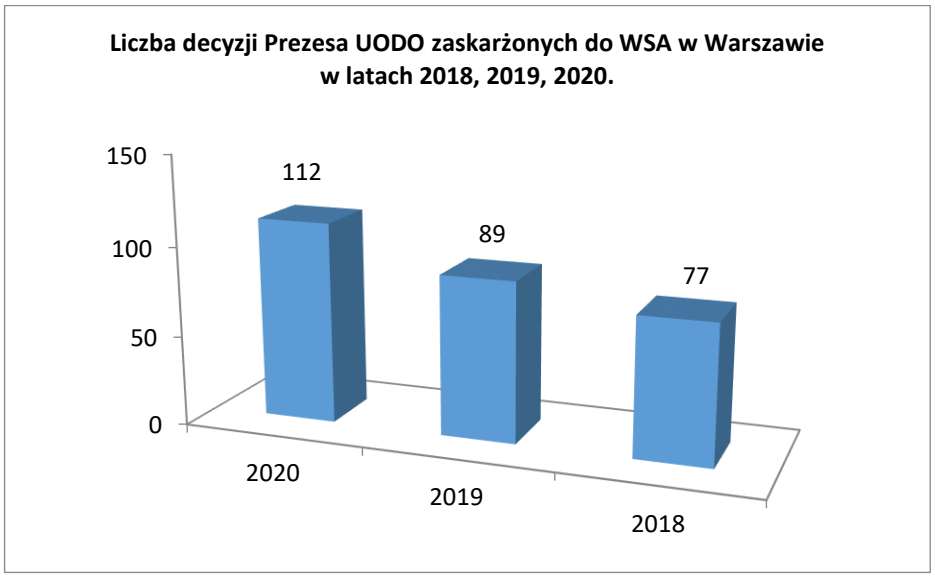
Ważnym zadaniem nałożonym na organ nadzorczy przepisami ogólnego rozporządzenia jest także realizacja obowiązków i uprawnień przez administratorów i inspektorów ochrony danych. Zadania te polegały m.in. na przyjmowaniu zawiadomień o wyznaczeniu inspektora ochrony danych (IOD), udzielaniu odpowiedzi na 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 2020 r. wniesiono do Wojewódzkiego Sądu Administracyjnego w Warszawie **112 skarg** na decyzje lub postanowienia Prezesa UODO. Dla porównania – w 2019 roku skarg na decyzje lub postanowienia Prezesa UODO było 89.



Wykres 2. **Zestawienie liczby decyzji Prezesa UODO zaskarżonych do WSA w Warszawie w latach 2018 – 2020.**

Z ogólnej liczby 112 decyzji organu nadzorczego zaskarżonych do WSA w Warszawie, 20 decyzji zaskarżono do Naczelnego Sądu Administracyjnego.

Przykładem może być wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 26 sierpnia 2020 r.[19] oddalający skargę Burmistrza A. na decyzję Prezesa UODO z dnia 18 października 2019 r.[20] nakładającą na niego karę w wysokości 40 000 zł oraz nakazującą mu dostosowanie operacji przetwarzania danych osobowych do przepisów ogólnego rozporządzenia o ochronie danych, m.in. poprzez: zaprzestanie udostępniania danych osobowych w związku z prowadzeniem BIP bez uprzedniego zawarcia umów powierzenia danych osobowych, wdrożenie polityk określających okresy przetwarzania danych w BIP, przeprowadzenie analizy ryzyka w związku z publikacją nagrań sesji rady miejskiej, wdrożenie odpowiednich środków organizacyjnych i technicznych w związku z przetwarzaniem danych osobowych na kanale YouTube oraz mających na celu zabezpieczenie danych osób fizycznych pochodzących z nagrań sesji Rady Miasta poprzez zapewnienie dostępności kopii zapasowych, ujęcie w rejestrze czynności przetwarzania związanych z prowadzeniem BIP informacji o wszystkich odbiorcach danych i o planowanych terminach usunięcia danych. W uzasadnieniu wyroku sąd wskazał, iż całkowicie podziela dokonaną przez organ ocenę poszczególnych naruszeń przepisów prawa materialnego. Sąd nie znalazł podstaw do uchylenia zaskarżonej decyzji. Zdaniem Sądu Prezes UODO prawidłowo zastosował przepisy ogólnego rozporządzenia o ochronie danych osobowych, które mają zastosowanie do przetwarzania danych w BIP. Sąd uznał, że Prezes UODO należycie uzasadnił wymiar kary, biorąc pod uwagę bardzo długi czas trwania naruszeń, umyślny ich charakter, wysoki stopień odpowiedzialności administratora oraz brak jego współpracy z organem po wszczęciu postępowania. W ocenie Sądu nałożona na Burmistrza A. kara pieniężna w wysokości 40 000 zł jest karą adekwatną, proporcjonalną oraz została nałożona w sposób prawidłowy. Sąd w uzasadnieniu wyroku zwrócił uwagę, że „na skarżącego nałożono tylko 40% możliwej kary, co pozwala ocenić ją jako skuteczną, proporcjonalną i odstraszającą". Burmistrz A. złożył do Naczelnego Sądu Administracyjnego skargę kasacyjną od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie.

W innej sprawie, wyrokiem z 3 września 2020 r.[21], Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę na decyzję Prezesa UODO z 10 września 2019 r.[22], nakładającą na spółkę karę w wysokości ponad 2 800 000 zł, w związku z naruszeniem ochrony danych osobowych klientów sklepów internetowych należących do spółki, polegającym na nieuprawnionym dostępie

[19] sygn. akt: II SA 2826/19.
[20] sygn. akt: ZSPU.421.3.2019.
[21] sygn. akt: II SA/Wa 2559/19.
[22] sygn. akt: ZSPR.421.2.2019, ZSPR.405.67.2019.

osób trzecich do bazy danych klientów. Sąd uznał**,** że skarga nie zasługuje na uwzględnienie, ponieważ przeprowadzając kontrolę pod względem zgodności z prawem zaskarżonej decyzji administracyjnej, nie stwierdził, aby Prezes UODO, wydając decyzję, naruszył przepisy prawa. Wojewódzki Sąd Administracyjny w Warszawie stwierdził, że ww. decyzja spełnia warunki określone w art. 107 § 1 pkt 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[23], tj. zawiera m.in. powołanie podstawy prawnej, uzasadnienie faktyczne i prawne, zaś osnowa decyzji, czyli rozstrzygnięcie jest sformułowane jasno i precyzyjnie. Przedmiotem postępowania prowadzonego przez Prezesa UODO wobec spółki były uchybienia, które zostały stwierdzone w trakcie kontroli[24], w związku ze zgłoszeniami naruszeń ochrony danych osobowych klientów sklepów internetowych prowadzonych przez tę spółkę. W decyzji Prezes UODO wskazał, że spółka naruszyła zasadę poufności danych wyrażoną w art. 5 ust 1 lit. f rozporządzenia 2016/679, skonkretyzowaną w postaci obowiązków określonych w art. 24 ust 1, art. 25 ust. 1 oraz art. 32 ust. 1 lit. b i lit. d, art. 32 ust. 2, bowiem wywiązała się jedynie częściowo z obowiązku zapewnienia odpowiednich środków zabezpieczenia technicznego przetwarzanych danych. Niewypełnienie obowiązku wynikającego z art. 32 ust. 2 rozporządzenia 2016/679 polegało na doborze nieskutecznych środków technicznych i organizacyjnych na poziomie kontroli dostępu, uwierzytelniania i monitorowania ruchu sieciowego w środowisku produkcyjnym, braku oceny zdolności do ciągłego zapewnienia poufności, braku oceny ryzyka uzyskania dostępu do panelu pracownika spółki oraz ryzyka naruszenia praw lub wolności osób, których dane spółka przetwarza.

Spółka nie podejmowała wystarczających działań mających na celu ocenę doboru środków technicznych i organizacyjnych przez pryzmat adekwatności do ryzyka. W związku z tym doszło do nieuprawnionego dostępu do danych klientów i do uzyskania około 2 200 000 danych osób przez osoby nieuprawnione. Prezes UODO uznał, że spółka nie zapewniła odpowiednich procedur reagowania na wypadek pojawiania się nietypowego ruchu w sieci. Nakładając karę, Prezes UODO stwierdził, że naruszenie, do jakiego doszło, miało znaczną wagę i poważny charakter oraz dotyczyło dużej liczby osób. W wyniku naruszenia powstało wysokie ryzyko negatywnych skutków dla osób, których dane dostały się w niepowołane ręce, w tym między innymi ryzyko tzw. kradzieży ich tożsamości. W większości przypadków były to takie dane jak: imię i nazwisko, numer telefonu, e-mail oraz adres do doręczeń. Dodatkowe środki zabezpieczenia technicznego spółka wdrożyła już po stwierdzeniu naruszenia.

[23] Dz. U. z 2020 r. poz. 256 z późn. zm.
[24] sygn. akt: ZSPR.421.2.2019.

Spółka złożyła do Naczelnego Sądu Administracyjnego skargę kasacyjną zaskarżając w całości wyrok WSA.

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

Prezes UODO w roku 2020 rozstrzygał w sprawach dotyczących przetwarzania danych osobowych w kwestiach, które wielokrotnie były już przedmiotem postępowań w latach ubiegłych. Zmiana stanu prawnego, do której doszło za sprawą rozporządzenia 2016/679, spowodowała zarówno wzrost liczby skarg, jak i konieczność stawienia czoła nowym wyzwaniom, zarówno po stronie administratorów, jak i po stronie organu nadzorczego. 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 składali, zwłaszcza gdy kontakt z administratorem był dla nich utrudniony.

[25] tj. Dz. U. z 2018 r. poz. 2096 z późn. zm., dalej jako: K.p.a.

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 2019 roku, skarżący powielali błędy w zakresie wymogów formalnych w składanych przez nich pismach. Najczęściej skarżący wzywani byli do doprecyzowania żądania mieszczącego się w zakresie kompetencji przysługujących Prezesowi UODO, gdyż większość z nich wnosiła m.in. o samo wszczęcie postępowania w sprawie, nie wskazując podjęcia jakich działań w sprawie domagają się od Prezesa UODO. Skarżący wnosili o stwierdzenie, czy doszło do naruszenia ich prawa do ochrony danych osobowych, o przeprowadzenie kontroli w stosunku do skarżonego podmiotu, o nałożenie administracyjnej kary pieniężnej, o ustalenie podmiotu, który dopuszcza się naruszenia ich prawa do ochrony danych osobowych, a także wypłaty odszkodowania/zadośćuczynienia. Ponadto wnioskodawcy wzywani byli 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 było przez skarżących za pomocą środków komunikacji elektronicznej (ePUAP). Wnioskodawcy bowiem błędnie przyjmują, że samo podpisanie podania kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym, powinno pozwolić zidentyfikować ich jako strony postępowania**.** Skarżący zostali 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 byli do podania administratorów i linków stron internetowych. Sprawy, w których nie zostały usunięte braki formalne, pozostawione były bez rozpoznania.

W roku 2020 Prezes Urzędu Ochrony Danych Osobowych wydał 1866 decyzji administracyjnych, tj. o 497 więcej w stosunku do roku 2019, w którym wydanych było 1369 decyzji.

4.1. Skargi

Rozpatrywanie skarg jest jednym z głównych zadań organu nadzorczego, zgodnie z art. 57 ust. 1 lit. f RODO. Biorąc pod uwagę, że liczba skarg wpływających do Urzędu Ochrony Danych Osobowych w przedmiocie nieprawidłowości w procesie przetwarzania danych osobowych

gwałtownie wzrosła po 25 maja 2018 r., kluczowa była sprawna obsługa obywateli w tym zakresie. Zmiany w strukturze organizacyjnej Urzędu były konsekwencją doświadczeń wynikających z funkcjonowania w latach 2018 – 2019 zespołów tematycznych, które poza rozpatrywaniem skarg zajmowały się również opiniowaniem projektów aktów prawnych, działalnością edukacyjną, prowadzeniem kontroli, obsługą zgłaszanych przez administratorów naruszeń oraz innymi zadaniami. Podział spraw na sektory tematyczne okazał się działaniem w dobrym kierunku, dlatego chcąc zwiększyć efektywność prowadzonych postępowań w Urzędzie Ochrony Danych Osobowych, podjęto decyzję o stworzeniu Departamentu Skarg, a w ramach niego utworzono cztery wydziały tematyczne:

Wydział ds. Sektora Publicznego;

Wydział ds. Sektora Prywatnego;

Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa;

Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji.

Głównym zadaniem Departamentu Skarg i wchodzących w jego skład Wydziałów jest rozpatrywanie skarg na nieprawidłowości w procesie przetwarzania danych osobowych. Rok 2020 był pierwszym pełnym rokiem funkcjonowania Departamentu Skarg w strukturach Urzędu Ochrony Danych Osobowych.

W roku 2020 do Urzędu Ochrony Danych Osobowych wpłynęły w sumie **6442 skargi**. Postępowania zakończono w 6692 sprawach, z czego 1401 zakończono wydaniem decyzji administracyjnej. Jednocześnie do Urzędu wpłynęło 50 skarg, które zostały zakwalifikowane jako transgraniczne i przekazane wiodącemu organowi nadzorczemu, natomiast 10 skarg otrzymano od organów nadzorczych, dla których to postępowań organem wiodącym był Prezes UODO.

Liczba skarg, które w analizowanym okresie sprawozdawczym 2020 r. wpłynęły do UODO, z podziałem na sektory, przedstawia się następująco:

1303 skargi na podmioty sektora publicznego;

2519 skarg na podmioty sektora prywatnego;

926 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa;

1694 skargi na podmioty sektora finansowego, ubezpieczeń i telekomunikacji.

4.1.1. Sektor publiczny

Spośród 6442 skarg, które w 2020 r. wpłynęły do Urzędu, **1303** z nich dotyczyło podmiotów sektora publicznego. Poniżej omówione zostały przykłady kilku takich skarg.

Udostępnianie danych przez instytucje publiczne

W analizowanym 2020 r. organ właściwy do spraw ochrony danych osobowych odnotowywał skargi dotyczące kwestii przetwarzania i upubliczniania wizerunku osób fizycznych bez ich zgody.

Przedmiotem jednej ze skarg było opublikowanie w biuletynie Powiatowego Urzędu Pracy, w artykule dotyczącym współpracy tego urzędu z zakładem karnym, wizerunku skarżącego bez jego zgody. Skarżący wskazał, że wbrew twierdzeniom administratora danych, nie wyrażał zgody na przetwarzanie danych osobowych w zakresie jego wizerunku.

Jak ustalono, Powiatowy Urząd Pracy (PUP) opublikował w biuletynie informacyjnym o rynku pracy zbiorowe zdjęcie osób, które uczestniczyły w zajęciach organizowanych dla osób odbywających karę pozbawienia wolności, wśród których znajdował się również skarżący.

Zgodnie z art. 85 ust. 1 RODO państwa członkowskie zobowiązane są do przyjęcia przepisów pozwalających pogodzić prawo do ochrony danych osobowych na mocy RODO z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej. Prezes UODO wskazał, że na podstawie powyższego przepisu, prawodawca polski w art. 2 pkt 1 ustawy o ochronie danych osobowych[26], ograniczył stosowanie przepisów RODO (tzn. wyłączył stosowanie następujących przepisów tego rozporządzenia: art. 5-9, art. 11, art. 13-16, art. 18-22, art. 27, art. 28 ust. 2-10 oraz art. 30) w odniesieniu do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu Prawa prasowego[27], a także do wypowiedzi w ramach działalności literackiej lub artystycznej. Zwrócił uwagę, że art. 17 ust. 3 lit. a RODO stanowi, iż prawo do usunięcia danych nie ma zastosowania w przypadku, gdy przetwarzanie danych osobowych jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji. Tryb postępowania w sprawach prasowych, w tym dotyczący zarówno postępowania cywilnego, jak i karnego, uregulowany został w rozdziale 8 Prawa prasowego. O tym, czy w konkretnym przypadku opublikowanie materiału prasowego nastąpiło z naruszeniem prawa, orzekają właściwe rzeczowo i miejscowo sądy powszechne.

[26] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. z 2019 r. poz. 1781 z późn. zm.
[27] Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe, Dz. U. z 2018 r. poz. 1914.

Odnosząc się do kwestii rozpowszechniania wizerunku w biuletynie informacyjnym o rynku pracy, Prezes UODO w swoim rozstrzygnięciu przytoczył art. 81 ust. 1 ustawy o prawie autorskim i prawach pokrewnych[28], który stanowi, że rozpowszechnianie wizerunku wymaga zgody osoby na nim przedstawionej. W przypadku braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. Istotną kwestię stanowi problematyka udowodnienia uzyskania zgody od osoby, której wizerunek ma być rozpowszechniany. Prezes UODO w wydawanych decyzjach zawsze podkreśla, że istnienia zgody uprawnionego oraz jej zakresu nie domniemywa się. Skarżony podmiot ma obowiązek wykazać, że uzyskał zgodę uprawnionego na rozpowszechnianie jego wizerunku w oznaczonych warunkach[29]. Sąd Apelacyjny w Warszawie w wyroku z dnia 3 października 2018 roku[30] stwierdził, że zgoda osoby na rozpowszechnianie jej wizerunku w mediach musi zostać udzielona wyraźnie i nie może być domniemywana. Musi być udzielona wprost oraz w sposób niewątpliwy. Powinna określać warunki i płaszczyzny dopuszczalnego wykorzystania wizerunku. Zgodę można wyrazić też ustnie, jednak okoliczność jej udzielenia musi wówczas zostać wykazana na podstawie dowodów. Art. 4 pkt. 11 RODO wymaga, aby oświadczenie o zgodzie było dobrowolne, konkretne, świadome i jednoznaczne. Pozyskując zgodę w formie pisemnej (np. z wykorzystaniem wydrukowanego formularza, który podpisuje podmiot danych) administrator może łatwo udowodnić, że uzyskał zgodę osoby, której dane dotyczą. Korzystając z innych sposobów pozyskiwania zgody, administrator danych powinien zadbać o to, aby móc udowodnić fakt uzyskania zgody (np. odbierając oświadczenie o zgodzie w ramach rozmowy telefonicznej, a treść rozmowy powinna zostać utrwalona).

Również w przypadku wyciągania wniosku o udzielonej zgodzie z „wyraźnego działania potwierdzającego" na administratorze ciąży obowiązek zapewnienia możliwości wykazania, że osoba, której dane dotyczą, wyraziła zgodę. Może to wymagać utrwalenia informacji o istotnych okolicznościach gromadzenia danych, z których wynika, że osoby, których dane dotyczą, zostały poinformowane o tym, iż określone ich działania będą oznaczały zgodę na przetwarzanie danych[31]. Należy podkreślić, że zgodnie z zasadą przejrzystości wyrażoną w art. 5 RODO, przed uzyskaniem zgody cel przetwarzania danych nie może zostać określony ogólnie i blankietowo, ponieważ wtedy

[28] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz. U. z 2019 r. poz. 1231.
[29] Sieńczyło-Chlabicz Joanna. 7.3.2. Treść zgody. [w]: „Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna". Kantor Wydawniczy Zakamycze, 2006.
[30] Sygn. akt V ACa 655/17.
[31] P. Fajgielski, Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 7.

zgoda nie zostanie wyrażona w sposób świadomy, a w konsekwencji będzie bezskuteczna. Organ wskazał również, że prawodawca unijny, powielając wzorce przyjęte w dyrektywie 95/46/WE, w omawianej materii zdecydował się na przyjęcie modelu opt-in (konieczność aktywnego działania), a więc ustanowił wymóg uzyskania zgody, natomiast nie dopuścił praktyki zakładającej, że brak sprzeciwu oznacza zgodę na przetwarzanie danych[32]. Ponadto Grupa Robocza Art. 29 przyjęła 29.11.2017 r. Wytyczne dotyczące zgody (WP 259), w ramach których wskazano, że zgoda musi być świadoma. Aby uznać, że zgoda jest świadoma, osoba, której dane mają być przetwarzane, powinna być świadoma konsekwencji wyrażenia zgody także co do swoich praw, które powinny być jej przedstawione poprzez spełnienie obowiązku informacyjnego z art. 13 lub 14 RODO. Prezes Urzędu Ochrony Danych Osobowych uznaje, że nieważna jest zgoda, która nie jest dobrowolna, świadoma, konkretna oraz jednoznaczna. Z materiału dowodowego zgromadzonego w sprawie wynikało, że zgoda skarżącego nie spełniała ww. wymogów, a zatem była nieważna.

Biorąc pod uwagę działania administratora, który usunął zdjęcie wykonane skarżącemu oraz zanonimizował jego wizerunek znajdujący się w biuletynie informacyjnym o rynku pracy, którego jest on wydawcą, Prezes Urzędu Ochrony Danych Osobowych udzielił administratorowi upomnienia za naruszenie przepisów o ochronie danych osobowych[33].

Przetwarzanie danych osobowych na stronach Biuletynu Informacji Publicznej

W analizowanym okresie sprawozdawczym do organu właściwego do spraw ochrony danych osobowych zgłaszano skargi dotyczące udostępnienia danych osobowych na stronach internetowych Biuletynu Informacji Publicznej.

W jednej z takich spraw skarżący podniósł zarzut udostępnienia przez organ administracji publicznej, na stronie internetowej Biuletynu Informacji Publicznej, jego danych osobowych w zakresie imienia i nazwiska zawartych w uchwałach administracji publicznej, podjętych po rozpatrzeniu jego wniosków o stwierdzenie nieważności postępowań konkursowych na stanowisko kierownicze w podmiotach leczniczych podległych samorządowi województwa, w których brał udział, zorganizowanych na podstawie art. 41 ust. 2 pkt 6 ustawy o samorządzie województwa[34] w związku z art. 46 ust. 3 i art. 49 ust. 1 pkt 1 ustawy o działalności leczniczej[35] w związku z § 8 ust. 1 i ust. 2 oraz § 12 ust. 1 i ust. 2 rozporządzenia Ministra Zdrowia z dnia 6 lutego 2012 r. w sprawie

[32] P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 (….) op.cit.
[33] ZWOS.440.5297.2019.
[34] Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa, Dz.U. z 2019 r. poz. 512 z późn. zm.
[35] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, Dz. U. z 2018 r. poz. 2190 z późn. zm.

sposobu przeprowadzania konkursu na niektóre stanowiska kierownicze w podmiocie leczniczym niebędącym przedsiębiorcą[36].

Przepisy ustawy o działalności leczniczej i ww. rozporządzenia Ministra Zdrowia nie zawierają regulacji dotyczących udostępniania informacji publicznej w związku ze stwierdzaniem nieważności postępowania konkursowego. Dlatego kwestię tę należało rozpatrzyć na podstawie przepisów ustawy o dostępie do informacji publicznej[37], z uwzględnieniem wyłączenia określonego w jej art. 5 ust. 2. Artykuł 6 ust. 1 pkt 3 lit. g ustawy o dostępie do informacji publicznej stanowi, że udostępnieniu podlega informacja publiczna, w szczególności o zasadach funkcjonowania podmiotów, o których mowa w art. 4 ust. 1, w tym o naborze kandydatów do zatrudnienia na wolne stanowiska, w zakresie określonym w przepisach odrębnych. W myśl art. 4 ust. 1 ww. ustawy obowiązane do udostępniania informacji publicznej są władze publiczne oraz inne podmioty wykonujące zadania publiczne. W myśl § 12 ust. 3 ww. rozporządzenia Ministra Zdrowia kandydat zgłaszający się do konkursu składa oświadczenie, że wyraża zgodę na przetwarzanie danych osobowych w celach przeprowadzania postępowania konkursowego na dane stanowisko. W rozpatrywanej sprawie skarżący wyraził zgodę na przetwarzanie jego danych osobowych w celach przeprowadzenia dwóch postępowań konkursowych na stanowisko dyrektora w szpitalach.

Wydając rozstrzygnięcie w przedmiotowej sprawie Prezes UODO zaznaczył, że dane osobowe skarżącego w kwestionowanych uchwałach organu administracji publicznej nie zostały udostępnione w związku z postępowaniami konkursowymi na stanowisko publiczne (na co skarżący wraził zgodę), lecz po ich zakończeniu i rozpatrzeniu jego wniosków o unieważnienie tych postępowań. Zgodnie z § 8 ust. 2 w zw. z § 8 ust. 1 ww. rozporządzenia Ministra Zdrowia, o stwierdzenie nieważności ww. postępowania konkursowego może wystąpić nie tylko kandydat na stanowisko objęte konkursem, ale każdy, kto wykaże, że jego interes prawny został naruszony w toku postępowania konkursowego.

W ocenie Prezesa UODO dla spełnienia obowiązku wynikającego z ustawy o dostępie do informacji publicznej nie było niezbędne udostępnienie w uchwale organu administracji publicznej imienia i nazwiska osoby wnioskującej o unieważnienie postępowania konkursowego. Przy upublicznieniu uchwał jedynie w celu informacyjnym zbędne było (nieadekwatne do celu) ujawnianie imienia i nazwiska skarżącego. Podkreślenia wymaga, że publikacja dokumentu zawierającego dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych. W sprawie

[36] Dz. U. poz. 182 z późn. zm.
[37] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. z 2019 r. poz. 1429.

rozpatrywanej przed Prezesem UODO oznaczało to, że uchwały administracji publicznej mogły być upublicznione po uprzednim usunięciu z nich danych osobowych skarżącego w zakresie imienia i nazwiska. Zgodnie z zasadą minimalizacji danych, określoną 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.

Prezes UODO stwierdził, że przetwarzanie przez organ administracji publicznej danych osobowych skarżącego w postaci imienia i nazwiska poprzez ich udostępnienie w Biuletynie Informacji Publicznej w uchwałach podjętych po rozpatrzeniu jego wniosków o stwierdzenie nieważności postępowań konkursowych, było sprzeczne z zasadą minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c RODO. W ocenie Prezesa UODO nie znajdowało również uzasadnienia w przesłankach określonych w art. 6 ust. 1 RODO. Biorąc pod uwagę, że w wyniku ustaleń poczynionych w toku postępowania w niniejszej sprawie stwierdzono, że dane osobowe skarżącego zawarte we wskazanych uchwałach zostały zanonimizowane, Prezes UODO, uwzględniając wagę i charakter stwierdzonego naruszenia, udzielił administratorowi upomnienia za stwierdzone naruszenie[38]. Skarżący od ww. rozstrzygnięcia złożył skargę do Wojewódzkiego Sądu Administracyjnego, która została następnie oddalona przez Sąd[39].

W analizowanym okresie sprawozdawczym do Prezesa UODO kierowane były również skargi dotyczące publikowania na stronie internetowej Biuletynu Informacji Publicznej danych osobowych w związku z publikacją petycji, oraz danych osobowych radnych, którzy złożyli interpelacje i zapytania do wójta (burmistrza, prezydenta) w sprawach dotyczących gminy.

Zgodnie z art. 24 ust. 3 ustawy o samorządzie gminnym[40] w sprawach dotyczących gminy radni mogą kierować interpelacje i zapytania do wójta. Interpelacje i zapytania składa się w trybie określonym w art. 24 ust. 4-6. Stosownie do art. 24 ust. 7 ww. ustawy treść interpelacji i zapytań oraz udzielonych odpowiedzi podawana jest do publicznej wiadomości poprzez niezwłoczną publikację w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty. Ustawodawca w art. 4 ust. 1 ustawy o dostępie do informacji publicznej zobowiązuje podmioty publiczne i inne wykonujące zadania publiczne do udostępniania informacji publicznej w BIP (art. 7 ust. 1 pkt 1 ww. ustawy). Ograniczenia prawa do przedmiotowej publikacji wynikają z przepisów o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo

[38] ZSPU.440.718.2018.
[39] Sygn. akt II SA/Wa 768/20.
[40] Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz. U. z 2019 r. poz. 506.

chronionych (art. 5 ust. 1 ustawy o dostępie do informacji publicznej), a także ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy (art. 5 ust. 2 zdanie pierwsze ww. ustawy).

Prezes UODO zwrócił uwagę, że powyższe regulacje, zobowiązujące do publikacji interpelacji i zapytań złożonych przez radnych w sprawach gmin, nie określają kategorii danych osobowych, jakie mogą być udostępniane o osobie ją wnoszącej. Do określenia tego zakresu zastosowanie znajdują przepisy RODO. Przy udostępnianiu danych osobowych należy zwrócić szczególną uwagę, aby zostały zachowane zasady określone w art. 5 ust. 1 RODO. W swoich rozstrzygnięciach Prezes UODO wskazywał, że organ administracji publicznej, jako administrator danych osobowych publikowanych w Biuletynie Informacji Publicznej, przy publikacji interpelacji i zapytań wnoszonych przez radnego, w których zawarte są dane osobowe wnoszącego, jest zobowiązany do dokonania oceny zarówno zasadności upubliczniania tych danych, ich zakresu, jak i określenia dalszej retencji (zgodnie z art. 5 ust. 1 lit. b oraz lit. c RODO). W świetle art. 5 ust. 1 lit. b RODO dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczenia celu). Jednocześnie w myśl art. 5 ust 1 lit. c RODO administrator jest każdorazowo zobowiązany do ustalenia zależności między celem a zakresem przetwarzania danych oraz powinien ograniczyć przetwarzanie danych jedynie do tych, które są niezbędne do osiągnięcia celu (zasada minimalizacji danych). Wskazany przepis wymaga, aby cel zbierania danych był również prawnie uzasadniony, co należy rozumieć jako jego zgodność z prawem, w odniesieniu do całego systemu prawnego i innych norm regulujących działalność administratora. W świetle art. 6 ust. 4 RODO przetwarzanie danych w celu innym niż cel, w którym zostały one zebrane, może odbywać się na podstawie zgody osoby, której dane dotyczą, albo 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. W konsekwencji przy publikacji danych osobowych na stronach Biuletynu Informacji Publicznej organ administracji publicznej nie powinien kierować się automatyzmem. Prezes UODO w rozstrzyganej sprawie wskazał, że upublicznienie przez burmistrza interpelacji i zapytań radnego zawierającego jego dane osobowe w postaci adresu zamieszkania należy uznać za przetwarzanie w zakresie zbędnym dla osiągnięcia celu, jakim było opublikowanie przedmiotowych interpelacji i zapytań w Biuletynie Informacji Publicznej z uwagi na art. 24 ust. 7 ustawy o samorządzie gminnym, który stanowi o obowiązku podawania jedynie „treści interpelacji i zapytań oraz udzielonych odpowiedzi”.

Wobec powyższego Prezes UODO uznał opublikowanie na stronie internetowej Biuletynu Informacji Publicznej adresu zamieszkania radnego w treści złożonej przez niego interpelacji za przetwarzanie z naruszeniem zasad określonych w art. 5 ust. 1 lit. b oraz c RODO. Biorąc pod uwagę, że na skutek złożenia skargi do Prezesa UODO przez radnego, burmistrz usunął adres zamieszkania radnego z treści interpelacji opublikowanej na stronie Biuletynu Informacji Publicznej, Prezes UODO, uwzględniając wagę i charakter stwierdzonego naruszenia, udzielił burmistrzowi upomnienia na podstawie art. 58 ust. 2 lit. b RODO[41].

W innej sprawie, zgodnie z art. 8 ust. 1 ustawy o petycjach[42], na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego, niezwłocznie zamieszcza się informację zawierającą odwzorowanie cyfrowe (skan) petycji, datę jej złożenia oraz – w przypadku wyrażenia zgody, o której mowa w art. 4 ust. 3 – imię i nazwisko albo nazwę podmiotu wnoszącego petycję lub podmiotu, w interesie którego petycja jest składana. Zgodnie zaś z art. 4 ust. 3 ustawy o petycjach może ona zawierać zgodę na ujawnienie danych osobowych podmiotu wnoszącego petycję na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego. Petycja zawierać musi m.in. oznaczenie podmiotu, który wnosi petycję (art. 4 ust. 2 pkt 1) oraz jego miejsce zamieszkania lub siedzibę (art. 4 ust. 2 pkt 2).

Kwestia udostępniania danych osobowych wnoszącego petycję została uregulowana w art. 8 ust. 1 ww. ustawy. Artykuł ten określa wprost, że jedynymi danymi osobowymi wnoszącego petycję, umieszczanymi na stronie internetowej przez podmiot właściwy do rozpatrzenia petycji – pod warunkiem wyrażenia zgody wnoszącego petycję na powyższe – jest imię i nazwisko. Wobec powyższego podmiot rozpatrujący petycję ma obowiązek niezwłocznego umieszczenia na stronie internetowej Biuletynu Informacji Publicznej informacji zawierającej cyfrowe odwzorowanie petycji (skan), datę jej złożenia oraz (w przypadku wyrażenia zgody, o której mowa w art. 4 ust. 3 ww. ustawy) imię i nazwisko wnoszącego petycję.

Po przeprowadzeniu postępowania wyjaśniającego w sprawie Prezes UODO stwierdził, że wójt legitymował się podstawą prawną do przetwarzania danych osobowych osoby, która wniosła petycję, na stronie internetowej Biuletynu Informacji Publicznej na podstawie art. 4 ust. 3 w zw. z art. 8 ust. 1 ustawy o petycjach, tylko w zakresie imienia i nazwiska. Jednocześnie wójt nie posiadał podstawy prawnej do udostępnienia takich danych osobowych, jak adres zamieszkania osoby wnoszącej petycję. Działanie to naruszyło zasadę zgodności z prawem i tym samym przepis art. 6 ust. 1 RODO.

[41] ZSPU.440.553.2019.
[42] Ustawa z dnia 11 lipca 2014 r. o petycjach, Dz. U. z 2018 r. poz. 870.

Biorąc pod uwagę podjęte przez administratora danych czynności naprawcze skutkujące usunięciem stwierdzonego uchybienia w procesie przetwarzania danych osobowych, Prezes UODO, uwzględniając wagę i charakter stwierdzonego naruszenia, udzielił wójtowi upomnienia na podstawie art. 58 ust. 2 lit. b RODO[43].

Przetwarzanie danych osobowych przez administratora w celu innym niż cel, do którego dane te zostały pozyskane

Do Urzędu Ochrony Danych Osobowych wpłynęła **skarga dotycząca doręczenia korespondencji zawierającej decyzję administracyjną osobie niebędącej stroną postępowania administracyjnego**. Głównym zarzutem było przetwarzanie przez organ publiczny danych osobowych skarżącej w zakresie imienia i nazwiska oraz adresu zamieszkania bez podstawy prawnej oraz niezrealizowania wobec niej obowiązku informacyjnego.

Podając motywy rozstrzygnięcia Prezes UODO wskazał, że dane osobowe w każdym przypadku muszą być przetwarzane przez administratora zgodnie ze wszystkimi zasadami określonymi w art. 5 RODO, w tym m.in. z tzw. zasadą legalności oraz zasadą ograniczonego celu. Zasada legalności mówi, że dane osobowe muszą być przetwarzane przez administratora zgodnie z prawem, tj. na podstawie przynajmniej jednej z przesłanek określonych w art. 6 RODO. Z uwagi na konstytucyjnie uregulowaną zasadę legalizmu, według której organy władzy publicznej działają na podstawie i w granicach prawa, w niniejszej sprawie istotne znaczenie miał art. 6 ust. 1 lit. c RODO. Z ww. przepisu wynika, że przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Natomiast z zasady ograniczonego celu wynika, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Postępowanie administracyjne prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych wykazało, że organ publiczny wykorzystał dane osobowe skarżącej w zakresie imienia i nazwiska oraz adresu zamieszkania w celu dostarczenia korespondencji dla jej ojca, bez podstawy prawnej (niezgodnie z celem, w związku z którym te dane zostały zebrane). Skarżąca nie była stroną postępowania w sprawie, w której została wydana doręczona jej decyzja. Przesyłka zawierająca egzemplarz ww. decyzji była przeznaczona dla ojca skarżącej, lecz została zaadresowana na skarżącą. W toku sprawy nie ustalono, aby skarżąca została ustanowiona pełnomocnikiem swojego ojca.

[43] ZSPU.440.587.2019.

Skarżony organ w złożonych wyjaśnieniach wskazał, że uzyskał dane osobowe skarżącej w zakresie imienia i nazwiska oraz adresu zamieszkania w związku z wykonaniem przez skarżącą przelewu bankowego, zrealizowanego w celu uregulowania w imieniu jej ojca terminowej należności – opłaty za odpady komunalne. Prezes UODO podkreślił ponadto, że stosownie do art. 5 ust. 1 lit. b RODO, dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu). Cel, w jakim administrator zbiera dane osobowe, musi być konkretny, tj. realnie istniejący i precyzyjnie określony i wyraźny, czyli dający się łatwo i jednoznacznie zrozumieć. Co więcej, wskazany cel musi być prawnie uzasadniony, zatem oparty na obiektywnie dających się usprawiedliwić przesłankach. Mając powyższe na uwadze, za cel przetwarzania danych osobowych skarżącej w zakresie imienia i nazwiska oraz adresu przez skarżony organ należy uznać potwierdzenie realizacji czynności bankowych przez skarżącą. Wobec powyższego wykorzystanie przez skarżony organ danych osobowych skarżącej, pozyskanych z informacji przelewu bankowego, w celu skierowania do niej korespondencji zawierającej pismo, której nie była adresatem, było nieprawidłowe. Wykorzystanie tych danych w powyższym celu było niezgodne z celem, dla którego dane te zostały pozyskane, a zarazem brak było jakiejkolwiek podstawy prawnej do ich przetwarzania przez skarżony organ w celu doręczenia korespondencji przeznaczonej dla jej ojca. Prezes UODO, uwzględniając wagę i charakter stwierdzonego naruszenia, udzielił administratorowi upomnienia na podstawie art. 58 ust. 2 lit. b RODO za naruszenie przepisów o ochronie danych osobowych[44].

Prawo dostępu do danych osobowych przysługujące osobie, której dane dotyczą

W analizowanym okresie sprawozdawczym do Prezesa UODO kierowane były skargi dotyczące niedopełnienia obowiązku informacyjnego (art. 15 RODO[45]) wobec osoby, której dane dotyczą, oraz niedostarczenia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu przez administratora.

Przedmiotem jednej z rozpatrywanych spraw była skarga na nieprawidłowości w procesie przetwarzania danych osobowych, polegające na niewypełnieniu obowiązku informacyjnego określonego w art. 15 RODO względem osoby, której dane dotyczą, w tym nieudostępnieniu kopii danych osobowych przez Ministra Środowiska. Żądanie

[44] DS.523.1686.2020.
[45] 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, Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.

spełnienia obowiązku informacyjnego było kierowane do administratora kilkukrotnie w krótkich odstępach czasu.

Przyjęte na gruncie RODO regulacje prawne, przeciwnie do przepisów uchylonej ustawy o ochronie danych osobowych z 1997 r., nie zawierają ograniczeń w zakresie uprawnień informacyjnych poprzez określenie, że podmiot danych jest uprawniony do skorzystania z nich nie częściej niż raz na 6 miesięcy (art. 32 ust. 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[46]). Celem prawodawcy unijnego, przyznającego podmiotowi danych uprawnienia informacyjne, było zagwarantowanie mu prawa do kontroli przetwarzanych przez administratora jego danych osobowych. Prezes UODO zaznaczył, że prawo to nie powinno być jednakże nadużywane w taki sposób, aby mogło kolidować z pracą jednostki i wpływać na jej funkcjonowanie, czym niewątpliwie jest składanie przez tę samą osobę kilku wniosków w krótkim odstępie czasu. W związku z tym, że w toku postępowania ustalono, że Minister udzielił skarżącemu, na jego wniosek, wyczerpującej odpowiedzi dotyczącej przetwarzania jego danych osobowych, w ocenie Prezesa Urzędu Ochrony Danych Osobowych nie było konieczności ponownego udzielenia skarżącemu informacji o przetwarzaniu jego danych w niespełna 10 dni po ich udzieleniu.

W rozstrzygnięciu Prezes UODO wskazał również, że na podstawie art. 15 ust. 3 RODO administrator, dostarczając osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu, nie ma obowiązku udostępniania osobie zainteresowanej nośnika, na którym przetwarzane są dane osobowe, ani tych zawartych na nim danych, które nie stanowią danych osobowych w rozumieniu art. 4 pkt 1 RODO, ani danych, które nie dotyczą wnioskującego. Realizując obowiązek wynikający z art. 15 ust. 3 RODO, administrator może poprzestać na podaniu treści danych dotyczących osoby, z wyłączeniem pozostałych informacji zawartych na nośniku. Wykonanie ww. obowiązku może być realizowane zarówno poprzez sporządzenie kopii lub odpisu dokumentu (nośnika) zawierającego dane osobowe wnioskującego oraz inne dane, jak i poprzez podanie uprawnionemu treści jego danych osobowych, z pominięciem pozostałych informacji znajdujących się na nośniku. Osoba, której dane dotyczą, ma prawo zwrócić się do administratora o udostępnienie kopii jej danych osobowych, które są przez niego przetwarzane. Brak jest natomiast podstaw do żądania wydania kopii nośnika, na którym te dane się znajdują. Prezes UODO wskazał, że osoba, której dane dotyczą, nie jest ponadto uprawniona do żądania innych niż dotyczących jej danych osobowych. Z akt analizowanej sprawy wynikało, że obowiązek informacyjny określony

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

w art. 15 ust. 3 RODO nie został przez Ministra w stosunku do skarżącego spełniony, dlatego Prezes UODO nakazał Ministrowi Środowiska wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego poprzez spełnienie wobec niego obowiązku informacyjnego określonego w art. 15 ust. 3 RODO[47].

Przetwarzanie danych osobowych w Krajowym Systemie Informacyjnym Policji

Prezes UODO odnotowuje skargi dotyczące nieprawidłowości w procesie przetwarzania danych osobowych w Krajowym Systemie Informacji Policyjnej (KSIP), prowadzonym przez Komendanta Głównego Policji w Warszawie. Skarżący w tego rodzaju sprawach przede wszystkim kwestionowali zasadność odmowy usunięcia ich danych z KSIP.

W swoich rozstrzygnięciach Prezes UODO wskazywał, że zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, zostały określone w ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[48]. W myśl przepisów ww. ustawy Komendant Główny Policji może przetwarzać dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnień bądź spełnienia obowiązków wynikających z przepisów prawa. Zakres uprawnień oraz ustawowych zadań organów Policji został określony w ustawie o Policji[49]. Do podstawowych zadań ustawowych Policji należy m.in: ochrona bezpieczeństwa i porządku publicznego, inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców. W granicach zaś ustawowych zadań Policja wykonuje czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe w celu rozpoznawania, zapobiegania i wykrywania przestępstw, przestępstw skarbowych i wykroczeń[50].

Organy Policji są uprawnione do przetwarzania danych osobowych na podstawie art. 20 ust. 1 i 1c ustawy o Policji. Przepis ten stanowi podstawę do przetwarzania przez Policję nie tylko danych wrażliwych, ale również danych osobowych dotyczących wyroków skazujących

[47] ZSPU.440.730.2018.
[48] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz. U. z 2019 r. poz. 125.
[49] Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. z 2020 r. poz. 360.
[50] DS.523.1488.2020.

i czynów zabronionych, poprzez bezpośrednie odesłanie do art. 9 i 10 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)[51].

Prezes UODO zwraca jednak uwagę, że powyższe nie oznacza możliwości nieograniczonego w czasie przetwarzania przez organy Policji danych osobowych gromadzonych w KSIP. Na gruncie przepisów obowiązującej ustawy z dnia 14 grudnia 2018 r. przetwarzane dane osobowe podlegają okresowej weryfikacji i usunięciu w przypadku uznania za niecelowe dalsze ich przetwarzanie. Komendant Główny Policji ma obowiązek dokonywania weryfikacji danych osobowych nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji tych danych. Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne.

Prezes UODO jednocześnie podziela w pełni dotychczasowe stanowisko sądów administracyjnych podkreślające, że to organy Policji oceniają przydatność zebranych informacji zawierających dane osobowe, które są przetwarzane w związku z realizacją jej zadań ustawowych[52].

Należy również podkreślić, że organ ochrony danych osobowych wydaje nakaz usunięcia uchybień w procesie przetwarzania danych osobowych wówczas, gdy stwierdzi naruszenie norm prawnych w zakresie przetwarzania danych osobowych. Wystąpienie przesłanek legalizujących przetwarzanie warunkuje uznanie kwestionowanych czynności przetwarzania za zgodne z prawem. Wobec powyższego, w postępowaniu prowadzonym w ramach ustawy z dnia 14 grudnia 2018 r., Prezes UODO badał legalność procesów przetwarzania przez Policję danych osobowych w KSIP oraz realizację przez organy Policji obowiązku weryfikacji danych, określonego w art. 16 tej ustawy.

4.1.2. Sektor prywatny

Spośród 6442 skarg, które w 2020 r. wpłynęły do Urzędu, **2519** z nich dotyczyło podmiotów sektora prywatnego. Poniżej omówione zostały przykłady kilku takich skarg.

Upublicznienie danych osobowych mieszkańca wspólnoty mieszkaniowej w częściach wspólnych budynku

W roku 2020 Prezes Urzędu odnotował skargi dotyczące przetwarzania danych osobowych przez spółdzielnie oraz wspólnoty mieszkaniowe. Ocenie podlegała m.in. kwestia przetwarzania

[51] Dz. Urz. UE L 119 z 04.05.2016, str. 1.
[52] Zob. wyrok WSA w Warszawie z dnia 19 grudnia 2018 r. sygn. II SA/Wa 700/18; wyrok WSA w Warszawie z dnia 10 października 2017 r. sygn. akt: II SA/Wa 314/17.

danych osobowych w związku z zamieszczaniem na tablicach ogłoszeń znajdujących się w miejscach ogólnodostępnych (np. klatki schodowe budynków) danych osobowych członków spółdzielni lub wspólnot mieszkaniowych.

Przedmiotem jednego z postępowań było udostępnienie przez wspólnotę mieszkaniową danych osobowych jej członka (nazwiska) na tablicach ogłoszeń w budynku wspólnoty[53].

Z informacji zgromadzonych przez organ ds. ochrony danych osobowych wynikało, że skarżący i wspólnota są stronami kilku postępowań cywilnych z powództwa skarżącego przeciwko wspólnocie. W kwestionowanym przez skarżącego ogłoszeniu, umieszczonym na klatkach schodowych w budynku wspólnoty, zarząd wspólnoty informował mieszkańców o zbliżających się terminach rozpraw cywilnych z powództwa skarżącego przeciwko wspólnocie, posługując się przy tym nazwiskiem skarżącego oraz jednocześnie wskazując sygnatury spraw i określając sąd, przed którym sprawy te się toczą. Przy czym, w ocenie wspólnoty, posłużenie się w ogłoszeniu do członków wspólnoty jedynie nazwiskiem skarżącego, nie pozwalało na jego identyfikację jako konkretnej osoby fizycznej.

W stanie faktycznym analizowanej sprawy nazwisko skarżącego zostało ujawnione w kontekście bycia członkiem określonej wspólnoty mieszkaniowej i bycia uczestnikiem określonych postępowań sądowych przeciwko wspólnocie. Udostępniając nazwisko skarżącego, ujawniono jednocześnie, że jest on mieszkańcem określonej wspólnoty mieszkaniowej oraz powodem we wskazanych postępowaniach toczących się przed sądem.

W ocenie Prezesa UODO wskazane informacje pozwalały na identyfikację skarżącego jako konkretnej osoby fizycznej i wobec tego stanowiły dane osobowe w rozumieniu art. 4 pkt 1 RODO. Prezes UODO zwrócił przy tym uwagę, że dostęp do tablic informacyjnych znajdujących się na terenie wspólnoty mieszkaniowej mają nie tylko członkowie wspólnoty, ale także osoby postronne, jak np. osoby odwiedzające, roznoszące ulotki, czy świadczące usługi na rzecz mieszkańców.

W swoim rozstrzygnięciu Prezes UODO wskazał, że wspólnota powinna zastosować taki system wymiany informacji z jej członkami, by był on współmierny z celem przetwarzania danych osobowych oraz chronił dane osobowe przed dostępem osób nieuprawnionych. Ujawnienie danych osobowych skarżącego poprzez ich opublikowanie na tablicach ogłoszeń znajdujących się na terenie wspólnoty w ocenie organu nadzorczego UODO nie znajdowało oparcia w żadnej z przesłanek z art.

[53] ZSPU.440.369.2019.

6 ust. 1 RODO. Wobec powyższego Prezes UODO udzielił wspólnocie upomnienia za udostępnienie osobom nieuprawnionym bez podstawy prawnej danych osobowych skarżącego.

Upublicznienie danych osobowych zawartych w obwieszczeniu komornika o licytacji

Przedmiotem innej sprawy[54] było upublicznienie przez spółdzielnię danych osobowych członka spółdzielni mieszkaniowej poprzez zamieszczenie kopii „Obwieszczenia Komornika Sądowego o licytacji spółdzielczego własnościowego prawa do lokalu" na tablicach ogłoszeń w należących do spółdzielni budynkach. Prezes UODO dokonał analizy przepisów regulujących ochronę danych osobowych ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych[55], ustawy z dnia 16 września 1982 r. Prawo spółdzielcze[56] oraz przepisów ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego[57]. Zgodnie z przepisami kodeksu postępowania cywilnego (art. 955) obwieszczenie o licytacji należy co najmniej dwa tygodnie przed jej terminem ogłosić publicznie na stronie internetowej oraz tablicy ogłoszeń sądu sprawującego nadzór nad egzekucją z nieruchomości, w lokalu organu gminy właściwego ze względu na miejsce położenia nieruchomości oraz na stronie internetowej Krajowej Rady Komorniczej. Komornik może ponadto na wniosek i koszt strony zarządzić ogłoszenie również w inny wskazany przez nią sposób, w szczególności w dzienniku poczytnym w danej miejscowości. Przepisy określają więc precyzyjnie możliwe sposoby upubliczniania wiadomości o planowanej licytacji. Jeżeli więc Komornik Sądowy nie zarządzi na wniosek strony zamieszczenia ogłoszenia w inny wskazany przez nią sposób, a spółdzielnia mieszkaniowa nie jest w stanie wykazać innej podstawy prawnej upublicznienia danych osobowych zawartych w obwieszczeniu komornika o licytacji, takie upublicznienie nie znajduje uzasadnienia w żadnej z przesłanek legalizujących proces przetwarzania danych osobowych. Prezes UODO stwierdził, że spółdzielnia upubliczniając dane osobowe skarżącej w zakresie imienia i nazwiska oraz adresu zamieszkania zawarte w obwieszczeniu o licytacji komorniczej, naruszyła przepisy o ochronie danych osobowych. Nie działała bowiem zgodnie z zasadą „zgodności z prawem, rzetelności i przejrzystości", w myśl której dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a RODO) oraz z zasadą „ograniczonego celu", który stanowi, że dane mogą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (art. 5 ust.

[54] DS.523.781.2020.
[55] DZ.U. z 2020 r. poz. 1465.
[56] Dz.U. z 2020 r. poz. 275.
[57] Dz.U. z 2020 r. poz. 1575.

1 lit. b RODO). W związku z powyższym Prezes Urzędu udzielił spółdzielni – jako administratorowi danych osobowych skarżącej – upomnienia w związku z zaistniałą sytuacją.

Przetwarzanie wizerunku utrwalonego za pomocą monitoringu wizyjnego

Przedmiotem jednej ze spraw[58], zainicjowanej przez członka wspólnoty mieszkaniowej, była kwestia utrwalania, przeglądania oraz przesłania przez wspólnotę mieszkaniową do członków zarządu wspólnoty w wiadomościach e-mail jego danych osobowych w postaci wizerunku, w związku z funkcjonującym na terenie nieruchomości wspólnej wspólnoty systemem monitoringu wizyjnego. Dla możliwości oparcia przetwarzania danych osobowych na przepisie art. 6 ust. 1 lit. f RODO konieczne było wykazanie, iż administrator danych osobowych, przetwarzając dane, posiada „prawnie uzasadniony interes", który nie koliduje z podstawowymi prawami i wolnościami osoby, której dane dotyczą. Celem funkcjonowania systemu monitoringu wizyjnego na terenie nieruchomości wspólnej wspólnoty było zapewnienie bezpieczeństwa osób oraz mienia znajdującego się na jej terenie. Wspólnota wykazała także, że dane osobowe członka wspólnoty w postaci jego wizerunku, zarejestrowane przez system monitoringu, zostały wykorzystane dla celów zapewnienia bezpieczeństwa mieszkańcom budynku, w celu ustalenia sprawcy zdarzenia, w związku z powtarzającą się sytuacją zamykania na klucz drzwi przeciwpożarowych, będących częścią drogi ewakuacyjnej w budynku. Prezes UODO uznał, że przekazanie danych osobowych w wiadomości e-mail skierowanej do członków zarządu, którzy zgodnie z regulaminem funkcjonowania monitoringu byli uprawnieni do jego przeglądania, nie naruszyło przepisów o ochronie danych osobowych. Z uwagi jednak na treść przepisu art. 5 ust. 1 lit. e RODO, który stanowi, że 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, oraz na fakt, iż cel, dla którego wspólnota mieszkaniowa przetwarzała dane osobowe swojego członka w postaci jego wizerunku, został osiągnięty, nakazał wspólnocie wyeliminowanie nieprawidłowości w przetwarzaniu danych osobowych skarżącego poprzez usunięcie tych danych, zawartych w wiadomości e-mail skierowanej do członków zarządu wspólnoty, ze skrzynki poczty elektronicznej.

[58] ZSPU.440.514.2019.

Przetwarzanie danych w celach marketingowych

W 2020 r. przedmiotem wpływających do UODO skarg było przetwarzanie danych w celach marketingowych. Najczęściej skarżący wskazywali na otrzymywanie połączeń telefonicznych od nieznanych im wcześniej podmiotów i notoryczne otrzymywanie niechcianych wiadomości e-mail o charakterze marketingowym, gdy nie posiadali wiedzy o źródle pozyskania ich danych przez te podmioty. Nie w każdym bowiem przypadku pozyskanie danych następuje bezpośrednio od osoby, której dane dotyczą. Sytuacje takie skutkowały zazwyczaj wnioskiem o dostęp do danych[59], wydaniem ich kopii [60] lub ich usunięciem[61]. Powyższe wynika z faktu, że osoby, których dane dotyczą, nabierają podejrzeń, co do legalności przetwarzania ich danych osobowych przez administratorów. Wskazać należy, że podstawę prawną do prowadzenia tego typu działań stanowi najczęściej art. 6 ust. 1 lit. f rozporządzenia 2016/679[62], tj. uzasadniony interes[63] administratorów danych w prowadzeniu działań marketingowych. W motywie 47 rozporządzenia 2016/679 wskazane jest, że za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego. Działania marketingowe można także prowadzić na podstawie zgody[64] uzyskanej od osoby, której dane dotyczą. Odnosi się to zwłaszcza do partnerów handlowych podmiotów, które dane pozyskały, gdy zgoda ta obejmuje udostępnienie danych osobowych w celach prowadzenia marketingu na ich rzecz. W przypadku marketingu trzeba jednak mieć na uwadze, że podmioty danych mają prawo do skorzystania z przysługujących im na

[59] Zgodnie z art. 15 rozporządzenia 2016/679 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 przewidzianych w omawianym artykule informacji.

[60] Zgodnie z art. 15 ust. 3 rozporządzenia 2016/679, cyt.: *Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej*.

[61] Zgodnie z art. 17 ust. 1 rozporządzenia 2016/679, 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 przewidzianych w tym artykule okoliczności.

[62] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.

[63] Zgodnie z art. 6 ust. 1 lit. f rozporządzenia 2016/679, cyt.: *przetwarzanie jest zgodne z prawem, gdy – i w takim zakresie, w jakim jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem*.

[64] Zgodnie z art. 4 pkt 11 rozporządzenia 2016/679, cyt.: *„zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych*.

mocy rozporządzenia 2016/679 praw, w tym wniesienia sprzeciwu[65] wobec przetwarzania. Sposób realizacji tych praw (lub jej brak) budził jednak zastrzeżenia osób, których dane dotyczą, będąc przyczyną składania skarg.

W 2020 r. Prezes UODO rozstrzygał m.in. sprawy dotyczące przetwarzania danych osobowych osób prowadzących działalność gospodarczą przez podmioty prowadzące wobec nich działania marketingowe[66]. Dane takich osób w zakresie ich imienia i nazwiska czy też adresu e-mail i numeru telefonu były udostępniane w ogólnodostępnych źródłach[67]. Podmioty prowadzące wobec takich osób działania marketingowe opierały legalność przetwarzania na zgodzie lub prawnie uzasadnionym interesie administratora. Zadaniem Prezesa UODO w tym zakresie było zbadanie poprawności wskazywanych przez administratorów przesłanek, tj. legalności procesu przetwarzania.

W jednej ze spraw, z powodu niepoprawnej interpretacji lub nieznajomości przepisów, przetwarzanie danych oparto na złej przesłance. Administrator wyszedł z założenia, że skoro podmiot danych upublicznił swój adres e-mail, to wyraził chęć nawiązania kontaktów gospodarczych, wobec czego spółka domniemała legalność przetwarzania danych skarżącego na podstawie zgody. Prezes UODO wskazał wówczas, że samo umieszczenie adresu e-mail w ogólnodostępnym rejestrze nie może stanowić podstawy przetwarzania danych właściciela tego adresu opartej na zgodzie. Mając na uwadze motyw 32 rozporządzenia 2016/679, zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba ta wyraziła zgodę na operację przetwarzania[68]. Dopóki zgoda w tym konkretnym celu, tj. w celu prowadzenia działań

[65] Zgodnie z art. 21 ust. 2 rozporządzenia 2016/679, cyt.: *Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim*.

[66] Decyzja Prezesa UODO z dnia 11 sierpnia 2020 r. o sygn.: ZSPR.440.1417.2019; Decyzja Prezesa UODO z dnia 24 września 2020 r. o sygn.: ZSPR.440.1194.2019; Decyzja Prezesa UODO z dnia 16 grudnia 2020 r. o sygn.: DS.440.307.2019.

[67] np. w Centralnej Ewidencji i Informacji o Działalności Gospodarczej, książkach telefonicznych, stronach internetowych czy też rejestrach osób wykonujących określone zawody.

[68] Zgodnie z motywem 42 rozporządzenia 2016/679, cyt.: *Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu. Zgodnie z dyrektywą Rady 93/13/EWG (1) oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków.*

marketingowych przez konkretny podmiot, nie zostanie rzeczywiście zebrana, nie można domniemywać, że poprzez upublicznienie adresu e-mail została ona wyrażona.

W niniejszej sprawie spółka uprawniona była do prowadzenia marketingu wobec skarżącego na podstawie uzasadnionego interesu administratora, jednak tylko do momentu, w którym skarżący wniósł sprzeciw wobec przetwarzania. Działania marketingowe nadal jednak były wobec niego prowadzone, pomimo sprzeciwu, który powinien być uznany za skuteczny[69]. Ponadto skarżącemu nie udzielono żadnej odpowiedzi w związku ze złożonym żądaniem, pomimo faktu, że art. 12 rozporządzenia 2016/679 przewiduje terminy, w których administratorzy mają obowiązek udzielić osobie, której dane dotyczą, informacji o podjętych działaniach w związku ze złożonym przez nią żądaniem. Termin ten wynosi miesiąc od otrzymania żądania. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Jednak w terminie miesiąca należy poinformować osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Administrator wskazał, że sytuacja ta spowodowana była błędem systemowym oraz dużą liczbą pracowników. Biorąc pod uwagę powyższe okoliczności oraz fakt, że spółka nie przetwarzała już danych osobowych skarżącego, Prezes UODO skorzystał z prawa do udzielenia administratorowi upomnienia[70] za naruszenie przepisów rozporządzenia 2016/679.

W kolejnej ze spraw administrator, wykonujący do skarżącego połączenia telefoniczne o charakterze marketingowym, utrudniał realizację przysługujących mu na mocy rozporządzenia 2016/679 praw. Swoje działanie argumentował brakiem zastosowania w tym przypadku przepisów o ochronie danych osobowych, wskazując, że przetwarzany przez niego numer telefonu nie jest powiązany z żadnymi innymi informacjami dotyczącymi skarżącego, a sam w sobie nie stanowi danych osobowych[71]. Prezes UODO nie podzielił jednak ww. stanowiska. Dysponując bowiem

---

Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

[69] Zgodnie z art. 21 ust. 3 rozporządzenia 2016/679, cyt.: *Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów*.

[70] Zgodnie z art. 58 ust. 2 lit. b rozporządzenia 2016/679, cyt.: *Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia naprawcze: b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania*.

[71] Zgodnie z art. 4 pkt 1 rozporządzenia 2016/679, cyt: *„dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, 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*.

informacją w postaci numeru telefonu, podmiot skarżony podejmował działania nakierowane na identyfikację osób. Identyfikacja ta nie wymagała od podmiotu nadmiernych kosztów bądź czasu, a przetwarzanie numeru telefonu służyło identyfikacji danej osoby jako klienta dla podmiotów współpracujących ze skarżonym. Prezes UODO powołał się przy tym na Opinię 4/2007 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29.

W omawianej sprawie Prezes UODO uznał, że wspomniana wyżej przesłanka z art. 6 ust. 1 lit. f rozporządzenia 2016/679, uprawniająca niekiedy do prowadzenia działań marketingowych, nie będzie miała w tym przypadku zastosowania, oraz że nie istnieje żadna inna przesłanka uprawniająca administratora do przetwarzania danych. Nie zachodziło bowiem żadne powiązanie pomiędzy skarżącym a spółką, np. w postaci zawarcia umowy. Podmiot skarżony kupił bazę danych obejmującą dane osobowe skarżącego. Sama umowa sprzedaży bazy danych, stanowiąca źródło pozyskania przez administratora numeru telefonu skarżącego, nie jest bowiem przesłanką legalizującą proces przetwarzania danych osobowych do celów marketingowych. Odmienne stanowisko oznaczałoby możliwość swoistego następczego wykreowania podstawy prawnej dla tego procesu przetwarzania. Trudno jest mówić o nienaruszeniu praw i wolności osoby, której dane są sprzedawane, zwłaszcza gdy nie jest przy tym wobec niej wypełniany obowiązek informacyjny.

Biorąc pod uwagę fakt, że administrator nie realizował przysługującego osobie, której dane dotyczą, prawa dostępu do tych danych wraz z wydaniem ich kopii, Prezes UODO rozstrzygnął sprawę[72], upominając i nakazując administratorowi spełnienie ww. żądania we wskazanym przez skarżącego zakresie. Dodatkowo, w związku z pozyskaniem i przetwarzaniem danych bez podstawy prawnej, nakazał usunięcie tych danych.

W rozpatrywanych przez Prezesa UODO w ubiegłym roku sprawach zdarzały się również takie sytuacje, w których administrator danych prowadzący wobec osoby, której dane dotyczą, działania marketingowe, nie był w stanie zrealizować jej żądania wynikającego z przepisów rozporządzenia 2016/679 z powodu braku odpowiedniej ilości informacji. Należy mieć na uwadze, że zapisując się do różnego rodzaju klubów lojalnościowych czy wypełniając wnioski o kartę stałego klienta, podmiot, z którym zawieramy taką umowę, może kierować do nas treści marketingowe, czy to na podstawie wyrażonych przez nas zgód, czy też na podstawie wyżej już wspomnianego prawnie uzasadnionego interesu. W takich sytuacjach na podstawie art. 21 ust. 2 rozporządzenia 2016/679 można skorzystać z prawa do sprzeciwu, jednak nie zawsze będzie on skuteczny. Kiedy żądanie

[72] Decyzja Prezesa UODO z dnia 31 lipca 2020 r. o sygn. ZSPR.440.1865.2019.

skierowane jest do administratora z innego adresu e-mail, niż ten, który został mu podany podczas zapisywania się do programu lojalnościowego i którego administrator ten nie posiada w swojej bazie danych, identyfikacja osoby zgłaszającej sprzeciw staje się utrudniona lub niemożliwa.

Rozstrzygając taką sprawę[73], Prezes UODO wskazał treść motywu 57 rozporządzenia 2016/679, zgodnie z którym, jeżeli dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej, nie powinien on mieć obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów niniejszego rozporządzenia. Skarżony podmiot próbował jednak, w odpowiedzi na przesłany pocztą elektroniczną sprzeciw, uzyskać dodatkowe informacje pozwalające na jednoznaczną identyfikację osoby zgłaszającej sprzeciw, jednak bezskutecznie. Wobec powyższego administrator potrzebował więcej czasu na realizację omawianego żądania.

Po dokonaniu weryfikacji tożsamości osoby zgłaszającej sprzeciw, administrator uwzględnił jej wniosek i przestał przetwarzać dane osobowe w celach marketingowych. Biorąc powyższe pod uwagę, Prezes UODO ocenił, że działanie spółki było prawidłowe, w związku z czym odmówił uwzględnienia wniosku skarżącej.

4.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa

Spośród 6442 skarg, które w 2020 r. wpłynęły do Urzędu, **926** z nich dotyczyło podmiotów działających w obszarze zdrowia, zatrudnienia i szkolnictwa. Poniżej omówione zostały przykłady kilku takich skarg.

Przetwarzanie danych osobowych w sektorze zdrowia

Głównym powodem skarg na podmioty tego sektora, które w 2020 r. wpłynęły do Prezesa Urzędu Ochrony Danych Osobowych, były skargi na uzyskiwanie przez lekarzy dostępu do danych osobowych przetwarzanych w systemach ZUS. Skarżący kwestionowali działania lekarzy, wskazując, że nie byli ich pacjentami lub że w czasie, gdy uzyskanie dostępu do ich danych osobowych miało miejsce, nie korzystali z usług medycznych danego lekarza. W niektórych sprawach zakresem skargi było objęte również przetwarzanie danych przez Zakład Ubezpieczeń Społecznych.

[73] Decyzja Prezesa UODO z dnia 18 grudnia 2020 r. o sygn. DS.440.99.2019.

Jedna z takich spraw dotyczyła:

nieprawidłowości w procesie przetwarzania danych osobowych przez lekarza prowadzącego indywidualną praktykę lekarską oraz przez Zakład Ubezpieczeń Społecznych.

Skarga dotyczyła zarzutu nieuprawnionego udostępnienia przez ZUS danych osobowych lekarzowi oraz ich przetwarzania przez lekarza bez podstawy prawnej. Skarżąca wskazała, że zgodnie z informacją otrzymaną na platformie elektronicznej PUE ZUS lekarz, wykorzystując uprawnienia nadane mu przez ZUS w celu wystawienia zaświadczeń ZUS ZLA, posługiwał się jej danymi osobowymi (nr PESEL) i wielokrotnie uzyskiwał dostęp do jej danych wrażliwych w okresie, kiedy nie korzystała ona z jego usług medycznych. Jednocześnie działanie lekarza nie było zakończone wystawieniem zwolnienia lub jego anulowaniem.

Organ ocenił, że ZUS, udostępniając lekarzowi dane osobowe skarżącej, działał na podstawie art. 55a ust. 2 ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa[74], co stanowi wypełnienie przesłanek legalizujących proces przetwarzania danych osobowych, określonych w art. 6 ust. 1 lit. c RODO oraz art. 9 ust. 2 lit. h RODO w zakresie szczególnych kategorii danych osobowych skarżącej. Udostępnienie powyższe nastąpiło przy wykorzystaniu platformy PUE ZUS, służącej do udostępniania osobom wystawiającym zaświadczenia lekarskie usług umożliwiających wystawienie zaświadczenia lekarskiego. Podmiotem zobowiązanym do oceny zasadności wystawienia zaświadczenia lekarskiego jest lekarz, nie zaś ZUS. Ponadto udostępnienie przez ZUS danych osobowych skarżącej lekarzowi nastąpiło po podaniu przez lekarza, za pośrednictwem PUE ZUS, wymaganych danych identyfikacyjnych, określonych w art. 55a ust. 3 ww. ustawy. ZUS zobowiązany był zatem udostępnić dane osobowe skarżącej i udostępnienie to nastąpiło, w ocenie organu, w sposób legalny.

W odniesieniu do oceny legalności procesu przetwarzania danych osobowych skarżącej przez lekarza organ stwierdził, że nie została spełniona żadna z przesłanek określonych w art. 6 lub art. 9 RODO odnośnie do kwestionowanego przez skarżącą nieuprawnionego dostępu do jej danych osobowych przetwarzanych za pośrednictwem PUE ZUS, w tym danych dotyczących stanu zdrowia skarżącej. W przedmiotowej sprawie lekarz pozyskał informacje dotyczące skarżącej z PUE ZUS w celach prywatnych, m.in. w celu weryfikacji informacji co do długości trwania zwolnienia lekarskiego skarżącej, które zostało przedstawione przez skarżącą na kilka dni przed mającą się rozpocząć mediacją sądową w sprawie, w której lekarz i skarżąca byli stronami. Organ wskazał, że

[74] Dz. U. z 2017 r. poz. 1368.

brak jest przepisów, które legalizowałyby pozyskiwanie przez lekarzy dostępu do danych osobowych za pośrednictwem PUE ZUS w celu innym niż wystawienie, anulowanie lub sprostowanie zaświadczenia lekarskiego. Organ podkreślił, że dane osobowe udostępniane wystawiającym zaświadczenie lekarskie w PUE ZUS dotyczą między innymi stanu zdrowia pacjentów, zatem informacji, które podlegać powinny szczególnej ochronie.

Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b RODO, Prezes Urzędu Ochrony Danych Osobowych udzielił lekarzowi upomnienia za naruszenie art. 5 ust. 1 lit. a, art. 6 ust. 1 oraz art. 9 ust. 2 RODO poprzez pozyskanie danych osobowych skarżącej bez podstawy prawnej z zasobów PUE ZUS oraz odmówił uwzględnienia wniosku w pozostałym zakresie.

W rozpatrywanych sprawach w 2020 r. Prezes Urzędu dokonywał oceny przetwarzania danych osobowych klientów przez psychologów prowadzących indywidualną działalność gospodarczą. Jedna z takich spraw dotyczyła:

przetwarzania danych osobowych klienta przez psychologa, które polegało na udostępnieniu przez psychologa danych osobowych klienta zawartych w prywatnej opinii psychologicznej na rzecz sądu.

Przetwarzanie danych klienta nie było jednak realizowane w omawianej sprawie na zlecenie sądu. W toku postępowania wyjaśniającego ustalono, że psycholog udostępnił sporządzoną przez siebie opinię na rzecz sądu, uzasadniając swoje działanie uznaniem, że zagrożone jest dobro dzieci osoby składającej skargę.

W decyzji wydanej w omawianej sprawie Prezes UODO wskazał, że zgodnie art. 13 ust. 1 ustawy z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów[75], psycholog jest zobowiązany poinformować klienta o sposobie i celu udostępniania sporządzanej przez niego opinii oraz powinien uzyskać akceptację planowanych czynności. Jeżeli wyniki badań mają służyć nie tylko jako informacja dla klienta, stosuje się przepisy o ochronie danych osobowych. Z powyższej regulacji wynika, że w zależności od metod i charakteru pracy, jeżeli psycholog wykorzystuje informacje o kliencie, w tym jego dane osobowe, do innych celów niż do informacji klienta, wymagane jest uzyskanie jego zgody na przetwarzanie zwykłych lub również szczególnych kategorii danych osobowych, zgodnie z art. 6 ust. 1 lit. a i art. 9 ust. 2 lit a RODO. Zgodnie z art. 14

[75] Dz. U. z 2019 r. poz. 1026.

ust. 1 ustawy o zawodzie psychologa, psycholog ma obowiązek zachowania w tajemnicy informacji związanych z klientem, uzyskanych w związku z wykonywaniem zawodu. Przypadki zwolnienia psychologa z zachowania poufności zostały ściśle określone w ustawie o zawodzie psychologa. Psycholog nie będzie zobowiązany do zachowania tajemnicy zawodowej tylko wtedy, gdy poważnie zagrożone jest życie klienta lub innych osób, albo gdy stanowią tak przepisy innych ustaw. Na jej podstawie, pomimo obowiązku zachowania informacji w tajemnicy, psycholog, który w związku z wykonywaniem swoich obowiązków zawodowych powziął podejrzenie o popełnieniu ściganego z urzędu przestępstwa z użyciem przemocy w rodzinie, powinien niezwłocznie zawiadomić o tym policję lub prokuratora. Co więcej, organ zwrócił uwagę, że RODO określa obowiązki administratora danych, do których należy przetwarzanie danych osobowych z zachowaniem przesłanek określonych w tym rozporządzeniu. Przepisem uprawniającym administratorów danych do przetwarzania zwykłych oraz szczególnych danych osób fizycznych jest odpowiednio art. 6 ust. 1 RODO oraz art. 9 ust. 2 RODO. Prezes Urzędu wskazał również, że przetwarzanie danych osobowych powinno być także zgodne z zasadami określonymi w art. 5 ust. 1 RODO.

Mając na uwadze powyższe Prezes Urzędu rozstrzygnął, że w sprawie brak było podstawy prawnej zezwalającej na udostępnienie prywatnej opinii psychologicznej klienta na rzecz osób trzecich bez jego zgody, bądź gdy nie występują okoliczności zwalniające psychologa z tajemnicy zawodowej. Prezes UODO uznał udostępnienie przez psychologa opinii swojego klienta na rzecz sądu dla toczącego się postępowania rozwodowego za naruszające przepisy o ochronie danych osobowych, wobec czego udzielił administratorowi upomnienia.

Przetwarzanie danych osobowych w sektorze zatrudnienia

Spektrum skarg zakwalifikowanych do działu zatrudnienia było bardzo szerokie. Najczęściej zgłaszane nieprawidłowości dotyczyły udostępnienia operacji przetwarzania danych osobowych osób składających skargę. Jedna z takich spraw dotyczyła:

udostępnienia przez pracodawcę danych osobowych pracownika podmiotowi trzeciemu, celem wykonania przelewu i dalszego powierzenia tych danych.

Powyższa skarga dotyczyła udostępnienia danych osobowych pracownika w zakresie imienia, nazwiska, numeru konta bankowego, wysokości wynagrodzenia. W sprawie zostały uwzględnione przepisy ustawy o ochronie danych osobowych z 1997 r. z uwagi na fakt, że skarga dotyczyła zdarzenia z 2017 r. i wpłynęła do organu przed 25 maja 2018 r. W treści skargi skarżąca wskazała,

że jej ostatnie wynagrodzenie od pracodawcy przelane zostało na jej konto bankowe przez nieznany jej podmiot (spółkę) bez jej zgody i wiedzy.

W toku postępowania ustalono, że skarżąca podpisała oświadczenie o wyrażeniu zgody na dokonywanie wypłaty wynagrodzenia za pracę w innej formie niż do rąk pracownika, tj. za pośrednictwem wskazanego przez nią rachunku oszczędnościowo-rozliczeniowego. Pracodawca dokonał przelewu wynagrodzenia pracownikowi za pośrednictwem systemu bankowości internetowej banku, korzystając z usługi ekspresowych przelewów. Celem wykonania przelewu pracodawca przekazał bankowi dane osobowe skarżącej w ww. zakresie. Usługa została wykonana za pośrednictwem systemu spółki umożliwiającego wykonanie ekspresowych przelewów środków pieniężnych pomiędzy rachunkami bankowymi. Przekazanie danych pomiędzy bankiem a spółką nastąpiło na podstawie zawartej umowy o uczestnictwo w systemie płatności ekspresowych.

Biorąc pod uwagę stan faktyczny sprawy i obowiązujące przepisy Prezes UODO odmówił uwzględnienia wniosku skarżącej, wskazując, że jej dane osobowe zostały udostępnione przez pracodawcę na rzecz banku na podstawie art. 23 ust. 1 pkt 2 ustawy z 1997 r. w związku z art. 86 § 3 K.p. w celu realizacji przelewu wynagrodzenia.

Odnosząc się zaś do przetwarzania, w tym przekazania danych przez bank na rzecz spółki, Prezes UODO wskazał, że zgodnie z art. 31 ustawy z 1997 r. administrator danych mógł powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych (ust. 1). Podmiot, o którym mowa w ust. 1, mógł przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie (ust. 2). Podmiot, o którym mowa w ust. 1, był obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosił odpowiedzialność jak administrator danych (ust. 3). W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywała na administratorze danych, co nie wyłączało odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową (ust. 4). Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosowało się odpowiednio przepisy art. 14-19 (ust. 5).

W przedmiotowej sprawie bank zawarł ze spółką umowę o uczestnictwo w systemie, na podstawie której klienci banku mogą realizować płatności ekspresowe za pomocą systemu spółki. Na podstawie ww. umowy bank powierzył spółce przetwarzanie danych osobowych nadawców (tu: pracodawca) i odbiorców (tu: skarżąca) przelewów natychmiastowych realizowanych za

pośrednictwem systemu spółki. W związku z powyższym spółka przetwarzała dane osobowe skarżącej w zakresie imienia, nazwiska, numeru konta bankowego i wysokości wynagrodzenia na podstawie art. 31 ustawy z 1997 r.

W ramach zatrudniania pracowników pracodawcy zobowiązani są nie tylko do przestrzegania przepisów o ochronie danych osobowych w odniesieniu do wielu operacji przetwarzania danych, ale również do dbania o to, aby przetwarzać dane prawdziwe, aktualne, z wypełnieniem ciążących na nich obowiązków informacyjnych. Obowiązkiem pracodawcy jest wykazanie, że przetwarza dane zgodnie z prawem i w sposób przejrzysty dla pracownika. Jedna ze spraw rozpatrywana przez Prezesa Urzędu w 2020 r. obejmowała wszystkie wymienione poniżej kwestie:

obowiązki dowodowe stron postępowania; przesłanki przetwarzania danych osobowych pracownika przez pracodawcę w celu obrony jego praw przed sądem powszechnym; konieczność wykazania spełnienia obowiązku informacyjnego wobec pracownika.

Organ właściwy do spraw ochrony danych osobowych otrzymał skargę, której przedmiot dotyczył udostępnienia danych dotyczących zawartej umowy szkoleniowej, udzielonej kary porządkowej, czasu pracy, zwolnień lekarskich oraz treści pozwu sądowego nieuprawnionym osobom trzecim, bezprawnego usunięcia części danych osobowych z akt pracowniczych, braku realizacji obowiązku informacyjnego oraz bezprawnego wykorzystywania danych dotyczących zdrowia poprzez telefoniczne kontakty z lekarzem w sprawie zakazu wystawiania zwolnień lekarskich po ustaniu stosunku pracy.

Po przeanalizowaniu treści skargi organ stwierdził, że strona skarżąca podniosła szereg zarzutów w stosunku do administratora, które nie dotyczyły jej uprawnień wynikających z przepisów prawa ochrony danych osobowych, zaś odnosiły się do takich obszarów, jak organizacja pracy, stosunek pracodawcy do pracownika, mobbing, naruszanie dóbr osobistych, naruszanie tajemnicy korespondencji, dyskryminacja. Prezes zwrócił w związku z tym uwagę, że kompetencje we wskazanym powyżej zakresie, w zależności od zagadnienia, posiada sąd powszechny lub Państwowa Inspekcja Pracy. Rolą Prezesa Urzędu Ochrony Danych Osobowych jest stwierdzenie oraz ocena procesów przetwarzania danych w oparciu o przepisy o ochronie danych osobowych.

Mając powyższe na uwadze Prezes UODO, dokonując oceny udostępnienia danych dotyczących zawartej umowy szkoleniowej, udzielonej kary porządkowej, czasu pracy, wskazał, że jako organ administracji publicznej może uznać stan faktyczny rozstrzyganej sprawy za ustalony jedynie na podstawie niebudzących wątpliwości dowodów i nie może poprzestać w tym zakresie na

uprawdopodobnieniu, chyba że przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego[76] stanowią inaczej (np. art. 24 § 3 K.p.a). Z uwagi na powyższe organ uznał, że strona skarżąca nie dostarczyła dowodów, pozwalających na bezsporne potwierdzenie swoich zarzutów, tym samym umorzył postępowanie w tym zakresie.

Odnosząc się do udostępnienia danych strony skarżącej w zakresie informacji dotyczących zwolnień lekarskich, Prezes UODO w treści decyzji wskazał, że przeprowadzone postępowanie wyjaśniające nie dostarczyło dowodów pozwalających na bezsporne potwierdzenie okoliczności dokonania udostępnienia danych na rzecz osób nieuprawnionych. Z uwagi na brak dowodów, działając na podstawie art. 105 K.p.a., organ nadzorczy umorzył postępowanie w tym zakresie.

Odnosząc się do udostępnienia treści pozwu zawierającego dane strony skarżącej przez stronę skarżoną na rzecz osoby nieuprawnionej, organ do spraw ochrony danych osobowych na podstawie uzyskanego w przedmiotowej sprawie materiału dowodowego wskazał, że powyższe udostępnienie zostało dokonane na podstawie art. 6 ust. 1 lit. f RODO z uwagi na prawnie uzasadniony interes administratora, jakim jest obrona swoich praw przed sądem przez stronę skarżoną.

W ocenie Prezesa UODO w przedmiotowej sprawie nie doszło do naruszenia przepisów RODO w zakresie usunięcia danych strony skarżącej z akt osobowych, odnoszących się do informacji o udzielonej karze porządkowej. Organ wskazał, że administrator w zakresie informacji legitymował się przesłanką wynikającą z art. 6 ust. 1 lit. c RODO w zw. z art. 113 § 1 i § 2 K.p.

Odnosząc się do niezgodnego z prawem wykorzystania danych wrażliwych strony skarżącej, poprzez przeprowadzenie rozmów telefonicznych z lekarzem w sprawie zakazu wystawiania zwolnień lekarskich po ustaniu pracy, organ w treści decyzji wskazał, że w wyniku funkcjonowania niezależnego systemu informatycznego, jakim jest PUE ZUS, nie można stwierdzić, że strona skarżona w związku z otrzymaniem danych dotyczących zdrowia strony skarżącej stała się ich administratorem lub odbiorcą w rozumieniu art. 4 ust. 1 pkt 7 RODO oraz art. 9 RODO. Powyższe wynikało z faktu, że administrator mimowolnie otrzymał z systemu PUE ZUS informację o przebywaniu na zwolnieniu lekarskim strony skarżącej. Administrator, chcąc uniknąć takiej sytuacji w przyszłości, skontaktował się z lekarzem i poinformował go o błędnym podaniu numeru NIP zakładu pracy. Tym samym organ rozstrzygnął, że nie potwierdziły się zarzuty ingerencji pracodawcy w treść zwolnień lekarskich lub zakazywania lekarzowi ich wystawiania.

[76] Dz.U. z 2020 r. poz. 256 z późn. zm.

W odniesieniu natomiast do braku spełnienia obowiązku informacyjnego przez stronę skarżoną, zgodnie z przepisami o ochronie danych osobowych, organ w treści swojej decyzji wskazał, że zarzut zasługuje w pełni na uwzględnienie z uwagi na to, że zgodnie z art. 12 ust. 1 RODO administrator ma obowiązek podejmować odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 RODO. Na podstawie zebranego w przedmiotowej sprawie materiału dowodowego, Prezes UODO ustalił, że strona skarżona nie spełniła ciążącego na niej obowiązku informacyjnego wobec strony skarżącej, co stanowi naruszenie art. 12 ust. 1 oraz art. 13 ust. 1 i 2 RODO.

Mając na uwadze powyższe Prezes Urzędu nakazał pracodawcy spełnienie obowiązku informacyjnego wobec strony skarżącej, odmówił uwzględnienia wniosku w zakresie zarzutu bezprawnego udostępnienia w miejscu pracy danych osobowych dotyczących treści akt pracowniczych oraz treści pozwu sądowego osobom trzecim, bezprawnego usunięcia części danych osobowych z akt pracowniczych oraz bezprawnego wykorzystywania danych dotyczących zdrowia poprzez telefoniczne kontakty z lekarzem w sprawie zakazu wystawiania zwolnień lekarskich po ustaniu stosunku pracy, zaś w pozostałym zakresie umorzył postępowanie.

Przetwarzanie danych osobowych pracowników przez podmioty publiczne wiąże się nierzadko z koniecznością wyważania przez nie prawa do ochrony danych osobowych pracownika z prawem obywatela do dostępu do informacji publicznej i obowiązkiem jej udostępniania przez ten podmiot. Jedna z takich spraw dotyczyła:

udostępnienia danych osobowych pracownika w Biuletynie Informacji Publicznej.

Prezes Urzędu przeprowadził postępowanie w sprawie skargi na udostępnienie w opublikowanych w Biuletynie Informacji Publicznej (BIP) zarządzeniach burmistrza danych osobowych skarżącej w zakresie informacji o przebywaniu przez nią na zwolnieniu lekarskim. Kwestionowane udostępnienie wynikało z opublikowania przez burmistrza zarządzeń w Biuletynie Informacji Publicznej (BIP) bez ich uprzedniej anonimizacji, a dotyczących odwołania skarżącej ze stanowiska dyrektora szkoły i powołania innej osoby na to stanowisko. W uzasadnieniu obu tych zarządzeń zostało wskazane, że powodem odwołania skarżącej ze stanowiska i powołania na nie innej osoby, była nieobecność skarżącej spowodowana przebywaniem na zwolnieniu lekarskim, i konieczność zapewnienia ciągłości zarządzania szkołą. Skarżąca nie składała do burmistrza wniosku

z żądaniem usunięcia czy ograniczenia jej danych osobowych, lecz od razu złożyła skargę do Prezesa Urzędu.

Z uwagi na to, że dane osobowe skarżącej zostały zamieszczone w BIP, organ dokonał oceny, czy skarżąca była osobą publiczną i czy burmistrz miał obowiązek publikowania jej danych osobowych w zarządzeniach w BIP.

W ocenie Prezesa Urzędu skarżąca jako dyrektor szkoły była osobą publiczną, zaś burmistrz jako podmiot publiczny był zobligowany do udostępniania informacji publicznej w BIP. Prezes Urzędu uznał także, że informacja o odwołaniu skarżącej ze stanowiska dyrektora szkoły i powołanie innej osoby na to stanowisko, stanowiła informację publiczną.

Organ ustalił przy tym, że informacja o tym, że skarżąca przebywała na zwolnieniu lekarskim, była ściśle związana z pełnioną wówczas przez nią funkcją. Informacja o przebywaniu skarżącej na zwolnieniu lekarskim była jednocześnie jedną z informacji, jakie uzasadniały podjętą decyzję o odwołaniu skarżącej ze stanowiska i powierzeniu go innej osobie. Tym samym informacja ta związana była ścisłe z jej życiem zawodowym jako dyrektora szkoły. W udostępnionych przez burmistrza w BIP zarządzeniach nie została wskazana choroba skarżącej, lecz wyłącznie informacja wskazująca na niemożność sprawowania przez nią zajmowanej wówczas funkcji, z uwagi na jej absencję spowodowaną przebywaniem na zwolnieniu lekarskim.

Prezes Urzędu stwierdził w decyzji, że skarżąca jako dyrektor szkoły była osobą pełniącą funkcję publiczną, w stosunku do której ograniczenie prawa do informacji publicznej ze względu na prywatność osoby fizycznej nie ma zastosowania. Absencja skarżącej w pracy spowodowana niezdolnością do niej i przebywanie na zwolnieniu lekarskim istotnie wpływa na sprawowaną przez skarżącą funkcję, tym samym informacja ta znalazła się w uzasadnieniu opublikowanych w BIP zarządzeń burmistrza i jej udostępnienie nie naruszało prawa do ochrony danych osobowych skarżącej. Przesłankami legalizującymi ww. proces był art. 6 ust. 1 lit. c i lit. e oraz art. 9 ust. 2 lit. g RODO.

Prezes Urzędu zwrócił również uwagę, że zarządzenia przechowywane przez burmistrza stanowią dokumenty wytworzone przez organ administracji publicznej i dotyczą sfery faktów przez ten organ dokonanych, więc co do zasady podlegają archiwizacji. Dlatego też Prezes Urzędu nie mógł uczynić zadość żądaniu skarżącej nakazania ograniczenia przetwarzania jej danych, gdyż nie było to możliwe przed upływem czasu niezbędnego na jego archiwizację wynikającego z przepisów prawa.

Przedmiotem rozpatrywanych przez Prezesa Urzędu skarg było nie tylko udostępnianie danych osobowych pracownika do publicznej wiadomości w Biuletynie Informacji Publicznej, ale również z wykorzystaniem platform społecznościowych. Jedna z takich spraw dotyczyła:

udostępnienia nieprawdziwych danych osobowych nauczyciela na ogólnodostępnej tablicy informacyjnej w siedzibie administratora oraz na profilu szkoły w serwisie społecznościowym i braku reakcji administratora na żądanie usunięcia danych.

Przedmiotem tej skargi był zarzut niezgodnego z prawem udostępnienia w czasie ogólnopolskiego strajku danych osobowych nauczyciela w zakresie imienia, nazwiska i informacji o dniach pracy na ogólnodostępnej tablicy informacyjnej w siedzibie administratora oraz na jego profilu w serwisie społecznościowym, jak również braku ustosunkowania się do żądania usunięcia tych danych. Udostępniona informacja dotyczyła pełnienia przez nauczyciela dyżuru w okresie, w którym faktycznie pracownik ten przebywał na zwolnieniu lekarskim. Istotą sprawy było przetwarzanie przez administratora danych osobowych, które nie były prawdziwe. Chodziło o podanie tych danych do publicznej wiadomości, co sugerowało, że nauczyciel ten nie przystąpił do ogólnopolskiego strajku.

Organ właściwy do spraw ochrony danych osobowych negatywnie ocenił działanie administratora. Art. 5 ust. 1 lit. d RODO nakłada na administratora obowiązek zapewnienia, aby przetwarzane przez niego dane w każdym wypadku były prawidłowe i w razie potrzeby uaktualniane. Natomiast dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, aby zostały niezwłocznie usunięte lub sprostowane. W przedmiotowej sprawie administrator dysponował informacją o przebywaniu swojego pracownika (nauczyciela) na zwolnieniu lekarskimi i jego nieobecności w określonych dniach. Pomimo tego administrator opublikował komunikat zawierający dane i informacje dotyczące tego pracownika, wskazujące, że pełnił on dyżur u administratora, czyli stawił się w pracy w okresie, w którym w rzeczywistości pozostawał na zwolnieniu lekarskim. Dodatkowo publiczne poinformowanie o rzekomej obecności pracownika w pracy we wskazanych dniach było równoznaczne z uznaniem, że nie przystąpił on do ogólnopolskiego strajku. Administrator przetwarzał więc dane niemające odzwierciedlenia w stanie faktycznym i nie podjął działań mających na celu niezwłoczne sprostowanie tych danych.

Kolejnym naruszeniem ochrony danych przez administratora w przedmiotowej sprawie był brak jego reakcji na żądanie nauczyciela usunięcia jego danych osobowych przetwarzanych w ww. kwestionowany sposób. W toku postępowania organ ustalił, że administrator nie ustosunkował się do

żądania nauczyciela w terminie określonym w art. 12 ust. 3 RODO. Ostatecznie administrator usunął nieprawdziwe informacje dotyczące nauczyciela, niemniej nastąpiło to z naruszeniem art. 12 ust. 3 RODO w zw. z obowiązkiem usunięcia danych, określonym w art. 17 ust. 1 lit. c i d RODO.

Prezes Urzędu ocenił, że przetwarzanie przez administratora danych osobowych nauczyciela nie miało pokrycia w rzeczywistym stanie faktycznym i w myśl zasady określonej w art. 5 ust. 1 lit. d RODO stanowiło naruszenie, podobnie jak zaniechanie podjęcia działań w związku z wniesionym sprzeciwem i żądaniem. Wobec czego organ nadzorczy udzielił administratorowi upomnienia za naruszenie art. 6 ust. 1 w zw. z art. 5 ust. 1 lit. d oraz art. 17 ust. 1 w zw. z art. 12 ust. 3 RODO.

Przetwarzanie danych osobowych pracowników przez pracodawców wiąże się także z ciążącymi na nich obowiązkami informacyjnymi oraz obowiązkami zapewnienia prawa dostępu do danych, a także obowiązkiem wykazania ich spełnienia. Jedna z takich spraw dotyczyła:

niezrealizowania obowiązku informacyjnego i prawa dostępu do danych osoby, której dane dotyczyły, przez podmiot zatrudniający osoby bezrobotne, kierowane z urzędu pracy.

Przedmiotowa sprawa dotyczyła nieprawidłowości w procesie przetwarzania danych osobowych, które polegały na braku realizacji obowiązku informacyjnego wynikającego z art. 13 RODO oraz niezrealizowaniu prawa dostępu do danych osobowych osoby, której dane dotyczyły, wynikającego z art. 15 RODO. Skarżący był osobą bezrobotną, zarejestrowaną w powiatowym urzędzie pracy. Osoba ta została zobowiązana przez urząd pracy do złożenia aplikacji (CV wraz z danymi osobowymi) na adres mailowy należący do spółki i otrzymała potwierdzenie, że dokumenty wpłynęły i zostały przekazane do kierownika. Spółka nie zrealizowała jednak wobec tej osoby obowiązku informacyjnego wynikającego z art. 13 RODO. W związku z tym skarżący zwrócił się dwukrotnie do spółki z żądaniem jego realizacji. Ponadto w związku z brakiem odpowiedzi na żądanie, a także brakiem na stronie internetowej spółki jakichkolwiek informacji o zasadach przetwarzania przez nią danych osobowych, wysyłając wiadomość na kilka ogólnodostępnych adresów e-mail, skarżący zwrócił się do spółki z żądaniem realizacji jego prawa dostępu do danych. W odpowiedzi od spółki otrzymał on jedynie lakoniczną informację, że jego dane nie widnieją w żadnej z użytkowanych przez spółkę baz danych. Ponadto skarżący wskazał, że urząd pracy zobowiązał go do ponownego wysłania dokumentów aplikacyjnych do spółki, przez co po raz drugi skierował on do spółki swoją aplikację, a także ponownie skierował do tego podmiotu żądanie realizacji jego prawa dostępu do dotyczących go danych. Skarżący poprosił tym razem także

o przekazanie mu przez spółkę kopii jego danych. W odpowiedzi spółka wskazała skarżącemu, że jego dane osobowe nie widnieją w żadnej z użytkowanych przez spółkę bazie danych.

W toku postępowania wyjaśniającego przed organem spółka wskazała, że w związku z zakończeniem współpracy z pracownikiem, z którym była prowadzona korespondencja, zgodnie z polityką bezpieczeństwa spółki, jego skrzynka wraz z całą zawartością została usunięta. W związku z powyższym spółka nie była w stanie wykazać, czy spełniła wobec skarżącego obowiązek informacyjny z uwagi na fakt, iż nie jest w posiadaniu korespondencji mailowej pomiędzy skarżącym a wspomnianym pracownikiem. Niemniej spółka udzieliła skarżącemu odpowiedzi na jego wiadomość mailową, wskazując, że jego dane nie są przez nią przetwarzane.

Spółka wyjaśniła także, że zgodnie z przyjętą przez nią polityką przetwarzania danych w procesie rekrutacyjnym, przetwarzała ona dane jedynie z tych aplikacji, które zostały pozytywnie zarekomendowane do dalszego procesowania w ramach prowadzonej rekrutacji, natomiast brak pozytywnej rekomendacji skutkował niezwłocznym usunięciem danych i zaprzestaniem ich przetwarzania. Z uwagi na fakt, iż dane skarżącego nie zostały pozytywnie zarekomendowane do dalszego procedowania w ramach prowadzonej rekrutacji, jego dane osobowe zostały usunięte i w okresie składania wniosków nie były przetwarzane przez spółkę.

W przedmiotowej sprawie Prezes Urzędu miał za zadanie dokonać oceny, czy w związku z prowadzonym przez spółkę procesem rekrutacji zrealizowała ona wobec skarżącego (jako osoby biorącej udział w rekrutacji) obowiązek informacyjny wynikający z art. 13 RODO, jak również czy wobec skarżącego spółka zrealizowała jego prawo dostępu do danych osobowych wynikające z art. 15 RODO. W uzasadnieniu decyzji Prezes Urzędu wskazał, iż zgodnie z art. 12 ust. 1 RODO, administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 w sprawie przetwarzania. Powyższy przepis pozostaje w związku z art. 13 RODO, który stanowi, że jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas ich pozyskiwania podaje jej wszystkie informacje wskazane w ust. 1 i ust. 2 tego przepisu. Obowiązek taki powinien zostać zrealizowany przez administratora niezwłocznie po otrzymaniu danych osobowych, w tym wypadku od skarżącego, nie później jednak niż przy pierwszym kontakcie z podmiotem danych. W ocenie Prezesa Urzędu spółka nie wykazała, aby zrealizowała wobec skarżącego obowiązek informacyjny z art. 13 RODO w momencie złożenia przez niego dwukrotnej aplikacji, czy też w kierowanej do niego korespondencji mailowej, przez co naruszyła zasadę

rozliczalności (art. 5 ust. 2 RODO) oraz zasadę przejrzystości (art. 5 ust. 1 lit. a RODO). Spółka co prawda opracowała politykę przetwarzania danych w procesie rekrutacji, ale obejmowała ona wyłącznie postępowanie w stosunku do tych osób, które uzyskały pozytywną rekomendację pracownika spółki zajmującego się rekrutacją. W dokumencie tym nie poruszano kwestii dotyczących obowiązków spółki jako administratora w stosunku do osób, które takiej rekomendacji nie uzyskały. W ocenie Prezesa Urzędu brak uregulowania w nim m.in. kwestii realizacji obowiązku informacyjnego (art. 13 RODO) w stosunku do osób, które nie uzyskały pozytywnej rekomendacji pracownika spółki, naruszyło prawo skarżącego do informacji wynikające z art. 13 RODO.

Odnosząc się do zarzutu niespełnienia przez spółkę prawa skarżącego wynikającego z art. 15 RODO, Prezes Urzędu zwrócił uwagę, że 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 ust. 1 lit. a – h tego przepisu. Co więcej, zgodnie z art. 12 ust. 3 RODO, spółka była zobowiązana do udzielenia osobie, której dane dotyczą informacji o działaniach podjętych w związku z jej żądaniem bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania. Z materiału dowodowego zgromadzonego w sprawie wynikało, że spółka udzieliła skarżącemu odpowiedzi, że nie przetwarza jego danych osobowych, co skutkowało nieudzieleniem odpowiedzi na pozostałe pytania skarżącego, np. w jakim zbiorze są one przetwarzane. Tym samym spółka nie naruszyła prawa skarżącego bowiem udzieliła mu odpowiedzi na żądanie w terminie wynikającym z art. 12 ust. 3 RODO.

W przedmiotowej sprawie Prezes Urzędu, na podstawie art. 58 ust. 2 lit. b RODO, skorzystał z przysługujących mu uprawnień naprawczych, a konkretnie udzielenia upomnienia spółce za naruszenie art. 5 ust. 2 oraz art. 13 RODO w związku z niezrealizowaniem obowiązku informacyjnego, a w pozostałym zakresie odmówił uwzględnienia wniosku.

Przetwarzanie przez lekarzy danych osobowych pacjentów zawartych w systemach ZUS powinno być zawsze uzasadnione względami medycznymi i udzielaniem pacjentowi usług zdrowotnych. Zagadnienie to zostało omówione w części poświęconej dla działu zdrowia. W zakresie skarg na przetwarzanie danych osobowych pochodzących z systemów ZUS Prezes Urzędu rozpoznał w 2020 r. sprawę przetwarzania danych osobowych nie tylko pacjenta, ale i pracownika podmiotu medycznego, którego skarga dotyczyła. Przykład poniższy opisuje:

przetwarzanie danych osobowych byłego pracownika zawartych w systemach ZUS w celach szkoleniowych przez personel administratora.

W sprawie tej ustalono, że skarżąca po zalogowaniu się na swoje konto na Platformie Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE ZUS) uzyskała informację, że próbowano na jej dane osobowe wystawić zaświadczenia lekarskie. Skarżąca oświadczyła, że nie była pacjentką lekarza, który próbował wystawić ww. dokumenty. Skarżąca złożyła skargę do Prezesa UODO, ponieważ według niej bezprawnie zostały użyte jej dane osobowe. W toku przeprowadzonego postępowania ustalono, że skarżąca i lekarz pracowali w tej samej placówce medycznej. W dniu, w którym były próby wystawienia dokumentów lekarz nie dyżurował. W toku postępowania wyjaśniającego ustalono, że to asystentki medyczne, które posiadały upoważnienia do wystawiania zaświadczeń w imieniu lekarza, posłużyły się danymi osobowymi skarżącej przetwarzanymi w zasobach placówki medycznej. Wykorzystując numer PESEL skarżącej uzyskały one dostęp do jej danych za pośrednictwem PUE ZUS, następnie w celach szkoleniowych wystawiły elektroniczne zwolnienia lekarskie. Ostatecznie ww. dokumenty zostały anulowane.

W decyzji Prezes Urzędu zwrócił uwagę, że obowiązkiem każdego pracodawcy jest chronić dane osobowe byłych 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. W związku z czym obowiązkiem placówki medycznej było, aby dane w posiadanych przez nią zbiorach przetwarzane były wyłącznie w celach związanych z prowadzeniem dokumentacji dotyczącej skarżącej jako byłego pracownika, nie zaś w celach szkoleniowych. Organ zaznaczył, że dane osobowe znajdujące się w PUE ZUS dotyczą między innymi zdrowia osób korzystających z usług medycznych, zatem stanowią one dane, które podlegać powinny szczególnej ochronie.

Prezes Urzędu wyjaśnił w omawianej decyzji, że w obecnym stanie prawnym brak jest przepisów, które legalizowałyby pozyskiwanie powyższych danych do celów innych niż wystawienie, anulowanie lub sprostowanie zaświadczenia lekarskiego. Zgodnie z art. 6 ust. 4 RODO, jeżeli przetwarzanie w celu innym niż ten, dla którego 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 musi ustalić, czy przetwarzanie w innym celu jest zgodne z pierwotnym celem ich zbierania. Skarżąca nie została poinformowana o zmianie celu przetwarzania jej danych osobowych przez byłego pracodawcę.

Rozstrzygając omawianą sprawę Prezes Urzędu ocenił, że uzyskanie przez asystentki medyczne, przy użyciu numeru PESEL skarżącej, dostępu do jej danych osobowych za

pośrednictwem PUE ZUS w celach szkoleniowych, na potrzeby doskonalenia przez nie umiejętności wystawiania elektronicznych zwolnień lekarskich, stanowiło naruszenie prawa do ochrony danych osobowych skarżącej. Użycie danych osobowych skarżącej, jako byłego pracownika placówki medycznej, nastąpiło w celu innym niż ten, dla którego były pierwotnie przetwarzane (tzn. przechowywanie akt osobowych byłego pracownika). Przetwarzanie ich w celach szkoleniowych nastąpiło bez podstawy prawnej. Prezes Urzędu podkreślił, że placówka medyczna jako pracodawca ponosi odpowiedzialność za przetwarzanie danych osobowych, w tym za ich należyte zabezpieczenie oraz za prawidłowe wykorzystywanie ich przez zatrudnionych przez siebie pracowników.

W związku z powyższym Prezes UODO wydał decyzję upominającą placówkę medyczną za przetwarzanie danych osobowych skarżącej, polegające na uzyskaniu do nich dostępu bez jej wiedzy i zgody, w celu innym niż zostały pozyskane, co stanowiło naruszenie norm z zakresu ochrony danych osobowych art. 5 ust. 1 lit. b, c RODO oraz art. 6 ust. 1 i ust. 4 RODO.

Przetwarzanie danych osobowych w sektorze szkolnictwa

Przetwarzanie danych osobowych przez podmioty prowadzące placówki oświatowe wiąże się z obowiązkami w zakresie współpracy przez nie z organami prowadzącymi i organami nadzoru oraz kontroli. Jedna z takich spraw dotyczyła:

udostępnienia przez burmistrza danych osobowych nauczyciela, jako osoby składającej skargę, i treści skargi na rzecz osoby, której ta skarga dotyczyła.

Przedmiotowa sprawa dotyczyła udostępnienia przez burmistrza danych osobowych skarżącej zawartych w skierowanej do niego skardze na p.o. dyrektora szkoły, w której skarżąca była zatrudniona jako nauczyciel.

Skarżąca wskazała, że wraz z innymi nauczycielami złożyła do burmistrza miasta skargę na p.o. dyrektora szkoły, w której pracowała jako nauczyciel. Burmistrz na pisemną prośbę dyrektora szkoły udostępnił mu kserokopię tej skargi bez anonimizacji danych osób ją składających, w tym danych skarżącej. Udostępnienie kopii skargi złożonej na p.o. dyrektora szkoły nastąpiło w ramach dostępu do informacji publicznej. Zasadniczą kwestią rozstrzyganą w sprawie była ocena legalności udostępnienia przez burmistrza danych osobowych skarżącej zawartych w skardze na rzecz p.o. dyrektora szkoły na podstawie przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Organ nadzorczy nie dopatrzył się w niniejszej sprawie naruszenia prawa do ochrony danych osobowych skarżącej i odmówił uwzględnienia jej wniosku.

Prezes UODO dokonał w sprawie oceny, czy burmistrz był podmiotem uprawnionym do wydania kopii skargi w ramach dostępu do informacji publicznej. Zgodnie z art. 4 ust. 1 pkt 1 ww. ustawy zobowiązane do udostępniania informacji publicznej są władze publiczne oraz inne podmioty wykonujące zadania publiczne, w szczególności organy władzy publicznej. Organami władzy publicznej w rozumieniu powołanego przepisu są też organy samorządu terytorialnego, a więc organy gminy, powiatu i województwa. Natomiast organami gminy są: rada gminy i wójt (burmistrz, prezydent miasta). Działalność organów gminy jest jawna i obejmuje w szczególności prawo obywateli do uzyskiwania informacji, a także dostępu do dokumentów wynikających z wykonywania zadań publicznych. Natomiast zasady dostępu do dokumentów i korzystania z nich określa statut gminy. Mając na uwadze przepisy ustawy o dostępie do informacji publicznej oraz treść statutu gminy Prezes Urzędu ustalił, że burmistrz był organem zobowiązanym do udostępnienia informacji publicznej będącej w posiadaniu urzędu.

Następnie Prezes UODO dokonał oceny, czy udostępniona skarga była dokumentem zawierającym informację publiczną i czy podlegała udostępnieniu w ramach ustawy o dostępie do informacji publicznej. Prezes UODO wskazał, że zgodnie z art. 1 ust. 1 ww. ustawy, informację publiczną stanowi każda informacja o sprawach publicznych. Natomiast informacja o sprawach publicznych to każda informacja wytworzona przez szeroko rozumiane władze publiczne oraz osoby pełniące funkcje publiczne, a także inne podmioty, które tę władzę realizują, bądź gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa w zakresie tych kompetencji, a także wiadomość niewytworzona przez podmioty publiczne, lecz odnosząca się do nich. Do tej kategorii, w ocenie Prezesa UODO, zaliczała się skarga na działalność p.o. dyrektora szkoły.

Prezes UODO, oceniając legalność udostępnienia danych osobowych skarżącej zawartych w skardze na p.o. dyrektora szkoły, miał na względzie także art. 5 ust. 2 ustawy o dostępie do informacji publicznej. Zgodnie z jego treścią prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy natomiast informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji. W ocenie Prezesa UODO, w oparciu o przepisy ustawy o dostępie do informacji publicznej i aktualne orzecznictwo, skarżąca w chwili składania skargi na p.o. dyrektora szkoły była osobą pełniącą funkcję publiczną.

Prezes UODO wskazał, że skarżąca w momencie udostępnienia danych zatrudniona była na stanowisku nauczyciela w szkole, a zatem pełniła ona funkcję publiczną poprzez realizację zadań nałożonych na szkołę jako instytucję publiczną. Ponadto skarga na p.o. dyrektora szkoły została

złożona przez skarżącą w związku ze sprawowaną funkcją nauczyciela, a więc w związku z pełnioną funkcją publiczną oraz dotyczyła kwestii ściśle związanych m.in. z osobą p.o. dyrektora szkoły oraz organizacją i funkcjonowaniem szkoły. W przedmiotowej sprawie nie miało zatem zastosowania ograniczenie prawa do informacji publicznej ze względu na prywatność osoby fizycznej.

Mając powyższe na uwadze, Prezes UODO odmówił uwzględnienia wniosku, stwierdzając, że przetwarzanie danych osobowych skarżącej przez burmistrza, polegające na udostępnieniu zawierającej dane osobowe skarżącej skargi na rzecz p.o. dyrektora szkoły, miało oparcie w przesłance z art. 6 ust. 1 lit. c i e rozporządzenia 2016/679.

Przetwarzając dane osobowe uczniów i ich rodziców, placówki oświatowe zobowiązane są do przestrzegania przepisów o ochronie danych osobowych. Obowiązek ten nie odnosi się tylko do przetwarzania danych osobowych w związku z działalnością oświatową, ale również w związku z towarzyszącymi jej obowiązkami, w tym dotyczącymi rozpatrywania przez placówki oświatowe skarg na ich działalność. Jedna z takich spraw dotyczyła skargi w przedmiocie:

udostępnienia danych osobowych skarżącej oraz danych osobowych jej małoletniego dziecka przez szkołę podstawową osobie nieuprawnionej.

W treści skargi wskazano, że wicedyrektor szkoły (pracownik szkoły) ujawnił swojemu synowi, jako osobie trzeciej, niezwiązanej w żaden sposób ze szkołą, informacje dotyczące sytuacji szkolnej dziecka skarżącej oraz jej życia prywatnego. O fakcie ww. udostępnienia danych osobowych skarżąca dowiedziała się z treści skargi wniesionej przez syna pracownika szkoły do Komendy Głównej Policji w Warszawie na czynności skarżącej podejmowane wobec niego w związku z pełnieniem przez skarżącą funkcji kierowniczej w jednej z komend powiatowych policji.

Organ ustalił, że osobie trzeciej zostały udostępnione informacje dotyczące przebiegu zebrania rodziców w szkole, poświęconego wyłącznie dziecku skarżącej oraz wyników i ustaleń pomiędzy szkołą a rodzicem dziecka, o czym świadczyła treść skargi do Komendy Głównej Policji. Osoba ta następnie wykorzystała informacje w złożonej skardze, wykazując w ten sposób, że zachowanie skarżącej wobec niej nie było obiektywne i rzetelne oraz że zatrzymanie ww. osoby przez funkcjonariuszy Policji miało jedynie na celu odegranie się na jej rodzinie. W ocenie dyrektora szkoły sprawa nie dotyczyła bezpośrednio szkoły i była wyłącznie wynikiem osobistego konfliktu istniejącego pomiędzy skarżącą a wicedyrektorem szkoły.

Organ ochrony danych osobowych nie zgodził się ze stanowiskiem prezentowanym przez dyrektora szkoły i uznał, że w niniejszej sprawie doszło do naruszenia ochrony danych osobowych.

Obowiązkiem ciążącym na szkole jako administratorze danych jest bowiem właściwe zabezpieczenie danych osobowych. Ponieważ zarówno złożenie skargi przez skarżącą, jak i samo udostepnienie danych miało miejsce przed 25 maja 2018 r., do niniejszej sprawy zastosowanie miały przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zgodnie z art. 36 ust. 1 ww. ustawy administrator danych był obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane m.in. przed ich udostępnieniem osobom nieupoważnionym. Organ uznał, że szkoła jako administrator, reprezentowana przez dyrektora, musi mieć pełną kontrolę nad procesem przetwarzania danych tak, aby był on zgodny z przepisami prawa. Musi też mieć pełną wiedzę na temat całości procesu przetwarzania danych oraz musi weryfikować zachowania pracowników pod kątem przestrzegania przez nich zasad ochrony danych osobowych. Prezes Urzędu Ochrony Danych Osobowych zwrócił również uwagę na stanowisko Naczelnego Sądu Administracyjnego w Warszawie wyrażone w wyroku z 4 kwietnia 2003 r., (II SA 2935/02), że za działania swoich pracowników w zakresie naruszenia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych odpowiada administrator. Niedopuszczalne było zatem udostępnienie przez pracownika osobie nieuprawnionej danych osobowych pozyskanych w ramach pełnionych przez niego obowiązków służbowych, a administrator odpowiada za czyny swoich pracowników w zakresie naruszenia ustawy o ochronie danych osobowych.

Przetwarzanie danych osobowych absolwentów powinno być ograniczone do celów i zakresu wynikających z przepisów prawa. Przetwarzanie danych osobowych w sposób wykraczający poza te cele i zakres powinno być dokonywane z najwyższą ostrożnością i z poszanowaniem przepisów o ochronie danych osobowych. Jedna z takich spraw dotyczyła:

pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji oraz interesu publicznego jako podstawy prawnej przetwarzania danych osobowych.

Prezes UODO rozpoznawał sprawę dotyczącą skargi absolwenta jednej z wyższych uczelni, w której zgłosił on nieprawidłowości w procesie przetwarzania jego danych osobowych związane z udostępnieniem jego imienia i nazwiska w publikacji cyfrowej uczelni dostępnej dla nieograniczonej liczby osób.

Prezes UODO w wydanej decyzji dokonał oceny przetwarzania danych osobowych zawartych w ww. wykazie, biorąc pod uwagę występujące w sprawie okoliczności dotyczące formy i sposobu udostępnienia takich danych. Dokonując oceny stanu faktycznego organ miał

na uwadze możliwości udostępniania danych w związku z realizacją zadania w interesie publicznym oraz konieczności zbadania potencjalnego wyłączenia stosowania przepisów w zakresie ochrony danych osobowych z uwagi na dyspozycję przepisów odnoszących się do działalności związanej z materiałami prasowymi, działalności literackiej, artystycznej oraz wypowiedzi akademickich.

Prezes UODO wskazał w wydanej decyzji, że kluczowym aspektem przetwarzania danych osobowych w ramach działalności artystycznej czy literackiej będzie cel przetwarzania danych potrzebny dla realizacji ww. działalności. Publikacja danych osobowych absolwenta w wykazie absolwentów nie korzysta z wyłączenia przewidzianego w art. 2 ustawy o ochronie danych osobowych, bowiem wykaz ten pozbawiony jest indywidualnego charakteru twórczego dzieła oraz nie stanowi artystycznego przejawu myśli w tworzeniu sztuki prasowej. Prezes UODO wskazał, że wykaz absolwentów jest jedynie spisem zawierającym imiona, nazwiska absolwentów wraz z ukończonym przez nich kierunkiem studiów, co sprawia, że brak jest w nim indywidualnych cech, które można przypisać do dzieła literackiego czy artystycznego, decydujących o ich twórczym aspekcie, stąd nie korzysta z wyłączenia określonego w art. 2 ustawy o ochronie danych osobowych. Prezes UODO rozważał ponadto, czy uczelnia przetwarzała dane osobowe skarżącego w celu niezbędnym do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, czyli podstawy przetwarzania określonej w art. 6 ust. 1 lit. e RODO. Oceny takiej dokonano z uwagi na fakt podniesionej argumentacji, odnoszącej się do przetwarzania danych absolwenta w celach archiwalnych w interesie publicznym, na podstawie art. 6 ust. 1 lit. e RODO, w związku z treścią art. 89 ust. 1 RODO. W związku z tym Prezes UODO wskazał, że z treści motywu 156 RODO wynika, że przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, powinno podlegać odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą, zgodnie z omawianym rozporządzeniem. Zabezpieczenia te powinny polegać na wdrożeniu środków technicznych i organizacyjnych zapewniających w szczególności poszanowanie zasady minimalizacji danych. Dodatkowo wskazano w tym motywie, że państwa członkowskie powinny ustanowić odpowiednie zabezpieczenia w odniesieniu do przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych. Dokonując analizy regulacji dotyczących przetwarzania danych w celach archiwalnych, Prezes UODO zwrócił uwagę na treść

przepisów ustawy z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[77]. W ustawie tej w art. 2 ust. 1 wskazano, że narodowy zasób archiwalny służy nauce, kulturze, gospodarce narodowej oraz potrzebom obywateli. Podkreślono, że uczelnia na podstawie art. 22c ww. ustawy zobowiązana jest do wdrożenia zabezpieczeń wolności i praw osób, których dotyczą dane, zawartych w materiałach archiwalnych, w szczególności w trakcie ich udostępniania przez anonimizację danych osobowych, zawieranie z użytkownikami zasobu archiwalnego umów wyłączających dalsze przetwarzanie danych osobowych oraz przez pseudonimizację danych w systemach informatycznych i teleinformatycznych. Stosowanie zabezpieczeń – jak wskazuje ust. 2 tego przepisu ustawy o archiwach – w postaci anonimizacji i pseudonimizacji nie jest obowiązkowe, jeżeli: przetwarza się, w tym udostępnia, dane osobowe za zgodą osoby, której dane dotyczą, jej pełnomocnika, przedstawiciela ustawowego lub opiekuna prawnego (pkt 1) lub osoba, której dane dotyczą, dobrowolnie i świadomie podała je uprzednio do publicznej wiadomości (pkt 2). Prezes UODO stwierdził, że powyższe przepisy ustawy o archiwach nie stanowią podstawy do przetwarzania danych osobowych absolwenta i nie są niezbędne do wykonania zadania realizowanego w interesie publicznym. Ponieważ absolwent nie wyrażał zgody na przetwarzanie jego danych osobowych w zakresie imienia i nazwiska ani dobrowolnie nie podał tych danych do publicznej wiadomości oraz z uwagi na okoliczność, że uczelnia nie określiła zasad i trybu udostępniania danych osobowych absolwenta, w tym dotyczących ewidencjonowania, przechowywania i zabezpieczenia tych danych, to publikacja tych danych osobowych w zakresie imienia i nazwiska absolwenta możliwa była jedynie w drodze przesłanki określonej w art. 6 ust. 1 lit. a RODO, tj. zgody skarżącego wyrażonej zgodnie z treścią art. 7 i art. 4 pkt 11 RODO. Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust 2 lit. c, Prezes Urzędu Ochrony Danych Osobowych nakazał uczelni usunięcie danych absolwenta w zakresie jego imienia i nazwiska z publikacji cyfrowej uczelni, dostępnej dla nieograniczonej liczby osób, z uwagi na brak podstawy prawnej dla takiego procesu przetwarzania danych osobowych.

4.1.4. Sektor finansów, telekomunikacji i ubezpieczeń

Spośród 6442 skarg, które w 2020 r. wpłynęły do Urzędu, **926** z nich dotyczyło podmiotów sektora bankowego i instytucji finansowych, telekomunikacji i ubezpieczeń. Poniżej przedstawione zostały wybrane przykłady kilku takich skarg.

[77] Dz. U. 2020 poz. 164 z późn. zm.

Przetwarzanie danych osobowych w sektorze finansowym

Przetwarzanie danych osobowych przez banki w celu oceny zdolności kredytowej i analizy ryzyka kredytowego

Podobnie jak w latach poprzednich, także w analizowanym roku sprawozdawczym Prezes UODO prowadził liczne sprawy dotyczące przetwarzania przez banki danych osobowych osób, które nie wywiązały się terminowo z zobowiązań wynikających z zawartych z tymi bankami umów w bazach instytucji utworzonych na podstawie art. 105 ust. 4 Prawa bankowego[78], tj. w tzw. biurach informacji kredytowej. W swoich rozstrzygnięciach organ wskazywał na istnienie przepisów legalizujących ww. procesy przetwarzania danych osobowych po wygaśnięciu roszczenia wobec banku, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, wskazując jednocześnie, że przetwarzanie to musi odbywać się w sposób zgodny z tymi przepisami.

Najczęściej kwestionowano przetwarzanie danych osobowych przez banki w zasobach instytucji utworzonych na podstawie art. 105 ust. 4 Prawa bankowego, po wygaśnięciu zobowiązania, bez zgody osoby, której dane te dotyczą. Taki proces uregulowany został w art. 105a ust. 3 Prawa bankowego. Jednak aby był on legalny, konieczne jest uprzednie poinformowanie osoby, której dane dotyczą, o zamiarze przetwarzania jej danych osobowych bez jej zgody po wygaśnięciu zobowiązania, gdy osoba ta nie wykonała tego zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od tego poinformowania. Sam fakt, że dłużnik nie wykonał zobowiązania lub spóźnił się z jego wykonaniem co najmniej 60 dni, nie upoważnia jeszcze banku do przetwarzania jego danych na warunkach określonych w art. 105a ust. 3 Prawa bankowego. Moment, od którego należy liczyć sześćdziesięciodniowy termin, w którym klient banku dopuszcza się zwłoki w wykonaniu zobowiązania, to termin wykonania zobowiązania. Dopiero po upływie 60 dni zaczyna biec trzydziestodniowy termin, w którym instytucja jeszcze oczekuje na wykonanie zobowiązania klienta. Ostatecznie to bezskuteczny upływ 30 dni od momentu skutecznego poinformowania stanowi wypełnienie przesłanek z art. 105a ust. 3 Prawa bankowego[79]. Oznacza to, że bank musi dysponować dowodem, że osoba, której dane dotyczą, została poinformowana o zamiarze przetwarzania ich bez jej zgody.

Prezes UODO wielokrotnie podkreślał, że samo oświadczenie o wysłaniu korespondencji nie stanowi dowodu na jej dostarczenie lub poinformowanie o jej treści adresata. Przepisy powszechnie

[78] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz. U. z 2020 r. poz. 1896.
[79] ZSPR.440.332.2018, ZSPR.440.913.2019, ZSPR.440.1226.2019, ZSPR.440.1430.2019.

obowiązujące nie formułują obowiązku wysłania informacji, o której mowa w art. 105a ust. 3 Prawa bankowego, w szczególnej formie. To do podmiotu informującego należy zatem wybór formy przekazania odbiorcy komunikatu o zamiarze przetwarzania danych osobowych bez jego zgody[80]. Jednocześnie to podmiot informujący wywodzi z powyższego skutki prawne, zatem to on musi wykazać, że poinformował osobę o zamiarze przetwarzania danych, stanowiących tajemnicę bankową, bez jej zgody na podstawie art. 105a ust. 3 Prawa bankowego, w szczególności gdy osoba, której te dane dotyczą, przeczy otrzymaniu ww. informacji[81].

Przetwarzanie danych osobowych przez banki w celu realizacji obowiązku prawnego wynikającego z ustawy o rachunkowości

Prezes UODO w 2020 r. w drodze decyzji, rozpatrywał skargi wniesione przez byłych klientów banków, którzy zarzucali tym podmiotom, że pomimo braku na dzień wniesienia skargi umów wiążących ich z bankiem, ich dane osobowe były nadal przetwarzane przez skarżony podmiot. Należy wskazać, że jedną z przesłanek legalizujących proces przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO, zgodnie z którym administrator uprawniony jest do przetwarzania danych osobowych osoby, której dane dotyczą, gdy jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Przykładem takiego obowiązku jest obowiązek określony w art. 74 ust. 2 pkt. 4 ustawy o rachunkowości[82], zgodnie z którym dowody księgowe dotyczące środków trwałych w budowie, pożyczek, kredytów oraz umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętych postępowaniem karnym albo podatkowym, przechowuje się przez okres 5 lat, licząc od początku roku następującego po roku obrotowym, w którym operacje, transakcje i postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione[83]. Ponadto zgodnie z art. 74 ust. 2 pkt 8 ustawy o rachunkowości pozostałe dowody księgowe i sprawozdania, niewymienione w art. 74 ust. 2, należy przechowywać przez okres 5 lat[84]. W ocenie Prezesa Urzędu powyższe przepisy prawa nakładają na bank – jako administratora – obowiązek, którego realizacja wiąże się z koniecznością przetwarzania danych osobowych i jako takie znajdują oparcie w przesłance określonej w art. 6 ust. 1 pkt c RODO.

[80] ZSPR.440.435.2018.
[81] por. wyrok Wojewódzkiego Sądu Administracyjnego z dnia 15 marca 2017 r. sygn. akt II SA/Wa 1695/16.
[82] Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz. U. z 2021 r. poz. 217.
[83] ZSPR.440.1107.2019.
[84] ZSPR.440.1401.2018, ZSPU.440.935.2019.

Realizacja przez banki obowiązku dostarczenia kopii danych na podstawie art. 15 ust. 3 RODO

W okresie sprawozdawczym 2020 roku Prezes UODO rozstrzygał także sprawy dotyczące niespełnienia przez banki obowiązku informacyjnego wynikającego z art. 15 ust. 3 RODO.

Odnosząc się do zarzutu niespełnienia obowiązku informacyjnego przez bank z art. 15 ust. 3 RODO, polegającego na dostarczeniu kopii danych osobowych, Prezes UODO wskazywał, że obowiązek udostępnienia kopii danych osobowych nie jest równoznaczny z obowiązkiem udostępnienia kopii dokumentacji dotyczącej umów zawartych z bankiem. Administrator nie ma obowiązku udostępnienia osobie zainteresowanej kopii 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 pozostałych informacji zawartych na nośniku. Wykonanie obowiązku określonego w art. 15 ust. 3 RODO może być zatem realizowane zarówno poprzez sporządzenie kopii lub odpisu dokumentu (nośnika) zawierającego dane osobowe oraz inne dane, jak i poprzez podanie uprawnionemu treści jego danych osobowych, z pominięciem informacji znajdujących się w nośniku, które nie są danymi osobowymi w rozumieniu art. 4 pkt 1 RODO. W przypadku zwrócenia się do administratora o kopię przetwarzanych danych osobowych, administrator każdorazowo podejmuje decyzję, w jaki sposób zrealizuje to uprawnienie. Administrator może dokonać wyboru, czy udostępnia kopię dokumentów, czy też udostępnia kopię danych zawartych w tych dokumentach[85].

Należy wskazać, że przy ocenie prawidłowości spełnienia obowiązku określonego w art. 15 ust. 3 RODO, należy uwzględnić również zachowanie przez administratora terminów określonych w art. 12 ust. 3 RODO. Ponadto administrator, spełniając żądanie osoby, której dane dotyczą, powinien również uwzględnić żądanie odnośnie określonej formy spełnienia obowiązku informacyjnego wynikającego z art. 15 RODO. W przypadku jeśli osoba, której dane osobowe są przetwarzane, żąda spełnienia obowiązku dotyczącego przekazania jej w formie papierowej kopii jej danych osobowych, a administrator przekaże jej kopię danych osobowych w formie elektronicznej, będzie to stanowiło nieprawidłowość w procesie przetwarzania danych osobowych[86].

[85] ZSPR.440.773.2019, ZWOS.440.5703.2019.
[86] ZSPR.440.1622.2019.

Realizacja przez banki prawa do przenoszenia danych zgodnie z art. 20 RODO

W omawianym okresie sprawozdawczym Prezes UODO otrzymał skargę na niewykonanie przez bank prawa do przenoszenia danych osobowych. Organ nakazał bankowi przekazanie – na podstawie art. 20 ust. 1 RODO – dostarczonych przez osobę, której dane dotyczyły, danych osobowych, których przetwarzanie odbywało się w sposób zautomatyzowany w strukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego.

Organ nadzorczy wskazywał, że na podstawie art. 20 ust.1 RODO osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO i przetwarzanie odbywa się w sposób zautomatyzowany.

Podkreślenia wymaga, że bank, będący administratorem, w chwili rozpoczęcia stosowania przepisów RODO powinien być przygotowany na zapewnienie swoim klientom możliwości realizowania wszystkich praw wynikających z przepisów o ochronie danych osobowych. Po wpłynięciu wniosku dotyczącego prawa do przenoszenia danych, na administratorze spoczywa obowiązek dokonania analizy, czy złożony wniosek jest zasadny i czy zachodzą przesłanki do zastosowania prawa do przenoszenia danych osobowych. W przypadku stwierdzenia zasadności takiego wniosku, administrator jest zobowiązany do poinformowania osoby składającej wniosek o sposobie jego realizacji. Informacja taka powinna zostać przekazana bez zbędnej zwłoki – najpóźniej do miesiąca od daty wpłynięcia przedmiotowego wniosku do administratora.

Prawo do przenoszenia danych może zostać zrealizowane w przypadku, gdy operacje przetwarzania danych osobowych odbywają się na podstawie zgody osoby, której te dane dotyczą (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a) RODO) albo na podstawie umowy, której taka osoba jest stroną (art. 6 ust. 1 lit. b RODO). Ponadto przenoszenie danych może mieć miejsce tylko w sytuacjach, w których przetwarzanie danych osobowych odbywa się w sposób zautomatyzowany, nie znajdzie zatem zastosowania wobec zbiorów papierowych.

Prawo do przenoszenia danych może zostać zrealizowane tylko w zakresie danych osobowych wnioskującego o spełnienie tego prawa oraz danych przez niego przekazanych administratorowi. W związku z powyższym wszelkie dane będące danymi anonimowymi lub niedotyczącymi takiej osoby nie będą wchodziły we wskazany powyżej zakres. Wskazania także wymaga, że dane

wywnioskowane i wywiedzione na podstawie danych przekazanych przez osobę, której dotyczą, należy uznać za dane wytworzone przez administratora, które nie mogą zostać uznane za przekazane przez osobę, której dotyczą. Administrator realizując wniosek o przeniesienie danych jest uprawniony do wyłączenia takich wytworzonych przez siebie danych, ale powinien uwzględnić wszystkie inne dane przekazane przez osobę, która chce skorzystać z przysługującego jej prawa[87].

Przetwarzanie danych osobowych dłużników w celu dochodzenia roszczeń

Podobnie jak w latach ubiegłych, do organu właściwego do spraw ochrony danych osobowych zgłaszano skargi dotyczące przetwarzania danych osobowych w związku z dochodzeniem roszczeń od dłużników. W kierowanych do organu skargach dłużnicy wskazywali na brak ich zgody na przetwarzanie danych osobowych przez wierzyciela oraz wyrażali żądanie usunięcia ich danych, które w ich opinii przetwarzane są bez podstawy prawnej.

W ocenie Prezesa UODO przetwarzanie danych osobowych dłużnika w celu dochodzenia od niego zaspokojenia roszczeń stanowi prawnie usprawiedliwiony interes wierzyciela oraz nie narusza jego praw i wolności[88]. Przepisy dotyczące ochrony danych osobowych nie mogą być wykorzystywane jako podstawa dla uchylania się przez dłużników od spełnienia zaległych zobowiązań. Dłużnik, który nie wywiązuje się ze swoich zobowiązań, musi liczyć się z konsekwencjami wynikającymi z przepisów regulujących obrót gospodarczy[89].

Organ w tego typu sprawach wskazywał także, że obowiązujące przepisy prawa nie określają katalogu, który przewidywałby możliwe sposoby postępowań służące dochodzeniu roszczeń. Oznacza, że za mieszczące się w granicach obowiązujących przepisów należy uznać zarówno sądowe, jak i pozasądowe działania wierzyciela zmierzające do zaspokojenia wierzytelności[90].

Przetwarzanie danych osobowych w celu ochrony przed ewentualnymi roszczeniami

W toczących się przed Prezesem UODO w 2020 roku sprawach zarówno administratorzy, jak i podmioty przetwarzające dane na zlecenie administratorów podnosili, że przetwarzają dane osobowe w celu ochrony przed ewentualnymi roszczeniami na podstawie art. 6 ust. 1 lit. f RODO, uzależniając okres przetwarzania od okresu przedawnień roszczeń.

[87] ZSPR.440.773.2019.
[88] ZSPR.440.1415.2018, DS.523.2368.2020, ZSPR.440.1181.2018, ZSZZS.440.592.2019.
[89] por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 30 listopada 2004 r. sygn. akt II SA/Wa 1057/04.
[90] por. wyrok Naczelnego Sąd Administracyjnego z dnia 10 listopada 2015 r. sygn. akt I OSK 1210/14.

W ocenie Prezesa UODO, przesłanka z art. 6 ust. 1 lit. f RODO dotyczy sytuacji już istniejącej, w której celem wynikającym z prawnie uzasadnionych interesów realizowanych przez administratora jest konieczność udowodnienia, potrzeba dochodzenia lub obrony przed roszczeniem istniejącym, nie dotyczy zaś sytuacji, gdy dane są przetwarzane w celu zabezpieczenia się przed ewentualnym, przyszłym i niepewnym roszczeniem[91], a więc „na zapas". W swoich rozstrzygnięciach Prezes UODO wskazywał, że przyjęcie odmiennej interpretacji pozbawiałoby osoby fizyczne ochrony na gruncie RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Wskazać również należy, że brak jest uzasadnienia dla przyjęcia, iż terminy dotyczące przedawnienia roszczeń wynikających ze stosunków zobowiązaniowych określają jednocześnie ramy czasowe, w których dane osobowe mogą być przetwarzane. Przedawnienie roszczenia nie wywołuje skutków na gruncie ochrony danych osobowych, nie wpływa bowiem na fakt istnienia roszczenia, a powoduje jedynie zmianę w sferze zarzutów procesowych w postaci możliwości podniesienia okoliczności przedawnienia w sporze sądowym. Okolicznością usprawiedliwiającą przetwarzanie danych osobowych w celu dochodzenia roszczeń jest sam fakt istnienia roszczenia oraz zamiar jego dochodzenia, nie jest nią natomiast zmiana w uprawnieniach procesowych podmiotu pozwanego[92].

Powierzenie przetwarzania danych osobowych dłużników przez fundusze sekurytyzacyjne

Do organu nadzorczego wpływały także skargi, w których kwestionowano legalność powierzenia podmiotom trzecim danych osobowych dłużników przez fundusze sekurytyzacyjne, w celu dochodzenia wierzytelności.

Istotne jest, że w przypadku wierzycieli będących funduszami sekurytyzacyjnymi zastosowanie znajduje art. 193 ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[93], zgodnie z którym fundusz sekurytyzacyjny oraz podmiot, z którym towarzystwo zawarło umowę o zarządzanie sekurytyzowanymi wierzytelnościami, zbierają i przetwarzają dane osobowe dłużników sekurytyzowanych wierzytelności jedynie w celach związanych z zarządzaniem wierzytelnościami sekurytyzowanymi. Podkreślić jednak należy, że podmioty przetwarzające przetwarzają dane osobowe skarżących w imieniu wierzycieli, którzy wciąż pozostają ich wyłącznymi administratorami. W związku z powyższym w przypadku zawarcia w oparciu o art. 28 ust. 3 rozporządzenia 679/2019 z podmiotem, z którym towarzystwo zawarło umowę o zarządzanie

[91] ZSPR.440.1641.2018.
[92] ZSPR.440.1641.2018, ZSPR.440.1107.2019.
[93] DS.523.2368.2020, ZSPR.440.118.2019.

sekurytyzowanymi wierzytelnościami, umowy powierzenia przetwarzania danych osobowych w celu windykacji istniejących wierzytelności, organ nadzorczy wskazywał, że przedmiotowe powierzenie przetwarzania danych osobowych dłużników jest zgodne z prawem[94].

Dopuszczalność udostępnienia danych osobowych Straży Miejskiej dla celów prowadzonych czynności wyjaśniających w sprawach o wykroczenia

W analizowanym okresie sprawozdawczym Prezes UODO rozstrzygał w sprawie skargi Komendanta Straży Miejskiej na nieudostępnienie przez spółkę telekomunikacyjną danych osobowych abonenta, w związku z prowadzonymi czynnościami wyjaśniającymi w sprawie o wykroczenie. Podmiot skarżony odmówił udostępnienia wnioskowanych informacji zawierających dane osobowe, powołując się na tajemnicę telekomunikacyjną, wynikającą z art. 159 ust. 1 Prawo telekomunikacyjne[95].

Zgodnie z art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi.

Wskazać należy, że na podstawie art. 10 ust. 1 oraz art. 10 a ust. 1 ustawy o strażach gminnych[96], straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. W celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych ujawniających dane wrażliwe. Strażnik wykonując zadania ustawowe ma prawo do dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych – w trybie i zakresie określonych w Kodeksie postępowania w sprawach o wykroczenia. Realizacja przez straż miejską zadań nałożonych na nią ustawowo wymaga wykorzystywania informacji o osobach, których działania te dotyczą. W ocenie Prezesa UODO oznacza to, że Komendant Straży Miejskiej, na mocy stosownych przepisów rangi ustawowej, ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie danych osobowych, zaś operator ten winien – mając na względzie fakt realizacji obowiązku czuwania przez straż miejską nad przestrzeganiem prawa przez obywateli – udostępnić informacje niezbędne straży miejskiej do realizacji jej zadań. W takiej sytuacji dochodzi bowiem do realizacji dyspozycji z przepisu art. 161 ust. 1 zdanie drugie Prawa telekomunikacyjnego.

[94] ZSPR.440.712.2019, ZSPR.440.1247.2018, ZSPR.440.1181.2018.
[95] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2019 r. poz. 2460 z późn. zm.
[96] Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych, Dz.U. z 2019 r. poz. 1795.9.

Jednocześnie Prezes UODO podkreślił, że nie stoją na przeszkodzie udostępnieniu danych osobowych abonenta przepisy art. 159 ust. 2 i 4 Prawa telekomunikacyjnego. Taki pogląd potwierdził również Naczelny Sąd Administracyjny w wyroku z dnia 14 marca 2019 r.[97], gdzie wskazał, że podziela stanowisko, iż „(…) przetworzenie (…) danych osobowych objętych tajemnicą telekomunikacyjną w celu przekazania ich Straży Miejskiej na potrzeby prowadzonego postępowania nie jest zakazane w świetle art. 159 ust. 1-4 ustawy Prawo telekomunikacyjne".

W ocenie Prezesa UODO, Komendant Straży Miejskiej posiada podstawę prawną do pozyskania danych osobowych abonenta, niezbędnych do przeprowadzenia czynności wyjaśniających i sporządzenia wniosku o ukaranie. W konsekwencji Prezes UODO nakazał ich udostępnienie[98].

Przetwarzanie danych w sektorze telekomunikacji

Przetwarzanie przez operatorów telekomunikacyjnych danych osobowych zawartych w kserokopii dokumentów tożsamości w celu potwierdzenia możliwości wykonania umowy

Prezes UODO wielokrotnie wskazywał, że dane osobowe zawarte w dowodzie osobistym, takie jak wizerunek i rysopis nie są danymi, które mogą być przetwarzane w celu wykonania umowy o świadczenie usług telekomunikacyjnych. Powyższe stoi w sprzeczności z zasadą minimalizacji, o której mowa w art. 5 ust. 1 lit. c RODO, zgodnie z którą administrator może przetwarzać dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Prezes UODO, rozstrzygając w sprawach skarg dotyczących przetwarzania danych osobowych zawartych w kserokopii dowodów osobistych, nie podzielał stanowiska wyrażanego przez operatorów telekomunikacyjnych, zgodnie z którym podstawą do przetwarzania danych osobowych zawartych w kserokopii ww. dokumentu może być art. 161 ust. 2 ustawy Prawo telekomunikacyjne[99]. Dowód osobisty nie jest w ocenie organu nadzorczego dokumentem potwierdzającym możliwość wykonania umowy o świadczenie usług telekomunikacyjnych. Dane zawarte w dowodzie służą przede wszystkim identyfikacji osoby, nie zaś potwierdzeniu, czy użytkownik będzie w stanie regulować rachunki za udostępnione mu usługi telekomunikacyjne"[100].

[97] Sygn. akt: I OSK 1429/17.
[98] DS.523.3050.2020.
[99] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. z 2019 r. poz. 2460.
[100] por. wyrok Naczelnego Sądu Administracyjnego z dnia 18 kwietnia 2018 r. sygn. akt I OSK 1354/16.

Udostępnienie przez operatorów telekomunikacyjnych danych osobowych podmiotom nieuprawnionym w wyniku incydentów bezpieczeństwa

W 2020 r. do Prezesa UODO wpłynęły liczne skargi dotyczące udostępnienia przez jednego z operatorów telekomunikacyjnych danych osobowych klientów podmiotom nieuprawnionym w wyniku incydentu bezpieczeństwa.

Prezes UODO wskazywał, że zgodnie z art. 4 pkt 7 RODO, na administratorze danych osobowych ciąży obowiązek prawny ich przetwarzania zgodnie z obowiązującymi przepisami. W szczególności obowiązek zapewnienia, by przetwarzanie odbywało się na podstawie co najmniej jednej z enumeratywnie wymienionych przesłanek art. 6 ust. 1 RODO. Przepis art. 5 ust. 1 lit. f RODO nakłada na administratora danych obowiązek przetwarzania danych osobowych zgodnie z zasadą integralności i poufności. Oznacza to, że administrator powinien 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.

W prowadzonych postępowaniach zainicjowanych indywidualną skargą, organ właściwy do spraw ochrony danych osobowych wskazywał, że mógł dokonać wyłącznie oceny legalności przetwarzania danych. Natomiast ogólne praktyki stosowane przez administratora danych w procesach ich przetwarzania, w tym sposoby zabezpieczeń, jak również ich adekwatność oraz skuteczność, mogły być jedynie przedmiotem postępowania wszczętego przez organ z urzędu. Prezes Urzędu stoi na stanowisku, iż skarga nie służy dokonywaniu kontroli zabezpieczenia danych na wniosek osoby, której dane dotyczą. Funkcją skargi jest egzekwowanie przestrzegania przepisów o ochronie danych osobowych w operacjach przetwarzania danych, które bezpośrednio wpływają na osobę, której przetwarzane dane dotyczą. Ocena prawidłowości zabezpieczeń następuje zatem wyłącznie w postępowaniu wszczętym przez organ z urzędu. Przyjęcie przeciwnego stanowiska oznaczałoby *de facto* możliwość zapoznania się przez wnioskodawcę, w ramach postępowania przed organem, ze sposobem zabezpieczenia danych (w tym danych innych osób) przez administratora danych osobowych, co samo w sobie zmniejsza poziom ochrony danych oraz może zwiększyć ryzyko ich naruszenia[101].

[101] DS.523.351.2020.

Przetwarzanie danych osobowych w ramach prowadzenia monitoringu

Przetwarzanie danych osobowych w postaci wizerunku, za pomocą monitoringu wizyjnego, jest co roku poruszane w bardzo wielu skargach. Monitoring stosowany jest w celu ochrony własności mienia oraz zdrowia i życia mieszkańców nieruchomości. Większość skarg związana była z konfliktem sąsiedzkim i narastającym brakiem zaufania wobec sąsiadów, co skutkowało wzajemnym niszczeniem mienia i stwarzania dodatkowych uciążliwości. W skrajnych sytuacjach spory sąsiedzkie przybierały formę „wyścigu zbrojeń" i wzajemnych skarg do organów państwowych, w tym do Prezesa UODO. W zakresie monitoringu nagminną sytuacją było kierowanie skarg do organu nadzorczego bez jakiejkolwiek wcześniejszej komunikacji z administratorem danych. O ile w przypadku osób fizycznych taki kontakt mógłby okazać się bezcelowy, o tyle w przypadku podmiotów prowadzących działalność gospodarczą, pozwalałby na uniknięcie wszczęcia postępowania. Często bowiem przedmiotem skarg była odmowa udostępnienia kopii danych w postaci fragmentu nagrania. Administratorzy jako podstawę odmowy wskazywali ochronę danych osobowych innych osób znajdujących się na nagraniu, bez przeanalizowania formy lub możliwości ochrony ich danych za pomocą prostych narzędzi informatycznych, służących anonimizacji danych.

Warto w tym miejscu zauważyć, że w dniu 29 stycznia 2020 r., po publicznych konsultacjach, Europejska Rada Ochrony Danych przyjęła drugą wersję Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo[102], która określiła jasne wytyczne, co do sposobu prowadzenia monitoringu, w tym również przez osoby fizyczne.

Poniżej omówiono kilka spraw w tym temacie.

W jednej ze spraw[103], wszczętej na wniosek przedstawiciela ustawowego małoletniego, skarżący podniósł, że odmówiono mu udostępnienia kopii dotyczących go danych osobowych w postaci nagrania z monitoringu wizyjnego. W trakcie zabawy dzieci doszło do wypadku, w wyniku którego małoletni doznał znacznego uszczerbku na zdrowiu. Spółka odmówiła udostępnienia nagrania monitoringu wizyjnego, powołując się na wyłączenie, o którym mowa w art. 15 ust. 4 rozporządzenia 2016/679[104]. W uzasadnieniu swojej odmowy wskazano, że na nagraniu monitoringu ujawnione są wizerunki innych dzieci, a udostępnienie nagrania naruszy ich prawa.

[102] Dostępne w języku polskim pod adresem https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_pl (dostęp: 12.02.2021).
[103] Decyzja z dnia 30 listopada 2020 r. sygn. ZWOS.440.5216.2019.
[104] Zgodnie z art. 15 ust. 4 rozporządzenia 2016/679, prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

W przedmiotowej sprawie skarżący wskazał spółce, że nagranie jest mu niezbędne do ustalenia i dochodzenia roszczeń odszkodowawczych, w tym również na drodze sądowej. Należy jednak zauważyć, że osoba, której dane dotyczą, nie ma obowiązku uzasadniania wniosku o wydanie kopii danych, gdyż przepisy nie przewidują takiego wymogu. W kompetencji administratora leży ocena, czy udostępnienie danych osobowych skarżącego w postaci nagrania z monitoringu nie będzie negatywnie wpływać na prawa i wolności innych osób. Uznanie, że do takiego wpływu dochodzi, nie może jednak stać się podstawą do pozbawienia podmiotu danych możliwości realizacji jego uprawnień wynikających z art. 15 ust. 3 rozporządzenia 206/679[105]. Administrator winien rozważyć, czy taką możliwość może wyeliminować, np. poprzez anonimizację.

Prezes UODO nakazał udostępnienie danych osobowych małoletniego w postaci nagrania z monitoringu wizyjnego, wskazując dzień i godziny nagrania, po uprzedniej anonimizacji danych osobowych osób postronnych, znajdujących się na nagraniu.

W kolejnej ze spraw skarżąca złożyła skargę na przetwarzanie jej danych osobowych bez podstawy prawnej za pomocą monitoringu wizyjnego, niespełnienie obowiązku informacyjnego spełnianego w przypadku zbierania danych od osoby, której dane dotyczą[106] oraz nieudostępnienie kopii przetwarzanych danych osobowych w zakresie wizerunku[107].

Pomiędzy stronami postępowania istniał silny konflikt sąsiedzki. Wizerunek skarżącej przetwarzany był wyłącznie w celu zapewnienia bezpieczeństwa. Materiał dowodowy zebrany w sprawie wskazał, że monitoring został zainstalowany w wyniku zachowania skarżącej i członków jej rodziny wobec skarżonej. Część z nagrań, na których utrwalony został wizerunek skarżącej i członków jej rodziny, m.in. ukazujący przerzucanie kamieni przez ogrodzenie na posesję skarżonej, została udostępniona na rzecz policji, jako materiał stanowiący dowód w prowadzonym postępowaniu karnym. W toku postępowania przed Prezesem UODO ustalono, że system monitoringu wizyjnego składał się z pięciu kamer, w tym trzech kamer stałych, jednej kamery obrotowej oraz jednej kamery atrapy. System monitoringu nie obejmował zasięgiem posesji skarżącej, ale wykraczał poza nieruchomość osoby, do której należał monitoring. Przy wejściu do

[105] Zgodnie z art. 15 ust. 3 rozporządzenia 2016/679 administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
[106] Zob. art. 13 rozporządzenia 2016/679.
[107] Decyzja z dnia 16 listopada 2020 r. sygn. DS.440.122.2019.

budynku umieszczona została tablica informująca o zainstalowanym monitoringu. Nagrania zapisywane były na laptopie skarżonej, który zabezpieczony był hasłem dostępu. Skarżąca nigdy nie zwracała się z wnioskiem o uzyskanie kopii danych.

Prezes UODO uznał, że podstawą prawną przetwarzania danych osobowych skarżącej w zakresie jej wizerunku jest art. 6 ust. 1 lit. f rozporządzenia 2016/679[108]. Zapewnienie bezpieczeństwa osób i mienia w obszarze objętym monitoringiem jest prawnie usprawiedliwionym celem skarżonej – administratora danych osobowych. Ze względu na to, że zasięg kamer monitoringu wizyjnego należącego do skarżonej wykraczał poza jej nieruchomość – monitoring wizyjny obejmował swym zasięgiem przestrzeń publiczną – przetwarzanie dokonywane za jego pomocą musiało być zgodne z przepisami o ochronie danych osobowych. Tym samym uznano, że skarżona zobowiązana była między innymi do zrealizowania obowiązku informacyjnego, rozpatrywania żądań osób obserwowanych i właściwego zabezpieczania nagrań.

W wyjaśnieniach złożonych przed Prezesem UODO skarżona wskazała, że na budynku obok wejścia zamontowana została tablica informacyjna o treści „Obiekt Monitorowany". Skarżona nie wskazała jednak skarżącej informacji podawanych w przypadku zbierania danych od osoby, której dane dotyczą[109], m.in. w zakresie celu przetwarzania jej danych, okresie ich przechowywania, ich odbiorcach czy przysługujących skarżącej prawach. Stwierdzono, że zamontowanie znaku informującego o monitorowaniu nieruchomości nie stanowiło wypełnienia norm art. 13 rozporządzenia 2016/679 w pełnym zakresie. Nakazano uzupełnienie treści obowiązku informacyjnego.

Uprawnienie wynikające z art. 15 ust. 3 rozporządzenia 2016/679 (prawo uzyskania kopii danych) zobowiązuje administratora do wynikającego z treści tego przepisu działania dopiero wówczas, gdy osoba ta zwróci się do administratora z żądaniem uzyskania kopii dotyczących jej danych. Prezes UODO może podjąć działania naprawcze, gdy administrator nie ustosunkuje się do żądania tej osoby w wyznaczonym do tego przepisami terminie[110] lub ustosunkuje się do otrzymanego żądania, ale w sposób odmowny lub niepełny. Skarżąca nigdy nie zwracała się do

[108] Zgodnie z art. 6 ust. 1 lit. f rozporządzenia 2016/679, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
[109] Wynikających z treści art. 13 rozporządzenia 2016/679.
[110] W terminie określonym w art. 12 ust. 3 rozporządzenia 2016/679, tj. miesięcznym od otrzymania żądania, który w szczególnych sytuacjach może zostać przedłużony o dwa kolejne miesiące.

skarżonej z wnioskiem o realizację prawa do uzyskania kopii dotyczących jej danych osobowych, ani nie przedstawiła przed organem żadnych dowodów na potwierdzenie skierowania do skarżonej takiego żądania. Prezes UODO odmówił więc uwzględnienia wniosku skarżącej w tym zakresie.

Kolejna sprawa dotyczyła monitoringu składającego się z kilku kamer, który obejmował swoim zasięgiem zarówno nieruchomość skarżonego, jak i przestrzeń publiczną[111]. Skarżony podkreślił, że jego działanie stanowiło przetwarzanie danych w trakcie czynności o czysto osobistym lub domowym charakterze, tym samym wyłączone jest zastosowanie norm rozporządzenia 2016/679. Monitoring wizyjny został zainstalowany na terenie należącej do niego nieruchomości z konieczności przeciwdziałania czynom karalnym, popełnionym na jego szkodę, do których to czynów miał również podżegać skarżący.

Prezes UODO uznał, że skarżony nie wykazał żadnej podstawy prawnej, która uzasadniałaby przetwarzanie przez skarżonego danych osobowych skarżących, pochodzących z monitoringu wizyjnego wykraczającego poza granice jego nieruchomości. Wskazana przez skarżonego potrzeba zapewnienia bezpieczeństwa mieniu i ludziom jest uzasadnieniem dla wykonywania monitoringu wizyjnego ograniczonego swoim zasięgiem wyłącznie do terenu nieruchomości będącej własnością skarżonego. Brak technicznych możliwości ograniczenia głębi obrazu nie oznacza posiadania przesłanki dla legalności przetwarzania danych innych osób przebywających w przestrzeni publicznej poza nieruchomością należącą do skarżącego. Skarżony nie wykazał również, że dokonuje blokowania wyświetlania nieistotnych obszarów lub ich zamazywania.

Prezes UODO wydał decyzję nakazującą skarżącemu zaprzestania przetwarzania danych osobowych skarżących, pochodzących z nagrań z monitoringu wizyjnego, wykraczającego poza granice należącej do niego nieruchomości.

W innej ze spraw skarżąca złożyła skargę na przetwarzanie jej danych osobowych za pomocą monitoringu przez właściciela sąsiedniej posesji. W toku postępowania ustalono, że system monitoringu składał się z imitacji 3 kamer przemysłowych, które pozbawione były możliwości rejestracji i zapisu obrazu. Imitacje zasilane były bateriami, posiadały wbudowaną sygnalizację LED oraz symulację ruchu. Ze względu na brak procesu przetwarzania danych osobowych Prezes UODO umorzył postępowanie[112].

[111] Decyzja z dnia 18 sierpnia 2020 r. sygn. ZSPR.440.1194.2018.
[112] Decyzja z dnia 9 listopada 2020 r. sygn. ZWOS.440.4572.2019.

Kolejna ze spraw dotyczyła przetwarzania danych osobowych osoby fizycznej przez spółkę[113]. Skarżący wskazał, że w trakcie jego pobytu w zakładzie produkcyjno-handlowym zauważył, że na sąsiadującej działce znajduje się nieoznaczona kamera wideo.

Ustalono, że zasięg monitoringu obejmował teren należącego do spółki składu, teren wzdłuż ogrodzenia z każdej ze stron, parkingi oraz drogę wewnętrzną wykorzystywaną wspólnie z innymi podmiotami prowadzącymi działalność gospodarczą. Spółka legitymowała się podstawą prawną do przetwarzania danych osobowych, wynikającą z jej uzasadnionego interesu. Należy jednak podkreślić, że uzasadniony interes administratora danych musi zostać wykazany oraz nie może mieć on charakteru hipotetycznego. W ocenie organu w przedmiotowej sprawie przesłanki te zostały spełnione. Spółka wskazała, że charakter prowadzenia działalności, oraz w szczególności obecność na składach towaru wartego przeszło kilka milionów złotych, specjalistycznego sprzętu i pojazdów uzasadnia zastosowanie przez nią monitoringu wizyjnego w celu zapewnienia właściwej ochrony mienia spółki. Przemysłowy charakter okolicznych terenów, obecność linii kolejowych, fakt popełniania przestępstw przeciwko mieniu na przedmiotowym terenie oraz brak budownictwa mieszkaniowego stwarza znaczne zagrożenie dla mienia spółki. Ponadto w toku postępowania spółka w sposób wyczerpujący przedstawiła zasady działania stosowanego przez nią monitoringu wizyjnego, stosowane zabezpieczenia oraz procedurę realizacji praw podmiotów danych.

Jak ustalono, wskazywana w treści skargi kamera nie była sprawna i nie była podłączona do zapisywania monitoringu, stanowiła w zasadzie tzw. atrapę kamery. Nie była również wprost skierowana na teren należący do zakładu, z którego korzystał skarżący, a w okolice wspólnej drogi wewnętrznej. Ze względu jednak na to, że zasięgiem monitoringu wizyjnego spółki objęta była również m.in. droga wewnętrzna oraz że dane osobowe skarżącego były przetwarzane przez spółkę podczas jego wizyty na jej terenie, konieczne było spełnienie stosownych obowiązków informacyjnych.

Spółka wskazała, że na terenie jej zakładu, pomiędzy bramą główną a bramami wjazdowymi, na tablicach znajduje się informacja wskazująca, że teren jest monitorowany. Ponadto szczegółowa informacja udzielana jest telefonicznie lub osobiście w siedzibie firmy poprzez okazanie stosownego regulaminu. Ustalono, że spółka nie wskazała jednak skarżącemu informacji wynikających z treści art. 13 rozporządzenia 2016/679 w pełnym zakresie, m.in. w zakresie celu przetwarzania danych

[113] Decyzja z dnia 2 grudnia 2020 r. sygn. ZSPR.440.992.2019.

osobowych, okresie ich przechowywania, ich odbiorcach czy przysługujących podmiotom danych prawach. Prezes UODO nakazał uzupełnienie informacji.

Należy podkreślić, że dla jasności i przejrzystości przekazu, administratorzy danych osobowych mogą przyjąć tzw. warstwowe spełnienie obowiązku informacyjnego, spełnianego wobec osób, których dane osobowe są lub mogą być pozyskiwane za pomocą monitoringu wizyjnego. Podejście to zakłada rozdzielenie informacji, które mają zostać przekazane na poszczególne etapy (warstwy), które są ze sobą spójne i umieszczone w miejscach łatwo dostępnych dla osoby, której dane dotyczą. Szczegółowe zakresy informacji dla poszczególnych warstw określone zostały m.in. w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urząd.

4.1.5. Inne decyzje zainicjowane skargą

Kontaktowanie się partii politycznej z byłym członkiem

Przedmiotem postępowania administracyjnego prowadzonego przez Prezesa UODO w 2020 r. była legalność wysyłania do byłego członka partii politycznej zaproszeń na spotkania okolicznościowe kierowane do członków tej partii.

Osoba otrzymująca te zaproszenia przez pewien czas była zatrudniona w tej partii oraz była jej członkiem. Jednak po ustaniu zatrudnienia i po złożeniu rezygnacji z członkostwa w partii oraz mimo przesłania wniosku o usunięcie danych osobowych z rejestrów partii, były jej członek wciąż otrzymywał zaproszenia na różne spotkania okolicznościowe wysyłane do członków partii, co stało się przedmiotem jego skargi do organu ds. ochrony danych osobowych.

Prezes UODO, po przeanalizowaniu wszystkich okoliczności, uznał, że działanie takie było bezprawne i wydał decyzję[114] udzielającą partii upomnienia. Wskazał, że dane osobowe w każdym przypadku muszą być przetwarzane przez administratora zgodnie ze wszystkimi zasadami określonymi w art. 5 RODO, w tym m.in. z tzw. zasadą legalności oraz zasadą ograniczonego celu. Pierwsza z nich stanowi, że dane osobowe muszą być przetwarzane przez administratora zgodnie z prawem, tj. na podstawie przynajmniej jednej z przesłanek określonych w art. 6 RODO. Z zasady ograniczonego celu wynika natomiast, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

[114] ZSPU.440.454.2019.

Organ nadzorczy wskazał, że przepisy RODO przyznają osobie, której dane dotyczą, liczne uprawnienia związane z przetwarzaniem jej danych osobowych przez administratora, w tym prawo do żądania usunięcia danych osobowych. Jednak może ono zostać skutecznie zrealizowane w przypadku, gdy zostaną spełnione przesłanki wprost wskazane w art. 17 ust. 1 lit. a – f RODO. Co istotne, prawo do usunięcia danych osobowych jest w określonych sytuacjach wyłączone. Stosownie bowiem do art. 17 ust. 3 RODO prawo do usunięcia danych osobowych nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne m.in. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W przypadku zaistnienia tej okoliczności, podmiot danych nie będzie uprawniony do żądania od administratora usunięcia jego danych osobowych.

W wydanej decyzji Prezes UODO wskazał, że w analizowanej sprawie partia była zobowiązana do przechowywania dokumentacji pracowniczej skarżącego, który kiedyś był jej pracownikiem – tym samym miała prawo do przetwarzania w tym celu jego danych osobowych. Zgodnie bowiem z art. 94 pkt 9a Kodeksu pracy[115] pracodawca jest obowiązany prowadzić i przechowywać w postaci papierowej lub elektronicznej dokumentację w sprawach związanych ze stosunkiem pracy oraz akta osobowe pracowników (dokumentacja pracownicza). Zgodnie z pkt 9b tego przepisu pracodawca jest także obowiązany przechowywać dokumentację pracowniczą w sposób gwarantujący zachowanie jej poufności, integralności, kompletności oraz dostępności, w warunkach niegrożących uszkodzeniem lub zniszczeniem przez okres zatrudnienia, a także przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł, chyba że odrębne przepisy przewidują dłuższy okres przechowywania dokumentacji pracowniczej. W myśl art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych[116] płatnik składek jest zobowiązany przechowywać listy płac, karty wynagrodzeń albo inne dowody, na podstawie których następuje ustalenie podstawy wymiaru emerytury lub renty – co do zasady – przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracy u danego płatnika. Tym samym przetwarzanie danych osobowych skarżącego we wskazanych wyżej celach było uprawnione, gdyż spełniało przesłankę z art. 6 ust. 1 lit. c RODO.

[115] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, t.j. Dz. U. z 2019 r. poz. 1040 z późn. zm.
[116] Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, t.j. Dz. U. z 2020 r. poz. 53 z późn. zm.

Jednocześnie Prezes UODO uznał, że wniosek skarżącego o usunięcie wszystkich jego danych osobowych przetwarzanych przez partię nie mógł zostać przez nią zrealizowany. Prawo do usunięcia danych osobowych jest bowiem wyłączone, jeśli ich przetwarzanie jest niezbędne do wywiązania się z obowiązku prawnego (stosownie do treści powołanego art. 17 ust. 3 lit. b RODO).

Natomiast od dnia, od którego skarżący przestał być członkiem partii, nie powinna ona przetwarzać jego danych osobowych w celach związanych z zapraszaniem go na wydarzenia okolicznościowe organizowane dla członków tej partii. Działanie takie Prezes UODO uznał za naruszające zasadę ograniczonego celu, o której mowa w art. 5 ust. 1 lit. b RODO, za co udzielił partii upomnienia.

Zaświadczenie o przekształceniu prawa użytkowania wieczystego w prawo własności

Na skutek otrzymanej skargi, Prezes UODO w 2020 r. analizował kwestię tego, czy zaświadczenie o przekształceniu prawa użytkowania wieczystego w prawo własności powinno zawierać dane osobowe beneficjenta przekształcenia.

Osoba wnosząca skargę uważała, że burmistrz, wpisując jej dane osobowe w takie zaświadczenie i rozsyłając je do wszystkich dotychczasowych 11 współużytkowników wieczystych nieruchomości, bezprawnie udostępnił jej dane osobowe. Burmistrz w wyjaśnieniach skierowanych do Prezesa UODO wskazał, że podstawą prawną wydania zaświadczenia o przekształceniu prawa użytkowania wieczystego była ustawa z dnia 20 lipca 2018 r. o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów[117]. Podniósł, że w obowiązującym stanie prawnym zaświadczenie wydawane jest m.in. na wniosek właściciela lokalu, uzasadniony potrzebą dokonania czynności prawnej mającej za przedmiot lokal, zaś organ zobowiązany jest do wydania zaświadczenia w terminie 30 dni od dnia otrzymania wniosku. Zaznaczył, że z przepisów powołanej ustawy nie wynika przy tym, by organ zobowiązany był wydać kilka zaświadczeń – odrębnie dla każdego lokalu i związanego z tym lokalem udziału w gruncie. Burmistrz wskazał również, że dane użytkowników wieczystych tej nieruchomości są danymi pozyskanymi jeszcze przed wejściem w życie RODO, zaś dane zawarte w wydanym zaświadczeniu (oprócz adresu) są danymi zawartymi w księdze wieczystej gruntowej i księgach wieczystych lokalowych, które są dostępne dla każdego z właścicieli nieruchomości.

[117] Ustawa z dnia 20 lipca 2018 r. o przekształceniu prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów, t.j. Dz.U. z 2020 r. poz. 139.

Prezes UODO ustalił, że zakres danych osobowych osoby, która wniosła skargę, udostępnionych w zaświadczeniu wydanym przez burmistrza na rzecz 11 współwłaścicieli nieruchomości, mieści się w granicach tzw. danych zwykłych. Przesłanki legalizujące przetwarzanie takich danych zawarte są w art. 6 ust. 1 RODO. Ich katalog ma charakter zamknięty, zaś każda z nich jest przesłanką autonomiczną i niezależną. Oznacza to, że przesłanki te co do zasady są równoprawne, toteż spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych.

Na burmistrzu jako administratorze ciąży zaś obowiązek przetwarzania danych osobowych zgodnie z obowiązującymi przepisami, w tym z poszanowaniem zasad określonych w art. 5 ust. 1 RODO, a więc m.in. zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą.

Organ właściwy ws. ochrony danych osobowych podzielił opinię burmistrza, iż na gruncie powołanej ustawy z dnia 20 lipca 2018 r., przekształcenie prawa użytkowania wieczystego gruntów zabudowanych na cele mieszkaniowe w prawo własności tych gruntów, w każdym przypadku dotyczy całej nieruchomości gruntowej, niezależnie od tego, czy jest ona przedmiotem współużytkowania wieczystego. Podstawę ujawnienia prawa własności gruntu w księdze wieczystej oraz ewidencji gruntów i budynków stanowi zaświadczenie potwierdzające przekształcenie, zatem zasadne będzie stwierdzenie, iż jedno przekształcenie to jedno zaświadczenie.

Zgodnie z art. 4 ust. 3 powołanej ustawy, zaświadczenie zawiera oznaczenie nieruchomości gruntowej lub lokalowej według ewidencji gruntów i budynków oraz ksiąg wieczystych prowadzonych dla tych nieruchomości. Artykuł 4 ust. 4 ustawy stanowi natomiast, że w zaświadczeniu potwierdza się przekształcenie oraz informuje o obowiązku wnoszenia rocznej opłaty przekształceniowej, wysokości i okresie jej wnoszenia, a także możliwości wniesienia opłaty jednorazowej, o której mowa w art. 7 ust. 7 ustawy, i zasadach jej wnoszenia.

Prezes UODO podkreślił, iż przepisy nie wymagają, aby w zaświadczeniu wskazany był beneficjent przekształcenia. Właściwy organ jest bowiem zobowiązany do wydania zaświadczenia właścicielowi nieruchomości (na wniosek, bądź z urzędu). W związku z tym, iż z przekształceniem wiąże się m.in. obowiązek uiszczania opłat przekształceniowych i obowiązanym do uiszczania tych opłat jest każdy obecny współwłaściciel nieruchomości podlegającej przekształceniu w różnych częściach, w ocenie Prezesa UODO, wskazane byłoby umieszczenie danych beneficjenta przekształcenia wyłącznie w rozdzielniku, zawierającym informacje, dla kogo przeznaczone są kopie pisma.

Zatem w ocenie Prezesa UODO doszło w tym przypadku do naruszenia przepisów o ochronie danych osobowych, tj. art. 5 ust. 1 lit. a RODO oraz art. 6 ust. 1 RODO. Dlatego w wydanej w tej sprawie decyzji[118] organ nadzorczy udzielił burmistrzowi upomnienia.

Dopełnianie obowiązku informacyjnego

Przepisy RODO wprowadziły istotne zmiany dotyczące dopełniania tzw. obowiązku informacyjnego, w tym rozszerzyły jego zakres. Ma to służyć zapewnieniu osobom, których dane dotyczą, podstawowej wiedzy o tym, co będzie się działo z ich danymi osobowymi.

O tym, że obowiązek informacyjny nie zawsze bywa realizowany prawidłowo może świadczyć sprawa zainicjowana skargą osoby będącej stroną postępowania administracyjnego prowadzonego przez policję.

O ile w toku postępowania pierwszej instancji Komendant Wojewódzki Policji dopełnił obowiązek informacyjny, o którym mowa w art. 13 RODO, o tyle Komendant Główny Policji, wszczynając postępowanie drugiej instancji, tego obowiązku nie zrealizował. Dlatego Prezes UODO w wydanej w tej sprawie decyzji[119] nakazał jego dopełnienie.

W uzasadnieniu organ nadzorczy podniósł, że „stosownie do art. 61 § 5 K.p.a.[120] organ administracji publicznej przekazuje informacje, o których mowa w art. 13 ust. 1 i 2 RODO, przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie, zaś zgodnie z art. 140 K.p.a., w sprawach nieuregulowanych w art. 136-139 K.p.a., w postępowaniu przed organami odwoławczymi mają odpowiednie zastosowanie przepisy o postępowaniu przed organami pierwszej instancji".

Organ nadzorczy wskazał, że w zakresie prowadzenia postępowania administracyjnego pierwszej i drugiej instancji, Komendant Wojewódzki Policji oraz Komendant Główny Policji są odrębnymi administratorami, zatem obaj byli zobowiązani do wypełnienia wobec skarżącego obowiązku informacyjnego w związku z wszczęciem postępowania – odpowiednio – pierwszej i drugiej instancji. Wskazać jednak należy, że wydana w tej sprawie decyzja Prezesa UODO nie jest prawomocna, gdyż sprawa – na skutek złożonej wcześniej skargi na bezczynność organu – trafiła do WSA w Warszawie.

[118] ZSPU.440.218.2019.
[119] ZWOS.440.5927.2019.
[120] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, t.j. Dz. U. z 2020 r. poz. 256.

Wykorzystanie danych służbowych w celach prywatnych

Rozpatrywane przez organ nadzorczy sprawy dowodzą także, że wciąż zdarzają się sytuacje wykorzystywania do celów prywatnych danych osobowych, do których pracownicy administratora mają dostęp w związku z wykonywaną pracą.

W 2020 r. w jednym z takich przypadków Prezes UODO udzielił prezydentowi miasta upomnienia[121]. W toku zainicjowanego skargą postępowania okazało się bowiem, że kierownik jednego z referatów w urzędzie miasta wykorzystał dane osobowe skarżących, zawarte w piśmie dotyczącym udzielenia pomocy, a jednocześnie zawierającym skargę na jego zachowanie, do prywatnej korespondencji. Choć z kierownikiem przeprowadzono rozmowę pouczającą oraz wyciągnięto konsekwencje służbowe, udzielając mu upomnienia, to przed organem nadzorczym odpowiedzialność poniósł prezydent miasta będący administratorem danych interesantów.

W uzasadnieniu decyzji Prezes UODO wskazał, że zgodnie z art. 5 ust. 1 lit. f RODO, „obowiązkiem administratora jest przetwarzanie danych w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. (…) Z zebranego w niniejszej sprawie materiału dowodowego wynika, że prezydent w procesie przetwarzania danych osobowych skarżących naruszył zasadę celowości i poufności danych, dopuszczając, by pracownik urzędu, bez zgody i wiedzy administratora, wykorzystał posiadane informacje służbowe do celów prywatnych. Uprawnienie do dostępu i przetwarzania danych osobowych ze względu na pełnione obowiązki służbowe ogranicza się jedynie do zakresu tych obowiązków. Poprzez wdrażanie odpowiednich procedur oraz zwiększanie kompetencji pracowników, administrator zobowiązany jest dbać, by nie dochodziło u niego do wykorzystania danych osobowych w celach przekraczających przydzielone pracownikom zadania, a tym bardziej w celach prywatnych. W każdym przypadku bowiem to na administratorze spoczywa obowiązek przetwarzania ich zgodnie z zasadami przewidzianymi w art. 5 RODO”.

Dostęp do danych osób składających skargi

W analizowanym roku 2020 wciąż zdarzały się sytuacje nieuprawnionego udostępniania danych osób, które składały skargi do różnych instytucji.

[121] ZSPU.440.1092.2019.

Było tak m.in. w przypadku pasażera, który złożył do Miejskiego Przedsiębiorstwa Komunikacyjnego (MPK) skargę na kierowcę autobusu. Wykorzystał do tego elektroniczny formularz kontaktowy udostępniony przez MPK. Podał w nim swoje imię i nazwisko oraz adres e-mail. Wskutek niedopatrzenia pracownika, który przekazał kierowcy kopię skargi, dane skarżącego pasażera nie zostały zanonimizowane we wszystkich miejscach. Kierowca mógł więc poznać dane skarżącego, choć nie był do tego uprawniony. Realizacja celu, jakim było rozpatrzenie skargi, była bowiem możliwa bez przekazania danych osobowych.

W wydanej w tej sprawie decyzji[122] Prezes UODO podkreślił, że z chwilą otrzymania formularza skargi, MPK stało się administratorem zawartych w niej danych osobowych. Jego obowiązkiem – zgodnie z art. 5 ust. 1 lit. f RODO – było przetwarzanie danych w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Administrator powinien w tym celu wdrożyć właściwe środki techniczne i organizacyjne, odpowiednie do ryzyka związanego z przetwarzaniem tych danych. Bezsprzecznie w analizowanym przypadku doszło do naruszenia przez MPK zasady poufności danych, gdyż podmiot ten dopuścił do tego, by z danymi pasażera, który złożył skargę, zapoznała się osoba nieuprawniona, tj. kierowca autobusu.

Niemniej Prezes UODO, stwierdzając naruszenie, uznał upomnienie za wystarczającą reakcję w tej sprawie. Wziął bowiem pod uwagę jego incydentalny charakter oraz późniejsze działania MPK, tj. dodatkowe przeszkolenie pracowników oraz dokonanie analizy procedury rozpatrywania skarg pod kątem możliwości wprowadzenia anonimizacji danych osobowych osób składających skargi jeszcze przed ich przekazaniem do komórki organizacyjnej, rozpatrującej sprawę zgodnie z właściwością.

Brak właściwości Prezesa UODO

W niektórych prowadzonych w 2020 r. postępowaniach Prezes UODO stwierdzał brak swojej właściwości do ich rozstrzygania.

Przykładem może być sprawa, której przedmiotem było przetwarzanie danych osobowych przez ABW, w związku z przeprowadzeniem poszerzonego postępowania sprawdzającego w rozumieniu art. 23 ust. 2 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[123],

[122] ZSPU.440.557.2019.
[123] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. z 2019 r. poz. 742.

w zakresie szerszym niż uprawniają ją do tego przepisy. Po przeprowadzeniu postępowania wyjaśniającego Prezes UODO wydał decyzję[124], mocą której umorzył postępowanie, uznając brak swojej właściwości. Uznał, iż działania podjęte przez ABW wobec skarżącego nie mogą zostać ocenione w kontekście zgodności z przepisami regulującymi zasady przetwarzania danych osobowych, w tym z RODO i Dyrektywą 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[125]. Wskazał, że zgodnie z art. 6 pkt 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, przepisów tej ustawy oraz przepisów RODO nie stosuje się do działalności służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[126]. Zgodnie z treścią art. 5 ust. 1 pkt 3 tej ustawy do zadań ABW należy m.in. realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych. Jednocześnie zaznaczył, że zgodnie z art. 3 pkt 2 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[127], przepisów tej ustawy nie stosuje się do ochrony danych osobowych przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego.

W uzasadnieniu rządowego projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[128] wskazano, że: „Dyrektywa 2016/680 nie ma zastosowania do czynności podmiotów zajmujących się bezpieczeństwem narodowym (art. 2 ust. 3 lit. a w zw. z motywem 14 dyrektywy), a zatem w polskim systemie prawnym nie powinna być

[124] ZSPU.440.1238.2019.
[125] 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, Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.
[126] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2018 r. poz. 2387, 2245 i 2399 oraz z 2019 r. poz. 53, 125 i 1091.
[127] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz. U. z 2019 r. poz. 125.
[128] Druk nr 2989.

stosowana do służb specjalnych, tj. Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego. Realizacja szczegółowo określonych ustawowych zadań każdego z wymienionych podmiotów ma na celu zapewnienie bezpieczeństwa narodowego w różnych jego aspektach – zgodnie z zakresem kompetencyjnym każdej ze służb – co przemawia za podmiotowym wyłączeniem z zakresu regulacji projektowanej ustawy. (...) Mając na względzie, że analogiczne wyłączenia zostały przewidziane w rozporządzeniu 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 uchylające dyrektywę 95/46/WE, a także w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych, powstała potrzeba zmiany ustaw regulujących funkcjonowanie służb specjalnych (ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym) przez wprowadzenie przepisów stanowiących samoistną podstawę przetwarzania danych osobowych przez te podmioty".

Prezes UODO powołał również fragment uzasadnienia postanowienia WSA w Warszawie z 10 grudnia 2018 r.[129], w którym wskazano, że „(...) przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[130] nie mają zastosowania do działalności służb specjalnych, w tym ABW, z uwagi na wyłączenie wynikające z art. 6 pkt 2 tej ustawy".

Zgodnie z art. 2 ust. 2 lit. a RODO przepisy tego rozporządzenia nie mają zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa Unii. Jako przykład działalności nieobjętej zakresem prawa Unii w motywie 16 RODO wskazano zaś bezpieczeństwo narodowe. W myśl art. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Agencja Bezpieczeństwa Wewnętrznego jest właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

W związku z tym Prezes UODO postępowanie umorzył. Z tym rozstrzygnięciem organu nadzorczego nie zgodziła się jednak osoba, której sprawa dotyczyła i decyzję Prezesa UODO zaskarżyła do WSA.

[129] Sygn. akt II SAB/Wa 655/18, opubl. LEX nr 2734633.
[130] Dz. U. z 2018 r. poz. 1000 z późn. zm.

Brak swojej właściwości Prezes UODO stwierdził także w przypadku skargi osoby, która zarzucała sędzi sądu bezprawne udostępnienie radcom prawnym jej danych osobowych, zawartych w sprawozdaniu kuratora oraz w aktach prowadzonej przez sąd sprawy.

Po przeanalizowaniu zebranego w sprawie materiału dowodowego Prezes UODO umorzył postępowanie, stwierdzając brak swojej kompetencji do merytorycznego rozpatrywania skargi. W wydanej w tej sprawie decyzji[131] wskazał, że wbrew twierdzeniu osoby skarżącej nie doszło do bezprawnego udostępnienia akt postępowań toczących się przed sądem ani znajdujących się w nich danych osobowych osobom nieupoważnionym. Podkreślił, że przedmiot skargi dotyczy czynności z zakresu sprawowania przez sąd wymiaru sprawiedliwości, a zasady udostępniania akt cywilnego postępowania sądowego reguluje ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego[132], nie zaś przepisy dotyczące zasad ochrony danych osobowych. W tej sytuacji Prezes UODO, odwołując się m.in. do motywu 20 RODO[133], stwierdził brak właściwości rzeczowej Prezesa UODO w zakresie przetwarzania danych przez sądy w ramach sprawowania wymiaru sprawiedliwości.

Podkreślił, że podstawowym celem wyłączenia w tym zakresie jest ochrona niezawisłości sądów. Wykonywanie przez organ właściwy w sprawach ochrony danych nadzoru nad przetwarzaniem danych w zakresie orzekania, mogłoby stanowić niedopuszczalną ingerencję w działalność orzeczniczą. Prezes UODO, w ramach kompetencji przyznanych mu ustawą, nie może zatem ingerować w tok ani w sposób postępowań prowadzonych przez inne, uprawnione na podstawie odrębnych przepisów organy. Tym samym nie może ingerować także w zasady udostępniania dokumentów zgromadzonych przez sąd w aktach takich postępowań. Innymi słowy Prezes UODO nie może podejmować czynności dotyczących postępowań prowadzonych przez inne organy na podstawie właściwych przepisów prawa. Powyższy pogląd znajduje potwierdzenie w orzecznictwie Naczelnego Sądu Administracyjnego, który w wyroku z dnia 2 marca 2001 r.[134]

---

[131] ZSOSS.440.51.2019.

[132] t.j. Dz. U. z 2020 r. poz. 1575 z późn. zm.

[133] Motyw 20 RODO: „Niniejsze rozporządzenie ma zastosowanie między innymi do działań sądów i innych organów wymiaru sprawiedliwości, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość sprawowania wymiaru sprawiedliwości. Powinna istnieć możliwość powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim operacjami przetwarzania danych”.

[134] sygn. akt II SA 401/00.

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. Przetwarzanie przez sąd w ramach sprawowania wymiaru sprawiedliwości podlega kontroli organu nadzorczego innego niż Prezes Urzędu Ochrony Danych Osobowych. Sądy są administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej. Stosownie do art. 175 dd § 1 ustawy z dnia 27 lipca 2001 r. Prawa o ustroju sądów powszechnych[135], nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy, zgodnie z art. 175 da i art. 175 db, wykonują w zakresie działalności sądu: rejonowego – prezes sądu okręgowego; okręgowego – prezes sądu apelacyjnego; apelacyjnego – Krajowa Rada Sądownictwa. W sytuacji zatem, gdy osoba, której dane dotyczą, ma wątpliwości co do prawidłowego przetwarzania jej danych osobowych, może złożyć skargę do właściwego organu sądowego.

Z uwagi na powyższe organ nadzorczy podkreślił, że dane osobowe były przetwarzane przez sąd wyłącznie w postępowaniu sądowym i w związku ze sprawowanym wymiarem sprawiedliwości, co przesądza o braku kompetencji Prezesa UODO do merytorycznego rozpatrywania złożonej skargi. W tej sytuacji postępowanie zostało umorzone.

4.2. Zawiadomienie o podejrzeniu popełnienia przestępstwa

W analizowanym 2020 r. Prezes Urzędu Ochrony Danych Osobowych skierował do organów powołanych do ścigania przestępstw **2 zawiadomienia o podejrzeniu popełnienia przestępstwa przez osoby odpowiedzialne za przetwarzanie danych osobowych.**

Jedno z tych zawiadomień związane było z naruszeniem ochrony danych osobowych, drugie zaś dotyczyło utrudniania przeprowadzenia czynności kontrolnych w spółce świadczącej usługi telemarketingowe.

Dla przykładu, Prezes UODO, decyzją z 9 marca 2020 r.[136], nałożył na Vis Consulting Sp. z o.o. w likwidacji z siedzibą w Katowicach karę w wysokości 20 000 zł, za uniemożliwienie przeprowadzenia kontroli. Organ nadzorczy uznał za konieczne przeprowadzenie czynności kontrolnych w spółce w związku z uzyskaniem informacji, że dostarczyła ona innemu podmiotowi

[135] t.j. Dz. U. z 2020 r. poz. 365 z późn. zm.
[136] sygn. akt: ZSPR.421.19.2019.

system informatyczny, który wykonywał połączenia telefoniczne w celu przedstawienia ofert marketingowych i przetwarzał dane osobowe. Z dokonanych ustaleń wynika, że przedmiotowy system użytkowany był na podstawie umowy w zakresie outsourcingu usług telemarketingowych zawartej między tym podmiotem a spółką.

Pomimo że spółka została prawidłowo poinformowana o terminie i zakresie kontroli, kontrola nie mogła się odbyć, gdyż w siedzibie podmiotu nie zastano żadnej osoby uprawnionej do jego reprezentacji. W zaistniałej sytuacji kontrolerzy UODO próbowali bezskutecznie skontaktować się z ww. podmiotem telefonicznie. Pełnomocnik spółki nawiązał z nimi ostatecznie kontakt, informując, że kontrola nie odbędzie się. Takie działania podmiotu Prezes UODO uznał za odmowę współpracy z organem. 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, a także 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. Istotne znaczenie ma również fakt, że w terminie zaplanowanej kontroli władze spółki podjęły uchwałę o likwidacji tego podmiotu.

Wobec powyższego Prezes UODO uznał, że spółka swoim działaniem naruszyła przepis art. 31 w związku z art. 58 ust. 1 lit. e oraz lit. f rozporządzenia 2016/679, zgodnie z którym administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele, na żądanie mają obowiązek współpracować z organem nadzorczym w ramach wykonywania przez niego swoich zadań. Na tej podstawie Prezes UODO uznał, że zostały spełnione przesłanki do nałożenia kary pieniężnej.

Dodatkowo, w związku z podejrzeniem popełnienia przestępstwa z art. 108 ust. 1 ustawy o ochronie danych osobowych przez prezesa zarządu spółki, Prezes UODO złożył zawiadomienie do Prokuratury Rejonowej w Katowicach. Zgodnie z ww. przepisem, za udaremnianie lub utrudnianie prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych, grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności do lat dwóch. Prokuratura skierowała do sądu akt oskarżenia przeciwko prezesowi zarządu spółki.

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

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. Obowiązujące przepisy wzmacniają kompetencje kontrolerów UODO.

W okresie od 1 stycznia do 31 grudnia 2020 r. Prezes Urzędu Ochrony Danych Osobowych przeprowadzał czynności kontrolne w zakresie przestrzegania przepisów prawnych dotyczących ochrony danych osobowych **w dwunastu podmiotach.** Wymienione działania były realizowane na podstawie art. 58 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 rozporządzenia o ochronie danych)[137]. Kontrole były przeprowadzane zarówno na podstawie planu kontroli, jak i w rezultacie powzięcia przez Prezesa UODO informacji o występujących nieprawidłowościach.

Zgodnie z treścią planu kontroli sektorowych UODO na 2020 r., szczególny nacisk położono na badanie stanu przestrzegania przepisów w bankach oraz podmiotach korzystających z systemu zdalnego odczytu wodomierzy.

Ze względu na sytuację epidemiczną, która wystąpiła na początku 2020 r. oraz związane z nią przepisy ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[138], działania Prezesa UODO o charakterze kontrolnym musiały uwzględniać wyżej wskazane okoliczności. Zaistniała sytuacja determinowała zatem liczbę i sposób prowadzenia kontroli.

W 2020 r. UODO przeprowadził **12 kontroli** przestrzegania przepisów dotyczących ochrony danych osobowych między innymi u takich podmiotów, jak: Główny Geodeta Kraju, usługodawcy telekomunikacyjni, spółdzielnie mieszkaniowe, banki oraz zespół szkół ogólnokształcących.

5.1. Organy administracji publicznej

Prezes UODO, na skutek informacji uzyskanych m.in. z doniesień medialnych dotyczących kwestii publikowania na portalu internetowym danych osobowych (w tym numerów ksiąg wieczystych) pochodzących z ewidencji gruntów i budynków (EGiB) prowadzonych przez starostwa

[137] Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.
[138] Dz. U. z 2020 r. poz. 1842 z późn. zm.

powiatowe, przeprowadził kontrolę[139] w jednym z nich. W toku kontroli ustalono, że starosta nie publikuje na ww. portalu danych osobowych z ewidencji gruntów i budynków, lecz na podstawie zawartego porozumienia dane z przedmiotowej ewidencji przekazuje Głównemu Geodecie Kraju, który następnie dokonuje publikacji pozyskanych danych na wskazanym portalu.

Z uwagi na powyższe ustalenia Prezes UODO zdecydował o konieczności przeprowadzenia kontroli[140] u Głównego Geodety Kraju (GGK), której celem miało być zbadanie procesu udostępniania przez niego za pośrednictwem portalu internetowego danych osobowych z ewidencji gruntów i budynków. W pierwszym dniu zaplanowanej kontroli, GGK, po zapoznaniu się z wydanymi przez Prezesa UODO upoważnieniami imiennymi wskazującymi zakres kontroli, odmówił składania zeznań dotyczących procesu publikowania przedmiotowych informacji na portalu internetowym, jak również uniemożliwił kontrolującym dokonanie oględzin systemów informatycznych stosowanych w tym procesie. W toku kontroli pozyskana została jedynie dokumentacja określająca środki organizacyjne zastosowane przez GGK w celu zapewnienia bezpieczeństwa danych oraz dowody potwierdzające fakt wyznaczenia inspektora ochrony danych.

Zarówno okoliczności odmowy przeprowadzenia kontroli w pełnym zaplanowanym zakresie oraz pozostałe ustalenia zostały zawarte w sporządzonym przez kontrolujących protokole kontroli, który został podpisany bez wnoszenia zastrzeżeń przez GGK.

Powstałe okoliczności spowodowały, że Prezes UODO decyzją z 2 lipca 2020 r.[141] nałożył na GGK administracyjną karę pieniężną w związku z naruszeniem art. 31 oraz art. 58 ust. 1 lit. e i lit. f rozporządzenia 2016/679, polegającym na niezapewnieniu Prezesowi Urzędu Ochrony Danych Osobowych, w trakcie kontroli dostępu do pomieszczeń, sprzętu i środków służących do przetwarzania danych osobowych oraz dostępu do danych osobowych i informacji niezbędnych Prezesowi UODO do realizacji jego zadań, a także na braku współpracy z Prezesem UODO w trakcie tej kontroli. GGK, uzasadniając swoje stanowisko w sprawie odmowy zbadania przez Prezesa UODO procesu publikowania danych na portalu internetowym, złożył wyjaśnienia oraz przedłożył dowody, które w pełni potwierdziły ustalenia dokonane w toku przeprowadzonej kontroli.

Po zapoznaniu się z całością materiału dowodowego zgromadzonego w sprawie, Prezes UODO, stwierdzając naruszenie przez GGK zasady zgodności z prawem przetwarzania danych osobowych (art. 5 ust. 1 lit. a rozporządzenia 2016/679) oraz udostępnianie na portalu internetowym

[139] sygn. akt: DKN.5112.8.2020.
[140] sygn. akt: DKN.5112.13.2020.
[141] sygn. akt: DKE.561.3.2020.RZ.81624.

bez podstawy prawnej danych osobowych w zakresie numerów ksiąg wieczystych, pozyskanych z ewidencji gruntów i budynków prowadzonej przez starostów (art. 6 ust. 1 rozporządzenia 2016/679), decyzją z 24 sierpnia 2020 r.[142], nakazał GGK dostosowanie operacji przetwarzania danych osobowych do przepisów rozporządzenia 2016/679, poprzez zaprzestanie udostępniania na portalu internetowym danych osobowych w zakresie numerów ksiąg wieczystych, pozyskanych z ewidencji gruntów i budynków prowadzonych przez starostów. Jednocześnie za naruszenie przepisów art. 5 ust. 1 lit. a oraz art. 6 ust. 1 rozporządzenia 2016/679, nałożył na GGK administracyjną karę pieniężną w kwocie 100 000 zł. Na wydane przez Prezesa UODO decyzje GGK złożył skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie, wnosząc jednocześnie o wstrzymanie wykonania decyzji nakazującej zaprzestanie udostępniania danych. Wojewódzki Sąd Administracyjny w Warszawie postanowieniem z 16 grudnia 2020 r.[143] odmówił wstrzymania zaskarżonej decyzji.

5.2. Operator telekomunikacyjny

W związku ze zgłoszonym przez operatora telekomunikacyjnego naruszeniem ochrony danych osobowych, polegającym na uzyskaniu przez nieuprawnioną osobę dostępu do dużej ilości danych abonentów usług przedpłaconych, obejmujących m.in. imię i nazwisko, numer PESEL, serię i numer dowodu tożsamości, Prezes UODO przeprowadził kontrolę[144] zgodności przetwarzania danych osobowych z przepisami rozporządzenia 2016/679 oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Kontrola wykazała, że w procesie przetwarzania danych abonentów usług przedpłaconych, operator telekomunikacyjny, jako administrator, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na naruszeniu zasady poufności danych wyrażonej w art. 5 ust. 1 lit. f rozporządzenia 2016/679 oraz obowiązków, które stanowią odzwierciedlenie tej zasady, określonych w art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b i lit. d oraz art. 32 ust. 2 rozporządzenia 2016/679, poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych służących do rejestracji danych osobowych abonentów usług przedpłaconych.

Z uwagi na stwierdzone uchybienia Prezes UODO wszczął z urzędu postępowanie administracyjne zakończone wydaniem decyzji, w której stwierdził, że u operatora

[142] sygn. akt: DKN.5112.13.2020.88521.
[143] sygn. akt: II SA.Wa 2222/20.
[144] sygn. akt: DKN.5112.1.2020.

telekomunikacyjnego nie były dokonywane regularne testy pomiarów i oceny skuteczności stosowanych przez nią środków technicznych oraz organizacyjnych, mające zapewnić bezpieczeństwo przetwarzanych danych osobowych. Podejmowane przez operatora telekomunikacyjnego przeglądy zastosowanych środków bezpieczeństwa w sytuacji wystąpienia zmiany organizacyjnej lub prawnej, jak również podejmowane działania dopiero w przypadku podejrzenia zaistnienia podatności, nie mogły zostać uznane za regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych. Prezes UODO w uzasadnieniu decyzji podkreślił, że wskazane testowanie, mierzenie i ocenianie, aby stanowiło realizację wymogu wynikającego z art. 32 ust. 1 lit. d rozporządzenia 2016/679, musi być dokonywane w sposób regularny, co oznacza świadome zaplanowanie i zorganizowanie, a także dokumentowanie (w związku z zasadą rozliczalności) tych działań w określonych przedziałach czasowych, niezależnie od zmian w organizacji i przebiegu procesów przetwarzania danych spowodowanych np. zmianą organizacyjną u administratora danych. Administrator zobowiązany jest do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania. Kompleksowość tej weryfikacji powinna być oceniana przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania. Kontrola wykazała, że operator telekomunikacyjny nie przeprowadził testów weryfikujących stosowanych przez niego zabezpieczeń, dotyczących przekazywania danych pomiędzy aplikacjami, które służą do rejestracji usług przedpłaconych. Takie działania zostały podjęte dopiero po wystąpieniu zgłoszonego przez operatora telekomunikacyjnego naruszenia ochrony danych osobowych. Istniejąca od czasu stworzenia aplikacji luka w systemach informatycznych została wykorzystana przez osobę nieuprawnioną.

W wydanej decyzji Prezes UODO stwierdził, że zaistniały przesłanki do nałożenia administracyjnej kary pieniężnej w wysokości 1 968 524,00 zł, uznając, że naruszenie ma znaczną wagę i poważny charakter, ze względu na istnienie wysokiego ryzyka negatywnych skutków prawnych dla dużej liczby osób, np. wykorzystania danych osobowych w celu zaciągnięcia zobowiązań w imieniu osób, których dane trafiły w niepowołane ręce. Prezes UODO uznał, że wdrożenie i korzystanie z systemu służącego do przetwarzania danych, który nie zapewnia poprawnie działającej walidacji parametrów, było rażącym naruszeniem operatora telekomunikacyjnego jako administratora, a z uwagi na luki systemu informatycznego, ryzyko wycieku danych istniało od dawna.

5.3. Zespół Szkół Ogólnokształcących

W przypadku Zespołu Szkół Ogólnokształcących (ZSO) zakresem kontroli objęto przetwarzanie danych osobowych uczniów w związku z przeprowadzeniem wśród nich badań (wywiadów) ankietowych, dotyczących ich sytuacji osobistej. Przedmiotem ustaleń w toku kontroli były w szczególności następujące kwestie:

1) czy w ZSO były przeprowadzane badania ankietowe wśród uczniów, a jeżeli tak, to czy w zastosowanych ankietach lub w związku z nimi były przetwarzane dane osobowe uczniów i jakich kategorii były to dane, a także na jakiej podstawie prawnej i w jakim zakresie odbywało się ich przetwarzanie;
2) sposób oraz cel przetwarzania danych osobowych uczniów w związku z przeprowadzeniem badań ankietowych;
3) sposób dopełnienia przez ZSO obowiązków administratora danych wynikających z art. 12, art. 13 ust. 1 i ust. 2 oraz art. 14 ust. 1, ust. 2 i ust. 3 oraz art. 58 rozporządzenia 2016/679;
4) sposób realizacji praw osób, których dane dotyczą, wynikających z art. 15-22 rozporządzenia 2016/679;
5) czy przetwarzanie danych osobowych uczniów biorących udział w badaniach ankietowych odbywało się na podstawie upoważnienia nadanego przez administratora danych osobowych lub podmiot przetwarzający;
6) czy ZSO wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych objętych ochroną w związku z przeprowadzeniem badań ankietowych wśród uczniów;
7) czy ZSO wyznaczył inspektora ochrony danych;
8) czy ZSO prowadzi rejestr czynności przetwarzania danych osobowych lub rejestr kategorii czynności przetwarzania w sposób uwzględniający przeprowadzanie badań ankietowych wśród uczniów.

W toku kontroli ustalono, że przeprowadzone wśród uczniów badanie odbywało się z wykorzystaniem formularza ankietowego, w którym pozyskiwano dane osobowe uczniów ZSO, w tym także osób niepełnoletnich, w zakresie: imion i nazwisk, oznaczeń klas, określenia opiekunów prawnych (rodziców), informacji o stanie rodziny, a także informacji o śmierci opiekuna prawnego (rodzica), separacji opiekunów prawnych (rodziców), ich wykształcenia i sytuacji zawodowej, liczby osób w gospodarstwie domowym, sytuacji finansowej, itp. Przetwarzanie danych uczniów odbywało się w zakresie ich zbierania, przechowywania oraz usunięcia. W toku kontroli ustalono również, że

ankietę przeprowadzono w celu zidentyfikowania uczniów, którzy wymagają udzielenia wsparcia psychologicznego przez szkołę, do której uczęszczają.

Podczas kontroli stwierdzono, że ZSO, przeprowadzając ankietę wśród uczniów, naruszył zasadę przetwarzania danych zgodnie z prawem, wyrażoną w art. 5 ust. 1 lit. a rozporządzenia 2016/679, w myśl którego dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

ZSO, będąc jednostką budżetową, a więc także jednostką sektora finansów tożsamą z podmiotem publicznym w rozumieniu przepisów rozporządzenia 2016/679, może przetwarzać dane osobowe w zakresie wykonywanych przez niego zadań nałożonych ustawami wyłącznie w zgodzie z art. 5 ust. 1 lit. a oraz art. 6 ust. 1 lit. c rozporządzenia 2016/679. Z kolei w myśl art. 30a ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe[145] szkoły przetwarzają dane osobowe, w zakresie niezbędnym dla realizacji zadań i obowiązków wynikających z tych przepisów.

Przepisy ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe oraz pozostałe akty prawne regulujące zasady funkcjonowania instytucji oświatowych, nie określają zadań i obowiązków szkół, które uzasadniałyby przetwarzanie danych osobowych uczniów w sposób, w jaki uczyniono to w ZSO w związku z przeprowadzeniem ankiety. Przeprowadzenie ankiety, które pociągnęło za sobą przetwarzanie danych uczniów przez ZSO nie stanowiło wykonania ciążącego na tej placówce oświatowej obowiązku lub zadania wynikającego z ustawy i dlatego Prezes UODO uznał, iż doszło do naruszenia art. 6 ust. 1 lit. c rozporządzenia 2016/679.

Prezes UODO wszczął z urzędu postępowanie administracyjne w zakresie stwierdzonych uchybień, w celu wyjaśnienia okoliczności sprawy i na podstawie art. 58 ust. 2 lit. b rozporządzenia 2016/679 decyzją administracyjną udzielił ZSO upomnienia w zakresie stwierdzonego naruszenia przepisu art. 6 ust. 1 lit. c w związku z art. 5 ust. 1 lit. a rozporządzenia 2016/679.

Prezes UODO uznał, że udzielenie ZSO upomnienia będzie wystarczającym środkiem, ponieważ nie otrzymał wcześniej innych sygnałów, aby ze strony ZSO miały miejsce podobne działania skutkujące naruszeniami. Ponadto stwierdzone naruszenie przepisów o ochronie danych osobowych było jednorazowym incydentem, nie zaś systematycznym działaniem lub zaniechaniem, które stanowiłoby poważne zagrożenie dla praw osób, których dane osobowe są przetwarzane przez ZSO. Prezes UODO uznał za okoliczność łagodzącą fakt, że naruszenie przepisów przez ZSO miało charakter niezamierzony, a przed kontrolą ZSO niezwłocznie podjął szereg działań naprawczych

[145] Dz. U. z 2019 r. poz. 1148 z późn. zm.

takich, jak: zniszczenie formularzy ankiety lub jej nieprzeprowadzenie przez niektórych nauczycieli, zorganizowanie szkolenia pracowników ZSO w celu podniesienia ich świadomości z zakresu ochrony danych osobowych, a także dokonanie analizy zdarzenia, jakim było przeprowadzenie ankiety wśród uczniów, ze względu na wystąpienie ryzyka naruszenia praw i wolności osób fizycznych. Ponadto Prezes UODO nie stwierdził, aby osoby, których dane dotyczą, poniosły szkody na skutek działań tej placówki oświatowej.

5.4. Zdalna obsługa wodomierzy

Zgodnie z opracowanym planem kontroli sektorowych na rok 2020, upoważnieni przez Prezesa UODO pracownicy przeprowadzili kontrole w zakresie przetwarzania danych osobowych w związku ze stosowaniem i obsługą systemu zdalnego odczytu stanu wodomierzy[146] przez dwie spółdzielnie mieszkaniowe i operatora zajmującego się obsługą infrastruktury takiego systemu. Kontrole miały na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami rozporządzenia 2016/679 oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[147].

W okresie sprawozdawczym wiele działań kontrolnych koncentrowało się na badaniu sposobów, w jaki administratorzy danych osobowych zapewniali zachowanie poufności danych oraz czy dane osobowe nie były wykorzystywane w innych celach niż te, dla których zostały zebrane. Zakres przeprowadzonych kontroli obejmował ustalenie m.in. podstawy prawnej przetwarzania danych osobowych, źródła pozyskania danych osobowych, zakresu, celu i rodzaju przetwarzanych danych osobowych, sposobu dopełnienia obowiązków administratora danych wynikających z art. 13 i art. 14 rozporządzenia 2016/679, sposobu zapewnienia realizacji praw osób, których dane dotyczą, określonych w ogólnym rozporządzeniu o ochronie danych, a także sposobu i celu zbierania oraz udostępniania danych osobowych.

Ponadto upoważnieni kontrolerzy w ramach prowadzonych czynności sprawdzali, czy zostały wdrożone odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem 2016/679 oraz z uwzględnieniem charakteru, zakresu, kontekstu, celów przetwarzania i ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te były w razie potrzeby poddawane przeglądom i uaktualniane[148].

[146] Kontrole w tym zakresie przeprowadzane były także w wybranych podmiotach w 2019 roku.
[147] Dz. U. z 2019 r. poz. 1781.
[148] Art. 32 i art. 24 rozporządzenia 2016/679.

Sprawdzono również, czy zostały wdrożone polityki ochrony danych, o których mowa w art. 24 ust. 2 rozporządzenia 2016/679, czy wyznaczony został inspektor ochrony danych (art. 37 rozporządzenia 2016/679), czy administrator powierza przetwarzanie danych podmiotom przetwarzającym, a jeżeli tak, to czy powierzenie to nastąpiło przy spełnieniu warunków określonych w art. 28 rozporządzenia 2016/679. Kontroli poddano również kwestie podjęcia działań w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora, która ma dostęp do danych osobowych, przetwarzała je na polecenie administratora zgodnie z art. 29 i art. 32 ust. 4 rozporządzenia 2016/679.

Kontrolerzy UODO zbadali ponadto, czy została przeprowadzona ocena skutków dla ochrony danych, w związku z wprowadzeniem systemu zdalnego odczytu wodomierzy (art. 35 rozporządzenia 2016/679), czy dokumentowane były wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (art. 33 ust. 5 rozporządzenia 2016/679), a także czy prowadzony był rejestr czynności przetwarzania danych osobowych, w którym zamieszczono wszystkie informacje określone w art. 30 ust. 1 rozporządzenia 2016/679. Zakresem kontroli objęte były również systemy informatyczne wykorzystywane do przetwarzania danych osobowych, w tym w związku ze stosowaniem systemu zdalnego odczytu stanu wodomierzy oraz ustalenie, w jakim zakresie, jakie dane pozyskiwano, gdzie je przekazywano i jak długo były archiwizowane.

Na skutek przeprowadzonych kontroli wszczęte zostały postępowania administracyjne wobec dwóch administratorów, w wyniku których stwierdzone w czasie kontroli naruszenia zostały usunięte przez jednostki kontrolowane i w związku z tym wydane zostały decyzje umarzające postępowanie.

Nieprawidłowości stwierdzone w toku prowadzonych przez Prezesa UODO kontroli dotyczyły ogólnego sformułowania w umowach powierzenia przetwarzania, dotyczącego zakresu oraz rodzaju danych, które przekazywane były podmiotowi przetwarzającemu. Opis powierzenia nie zawierał postanowień pozwalających jednoznacznie interpretować jego zakres, a tym samym nie spełniał wymagań wymienionej w art. 5 ust. 1 lit. a rozporządzenia 2016/679 zasady przejrzystości, a także wskazanej w art. 5 ust. 2 ww. rozporządzenia zasady rozliczalności, w związku z nieodpowiednim udokumentowaniem przez administratora czynności powierzenia danych osobowych. Mając na uwadze powyższe okoliczności, Prezes UODO uznał, iż administratorzy naruszyli przepisy art. 28 ust. 3 oraz art. 5 ust. 1 lit. a w związku z art. 5 ust. 2 rozporządzenia 2016/679[149].

[149] sygn. akt: DKN.5112.2.2020, DKN.5112.9.2020.

Obowiązujące przepisy prawa nie regulują kwestii częstotliwości zdalnych odczytów stanu wodomierzy. Wdrożenie systemu zdalnych odczytów umożliwia dokonywanie odczytów bez konieczności bezpośredniego wejścia do lokalu mieszkalnego. Należy zauważyć, że bardzo często zdalne odczyty wskazań wodomierzy skutkują możliwością przetwarzania większej ilości informacji. Zbieranie i przechowywanie danych pozyskanych w ten sposób może oznaczać, że będą one przetwarzane w szerszym zakresie, niż gdyby odczyty odbywały się w sposób tradycyjny, i mogą posłużyć do tworzenia baz danych wykorzystywanych do profilowania osób. Przetwarzanie danych osobowych w ramach zdalnego odczytu stanu wodomierzy przy wykorzystaniu rozwiązań z zakresu nowych technologii, wymaga od administratora podjęcia szeregu działań już na etapie planowania i wdrożenia takiego systemu. Przeprowadzone kontrole nie wykazały, aby wobec przetwarzania danych opartego na zdalnym odczycie wodomierzy dochodziło do profilowania danych, o którym mowa w art. 4 pkt 4 rozporządzenia 2016/679.

Zakres przetwarzanych danych może różnić się w zależności od przyjętego sposobu odczytu. Dane osobowe, przetwarzane w związku ze stosowaniem systemu zdalnego odczytu stanu wodomierzy, były przekazywane podmiotom zewnętrznym, takim jak operatorzy dokonujący odczytu. W tym przypadku administrator danych musi zapewnić, aby przekazywanie danych takim podmiotom odbywało się w sposób bezpieczny, tj. powinny być zastosowane metody szyfrowania przesyłanych danych, a ponadto dane osobowe nie mogą być przesyłane w nadmiarowym zakresie.

Odnośnie kwestii zabezpieczeń zdalnego systemu odczytu stanu wodomierzy, rozporządzenie 2016/679 nie określa minimalnych wymagań w tym zakresie. Obowiązkiem administratora jest zapewnienie bezpieczeństwa przetwarzania danych osobowych m.in. poprzez wdrożenie szeregu działań, o których mowa w art. 32 ogólnego rozporządzenia o ochronie danych. Na etapie projektowania systemu do zdalnego odczytu stanu wodomierzy należy zwrócić uwagę na właściwy dobór urządzeń służących do tego celu. Wskazanym jest, aby administratorzy danych osobowych regularnie testowali stosowane rozwiązania, co jest bardzo ważne z uwagi na nieustanny rozwój nowoczesnych technologii i związane z tym zagrożenia. Pełna inwentaryzacja posiadanych urządzeń i programów, a także ich konfiguracji umożliwia administratorowi danych osobowych dobór odpowiednich zabezpieczeń danych przetwarzanych w systemach teleinformatycznych.

5.5. Kontrole sektorowe w bankach

W obszarze sektora bankowego Prezes UODO przeprowadził 5 kontroli. W związku z analizą materiału dowodowego, zebranego w toku kontroli przeprowadzonych w bankach, w zakresie

przetwarzania zawartych w kopiach dokumentów tożsamości danych osobowych klientów oraz potencjalnych klientów, ustalono, że banki różnie interpretują przepisy i zalecenia regulatorów. Przyczynkiem do poszerzonej dyskusji na temat kopiowania dokumentów tożsamości stała się ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[150], którą zostały znowelizowane wcześniej obowiązujące przepisy w tym obszarze. Zgodnie z art. 33 ust.1 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, instytucje obowiązane stosują wobec swoich klientów środki bezpieczeństwa finansowego. Środki te obejmują m.in. identyfikację klienta oraz weryfikację jego tożsamości[151]. W myśl art. 37 tej ustawy weryfikacja tożsamości klienta, osoby upoważnionej do działania w jego imieniu oraz beneficjenta rzeczywistego polega na potwierdzeniu ustalonych danych identyfikacyjnych na podstawie dokumentu stwierdzającego tożsamość osoby fizycznej, dokumentu zawierającego aktualne dane z wyciągu z właściwego rejestru lub innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła. Zgodnie zaś z art. 34 ust. 4 cytowanej ustawy, instytucje obowiązane 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.

Jeden z kontrolowanych banków wskazał znowelizowane przepisy ww. ustawy jako podstawę prawną zmiany dotychczasowej praktyki w zakresie kopiowania dokumentów tożsamości (wcześniej dokumenty te nie były kopiowane). Bank ten zaczął pozyskiwać kopie dokumentów tożsamości obecnych, nowych i potencjalnych klientów, np. wtedy, gdy zaszła konieczność aktualizacji danych zawartych w dokumencie tożsamości, w szczególności danych zawartych w dowodzie osobistym. Jako podstawę prawną zbierania danych zawartych w dokumentach tożsamości wskazano przepisy art. 34 ust. 4, art. 37 oraz art. 49 ust. 1 pkt 1 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Na potrzeby stosowanych w tym banku procedur, został zdefiniowany „dokument tożsamości" szerzej niż to wynika z przepisów (dowód osobisty, paszport). Stąd też za dokument tożsamości bank uznawał np. legitymację szkolną, legitymację studencką, skrócony akt urodzenia, kartę pobytu, prawo jazdy. Klient (osoba posiadająca produkt bankowy) miał możliwość odmowy wykonania skanu dokumentu, ale wtedy proszony był o podpisanie stosownego oświadczenia. Jednak przy nawiązywaniu relacji z bankiem brak zgody na zeskanowanie dokumentu

[150] Dz. U. z 2019 r. poz. 1115.
[151] Art. 34 ust. 1 pkt 1 ustawy.

tożsamości powodował odmowę świadczenia przez bank wybranej przez klienta usługi.

W kolejnym banku również ustalono, że w ramach czynności bankowych zbierane były dane w postaci kopii dokumentów tożsamości. Bank powołał jako podstawę prawną powyższych działań art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. a rozporządzenia 2016/679, art. 34 ust. 4, art. 35, art. 37 oraz art. 43 ust. 4 pkt 2 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu i art. 112b ustawy z 29 sierpnia 1997 r. Prawo bankowe. Zgodnie z obowiązującymi w tym banku procedurami, bank na potrzeby stosowania środków bezpieczeństwa finansowego może przetwarzać informacje zawarte w dokumentach tożsamości klienta i osób upoważnionych do działania w jego imieniu oraz sporządzać ich kopie, a w razie braku zgody na sporządzanie kopii, pozyskiwać oświadczenie zgodnie z regulacjami wewnętrznymi banku. Powyższa regulacja znajduje odzwierciedlenie w procedurach, regulaminach, instrukcjach i podręcznikach dotyczących poszczególnych produktów bankowych.

W innym z kontrolowanych banków, przy podpisywaniu umowy z klientem, nie było zalecenia sporządzania kserokopii dokumentów tożsamości. Pracownik banku pozyskiwał dokument tożsamości do wglądu i spisywał dane oraz potwierdzał to na przeznaczonym do tego celu formularzu. Kserokopia dokumentów pozyskiwana była jedynie w przypadkach podejrzenia prania pieniędzy, kiedy z informacji pochodzących z baz danych, z których korzystał bank wynikało, że mogą pojawić się wątpliwości, co do danego dokumentu tożsamości przedstawionego przez klienta. Pracownicy banku otrzymali wytyczne w zakresie kopiowania dokumentów tożsamości. Kopie dokumentów tożsamości pozyskiwane były w określonych przypadkach przewidzianych w procedurach bankowych, np. od klienta, którego dane bank już posiadał, ale występowała rozbieżność pomiędzy tymi danymi a danymi zawartymi we wniosku klienta. W przypadku takiej rozbieżności klient przekazywał skan dokumentu tożsamości, który był weryfikowany i usuwany z systemu banku po dokonaniu weryfikacji.

Banki pozyskiwały kserokopie dokumentów tożsamości klientów także w związku z oferowaniem usług obarczonych większym ryzykiem w zakresie identyfikacji klientów, związanym ze zdalnym zawieraniem umów.

Dokonane ustalenia wskazały na niejednolite podejście banków do kopiowania dokumentów tożsamości przy zawieraniu umów, jednak z uwagi na przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu, procedury wewnętrzne banków zawsze przewidywały możliwość wspomnianego kopiowania. Wobec trzech banków zostały wszczęte postępowania administracyjne

w zakresie niedopuszczalności przetwarzania danych osobowych, pozyskanych w wyniku sporządzenia kopii dokumentów tożsamości, w celach innych, niż wynikających z art. 35 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[152].

5.6. Uczelnia wyższa

Prezes UODO 21 sierpnia 2020 r. wydał wobec Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie (SGGW) decyzję, w której, stwierdzając naruszenie przepisów rozporządzenia 2016/679[153], nałożył na tę uczelnię karę pieniężną w wysokości 50 000 zł. Stało się tak po przeprowadzeniu postępowania administracyjnego na skutek naruszeń przepisów o ochronie danych osobowych, stwierdzonych w toku kontroli przeprowadzonej w grudniu 2019 r.

W Szkole Głównej Gospodarstwa Wiejskiego w Warszawie, w związku ze zgłoszonym naruszeniem ochrony danych, przeprowadzone zostały czynności kontrolne. Zakresem kontroli objęto przetwarzanie przez SGGW danych osobowych kandydatów na studia, których dotyczy naruszenie ochrony danych osobowych zgłoszone Prezesowi UODO[154].

Naruszenie ochrony danych osobowych kandydatów na studia w SGGW związane było z kradzieżą przenośnego prywatnego komputera pracownika uczelni, pełniącego funkcję sekretarza Uczelnianej Komisji Rekrutacyjnej SGGW. Skradziony laptop był używany przez ww. pracownika zarówno do celów prywatnych, jak i służbowych. Z systemu informatycznego, służącego do przetwarzania danych osobowych kandydatów na studia, za pomocą zaimplementowanej w nim funkcjonalności, importowane były na prywatny komputer zestawy danych osobowych obejmujących m.in. imię, nazwisko, nazwisko rodowe, imiona rodziców, numer identyfikacyjny PESEL, płeć, narodowość, obywatelstwo, adres zamieszkania, serię i numer dowodu osobistego bądź innego dokumentu tożsamości, w tym paszportu, numer telefonu komórkowego i/lub stacjonarnego, informacje o dotychczasowym wykształceniu, informacje o kwalifikacji na studia. Uczelnia, będąca administratorem tych danych osobowych, nie posiadała informacji o tym fakcie, zaś operacje te nie były rejestrowane w systemie tej szkoły. Pobrane zestawy danych służyły dokonaniu kwalifikacji w ramach rekrutacji oraz do celów statystycznych.

W ocenie Prezesa UODO uczelnia w sposób niezadowalający dokonywała oceny skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych

[152] Dz. U. z 2020 r. poz. 971 z późn. zm.
[153] art. 5 ust. 1 lit. e, art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1, art. 32 ust. 1 lit. b, art. 32 ust. 1 lit. d, art. 32 ust. 2, art. 38 ust. 1, art. 39 ust. 1 lit. b i art. 39 ust. 2.
[154] sygn. akt: ZWAD.405.5471.2019.

osobowych kandydatów na studia, w tym nie uwzględniała w wystarczającym stopniu zasady rozliczalności, korzystając z systemu informatycznego służącego do przetwarzania danych osobowych kandydatów na studia. Zgromadzony w sprawie materiał dowodowy dał podstawę do stwierdzenia, że inspektor ochrony danych wypełniał swoje zadania bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania danych. Uczelnia nie zgodziła się z przedmiotową decyzją i zaskarżyła ją do Wojewódzkiego Sądu Administracyjnego.

6. Czynności sprawdzające

Niezależnie od przeprowadzonych kontroli, Prezes UODO w okresie sprawozdawczym wykonywał w stosunku do wybranych podmiotów czynności sprawdzające, mające na celu zdalną weryfikację stosowanych przez nie praktyk, w świetle obowiązujących przepisów prawa o ochronie danych osobowych. Czynności te były podejmowane w rezultacie otrzymanych przez Prezesa UODO informacji o potencjalnie zaistniałych nieprawidłowościach w procesie przetwarzania danych przez ww. podmioty. Czynności sprawdzające, o których wyżej mowa, były realizowane w formie pisemnych wystąpień, w których Prezes UODO zwracał się do weryfikowanych podmiotów o udzielenie wyjaśnień w przedmiocie dokonywanych operacji przetwarzania danych osobowych.

W okresie sprawozdawczym **Prezes UODO prowadził z urzędu 24 sprawy, między innymi na podstawie informacji przekazanych przez inne organy,** w tym Prezesa Urzędu Ochrony Konkurencji i Konsumentów oraz Głównego Inspektora Pracy. Do Prezesa UODO o poczynienie stosownych ustaleń zwracali się także posłowie oraz Prezes Naczelnej Rady Aptekarskiej.

Przedmiotem podjętych przez Prezesa UODO czynności było zbadanie kwestii dotyczących przetwarzania danych osobowych m.in. przez związek działkowców stosujący monitoring wizyjny na terenie ogródków działkowych, lekarza prowadzącego prywatną praktykę lekarską, przechowującego dokumentację medyczną bez należytego nadzoru, pracodawców przetwarzających dane o stanie zdrowia swoich pracowników, a także stosujących monitoring w miejscu pracy, podmioty udostępniające aplikacje internetowe, gminę, która na stronach Biuletynu Informacji Publicznej – BIP udostępniała oświadczenia majątkowe radnych przez okres dłuższy, niż to jest dopuszczalne.

Na podstawie wniosku Prezesa Naczelnej Rady Aptekarskiej zwrócono się o wyjaśnienia do spółki wykorzystującej – w ramach aplikacji webowej znajdującej się na stronie internetowej – dane osobowe, w celu wyszukiwania produktów medycznych przepisywanych pacjentom na e-receptach, do czego konieczne było podanie danych pacjenta, któremu przepisano leki na receptę. W związku

zaś z sygnałem otrzymanym od niemieckiego organu nadzorczego (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) oraz doniesieniami medialnymi, Prezes Urzędu Ochrony Danych Osobowych podjął czynności zmierzające do ustalenia szczegółów funkcjonowania platformy internetowej, której działalność budziła zastrzeżenia ze względu na przetwarzanie wizerunku osób, których zdjęcia były wyszukiwane w sieci Internet i gromadzone celem ich powiązania ze zdjęciem wykorzystanym przez użytkownika platformy. Inny ze sprawdzanych portali stanowił witrynę, za pomocą której użytkownicy mogą dzielić się między sobą nieograniczoną liczbą wgrywanych dokumentów tekstowych tj. pdf, epub, mobi, txt, doc, xls, ppt itp. Portal ten jest darmową, technologicznie neutralną platformą hostingową. Sprawdzeniu przez organ nadzorczy zgodności przetwarzania danych osobowych z przepisami podlegało również pozyskiwanie danych osobowych w związku ze stosowaniem monitoringu wizyjnego w miejscu pracy bądź w innych okolicznościach (na terenie ogródków działkowych), a także żądanie przez pracodawcę danych o stanie zdrowia pracownika czy miejscu spędzania urlopu.

W ramach ustawowych kompetencji Prezes UODO skorzystał również z art. 11 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[155], występując w grudniu 2020 r. do inspektorów ochrony danych dziesięciu właściwych organów o dokonanie sprawdzenia zgodności z prawem przetwarzania danych osobowych w związku ze stosowaniem rozwiązań wykorzystujących technologię rozpoznawania twarzy, tj. do Policji, Straży Granicznej, Służby Ochrony Państwa. Ze względu na postępujący rozwój technologiczny zwiększyły się w znaczący sposób możliwości organów ścigania w zakresie przeciwdziałania i zwalczania przestępczości, które mogą wpływać na prawa i wolności obywatelskie. Szeroko komentowany jest ich wpływ na prawa i wolności obywatelskie oraz konieczność i proporcjonalność stosowania takich środków w demokratycznym państwie prawnym. W szczególności dotyczy to technik, które wiążą się z wykorzystywaniem szczególnych kategorii danych, jak np. dane biometryczne.

7. 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

[155] Dz. U. z 2018 r. poz. 125.

z zakresu ochrony danych osobowych. Dzięki temu Prezes UODO może prowadzić czynności mające na celu zapewnienie wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych. 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 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 procent jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Zadania związane z zapewnieniem wykonywania przez zobowiązanych obowiązków wynikających z decyzji administracyjnych Prezesa UODO, zarówno niepieniężnych (nakazy decyzji), jak i pieniężnych (nałożone kary) należały do Departamentu Kar i Egzekucji.

Egzekucji administracyjnej podlegają wszystkie decyzje administracyjne Prezesa Urzędu Ochrony Danych Osobowych:

a) nakładające na strony obowiązek (nakaz) do wykonania, które były ostateczne oraz te, którym nadano rygor natychmiastowej wykonalności. Jeżeli decyzja administracyjna zawiera postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlega egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek do wykonania nakładany na stronę (zobowiązanego) może polegać w szczególności na: usunięciu uchybień 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 zawiadomieniu osoby, której dane dotyczą o naruszeniu ochrony jej danych osobowych;

b) nakładające na strony administracyjne kary pieniężne, które stały się prawomocne lub gdy uprawomocniło się orzeczenie sądu administracyjnego po złożeniu skargi na decyzję z karą. Prezes Urzędu Ochrony Danych Osobowych ma prawo nałożyć na podmiot prywatny administracyjną karę pieniężną w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 procent jego całkowitego rocznego obrotu. Natomiast na jednostki sektora finansów publicznych (z wyjątkiem państwowych i samorządowych instytucji kultury), instytuty badawcze i Narodowy Bank Polski, Prezes Urzędu może nałożyć karę w wysokości do 100 000 zł. Wspomniane wyżej instytucje kultury mogą być ukarane karą sięgającą do 10 000 zł.

Działania egzekucyjne w liczbach

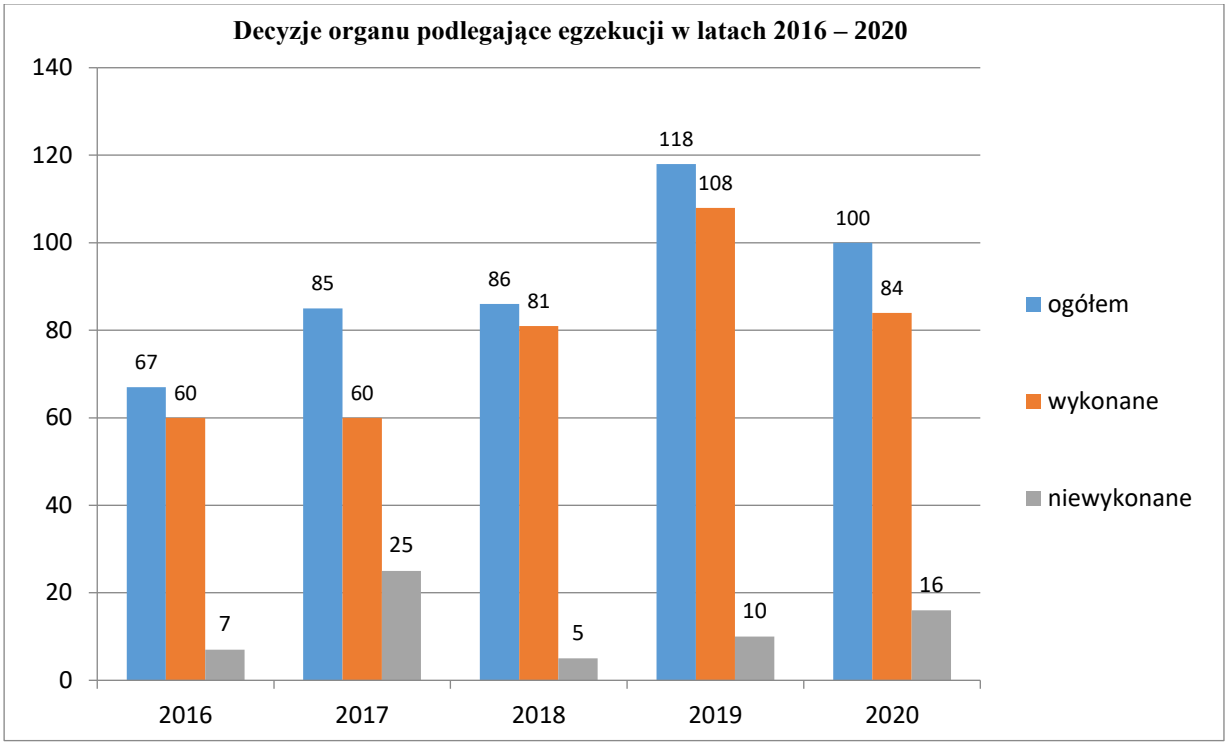
Prezes UODO prowadził w 2020 roku **działania egzekucyjne w stosunku do 100 decyzji administracyjnych**, z których **98** zawierało nałożony na strony nakaz do wykonania (obowiązek o charakterze niepieniężnym), zaś **2** nałożyły na strony administracyjne kary pieniężne. Wobec ww. dwóch podmiotów, zobowiązanych do zapłaty kary pieniężnej na podstawie przepisów o postępowaniu egzekucyjnym w administracji[156], wystawiono tytuły wykonawcze i przesłano je naczelnikom właściwych urzędów skarbowych, którzy pełnią rolę organów egzekucyjnych w tych sprawach, z wnioskiem o wszczęcie postępowania egzekucyjnego. Do 13 podmiotów, zobowiązanych do wykonania obowiązków o charakterze niepieniężnym, wysłano upomnienia wzywające do ich wykonania, przy czym w sprawach tych nie wystawiono tytułów wykonawczych z uwagi na wykonanie obowiązków przez zobowiązanych.

Liczba przekazywanych do egzekucji decyzji administracyjnych, z podziałem na lata w okresie lat 2016 – 2020, przedstawia się następująco:

- w **2016 r. – 67** decyzji,
- w **2017 r. – 85** decyzji, co stanowi wzrost o 27% w stosunku do roku poprzedzającego,
- w **2018 r. – 86** decyzji, co przełożyło się na niewielki, bo 1% wzrostu w stosunku do roku poprzedniego,
- w **2019 r. – 118** decyzji, co stanowi wzrost o 37% w stosunku do roku ubiegłego,

[156] Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, Dz. U. z 2020 r. poz. 1427 z późn. zm.

- w **2020 r. – 100** decyzji, co stanowi spadek o blisko 15% w stosunku do roku poprzedniego.



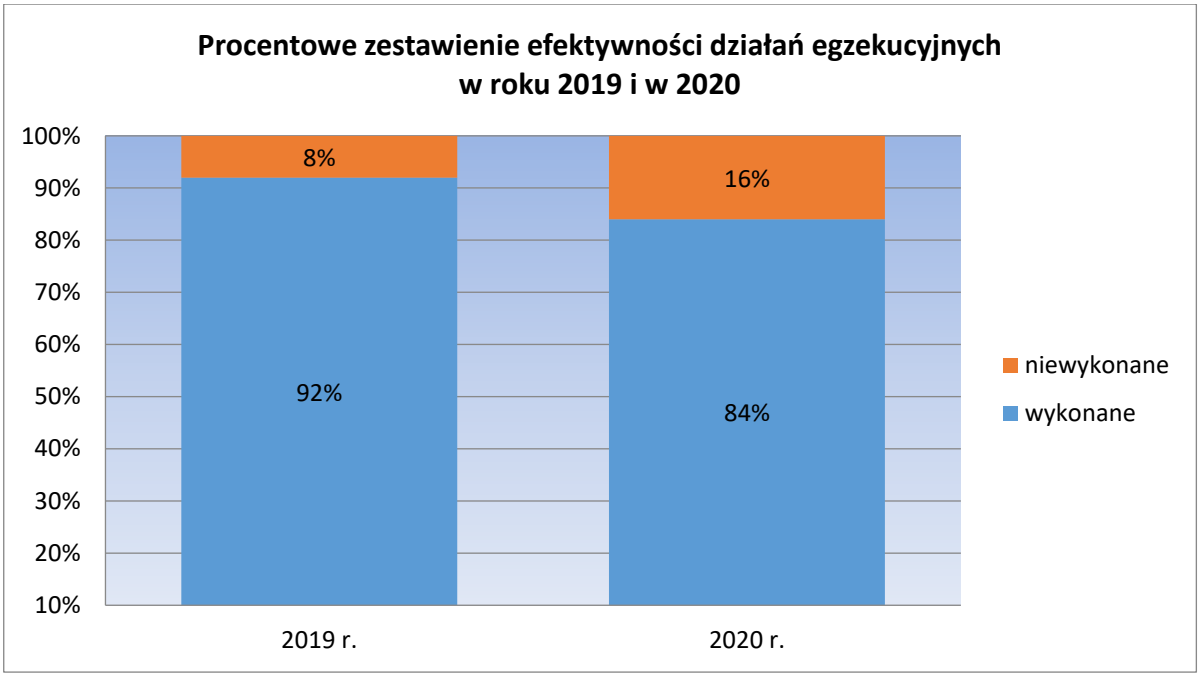
Wykres 3. **Zestawienie decyzji organu podlegających egzekucji administracyjnej i efektywność podejmowanych działań egzekucyjnych w latach 2016 – 2020.**

Efektywność prowadzonych działań egzekucyjnych mających na celu wykonanie przez zobowiązanych nałożonych na nich w decyzjach administracyjnych obowiązków w 2020 r. przedstawia się następująco: spośród wyżej wskazanych 100 decyzji **wykonanych zostało przez zobowiązanych 84 decyzji**, natomiast 16 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 Departamentowi Kar i Egzekucji UODO w 2020 roku wynosił **84%**.

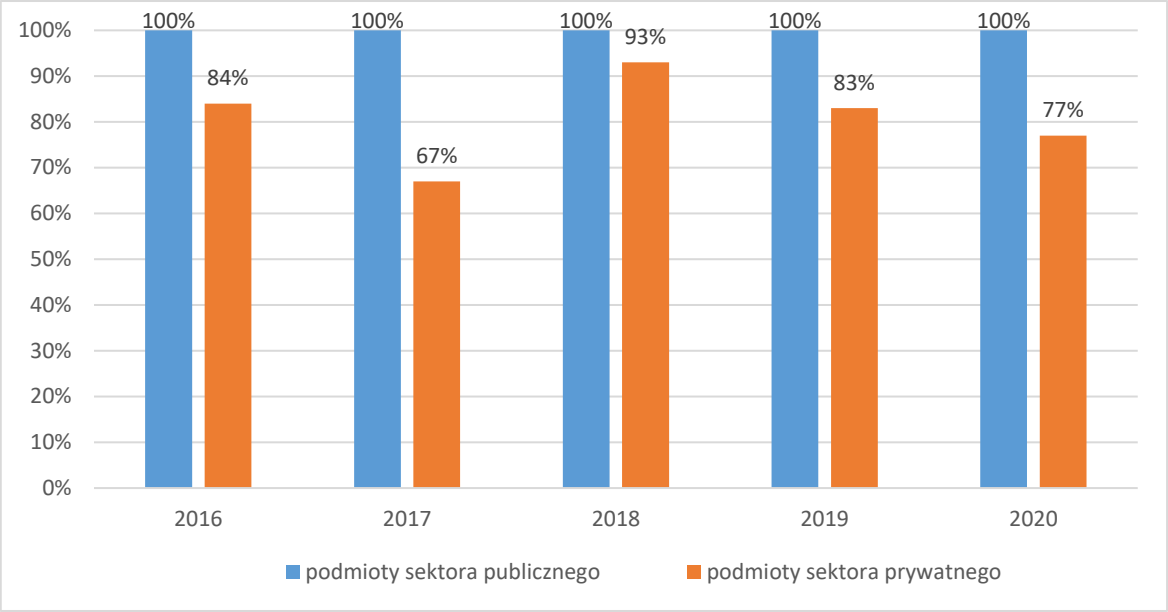
Porównując efektywność działań egzekucyjnych prowadzonych w 2020 r. do efektywności działań prowadzonych w roku 2019, która wynosiła 92%, można zauważyć, że mimo lekkiego spadku efektywności, w roku 2020 udało się zachować jej wysoki poziom (Wykres 3). Spadek efektywności

spowodowany jest w dużej mierze tym, że aż 7 spośród przekazanych do egzekucji decyzji wydanych zostało wobec tej samej spółki, która swą działalność na terenie RP postawiła w stan likwidacji i przeniosła ją poza Europejski Obszar Gospodarczy. Powyższe w znacznym stopniu komplikuje prowadzenie działań egzekucyjnych, w związku z czym nakazy tych decyzji wciąż pozostają niewykonane.



Wykres 4. **Zestawienie procentowej efektywności działań egzekucyjnych organu w 2019 i 2020 r.**

Działania egzekucyjne podejmowane przez Prezesa UODO w 2020 r. dotyczyły decyzji skierowanych w 66% przypadków do podmiotów z sektora prywatnego oraz w 34% przypadków do podmiotów z sektora publicznego. Natomiast 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, to w latach 2016 – 2020 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 2016 – 2020.**

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

Zgodnie z art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[157] *w związku z art. 57 ust. 1 lit. c RODO*[158]*, założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych – dotyczy to zarówno tych nowopowstających, jak i takich, które dotyczą tylko zmiany części przepisów prawa.*

Obowiązek ten jest realizowany przede wszystkim przez ministerstwa prowadzące konkretny proces legislacyjny, które przedkładają projekty aktów normatywnych do organu nadzorczego na etapie prac rządu nad projektem, zgodnie z § 38 ust. 1 pkt 3 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów[159].

[157] Art. 51. Założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu.
[158] Art. 57 ust. 1. lit. c: „Bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia każdy organ nadzorczy na swoim terytorium: (…) doradza, 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".
[159] § 38 ust. 1 pkt 3: Organ wnioskujący kieruje projekt dokumentu rządowego do zaopiniowania przez: (…) inne organy administracji rządowej lub inne organy i instytucje państwowe – jeżeli projekt dotyczy ich zakresu działania.

Jako przykład pozytywnego podejścia do tego obowiązku można wskazać **Ministerstwo Obrony Narodowej**, które w 2020 r. przekazało do zaopiniowania przez organ nadzorczy ponad 70 aktów prawnych, z których znaczna część została zaakceptowana bez uwag. Warto przy tym zaznaczyć, że mimo iż część działalności MON, dotycząca bezpieczeństwa narodowego oraz obrony (art. 23 ust. 1 lit. a i b RODO) nie podlega reżimowi RODO, ministerstwo to stale konsultowało opracowywane przez siebie akty normatywne z organem nadzorczym oraz uwzględniało jego uwagi, doskonaląc tym samym przepisy dotyczące przetwarzania informacji o osobach.

W analizowanym roku sprawozdawczym niektóre organy publiczne pomijały proces uzgodnień i opiniowania, i nie przekazywały do oceny organu nadzorczego istotnych projektów aktów normatywnych dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie. Praktyki takie naruszają przepisy RODO oraz ustawy o ochronie danych osobowych. W części przypadków projekty te były konsultowane dopiero przez Rządowe Centrum Legislacji oraz Kancelarię Sejmu, które przekazywały część tych projektów do Prezesa UODO, na właściwych dla tych podmiotów etapach prac legislacyjnych.

W 2020 r. Prezes UODO zaopiniował **747 projektów aktów prawnych**. Dla porównania w 2019 roku zaopiniowanych zostało **691** projektów aktów prawnych.

Przedmiotem szczególnego zainteresowania organu nadzorczego były takie zagadnienia, jak: ocena skutków dla ochrony danych, wywiązywanie się przez projektodawców z obowiązku przedkładania aktów prawnych do zaopiniowania, przetwarzanie danych na potrzeby realizacji prawa do informacji publicznej, akty prawne związane z epidemią COVID-19 oraz informatyzacja państwa. Poniżej przedstawiono wybrane przykłady niektórych z nich.

8.1. Ocena skutków dla ochrony danych

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**. Organ nadzorczy

wielokrotnie podkreślał, że w kontekście art. 35 ust. 10 RODO[160], uzasadnione i pożądane jest, aby dokonanie oceny skutków dla ochrony danych odbywało się już **w ramach oceny skutków regulacji projektowanej ustawy, w związku z przyjmowaniem podstawy prawnej dla danego przetwarzania danych osobowych**. Dokonanie oceny skutków dla ochrony danych na etapie projektu ustawy pozwala projektodawcy zminimalizować potencjalne zagrożenia związane z przetwarzaniem danych, zapobiec im poprzez stworzenie odpowiednich regulacji prawnych zapewniających stosowanie przepisów RODO, niektóre zaś z nich – o ile nie były niezbędne lub powodujące wysokie ryzyka – zupełnie wyeliminować.

W tym kontekście bardzo istotny jest komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[161]. Wspomniany dokument wskazywał – również w odniesieniu do projektów aktów normatywnych – jakie operacje przetwarzania danych obligatoryjnie wymagały przeprowadzenia oceny skutków dla ochrony danych. Należy jednak pamiętać, że nie jest to zamknięty katalog i o zasadności przeprowadzenia oceny skutków dla ochrony danych, już na etapie tworzenia przepisów prawa (tzw. OSR prywatności), decydują: kontekst danego aktu prawnego, cele przetwarzania danych, ich kategorie, prawa i obowiązki podmiotów związanych z danym aktem w zakresie przetwarzania danych osobowych. W ocenie organu nadzorczego, tworzenie rozwiązań prawnych dotyczących innowacyjnych technologii informatycznych, a także tych, które związane są z przetwarzaniem danych osobowych szczególnych kategorii (art. 9 i 10 RODO), zawsze powinno być poprzedzone oceną skutków dla ochrony danych. Dotyczy to zwłaszcza takich sytuacji i rozwiązań, jak np.: aplikacje mobilne, których administratorami danych są podmioty publiczne; nowe rozwiązania informatyczne z zakresu e-zdrowia; rozwój podpisu elektronicznego i cyfrowego obiegu dokumentów z wykorzystaniem numeru PESEL; wideo identyfikacja oraz obligatoryjny monitoring wizyjny czy profilowanie przeprowadzane przez podmioty publiczne.

W tym miejscu warto pozytywnie ocenić i wskazać na projekty procedowane przez **Ministerstwo Edukacji Narodowej (MEN)**, przy których przeprowadzono ocenę skutków dla

[160] Art. 35 ust. 10 RODO: Ust. 1-7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.
[161] M.P. z 2019 r. poz. 666.

ochrony danych. MEN wraz z projektem **ustawy o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw**[162] przedstawił do zaopiniowania organowi nadzorczemu dokument o nazwie „Ocena skutków dla ochrony danych: Monitorowanie karier absolwentów szkół ponadpodstawowych". Dokonana przez resort ocena odpowiadała na pytania o cel projektu ustawy, uzasadniała pozyskiwanie wskazanych w regulacji zakresów danych osobowych, opisywała planowany proces przetwarzania danych i oceniała ryzyko tego przetwarzania z punktu widzenia osób, których te dane dotyczyły. Były to kwestie niezbędne do właściwej oceny proporcjonalności i konieczności zastosowanych rozwiązań.

Również w przypadku projektu **ustawy o zmianie ustawy – Karta Nauczyciela oraz niektórych innych ustaw**[163], MEN przedstawił organowi nadzorczemu ocenę skutków dla ochrony danych dla narzędzia informatycznego – Zintegrowanej Platformy Edukacyjnej. Dokument ten w znacznej mierze przyczynił się do dość szybkiego uzgodnienia projektu z organem nadzorczym oraz wyeliminowania z planowanych rozwiązań tych niezgodnych z RODO.

8.2. Informacja publiczna

Prezes Urzędu Ochrony Danych Osobowych wielokrotnie zwracał uwagę, że w toku prac nad przepisami **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 (ogólne rozporządzenie o ochronie danych)**[164] – choć poddawano ocenie wiele przepisów krajowych pod kątem ich zgodności z RODO – to analizy takiej nie przeprowadzono w odniesieniu do przepisów **ustawy o dostępie do informacji publicznej**. Tymczasem zawiera ona liczne unormowania, które nie tylko nie uwzględniają wymogów wynikających z rozporządzenia 2016/679, ale wprost wyłączają ochronę danych osobowych. Pozbawia to osoby, których dane dotyczą możliwości realizacji ich fundamentalnych uprawnień wynikających z RODO. Przepisy ww. ustawy w obecnym kształcie przewidują dostęp do informacji publicznej jako zasadę, od której

[162] DOL.401.582.2020.
[163] DOL.401.280.2020.
[164] Dz. U. z 2019 r. poz. 730.

odstępstwa są m.in. zawarte w art. 5 ust. 2 tego aktu[165]. Przepis ten w istocie wyłącza w całości ochronę danych osób pełniących funkcję publiczną i pozbawia ich ochrony wynikającej z RODO, w tym realizacji praw osób, których dane dotyczą, w każdej sytuacji, gdy dane osobowe są w związku z pełnieniem tej funkcji przetwarzane. Wyłączenie to nie zostało przeanalizowane pod kątem zgodności zarówno z art. 23[166], jak i z art. 86 RODO, co może skutkować (i często skutkuje) znacznym naruszeniem nie tylko prywatności osób pełniących funkcje publiczne, ale i osób trzecich takiej funkcji niepełniących (np. członków rodzin). Analiza orzeczeń wydanych do ustawy o dostępie do informacji publicznej wskazuje, że sądy często muszą dokonywać wykładni pojęcia informacji o osobach pełniących funkcje publiczne i informacji mających związek z pełnieniem tych funkcji, a zróżnicowana linia orzecznicza obrazuje, jak niejednolicie kształtowane są granice ochrony prywatności tych osób[167]. W interpretacji wskazanych pojęć sądy posiłkowały się tezami z uzasadnienia wyroku Trybunału Konstytucyjnego z 20 marca 2006 r.[168] Orzeczenie to nie odnosiło się jednak bezpośrednio do kwestii ochrony danych i zostało wydane przed wejściem w życie oraz rozpoczęciem stosowania RODO.

W ocenie organu właściwego w sprawie ochrony danych osobowych, udostępnianie informacji publicznej przy jednoczesnym poszanowaniu przepisów RODO w praktyce rodzi liczne wątpliwości. Tymczasem art. 86 oraz motyw 154 RODO, dające podstawę do udostępniania dokumentów urzędowych i informacji o osobach pełniących funkcje publiczne, wskazują na konieczność wprowadzenia stosownych rozwiązań w zakresie poszanowania ochrony danych osobowych do aktów prawnych regulujących to zagadnienie, co nie jest tożsame z pozostawieniem tej kwestii wyłącznie orzecznictwu sądów i ograniczaniem kompetencji Prezesa UODO do rozpatrywania skarg w tym zakresie[169].

---

[165] Zgodnie z treścią art. 5 ust. 2 ustawy o dostępie do informacji publicznej, prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

[166] Organ nadzorczy wskazał na trwające prace Europejskiej Rady Ochrony Danych (EROD) dotyczące Wytycznych 10/2020 w sprawie ograniczeń na podstawie art. 23 rozporządzenia 2016/679. EROD podkreślił w tym dokumencie, że zgodnie z orzecznictwem TSUE, art. 23 rozporządzenia 2016/679 nie może być interpretowany jako uprawnienie do podważenia przez państwo członkowskie poszanowania życia prywatnego z naruszeniem art. 7 Karty Praw Podstawowych lub innych gwarancji w niej zawartych.

[167] Zob. wyrok Wojewódzkiego Sądu Administracyjnego w Gdańsku z 22 stycznia 2020 r. sygn. akt II SAB/Gd 125/19, wyrok Naczelnego Sądu Administracyjnego z 14 lutego 2020 r. sygn. akt I OSK 1644/18, wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 4 grudnia 2019 r. sygn. akt II SA/Wa 1187/19.

[168] Sygn. akt K 17/05 (OTK-A 2006 r. Nr 3, poz. 30).

[169] Por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 24 stycznia 2020 r. w sprawie o sygn. akt II SA/Wa1927/19.

W opinii organu właściwego w sprawie ochrony danych osobowych, udostępnianie danych osobowych będących informacją publiczną jest objęte przepisami RODO, co potwierdzają art. 2 i art. 86 rozporządzenia. Z kolei art. 6 ust. 2 RODO daje podstawę przyjęcia bardziej szczegółowych przepisów regulujących relację dostępu do dokumentów urzędowych i kwestie ochrony danych osobowych. Tymczasem polski ustawodawca zdecydował się nie wprowadzać zmian w tym zakresie w ustawie o dostępie do informacji publicznej ani w żadnej innej ustawie, dotyczącej prawa do informacji pochodzących z dokumentów publicznych. W konsekwencji ustawa o dostępie do informacji publicznej nie określa szczegółowych wymogów przetwarzania i innych środków w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności (art. 6 ust. 2 rozporządzenia 2016/679). W związku z tym w opinii Prezesa UODO przy udostępnianiu informacji publicznej przepisy RODO stosować należy bezpośrednio, uwzględniając główne zasady ochrony danych osobowych (art. 5-10 ogólnego rozporządzenia) oraz uprawnienia osób, których dane dotyczą (art. 12-22 RODO).

Podnoszone nieścisłości obecnie obowiązujących przepisów ustawy o dostępie do informacji publicznej w zakresie niedostosowania tego aktu do rozporządzenia 2016/679, można także dostrzec w orzecznictwie[170]. W ocenie UODO, ze względu na tego rodzaju zapadające orzeczenia, niedopuszczalne jest pozostawianie wyżej wskazanych luk w przepisach dotyczących dostępu do informacji publicznej, tym bardziej że – jak wyżej wskazano – możliwe jest zapewnienie ich zgodności z przepisami RODO. Pozostawienie obecnego kształtu przepisów nie może być zaakceptowane, gdyż pozbawia osobę, której dane dotyczą, możliwości skutecznego dochodzenia jej praw, a tym samym skutecznego wniesienia skargi do organu nadzorczego, jak również jakiejkolwiek kontroli organu nadzorczego, w tym w trybie art. 58 ust. 2 lit. c RODO.

Organ nadzorczy wskazał na powyższe kwestie w czasie prac nad projektem **ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego**[171], która implementuje do polskiego porządku prawnego dyrektywę 2019/1024/UE Parlamentu Europejskiego i Rady z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego.

[170] Patrz: Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 24 stycznia 2020 r. (sygn. akt II SA/Wa1927/19) – w którym Sąd uchylił postanowienie Prezesa UODO zobowiązujące Kancelarię Sejmu do ograniczenia przetwarzania danych osobowych sędziów zawartych w wykazach sędziów popierających zgłoszenia kandydatów do Krajowej Rady Sądownictwa, poprzez nakazanie powstrzymania się od ich upubliczniania oraz udostępniania w jakiejkolwiek formie innym podmiotom do czasu wydania decyzji kończącej postępowanie w sprawie.
[171] DOL.401.398.2020.WL.OJ.

Na kwestie związane z zapewnieniem jawności życia publicznego przy poszanowaniu prywatności organ nadzorczy zwracał uwagę również przy okazji opiniowania innych projektów aktów normatywnych. Jako przykład można wskazać **poselski projekt ustawy o zmianie ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne**[172]. Organ nadzorczy zakwestionował przedstawiony do zaopiniowania przez Kancelarię Sejmu projekt, w zakresie jego zgodności z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej, gdyż istotnie ograniczał prawo do prywatności osób niepełniących funkcji publicznych. Dotyczyło to udostępniania informacji o majątku odrębnym małżonka Prezydenta Rzeczypospolitej Polskiej, Marszałka Sejmu, Marszałka Senatu, Prezesa Rady Ministrów, wicemarszałka Sejmu, wicemarszałka Senatu, wiceprezesa Rady Ministrów oraz ministra. Obowiązek udostępnienia zawierających dane osobowe informacji dotyczących osób, które nie pełnią funkcji publicznych oznacza, że zerwany zostaje związek pomiędzy wkroczeniem w sferę prywatności danej osoby (którym jest podanie do publicznej wiadomości informacji o jej majątku odrębnym bez jej zgody) a faktem posiadania przez tę osobę określonego władztwa decyzyjnego, które to władztwo uzasadniało ograniczenie jej prawa do prywatności.

8.3. Stanowiska organu nadzorczego w związku z epidemią COVID-19

W 2020 r. wiele regulacji prawnych tworzonych było na potrzeby realizacji zadań mających na celu ograniczenie i złagodzenie skutków pandemii COVID-19. Mimo że zapewnienie adekwatnego poziomu ochrony danych osobowych przy wprowadzaniu **nowych instytucji prawnych w związku z trwającą epidemią COVID-19** było przedmiotem szczególnego zainteresowania organu nadzorczego, wiele aktów prawnych dotyczących tego zagadnienia nie zostało przedstawionych do zaopiniowania. Wynikało to być może z tempa prowadzonych procesów legislacyjnych, lecz nie powinno mieć miejsca.

Kluczowe z punktu widzenia stanowiska organu nadzorczego w związku z pandemią COVID-19 było **wystąpienie do Ministra Zdrowia o wprowadzenie zmian w rozporządzeniu Ministra Zdrowia z dnia 7 kwietnia 2020 r. w sprawie Krajowego Rejestru Pacjentów z COVID-19**[173]. Zaniepokojenie organu nadzorczego wywołała kwestia legalności oraz konieczności przetwarzania danych osobowych pacjentów, u których wynik testu na obecność wirusa SARS-CoV-2 okazał się negatywny. Gromadzenie informacji o stanie zdrowia jest nierozerwalnie związane z przetwarzaniem

[172] DOL.401.2.2020.WL.OJ.
[173] DOL.413.13.2020.

tej szczególnej kategorii danych w rozumieniu art. 9 ust. 1 RODO. Dane tej kategorii objęte są szczególnym reżimem przetwarzania – przetwarzanie tych danych jest możliwe, o ile spełniona zostanie jedna z przesłanek określona w art. 9 ust. 2 RODO, m.in. gdy przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych (lit. i). Niemniej uwzględnienie dopuszczalności przetwarzania danych wrażliwych, w pewnych ściśle określonych okolicznościach, nie oznacza, że prawo do ochrony danych osobowych jest prawem bezwzględnym. W świetle motywu 4 RODO prawo to należy wyważyć względem innych praw podstawowych zgodnie z zasadą proporcjonalności, co oznacza, że niekiedy będzie ono musiało ulec ograniczeniu na rzecz ochrony innego prawa. Projekt rozporządzenia Ministra Zdrowia z dnia 7 kwietnia 2020 r. w sprawie Krajowego Rejestru Pacjentów z COVID-19 nie został przekazany Prezesowi Urzędu Ochrony Danych Osobowych do zaopiniowania, a powinno to nastąpić już na etapie jego projektowania. Organ nadzorczy w powołanym wystąpieniu wskazał, że nie kwestionuje celu, w jakim został utworzony Krajowy Rejestr Pacjentów z COVID-19. Mając na uwadze obecną sytuację epidemiczną, niezbędne jest ewidencjonowanie danych pacjentów z COVID-19 w celu prowadzenia nadzoru nad efektami ich leczenia oraz możliwości porównywania efektów terapeutycznych uzyskiwanych lokalnie z danymi światowymi. Podkreślił jednak, że Rejestr powinien zawierać dane niezbędne dla celów, jakim ma służyć, tj. ewidencjonowaniu pacjentów z COVID-19, a służy również gromadzeniu danych wszystkich osób testowanych na obecność SARS-CoV-2.

Po ustosunkowaniu się Ministra Zdrowia do ww. wystąpienia, w którym stwierdzono m.in., że „Przetwarzanie w Krajowym Rejestrze Pacjentów z COVID-19 danych osobowych pacjentów z negatywnym wynikiem testu na obecność wirusa SARS-CoV-2 zostało ograniczone do oczekiwań związanych z nadzorem nad efektami leczenia oraz możliwością porównywania efektów terapeutycznych”, organ nadzorczy ponownie podkreślił wątpliwość tej argumentacji, ponieważ cele te mogą zostać zrealizowane na podstawie danych populacyjnych, tj. bez użycia indywidualnych danych osobowych. Organ nadzorczy zwrócił ponownie uwagę na fundamentalne znaczenie oceny skutków dla ochrony danych, o której mowa w art. 35 ust. 10 RODO, dla tworzenia tego typu rozwiązań legislacyjnych. Organ nadzorczy wskazał również, że w sprawie tej należy zwrócić uwagę na stanowisko Europejskiej Rady Ochrony Danych (EROD), która w oświadczeniu w sprawie przetwarzania danych osobowych w kontekście pandemii COVID-19 przyjętym 19 marca 2020 r.

wskazała m.in. na kwestię dotyczącą konieczności zapewnienia tymczasowości stosowania rozwiązań ingerujących w sferę prywatności, tj. korzystania z nich wyłącznie w czasie epidemii. Prezes UODO odniósł się również do kwestii okresu, w którym dokonany zostanie przegląd przepisów. Ponieważ resort zdrowia poinformował, że planuje dokonanie analizy i oceny funkcjonowania ww. rejestru dopiero po 12 miesiącach, Prezes UODO wskazał, że okres dwunastomiesięczny jest zbyt długi, jak na zbieranie danych, które nie wydają się być niezbędne. Podniósł, że w przypadku tworzenia rejestrów medycznych – ze względu na ich szczególny charakter – nie powinno mieć miejsca tak długie weryfikowanie zasadności funkcjonowania i przydatności regulacji obowiązujących w krajowym porządku prawnym, a odnośnie do Krajowego Rejestru Pacjentów z COVID-19 dotyczy to zarówno zakresu danych osobowych, jak i celu ich przetwarzania.

Projektem, który został przekazany do zaopiniowania organowi nadzorczemu dopiero na etapie prac sejmowych (przez Kancelarię Sejmu) był **projekt ustawy o zmianie niektórych ustaw w celu zapewnienia funkcjonowania ochrony zdrowia w związku z epidemią COVID-19 oraz po jej ustaniu**[174]. Prezes UODO zwrócił uwagę przede wszystkim na zmiany w funkcjonowaniu systemu informacji w ochronie zdrowia, których wprowadzenie zakładała ustawa. W ocenie organu nadzorczego uchylenie przepisu dotyczącego ram powierzenia danych podmiotom wyspecjalizowanym, przy pozostawieniu funkcjonującego obecnie podziału na administratora danych i administratora systemu, może doprowadzić do utraty faktycznej kontroli nad danymi sensytywnymi, powierzonymi podmiotom wyspecjalizowanym. Prezes UODO wskazał więc, że zasady powierzenia danych podmiotom wyspecjalizowanym – „powierzenie ustawowe" – muszą odpowiadać wymogom art. 28 RODO. Wprowadzanie do porządku prawnego tego typu rozwiązań dotyczących przetwarzania szczególnych kategorii danych, jakimi są dane o stanie zdrowia, powinno być poprzedzone pogłębioną analizą i zostać odzwierciedlone w ocenie skutków dla ochrony danych, o której mowa w art. 35 ust. 10 RODO. Takiej analizy w toku procesu legislacyjnego nie przedstawiono, a zatem nie jest znana ocena ryzyka związanego z przetwarzaniem danych na mocy tych przepisów.

Do problemu funkcjonowania w warunkach epidemii COVID-19 takich podmiotów, jak domy pomocy społecznej, organ nadzorczy odniósł się w stanowisku do projektu **rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej zmieniającego rozporządzenie w sprawie domów pomocy**

[174] DOL.401.312.2020.

społecznej[175]. Prezes UODO podniósł, że w projekcie rozporządzenia należy wprost wskazać, że w przypadku wystąpienia podejrzenia bądź potwierdzenia zakażenia np. wirusem SARS-CoV-2 wśród pracowników lub mieszkańców domu pomocy społecznej, to mieszkańcom i pracownikom domu pomocy społecznej zostanie przedstawiona informacja o takim zdarzeniu, która jednak będzie miała charakter ogólny – nie będzie zawierała w swej treści danych osobowych, m.in. nie będzie wiązała się z upublicznianiem danych osobowych.

Trwająca epidemia COVID-19 spowodowała konieczność wprowadzania do polskiego porządku prawnego nowych, ale jednocześnie mających charakter epizodyczny, rozwiązań normatywnych umożliwiających funkcjonowanie społeczeństwa w nadzwyczajnych warunkach. Organ nadzorczy w swoich opiniach legislacyjnych wskazywał, że rozumie konieczność i cele wprowadzanych rozwiązań, w tym w zakresie dostosowywania różnych instytucji prawnych do sytuacji, w której niemożliwy jest bezpośredni kontakt między osobami (obywatelami) a instytucjami państwa powołanymi do rozpatrywania konkretnych spraw. Podnosił jednak, że w tej sytuacji istotne jest zachowanie odpowiedniej hierarchii aktów prawnych (regulowanie fundamentalnych kwestii związanych z ochroną danych osobowych ustawą, a nie rozporządzeniem) oraz przeprowadzenie oceny skutków dla ochrony danych, o której mowa art. 35 ust. 10 RODO – szczególnie w przypadku innowacyjnych rozwiązań informatycznych oraz w związku z przetwarzaniem danych o szczególnym charakterze, sensytywnych.

Organ nadzorczy wskazał na te problemy m.in. w opinii do projektu **rozporządzenia Ministra Cyfryzacji w sprawie profilu zaufanego i podpisu zaufanego**[176]. Podniósł, że przepisy art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne zostały wprowadzone art. 33 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, oraz za sprawą niektórych innych ustaw w związku z trwającą epidemią. Mają więc charakter tymczasowy i nie powinny być utrzymywane w porządku prawnym dłużej niż jest to niezbędne dla ww. szczególnych celów. Projektodawca powinien więc rozważyć, jak długo zamierza utrzymać instytucje tymczasowego profilu zaufanego oraz potwierdzania go w formie transmisji audiowizualnej – gdyż takie rozwiązania, jako zapewniające niższy niż dotychczas poziom ochrony danych osobowych, powinny być utrzymane wyłącznie tymczasowo. Instytucja wideoidentyfikacji wnioskodawcy, jaką wprowadził art. 20ca

[175] DOL.401.370.2020.
[176] DOL.401.218.2020.

ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym nie tylko danych tzw. zwykłych, ale także szczególnych kategorii danych (w tym np. biometrycznych, danych dotyczących zdrowia) czy danych dotyczących krajowego numeru identyfikacyjnego – PESEL. Korzystanie z technologii, która będzie umożliwiała identyfikację wizerunku, ściśle wiąże się z koniecznością zrealizowania wielu przesłanek, dokonaniem oceny skutków dla ochrony danych oraz ograniczeniem do minimum potencjalnie uzyskiwanych danych. Zgodnie z art. 35 RODO, każdy podmiot, także projektodawca w związku z przyjmowaniem podstawy prawnej przetwarzania danych, musi ocenić, czy istnieje ryzyko naruszenia praw i wolności osób, w tym poufności, integralności oraz dostępności danych. W sytuacji, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych, w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO. Mając na uwadze istotny poziom ryzyka związanego z wideoweryfikacją tożsamości osoby – instytucja ta powinna zostać poddana analizie w ramach oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Unormowania ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne powinny określać wymogi techniczno-organizacyjne tej procedury, ustalać jednolite standardy techniczne oraz sposoby zabezpieczenia komunikacji gwarantujące odpowiedni poziom bezpieczeństwa usługi, a także zapewniać odpowiedni system jej wewnętrznej kontroli. W omawianej opinii Prezes UODO wskazał, że uzasadnione jest ponowne przeanalizowanie projektowanego rozporządzania – jako nakładającego prawa i obowiązki na adresatów tych norm, zarówno osoby, których dane dotyczą, jak i podmioty przetwarzające dane osobowe – pod kątem oceny, czy kwestie nim objęte nie powinny zostać uregulowane w przepisach rangi ustawy, a nie aktu wykonawczego. Zaznaczył też, że niezależnie od tego, czy projektodawca przed wprowadzeniem do polskiego porządku prawnego art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne przeprowadził ocenę skutków dla ochrony danych, ocena ta powinna zostać przeprowadzona również *ex post*, a jej wyniki uwzględnione przy najbliższej nowelizacji tej ustawy. Ministerstwo Cyfryzacji, odnosząc się do wątpliwości organu nadzorczego stwierdziło, że „przepisy art. 20ca ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne nie mają charakteru tymczasowego. Tymczasowy jest profil zaufany wydawany na ich podstawie, jak również tymczasowa może być usługa online, o której mowa w tym przepisie, gdyż minister

może, ale nie musi, udostępniać takiej usługi. Wideoweryfikacja jest to rozwiązanie przyszłościowe, które tylko pozornie jest mniej bezpieczne od potwierdzania tożsamości w trakcie fizycznej obecności w punkcie potwierdzającym".

Tak więc Ministerstwo Cyfryzacji nie traktuje rozwiązań wprowadzonych w związku z obecnie trwającą pandemią jako tymczasowych, uważając je jednocześnie za przyszłościowe i bezpieczne. Dlatego Prezes UODO będzie bacznie monitorował stosowanie tego rozwiązania.

8.4. Informatyzacja państwa

W 2020 r. Prezes UODO opiniował **wiele aktów normatywnych związanych z procesem informatyzacji państwa**. Podobnie jak w latach ubiegłych, organ właściwy w sprawie ochrony danych osobowych – przedstawiając swoje opinie do projektów i realizując eksperckie wsparcie z zakresu przetwarzania danych osobowych – zwracał uwagę na takie problemy, jak np.: ujawnianie numeru PESEL w czasie składania podpisu elektronicznego, daleko posunięta automatyzacja procesów decyzyjnych wobec osób fizycznych czy wielkoskalowe przetwarzanie informacji o osobach, również takich jak numery rejestracyjne samochodów.

W czasie prac nad projektem **ustawy o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw**[177], który został przekazany do organu nadzorczego dopiero przez Kancelarię Sejmu, Prezes UODO zwrócił uwagę na zagrożenia wynikające z ujawniania numeru PESEL przy składaniu różnych form podpisu elektronicznego. Zgodnie z deklaracją projektodawcy zawartą w uzasadnieniu ustawy, celem zmiany przepisów było umożliwienie wydawania zaświadczeń w postaci elektronicznej opatrzonych kwalifikowaną pieczęcią elektroniczną, co ma znacząco usprawnić procedury wydawania zaświadczeń z Krajowego Rejestru Karnego a także zaświadczeń wydawanych przez inne organy administracji publicznej. W dotychczasowym stanie prawnym jedynym sposobem skutecznego wydania zaświadczenia w formie elektronicznej było opatrzenie go kwalifikowanym podpisem elektronicznym. Nowe brzmienie art. 217 § 4 Kodeksu postępowania administracyjnego (K.p.a.), nadawane przez art. 1 projektu ustawy, stanowi, że zaświadczenie wydaje się w formie dokumentu elektronicznego, jeżeli zażąda tego osoba ubiegająca się o zaświadczenie. W takim przypadku zaświadczenie jest opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. O ile pozytywnie organ właściwy w sprawie ochrony danych

[177] DOL.401.521.2020.

osobowych ocenił umożliwienie używania dla podpisania zaświadczenia wydawanego w formie dokumentu elektronicznego 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 danej o tak szczególnym charakterze, jaką jest numer PESEL), o tyle przypomniał, że pogłębionej analizy wymaga analogiczne unormowanie w zakresie podpisu zaufanego oraz podpisu osobistego. Zwrócił uwagę, że 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). Konstrukcja projektowanego art. 217 § 4 K.p.a., która w równoważny sposób traktuje kwalifikowany podpis elektroniczny, pieczęć elektroniczną, podpis zaufany oraz podpis osobisty, może zatem 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. W przypadku tych ostatnich dwóch narzędzi nie ma możliwości wyłączenia numeru PESEL z certyfikatu podpisu, co stwarza zagrożenie dla prywatności osób, ze względu na – będące konsekwencją takiego rozwiązania – zobligowanie do ujawniania i dalszego posługiwania się identyfikatorami osobistymi (PESEL) dla celów służbowych. PESEL jest unikalnym identyfikatorem osoby, zawierającym w sobie wiele informacji, m.in. o wieku i płci. Ujawnienie numeru PESEL osobie niepowołanej może rodzić ryzyko kradzieży tożsamości. Dodatkowo, na podstawie art. 87 RODO, państwo członkowskie może określić w przepisach prawa szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym (którym w Polsce jest PESEL), ale przyjęte rozwiązania muszą zagwarantować zachowanie odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, jakie przewidują przepisy ogólnego rozporządzenia o ochronie danych.

Ze względu na nieprzeprowadzenie przez projektodawcę oceny skutków dla ochrony danych, organ nadzorczy nie został przekonany, że projektodawca dokonał ważenia interesów pomiędzy celami projektowanych zmian a prawami osób, których dane dotyczą, tj. nie wykazał niezbędności przyjmowanych rozwiązań z uwzględnieniem zasad wynikających z RODO. W świetle brzmienia art. 22^1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (K.p.) organ nadzorczy stwierdził także brak podstaw do wymagania przez pracodawcę od pracownika ujawniania swojego numeru PESEL, poprzez podpisywanie dokumentów elektronicznych (w tym przypadku zaświadczeń).

W czasie prac nad projektem **rozporządzenia Ministra Cyfryzacji w sprawie kontroli korzystania z dostępu do danych z rejestru dowodów osobistych w trybie ograniczonej teletransmisji danych**[178]**,** organ nadzorczy po raz kolejny wskazał na podnoszony wielokrotnie na przestrzeni lat problem, jaki generuje ujawnianie numeru PESEL podczas składania podpisu elektronicznego.

Zgodnie z projektem rozporządzenia, w części przypadków prowadzenia akt kontroli, protokół kontroli podpisuje się kwalifikowanym podpisem elektronicznym, podpisem osobistym lub podpisem zaufanym. Od decyzji ministra właściwego do spraw informatyzacji zależeć będzie, czy akta kontroli, w tym protokół, będą prowadzone w formie elektronicznej czy też papierowej. W przypadku gdy organ ten zdecyduje się na elektroniczną formę prowadzenia akt kontroli, jedyną skuteczną formą podpisania protokołu z kontroli przez kierownika podmiotu kontrolowanego lub osobę pełniącą jego obowiązki jest złożenie podpisu elektronicznego, podpisu osobistego lub podpisu zaufanego. Ze względu na konstrukcję certyfikatów podpisów elektronicznych, w przypadku takich kontroli będzie dochodzić do obligatoryjnego ujawniania numeru PESEL przez osoby zobligowane do podpisania protokołu kontroli w formie elektronicznej, tymczasem numer PESEL w przypadku protokołu w formie papierowej nie byłby ujawniany. Organ nadzorczy przestrzegał zatem projektodawcę, że numer PESEL podlega szczególnym warunkom ochrony na podstawie art. 87 RODO, a jednocześnie jego podanie nie będzie konieczne w przypadku protokołu kontroli prowadzonego w formie papierowej. Zwrócił też uwagę, że zgodnie z art. 68 ust. 4 pkt 2 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, dane z rejestru dowodów osobistych mogą być udostępniane wszystkim podmiotom, które wykażą w tym interes faktyczny. Tym samym projektowane rozporządzenie wymusza na kierownikach tych podmiotów (również niepublicznych) posługiwanie się narzędziami ujawniającymi ich numer PESEL.

W opinii Prezesa UODO, problem wskazany w opiniach legislacyjnych do ww. aktów normatywnych będzie tylko narastał, jeśli nie zostaną podjęte działania zmierzające do ograniczenia ujawniania numeru PESEL w certyfikatach podpisów elektronicznych – podpisu osobistego, podpisu zaufanego oraz kwalifikowanego podpisu elektronicznego.

Informatyzacja państwa prowadzi również do powstawania problemów związanych z tym, jakie informacje należy uznać za dane osobowe. Zgodnie z definicją zawartą w art. 4 ust. 1 RODO, dane osobowe są informacjami, za pośrednictwem których można zidentyfikować konkretną osobę

[178] DOL.401.477.2020.WL.PM.

fizyczną. Nie istnieje zamknięty katalog danych, które można uznać za dane osobowe. To, czy dana informacja stanowi dane osobowe zależy często od kontekstu, w którym występuje. W szczególności dla organów publicznych, dysponujących informacjami z rejestrów państwowych, dana informacja może stać się danymi osobowymi, których przetwarzanie powinno być objęte reżimem RODO.

Problem tego typu danych – a konkretnie numeru rejestracyjnego pojazdu – został podniesiony przez organ nadzorczy przy okazji prac nad projektem **ustawy o zmianie ustawy o autostradach płatnych oraz Krajowym Funduszu Drogowym oraz niektórych innych ustaw**[179]. Projektodawca, wśród danych, które ma zawierać bilet autostradowy wskazał m.in. numer rejestracyjny pojazdu. Numer ten jest informacją, za pośrednictwem której możliwe jest zidentyfikowanie – w sposób pośredni – osoby fizycznej, będącej właścicielem pojazdu. Jest tym samym daną osobową właściciela pojazdu. Z uwagi na zintegrowanie systemu teleinformatycznego, za pośrednictwem którego będą sprzedawane bilety autostradowe, z Systemem Poboru Opłaty Elektronicznej KAS, informacja o numerze rejestracyjnym pojazdu będzie wprowadzana do Systemu Poboru Opłaty Elektronicznej KAS. Tym samym Szef Krajowej Administracji Skarbowej uzyska dostęp do danych – numerów rejestracyjnych – wszystkich właścicieli pojazdów uiszczających opłatę za przejazd autostradą (alternatywną metodą uiszczenia opłaty będą dane z urządzenia, o którym mowa w art. 13i ust. 3a ustawy z dnia 21 marca 1985 r. o drogach publicznych, wśród których również znajdować się będą dane osobowe, w tym numer rejestracyjny pojazdu). Organ nadzorczy zwrócił zatem projektodawcy uwagę, że w dotychczasowym stanie prawnym nie było konieczności podawania danych osobowych dla dokonania przejazdu autostradą (opłata może być uiszczana „na bramce" autostrady bez podawania numeru rejestracyjnego pojazdu). Obecnie projektowane przepisy wprowadzą natomiast do polskiego porządku prawnego obowiązek podawania danych osobowych – numeru rejestracyjnego pojazdu – obligatoryjnie przy każdym przejeździe autostradą i zakupie biletu autostradowego. Organ nadzorczy zwrócił uwagę na związane z tym ryzyka i wskazał, że powinny być one przeanalizowane w ocenie skutków dla ochrony danych (zgodnie z art. 35 RODO). Przede wszystkim projektodawca powinien wyjaśniać, czy została przeprowadzona ocena niezbędności przyjmowania tych rozwiązań, powodujących przetwarzanie danych osobowych, czy celu projektodawcy nie da się osiągnąć przy pomocy danych nieidentyfikujących jednoznacznie osób (art. 11 RODO) oraz jakie są wyniki tej analizy, co do wpływu przyjmowanych rozwiązań na ochronę danych osobowych i prywatności użytkowników autostrad będących właścicielami pojazdów.

[179] DOL.401.554.2020.

Projektodawca powinien wykazać, czy wziął pod uwagę, że w wyniku projektowanych rozwiązań utworzy zasób/bazę danych wszystkich osób przejeżdżających autostradami, o ile są właścicielami pojazdów, zawierającą takie informacje, jak numer rejestracyjny pojazdu; przybliżony czas przejazdu oraz miejsce – odcinek autostrady, na którym przejazd się odbywał. Co za tym idzie, wyjaśnione powinno zostać, czy i jak projektodawca zapewnił odpowiednie gwarancje przetwarzania takiej bazy danych, która w bardzo łatwy sposób może posłużyć do wielkoskalowego monitorowania przemieszczania się/profilowania osób fizycznych. Przede wszystkim, czy wziął pod uwagę potencjalny kierunek rozwoju tej bazy, który w miarę poszerzenia spektrum danych w niej gromadzonych, może doprowadzić do materializacji na razie potencjalnych ryzyk. Prezes UODO wskazał, że przy tworzeniu tego typu rozwiązań warto wziąć pod uwagę dokumenty Grupy Roboczej Art. 29 oraz Europejskiej Rady Ochrony Danych, w tym m.in. Wytyczne dotyczące oceny skutków dla ochrony danych WP 248 oraz Wytyczne w sprawie zautomatyzowanego podejmowania decyzji WP 251[180].

Ponieważ proces legislacyjny jest w toku, Prezes UODO z uwagą będzie śledził dalsze prace w tym zakresie.

Problem zautomatyzowanego przetwarzania danych oraz monitorowania osób stał się bardzo doniosły w związku z wprowadzanymi w 2020 r. np. **systemami zdalnej nauki oraz przeprowadzania egzaminów**, które odpowiadać miały potrzebom porozumiewania się na odległość w dobie epidemii.

W czasie prac nad projektem **rozporządzenia Ministra Infrastruktury w sprawie Krajowego Programu Szkolenia w zakresie ochrony lotnictwa cywilnego**[181], organ nadzorczy przedstawił wątpliwości dotyczące sposobu rejestracji przebiegu egzaminu kończącego szkolenie lub ponowną certyfikację. W ocenie organu nadzorczego, wykorzystywanie monitoringu wizyjnego nie jest niezbędne do zapobiegania nieuczciwym praktykom egzaminowanych podczas egzaminu. Istota ochrony prawa do prywatności i prawa do ochrony danych osobowych wymaga, aby ograniczanie tych praw następowało tylko w niezbędnym zakresie. Jak wskazał organ w opinii legislacyjnej, ograniczanie praw poprzez stosowanie monitoringu może następować tylko wtedy, gdy nie można zastosować innych metod kontroli, jak np. wejście na salę egzaminacyjną bez urządzeń potencjalnie

[180] Przyjęte 4 kwietnia 2017 r. Wytyczne Grupy Roboczej Art. 29 (WP 248) dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 oraz przyjęte w dniu 3 października 2017 r. Wytyczne Grupy Roboczej Art. 29 (WP 251) w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE.
[181] DOL.401.412.2020.

wykorzystywanych do nieuczciwego udziału w egzaminie. Dokumentowanie zdarzeń i zachowań osób poprzez ich monitoring może być wprowadzane wtedy, kiedy inne, mniej inwazyjne metody zapewniania właściwego zachowania się osób zdających podczas egzaminów są niewystarczające. Ingerowanie w ww. prawa poprzez używanie kamer i utrwalanie w ten sposób przebiegu egzaminu będzie zbędne np. jeżeli pomieszczenia, w których przeprowadzane będą egzaminy, poddane zostaną obserwacji przez wyznaczone do tego osoby.

W czasie prac nad projektem **ustawy o zawodzie farmaceuty**[182] organ nadzorczy wskazał natomiast na potrzebę przeprowadzenia analizy konieczności, niezbędności i proporcjonalności zastosowanych rozwiązań, mogących mieć wpływ na ograniczenie prawa do prywatności w kontekście uregulowania w projekcie ustawy możliwości dokumentowania za pomocą urządzeń rejestrujących obraz i dźwięk przebiegu Farmaceutycznego Egzaminu Weryfikacyjnego (FEW), przebiegu udostępniania testów i pytań testowych FEW zdającemu egzamin, na jego wniosek, po ich wykorzystaniu w FEW, archiwizacji przez okres 3 miesięcy od dnia powstania zapisu zarejestrowanego obrazu i dźwięku związanego z przebiegiem FEW lub udostępnianiem testów i pytań testowych oraz dyskwalifikowania zdającego po zakończeniu FEW na podstawie analizy obrazu i dźwięku zarejestrowanych za pomocą urządzeń rejestrujących. Odnosząc się do rejestrowania dźwięku, Prezes UODO zaznaczył, 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. Zastosowanie rejestracji dźwięku w przypadku FEW wydaje się, w opinii organu ds. ochrony danych osobowych, nadmiarową formą przetwarzania danych. Zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO) i zasada ograniczenia celu (art. 5 ust. 1 lit. b RODO) oraz sporządzone na wykładni tych zasad dobre praktyki w odniesieniu do monitoringu wskazują, że nie powinno się stosować monitoringu wizyjnego w połączeniu z nagrywaniem dźwięku. Prezes UODO nie negował wskazanego w projektowanych przepisach celu przetwarzania danych. Zarekomendował projektodawcy przeprowadzenie oceny, czy również uzasadnione i niezbędne jest, aby poprzez nagrywanie obrazu – formę rejestracji zachowań osób zdających przedmiotowe egzaminy oraz udostępniania testów i pytań testowych – realizowane były cele wskazane w tych przepisach. Wskazał, aby projektowane przepisy realizowały potrzebę ochrony prawa do prywatności i ochrony danych osobowych oraz by prawa te ograniczane były tylko w niezbędnym zakresie. Tego rodzaju

[182] DOL.401.67.2020.

dokumentowanie zachowań osób może być wprowadzane wtedy, kiedy inne – mniej inwazyjne metody zapewniania właściwego zachowania się osób zdających egzaminy oraz osób, którym udostępnia się testy – są niewystarczające. Rejestrowanie za pomocą kamer przebiegu egzaminu oraz udostępniania testów będzie zbędne, jeżeli pomieszczenia, w których przeprowadzane będą egzaminy i udostępniane testy, będą nadzorowane przez osoby do tego wyznaczone. W związku z powyższym Prezes UODO nie zalecał stosowania kamer w celu udowodnienia zdającemu naruszenia zakazów, o których stanowią opiniowane przepisy. Zarekomendował natomiast przeprowadzenie oceny skutków dla ochrony danych w odniesieniu do przetwarzania danych osobowych za pośrednictwem kamer, tj. monitoringu przestrzeni i osób oraz nagrywania i zapisywania zarejestrowanego obrazu. Taka ocena skutków mogłaby wykazać konieczność lub brak niezbędności wprowadzenia możliwości zastosowania kamer z możliwością nagrywania dźwięku – jako jedynego środka mogącego zapewnić właściwe zachowanie osób zdających egzaminy. W swoim eksperckim stanowisku do tego projektu organ wskazał, że pomocne w sporządzeniu właściwej oceny skutków w kontekście nagrywania obrazu i dźwięku mogą być wytyczne Europejskiej Rady Ochrony Danych nr 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo wersja 2.0[183]. Prezes UODO zawnioskował o rozważenie możliwości wprowadzenia innych, mniej ingerujących w prywatność narzędzi niż nagrywanie obrazu i dźwięku, o którym mowa w projektowanych przepisach.

W 2020 r. rozpoczął się również proces legislacyjny ustawy – **Prawo komunikacji elektronicznej**[184], która ma zastąpić obecnie obowiązującą ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz wdrożyć do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r., ustanawiającej Europejski kodeks łączności elektronicznej. Organ nadzorczy uczestniczył zarówno w prekonsultacjach, jak i w opiniowaniu projektu ustawy. Zaangażowanie przez projektodawcę organu nadzorczego w te etapy prac ocenić należy pozytywnie. Niestety, projektodawca nie przeprowadził jednak oceny skutków dla ochrony danych, o której mowa w art. 35 ust. 10 RODO w odniesieniu do projektu ustawy.

[183] Przyjęte 29 stycznia 2020 r. Wytyczne Europejskiej Rady Ochrony Danych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo wersja 2.0.
[184] DOL.401.117.2020.

Projektowane regulacje Prawa komunikacji elektronicznej powielają znaczną część unormowań Prawa telekomunikacyjnego, budzących od wielu lat zastrzeżenia organu nadzorczego. Prezes UODO podkreślał, że projektowana ustawa powinna wprost zakazywać utrwalania zawierających dane osobowe dokumentów tożsamości przez dostawców usług telekomunikacyjnych, którzy uprawnienie to domniemują na podstawie ogólnych sformułowań dotyczących przetwarzania danych abonentów. Dokumenty tożsamości zawierają znacznie szersze spektrum danych niż jest niezbędne do weryfikacji tożsamości, dlatego nie może dochodzić do ich kopiowania przez dostawców usług telekomunikacyjnych. W przeciwnym razie dochodzi do naruszenia zasady zgodności z prawem oraz przejrzystości (art. 5 ust. 1 lit a RODO), zasady ograniczenia celu (art. 5 ust. 1 lit. b RODO) i zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO). Organ nadzorczy wskazywał również na potencjalną kolizję kompetencji pomiędzy Prezesem UODO a Prezesem Urzędu Komunikacji Elektronicznej. Rozwój nowych technologii prowadzi do uznania takich identyfikatorów, jak te zawarte w plikach „cookie" (motyw 30 RODO), za dane osobowe. Dlatego też unormowania Prawa komunikacji elektronicznej powinny wprost wskazywać, że uprawnienia Prezesa UKE do nakładania kar pieniężnych za przetwarzanie danych abonentów lub danych użytkowników końcowych bez podstawy prawnej, nie powinno być interpretowane jako wyłączające analogiczne uprawnienie Prezesa UODO, wynikające wprost z art. 83 RODO. Obecnie trwają, na poziomie Unii Europejskiej, prace **nad projektem rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), tzw. rozporządzeniem ePrivacy**. Będzie to akt prawny, który w sposób zasadniczy zmieni kształt przepisów dotyczących ochrony danych osobowych w sektorze telekomunikacyjnym. Dlatego też organ nadzorczy zakłada przeprowadzenie ponownej dyskusji nad podziałem kompetencji pomiędzy Prezesem UKE a Prezesem UODO, tak aby przyszła implementacja tego aktu prawnego do polskiego porządku prawnego umożliwiała tym dwóm organom jak najlepszą ochronę prywatności użytkowników końcowych usług telekomunikacyjnych. Oprócz powyższych zastrzeżeń Prezes UODO zgłosił do projektu ustawy wiele uwag dotyczących m.in. retencji danych telekomunikacyjnych, zasad przetwarzania danych użytkowników końcowych oraz uprawnień organów państwa nadawanych przez Prawo komunikacji elektronicznej.

Problem podziałów kompetencji pomiędzy organami nadzorującymi przetwarzanie danych osobowych został poruszony również podczas prac nad projektem **stanowiska Rządu RP**

dotyczącego Rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi[185]. Organ nadzorczy wskazał, że istotne jest doprecyzowanie kompetencji podmiotów sektorowych – których celem ma być wspieranie organów sektora publicznego udzielających dostępu do ponownego wykorzystywania kategorii danych – w zakresie dotyczącym egzekwowania przetwarzania danych osobowych, w tym nakładania kar i relacji tych podmiotów do organów nadzorczych. Pozwoli to uniknąć ewentualnych sporów kompetencyjnych, wynikających z podobnej materii, regulowanej przez rozporządzenie 2016/679 i projektowane rozporządzenie w sprawie europejskiego zarządzania danymi. Konieczne jest także podkreślenie prymatu roli organu nadzorczego, nadrzędnego ze względu na to, że zarówno obowiązujące przepisy rozporządzenia 2016/679, jak i projektowane przepisy rozporządzenia w sprawie europejskiego zarządzania danymi będą miały tę samą rangę i będą działały bezpośrednio, a przez to brak ww. doprecyzowania może powodować spory kompetencyjne i konieczność ich rozstrzygania. W ocenie organu nadzorczego należy dążyć do tego, żeby przepisy rozporządzenia w sprawie europejskiego zarządzania danymi były zgodne z przepisami rozporządzenia 2016/679 i wyrażonymi w nich zasadami dotyczącymi przetwarzania danych osobowych, a także by odzwierciedlały zawarte w tym akcie podejście do udostępniania, przetwarzania, przepływu i ochrony danych, a w szczególności, aby nie doprowadziły do obniżenia standardów ochrony danych osobowych. Niepożądane byłoby także wprowadzenie niezależnego, równoległego czy odmiennego – w stosunku do już istniejących w tej dziedzinie standardów – porządku przetwarzania danych osobowych czy udostępniania do ponownego wykorzystania informacji sektora publicznego. Nie kwestionując konieczności uściślenia warunków przetwarzania danych osobowych ze względu na specyfikę danego przetwarzania, powinno unikać się sytuacji rozproszenia przepisów i wymogów prawnych w wielu aktach prawnych, a także niespójności pomiędzy poszczególnymi rozwiązaniami sektorowymi, zwłaszcza w aktach prawnych tej samej rangi.

8.5. Podsumowanie

Wyżej wskazane zagadnienia nie wyczerpują całego katalogu spraw legislacyjnych, jakimi w 2020 r. zajmował się organ nadzorczy. Wśród projektów aktów normatywnych, które wpłynęły do zaopiniowania organu nadzorczego, były również umowy międzynarodowe, akty prawa wspólnotowego opiniowane w ramach prac na poziomie Unii Europejskiej oraz dokumenty

[185] DOL.401.660.2020.

o charakterze uchwał rady ministrów dotyczące danych osobowych. Wśród zagadnień, które od lat bacznie śledzi organ nadzorczy, znajdują się sprawy dotyczące sektora bankowego i ubezpieczeniowego, statystyki publicznej, przetwarzania danych przez organy ścigania oraz systemu ochrony zdrowia.

Dokonywana przez organ właściwy w sprawie ochrony danych osobowych analiza projektów aktów prawnych wskazuje, że projektodawcy ze wszystkich sektorów m.in.:

- nie wykonują oceny wpływu planowanych rozwiązań na ochronę danych – tj. oceny skutków dla ochrony danych w ramach oceny skutków regulacji w związku z przyjmowaniem podstawy prawnej przetwarzania danych osobowych (o czym szczegółowo była mowa wyżej), naruszają tym samym przepisy dotyczące oceny skutków i wprowadzają do porządku prawnego przepisy powodujące ryzyka dla administratorów przetwarzających dane i naruszanie praw lub wolności osób fizycznych;
- nie dostrzegają, że niewłaściwa konstrukcja norm prawnych zwiększa ryzyko przetwarzania przez administratorów danych w sposób nieodpowiadający zasadom wynikającym z rozporządzenia czy nakładania obowiązków na podmioty niezgodnie z rolami wyznaczonymi przepisami rozporządzenia 2016/679;
- nie uwzględniają w projektowanych regulacjach prawnych stosowania zasad przetwarzania danych osobowych określonych w RODO, zwłaszcza zasady zgodności z prawem, minimalizacji czy retencji danych;
- nie określają w ogóle albo określają błędnie czy niewyczerpująco role poszczególnych podmiotów i/lub organów biorących udział w procesach przetwarzania danych, w szczególności odpowiednio do celów przetwarzania danych, czy przewidując rozwiązania stanowiące w swej istocie współadministrowanie danymi osobowymi;
- przedstawiają przepisy, które mocą aktów wykonawczych zamiast rangi ustawy, nakładać mają prawa i obowiązki dotyczące przetwarzania danych osobowych;
- przedstawiają przepisy zobowiązujące osoby, których dane dotyczą, do udostępniania danych osobowych przepisami rangi rozporządzenia zamiast przepisami ustawy;
- określają sposoby przekazywania informacji, udostępniania danych i dokumentów zawierających dane osobowe w sposób zbyt ogólny, budzący wątpliwości interpretacyjne;
- niezbyt chętnie – powołując się na ogólne przepisy rozporządzenia 2016/679 i brak szczegółowych wymogów – proponują szczególne rozwiązania zmierzające do realizacji

zasady poufności i integralności sformułowane bardzo ogólnie – przepisy dotyczące zabezpieczania procesów przetwarzania danych osobowych, zwłaszcza w sytuacjach wprowadzania rozwiązań z zakresu nowych technologii;

- pomijają organ właściwy do spraw ochrony danych osobowych w procesie legislacyjnym, którego przedmiotem są przepisy dotyczące danych osobowych, ze szkodą dla jakości tych przepisów, powodując stanowienie przepisów niezgodnych z regulacją ogólnego rozporządzenia o ochronie danych.

Z zadowoleniem należy natomiast przyjąć okoliczności, że:

- niektórzy projektodawcy – przyjmując wcześniejsze wskazówki organu właściwego w sprawie ochrony danych osobowych – wykonują z własnej inicjatywy ocenę wpływu planowanych rozwiązań na ochronę danych, tj. ocenę skutków dla ochrony danych w ramach oceny skutków regulacji, w związku z przyjmowaniem podstawy prawnej przetwarzania danych osobowych, który to proces ułatwia im analizę planowanych rozwiązań, uświadamia potencjalne ryzyka i pozwala przyjąć rozwiązanie zgodne z zasadami dotyczącymi przetwarzania danych bez rezygnacji z zakładanych przepisami celów;
- coraz częściej projektodawcy wykazują zrozumienie, że konstrukcja tworzonych przez nich przepisów dotyczących przetwarzania danych osobowych, zapewniająca stosowanie przepisów rozporządzenia 2016/679, sprzyja nie tylko pozytywnej ocenie organu właściwego w sprawie ochrony danych osobowych, ale przede wszystkim zapewnia wprowadzanie do porządku prawnego regulacji zgodnych z prawem, sformułowanie przepisów jasnych i właściwie określających prawa i obowiązki dla stosujących je wykonawców norm (administratorów), a także gwarantujących prawa osób, których dane dotyczą;
- coraz rzadziej w analizowanych przepisach pojawiają się propozycje projektodawców, co do odbierania zgody na przetwarzanie danych osobowych, którego podstawą są obowiązujące przepisy prawa;
- coraz częściej projektodawcy – uwzględniając zasadę minimalizmu – proponują przetwarzanie danych jedynie w zakresie niezbędnym dla celów regulacji;
- coraz częściej projektodawcy – uwzględniając zasadę ograniczenia celu – wskazują w normach prawnych wyczerpująco cele przetwarzania danych osobowych;
- coraz więcej uwag organu właściwego w sprawie ochrony danych osobowych było analizowanych przez poszczególnych projektodawców pod kątem określenia ról w procesie

przetwarzania danych, co skutkowało wprowadzaniem do projektowanych regulacji rozwiązań zgodnych z RODO. Jako przykład można wskazać wcześniej omawiany projekt **ustawy o zmianie ustawy – Karta Nauczyciela oraz niektórych innych ustaw**[186]**,** gdzie już na etapie prac sejmowych projektodawca zrezygnował z niezgodnych z RODO rozwiązań w zakresie podziału ról w procesach przetwarzania.

Jako przykłady zmian wprowadzonych na skutek opinii Prezesa UODO można wskazać:

- Ustawę o zmianie ustawy o wspieraniu termomodernizacji i remontów oraz ustawy o Inspekcji Ochrony Środowiska[187] – w której w art. 27d ust. 1 doprecyzowano kwestie związane z udostępnieniem danych, wskazując, że dane i informacje zgromadzone w Centralnej Ewidencji Emisyjności Budynków udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, podmiotom wymienionym enumeratywnie w pkt 1-24. Dane tym podmiotom, stosownie do ust. 2, udostępnia się w systemie teleinformatycznym, obsługującym ewidencję w postaci elektronicznej za pomocą środków komunikacji elektronicznej, na zasadach określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- Ustawę o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2021-2027[188] – projektodawca doprecyzował, jakie szczególne kategorie danych osobowych, o których mowa w art. 9 RODO, będą przetwarzane w związku z realizacją zadań wynikających z projektu ustawy (dane dotyczące pochodzenia rasowego lub etnicznego lub zdrowia), nie uzasadnił jednak celu, dla którego przetwarzanie tych konkretnie danych osobowych jest niezbędne;
- Ustawę o kasach zapomogowo-pożyczkowych[189], w której doprecyzowano m.in. katalog przetwarzanych danych osobowych oraz okres ich przechowywania, a także wskazano administratora, który jest odpowiedzialny za przetwarzane dane.

[186] DOL.401.280.2020.
[187] DOL.401.43.2020.
[188] DOL.401.294.2020.
[189] DOL.401.307.2020.

9. Zgłaszanie naruszeń ochrony danych osobowych

Zadaniem Urzędu realizowanym od 25 maja 2018 r. jest przyjmowanie od administratorów zgłoszeń naruszeń ochrony danych osobowych, które stwarzają ryzyko naruszenia praw lub wolności osób fizycznych. 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.

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. Natomiast dostawca publicznie dostępnych usług telekomunikacyjnych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu danych osobowych w terminie nie późniejszym niż 24 godziny od wykrycia naruszenia danych osobowych, zgodnie z art. 174a ust. 1 ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne[190], w zw. z art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej.

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.

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

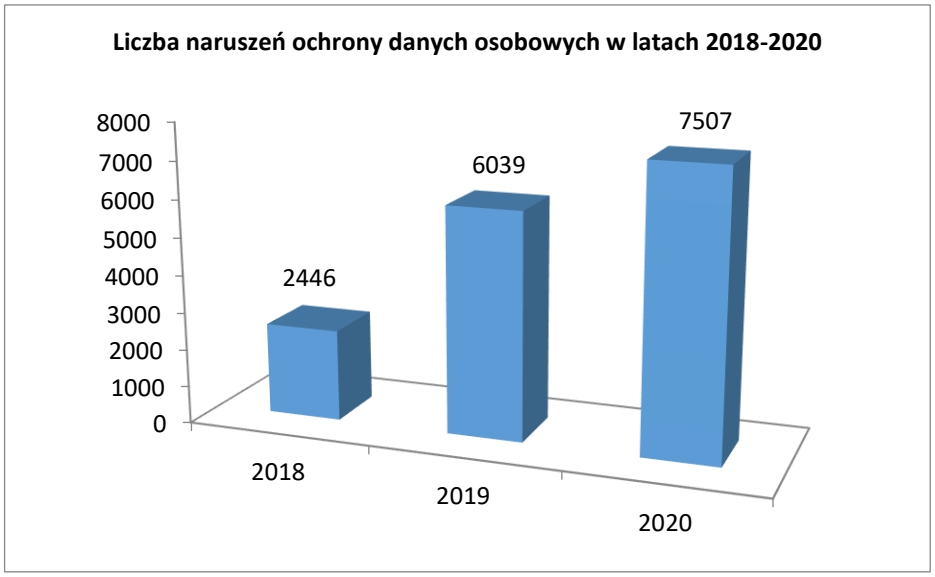
[190] Dz. U. z 2018 r. poz. 1954.

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 rozporządzenia 2016/679. 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 zapewniających ochronę osobom fizycznym i ich danym osobowym, które z jednej strony pozwolą na kontrolę skuteczności dotychczasowych rozwiązań, a z drugiej – ocenę modyfikacji i usprawnień służących zapobieżeniu nieprawidłowościom analogicznym do objętych zgłoszeniem.

9.1. Statystyka zgłaszanych naruszeń ochrony danych osobowych

W 2020 r. Urząd Ochrony Danych Osobowych dokonał analizy **7507 zgłoszeń naruszeń** m.in. pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

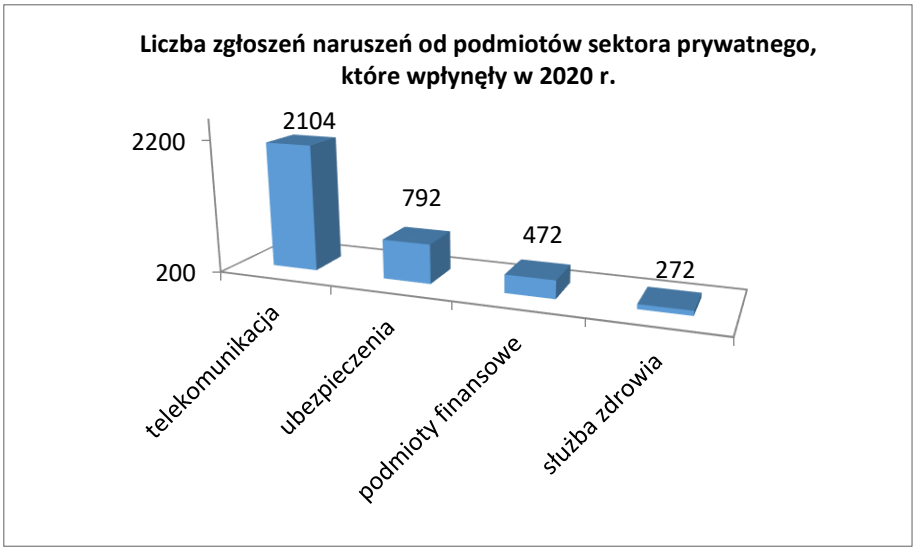
Porównanie liczby zgłoszeń naruszeń ochrony danych osobowych w latach 2018 – 2020 przedstawia poniższy wykres:



Wykres 6: **Liczba przeanalizowanych naruszeń ochrony danych osobowych, które wpłynęły do UODO w latach 2018 – 2020.**

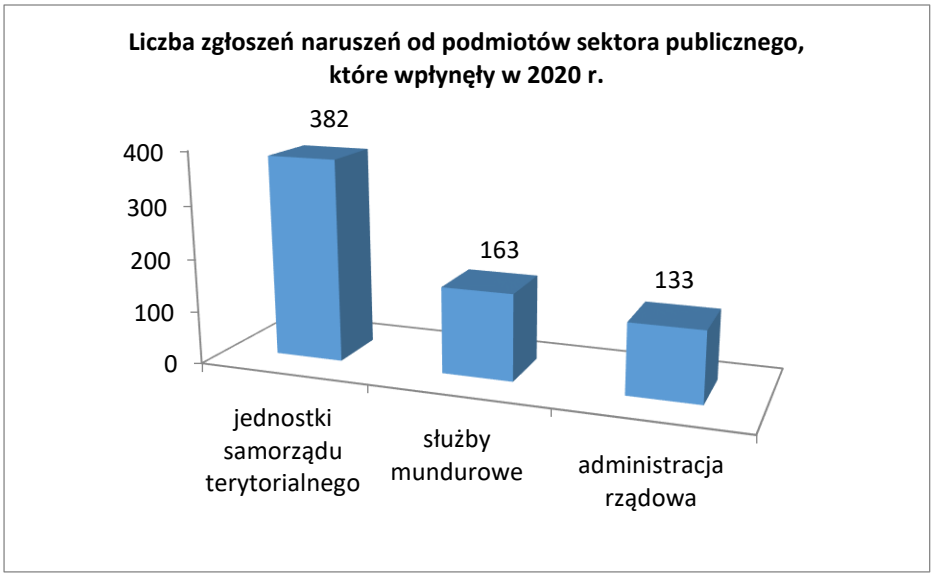
Spośród **7507** zgłoszeń naruszeń, które wpłynęły w 2020 r, **4661 zostało zgłoszonych przez podmioty sektora prywatnego**, **2691 przez podmioty sektora publicznego**, zaś około **155 zgłoszonych w międzynarodowym systemie informatycznym (IMI).**

W przypadku **sektora prywatnego** najwięcej zgłoszeń napłynęło od podmiotów: telekomunikacyjnych – 2104, ubezpieczeniowych – 792, banków i podmiotów finansowych – 472, służby zdrowia – 272.



Wykres 7: **Liczba zgłoszeń naruszeń ochrony danych osobowych od podmiotów prywatnych, które wpłynęły do UODO w latach 2018 – 2020**.

W **sektorze publicznym** zawiadomienia o incydentach z danymi osobowymi najczęściej nadsyłały: jednostki samorządu terytorialnego – 382, służby mundurowe – 163, administracja rządowa – 133.



Wykres 8: **Liczba zgłoszeń naruszeń ochrony danych osobowych od podmiotów publicznych, które wpłynęły do UODO w latach 2018 – 2020.**

Dla porównania w roku 2019 r. Urząd Ochrony Danych Osobowych dokonał analizy 6039 zgłoszeń naruszeń m.in. pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w tym 3894 naruszenia zostały zgłoszone przez podmioty sektora prywatnego, zaś 2145 przez podmioty sektora publicznego.

Wzrost liczby zgłoszeń naruszeń ochrony danych osobowych w 2020 r. wynika z jednej strony z coraz 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 przodowały podmioty prywatne, w szczególności prowadzące działalność w sektorach telekomunikacyjnym, ubezpieczeniowym oraz finansowym. W przypadku podmiotów publicznych najczęściej zgłaszano naruszenia w jednostkach samorządu terytorialnego, służbach mundurowych oraz administracji rządowej.

Poniższa tabela przedstawia liczbę przeanalizowanych naruszeń ochrony danych osobowych w latach 2018-2020.

ROK	Liczba przeanalizowanych naruszeń	Sektor prywatny	Sektor publiczny	Międzynarodowy System Informatyczny - IMI
2018	2446	1882	564	-
2019	6039	3894	2145	69
2020	7507	4661	2691	155

W 2020 r. nastąpił wyraźny wzrost zgłaszanych naruszeń z sektora służb mundurowych. Obowiązek zgłoszenia naruszenia ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, określony w art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, został odmiennie uregulowany przez ustawodawcę i uzależniony od wystąpienia ryzyka niezależnie od poziomu jego wysokości. Zgodnie z art. 44 ww. ustawy obowiązku zgłoszenia nie stosuje się, jeżeli nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych. Natomiast przesłanką zwalniającą administratora danych z obowiązku zgłoszenia naruszenia ochrony danych osobowych, zgodnie z art. 33 ust. 1 rozporządzenia 2016/679, jest małe prawdopodobieństwo, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zwiększona świadomość administratorów przetwarzających dane w związku z zapobieganiem i zwalczaniem przestępczości, co do konieczności zgłaszania naruszeń niezależnie od poziomu występującego ryzyka, niewątpliwie znalazła swoje odzwierciedlenie we wzroście zgłaszanych naruszeń w sektorze służb mundurowych.

9.2. Naruszenia a stan zagrożenia epidemiologicznego

Dodatkowo w roku 2020 r. do Prezesa Urzędu zgłaszano wiele naruszeń związanych z zagrożeniem epidemicznym, które wymogło na administratorach danych niezwłoczne podejmowanie dodatkowych środków w celu ochrony zdrowia osób, których dane dotyczą. To z kolei wiązało się z wystąpieniem incydentów bezpieczeństwa w sferach, które nie były wcześniej poddawane szczegółowej analizie pod kątem wystąpienia możliwych zagrożeń i podatności na zagrożenia.

W placówkach medycznych przyczynami tych naruszeń w szczególności był błąd ludzki, nierzadko będący skutkiem przemęczenia, stresu personelu administratora, a przede wszystkim

olbrzymiej ilości danych osobowych przetwarzanych w związku z walką z pandemią COVID-19. W wielu sytuacjach okazywało się, że procedury opracowane przed rokiem 2020 r., które w standardowych warunkach zapewniały dobre zabezpieczenie danych osobowych przetwarzanych w organizacji administratora, w nowych okolicznościach – światowej pandemii – nie zapewniały już takiej ochrony, np. procedura zakładająca podwójną weryfikację wydawanej dokumentacji nie mogła mieć miejsca w oddziałach szpitalnych przeznaczonych wyłącznie dla chorych na COVID-19. Często do naruszeń dochodziło w wyniku braku jakichkolwiek procedur, czy też rozwiązań tworzonych doraźnie np. wystawienie dokumentacji zawierającej dane osobowe w niestrzeżonym pomieszczeniu, przed wejściem do pomieszczeń administratora np. do rejestracji placówki medycznej. Znaczna liczba naruszeń polegających na omyłkowym wydaniu dokumentacji np. medycznej, wypisów, czy też recept nieuprawionym osobom trzecim, była wynikiem złamania obowiązujących w organizacji procedur, a niekiedy również – odpowiednich regulacji w tych procedurach, dotyczących kwestii prawidłowej weryfikacji tożsamości odbiorców dokumentacji medycznej. Sytuacja epidemiologiczna w Polsce wymusiła na administratorach stosowanie elektronicznych środków komunikacji z osobami, których dane dotyczą. Coraz częściej administratorzy wprowadzali procedury wymagające szyfrowania załączników z danymi osobowymi, wysyłanych do osób, których dane dotyczą, drogą elektroniczną, co w przypadku wielu naruszeń pozwoliło na obniżenie ryzyka zaistniałego naruszenia. Z drugiej strony coraz większa liczba e-rozwiązań skutkowała wzmożoną aktywnością hakerów, co w wielu przypadkach skutkowało atakami złośliwym oprogramowaniem (ransomware). W przypadku ataku na szpitale czy laboratoria, nie mniejszym zagrożeniem niż naruszenie poufności danych, było naruszenie ich dostępności, dlatego też organ nadzorczy nie tylko skupiał się na analizie przyjętych rozwiązań technicznych i organizacyjnych stosowanych w placówkach medycznych, ale również analizował incydenty, w szczególności pod kątem niezakłóconego dostępu administratora do danych osobowych swoich pacjentów. Należy podkreślić, że o ile obecnie wiele podmiotów prowadzi dokumentację w dwóch wersjach, tj. papierowo oraz elektronicznie, co znacząco obniża ryzyko naruszenia praw lub wolności osób fizycznych, niemniej stopniowe przechodzenie służby zdrowia wyłącznie na elektroniczną dokumentację medyczną oraz biorąc pod uwagę skuteczność ataków ransomware, postawiło przed administratorami bardzo ważne zadanie – opracowania i wdrożenia takich rozwiązań technicznych i organizacyjnych, które pozwolą ich organizacjom na niezakłócone wykonywanie zadań związanych ze świadczeniem usług medycznych ogółowi społeczeństwa.

W okresie pandemii dochodziło również do naruszeń ochrony danych osobowych polegających na ujawnieniu danych osób objętych kwarantanną medyczną, które miały kontakt z osobami z pozytywnym wynikiem testu na obecność koronawirusa SARS-CoV-2, osób objętych kwarantanną obowiązkową w związku z przekroczeniem granicy kraju czy też osób, które zostały poddane izolacji domowej ze względu na stwierdzone zakażenie – do tego typu naruszeń dochodziło w szeroko rozumianych podmiotach, które podejmowały działania w celu przeciwdziałania rozszerzeniu się epidemii. Naruszenia te polegały w szczególności na wysłaniu niewłaściwemu odbiorcy niezabezpieczonej korespondencji e-mail zawierającej wykaz osób objętych dochodzeniem epidemiologicznym lub upublicznieniu listy osób przebywających na kwarantannie poprzez wywieszenie jej w siedzibie administratora, czy upublicznieniu listy takich osób na portalach społecznościowych. Wyjaśniając powody naruszeń administratorzy często wskazywali na błędy pracowników związane ze znacznym obciążeniem pracą lub konieczność upublicznienia listy w celu zachowania bezpieczeństwa członków Zespołu Ratownictwa Medycznego, którzy mogli zastosować środki ochrony osobistej przy wyjazdach do osób objętych kwarantanną. Ponadto niektórzy administratorzy zajmowali stanowisko, że dane dotyczące adresu, pod którym przebywała osoba objęta kwarantanną, nie stanowią danych osobowych. Z tym stanowiskiem Prezes Urzędu nie mógł się zgodzić, ponieważ kategorie ujawnionych danych wypełniały przesłanki uznania przetwarzanych informacji za dane osobowe. Ponadto zdarzały się przypadki, że osoby, których dane osobowe ujawniono, zostały zidentyfikowane przez osoby postronne i z tego tytułu doznały niedogodności. W dwóch naruszeniach polegających na ujawnieniu danych ww. osób, Prezes Urzędu – po przeprowadzeniu postępowania administracyjnego – zdecydował się udzielić upomnienia administratorom oraz nakazać zawiadomienie o naruszeniu te osoby, których ono dotyczyło[191].

9.3. Najczęściej zgłaszane oraz typowe naruszenia w 2020 r.

Podobnie jak w latach ubiegłych do najczęściej zgłaszanych przez administratorów danych naruszeń ochrony danych osobowych należały:

a) **wysłanie korespondencji zawierającej dane osobowe zarówno w formie tradycyjnej, jak i na elektroniczną skrzynkę pocztową e-mail do niewłaściwego odbiorcy** – do tego typu incydentów najczęściej dochodziło w skutek błędu pracownika administratora danych odpowiedzialnego za przygotowanie i wysyłkę korespondencji. Źródło nieprawidłowości powstawało również na etapie gromadzenia danych, gdzie potencjalny odbiorca

[191] Sygnatura akt: DKN5131.1.2020, DKN.5101.25.2020.

nieprawidłowo wskazywał swój adres korespondencyjny. Administratorzy danych, aby zmniejszyć prawdopodobieństwo wystąpienia tego typu naruszeń w przyszłości, wdrażali środki bezpieczeństwa w postaci m.in. szyfrowania przesyłanej korespondencji, uniemożliwiającej dostęp do danych osobom nieuprawnionym, stosowali dodatkową weryfikację adresu korespondencyjnego w momencie gromadzenia danych, polegającą m.in. na konieczności przeliterowania adresu (w przypadku gromadzenia danych przez telefon) lub poprzez wymuszenie ponownego wpisania adresu e-mail w formularzach;

b) **ujawnienie danych niewłaściwej osobie –** do tego typu naruszeń najczęściej dochodziło poprzez wydanie dokumentów osobie, dla której nie były przeznaczone np. zaświadczeń czy deklaracji podatkowych. Administratorzy, w celu ograniczenia tego typu naruszeń w przyszłości, podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia czy instruktarze; dokonywali przeglądu obowiązujących procedur, dodatkowo zwracano się do osób nieuprawnionych o zwrot dokumentów lub ich trwałe zniszczenie;

c) **nieuprawnione uzyskanie dostępu do informacji** – w tym typie naruszeń do incydentów bezpieczeństwa najczęściej dochodziło poprzez: błędy programistyczne ujawniające się po wprowadzeniu aktualizacji danego oprogramowania, brak wewnętrznych testów bezpieczeństwa, które mogły wykazać podatność systemu, czy nieprawidłowe nadanie uprawnień w systemach informatycznych, czego skutkiem było zapoznanie się z danymi osobowymi przez osoby do tego nieuprawnione. Administratorzy podejmowali działania polegające na przeprowadzeniu dodatkowych testów systemów informatycznych w środowisku developerskim oraz przeprowadzali analizę nadanych uprawnień, ograniczając nadane uprawnienia do takich, które są niezbędne dla wykonywania obowiązków służbowych użytkowników;

d) **korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem do nadawcy** – w przypadku tego typu incydentów, najczęściej do naruszeń dochodziło w wyniku działań operatora pocztowego. Zagrożenie epidemiczne wymogło na administratorach podejmowanie nietypowych działań w celu ochrony zdrowia pracowników – niejednokrotnie odbierana od operatora pocztowego korespondencja była w pierwszej kolejności kierowana do przechowania w „kwarantannie", a po okresie kwarantanny następował formalny proces przyjęcia korespondencji, w którym dopiero następowało ujawnienie nieprawidłowości w postaci otwartej lub zniszczonej koperty. Co więcej, brak

weryfikacji korespondencji w momencie odbioru, uniemożliwiał ustalenie, na jakim etapie doszło do naruszenia poufności danych zawartych w korespondencji oraz złożenie skutecznej reklamacji do operatora pocztowego. Administratorzy, aby zapobiec tego typu naruszeniom w przyszłości, dokonywali aktualizacji instrukcji kancelaryjnej, składali reklamację do operatora pocztowego, podejmowali działania zmierzające do zmiany postanowień umownych zawartych z operatorem, zwracali się do operatora pocztowego o wyjaśnienia w szczególności, jakie środki zostały przez niego zastosowane w celu zmniejszenia prawdopodobieństwa wystąpienia naruszenia w przyszłości;

e) **dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji** – do tego typu naruszeń najczęściej dochodziło w wyniku niefrasobliwości pracowników, którzy wynosząc dokumenty poza zakład pracy pozostawiali je w miejscach publicznych. Również sami administratorzy w związku z zagrożeniem epidemicznym stosowali nieprawidłowe rozwiązania, polegające na gromadzeniu danych, np. poprzez wystawienie kartonowych pudeł z przeznaczeniem na dane osobowe przed budynkiem administratora lub w pomieszczeniach dostępnych dla wszystkich osób. W celu obniżenia prawdopodobieństwa wystąpienia tego typu naruszeń w przyszłości, administratorzy danych podejmowali działania podnoszące świadomość pracowników w zakresie zapewnienia bezpieczeństwa powierzonych dokumentów, upominali osoby odpowiedzialne za wystąpienie naruszenia, dokonywali przeglądu obowiązujących procedur regulujących sytuacje i warunki dopuszczalnego przetwarzania danych osobowych utrwalonych w dokumentacji papierowej lub na innych, przenośnych nośnikach danych, poza siedzibą lub obszarem pomieszczeń zajmowanych przez administratora danych, zgłaszali kradzież organom ścigania;

f) **niezamierzona publikacja lub nieprawidłowa anonimizacja danych w dokumencie** – do tego typu naruszeń należy zaliczyć publikację danych osobowych na stronie internetowej administratora, jak również udostępnienie w trybie dostępu do informacji publicznej, w tym w Biuletynie Informacji Publicznej, danych nieadekwatnych, nadmiarowych. W tych przypadkach powodem powstania naruszenia była najczęściej nieprawidłowa anonimizacja danych lub przeoczenie tego błędu przez pracowników udostępniających materiały i 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, a w przypadku publikacji

danych na stronie internetowej, w ramach działań naprawczych administratorzy usuwali treści ze swoich witryn internetowych;

g) **zgubienie lub kradzież nośnika danych / urządzenia umożliwiającego dostęp do danych** – do tego typu naruszeń najczęściej dochodziło w wyniku kradzieży komputera przenośnego lub zgubienia niezaszyfrowanego elektronicznego nośnika danych typu „pendrive". W celu zminimalizowania prawdopodobieństwa wystąpienia tego typu naruszeń w przyszłości, administratorzy danych decydowali się zastosować środki bezpieczeństwa w postaci szyfrowania elektronicznych nośników danych, uniemożliwiającego dostęp do danych osobom nieuprawnionym; dokonywali weryfikacji przestrzegania przez pracowników zasady ograniczonego (w aspekcie czasowym i zakresowym) przechowywania; wprowadzali rozwiązania umożliwiające zdalne usuwanie danych osobowych ze stacji roboczych znajdujących się poza siedzibą administratora, decydowali się na przechowanie danych „w chmurze", zwiększali świadomość pracowników w zakresie konieczności zapewnienia bezpieczeństwa powierzonym im elektronicznym nośnikom danych, zgłaszali kradzież organom ścigania;

h) **złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych oraz nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń –** do tych typów naruszeń najczęściej dochodziło w wyniku wykorzystania wyspecjalizowanych umiejętności osób prowadzących tego typu ataki oraz wykorzystania podatności atakowanych systemów. Niejednokrotnie przyczyniali się do tego sami administratorzy, wykorzystując do przetwarzania danych nieaktualne oprogramowanie, dla którego producent przestał zapewniać wsparcie techniczne. W celu zaradzenia naruszeniu administratorzy przywracali dane z kopii zapasowych, a w przypadku braku podejmowali decyzję o ich tworzeniu, korzystali ze wsparcia wyspecjalizowanych podmiotów dokonujących próby odszyfrowania danych, przeprowadzali dodatkowe testy bezpieczeństwa, decydowali się na zakup najnowszego oprogramowania antywirusowego oraz oprogramowania typu „firewall", dokonywali przeglądu oraz zmiany procedur w zakresie stosowania wymogu regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania, zgłaszali naruszenie organom ścigania oraz Zespołowi CERT Polska;

i) **ujawnienie danych związane ze zdalnym nauczaniem i pracą zdalną** – naruszenia polegały na nieuprawnionym upublicznieniu wizerunku uczniów oraz nauczycieli przez samych

uczniów lub osoby postronne. Do tego typu naruszeń możemy również zaliczyć udostępnienie nagrań, zawierających dane osobowe, osobom nieuprawnionym. W dobie pandemii popularność zyskała praca zdalna, która z jednej strony chroniła zdrowie pracowników, z drugiej zaś umożliwiała administratorom zapewnienie niezakłóconego funkcjonowania ich organizacjom. Organ nadzorczy odnotował naruszenia dotyczące pracy zdalnej, gdzie przyczyną wystąpienia naruszeń był przede wszystkim brak odpowiednich procedur dotyczących bezpiecznego przetwarzania danych w trakcie pracy zdalnej. Większość naruszeń tego typu dotyczyło placówek oświatowych, gdzie bezpośrednią przyczyną wystąpienia naruszeń były takie zdarzenia jak, np. udostępnianie przez uczniów loginów i haseł do lekcji online osobom trzecim, czy też nieumiejętne wykorzystywanie narzędzi do pracy zdalnej, w wyniku czego osoby postronne po zakończeniu spotkania (brak wylogowania się prowadzącego z platformy) miały możliwość zapoznania się z danymi osobowymi dotyczącymi konkretnych pracowników. Administratorzy danych, aby zapobiec wystąpieniu podobnych naruszeń w przyszłości, decydowali się przekazywać narzędzia do logowania tuż przed zajęciami (w celu utrudnienia przekazywania loginu i haseł osobom postronnym), przeprowadzali audyt stosowanych narzędzi do zdalnej nauki, zwracali nauczycielom uwagę na niebezpieczeństwo ingerencji osób trzecich w prowadzone zajęcia, czy informowali rodziców o konsekwencjach działań.

9.4. Wyjaśnienia

Korzystając m.in. z uprawnień określonych w art. 58 ust. 1 lit. a i lit. e rozporządzenia 2016/679, polegających na nakazaniu m.in. administratorowi i podmiotowi przetwarzającemu, dostarczenia wszelkich informacji oraz uzyskaniu dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań, Prezes Urzędu wystosował do podmiotów dokonujących zgłoszenia **3476 pisemnych wezwań do złożenia wyjaśnień** lub udzielił pisemnych informacji w związku z przypadkami naruszeń ochrony danych osobowych. Wątpliwości Prezesa Urzędu budziły zwłaszcza zastosowane lub proponowane przez administratorów środki bezpieczeństwa w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia, środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą, nieprawidłowe oszacowanie poziomu ryzyka naruszenia praw lub wolności osób fizycznych, termin dokonanego zgłoszenia oraz wyjaśnienia przyczyn opóźnienia powiadomienia organu nadzorczego o naruszeniu, dochowanie obowiązku

zawiadomienia osób, których dane dotyczą oraz wskazane przez administratorów kategorie i liczba osób oraz danych objętych naruszeniem. W zdecydowanej większości reakcją na wezwania były działania służące zagwarantowaniu odpowiedniego poziomu bezpieczeństwa danych i zminimalizowaniu ryzyka ich przetwarzania w sposób niezgodny z przepisami prawa oraz udzielenie organowi oczekiwanych wyjaśnień i informacji.

Analiza przebiegu obsługi zgłoszeń naruszenia ochrony danych osobowych prowadzi do wniosku, że realizacja kompetencji organu nadzorczego w trybie art. 58 ust. 1 lit. a i lit. e rozporządzenia 2016/679, pozytywnie wpływa na ochronę danych osobowych. Znacznie skraca bowiem proces przywrócenia stanu zgodnego z prawem, pozwalając organowi nadzorczemu na natychmiastowe działanie bez konieczności wcześniejszego wszczynania postępowania administracyjnego, które ze względu m.in. na zasadę pisemności, cechuje się znacznym formalizmem. Podkreślić należy, że cel, jakiemu służy obowiązek zgłaszania naruszeń ochrony danych osobowych i ich kontroli ze strony organu nadzorczego (tj. poprawa bezpieczeństwa danych osiągana również na drodze reagowania na niepożądane incydenty w tym obszarze) wymagała wyposażenia Prezesa Urzędu w instrumenty prawne pozwalające na możliwie najszybszą reakcję na zgłoszenia naruszenia ochrony danych osobowych tak, aby w jak najszybszym czasie osoby, których dane dotyczą mogły podjąć działania mające na celu zabezpieczenie się przed ewentualnymi konsekwencjami naruszenia, czy niezwłocznym zastosowaniu środków bezpieczeństwa w celu ograniczenia rozmiaru naruszenia i w konsekwencji wyrządzonych szkód.

9.5. Sygnaliści

W 2020 r. Prezes Urzędu został poinformowany w **224 przypadkach o zdarzeniach naruszających bezpieczeństwo danych przez podmioty inne niż administratorzy danych**. Często były to osoby, których dotyczyło naruszenie danych osobowych lub osoby, które w sposób niezamierzony weszły w posiadanie danych dla nich nieprzeznaczonych. Zdarzały się przypadki, w których na podstawie sygnałów uzyskanych w powyższy sposób Prezes Urzędu ustalił, że administrator danych, mimo świadomości wystąpienia naruszenia, nie poinformował o tym organu nadzorczego. Najczęściej brak dokonania zgłoszenia wynikał z błędnie ocenionego przez administratora danych poziomu ryzyka naruszenia praw lub wolności osoby fizycznej, od którego uzależniony jest obowiązek dokonania zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu. Przyczyny niezgłoszenia niektórych incydentów znajdowały również swoje źródło w braku odpowiedniego wdrożenia wewnętrznych procedur w zakresie identyfikowania naruszeń

i postępowania w przypadkach naruszenia bezpieczeństwa danych, czy braku świadomości pracowników co do zdarzeń naruszających bezpieczeństwo danych w kontekście konieczności zgłoszenia takiego zdarzenia przełożonym. Natomiast świadome i celowe podjęcie decyzji o zaniechaniu zgłoszenia naruszenia ochrony danych osobowych w obawie przed ewentualnymi konsekwencjami są szczególnie naganne i takie zachowania były oraz będą przedmiotem szczególnej analizy Prezesa Urzędu.

9.6. Postępowania administracyjne

W 2020 r. Prezes Urzędu wszczął z urzędu **28 postępowań administracyjnych w sprawie naruszenia przepisów o ochronie danych osobowych w związku z przypadkami naruszenia ochrony danych osobowych.** W przypadku niektórych naruszeń ochrony danych osobowych podjęta została decyzja o przeprowadzeniu u administratora danych kontroli przestrzegania przepisów o ochronie danych.

Wątpliwości Prezesa Urzędu w związku ze zgłoszonymi naruszeniami ochrony danych osobowych, wymagające przeprowadzenia postępowania administracyjnego, dotyczyły w szczególności:

a) przeprowadzonej przez administratorów danych oceny ryzyka naruszenia dla praw lub wolności osób fizycznych, skutkującej koniecznością zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia osób, których naruszenie dotyczyło;
b) terminowości dokonania zgłoszenia zgodnie z art. 33 ust 1 rozporządzenia 2016/679. Podkreślić należy, że analiza organu obejmuje również okres, jaki upłynął od momentu zaistnienia zdarzenia w obszarze naruszenia ochrony danych do momentu wskazanego przez administratora danych jako data stwierdzenia naruszenia – nieadekwatnie długi odstęp pomiędzy tymi zdarzeniami może skutkować co najmniej pytaniem o istnienie i prawidłowość procedur identyfikacji i oceny takich zdarzeń w kontekście obowiązków statuowanych w art. 33 i 34 rozporządzenia 2016/679, ale również może skutkować podejrzeniem celowego manipulowania okolicznościami zdarzenia, np. w celu stworzenia pozorów dokonania zgłoszenia w wymaganym przepisami terminie;
c) zawarcia umowy powierzenia, w tym zgodności zawartej umowy powierzenia z przepisami o ochronie danych osobowych, zakresu odpowiedzialności stron tej umowy, uwzględniając kryteria zawarte w art. 28 ust 3 rozporządzenia 2016/679 oraz sposobu ustalenia/zapewnienia gwarancji wdrożenia odpowiednich środków technicznych

i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą;

d) wdrożenia przez administratorów danych odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych, a w szczególności: zapewniających zdolność do ciągłego zapewnienia poufności usług przetwarzania oraz wymogu regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, o którym mowa w art. 32 ust. 1 lit. d rozporządzenia 2016/679.

W ocenie Prezesa Urzędu brak regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych miało istotny wpływ na błędne oszacowanie poziomu ryzyka i uniemożliwiło zastosowanie odpowiednich środków bezpieczeństwa dla wykorzystywanego zasobu. Doprowadziło to do zaniedbania i zwiększyło prawdopodobieństwo zmaterializowania się zagrożenia w postaci m.in. ataku złośliwego oprogramowania i nieuprawnionego dostępu do danych, poprzez przełamanie zabezpieczeń systemów informatycznych. Niejednokrotnie efektem powyższego było zmaterializowanie się ryzyka, które w ocenie administratora danych posiadało niski stopień prawdopodobieństwa.

9.7. Decyzje administracyjne

W odniesieniu do zgłoszeń naruszeń ochrony danych osobowych w 2020 roku, w postępowaniu administracyjnym, wydano **13 decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych.** W trzech decyzjach Prezes Urzędu udzielił upomnienia administratorowi danych, w sześciu – nakazał zawiadomienie o naruszeniu osób, których dane dotyczą, zaś w czterech – postępowanie administracyjne w części lub całości zostało umorzone. W przypadku dwóch naruszeń Prezes Urzędu po przeprowadzeniu postępowania administracyjnego, w wydanej decyzji administracyjnej zdecydował się nałożyć na administratora danych administracyjną karę pieniężną[192].

Niezależnie od zadań związanych z przyjmowaniem od administratorów zgłoszeń naruszeń ochrony danych osobowych, UODO w 2020 r. prowadził również postępowanie administracyjne[193]

[192] Decyzje te dotyczyły: Towarzystwa Ubezpieczeń i Reasekuracji Warta S.A. (DKN.5131.5.2020) oraz ID Finance Poland Sp. z o.o. w likwidacji (DKN.5130.1354.2020).
[193] Sygnatura akt ZWAD.405.31.331.2019.

w sprawie niewłaściwej realizacji przez jeden ze szpitali obowiązków określonych w art. 38 ust. 6 rozporządzenia 2016/679, poprzez zobowiązanie inspektorów ochrony danych do nadawania upoważnień personelowi w zakresie przetwarzania danych osobowych. **Organ nadzoru o nieprawidłowościach został poinformowany przez podmiot, który nie był administratorem danych.** Przedmiotowa informacja oraz złożone przez szpital wyjaśnienia dotyczące przyjętych rozwiązań w zakresie zapewnienia IOD skutecznego wykonywania zadań, stanowiły podstawę wystarczającą do wszczęcia z urzędu postępowania administracyjnego w sprawie naruszenia przez szpital przepisów o ochronie danych osobowych w rozumieniu rozporządzenia 2016/679.

W wydanej decyzji wskazano na niewłaściwą realizację przez szpital obowiązku określonego w art. 38 ust. 6 rozporządzenia 2016/679, poprzez zobowiązanie IOD do nadawania upoważnień personelowi w zakresie przetwarzania danych osobowych, udzielając upomnienia za czas, w którym naruszenie ww. przepisu prawa było przez szpital kontynuowane. W decyzji wykazano administratorowi, że z uwagi na specyfikę zadań IOD ogniskujących się na doradzaniu oraz kontrolowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, administrator nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych, pozostawiając IOD w procedurze wydawania tych upoważnień sprawowanie funkcji doradczej i nadzorczej. W ocenie organu nadzorczego przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za przeprowadzenie tej procedury, a jednocześnie miałby monitorować jej zgodność z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b) rozporządzenia 2016/679, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 rozporządzenia 2016/679. Podkreślono, iż nakładanie na IOD obowiązków prowadzących do powstania konfliktu interesów stawia pod znakiem zapytania nie tylko możliwość efektywnego wypełniania przez niego zadań, do realizacji których zobowiązuje go dyspozycja normy art. 39 rozporządzenia 2016/679, ale godzi w same fundamenty instytucji IOD, opartej w pierwszym rzędzie na niezależności jego funkcjonowania.

W decyzji wskazano również, że przywrócenie zgodności przyjętych przez szpital polityk ochrony danych osobowych z obowiązującym stanem prawnym, było dopiero wynikiem postępowań przeprowadzonych przez organ nadzorczy, a zgromadzony w przedmiotowej sprawie materiał dowodowy w sposób niepodważalny wskazywał na ponad roczny stan istnienia naruszenia prawa.

Niemniej Prezes Urzędu, realizując swoje uprawnienie na mocy art. 58 ust. 2 lit. b) rozporządzenia 2016/679, uznał, że cel przedmiotowego postępowania administracyjnego, jakim jest przywrócenie stanu zgodnego z prawem, może być jednak osiągnięty poprzez zastosowanie środka o charakterze mniej dolegliwym, a upomnienie szpitala za błędną realizację obowiązków spoczywających na nim, jako administratorze danych w rozumieniu art. 4 ust. 7 rozporządzenia 2016/679, stanowi właściwy przejaw realizacji zasady proporcjonalności.

Jednocześnie nie znajdując podstaw do uznania, że doszło do naruszenia przepisów o ochronie danych osobowych, tj. art. 29 i art. 32 ust. 1 i 4 w związku z art. 38 ust. 2 i 3 oraz art. 39 rozporządzenia 2016/679, postępowanie administracyjne zostało umorzone.

9.8. Działalność informacyjno-edukacyjna w sprawach naruszeń

Na stronie internetowej UODO opublikowane zostały obszerne wskazówki dotyczące naruszeń ochrony danych pod tytułem „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych”[194]. W poradniku tym znalazły się między innymi informacje dotyczące pojęcia naruszenia ochrony danych osobowych, wskazówki, 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 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 działaniem infolinii w UODO, na bieżąco aktualizowane na stronie internetowej UODO informacje w zakładce „Administrator”[195], dotyczące obowiązków administratorów w związku z naruszeniami ochrony

[194] https://uodo.gov.pl/pl/134/1029
[195] https://uodo.gov.pl/pl/p/najwazniejsze-tematy/administrator

danych osobowych oraz w zakładce „Inspektor Ochrony Danych”[196], a także wydawanie newslettera dla IOD[197].

10. Administracyjne kary pieniężne

Administracyjna kara pieniężna jako środek naprawczy przymuszający do wykonania nakazu decyzji administracyjnej Prezesa UODO

Faktem wartym odnotowania jest, że w 2020 r. Prezes UODO po raz pierwszy wszczął z urzędu postępowanie w sprawie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazu wydanej przez siebie decyzji, tj. zastosował przepis art. 83 ust. 6 RODO. W 2020 roku wszczęte zostały **2** postępowania w takich sprawach. Oba przypadki charakteryzowały się rażącym lekceważeniem przez zobowiązanych obowiązków nałożonych na nich nakazami decyzji administracyjnych. Nakazy organu nadzorczego to środki naprawcze, które służą przywróceniu stanu zgodnego z prawem i są elementem systemu ochrony danych osobowych. Należy podkreślić, że są one odpowiedzią na stan naruszenia jednego z podstawowych praw osoby fizycznej, jakim jest prawo do ochrony jej danych czy też szerzej – do ochrony jej prywatności. Dlatego też Prezes UODO, jako organ nadzorczy odpowiadający za monitorowanie przestrzegania przepisów o ochronie danych osobowych, nie mógł pozwolić na ignorowanie wydawanych przez siebie orzeczeń i dlatego zdecydował się na skorzystanie ze swojego uprawnienia do wszczęcia postępowań w sprawie nałożenia kary w tym zakresie.

Jedno z omawianych postępowań[198] toczyło się wobec przedsiębiorcy prowadzącego działalność z zakresu ochrony zdrowia, któremu Prezes UODO nakazał zawiadomienie jego pacjentów o naruszeniu ich danych osobowych oraz przekazanie tym osobom zaleceń dotyczących zminimalizowania potencjalnych negatywnych skutków zaistniałego incydentu. Gdy przeprowadzone postępowanie sprawdzające wykazało, że przedsiębiorca nie wykonał nakazu decyzji, Prezes UODO zdecydował o wszczęciu z urzędu postępowania w sprawie nałożenia na niego administracyjnej kary pieniężnej. Należy podkreślić, że przedsiębiorca nawet na etapie postępowania w sprawie nałożenia kary nie przedstawił kompletnych dowodów, które pozwoliłyby uznać, że

[196] https://uodo.gov.pl/pl/p/najwazniejsze-tematy/administrator
[197] Dostępny pod adresem: https://news.uodo.gov.pl/lists/. Teraz Inspektorzy Ochrony Danych 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.
[198] DKE.561.11.2020.

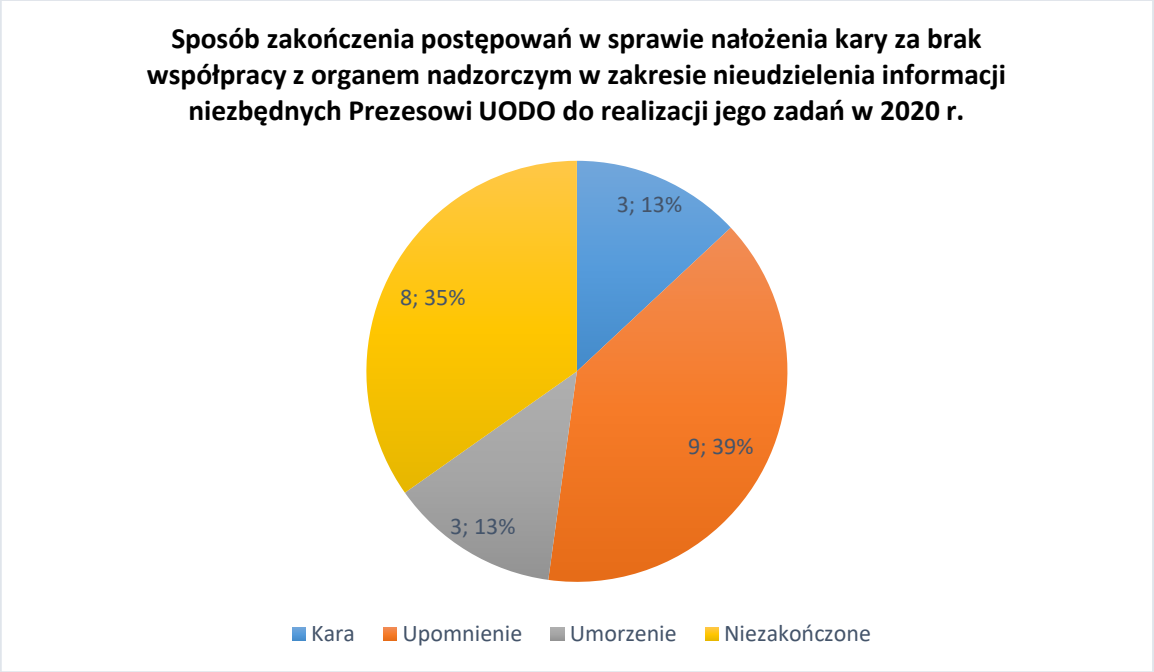
obowiązek wynikający z nakazu decyzji został przez niego wykonany, mimo udzielania mu przez Urząd szczegółowych wskazówek, m.in. dotyczących prawidłowego sformułowania zawiadomień i formy ich przekazania pacjentom. Dlatego też Prezes Urzędu Ochrony Danych Osobowych zdecydował o nałożeniu na tego przedsiębiorcę administracyjnej kary pieniężnej w kwocie ponad **85 588 zł** (20 000 EUR). Decyzja nakładająca tę karę została wydana na początku 2021 roku, więc nie może zostać ujęta w niniejszym okresie sprawozdawczym, jednak fakt jej nałożenia ma duże znaczenie z punktu widzenia zasadności działań Prezesa UODO, bowiem przedsiębiorca wykonał nakaz decyzji dopiero po nałożeniu na niego kary. Uznać zatem należy, że zastosowany przez organ nadzorczy środek naprawczy w postaci administracyjnej kary pieniężnej okazał się skuteczny. Drugie z prowadzonych postępowań w tym zakresie nie zostało zakończone w momencie sporządzania niniejszego sprawozdania.

Uchylanie się od obowiązku współpracy z organem nadzorczym i niezapewnienie dostępu do informacji niezbędnych do realizacji jego zadań

Brak współpracy z Prezesem Urzędu Ochrony Danych, poprzez nieudzielanie odpowiedzi na jego pisma, to poważny i dosyć częsty problem, z którym zmaga się UODO podczas wykonywania swoich zadań. Dlatego też kolejnym *novum* w działaniach podejmowanych przez Prezesa Urzędu w 2020 roku było wszczynanie postępowań w sprawie nałożenia kary za brak współpracy z organem nadzorczym i nieudzielenie dostępu do informacji niezbędnych organowi nadzorczemu do realizacji jego zadań, tj. naruszenie przepisów art. 31 oraz 58 ust. 1 RODO. Wspomniane naruszenia polegały na nieudzielaniu odpowiedzi na wezwania do złożenia wyjaśnień w prowadzonych postępowaniach, bądź na udzielaniu odpowiedzi niepełnych. Zachowania takie należy ocenić nagannie. Wydłużają one postępowania prowadzone w sprawach, a czasem nawet uniemożliwiają ich zakończenie. Nie oznacza to, że Prezes Urzędu sięgał po ten najbardziej represyjny środek naprawczy w każdym przypadku, gdy nie otrzymał w terminie odpowiedzi na swoje wezwanie do złożenia wyjaśnień, bądź gdy nie satysfakcjonowała go odpowiedź na pismo udzielona przez administratora. Każde naruszenie, które było powodem wszczęcia postępowania w omawianym zakresie nie było zdarzeniem incydentalnym, lecz długotrwałym i w każdym przypadku stało za nim przeświadczenie Urzędu o braku woli współpracy ze strony wzywanego podmiotu.

W omawianym okresie sprawozdawczym Prezes UODO **wszczął z urzędu 23 postępowania** w sprawie nałożenia kary za brak współpracy z organem nadzorczym poprzez nieudzielenie mu informacji niezbędnych do realizacji jego zadań. Decyzjami **nakładającymi administracyjne kary**

pieniężne w 2020 r. zakończyły się 3 z nich, z czego **2** decyzje stały się prawomocne z uwagi na niewniesienie skarg do Wojewódzkiego Sądu Administracyjnego, zaś pozostała **1** decyzja na skutek wniesionej skargi podlega kontroli sądowej – jednak w roku 2020 nie zapadło prawomocne orzeczenie sądu w jej przedmiocie. W **9** przypadkach, po wszczęciu postępowań, strony zaczęły współpracować z Prezesem Urzędu, tj. udzieliły wyczerpujących wyjaśnień bądź wyjaśniły przyczyny ich braku, co spowodowało podjęcie przez Prezesa UODO decyzji o nienakładaniu kar i **poprzestaniu na udzieleniu im upomnień**. Prowadzone postępowania w **3** sprawach nie potwierdziły, że doszło do naruszenia obowiązku współpracy z organem nadzorczym, w związku z tym postępowania te zostały umorzone. Pozostałe postępowania nie zostały zakończone w 2020 r.



Wykres 9: **Procentowe zestawienie sposobu zakończenia postępowań w sprawie nałożenia kary za brak współpracy w związku z nieudzieleniem informacji Prezesowi UODO niezbędnych do realizacji jego zadań w 2020 r.**

Wysokość administracyjnych kar pieniężnych nałożonych za brak współpracy w związku z nieudzieleniem informacji niezbędnych Prezesowi UODO do realizacji jego zadań w 2020 r.:

1. East Power Sp. z o.o. – **15 000 zł** (3 505,16 EUR),
2. Przedsiębiorca prowadzący przedszkole – **5 000 zł** (1 168,39 EUR),
3. Smart Cities Sp. z o.o. – **12 838,20 zł** (3 000 EUR).

Pierwsze z postępowań[199], wszczętych w przedmiocie nałożenia kary za nieudzielenie dostępu do informacji niezbędnych Prezesowi UODO do realizacji jego zadań, zostało wszczęte wobec spółki **East Power Sp. z o.o. z siedzibą w Jeleniej Górze**, która zajmuje się na terenie Polski i Niemiec pośrednictwem pracy. Skargę na działania tej spółki złożył obywatel Niemiec (w związku z przetwarzaniem jego danych w celach marketingowych) w niemieckim organie ochrony danych osobowych właściwym dla Nadrenii-Palatynatu, ale została ona przyjęta do rozpoznania przez Prezesa UODO, który był w tej sprawie wiodącym organem nadzorczym z uwagi na to, że spółka ma siedzibę w Polsce. W toku postępowania spółka nie wywiązywała się z obowiązku zapewnienia organowi dostępu do danych osobowych i innych informacji niezbędnych do realizacji zadań związanych z rozpatrzeniem skargi – na niektóre pisma Prezesa UODO nie odpowiadała, a na inne udzielała wyjaśnień, które były niepełne i wewnętrznie sprzeczne. Swoim działaniem spółka uniemożliwiała rozpatrzenie skargi obywatela Niemiec i wydanie przez Prezesa UODO decyzji rozstrzygającej sprawę. Postępowanie zakończyło się dla spółki nałożeniem kary w wysokości **15 000 zł**. Istotnym w tej sprawie jest fakt, że ukarana spółka złożyła skargę na decyzję nakładającą karę do Wojewódzkiego Sądu Administracyjnego w Warszawie, który to **Sąd oddalił skargę spółki uznając, że administracyjna kara pieniężna nałożona została zasadnie**.

Brak współpracy z Prezesem UODO w trakcie przeprowadzania kontroli

Brak współpracy z Prezesem UODO może również przybrać formę niezapewnienia dostępu do pomieszczeń administratora lub podmiotu przetwarzającego, w tym sprzętu i środków służących do przetwarzania danych podczas przeprowadzania czynności kontrolnych.

W omawianym okresie sprawozdawczym Prezes UODO wszczął **2** postępowania dotyczące utrudniania czynności kontrolnych.

Jedna z tych spraw dotyczyła postępowania[200] w sprawie nałożenia kary na **Głównego Geodetę Kraju** (GGK) za naruszenie polegające na niezapewnieniu Prezesowi UODO, w trakcie kontroli przestrzegania przepisów o ochronie danych osobowych, dostępu do pomieszczeń, sprzętu i środków służących do przetwarzania danych osobowych oraz dostępu do danych osobowych i informacji niezbędnych Prezesowi UODO do realizacji jego zadań, a także na braku współpracy z Prezesem Urzędu w trakcie tej kontroli. W efekcie postępowania Prezes UODO **nałożył na Głównego Geodetę Kraju administracyjną karę pieniężną w wysokości 100 000 zł**.

[199] DKE.561.1.2020.
[200] DKE.561.3.2020.

Prowadzone postępowanie dotyczyło sytuacji z marca 2020 r., kiedy to Prezes UODO zdecydował o konieczności przeprowadzenia kontroli przetwarzania przez Głównego Geodetę Kraju na portalu GEOPORTAL2 danych osobowych pochodzących z powiatowych ewidencji gruntów i budynków, o czym poinformował go pismem, w którym wskazał zakres kontroli oraz termin jej przeprowadzenia. W celu przeprowadzenia czynności kontrolnych kontrolujący, upoważnieni przez Prezesa UODO, okazali Głównemu Geodecie Kraju swoje legitymacje służbowe oraz przedłożyli upoważnienia imienne zawierające informację o zakresie kontroli. GGK nie dopuścił jednak do przeprowadzenia czynności kontrolnych w pełnym zakresie wynikającym z przedłożonych upoważnień. Uzasadniając swoje stanowisko wskazał, że według jego oceny z zakresu wskazanego w upoważnieniach wynika, że kontrola ma dotyczyć numerów ksiąg wieczystych, które według niego nie stanowią danych osobowych w rozumieniu przepisów Prawa geodezyjnego i kartograficznego. Z uwagi na kategoryczny brak zgody GGK na przeprowadzenie czynności kontrolnych w pełnym zakresie oraz jednoznacznie wyrażony przez niego brak woli współpracy, kontrolujący nie mogli ustalić, w jaki sposób i na jakiej podstawie prawnej, przy udostępnianiu informacji z ewidencji gruntów i budynków za pośrednictwem portalu internetowego GEOPORTAL2 (geoportal.gov.pl), możliwy był dostęp do danych osobowych zawartych w księgach wieczystych oraz czy GGK wdrożył odpowiednie środki techniczne w celu zapewnienia bezpieczeństwa danych. Podczas kontroli nie można było zbadać tego, co było jej głównym przedmiotem, z uwagi na uniemożliwienie przeprowadzenia wszystkich czynności. W tym zakresie bowiem kontrola została udaremniona przez Głównego Geodetę Kraju. O nałożeniu kary na GGK w jej maksymalnej wysokości zadecydowało m.in. to, że po stronie tego podmiotu istniał intencjonalny brak woli współpracy w zapewnieniu organowi nadzorczemu wszelkich informacji (dowodów) niezbędnych do ustalenia, czy stanowiące przedmiot kontroli procesy przetwarzania danych mają podstawę prawną i przetwarzane są zgodnie z prawem. Brak zgody Głównego Geodety Kraju na przeprowadzenie kontroli i jego deklaracja braku współpracy w tym zakresie wyrażone zostały w sposób jednoznaczny i stanowczy. Natomiast argumentacja przedstawiona w uzasadnieniu stanowiska Głównego Geodety, w ocenie Prezesa UODO była całkowicie niezasadna.

Główny Geodeta Kraju złożył skargę na przedmiotową decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie, który **oddalił skargę GGK, uznając, że administracyjna kara pieniężna nałożona została zasadnie**.

Urząd Ochrony Danych Osobowych prowadzi **Rejestr administracyjnych kar pieniężnych nałożonych przez Prezesa UODO**. W 2020 r. Prezes UODO nałożył łącznie 11 administracyjnych kar pieniężnych, z czego 4 kary zostały nałożone na podmioty publiczne, a 7 kar dotyczyło podmiotów prywatnych (jednego przedsiębiorcy i 6 spółek prawa handlowego).

Zestawienie administracyjnych kar pieniężnych nałożonych przez Prezesa Urzędu Ochrony Danych Osobowych w 2020 roku znajduje się w załączniku nr 1.

11. Uprzednie konsultacje

Do zadań Urzędu Ochrony Danych Osobowych należy udzielanie zaleceń na wniosek o uprzednie konsultacje złożony przez administratora. Uprzednie konsultacje z UODO to procedura służąca wsparciu administratorów w sytuacji stwierdzenia przez nich wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, którego sami nie są w stanie zminimalizować. Procedura ta uregulowana jest w art. 36 RODO oraz w art. 57 ustawy o ochronie danych osobowych.

Celem uprzednich konsultacji jest wypracowanie rozwiązań, które pozwolą administratorowi prawidłowo chronić dane osobowe.

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, podobnie jak w poprzednich latach, w niewielkim zakresie korzystali z tej formy współpracy z organem nadzorczym. W 2020 r. do Urzędu wpłynęły **3 wnioski o przeprowadzenie uprzednich konsultacji.** W poprzednim roku sprawozdawczym wpłynęło **5** takich wniosków, zaś w 2018 roku – **2**.

Złożone w 2020 r. wnioski nie mogły inicjować postępowania w sprawie uprzednich konsultacji, ponieważ dotyczyły wątpliwości w zakresie podstawy prawej udostępnienia danych osobowych, które powinny być rozstrzygane na podstawie obowiązujących przepisów regulujących opisane w tych wnioskach kwestie, nie zaś na podstawie art. 36 RODO. Procedura uprzednich konsultacji ustanowiona została bowiem w innym celu.

To, że administratorzy zwracali się do UODO z pytaniami prawnymi, powołując się na tryb uprzednich konsultacji, świadczyć mogło o braku zrozumienia celów instytucji uprzednich

konsultacji. Dostrzegając ten problem Prezes UODO postanowił ponownie przybliżyć i wyjaśnić administratorom, czemu ma służyć to rozwiązanie i w jakich sytuacjach może być wykorzystane. W tym celu 22 czerwca 2020 r. zamieszczony został na stronie internetowej UODO komunikat pt. „Uprzednie konsultacje – kto i kiedy może z nich skorzystać?". W materiale tym opisane zostały sytuacje, w których administratorzy mogą występować do UODO z wnioskiem o uprzednie konsultacje, a także przypomniano, że informacje dotyczące tego, co należy zrobić zanim wystąpi się z wnioskiem o przeprowadzenie uprzednich konsultacji, jak wypełnić formularz wniosku, a także opracowany przez UODO wzór takiego formularza, znajdują się na stronie internetowej Urzędu w specjalnej zakładce „Uprzednie konsultacje" w panelu „Administrator".

12. Kodeksy postępowania

Na mocy art. 40 RODO wprowadzony został instrument prawny w postaci kodeksów postępowania, 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 2020 r. w ramach realizacji zadania z art. 57 ust. 1 lit. m RODO[201], Prezes UODO prowadził prace nad zamknięciem systemu przyjmowania przewidzianych w RODO kodeksów postępowania, tak by umożliwić ich zatwierdzenie, tj. nad określeniem wymogów akredytacji podmiotów monitorujących. Jednocześnie ściśle współpracował ze środowiskami pracującymi nad projektami kodeksów postępowania i innymi zainteresowanymi podmiotami.

[201] Zgodnie z tym przepisem, bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia, każdy organ nadzorczy na swoim terytorium zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5.

W 2020 roku cztery (4) organizacje złożyły do Prezesa UODO wnioski o zatwierdzenie projektu kodeksu postępowania:

1) Polska Rada Centrów Handlowych – „Kodeks postępowania dla sektora handlu”[202];
2) Stowarzyszenie Bibliotekarzy Polskich – „Kodeks dla bibliotek”[203];
3) Krajowa Rada Doradców Podatkowych – „Kodeks postępowania Krajowej Izby Doradców Podatkowych w zakresie ochrony danych osobowych”[204];
4) Związek Pracodawców Organizacja Firm Badania Opinii i Rynku – „Kodeks postępowania dotyczący przetwarzania danych osobowych przez prywatne agencje badawcze”[205].

W odniesieniu do wcześniej złożonych wniosków, to najbardziej zaawansowane były prace nad dwoma kodeksami w służbie zdrowia, które zostały przedłożone przez Federację Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie” – „Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych”[206] oraz przez Polską Federację Szpitali – „Kodeks postępowania dla sektora ochrony zdrowia”[207]. W 2020 r. Prezes UODO korespondował z wnioskodawcami w celu przedstawienia ostatecznej wersji kodeksów. Na tej podstawie przygotował opinie o ich zgodności z RODO. Do końca 2020 r. trwały konsultacje dotyczące ostatecznej wersji stanowiska organu w tych sprawach. Wydanie tej opinii umożliwiło podmiotom monitorującym kodeks postępowania złożenie wniosku do Prezesa Urzędu o akredytację. Działania twórców wymienionych projektów kodeksów były także przedmiotem pytań wpływających do Urzędu[208].

Ze względu na stan pandemii przez większość roku sprawozdawczego nie było możliwości organizowania spotkań z przedstawicielami inicjatyw zainteresowanych tworzeniem kodeksów postępowania. Jednak w toku prowadzonych postępowań kodeksowych omawiano z ich autorami poszczególne postanowienia, poddawano ocenie sprawozdania z konsultacji i pozostałe elementy wniosku o zatwierdzenie kodeksu. Dużym wyzwaniem dla podmiotów zrzeszonych było nadal przyjęcie modelu monitorowania kodeksu, który będzie akceptowalny zarówno dla członków z punktu widzenia działalności organizacji i jej finansowania, jak i dla organu nadzorczego. Należy

[202] DOL.4421.3.2020.
[203] DOL.4421.4.2020.
[204] DOL.4421.1.2020.
[205] DOL.4421.2.2020.
[206] ZAS.070.2.2018.
[207] ZAS.070.4.2018.
[208] DOL.023.1163.2020.

podkreślić, że skuteczny system monitorowania wiąże się z ponoszeniem kosztów, które zapewnią efektywną kontrolę podmiotów objętych kodeksem, zarówno okresową, jak i nadzwyczajną, w przypadku wystąpienia naruszeń.

W 2020 r. do Prezesa UODO zwracały się także podmioty przygotowujące projekty kodeksów, zgłaszając różnego rodzaju wątpliwości powstałe w trakcie ich tworzenia. Prezes Urzędu udzielił tym podmiotom stosownych wyjaśnień, a dotyczyły one projektów:

– Kodeksu postępowania dla jednostek oświatowych, mającego na celu doprecyzowanie stosowania rozporządzenia 2016/679;

– Kodeksu postępowania dla Regionalnych Izb Obrachunkowych;

– Kodeksu postępowania dla fotografów;

– Kodeksu postępowania dla przedsiębiorców działających na rynku skupu i przetwarzania złomu.

Na podstawie art. 41 RODO, przy uwzględnieniu art. 29 ustawy o ochronie danych osobowych oraz wytycznych Europejskiej Rady Ochrony Danych nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679[209], UODO przygotował projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania. W celu zatwierdzenia kodeksu postępowania niezbędne jest bowiem, aby w jego treści został wskazany podmiot monitorujący (lub podmioty monitorujące). Podmiot monitorujący musi zostać akredytowany przez Prezesa UODO jako ten, który jest w stanie skutecznie monitorować kodeks.

Projekt wymogów akredytacji został poddany konsultacjom społecznym w lipcu 2020 r.[210] Po analizie nadesłanych uwag dokonano stosownych zmian w jego treści oraz przetłumaczono go na język angielski. Celem tych działań było wypełnienie dyspozycji z art. 41 ust. 3 RODO, zgodnie z którą Prezes UODO jest zobowiązany przedstawić Europejskiej Radzie Ochrony Danych do zaopiniowania projekt Wymogów akredytacji z wykorzystaniem mechanizmu spójności (art. 63 RODO). W związku z powyższym we wrześniu 2020 r. przedłożono ostateczny projekt proponowanych Wymogów akredytacji Radzie[211]. Wniosek o wydanie opinii EROD złożono za pośrednictwem systemu IMI w trybie art. 64 RODO.

Prace nad projektem Wymogów akredytacji w EROD prowadziła Ekspercka podgrupa Compliance, e-Government and Health. Opinia do tego dokumentu została przyjęta 7 grudnia 2020

[209] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pl.pdf.
[210] DOL.420.2.2020; zob. https://uodo.gov.pl/pl/138/1559.
[211] DOL.602.4.2020.

r. w głosowaniu pisemnym członków EROD[212]. Celem opinii jest utrzymanie spójności z przepisami RODO oraz innymi krajowymi wymogami akredytacji przy zachowaniu rozwiązań lokalnych zaproponowanych przez Urząd, podyktowanych specyfiką polskiego porządku prawnego. Wymogi akredytacji zostały przyjęte i opublikowane przez Prezesa Urzędu w styczniu 2021 r.[213]

13. 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.

13.1. Pytania prawne

Zgodnie z art. 57 ust. 1 RODO Prezes Urzędu Ochrony Danych Osobowych, w ramach swoich kompetencji, m.in. upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz udziela osobie, której dane dotyczą, na jej żądanie, informacji o jej prawach wynikających z RODO.

Ponadto, zgodnie z art. 57 ust. 3 RODO, zadaniem organu nadzorczego jest bezpłatne wypełnianie zadań na rzecz osoby, której dane dotyczą, i – gdy ma to zastosowanie – inspektora ochrony danych.

Udzielanie odpowiedzi na pytania prawne dotyczące ochrony danych osobowych stanowi bardzo ważną – z punktu widzenia obywateli – działalność. Nie została ona ujęta w kompetencjach 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. Udzielanie odpowiedzi na pytania przyczynia się do doskonalenia wiedzy na temat ochrony 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,

[212] https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-312020-draft-decision-competent_pl.
[213] https://uodo.gov.pl/pl/138/1861

wytyczne, itd.), których tematyka obejmuje niemalże wszystkie dziedziny życia publicznego. Niejednokrotnie bowiem organowi nadzorczemu w tego typu korespondencji sygnalizowane są problemy wspólne dla różnych grup podmiotów.

W roku 2020 **administratorzy oraz osoby fizyczne skierowali** do Prezesa Urzędu Ochrony Danych Osobowych łącznie **2774 pisma** zawierające pytania z zakresu ochrony danych osobowych. To tylko nieco mniej niż w roku ubiegłym, kiedy to wpłynęło ich 2812. Łącznie w 2020 r. organ nadzorczy **rozpatrzył 2939** takich pism.

Osobną grupę spraw stanowią pytania od inspektorów ochrony danych (IOD), do których Prezes UODO – biorąc pod uwagę szczególną rolę, jaką osoby wykonujące tę funkcję mają pełnić w systemie ochrony danych osobowych – podchodzi ze szczególną uwagą.

W 2020 r. do Prezesa UODO wpłynęło **338 pytań od inspektorów ochrony danych**. Udzielono zaś **434 odpowiedzi** na pytania od IOD.

W 2020 r. do najczęściej poruszanych zagadnień, na które w przesłanych do Urzędu pytaniach zwrócili uwagę zarówno administratorzy, osoby fizyczne oraz IOD, i które były przedmiotem analiz organu, należały m.in.:

1) przesłanki legalizujące przetwarzanie danych osobowych podczas pandemii COVID-19,
2) przetwarzanie danych osobowych w związku z wprowadzeniem zdalnego nauczania,
3) ochrona danych osobowych w związku z realizacją praw pacjenta w warunkach pandemii COVID-19,
4) przetwarzanie danych osobowych w związku z kampanią i wyborami na Prezydenta RP.

Ad. 1) Przesłanki legalizujące przetwarzanie danych osobowych podczas pandemii COVID-19

W 2020 r. wiele organów i podmiotów podejmowało działania mające na celu ograniczenie i złagodzenie skutków pandemii COVID-19. Były one realizowane w warunkach bardzo dynamicznych zmian prawa, wytycznych i decyzji służb sanitarnych oraz innych organów zaangażowanych w walkę z koronawirusem. Często wiązały się z przetwarzaniem danych osobowych, w tym tych szczególnych kategorii, jakimi są m.in. dane dotyczące stanu zdrowia.

Zapewnienie właściwej ich ochrony dla wielu administratorów i podmiotów przetwarzających było dużym wyzwaniem, czego dowodzą wpływające do UODO pytania.

Zgłaszane wątpliwości dotyczyły m.in. prawidłowości przetwarzania danych osobowych ww. celach, np. w zakresie podstawy prawnej mierzenia temperatury w celu zapobiegania

rozprzestrzeniania się COVID-19, udostępniania danych osób objętych kwarantanną czy tworzenia rejestrów zawierających informacje o takich osobach. Do wielu z przedstawianych przez inspektorów wątpliwości organ ds. ochrony danych osobowych odnosił się w różnych materiałach zamieszczanych na stronie internetowej Urzędu. Wśród nich warto wskazać wydane 12 marca 2020 r. „Oświadczenie Prezesa Urzędu Ochrony Danych Osobowych w sprawie koronawirusa”[214], oświadczenie Europejskiej Rady Ochrony Danych (EROD) w sprawie przetwarzania danych w kontekście pandemii COVID-19[215] zamieszczone 20 marca 2020 r., komunikat Prezesa UODO z 5 maja 2020 r. „Sprawdzanie temperatury w celu zapobiegania rozprzestrzeniania się COVID-19”[216] czy materiał „Szerokie uprawnienia GIS przy przetwarzaniu danych w związku z koronawirusem”[217]. Stanowiły one istotne, kierunkowe wskazówki, co do właściwego postępowania administratorów.

Odpowiedzi na najczęściej powtarzające się pytania od inspektorów w tym zakresie zamieszczone zostały w zakładce „Inspektor Ochrony Danych”.

Ad. 2) Przetwarzanie danych osobowych w związku z wprowadzeniem zdalnego nauczania

W związku z pandemią w 2020 r. również szkoły znalazły się w wyjątkowej sytuacji, w której musiały stawić czoła nowym wymaganiom związanym ze zdalnym nauczaniem. Szkoły i nauczyciele musieli w bardzo krótkim czasie zorganizować na te potrzeby efektywną komunikację z uczniami i ich rodzicami. Prowadząc zajęcia przy pomocy **programów do realizacji konferencji czy innych narządzi do pracy grupowej, a także komunikatorów internetowych lub poczty elektronicznej, szkoły** stały się odpowiedzialne za przetwarzane przy użyciu tych narządzi dane osobowe.

W związku z nauką zdalną do organu nadzorczego kierowano pytania dotyczące: zakresu danych osobowych, jaki może być wykorzystywany do przeprowadzenia nauki online, metod zabezpieczenia danych przy korzystaniu z programów lub aplikacji mobilnych, prowadzenia rady pedagogicznej, rejestrowania przeprowadzanych zdalnie egzaminów czy zasad bezpieczeństwa przy zdalnym łączeniu się z dziennikiem elektronicznym.

W odpowiedzi m.in. na takie sygnały od administratorów oraz inspektorów ochrony danych, UODO przygotował materiały, które zawierają wskazówki, jak korzystając z metod nauczania

[214] https://uodo.gov.pl/pl/138/1456
[215] https://uodo.gov.pl/pl/138/1463
[216] https://uodo.gov.pl/pl/138/1516
[217] https://uodo.gov.pl/pl/138/1471

online, dbać o bezpieczne przetwarzanie danych. Informacje te dostępne są na stronie internetowej UODO pod następującymi linkami:
– materiał pt. „Dane osobowe bezpieczne podczas zdalnego nauczania" – https://uodo.gov.pl/pl/138/1473,
– zapis szkolenia online, pt. „Praca zdalna a ochrona danych osobowych – porady dla nauczycieli" – https://uodo.gov.pl/pl/434/1540,
– zapis szkolenia pt. „Szkolenie dla inspektorów ochrony danych z sektora oświaty" – https://uodo.gov.pl/pl/190/1728.

Ww. materiały adresowane są do dyrektorów szkół, inspektorów ochrony danych i nauczycieli, ale zawierają również informacje przydatne rodzicom i uczniom.

W udzielanych wyjaśnieniach Prezes UODO przypominał, że podstawę prawną realizacji zajęć szkolnych w formie pracy zdalnej określa rozporządzenie Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19[218]. Szkoły zaś powinny zapewnić, aby przetwarzanie danych osobowych w nowych warunkach odbywało się zgodnie z zasadami określonymi w RODO – legalizmu, minimalizacji, celowości, ograniczenia czasowego, przeprowadzając odpowiednią analizę ryzyka dla ochrony danych osobowych.

Ad. 3) Ochrona danych osobowych w związku z realizacją praw pacjenta w warunkach pandemii COVID-19

W związku ze szczególną sytuacją związaną z pandemią, zarówno osoby fizyczne, jaki placówki ochrony zdrowia zwracały się do Prezesa UODO o opinię w sprawie przetwarzania danych osobowych podczas składania wniosków o **udostępnianie dokumentacji medycznej** i metod udostępniania dokumentacji medycznej w czasie epidemii wirusa COVID–19. Miały bowiem wątpliwości, czy rozwiązanie w postaci przesyłania dokumentacji medycznej na wniosek nie tylko samego pacjenta, ale i jego przedstawiciela ustawowego bądź osoby upoważnionej przez pacjenta, za pośrednictwem środków komunikacji elektronicznej, w tym profilu ePUAP, jest zgodne z RODO. Często bowiem pacjenci, szczególnie osoby starsze, nie mają dostępu do Internetu ani do skrzynki na profilu ePUAP, a także podpisu elektronicznego, a ze względu na wiek czy stan zdrowia – wówczas,

[218] Dz.U. z 2020 r. poz. 493.

gdy muszą osobiście odebrać swoją dokumentację medyczną, są szczególnie narażone na utratę życia lub zdrowia z powodu zarażenia COVID-19.

Organ nadzorczy w komunikacie zamieszczonym na stronie internetowej[219] wskazał, że obowiązujące przepisy umożliwiają udostępnianie dokumentacji medycznej drogą elektroniczną zarówno pacjentom, jak i ich przedstawicielom ustawowym bądź osobom upoważnionym. Zatem osoby starsze, które w okresie pandemii chcą pozyskać taką dokumentację bez składania wizyty w placówce ochrony zdrowia, a same nie dysponują niezbędnymi środkami technicznymi, mogą skorzystać z pośrednictwa innych osób. Muszą tylko do tego je upoważnić.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych, wyrażonej zarówno w udzielanych odpowiedziach, jak i w zamieszczonej na stronie internetowej opinii[220], obecnie obowiązujące regulacje prawne są wystarczające dla realizacji prawa pacjenta do pozyskania dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych (o którym mowa w art. 23 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[221]).

Artykuł 26 ust. 1 tej ustawy stanowi, że podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta. Z kolei art. 27 ust. 1 ustawy o prawach pacjenta, określający sposoby udostępniania dokumentacji pacjenta, wskazuje m.in. możliwość udostępnienia dokumentacji za pośrednictwem środków komunikacji elektronicznej. W rozporządzeniu Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania wskazano (w § 70 ust. 1), że dokumentację udostępnia się z zachowaniem jej integralności, poufności oraz autentyczności, bez zbędnej zwłoki, natomiast w § 71 określono, że w przypadku, gdy udostępnienie dokumentacji nie jest możliwe, odmowę przekazuje się w postaci elektronicznej albo papierowej, zgodnie z żądaniem uprawnionego organu lub podmiotu. W każdym przypadku wymagane jest podanie przyczyny odmowy. Prezes UODO zaznaczył, że udostępnianie dokumentacji medycznej za pośrednictwem środków komunikacji elektronicznej powinno odbywać się przy zachowaniu zasad bezpieczeństwa, umożliwiających weryfikację osoby składającej wniosek oraz gwarantujących bezpieczeństwo przesyłanych danych.

[219] https://uodo.gov.pl/pl/138/1517
[220] https://uodo.gov.pl/pl/138/1517
[221] Dz. U. z 2019 r. poz. 1127 z późn. zm.

W ocenie organu nadzorczego, rozwiązanie w postaci przesyłania dokumentacji medycznej na wniosek nie tylko samego pacjenta, ale i jego przedstawiciela ustawowego, bądź osoby upoważnionej przez pacjenta, za pośrednictwem profilu ePUAP, przy zachowaniu procedur wynikających z regulacji ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, jest dopuszczalne w świetle przepisów RODO. Rozwiązanie to pozwala realizować prawo pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych przy zmniejszeniu ryzyka bezpośredniego odbioru dokumentacji w okresie epidemii wirusa COVID–19.

W przypadku korzystania z innych środków komunikacji elektronicznej szpital, jako administrator, powinien ocenić, czy gwarantują one odpowiedni stopień bezpieczeństwa przesyłanych danych zawartych w dokumentacji medycznej.

Z kolei biorąc pod uwagę wielość pytań związanych z dostępem do informacji o stanie zdrowia pacjenta na odległość, Prezes UODO we współpracy z Rzecznikiem Praw Pacjenta przygotowali **„Wytyczne w sprawie realizacji przez osoby uprawnione prawa do informacji o stanie zdrowia pacjenta na odległość”**[222], które zostały opublikowane na stronach internetowych obu podmiotów. Dokument ten zawiera rekomendowane rozwiązania, pozwalające na realizację prawa osoby upoważnionej do informacji o stanie zdrowia pacjenta na odległość, z uwzględnieniem praw pacjenta oraz zasad wynikających z regulacji dotyczących ochrony danych osobowych. Wytyczne odnoszą się również do postępowania zalecanego w sytuacji kontaktu na odległość z osobą bliską, której pacjent, ze względu na swój stan zdrowia, nie mógł upoważnić do przekazania informacji.

Ad. 4) Przetwarzanie danych osobowych w związku z kampanią i wyborami na Prezydenta RP

Rok 2020 to także okres zarówno prowadzenia kampanii, jak i przeprowadzania wyborów na Prezydenta RP. Organ nadzorczy wspierał podmioty zaangażowane w realizację tego zadania na różnych jego etapach.

W związku z kampanią wyborczą i wpływającymi wówczas pytaniami przygotował i zamieścił na stronie internetowej Urzędu komunikat dotyczący tego, **jak z danymi osobowymi powinny postępować komitety wyborcze**[223]. Przypomniał w nim, że podmioty te będą przetwarzać na dużą skalę dane osobowe, w tym dane szczególnej kategorii, o których mowa w art. 9 RODO, takie jak ujawniające poglądy polityczne czy światopoglądowe**,** a także mają obowiązek przetwarzania ich

[222] https://uodo.gov.pl/pl/138/1787
[223] https://uodo.gov.pl/pl/138/1444

zgodnie z prawem oraz wdrożenia adekwatnych środków zapewniających odpowiedni poziom ochrony danych. Są również zobowiązane do przeprowadzenia oceny skutków dla ochrony danych.

Wskazał też, że komitety wyborcze mogą przekazywać przetwarzane przez siebie dane osobowe pozyskane bezpośrednio na podstawie przepisów Kodeksu wyborczego (np. dane osobowe z list poparcia) wyłącznie organom wskazanym w przepisach prawa wyborczego. Nie mogą zaś udostępniać ich innym podmiotom, np. partiom politycznym wspierającym kandydata na Prezydenta Rzeczypospolitej Polskiej czy firmom wynajętym do prowadzenia działań marketingowych.

Prezes UODO odniósł się także do zbieraniu podpisów na listach poparcia danego kandydata. Zaznaczył, że należy robić to tak, by osoby podpisujące taką listę nie mogły się zapoznać z danymi osób, które uczyniły to wcześniej, a więc zasłaniać te dane np. stosując proste nakładki. Przestrzegał także, by nie chwalić się widocznymi listami w mediach społecznościowych. Przekazał również praktyczne wskazówki dotyczące prowadzenia działań marketingowych w sieci.

Tematyka ta stała się także przedmiotem analiz organu nadzorczego w związku z licznymi pytaniami dotyczącymi legalności **udostępnienia przez jednostki samorządu terytorialnego spisu wyborców Poczcie Polskiej**, na potrzeby podjęcia przez nią czynności niezbędnych do przygotowania i przeprowadzenia wyborów na Prezydenta RP w tzw. trybie korespondencyjnym, które miały się odbyć 10 maja 2020 r. Pytania w tej sprawie wpływały zarówno od administratorów, inspektorów ochrony danych, jak i od osób fizycznych.

Prezes UODO, reagując niezwłocznie na podnoszone wątpliwości, zamieścił oświadczenie w tej sprawie na stronie internetowej Urzędu[224]. Zaznaczył w nim, że w **świetle obowiązujących przepisów prawa to Państwowa Komisja Wyborcza, a nie Prezes UODO, jest organem odpowiedzialnym za właściwy przebieg wyborów na Prezydenta RP.** Wskazał też, że PKW zajęła stanowisko, określające rolę operatora pocztowego, a także obowiązek współpracy z nim w zakresie udostępnienia danych ze spisu wyborców[225].

Jednocześnie w odpowiedziach[226] na liczne wpływające do Urzędu pytania, Prezes UODO, odwołując się do zamieszczonego na stronie internetowej Oświadczenia, dodatkowo wskazywał, że każdy administrator ma prawo i obowiązek przeprowadzenia dokładnej analizy wniosku o udostępnienie danych, który do niego wpływa, zarówno pod względem spełnienia warunków

[224] https://uodo.gov.pl/pl/138/1508
[225] Pismo Pana Sylwestra Marciniaka, Przewodniczącego Państwowej Komisji Wyborczej z dnia 23 kwietnia 2020 r. (znak: ZPOW-421-10/20) kierowane do komisarzy wyborczych, w celu przekazania wyjaśnień wójtom, burmistrzom i prezydentom miast.
[226] m.in. DOL.023.624.2020, DOL.023.720.2020, DOL.023.823.2020, DOL.023.862.2020.

formalnych, np. dotyczących podpisu, jak i aspektów materialnych, tj. weryfikacji podstaw prawnych (art. 6 RODO oraz w niektórych przypadkach również art. 9 i 10 RODO) żądania udostępnienia danych osobowych. W sytuacji, gdy o udostępnienie danych osobowych występuje podmiot realizujący zadania publiczne, powinien on w pierwszej kolejności wyraźnie wskazać przepisy uprawniające go do pozyskania danych. Jeżeli wniosek o udostępnienie danych osobowych zawiera braki formalne lub gdy uzasadnienie prawne wniosku budzi wątpliwości, celowe jest zwrócenie się do wnioskodawcy o uzupełnienie tych braków, a także o uzyskanie od wnioskującego wyjaśnień lub dodatkowych informacji. Zgromadzenie powyższych informacji pozwoli podmiotowi, do którego zwrócono się o udostępnienie danych, na dokonanie szczegółowej analizy dopuszczalności takiego udostępnienia. To do administratora należy bowiem ostateczna ocena, czy udostępni wnioskowane dane.

Prezes UODO wskazywał też na rozporządzenie Ministra Aktywów Państwowych z dnia 9 maja 2020 r. w sprawie przekazania spisu wyborców gminnej obwodowej komisji wyborczej oraz operatorowi wyznaczonemu w związku z przeprowadzeniem wyborów powszechnych na Prezydenta Rzeczypospolitej Polskiej zarządzonych w 2020 r.[227]

W dalszej części omówione zostaną bardziej szczegółowe lub szczególnie interesujące wyjaśnienia Prezesa UODO na pytania wpływające od administratorów, osób fizycznych oraz od IOD, w tym również te związane z pandemią COVID-19.

13.1.1. Pytania prawne od administratorów i osób fizycznych

W analizowanym 2020 r. dominującym zagadnieniem była ochrona danych osobowych w czasie epidemii wirusa SARS-CoV-2**.** Większość zagadnień, o które pytali administratorzy i osoby fizyczne znajdowała uregulowanie w przepisach szczególnych, które Prezes UODO wskazywał w swoich pismach, tzn. w ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[228] (tzw. specustawa covidowa), ustawie z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi[229], ustawie z dnia 14

[227] Rozporządzenie Ministra Aktywów Państwowych z dnia 9 maja 2020 r. w sprawie przekazania spisu wyborców gminnej obwodowej komisji wyborczej oraz operatorowi wyznaczonemu w związku z przeprowadzeniem wyborów powszechnych na Prezydenta Rzeczypospolitej Polskiej, zarządzonych w 2020 r. – Dz.U. z 2020 r. poz. 828.
[228] Dz. U. z 2020 r. poz. 374 z późn. zm.
[229] Dz. U. z 2020 r. poz. 1845 z późn. zm.

marca 1985 r. o Państwowej Inspekcji Sanitarnej[230], czy wydanych na ich podstawie rozporządzeniach. Warto jednak podkreślić, że przepisy te zmieniały się dynamicznie, tak samo jak sytuacja epidemiczna w kraju. Szczególnie rozporządzenia Rady Ministrów w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, wydawane na podstawie ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi, były cyklicznie zmieniane lub uchylane i zastępowane nowymi przepisami w zależności od stopnia rozwoju epidemii w kraju[231].

Zapytania od osób fizycznych związane z COVID-19

Wątpliwości osób fizycznych budziła przede wszystkim kwestia uprawnień służb sanitarno-epidemiologicznych w czasie epidemii COVID-19, np. zakresu i sposobu pozyskiwania danych osobowych od osób objętych kwarantanną lub izolacją domową[232]. Przykładowo kwestionowane było żądanie podania danych osobowych przez telefon z punktu widzenia bezpieczeństwa danych osobowych przewidzianego w RODO. Prezes UODO wyjaśniał, że rozporządzenie Rady Ministrów z dnia 7 sierpnia 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[233] regulowało w § 5, że osoba poddana obowiązkowi kwarantanny odbywa ją razem z osobami wspólnie zamieszkującymi lub gospodarującymi oraz informuje ona policję albo organy Państwowej Inspekcji Sanitarnej o imieniu i nazwisku oraz numerze PESEL i numerze telefonu tych osób, jeżeli go posiadają. Informację tę przekazuje się za pośrednictwem systemów teleinformatycznych lub systemów łączności, w tym przez telefon[234].

Z kolei zakres informacji, jakich może żądać państwowy inspektor sanitarny lub Główny Inspektor Sanitarny w związku z prowadzonym dochodzeniem epidemiologicznym, określa art. 32a

[230] Dz. U. z 2019 r. poz. 59 z późn. zm.

[231] Pierwsze rozporządzenie Rady Ministrów w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii zostało wydane 31 marca 2020 r., a uchylone 10 kwietnia 2020 r. Było ono zmieniane dwa razy rozporządzeniami z 1.04.2020 r. i 7.04.2020 r. Na dzień 1 grudnia 2020 r. Rada Ministrów wydała kolejne (11 z kolei) rozporządzenie w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii.

[232] DOL.023.1669.2020, DOL.023.1973.2020.

[233] Dz. U. z 2020 r. poz. 1356. Rozporządzenie to utraciło moc z dniem 10 października 2002 r. poprzez uchylenie rozporządzeniem z dnia 9 października 2020 r. – Dz. U. z 2020 r. poz. 1758.

[234] § 5 uchylony przez § 1 pkt 5 rozporządzenia z dnia 23 października 2020 r. (Dz.U. z 2020 r. poz. 1871) zmieniającego to rozporządzenie z dniem 24 października 2020 r. Na medyczne laboratoria diagnostyczne wykonujące diagnostykę zakażenia wirusem SARS-CoV-2 nałożono wówczas obowiązek wprowadzania do systemu teleinformatycznego, udostępnionego przez jednostkę podległą ministrowi właściwemu do spraw zdrowia, właściwą w zakresie systemów informacyjnych ochrony zdrowia informację o pozytywnym wyniku testu diagnostycznego w kierunku SARS-CoV-2, finansowanego ze środków innych niż środki publiczne oraz informacje o osobie, której dotyczy badanie diagnostyczne, w tym informację o numerze telefonu do bezpośredniego kontaktu z tą osobą, w przypadku, gdy informacje te nie znajdują się w tym systemie.

ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi. Organ informował, że powyższe przepisy stanowią przesłanki przetwarzania danych osobowych wskazane w art. 6 ust. 1 lit. c RODO – gdy przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze oraz w art. 6 ust. 1 lit. d RODO – gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

Zapytania od organów publicznych związane z COVID-19

Do Prezesa UODO zwrócił się przedstawiciel **Departamentu Gospodarki Odpadami w Ministerstwie Klimatu** o zajęcie stanowiska w sprawie podstaw prawnych do udostępniania danych osobowych, a dokładnie adresu osób przebywających na kwarantannie domowej lub w izolacji, podmiotom administracji publicznej oraz innym podmiotom zobowiązanym do odbioru i zagospodarowania odpadów komunalnych wytwarzanych przez te osoby[235]. Wątpliwości te pojawiły się w związku z wytycznymi Głównego Inspektora Sanitarnego opracowanymi we współpracy z Ministrem Klimatu, zgodnie z którymi odpady pochodzące od osób objętych kwarantanną należało traktować jako odpady komunalne. Pojawiło się zatem pytanie, czy informacje dotyczące osób objętych kwarantanną/izolacją (np. adres zamieszkania) mogą być udostępniane przez m.in. organy Państwowej Inspekcji Sanitarnej, wojewodów władzom jednostek samorządu terytorialnego, a następnie przedsiębiorstwom odbierającym odpady komunalne. Prezes UODO zajął stanowisko, że skoro w rozporządzeniu Rady Ministrów z dnia 19 kwietnia 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[236] zostały enumeratywnie wymienione podmioty, którym udostępnia się informacje o osobach objętych kwarantanną (w tym adresy miejsca zamieszkania lub pobytu, w którym osoba objęta obowiązkową kwarantanną będzie ją odbywać), to pozyskiwanie tych informacji przez inne podmioty, np. jednostki samorządu terytorialnego, przedsiębiorstwa odbierające odpady, nie znajduje podstaw prawnych. Jednocześnie organ nadzorczy przypomniał o ochronie prywatności osób objętych kwarantanną lub izolacją domową. Wyjaśnił, że praktyki dostarczania im specjalnych

[235] DOL.023.566.2020.

[236] Dz. U. z 2020 r. poz. 697. Zgodnie z § 2 ust. 6, dane, o których mowa w ust. 3 i 4 (a więc m.in. o adresach odbywania kwarantanny) są udostępniane organom Państwowej Inspekcji Sanitarnej, Narodowemu Funduszowi Zdrowia, Zakładowi Ubezpieczeń Społecznych, Kasie Rolniczego Ubezpieczenia Społecznego, Narodowemu Instytutowi Zdrowia Publicznego – Państwowemu Zakładowi Higieny, Narodowemu Instytutowi Kardiologii Stefana Kardynała Wyszyńskiego – Państwowemu Instytutowi Badawczemu, wojewodom, Policji, Państwowej Straży Pożarnej, Systemowi Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego i operatorowi wyznaczonemu w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2018 r. poz. 2188 z 2019 r. poz. 1051, 1495 i 2005 oraz z 2020 r. poz. 695).

kontenerów lub worków na odpady albo oznaczania nieruchomości nie powinny mieć miejsca, gdyż powoduje to niepotrzebną stygmatyzację osób objętych kwarantanną lub izolacją domową. Prezes UODO odwołał się jednocześnie do Oświadczenia Przewodniczącej EROD ws. przetwarzania danych podczas pandemii COVID-19 przyjętego 19 marca 2020 r., w którym wskazano, że „*organy publiczne powinny w pierwszej kolejności starać się przetwarzać dane dotyczące lokalizacji w sposób anonimowy. Zawsze należy preferować rozwiązania najmniej inwazyjne, biorąc pod uwagę konkretny cel, który ma zostać osiągnięty”.*

Podobne stanowisko Prezes UODO zaprezentował w sprawie dotyczącej **jednej ze spółdzielni**, która w związku z koniecznością usuwania awarii lub wykonywania niezbędnych robót, mając na względzie dobro pracowników, chciała pozyskać dostęp do wykazu lokali objętych kwarantanną[237]. Organ wyjaśnił, że skoro ustawodawca zdecydował, aby uregulować w przepisach szczególnych wykaz podmiotów, którym udostępnia się informacje o osobach odbywających kwarantannę (w tym o adresie ich miejsca zamieszkania lub pobytu), to pozyskiwanie tych informacji przez inne podmioty, np. spółdzielnie, nie znajduje podstaw prawnych. Jednocześnie Prezes UODO wskazał spółdzielni na uprawnienia Głównego Inspektora Sanitarnego lub działającego z jego upoważnienia innego organu Państwowej Inspekcji Sanitarnej do wydawania osobom prawnym, osobom fizycznym i jednostkom organizacyjnym nieposiadającym osobowości prawnej, w szczególności podmiotom wykonującym działalność leczniczą czy pracodawcom, zaleceń i wytycznych określających sposób postępowania w trakcie realizacji zadań w przypadku stanu zagrożenia epidemiologicznego, stanu epidemii[238]. Jeśli zatem pracownicy spółdzielni w toku realizacji swoich obowiązków, w czasie stanu zagrożenia epidemiologicznego czy stanu epidemii, obawiają się o swoje bezpieczeństwo, istnieje możliwość zwrócenia się do Głównego Inspektora Sanitarnego lub właściwego organu Państwowej Inspekcji Sanitarnej o wydanie zalecenia czy wytycznych, jak postępować w danej sytuacji, aby nie narażać życia i zdrowia osób wykonujących swoje zadania. Organ nadzorczy wyraźnie podkreślił, że nie można uznawać, że ochrona danych osobowych osób objętych kwarantanną nie pozwala na prawidłowe i bezpieczne wykonywanie obowiązków przez określone podmioty w czasie stanu epidemii, gdyż to przepisy szczególne, a nie RODO, przyznają służbom sanitarnym szczegółowe uprawnienia w tym zakresie. Podkreślenia wymaga, że z ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych[239] wynika, że usterki w lokalach są usuwane zazwyczaj po

[237] DOL.023.336.2020.
[238] Art. 8a ust. 5 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej.
[239] t.j. Dz. U. z 2018 r. poz. 845 z późn. zm. - art. 6^1.

zgłoszeniu ich przez samych mieszkańców (właścicieli, użytkowników), co oznacza, że to oni mogą (lub nawet powinni) informować pracowników spółdzielni o odbywanej kwarantannie. Za właściwe można też uznać sytuacje, gdy spółdzielnia sama wprowadzi własne procedury zapewniające bezpieczeństwo należącego do niej i do jej członków mienia, m.in. regulując sposób pozyskiwania informacji o lokalach objętych kwarantanną bezpośrednio od osób w nich przebywających, za ich zgodą, przy uwzględnieniu odpowiednio przyjętych reguł bezpieczeństwa pracowników z jednoczesnym zachowaniem prywatności członków spółdzielni objętych kwarantanną. Przy czym nie chodzi tu o pozyskiwanie informacji o osobach objętych kwarantanną, ale jedynie o informację, że dany lokal objęty jest kwarantanną.

Warto wspomnieć, że katalog podmiotów uprawnionych do pozyskania informacji o osobach objętych obowiązkową kwarantanną lub izolacją w warunkach domowych, przewidziany w rozporządzeniu w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, był przez ustawodawcę stopniowo rozszerzany, co można było już zauważyć w kolejnych miesiącach trwania pandemii. Znajdowało to odzwierciedlenie w kolejnych opiniach Prezesa UODO.

Wątpliwości interpretacyjne, co do przepisów specustawy covidowej, miał jeden **z urzędów wojewódzkich**[240]. Zwrócił się on do Prezesa UODO o stanowisko w sprawie możliwości udostępniania danych osób przebywających na kwarantannie lub w izolatorium domowym innym organom lub podmiotom przez ośrodki pomocy społecznej na podstawie polecenia wojewody. W specustawie covidowej przewidziano bowiem, że wojewoda może wydawać polecenia obowiązujące wszystkie organy administracji rządowej działające w województwie i państwowe osoby prawne, organy samorządu terytorialnego, samorządowe osoby prawne oraz samorządowe jednostki organizacyjne nieposiadające osobowości prawnej, w związku z przeciwdziałaniem COVID-19. Polecenia podlegają natychmiastowemu wykonaniu. O wydanych poleceniach wojewoda niezwłocznie informuje właściwego ministra[241]. Prezes UODO zajął stanowisko, że takie polecenia nie mogą być podstawą do udostępnienia danych o osobach objętych kwarantanną lub przebywających w izolacji domowej.

Skoro bowiem ustawodawca zadecydował, jakie podmioty są uprawnione do udostępniania im danych o osobach objętych kwarantanną lub przebywających w izolacji domowej, to nie można

[240] DOL.023.1067.2020.
[241] Zgodnie z art. 11 ust. 1 specustawy covidowej (Dz. U. z 2020 r. poz. 374), przepis był zmieniany, a ostatecznie został uchylony z dniem 4 września 2020 r.

dowolnie rozszerzać ani zakresu podmiotowego, ani przedmiotowego tych przepisów, chyba że poprzez dokonanie stosownych zmian legislacyjnych.

Zapytania od pracodawców związane z COVID-19

Wątpliwości pracodawców budziła przede wszystkim kwestia podstaw prawnych mierzenia temperatury ciała pracownikowi w związku z podejrzeniem zakażenia COVID-19 i dlatego Prezes UODO opublikował swoje stanowisko w tej sprawie na stronie internetowej Urzędu[242].

W ocenie Prezesa art. 17 specustawy nie wyklucza możliwości wprowadzenia przez pracodawców czy przedsiębiorców ww. rozwiązań, mających na celu zwalczanie COVID-19. Jeżeli inspektor sanitarny uzna, że niezbędne jest przyjęcie rozwiązania w postaci mierzenia temperatury pracownikom i gościom wchodzącym na teren zakładu pracy, czy też pozyskiwania od pracowników oświadczeń dotyczących ich stanu zdrowia, może skorzystać z właściwego dla niego środka prawnego. W efekcie czego na zakład pracy nałożony zostanie obowiązek w postaci decyzji o dokonywaniu pomiaru temperatury, czy też zbieraniu oświadczeń pracowników dotyczących ich stanu zdrowia. Służby sanitarne mogą również podjąć decyzję o konieczności dokonywania pomiarów temperatury ciała interesantów, którzy wchodzą do budynku w celu załatwienia sprawy.

Wszelkie działania, jakie będzie podejmował inspektor sanitarny oraz podmioty, na które będzie on oddziaływał, będą wynikały z przepisów prawa, które regulują jego działania oraz z ww. decyzji, wytycznych oraz zaleceń – czyli uprawnień wynikających ze specustawy. Środki te będą stanowiły podstawę prawną tych działań, w tym podstawę do przetwarzania danych osobowych dotyczących stanu zdrowia.

Organ nadzorczy wyraźnie zaznaczył, że w kwestii dotyczącej podejmowania działań związanych z przeciwdziałaniem COVID-19 w miejscu pracy, podstawą legalizującą przetwarzanie danych dotyczących zdrowia w sektorze zatrudnienia, a zatem w relacji pracodawca – pracownik oraz w relacji z podmiotem publicznym, nie może być art. 9 ust. 2 lit. a RODO, tj. zgoda osoby, której dane dotyczą. Wynika to wprost z ogólnego rozporządzenia o ochronie danych, które wskazuje, że zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą a administratorem. W szczególności, gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich

[242] https://uodo.gov.pl/pl/138/1516

przypadkach. W relacji pracodawca – pracownik również występuje nierówność tych dwóch podmiotów. Pracodawca nie może nakazać pracownikom i gościom wchodzącym na teren zakładu pracy, dokonywania pomiaru temperatury. W każdym przypadku musi wykazać podstawę prawną, która dawałaby takie uprawnienie. Podkreślił, że przepisy prawa nie regulują, jaka wysokość temperatury daje podstawę do stwierdzenia, że pracownik jest chory bądź zarażony wirusem COVID-19. To służby sanitarne, a nie pracodawca, podejmując określone działania, wskazują w konkretnych przypadkach na przyjmowanie właściwych rozwiązań. Podkreślił przy tym, że rozwiązania przyjmowane przez przedsiębiorców, pracodawców i inne podmioty będą legalne jedynie w sytuacji, gdy administrator będzie realizował je na podstawie przepisów prawa – zgodnie z zasadą legalności określoną w art. 5 ust. 1 RODO.

Dokumentacja papierowa zawierająca dane osobowe a praca zdalna

Wobec pojawiających się pytań dotyczących możliwości wykorzystywania przez pracowników świadczących pracę zdalną dokumentacji papierowej zawierającej dane osobowe, Prezes UODO udostępnił na stronie internetowej Urzędu podstawowe zasady, którymi należy się w takiej sytuacji kierować[243].

Przypomniał pracodawcom, że to oni, jako administratorzy danych przetwarzanych przez pracowników podczas pracy zdalnej, mają obowiązek zapewnić przestrzeganie zasad przetwarzania danych, w tym zagwarantować ich bezpieczeństwo, biorąc pod uwagę większe ryzyko związane z takimi działaniami. Odnosi się to zarówno do przetwarzania danych przy wykorzystaniu środków komunikacji elektronicznej, jak i danych zawartych w dokumentach papierowych. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych oraz muszą zapewnić ich bezpieczeństwo, przestrzegając wewnętrznych polityk oraz innych procedur przyjętych w tym zakresie przez pracodawcę. Na pracownikach spoczywa również ogólny obowiązek dbałości o dobro zakładu pracy w zakresie ochrony danych osobowych.

O ile Kodeks pracy wprost reguluje niektóre kwestie dotyczące ochrony danych osobowych w ramach wykonywania telepracy, o tyle żadne przepisy szczególne nie określają odrębnych wymogów ochrony danych osobowych podczas pracy zdalnej. Dlatego pracodawca, kierując do niej pracownika, musi zapewnić zgodność z ogólnymi przepisami RODO dotyczącymi ochrony

[243] https://uodo.gov.pl/pl/138/1513

i bezpieczeństwa danych osobowych. W tym celu powinien wdrożyć odpowiednie procedury oraz środki organizacyjne i techniczne tak, aby pracownicy mieli wystarczającą świadomość i narzędzia umożliwiające im przestrzeganie przepisów o ochronie danych osobowych.

Jednocześnie organ nadzorczy opublikował w newsletterze UODO dla IOD[244] pomocne dla pracodawców materiały informacyjne zawierające wskazówki i porady, dotyczące bezpieczeństwa danych osobowych podczas pracy poza biurem.

Przetwarzanie danych osobowych w aplikacji ProteGo Safe

Na prośbę Ministra Cyfryzacji, a następnie Kancelarii Prezesa Rady Ministrów, Prezes UODO opiniował kolejne wersje dokumentacji aplikacji ProteGo Safe (a następnie w zmienionej nazwie STOP COVID ProteGo Safe), tj. regulamin i politykę prywatności[245]. Była to aplikacja, dzięki której użytkownik mógł bezpłatnie otrzymywać wsparcie w profilaktyce i zapobieganiu zarażeniu, informacje związane z pandemią COVID-19, w tym o bieżącym statusie powiatu (status żółty lub czerwony) oraz przypomnienia dotyczące bezpiecznych zachowań i nawyków codziennej higieny. W jej regulaminie można była przeczytać, że aplikacja ta ma przekazywać użytkownikom informacje i wytyczne WHO oraz GIS, ale przekazywane informacje nie mają charakteru konsultacji medycznej lub świadczenia zdrowotnego (w tym w szczególności medycznego lub farmaceutycznego).

W toku korespondencji prowadzonej w związku z kolejnymi wersjami tej aplikacji, Prezes UODO wskazywał na liczne zagrożenia, jakie wiążą się z budową i funkcjonowaniem takich rozwiązań. Już w pierwszych pismach w tej sprawie podnosił, że problematyka wykorzystywania aplikacji w walce z pandemią wywołaną zarażeniami wirusem SARS-CoV-2 jest przedmiotem szczególnego zainteresowania zarówno poszczególnych krajowych organów do spraw ochrony danych osobowych, jak i Europejskiej Rady Ochrony Danych oraz Komisji Europejskiej, czego wyrazem są m.in. wypracowane przez te instytucje dokumenty[246].

Powołując się na ww. dokumenty, Prezes UODO zgłaszał swoje zastrzeżenia, co do określenia administratora tej aplikacji oraz statusu prawnego podmiotów współdziałających. Wskazywał m.in., że Komisja Europejska w Wytycznych dotyczących aplikacji pomocnych w walce z pandemią

[244] Newsletter UODO dla IOD nr 4/2020.
[245] DOL.023.585.2020.
[246] Komunikat Komisji Europejskiej – Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych (Dz. Urz. UE C 124I z 17.04.2020, str. 1; Wytyczne 04/2020 o wykorzystaniu geolokalizacji i innych narzędzi ustalania kontaktów w kontekście wybuchu epidemii COVID-19, wydane przez Europejską Radę Ochrony Danych dnia 21 kwietnia 2020 r., dostępne na stronie internetowej https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contac.

COVID-19, w odniesieniu do ochrony danych wyraźnie opowiedziała się za tym, by za przesłankę dopuszczalności przetwarzania danych osobowych w aplikacji przyjąć przesłankę zgody, o której mowa w art. 6 ust. 1 lit. a oraz art. 9 ust. 2 lit. a RODO. Ponadto w wydanych przez EROD Wytycznych 04/2020 o wykorzystaniu geolokalizacji i innych narzędzi ustalania kontaktów w kontekście wybuchu epidemii COVID-19 wyrażono pogląd, że stosowanie aplikacji umożliwiających śledzenie kontaktów zakaźnych powinno być dobrowolne i nie powinno opierać się na śledzeniu przemieszczania się poszczególnych osób, lecz na informacjach o bliskości użytkowników.

Organ zwrócił także uwagę na konieczność prawidłowego wykonywania przez administratora obowiązku informacyjnego z art. 13 RODO wobec osób, które są dotychczasowymi użytkownikami kolejnych wersji aplikacji ProteGO Safe. Wskazywał, że osoby te powinny być w sposób przejrzysty informowane o przysługujących im prawach wynikających z RODO, tak aby ich zgoda na przetwarzanie danych osobowych była świadoma i dobrowolna – zgodnie z art. 4 pkt 11 RODO.

W swojej opinii Prezes UDOO wskazał projektodawcom aplikacji również na konieczność przeprowadzenia oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO. Powinna ona dokumentować z wyprzedzeniem, jaki jest cel wykorzystania danych i identyfikować zagrożenia, jakie może spowodować wykorzystanie danych przez tę aplikację.

Na skutek zgłaszanych przez Prezesa UODO uwag, projektodawcy aplikacji dokonywali zmian w regulaminie i polityce prywatności, jednak nie wszystkie sugestie organu nadzoru zostały uwzględnione. Przykładowo za podstawę prawną przetwarzania danych osobowych użytkowników przez administratora uznano nie przesłankę zgody – na którą wskazywał Prezes UODO – lecz interes publiczny polegający na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 (art. 6 ust. 1 lit. e RODO), a także realizację zadania publicznego polegającego na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego (art. 9 ust. 2 lit. i RODO). Wskutek uwag organu nadzorczego dla zmodyfikowanej aplikacji STOP COVID ProteGo Safe dokonana została natomiast ocena skutków dla ochrony danych, a w jej regulaminie i polityce prywatności uwzględniono postanowienia dotyczące dezaktywacji tej aplikacji po zakończeniu pandemii, o co organ wnosił w prowadzonej w tej sprawie korespondencji.

Mimo tych działań, w kolejnym z pism Prezes UODO wskazał, że ocena skutków dla ochrony danych, oprócz odniesienia się do spełnienia wymogów prawnych, powinna wziąć pod uwagę

spełnienie norm dotyczących bezpieczeństwa informacji PN-EN ISO/IEC 27001 oraz ISO/IEC 27002, które określają wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądaniem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Ponadto warto zastanowić się nad wdrożeniem standardu PN-EN ISO 22301, który może przyczynić się do zwiększenia prawdopodobieństwa skutecznego przeciwdziałania zagrożeniom (takim jak nieautoryzowane czynności na urządzeniu z włączonym Bluetoothem czy deanonimizacja i odtworzenie mapy powiązań społecznych) oraz PN-ISO/IEC 29151, która określa praktyczne zasady dotyczące wdrożenia zabezpieczeń, w celu spełnienia wymagań zidentyfikowanych w trakcie szacowania ryzyka i oceny skutków związanych z ochroną informacji o identyfikowalnych osobach. Podkreślił, że ze względu na wrażliwy charakter danych oraz cele ich przetwarzania aplikacja wymaga wdrożenia odpowiednich procedur oraz zapewnienia zgodności podejmowanych działań przy przetwarzaniu informacji nie tylko z wymogami prawnymi, ale również z zasadami określonymi w normie ISO/IEC 29100.

Prezes zaznaczył też, że ocena skutków dla ochrony danych powinna być w razie potrzeby powtarzana i aktualizowana, szczególnie ze względu na dynamiczne zmiany, jakie towarzyszą realizacji ww. projektu.

Możliwość przesyłania przez przedsiębiorców telekomunikacyjnych do wjeżdżających do Polski użytkowników telefonów komórkowych komunikatów związanych z rozprzestrzenianiem się wirusa COVID–19

W odpowiedzi na to pytanie skierowane do UODO przez **Ministra Cyfryzacji**[247], Prezes UODO wydał opinię, że w niniejszej sprawie powinny mieć zastosowanie przepisy ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[248], w szczególności jej art. 21a, który wskazuje na obowiązek wysyłania komunikatów o zagrożeniu wystąpieniem sytuacji kryzysowej przez operatorów sieci telekomunikacyjnej, na żądanie dyrektora Rządowego Centrum Bezpieczeństwa. Ponadto w rozporządzeniu Rady Ministrów z dnia 7 grudnia 2018 r. w sprawie współpracy dyrektora Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w celu powiadamiania użytkowników końcowych o zagrożeniu[249], uregulowano procedurę, na podstawie której komunikat związany z rozprzestrzenianiem się koronawirusa może być przesłany

[247] DOL.023.208.2020.
[248] Dz. U. z 2019 r. poz. 1398 z późn. zm.
[249] Dz. U. z 2018 r. poz. 2309.

do użytkowników telefonów komórkowych. Dlatego w opinii organu nadzorczego, przy zachowaniu ścisłych procedur wynikających z ww. aktów prawnych, przesyłanie takich komunikatów nie będzie naruszać przepisów RODO.

Zapytania dotyczące monitoringu wizyjnego

Wykorzystywanie monitoringu wizyjnego zarówno przez podmioty publiczne, jak i prywatne jest przedmiotem szczególnego zainteresowania Prezesa Urzędu Ochrony Danych Osobowych.

Stosowanie tego narzędzia może bowiem stanowić szczególne zagrożenie dla prawa do prywatności wielu osób, często nieinformowanych o objęciu ich tego rodzaju nadzorem. W 2020 r. problematyka ta pojawiała się w pytaniach wielu podmiotów, takich jak **apteki, hospicja, żłobki**, ale także w korespondencji od osób fizycznych zainteresowanych zastosowaniem monitoringu na ich **prywatnej posesji**.

Prezes UDOO wskazywał, że Europejska Rada Ochrony Danych 10 lipca 2019 r. przyjęła Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo, które mają na celu wyjaśnienie, w jaki sposób rozporządzenie 2016/679 ma zastosowanie do przetwarzania danych osobowych w przypadku korzystania z urządzeń wideo oraz zapewnienie jego spójnego stosowania w tym zakresie. Informacje te, a także Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, zostały zamieszczone na stronie internetowej Urzędu[250].

Odpowiadając na pismo **Śląskiej Izby Aptekarskiej** (przesłane również do wiadomości Rzecznika Praw Pacjenta)[251] w sprawie możliwości prowadzenia w izbach ekspedycyjnych aptek ogólnodostępnych nagrań audiomonitoringu (monitoringu rejestrującego dźwięk), organ nadzorczy wskazał, że przepisy odnoszące się do monitoringu – przepisy prawa pracy oraz przepisy dotyczące działalności leczniczej – nie zezwalają co do zasady na nagrywanie dźwięku.

Zainstalowanie systemu monitoringu rejestrującego dźwięk w aptece może prowadzić do przetwarzania wielu danych osobowych, w tym zwłaszcza danych dotyczących zdrowia, które zgodnie z RODO powinny zostać objęte większą (szczególną) ochroną. Zatem stosowanie audiomonitoringu może, w przypadkach nieuregulowanych przepisami prawa, zostać uznane za naruszenie prywatności oraz nadmiarową formę przetwarzania danych, a co za tym idzie wiązać się z odpowiedzialnością nie tylko administracyjną i cywilną, ale również karną. Jednocześnie organ

[250] https://uodo.gov.pl/pl/3/1343
[251] DOL.023.1399.2020.

nadzorczy zaznaczył, że w celu zwiększenia bezpieczeństwa można rozważyć wprowadzenie innych rozwiązań, mniej ingerujących w prywatność.

Podobne stanowisko Prezes UODO zajął w sprawie możliwości zastosowania monitoringu w **hospicjach**[252], do których mają zastosowanie przepisy ustawy o działalności leczniczej. Przepisy te nie przewidują możliwości monitorowania pomieszczeń w formie dźwiękowej. Potrzeba zapewnienia bezpieczeństwa, w tym również przestrzegania praw pacjenta, nie może nie uwzględniać prawa do prywatności i godności personelu medycznego i pacjentów. Prezes UODO odwołał się także do motywu 35 RODO, zgodnie z którym do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie jej zdrowia fizycznego lub psychicznego. Ogólne rozporządzenie również w motywie 53 wskazuje, że szczególne kategorie danych osobowych, zasługujące na większą ochronę, powinny być przetwarzane do celów zdrowotnych wyłącznie w przypadkach, gdy jest to niezbędne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa.

W niektórych obszarach kwestia stosowania monitoringu wizyjnego została uregulowana w przepisach prawa, które określają, w jakich celach, na jakich zasadach i w jakich pomieszczeniach może być wykorzystywany monitoring wizyjny (np. kodeks pracy, prawo oświatowe). Brak jest natomiast aktu prawnego, który kompleksowo regulowałby kwestię wykorzystywania monitoringu wizyjnego w **placówkach sprawujących opiekę nad dziećmi do lat 3.** Natomiast w praktyce monitoring taki bywa stosowany i regulowany jedynie w przepisach wewnętrznych danej placówki (np. w regulaminach). Tym samym zasady wykorzystywania nagrań z monitoringu nie są jednolite i budzą wiele wątpliwości. Dlatego wśród zgłaszanych organowi problemów pojawiła się kwestia dostępu rodziców dzieci do nagrań z monitoringu w związku z podejrzeniem popełnienia przestępstwa przez jedną z **opiekunek żłobka.**

W związku z tym zagadnieniem organ nadzorczy dostrzegł potrzebę stworzenia przepisów prawa, które określiłyby zasady wykorzystywania monitoringu wizyjnego w opiece nad dziećmi do lat 3, w tym m.in.: obszary w placówkach, które mogłyby zostać objęte monitoringiem, cel wykorzystywania monitoringu czy okres przechowywania zgromadzonego z nagrań materiału. W tym celu Prezes UODO wystąpił do Ministra Rodziny, Pracy i Polityki Społecznej z wnioskiem o rozważenie uregulowania w ustawie z dnia 4 lutego 2011 r. o opiece nad dziećmi do lat 3 kwestii

[252] DOL.023.283.2020.

stosowania monitoringu wizyjnego przez podmioty sprawujące nad nimi opiekę[253]. W odpowiedzi na to wystąpienie Minister Rodziny, Pracy i Polityki Społecznej zgodził się z koniecznością uregulowania tej kwestii.

Z kolei odnosząc się do pytań osób fizycznych stosujących monitoring na swojej **prywatnej posesji,** organ nadzoru zwracał uwagę na konieczność oceny, czy zasięgiem kamer nie jest obejmowany również teren, który nie jest przestrzenią prywatną. Jeśli tak jest, wówczas powinny być stosowane zasady ogólne określone w RODO, a wobec osób nagrywanych, zgodnie z zasadą przejrzystości, powinien być spełniany obowiązek informacyjny.

Prezes UODO przypominał w tym kontekście wyrok Europejskiego Trybunału Sprawiedliwości (ETS) w sprawie Ryneš[254], dotyczący wykorzystywania systemu kamer przechowującego zapis obrazu osób na sprzęcie nagrywającym w sposób ciągły, takim jak dysk twardy, zainstalowany przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu. W wyroku tym uznano, że jeżeli system monitoruje również przestrzeń publiczną, nie stanowi przetwarzania danych o czysto osobistym lub domowym charakterze. Oznacza to, że nagrywanie przestrzeni poza prywatną działką musi być zgodne z RODO, a w konsekwencji konieczne będzie realizowanie obowiązków informacyjnych, rozpatrywanie żądań osób obserwowanych i właściwe zabezpieczanie nagrań.

W celu usystematyzowania i upowszechnienia podstawowych informacji na temat korzystania z monitoringu wizyjnego na prywatnych posesjach, Prezes UODO zamieścił na stronie internetowej Urzędu 10 podstawowych wskazówek w tym zakresie[255].

Przetwarzanie danych osobowych w sektorze bankowym

W związku z przygotowywanym przez Komisję Etyki Bankowej „Raportem o relacjach pomiędzy bankami a ich interesariuszami w 2019 r.", na prośbę Prezesa Związku Banków Polskich, organ nadzorczy wyrażał swoją opinię na temat problemów zgłaszanych przez klientów banków w obszarze ochrony danych osobowych[256]. Wśród nich, jako najważniejsze, wymienił brak wypełnienia wszystkich przesłanek legalizujących przetwarzanie danych osobowych przez banki w Biurze Informacji Kredytowej na podstawie art. 105a ust. 3 Prawa bankowego, czy brak

[253] DOL.413.7.2020.
[254] Wyrok Trybunału Sprawiedliwości z 11 grudnia 2014 r. w sprawie C-212/13 František Ryneš przeciwko Úřad pro ochranu osobních údajů.
[255] https://uodo.gov.pl/pl/138/1455
[256] DOL.023.1382.2020.

przejrzystości w podawaniu informacji na temat procesu przetwarzania danych osobowych klientów w biurach informacji gospodarczej, w szczególności w zakresie informowania o tym, który z podmiotów (bank czy biuro informacji gospodarczej) pełni rolę administratora, a który podmiotu przetwarzającego.

Wskazał też na pytania dotyczące kopiowania dowodów osobistych przez banki oraz na kwestie związane z realizacją praw i obowiązków wynikających z art. 70a ust. 1 Prawa bankowego, który stanowi, że wyjaśnienia dotyczące oceny zdolności kredytowej mają być udzielane na wniosek. Klienci twierdzili bowiem, że banki nie informują ich szczegółowo o powodach odmowy udzielenia im pożyczki lub kredytu.

Wśród zgłaszanych Prezesowi UODO zagadnień znalazło się również przetwarzanie danych osobowych klientów w celach marketingowych, mimo niewyrażenia zgody bądź złożenia sprzeciwu wobec takiego przetwarzania, przesyłanie korespondencji bankowej do niewłaściwej osoby (np. błędny adres, błędne dane osobowe), zaciąganie zobowiązań pieniężnych przy użyciu skradzionych danych oraz brak realizacji przez instytucje bankowe obowiązków informacyjnych wynikających z art. 13, 14 i 15 RODO.

Administrator w procesie badań klinicznych

Wyjaśniając wątpliwości dotyczące ról podmiotów biorących udział w badaniu klinicznym, Prezes UODO zwrócił uwagę, że na gruncie polskich przepisów prawa, badacza i ośrodek badawczy oraz sponsora należy zakwalifikować jako odrębnych administratorów w rozumieniu art. 4 pkt 7 RODO, jednak wyłącznie w zakresie danych osobowych, w stosunku do których są w stanie określić niezależnie od siebie cele oraz sposoby przetwarzania.

Istotne jest jednak to, czy badacz jest odrębnym podmiotem, który decyduje o celach i sposobach przetwarzania danych, czy też jest osobą zatrudnioną w ośrodku badawczym (czyli pracownikiem ośrodka). W sytuacji, kiedy badacz jest zatrudniony w ośrodku badawczym, to administratorem jego danych oraz danych, które on przetwarza prowadząc badanie kliniczne na podstawie zawartej umowy, jest ośrodek badawczy. Wówczas w badaniu klinicznym wyodrębnić należy dwóch administratorów, tj. sponsora i ośrodek badawczy.

W swojej opinii Prezes UODO odwołał się do przepisów ustawy Prawo farmaceutyczne, które wskazują, że sponsor badania jest odpowiedzialny za podjęcie, prowadzenie i finansowanie badania klinicznego. To on decyduje zatem o celach i sposobach przetwarzania danych osobowych uczestników badania klinicznego. Zgodnie natomiast z rozporządzeniem w sprawie Dobrej Praktyki

Klinicznej, sponsor zawiera z badaczem i z ośrodkiem badawczym pisemne umowy dotyczące prowadzenia badania klinicznego. Taka umowa, zawarta między sponsorem a badaczem, zobowiązuje strony w szczególności do umożliwienia dostępu do dokumentów źródłowych przedstawicielom sponsora oraz ochrony danych osobowych uczestników badania klinicznego, uzyskanych w związku z prowadzeniem tego badania. Zdaniem organu nadzorczego, w sytuacji, gdy ośrodek badawczy przetwarza dane osobowe uczestników badania i decyduje – niezależnie od sponsora – o celach oraz sposobach przetwarzania danych osobowych uczestników badania oraz wykorzystuje wyniki przeprowadzonych badań do celów naukowych, innych badań czy też np. publikacji, należy uznać go za odrębnego administratora danych osobowych uczestników badania klinicznego.

Jednocześnie Prezes UODO wskazał, że do kwestii badań klinicznych w kontekście RODO odnosi się też opublikowana 23 stycznia 2019 r. Opinia EROD nr 3/2019 w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK) a ogólnym rozporządzeniem o ochronie danych (art. 70 ust. 1 lit. b).

Wątpliwości dotyczące pojęcia „odbiorca danych”

W roku 2020 do organu nadzorczego wpływały też – zarówno od podmiotów publicznych, jak i prywatnych – pytania świadczące o trudnościach w ustaleniu, kogo należy uznać za odbiorcę danych.

W jednym z takich pism **Ministerstwo Edukacji Narodowej** zwróciło się do Prezesa UODO o opinię, czy osoba fizyczna, której ujawniono dane innej osoby fizycznej (w wyniku błędu, którego konsekwencją było naruszenie ochrony danych osobowych) jest odbiorcą w rozumieniu art. 4 pkt 9 RODO, a w konsekwencji, czy można informacje o niej przekazać podczas spełniania obowiązku informacyjnego z art. 15 RODO oraz w ramach realizacji obowiązku poinformowania o naruszeniu osoby, której dane dotyczą.

Organ nadzorczy wyjaśnił[257], że w przypadku wystąpienia naruszenia ochrony danych osobowych (incydentu), polegającego na ujawnieniu (udostępnieniu) danych osobowych nieuprawnionej osobie, takiej osoby nie należy uznawać za odbiorcę danych. Osoba, której w sposób nieuprawniony ujawniono dane osobowe innej osoby, to strona trzecia w rozumieniu art. 4 pkt 10 RODO. Wobec tego administrator nie jest uprawniony do podawania danych takich osób w ramach

[257] DOL.023.288.2020.

wykonywania obowiązku z art. 15 RODO. Sama definicja odbiorcy danych określona w art. 4 pkt 9 RODO odnosi się jedynie do odbiorców legalnych, czyli takich, którym ujawnia się lub którym zostaną ujawnione dane osobowe zgodnie z RODO i innymi przepisami. Definicja odbiorcy nie jest tożsama z definicją podmiotu nieuprawnionego, tzn. podmiotu, któremu w sposób niezgodny z prawem ujawniono dane. Organ nadzorczy uznał także, że co do zasady administrator nie powinien udostępniać osobie, której dotknęło naruszenie, danych osobowych osoby fizycznej, której bezprawnie ujawniono dane. Niemniej nie można w sposób kategoryczny wykluczyć, że w niektórych przypadkach incydentów udostępnienia danych – podanie osobie, której dane dotyczą informacji o konkretnym podmiocie/osobie fizycznej, której bezprawnie ujawniono dane – pozwoli na skuteczną ochronę swoich interesów, które mogą być zagrożone poprzez powstały incydent. Dlatego w zależności od charakteru naruszenia oraz oceny skutków dla ochrony danych osoby, której dane zostały ujawnione w sposób nieuprawniony, administrator powinien przeprowadzić taką ocenę indywidualnie. Wskazuje na to art. 34 ust. 2 RODO, który wymienia minimalny zakres informacji, które należy podać w zawiadomieniu w przypadku możliwości wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (przy uwzględnieniu wyłączeń z art. 34 ust. 3 RODO).

Z kolei jeden z podmiotów prywatnych miał problem z ustaleniem, czy w rejestrze czynności przetwarzania danych należy wpisywać **komornika** jako podmiot, któremu dane zostały ujawnione. Odniósł się przy tym do stanowiska Prezesa UODO zawartego w newsletterze UODO dla Inspektorów Ochrony Danych[258], zgodnie z którym komornik nie jest odbiorcą danych. W odpowiedzi[259] organ wskazał, że informacje, które ma zawierać rejestr czynności przetwarzania danych osobowych określa art. 30 RODO, zaś art. 4 pkt 9 RODO zawiera definicję odbiorcy, zgodnie z którą organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców. Skoro komornik sądowy jest organem egzekucyjnym, którego działania są określone przepisami prawa (ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego oraz ustawa z dnia 22 marca 2018 r. o komornikach sądowych), to nie należy traktować go jako odbiorcy danych w rozumieniu RODO. Tym samym Prezes UODO potwierdził stanowisko zaprezentowane w newsletterze. Jednocześnie wskazał, że zarówno przy realizacji prawa dostępu osoby do dotyczących jej danych, o którym mowa w art. 15 RODO, jak i realizując obowiązek prowadzenia

[258] Newsletter UODO dla IOD Nr 9/2020 z września 2020 r.
[259] DOL.023.1866.2020.

rejestru czynności przetwarzania danych (art. 30 RODO), administrator nie musi wskazywać komornika jako podmiotu, któremu dane zostały udostępnione.

Inne zagadnienia

Jak już zostało wskazane, zakres tematyczny pytań prawnych kierowanych do Prezesa UODO przez administratorów i osoby fizyczne, dotyczył różnych aspektów przetwarzania danych osobowych oraz stosowania nie tylko RODO, ale także innych, szczególnych przepisów prawa.

Podobnie jak w latach ubiegłych Prezes UODO otrzymywał pytania związane z **udostępnianiem informacji publicznej.** Wśród nich pojawiły się te dotyczące usuwania z Biuletynu Informacji Publicznej danych osobowych, pozyskanych w związku z prowadzonymi naborami na wolne stanowiska pracy w Służbie Cywilnej[260], jak również takie, czy **wynagrodzenie nauczycieli stanowi informację publiczną i w jakim zakresie można ją ujawnić**[261]. **Wątpliwości zgłaszali także przedsiębiorcy, których dane ujawniono w związku z korzystaniem ze środków publicznych w ramach tarczy antykryzysowej**[262].

Prezes UODO przypominał, że sądy administracyjne wielokrotnie wypowiadały się w kwestii zasadności udostępnienia w trybie dostępu do informacji publicznej danych kontrahentów, którzy podpisywali z organami publicznymi umowy cywilnoprawne dotyczące korzystania ze środków publicznych, przyznając wnioskującym prawo do ich pozyskania[263].

Reakcją na wpływające pytania były również zamieszczone na stronie internetowej Urzędu stanowiska dotyczące przetwarzania danych pracowników zawartych w orzeczeniach o niepełnosprawności[264] czy rejestracji czasu pracy za pomocą danych biometrycznych[265]. Z kolei w związku z pytaniami od przedsiębiorców organ nadzorczy wyjaśniał, kiedy i na jakich zasadach **instytucje państwowe, takie jak Zakład Ubezpieczeń Społecznych (ZUS) czy Państwowa Inspekcja Pracy (PIP),** mogą mieć wgląd do akt osobowych pracowników[266]**.**

Mimo że od wielu lat organ nadzorczy konsekwentnie wyraża swoje stanowisko w sprawie przetwarzania danych osobowych przez firmy windykacyjne, nadal pojawiały się wątpliwości w tej

[260] DOL.023.1345.2020.
[261] DOL.023.97.2020.
[262] DOL.023.1326.2020.
[263] np. wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z 6 listopada 2019 r. sygn. akt IV SAB/Wr 167/19 czy wyrok Naczelnego Sądu Administracyjnego z 23 listopada 2016 r. sygn. akt I OSK 2606/15.
[264] https://uodo.gov.pl/pl/138/1639
[265] https://uodo.gov.pl/pl/138/1521
[266] https://uodo.gov.pl/pl/138/1628

kwestii. Przykładowo, zgłosił je **Rzecznik Małych i Średnich Przedsiębiorców,** pytając w jakich sytuacjach konieczne jest zawarcie umowy powierzenia przez firmy windykacyjne na podstawie RODO[267].

Podobnie jak w latach ubiegłych, wpływały również pytania **od spółdzielni i wspólnot mieszkaniowych,** dotyczące m.in. stosowania monitoringu, zawierania umów powierzenia czy upubliczniania korespondencji organów na stronach internetowych.

Z kolei **organizacje związkowe** występowały do organu z prośbą o wyjaśnienie kwestii spornych wynikłych podczas negocjacji regulaminu pracy w zakresie identyfikatorów pracowniczych, wyrażenia zgody na dodatkowe zatrudnienie, monitoringu pracowniczego, w tym stosowania GPS w samochodach.

W **jednostkach samorządu terytorialnego** pojawiały się wątpliwości związane z wydawaniem upoważnień dla pracowników jednostek organizacyjnych tzw. jednostek obsługujących czy zasadności podpisania umowy powierzenia przetwarzania danych pomiędzy powiatem a jego jednostką organizacyjną, np. urzędem pracy. Udzielając wyjaśnień, Prezes UDOO przypominał, że na podstawie art. 37 ust.1 lit. a RODO, administrator jest zobowiązany do wyznaczenia inspektora ochrony danych w przypadku, kiedy administrator jest organem lub podmiotem publicznym. Inspektor taki powinien poddać analizie opisaną sytuację i przedstawić opinię, która powinna być pomocna w powyższej sprawie.

13.1.2. Pytania prawne od inspektorów ochrony danych

Rola inspektorów ochrony danych ma fundamentalne znaczenie dla budowy systemu skutecznej ochrony danych osobowych, co organ nadzorczy niezmiennie podkreśla w swoich stanowiskach i wypowiedziach. Docenia też rolę inspektorów jako punktu kontaktowego oraz pośrednika pomiędzy administratorem i organem nadzorczym.

W celu zapewnienia skuteczności wywiązywania się z tej roli, kontakt organu i IOD powinien być zapewniony w obu kierunkach. Rola organu w tym zakresie polegała w szczególności na udzielaniu inspektorom konsultacji i porad w stosownych przypadkach. Inspektorzy chętnie korzystali z tej formy współpracy, czego wyrazem były kierowane do UODO liczne pytania informujące o problemach napotkanych przez nich w codziennej pracy. Wspieranie inspektorów

[267] DOL.023.895.2020.

realizowane było również poprzez zamieszczanie skierowanych do nich materiałów na stronie internetowej UODO, w szczególności poprzez bieżące wzbogacanie zakładki „Inspektor Ochrony Danych" oraz zamieszczanie komunikatów i wytycznych, a także poprzez wydawanie newslettera, czy prowadzenie szkoleń.

Jak już wskazano, w 2020 r. do UODO wpłynęło **338 pytań od inspektorów ochrony danych**. A zatem można zaobserwować tendencję spadkową w stosunku do ubiegłego roku, kiedy to wpłynęło ich o 191 więcej. Spadek ten mógł być spowodowany tym, że wiele kwestii związanych z właściwym stosowaniem przepisów dotyczących ochrony danych osobowych zostało wyjaśnionych m.in. w materiałach zamieszczonych na stronie internetowej UODO, w tym w specjalnej zakładce dedykowanej inspektorom, a także w newsletterze UODO dla IOD. Te udzielone w poprzednich latach wyjaśnienia, będące odpowiedziami na pytania inspektorów, niejednokrotnie wskazywały kierunek i zasady interpretacji przepisów, mogły posłużyć również jako wskazówki dla rozstrzygania nowych pojawiających się wątpliwości.

Pytania przesyłane przez inspektorów są dla organu nadzorczego bardzo ważne, ponieważ pochodzą od osób, które na co dzień mierzą się ze stosowaniem przepisów o ochronie danych osobowych. Dają one wiedzę na temat funkcjonowania rozwiązań wymaganych tymi przepisami w praktyce i pozwalają spojrzeć na te regulacje z punktu widzenia administratora, podmiotu przetwarzającego, czy też inspektora ochrony danych.

W 2020 r. do najczęściej poruszanych lub szczególnie interesujących zagadnień, na które zwrócili uwagę inspektorzy w przesłanych do Urzędu pytaniach i które były przedmiotem analiz organu, należą (oprócz tych wskazanych wyżej) takie kwestie, jak:

1) przekazywanie danych do państw trzecich w związku z wyrokiem TSUE w sprawie Schrems II,
2) określanie statusu podmiotów w procesie przetwarzania danych osobowych,
3) przetwarzanie danych osobowych osób reprezentujących osoby prawne,
4) status i zadania inspektora ochrony danych.

Przetwarzania danych osobowych podczas pandemii COVID-19 – wątpliwości IOD

W związku z podejmowaniem działań mających na celu ograniczenie i złagodzenie skutków pandemii COVID-19, wielu IOD kierowało do Prezesa UODO szczegółowe pytania z tym związane.

Przykładem może być pytanie: **Czy w związku z wymaganiami Głównego Inspektora Sanitarnego rzeczywiście należy odbierać zgody od osób na przekazywanie ich danych osobowych ośrodkom pomocy społecznej oraz innym podmiotom uczestniczącym w udzielaniu pomocy**[268]**?**

Zgodnie z informacjami zawartymi w pytaniu inspektora chodziło o działania podejmowane w celu zapewnienia pomocy osobom w podeszłym wieku, samotnym, niepełnosprawnym, na które nakładana jest decyzja o kwarantannie.

W odpowiedzi organ nadzoru odwołał się do wskazanych wyżej oświadczeń Prezesa UODO oraz EROD. W pierwszym z dokumentów wskazano m.in., że przepisy o ochronie danych osobowych nie mogą być stawiane jako przeszkoda w realizacji działań w związku z walką z koronawirusem. Z kolei EROD podniosła, że RODO jest obszernym aktem prawnym, który zawiera przepisy mające zastosowanie również do przetwarzania danych osobowych w takim kontekście, jak ten dotyczący COVID-19. RODO pozwala właściwym organom ds. zdrowia publicznego i pracodawcom na przetwarzanie danych osobowych w kontekście epidemii, zgodnie z prawem krajowym i na określonych w nim warunkach. Na przykład, gdy przetwarzanie danych jest konieczne ze względu na istotny interes publiczny w dziedzinie zdrowia publicznego. W tych okolicznościach nie ma potrzeby polegania na zgodzie osób fizycznych. EROD wskazała, że art. 6 i art. 9 RODO umożliwiają przetwarzanie danych osobowych, w szczególności gdy wchodzą one w zakres mandatu prawnego organu publicznego przewidzianego w ustawodawstwie krajowym oraz warunków wskazanych w RODO.

Prezes UODO wskazał, że w przedstawionej sytuacji pozyskiwanie zgody od osób, których dane dotyczą, może budzić uzasadnione wątpliwości. Właściwymi podstawami powinny być raczej przesłanki określone w art. 6 ust. 1 lit. c lub lit. e RODO, w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji, jak np. ustawa z dnia 5 grudnia 2008 r. o zapobieganiu i zwalczaniu zakażeń i chorób zakaźnych u ludzi, ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, ustawa z dnia 12 marca 2004 r. o pomocy społecznej czy ustawy określające zadania poszczególnych podmiotów, w tym przede wszystkim tzw. specustawa o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (z uwzględnieniem jej ostatnich zmian), która określa uprawnienia właściwych organów (tj.

[268] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1486

Głównego Inspektora Sanitarnego, Prezesa Rady Ministrów) do wydawania zaleceń i decyzji co do działań, jakie należy podejmować. Konieczne było zatem śledzenie na bieżąco wydawanych przepisów prawa.

W kontekście zadanego pytania warto zwrócić uwagę na § 2 ust. 7 rozporządzenia Rady Ministrów z dnia 31 marca 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[269]. Zgodnie z tym przepisem organy Państwowej Inspekcji Sanitarnej udostępniają dane, o których mowa w ust. 3 i 4, dotyczące osób poddanych obowiązkowej kwarantannie lub izolacji w warunkach domowych, właściwym ze względu na miejsce zamieszkania lub pobytu tych osób ośrodkom pomocy społecznej, na ich wniosek. Dopiero w sytuacji, gdy przesłanki z art. 6 ust. 1 lit. c lub lit. e nie mogłyby być zastosowane lub okazałyby się niewystarczające, a konieczne jest prowadzenie pilnych i niezbędnych działań mających na celu ratowanie zdrowia i zapobieganie rozprzestrzenianiu się epidemii, można rozważyć powołanie się na przesłankę określoną w art. 6 ust. 1 lit. d RODO, która wskazana została również w ww. oświadczeniu Prezesa UODO. Na możliwość jej zastosowania wskazuje również motyw 46 RODO, zgodnie z którym przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest to niezbędne do ochrony interesu, mającego istotne znaczenie dla życia osoby, której dane dotyczą, np. gdy przetwarzanie jest potrzebne do celów humanitarnych, w tym monitorowania epidemii i jej rozprzestrzeniania się.

Kolejne pytanie związane z pandemią koronawirusa brzmiało: **Czy wojewoda może utworzyć bazę wyników badań w kierunku wirusa SARS-CoV-2?**[270]

Co do zasady wszelkie działania podejmowane przez podmioty publiczne powinny mieć oparcie w obowiązujących przepisach prawa regulujących ich działalność. Wobec tego podstawa prawna do przetwarzania (w tym udostępniania) danych osobowych przez takie podmioty również powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami. Dane dotyczące zdrowia zaliczane są do szczególnych kategorii danych, przetwarzanie których może stanowić poważną ingerencję w sferę prywatności (a nawet intymności) osób, których dane dotyczą, lub pociągać za sobą znacznie większe zagrożenia niż przetwarzanie tzw. danych zwykłych. Dlatego administrator, pozyskując takie dane, powinien zachować szczególną staranność oraz przetwarzać jedynie takie dane, które są konieczne do realizacji celu przetwarzania.

[269] Rozporządzenie weszło w życie 31 marca 2020 r.
[270] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1553

Rozważane w przedstawionym pytaniu przedsięwzięcie dotyczyło utworzenia przez wojewodę bazy zawierającej dane osobowe osób poddanych badaniu w kierunku SARS-CoV-2 oraz wyników tych badań (imienia i nazwiska, numeru PESEL, wyniku badania, daty pobrania materiału, wieku, adresu, telefonu). Informacje te wojewoda pozyskiwałby od laboratoriów prowadzących badania w kierunku SARS-CoV-2 na terenie województwa, a następnie udostępniał, np. podmiotom leczniczym, szpitalom, stacjom ratownictwa medycznego.

Administrator rozważał możliwość przyjęcia za podstawę prawną do prowadzenia takiej bazy przepisów prawa zawartych w art. 14 ust. 2 pkt 1 i art. 20a ustawy o zarządzaniu kryzysowym. Zgodnie z pierwszym z powołanych przepisów, do zadań wojewody w sprawach zarządzania kryzysowego należy kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa. Natomiast zgodnie z art. 20a tej ustawy organy właściwe w sprawach zarządzania kryzysowego mają prawo żądania udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie.

Celem utworzenia takiej bazy miałoby być usprawnienie sposobu przekazywania kompleksowych informacji nt. wyników badań laboratoryjnych wykonywanych w kierunku SARS-CoV-2. Administrator nie doprecyzował jednak, dla realizacji którego z zadań spośród tych wskazanych w art. 14 ust. 2 pkt 1, niezbędne jest przetwarzanie wskazanych powyżej danych osób poddanych badaniom, ani w jakim celu i na jakiej podstawie dane te udostępniane byłyby podmiotom leczniczym.

Analiza powyższych przepisów wskazała, że słuszne były wątpliwości inspektora ochrony danych, co do uznania ich za podstawę prawną do prowadzenia takiego przetwarzania. Trudno bowiem wywieść z nich uprawnienie do utworzenia przez wojewodę bazy/rejestru zawierającego powyższe dane osobowe. Jednocześnie przypomnieć należy, że z uwagi na określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa, organ publiczny nie może domniemywać swoich kompetencji, jeśli nie wynikają one wprost z przepisu prawa. Jednocześnie pomocniczo wskazano, że zagadnienie gromadzenia oraz udostępniania informacji o osobach, u których stwierdzono COVID-19 uregulowane zostało w szczególności w rozporządzeniu Rady Ministrów z dnia 16 maja 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii oraz w rozporządzeniu Ministra Zdrowia z dnia 7 kwietnia 2020 r. w sprawie Krajowego Rejestru Pacjentów z COVID-19.

Zgodnie z przepisami pierwszego z rozporządzeń, w systemie teleinformatycznym udostępnionym przez jednostkę podległą ministrowi właściwemu do spraw zdrowia, właściwą

w zakresie systemów informacyjnych ochrony zdrowia, mogą być również przetwarzane dane innych osób podlegających obowiązkowej kwarantannie w związku z epidemią, o której mowa w § 1, a także osób podlegających izolacji w warunkach domowych, osób, w stosunku do których podjęto decyzję o wykonaniu testu diagnostycznego w kierunku SARS-CoV-2 oraz osób zakażonych tym wirusem (§ 2 pkt 4). Ponadto zgodnie z § 2 pkt 5 tego rozporządzenia dane osób, w stosunku do których podjęto decyzję o wykonaniu testu diagnostycznego w kierunku SARS-CoV-2, w tym dane zawarte w zleceniach wykonania takich testów wystawionych przez podmioty inne niż organy Państwowej Inspekcji Sanitarnej oraz wyniki tych testów, mogą być również przetwarzane w systemie teleinformatycznym stanowiącym moduł Krajowego Rejestru Pacjentów z COVID-19, prowadzonego przez Narodowy Instytut Kardiologii Stefana Kardynała Wyszyńskiego – Państwowy Instytut Badawczy w Warszawie. W kolejnych przepisach tego rozporządzenia został określony sposób udostępniania danych z powyższego systemu teleinformatycznego oraz Krajowego Rejestru Pacjentów z COVID-19.

Biorąc powyższe pod uwagę Prezes UODO wskazał, że w przedstawionej sytuacji należałoby w pierwszej kolejności dokonać analizy, czy ww. podmioty lecznicze nie są uprawnione do pozyskiwania powyższych danych z istniejących już ewidencji. Ponadto podkreślił, że zadania związane z przeciwdziałaniem COVID-19 w obecnej sytuacji muszą być realizowane przez poszczególne podmioty we współpracy z Państwową Inspekcją Sanitarną. Ponadto, jak to zostało wskazane w oświadczeniu Prezesa UODO w sprawie koronawirusa z 12 marca 2020 r., wszelkie problemy związane ze zwalczaniem i zapobieganiem rozprzestrzeniania się koronawirusa powinny być, w świetle powyższych unormowań, w pierwszej kolejności zgłaszane i wyjaśniane z GIS, jako organem właściwym w tych sprawach.

Przekazywanie danych do państw trzecich w związku z wyrokiem TSUE w sprawie Schrems II

Kolejnym zagadnieniem, z którym administratorzy musieli się zmierzyć w 2020 r. oraz którego dotyczyły pytania od inspektorów ochrony danych, było przekazywanie danych do państw trzecich w związku z wyrokiem Trybunału Sprawiedliwości UE wydanym 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems.

W wyroku tym TSUE stwierdził nieważność decyzji wykonawczej Komisji Europejskiej (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA. W konsekwencji od dnia ogłoszenia wyroku, tj. 16 lipca 2020 r., przekazywanie danych do importerów w Stanach Zjednoczonych Ameryki nie może się już odbywać na tej podstawie.

Jednocześnie TSUE potwierdził dalsze obowiązywanie decyzji Komisji Europejskiej 2010/87 w sprawie standardowych klauzul umownych (SCC) dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane, które mają siedzibę w krajach trzecich. Trybunał zastrzegł jednak, że należy zapewnić, aby prawa osób, których dane osobowe są przekazywane do państwa trzeciego na podstawie standardowych klauzul umownych ochrony danych, były chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w UE przez RODO w świetle postanowień Karty Praw Podstawowych UE.

Pytania od inspektorów ochrony danych dotyczyły przede wszystkim tego, jakie działania powinni podejmować administratorzy w związku z tym wyrokiem, czy można nadal stosować standardowe klauzule umowne, a także czy wciąż możliwe jest przekazywanie danych na podstawie wyjątków przewidzianych w art. 49 RODO.

Udzielając na nie odpowiedzi, Prezes UODO informował, że dla administratorów przekazujących dane do państw trzecich powyższy wyrok oznacza konieczność dokonania przez nich indywidualnej oceny stopnia ochrony danych zapewnianego w ramach transgranicznego przekazywania danych, która musi uwzględniać nie tylko same postanowienia umowne uzgodnione między eksporterami i importerami danych, lecz również przepisy prawa w państwie trzecim, w szczególności odnoszące się do ewentualnego dostępu organów władzy publicznej tego państwa do przekazywanych danych. Gdy w świetle dokonanej oceny poziom ochrony danych osobowych nie będzie merytorycznie równoważny z poziomem gwarantowanym w UE, przekazywanie danych może być uzależnione od zapewnienia równoważnego poziomu ich ochrony za pomocą innych środków.

Prezes UODO informował też o prowadzonych przez EROD pracach nad wskazówkami w tym zakresie. Zaznaczał, że odpowiedzi na wiele ze zgłaszanych wątpliwości znaleźć można w przyjętym przez EROD dokumencie z najczęściej zadawanymi pytaniami[271], zawierającym wstępne wyjaśnienia i wskazówki, co do stosowania instrumentów prawnych dotyczących przekazywania danych osobowych do państw trzecich, a także w przyjętych przez EROD zaleceniach w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE (przedstawionych do konsultacji społecznych), jak również

[271] Komunikat dot. przyjętego przez EROD dokumentu z najczęściej zadawanymi pytaniami zamieszczony jest pod linkiem: https://uodo.gov.pl/pl/138/1614

w zaleceniach w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, a także wskazywał, gdzie można zapoznać się z treścią tych dokumentów [272].

Organ nadzoru zwracał przy tym uwagę na konieczność spójnego podejścia do oceny skutków wyroku TSUE w całej Unii Europejskiej oraz niezbędność wspólnych działań w tym zakresie krajowych organów nadzorczych współpracujących w ramach EROD, w której pracach Prezes UODO uczestniczy[273]. Wskazywał, że informacja o efektach tych prac jest na bieżąco zamieszczana na stronie internetowej Urzędu.

Jednocześnie warto podkreślić, że Prezes UODO popiera inicjatywę Komisji Europejskiej, która 19 listopada 2020 r. przedstawiła Europejskiej Radzie Ochrony Danych projekty standardowych klauzul umownych, dotyczących m.in. przekazywania danych osobowych do państw trzecich. Zgodnie z oświadczeniem EROD[274] „*Nowe standardowe klauzule umowne zastąpią te dotyczące przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE, a które wymagały aktualizacji, aby były zgodne z wymogami RODO, a także z wyrokiem TSUE w sprawie Schrems II oraz żeby lepiej odzwierciedlały powszechne prowadzenie nowych i bardziej złożonych operacji przetwarzania, często z udziałem wielu podmiotów odbierających i przekazujących dane*”[275].

Dodatkowo warto zaznaczyć, że skutki wyroku TSUE w sprawie C-311/18 były również omawiane podczas spotkań organu nadzorczego z organizacjami zrzeszającymi przedsiębiorców[276].

---

[272] Komunikaty Prezesa UODO dot. zaleceń EROD zamieszczone zostały pod linkami: https://uodo.gov.pl/pl/185/1766 oraz https://uodo.gov.pl/pl/138/1768; Zalecenia 01/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE są zaś dostępne pod linkiem https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransfertools_pl.pdf.

[273] Komunikat Prezesa UODO w tej sprawie dostępny jest pod linkiem: https://uodo.gov.pl/pl/138/1603.

[274] Zob. link https://edpb.europa.eu/news/news/2020/european-data-protection-board-42nd-plenary-session-presentation-two-new-sets-sccs_pl.

[275] Informacje na ten temat znajdują się na stronie internetowej UODO pod adresem: https://uodo.gov.pl/pl/185/1775 oraz https://uodo.gov.pl/pl/185/1826. Dodatkowo warto zaznaczyć, że EROD i Europejski Inspektor Ochrony Danych, podczas 44. posiedzenia plenarnego EROD (14.01.2021 r.) przyjęli wspólne opinie w sprawie dwóch zestawów standardowych klauzul umownych, tj. opinię w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz opinię w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich. Standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi będą miały skutek ogólnounijny i mają na celu zapewnienie pełnej harmonizacji i pewności prawa na terenie UE, w odniesieniu do umów między administratorami a podmiotami przetwarzającymi. Więcej informacji na temat tego posiedzenia znajduje się na stronie internetowej UODO, zob. https://uodo.gov.pl/pl/185/1826.

[276] Dla przykładu, 10.11.2021 r. Prezes UODO zorganizował wideokonferencję, w której pod przewodnictwem Amerykańskiej Izby Handlowej uczestniczyło kilkudziesięciu reprezentantów zrzeszonych w niej firm. Podczas tego spotkania przedstawiciele organu nadzorczego w sposób kompleksowy omówili skutki niniejszego wyroku i przedstawili zakres dalszych działań zarówno krajowego organu nadzorczego, jak i organów UE podejmowanych w sygnalizowanej sprawie. Podobne konsultacje były prowadzone w Urzędzie Ochrony Danych Osobowych także z innymi

Określanie statusu podmiotów w procesie przetwarzania danych osobowych

W 2020 r. wiele wątpliwości inspektorów ochrony danych dotyczyło statusu podmiotów biorących udział w procesie przetwarzania danych osobowych.

Ustalenie, czy w danym przypadku mamy do czynienia z administratorem, współadministratorem czy podmiotem przetwarzającym miało kluczowe znaczenie dla wskazania, kto ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych oraz do kogo osoby, których dane dotyczą, mogą zwracać się z żądaniem realizacji swoich praw w praktyce.

Odpowiadając na dotyczące tego zagadnienia pytania inspektorów, Prezes UODO przekazywał wskazówki, które mogą być pomocne przy określaniu, kto pełni rolę administratora, a kto podmiotu przetwarzającego czy współadministratora. Przypominał, że w przypadku wątpliwości w tym zakresie warto mieć na uwadze wskazówki zawarte w wytycznych Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO[277]. Niejednokrotnie organ nadzoru, analizując konkretne przypadki, wprost wskazywał kryteria pomocne w ostatecznej ocenie statusu i cele, które determinowały określone role.

W odpowiedziach na pytania dotyczące **statusu podmiotów z sektora publicznego** akcentowana była zasada legalizmu, zgodnie z którą działania takich podmiotów muszą mieć oparcie w przepisach prawa. Wobec tego rola poszczególnych podmiotów publicznych w procesach przetwarzania wynika najczęściej z nadanych im przez prawo kompetencji lub zadań. Do uznania danego podmiotu za administratora danych potrzebna jest zatem zawsze analiza konkretnych przepisów prawa.

Natomiast w przypadku **pytań o status podmiotów prywatnych** wskazywano na decydujące znaczenie analizy stanu faktycznego, w ramach którego funkcjonują te podmioty, w tym ustalenia, jakie zadania/cele są realizowane, do którego z podmiotów one należą, a w związku z tym, który podmiot decyduje o celach przetwarzania, a który działa na zlecenie administratora i realizuje jego cele. Przy czym również i tutaj istnieje wiele przepisów prawa szczegółowo określających zadania, cele lub sposoby postępowania z danymi osobowymi w poszczególnych dziedzinach działalności zawodowej lub gospodarczej (przepisy branżowe).

interesariuszami, np. we wrześniu 2020 r. ze Związkiem Pracodawców Branży Internetowej IAB Polska i Polską Izbą Informatyki i Telekomunikacji.

[277] Komunikat Prezesa UODO w sprawie tych wytycznych dostępny jest na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/1712.

Poniżej przedstawiono przykłady pytań i odpowiedzi dotyczące statusu podmiotów z różnych sektorów.

Pytania dotyczące statusu podmiotów sektora publicznego

Który podmiot należy uznać za administratora danych przetwarzanych poza systemem EKSMON?[278]

W swoim pytaniu inspektor wskazywał m.in., że z przepisów prawa wynika, iż powiatowe zespoły ds. orzekania o niepełnosprawności są administratorami danych przetwarzanych w prowadzonych przez siebie bazach danych Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności (EKSMON). Pytał, czy powiatowy zespół jest także administratorem danych przetwarzanych poza tym systemem, czy jest nim może starosta? Czy można tutaj mówić o współadministrowaniu?

W odpowiedzi na te pytania Prezes UODO przywołał zawarte w RODO definicje „administratora"[279] oraz „współadministratorów"[280]. Wskazał, że w przypadku podmiotów realizujących zadania określone w przepisach prawa, cele, a często i sposoby przetwarzania, określone są w tych przepisach prawa. Podmioty te są zobowiązane do przetwarzania danych osobowych dla realizacji określonych prawem celów (zadań), zazwyczaj także przy użyciu wskazanych środków. Zatem o tym, czy dany organ, jednostka organizacyjna albo innego rodzaju podmiot jest administratorem, decyduje przede wszystkim rodzaj i charakter wyznaczonych im ustawowo zadań. Zatem do uznania danego podmiotu za administratora potrzebna jest zawsze analiza przepisów regulujących jego działalność.

Zadania oraz zasady funkcjonowania powiatowego zespołu ds. orzekania o niepełnosprawności określone zostały w szczególności w ustawie o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz w rozporządzeniu Ministra Gospodarki, Pracy i Polityki Społecznej w sprawie orzekania o niepełnosprawności i stopniu niepełnosprawności. Do zadań zespołu, zgodnie z powołanymi przepisami, należy przede wszystkim merytoryczne rozpatrywanie wniosków w celu wydania orzeczenia o niepełnosprawności, stopniu niepełnosprawności lub

[278] Pytanie i odpowiedź dostępne na pod linkiem: https://uodo.gov.pl/pl/225/1533.

[279] Zgodnie z art. 4 pkt 7 RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

[280] Zgodnie z art. 26 ust. 1 RODO, jeśli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni wówczas współadministratorami. W takim przypadku współadministratorzy – w drodze wspólnych uzgodnień – określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

wskazaniach do ulg i uprawnień osób posiadających orzeczenia o inwalidztwie lub niezdolności do pracy (§ 2 ww. rozporządzenia). Zgodnie z art. 6 ust. 5 powyższej ustawy zespoły orzekające o niepełnosprawności przetwarzają dane osobowe, w tym dane o stanie zdrowia, wyłącznie dla celów realizacji zadań oraz w zakresie niezbędnym do ich wykonania. Zgodnie z art. 6 ust. 6 tej ustawy zabezpieczenia przetwarzania danych osobowych przez zespoły orzekające o niepełnosprawności polegają co najmniej na dopuszczeniu do przetwarzania danych osobowych wyłącznie osób posiadających pisemne upoważnienie wydane przez administratora oraz na pisemnym zobowiązaniu osób upoważnionych do przetwarzania danych osobowych do zachowania ich poufności.

Powyższe przepisy prawa przesądzają o statusie powiatowego zespołu, jako administratora w rozumieniu art. 4 pkt 7 RODO, niezależnie od tego, czy jest umiejscowiony w strukturze powiatu, czy nie. Za przyjęciem takiego stanowiska przemawia również treść art. 6d ust. 2 ww. ustawy, zgodnie z którym powiatowe zespoły są administratorami danych w prowadzonych przez siebie bazach danych Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności, w którym przetwarza się dane w celu usprawnienia i podniesienia jakości orzekania o niepełnosprawności oraz realizacji zadań przez zespoły orzekające o niepełnosprawności.

Analiza przepisów ww. ustawy o rehabilitacji oraz rozporządzenia wskazuje także na zadania starosty związane z funkcjonowaniem powiatowych zespołów, który w ramach zadań z zakresu administracji rządowej powołuje powiatowy zespół, po uzyskaniu zgody wojewody oraz przedkłada wojewodzie informacje o realizacji zadań (art. 6a ust. 1 ustawy), a także powołuje i odwołuje przewodniczącego oraz członków powiatowego zespołu (§ 18 ust. 2 i 3 ww. rozporządzenia). Powołane wyżej regulacje nie precyzują jednak kwestii organizacyjnych, w szczególności w jaki sposób mają działać powiatowe zespoły (czy jako odrębne podmioty, czy w strukturach starostwa), a także w jaki sposób ma być realizowana ich obsługa administracyjna, finansowa czy kadrowa. Jedynie w § 18 ust. 5 ww. rozporządzenia wskazano, że przewodniczący powiatowego zespołu reprezentuje zespół na zewnątrz i organizuje jego obsługę administracyjno-biurową.

Powiatowy zespół, nawet jeśli umiejscowiony jest w strukturach starostwa, jest administratorem przetwarzanych przez siebie danych. Jednakże w takiej sytuacji również starosta przetwarza dane osobowe wnioskodawców powiatowego zespołu, np. w związku z obsługą składanej przez nich korespondencji adresowanej do powiatowego zespołu albo też w związku z archiwizacją akt postępowań i w tym zakresie jest ich administratorem. Zgodnie z art. 34 oraz art. 35 ust. 2 i 3 ustawy o samorządzie powiatowym starosta jest kierownikiem starostwa powiatowego i organizuje jego pracę, a także zwierzchnikiem służbowym pracowników starostwa i kierowników

jednostek organizacyjnych powiatu. Zatem w sytuacji, gdy starosta zapewnia obsługę działalności powiatowego zespołu, podmioty te będą wspólnie ustalać cele i sposoby przetwarzania danych osobowych, w ramach tych zadań. Pomiędzy tymi administratorami można zatem przyjąć relację współadministrowania uregulowaną w art. 26 RODO. Wówczas powiatowy zespół oraz starosta, jako współadministratorzy, powinni w drodze wspólnych uzgodnień w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw.

Prezes UODO podniósł, że takie wspólne uzgodnienia muszą uwzględniać faktyczne obowiązki powiatowego zespołu i starosty, związane z przetwarzaniem danych osobowych osób występujących do powiatowego zespołu, a wynikające m.in. z przepisów ustawy o rehabilitacji oraz wewnętrznych regulacji. Zarówno powiatowy zespół, jak i starosta mają swoje autonomiczne uprawnienia, z którymi związane jest przetwarzanie danych ww. osób w innych celach. Przykładowo, jedynie powiatowy zespół uprawniony jest do przetwarzania danych osobowych w celu orzekania o niepełnosprawności. Starosta, w ramach współadministrowania, może być uprawniony np. do zapewnienia ochrony pomieszczeń czy przetwarzania tych danych w celach archiwizacyjnych. Organ nadzoru podkreślił, że co do zasady odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w zakresie realizacji takich autonomicznych uprawnień kształtują przepisy prawa. Powiatowy zespół i starosta, w ramach wspólnych uzgodnień, powinni więc określić inne kwestie, nieuregulowane wprost w przepisach prawa, w tym m.in. kwestię odpowiedniego zabezpieczenia danych osobowych wnioskodawców czy też realizacji określonych obowiązków informacyjnych.

Warto nadmienić, że analogiczne podejście zostało zaprezentowane przez Prezesa UODO wobec relacji pomiędzy wojewodą a wojewódzką komisją do spraw orzekania o zdarzeniach medycznych[281].

Kto jest administratorem danych osobowych przetwarzanych w urzędzie wojewódzkim?[282]

W przypadku podmiotów szeroko rozumianego sektora publicznego, podmiot będący administratorem może być wprost wskazany w konkretnym przepisie prawa, jednak najczęściej ma miejsce sytuacja, w której wskazanie podmiotu pełniącego tę rolę wymaga analizy przepisów

[281] Newsletter UODO dla Inspektorów Ochrony Danych Nr 2/2019.
[282] https://uodo.gov.pl/pl/225/1640

stanowiących podstawę przetwarzania danych osobowych. O tym, czy dany organ jest administratorem, decyduje przede wszystkim rodzaj i charakter nadanych mu przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania. W zależności więc od danych, które są przetwarzane, oraz podstawy prawnej przetwarzania i kompetencji poszczególnych podmiotów (organów) do przetwarzania, administratorem może być urząd, organ albo np. jednostka samorządu terytorialnego.

Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ocena będzie zależała od tego, o jakie dane osobowe oraz o jakie zadania chodzi w określonym przypadku.

W odniesieniu do urzędu wojewódzkiego pomocniczo można wskazać, że co do zasady w przypadku przetwarzania danych pracowników lub kandydatów do pracy administratorem jest jednostka organizacyjna będąca pracodawcą w rozumieniu prawa pracy (w przypadku pracowników urzędu wojewódzkiego pracodawcą jest ten urząd). Natomiast wobec danych interesantów (w tej samej jednostce organizacyjnej) za administratora może być uznany właściwy do realizacji określonych zadań (podejmowania decyzji, uchwał) organ jednoosobowy lub kolegialny. W tym przypadku organem takim będzie zazwyczaj wojewoda, nie zaś dyrektor generalny. Dyrektor generalny urzędu co do zasady dokonuje jedynie pewnych czynności w imieniu kierownika jednostki, a nie w swoim. Regulamin organizacyjny, plany działalności i inne wewnętrzne dokumenty warunkujące cel przetwarzania danych zatwierdza kierownik jednostki, a nie dyrektor generalny. Ponadto dyrektor również sam nie decyduje o sposobach przetwarzania, gdyż np. kwestie finansowe muszą być zatwierdzone przez kierownika jednostki, co w znaczący sposób determinuje możliwość samodzielnego decydowania w tym zakresie.

W pytaniach dotyczących statusu podmiotów, zwłaszcza publicznych, często pojawiało się również dodatkowe pytanie: **czy administratorzy funkcjonujący w ramach tej samej jednostki mogą opracować wspólną dokumentację ochrony danych osobowych?**[283]

Prezes UODO wskazywał, że istnienie w strukturach, np. urzędu gminy czy starostwa, więcej niż jednego podmiotu będącego odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych osobowych w odrębnych dokumentach dla każdego

[283] https://uodo.gov.pl/pl/225/1782

z nich. Zaznaczył jednak, że kwestię tę należy starannie przemyśleć oraz zapewnić, by z dokumentacji jasno wynikało, jakich administratorów i danych, za które oni odpowiadają, dokumentacja ta dotyczy. Podkreślił, że w świetle zasady rozliczalności do administratora należy decyzja, w jaki sposób skonstruuje funkcjonujący u siebie system ochrony danych osobowych. Przy czym system ten powinien dotyczyć całości procesów przetwarzania prowadzonych u danego administratora i realnie wpływać na prawidłowość, bezpieczeństwo oraz przejrzystość przetwarzania.

W przypadku podmiotów publicznych charakter, zakres, kontekst i cele prowadzonego przez nie przetwarzania, wskazują na obowiązek wdrożenia odpowiednich polityk ochrony danych osobowych. W art. 24 ust. 2 RODO jest wręcz mowa o politykach ochrony danych osobowych, tak więc może to być nie jeden dokument, a zespół kilku dokumentów (polityk tematycznych) obejmujących wszelkie informacje o stosowanych środkach i procedurach związanych z ochroną danych osobowych. W odniesieniu do poszczególnych elementów tej dokumentacji należy również przemyśleć, jakie kategorie osób zatrudnionych w jednostce organizacyjnej muszą się z nimi zapoznać i stosować w związku z wykonywanymi przez siebie zadaniami.

Zdarzyć się też mogą sytuacje, w których poszczególni administratorzy funkcjonujący w ramach jednej jednostki organizacyjnej podlegać będą jednocześnie również innym niż RODO regulacjom dotyczącym ochrony danych osobowych, np. ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Regulacje te mogą przewidywać specyficzne rozwiązania dotyczące prowadzenia dokumentacji ochrony danych, które również powinny być uwzględnione przez administratorów w prowadzonej dokumentacji[284].

Pytania dotyczące statusu podmiotów sektora prywatnego

Pogłębionej analizy wymagało udzielenie odpowiedzi na pytanie: **Kto jest administratorem w przypadku Pracowniczej Kasy Zapomogowo – Pożyczkowej (PKZP) działającej przy pracodawcy?**[285]

Prezes UODO wskazał m.in., że art. 39 ustawy z dnia 23 maja 1991 r. o związkach zawodowych przewiduje możliwość tworzenia u pracodawców PKZP. Członkami tych kas mogą być pracownicy, emeryci, renciści. Szczegółowe zasady organizowania i działania tych kas określa

[284] Więcej informacji na ten temat znaleźć można w odpowiedzi na pytanie „Czy komendant straży miejskiej musi posiadać odrębną politykę ochrony danych?", zob. https://uodo.gov.pl/pl/225/1214.
[285] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1619.

rozporządzenie Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy. Zarówno pracodawca (zakład pracy), jak i PKZP, w zakresie przetwarzanych przez siebie danych osobowych, samodzielnie ustalają własne cele i sposoby ich przetwarzania, dlatego też zasadnie można uznać, że powinni być traktowani jako oddzielni administratorzy.

Natomiast w § 4 rozporządzenia w sprawie PKZP przewidziano pomoc ze strony pracodawcy (zakładu pracy) przy realizacji zadań PKZP (m.in. prowadzenia księgowości, obsługi kasowej i prawnej, dokonywania na rzecz PKZP potrąceń w listach płac, listach wypłat zasiłków chorobowych i zasiłków wychowawczych, wpisowego, wkładów miesięcznych i rat pożyczek, przyjmowania wpłat wnoszonych przez emerytów i rencistów oraz osoby przebywające na urlopach wychowawczych), a szczegółowe warunki świadczonej pomocy ma określać umowa zawierana pomiędzy pracodawcą a PKZP. W ramach tak prawnie ukształtowanych relacji, można zasadnie uznać, że podmioty te współdziałają ze sobą, a zatem wspólnie ustalają cele i sposoby przetwarzania danych osobowych wykorzystywanych w tym celu, przetwarzają je więc jako współadministratorzy.

Dlatego nie ma podstaw, aby w opisanym przypadku zawierać umowy powierzenia przetwarzania danych. Podmiot przetwarzający ma bowiem zupełnie inny status – przetwarza dane osobowe w imieniu administratora i w tym zakresie podlega jego kontroli. Wzajemne relacje pomiędzy tymi podmiotami w kwestiach nieuregulowanych przepisami rozporządzenia w sprawie PKZP powinny być określone, np. w porozumieniu lub umowie pomiędzy uprawnionymi podmiotami. W drodze wspólnych uzgodnień podmioty te powinny w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

Temu, **czy z firmą szkoleniową trzeba zawrzeć umowę powierzenia**[286], poświęcone było kolejne z pytań IOD. Wątpliwości budziło bowiem to, jak prawidłowo określić rolę pracodawcy i firmy szkoleniowej w procesie przetwarzania danych osobowych.

W tym przypadku organ nadzoru również wskazał, że w pierwszej kolejności należy dokonać analizy okoliczności faktycznych z uwzględnieniem zadań określonych podmiotów, wynikających m.in. z przepisów prawa oraz zawartej pomiędzy nimi umowy. Trzeba brać pod uwagę, jak w szczegółach realizowane są obowiązki przeprowadzenia szkolenia w konkretnym przypadku i jak pracodawca i firma szkoleniowa uzgodniły swoje role oraz zadania w zakresie przetwarzania

[286] https://uodo.gov.pl/pl/225/1736

danych, a także na ile samodzielnie i w jakich celach podmioty te przetwarzają dane w celach związanych ze szkoleniem.

W wielu przypadkach, gdy pracodawca przekazywał realizację zadania innemu podmiotowi, który dokonywał tego samodzielnie (także w zakresie przetwarzania danych), decydując przy tym o sposobach i celach przetwarzania, a zadania i obowiązki tego podmiotu były dodatkowo dość szczegółowo określone w przepisach prawa, istniały podstawy do uznania ich za odrębnych administratorów. Powierzenie przetwarzania powinno mieć natomiast miejsce wówczas, jeśli zewnętrzny podmiot przetwarza dane w imieniu administratora, w celach i w sposób przez niego określony. W niektórych przypadkach warto zwrócić uwagę na rozwiązanie określone w art. 26 RODO, tj. instytucję współadministrowania. Zgodnie z art. 94 pkt 4 ustawy Kodeks pracy, pracodawca jest obowiązany w szczególności zapewniać bezpieczne i higieniczne warunki pracy oraz prowadzić systematyczne szkolenie pracowników w zakresie bezpieczeństwa i higieny pracy. Natomiast zgodnie z brzmieniem § 4 ust. 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy, szkolenie może być organizowane i prowadzone przez pracodawców lub (na ich zlecenie) przez jednostki organizacyjne prowadzące działalność szkoleniową w dziedzinie bezpieczeństwa i higieny pracy. Pracodawca może zatem realizować obowiązek nałożony na niego w art. 94 pkt 4 Kodeksu pracy samodzielnie lub za pośrednictwem firmy zewnętrznej i świadczonych przez nią usług.

Firma zewnętrzna w procesie przetwarzania może występować w roli organizatora szkolenia, o którym mowa w § 4 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy. W jego § 5 pkt. 1-6 zostały określone obowiązki organizatora szkolenia. Należy do nich zapewnienie: programu poszczególnych rodzajów szkolenia opracowanego dla określonych grup stanowisk; programu szkolenia instruktorów w zakresie metod prowadzenia instruktażu – w przypadku prowadzenia takiego szkolenia; wykładowców i instruktorów posiadających zasób wiedzy, doświadczenie zawodowe i przygotowanie dydaktyczne zapewniające właściwą realizację programów szkolenia; odpowiednich warunków lokalowych do prowadzenia działalności szkoleniowej; wyposażenie dydaktyczne niezbędne do właściwej realizacji programów szkolenia; właściwy przebieg szkolenia oraz prowadzenia dokumentacji w postaci programów szkolenia, dzienników zajęć, protokołów przebiegu egzaminów i rejestru wydanych zaświadczeń. Jednostka organizacyjna prowadząca działalność szkoleniową w dziedzinie bezpieczeństwa i higieny pracy, realizując obowiązki nałożone na nią przepisami ww. rozporządzenia, przetwarza dane pracownika w związku ze sporządzaniem

protokołów z przebiegu egzaminów i rejestru wydanych zaświadczeń oraz w zakresie nawiązania współpracy (zawarcia stosownych umów) z wykładowcami i instruktorami posiadającymi zasób wiedzy, doświadczenie zawodowe i przygotowanie dydaktyczne, zapewniające właściwą realizację programów szkolenia. W tym zakresie zasadnie można uznać, że przetwarza dane jako administrator w rozumieniu przepisów o ochronie danych osobowych.

Odnosząc się do zagadnienia, kto jest administratorem w przypadku „szkoleń podnoszących kwalifikacje pracowników", Prezes UODO wskazał, że również w tym wypadku należy dokonać analizy, kto podejmuje decyzje w zakresie kluczowych kwestii dla danego procesu przetwarzania. Na przykład rola pracodawcy, który kieruje swoich pracowników na szkolenie, może ograniczać się tylko do rozdysponowania formularzy przygotowanych przez firmę, która oferuje szkolenie, a wszystkie kluczowe decyzje co do procesu przetwarzania danych należą do firmy szkoleniowej.

Przetwarzanie danych osobowych osób reprezentujących osoby prawne

Zarówno administratorzy, jak i inspektorzy ochrony danych mieli trudności w rozumieniu pojęcia „dane dotyczące osoby prawnej" użytego w motywie 14 preambuły.

Do tego zagadnienia Prezes UODO odniósł się w materiale: **Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?**[287], będącym odpowiedzią na wątpliwości inspektora ochrony danych dotyczące tego, czy należy dopełniać obowiązek informacyjny na mocy art. 13 i 14 RODO w sytuacji, gdy w treści dokumentacji dotyczącej postępowań administracyjnych pojawiają się dane osób upoważnionych do reprezentacji spółek, np. członków zarządu (organów spółek) bądź osób uprawnionych do składania oświadczeń w imieniu określonego podmiotu? W odpowiedzi Prezes UODO wskazał, że zgodnie z art. 1 ust. 2 RODO, regulacja ta chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych, a ponadto w motywie 14 RODO wyjaśniono, że ochrona zapewniana przez RODO dotyczy „osób fizycznych, niezależnie od ich obywatelstwa lub miejsca zamieszkania, w związku z przetwarzaniem ich danych osobowych". W zdaniu drugim motywu 14 RODO wyjaśniono, że RODO nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. Oznacza to, że RODO chroni dane osobowe

[287] https://uodo.gov.pl/pl/225/1577

możliwych do zidentyfikowania osób fizycznych i wyklucza spod tej ochrony dane dotyczące osób prawnych.

Wskazano również, że zdarzają się sytuacje, w których dane o charakterze osobowym będą związane z danymi dotyczącymi osób prawnych. Przykładem tego mogą być dane osobowe osób pełniących funkcję organów osoby prawnej. W takich sytuacjach spełnienie przesłanki identyfikowalności przesądzić powinno o objęciu zakresem ochronnym RODO danych osobowych również w takich konfiguracjach. W przypadku osób fizycznych pełniących funkcję członków organów osoby prawnej możliwość ich identyfikacji wynika w szczególności z faktu, iż dane takich osób ujawniane są w KRS. Oznacza to, że należy odmiennie odnosić się do informacji o osobach prawnych i osobach fizycznych reprezentujących osoby prawne.

Wobec powyższego należy przyjąć, że dane osób fizycznych pełniących funkcje członków organów osoby prawnej będą stanowiły dane osobowe, a nie będą zaś mieściły się w zakresie pojęcia danych osoby prawnej (w rozumieniu motywu 14 RODO). Podobnie sytuacja wygląda w odniesieniu do danych pełnomocników i pracowników osób prawnych, co potwierdza odpowiedź Komisji Europejskiej z 21 lutego 2018 r. na pisemne pytanie członka Parlamentu Europejskiego Richarda Sulika, w której wskazano, że motyw 14 RODO wyjaśnia, że rozporządzenie nie ma zastosowania do przetwarzania danych osobowych, które dotyczą osób prawnych, w tym nazwy i formy osoby prawnej oraz danych kontaktowych osoby prawnej. Adres e-mail osoby prawnej, taki jak ikeacontact@ikea.com, nie wchodzi w zakres rozporządzenia. Jednak dane osobowe pracowników osoby prawnej, w tym ich profesjonalne adresy e-mail, byłyby objęte zakresem rozporządzenia (np. Johnsmith@ikea.sk)[288].

W wyjaśnieniach Prezes UODO odwołał się również do wyroku Trybunał Sprawiedliwości UE z 9 marca 2017 r. w sprawie C-398/15. Okoliczność, iż informacje wpisują się w ramy działalności zawodowej nie oznacza, że nie można ich scharakteryzować jako dane osobowe. Definicja danych osobowych odnosi się zatem do osób fizycznych bez względu na rolę, jaką odgrywają – czy są konsumentami, przedsiębiorcami lub pracownikami, itd.

W ocenie Prezesa UODO powyższe daje podstawę, aby uznać, że dane członków zarządu reprezentujących osobę prawną, dane pełnomocników osób prawnych, a także dane pracowników, którzy są osobami kontaktowymi osoby prawnej, będących możliwymi do zidentyfikowania osobami fizycznymi, będą danymi osobowymi podlegającymi ochronie RODO. Wobec tego administrator jest

[288] odpowiedź Komisji Europejskiej dostępna pod linkiem: https://www.europarl.europa.eu/doceo/document/E-8-2017-007174-ASW_EN.html?redirect

zobligowany do wypełnienia w stosunku do takich osób obowiązku informacyjnego określonego w art. 13 lub 14 RODO, o ile nie zachodzi jedna z przesłanek zwalniających go z tego obowiązku.

Stanowisko przestawione w powyższej odpowiedzi spotkało się z dużym zainteresowaniem, a także wywołało ożywioną dyskusję wśród specjalistów z zakresu ochrony danych osobowych i dalsze wypowiedzi prasowe UODO. W wyjaśnieniach UODO z 9 lipca 2020 r. dla Dziennika Gazeta Prawna[289] wskazano, że ww. stanowisko miało na celu przede wszystkim zwrócenie uwagi na konieczność wypełniania wobec członków zarządu czy osób uprawnionych do reprezentowania danego podmiotu obowiązków wynikających z RODO, w tym obowiązku informacyjnego. Sama zaś forma wywiązywania się podmiotów z tego obowiązku jest kwestią indywidualną i zależy od konkretnej sytuacji. Jeżeli przykładowo w momencie podjęcia zatrudnienia lub współpracy został wypełniony prawidłowo obowiązek informacyjny, to nie ma potrzeby powtarzać go przy każdej kolejnej czynności. Wyjątkiem od tej zasady będą sytuacje, w których zmianie miałby ulec zakres czy sposób przetwarzania danych osobowych, określony w pierwszym piśmie adresowanym do osoby, której dane dotyczą.

Wskazano ponadto, że w odniesieniu do wypełniania obowiązku informacyjnego w toku postępowania administracyjnego należy także pamiętać o szczegółowych regulacjach w tym zakresie, które zostały dodane do kodeksu postępowania administracyjnego na mocy ustawy z 21 lutego 2019 r. dostosowującej do RODO. W myśl art. 61 par. 5 kodeksu postępowania administracyjnego, „organ administracji publicznej przekazuje informacje, o których mowa w rozporządzeniu 2016/679, przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treści nie uległy zmianie". Ponadto możliwość zastosowania zwolnienia z obowiązku informacyjnego na podstawie art. 13 ust. 4 lub art. 14 ust. 5 lit. a RODO będzie zależna od konkretnej sytuacji. Przesłanką do skorzystania ze zwolnienia z obowiązku informacyjnego nie może być założenie, że ze względu na specyfikę pełnionych funkcji i rolę w organizacji, członkowie zarządów wiedzą, w jaki sposób spółka, w której pełnią funkcję oraz kontrahenci tej spółki przetwarzają dane takich członków zarządu. Przede wszystkim istotne jest, że bez względu na to, kim jest administrator i wobec jakich konkretnie osób wypełnia obowiązek informacyjny zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO), musi być w stanie wykazać, że rzetelnie przekazał informacje, o których mowa w art. 13 lub 14 RODO.

[289] Dziennik Gazeta Prawna (Firma i Prawo) z 14 lipca 2020 r.

Rozwiązanie polegające na zamieszczeniu w stopce e-mailowej informacji o administratorze danych osobowych wraz z odniesieniem do linku z szerszymi informacjami, będzie stanowiło tzw. warstwowe informowanie i jest jak najbardziej dopuszczalne. Należy jednak pamiętać o aktualizacji zarówno informacji zamieszonych w stopce, jak i tych, do których odsyła administrator.

Status i zadania inspektora ochrony danych

W 2020 r. do UODO wpływały również pytania dotyczące statusu i zadań inspektora ochrony danych, a także zawiadamiania o danych do kontaktu z IOD. Udzielanie odpowiedzi na nie było dla organu nadzoru okazją do wyjaśniania, jak prawidłowo należy rozumieć rolę IOD i jak istotne jest należyte przestrzeganie przepisów gwarantujących prawidłowe i niezależne pełnienie przez niego funkcji. W odpowiedziach na takie pytania Prezes UODO podkreślał, że rola inspektora koncentruje się na monitorowaniu przestrzegania przepisów o ochronie danych osobowych i wewnętrznych polityk oraz prawidłowego wykonywania wynikających z nich obowiązków, a także doradzaniu i podnoszeniu świadomości w zakresie tych obowiązków, a ponadto pełnieniu funkcji punktu kontaktowego. Inspektor nie powinien natomiast podejmować zadań, które mogą stać się następnie przedmiotem dokonywania przez niego czynności monitorowania ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych.

Czy praca IOD może być kontrolowana?[290]

Wątpliwości inspektora dotyczyły tego, czy działania podejmowane przez IOD w związku z wykonywaniem przez niego jego zadań mogą podlegać kontroli przeprowadzanej przez administratora bezpośrednio lub za pośrednictwem podmiotów, którym zleca on taką kontrolę, np. wewnętrznych lub zewnętrznych audytorów oraz czy w jednostkach sektora finansów publicznych audytor może inspektorowi wydać zalecenia na gruncie przepisów dotyczących audytu wewnętrznego?

W odpowiedzi Prezes UODO podkreślił, że niezależność IOD, o której mowa w motywie 97 RODO oraz w art. 38 RODO, jest jedną z najważniejszych gwarancji skutecznego i prawidłowego wykonywania jego zadań, a tym samym realnego zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa. Jednocześnie zwrócił uwagę, że to administrator ponosi pełną odpowiedzialność za zgodne z przepisami ochrony danych osobowych przetwarzanie danych. Inspektor ochrony danych podlega bezpośrednio administratorowi i w związku z tym sposób wykonywania funkcji przez IOD musi podlegać jego kontroli, przy czym może to być kontrola

[290] https://uodo.gov.pl/pl/223/1765

wewnętrzna lub zlecona przez administratora podmiotowi zewnętrznemu. W jednym i drugim przypadku taka kontrola (audyt) musi uwzględniać niezależne funkcjonowanie (gwarancje niezależności) IOD, tak wyraźnie podkreślane w RODO. Dotyczy to również wdrożonych w danej organizacji systemów wewnętrznej kontroli (systemy oceny zgodności). Systemy te nie mogą w jakikolwiek sposób ograniczać możliwości wykonywania przez IOD jego zadań, w tym dokonywania kompleksowej, bieżącej oceny zgodności przetwarzania danych osobowych z przepisami prawa.

Prezes UODO wskazał, że administratorzy będący jednostkami sektora finansów publicznych, w celu zapewnienia zgodnego z prawem przetwarzania danych osobowych i właściwej organizacji bezpieczeństwa informacji, korzystają z pomocy zarówno audytorów, jak i inspektorów ochrony danych. Audytor wewnętrzny dokonuje systematycznej oceny kontroli zarządczej, obejmując zasięgiem swojego działania wszystkie obszary jednostki, w tym działania podejmowane przez IOD. Sposób przeprowadzania audytu wewnętrznego został określony w przepisach prawa (m.in. w rozporządzeniu Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu), ale musi on uwzględniać przepisy RODO, w tym m.in. w art. 38 ust. 3 RODO.

Gdy audyt (kontrola) dotyczy pracy IOD, respektowanie niezależnego wykonywania jego zadań oznacza zakaz wydawania IOD przez osoby kontrolujące jakichkolwiek bezpośrednich poleceń/zaleceń odnośnie tych zadań. Ostateczne decyzje co do oceny wyników audytu dotyczącego prawidłowości wykonywania ciążących na IOD obowiązków podejmuje kierownik jednostki, a inspektor musi mieć możliwość przedstawienia swojego stanowiska. Racje obu stron powinny zostać uzasadnione i udokumentowane. Materiał ten może być przydatny w celach dowodowych w przypadkach oceny prawidłowości wykonywania funkcji IOD w kontekście jego odpowiedzialności na gruncie przepisów prawa pracy lub Kodeksu cywilnego (odpowiedzialności kontraktowej) albo odpowiedzialności karnoprawnej[291].

Czy IOD może w imieniu administratora zawierać umowy powierzenia?[292]

W odpowiedzi na to pytanie Prezes UODO wskazał, że przepisy RODO wymagają przeprowadzenia w tym zakresie oceny pod kątem wypełnienia przez administratora obowiązku określonego w art. 38 ust. 6 RODO. Przepis ten wskazuje, że IOD może wykonywać inne (niż te, które zostały mu przypisane w RODO) zadania i obowiązki. Zawiera jednak zastrzeżenie, iż

[291] więcej na ten temat pod linkiem https://uodo.gov.pl/pl/138/445.
[292] https://uodo.gov.pl/pl/225/1804

administrator lub podmiot przetwarzający zobowiązani są zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Konflikt interesów następuje m.in. wtedy, gdy nie można pogodzić prawidłowego wykonywania zadań inspektora, przypisanych mu w art. 38 ust. 4 oraz art. 39 RODO, z realizacją innych zadań, gdyż pomiędzy zadaniami występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. W przypadku inspektora sprzeczność taka może wynikać z występowania przez niego jednocześnie w dwóch rolach lub podejmowanie przez niego działań bądź decyzji, które następnie muszą podlegać jego ocenie. Może się tak stać zwłaszcza w sytuacji, gdy inspektor jest obciążany obowiązkami, które przepisy nakładają na administratora. Konflikt interesów może być również rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD. Powyższe sytuacje często wynikają z problemu błędnego postrzegania inspektora jako osoby, która jako jedyna w organizacji odpowiedzialna jest za wykonywanie obowiązków z zakresu ochrony danych osobowych.

W odpowiedzi organ nadzoru podkreślił, że inspektor ochrony danych to funkcja, która ma szczególny status w świetle RODO. W związku z monitorowaniem przestrzegania przepisów o ochronie danych osobowych, inspektor musi mieć zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację swojej roli i obowiązków wynikających wprost z przepisów prawa.

Dlatego w opisanym przypadku konieczne było zbadanie, na czym konkretnie miałyby polegać czynności, które inspektor miałby podjąć w związku z zawieraniem umów powierzenia przetwarzania. Trzeba ustalić, czy np. inspektor nie został obarczony zadaniem sporządzenia projektu umowy i w związku z tym, czy to do niego nie należało określenie, w jaki sposób ukształtowana będzie relacja między administratorem i podmiotem przetwarzającym oraz prawa i zobowiązania stron tej umowy. Taka sytuacja powodowałaby konflikt interesów, ponieważ IOD następnie w ramach swoich ustawowych obowiązków zobowiązany byłby ocenić prawidłowość i zgodność z przepisami podjętych w tym zakresie decyzji. Inspektor nie powinien zatem podejmować zadań, które mogą stać się następnie przedmiotem dokonywania przez niego czynności monitorowania ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych. Zwraca na to uwagę Grupa Robocza Art. 29 w Wytycznych dotyczących inspektorów ochrony danych[293] wskazując, że inspektor nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Wymóg niepowodowania

[293] https://uodo.gov.pl/pl/10/7

konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu[294].

W jaki sposób identyfikować osoby, które zwracają się do IOD, jako punktu kontaktowego?[295]

Jeden z IOD zastanawiał się, jakie działania należy podjąć, by właściwie zidentyfikować osoby zwracające się do IOD jako punktu kontaktowego, a tym samym zapewnić poufność informacji i zapobiec ewentualnemu przypadkowemu ujawnieniu danych osobowych osobie nieuprawnionej, np. podszywającej się pod konkretną osobę z imienia i nazwiska podczas rozmowy telefonicznej lub prowadzonej korespondencji.

Prezes UODO wskazał, że każdy z administratorów, aby móc sprawnie realizować swoje obowiązki związane z zasadą przejrzystości oraz realizacją praw osób, których dane dotyczą, w tym w sytuacji wystąpienia naruszenia ochrony danych osobowych, powinien, zgodnie z art. 12 oraz art. 24 ust. 2 RODO, dysponować odpowiednimi procedurami w zakresie obsługi takich praw i wniosków. W takich procedurach powinny być odzwierciedlone rozwiązania w zakresie weryfikacji tożsamości osoby uprawnionej do uzyskania informacji oraz bezpiecznego kanału udostępniania informacji o przetwarzanych danych. Art. 12 ust. 1 RODO wskazuje, że informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Osoba, której dane dotyczą, może wprawdzie zwrócić się o informacje za pośrednictwem takich środków komunikacji, jak np. telefon czy poczta elektroniczna, jednak w tym przypadku podmiot realizujący wniosek powinien zwrócić szczególną uwagę na obowiązek podjęcia stosownych działań w celu uniemożliwienia udostępnienia informacji osobom do tego nieuprawnionym (istotne jest ustalenie tożsamości wnioskodawcy). Przy realizacji uprawnienia na odległość możliwość weryfikacji osoby uprawnionej może odbyć się np. poprzez uprawdopodobnienie tożsamości przez konieczność podania szczegółowych danych, które tę osobę jednoznacznie identyfikują i pozwalają zweryfikować jej tożsamość (nie wystarczy spytać o imię i nazwisko oraz adres, gdyż te informacje mogą być powszechnie dostępne, ale trzeba dokonać

[294] Podobne stanowisko organ nadzorczy zajął w sprawie dotyczącej tego, **c**zy administrator może udzielić IOD upoważnienia do nadawania upoważnień do przetwarzania danych osobowych – dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/225/1277.

[295] https://uodo.gov.pl/pl/225/1529

weryfikacji na podstawie znacznie bardziej szczegółowych danych, co do których prawdopodobieństwo, że będą one znane przez osoby postronne, jest znikome). Taką argumentację potwierdza treść art. 12 ust. 6 RODO, zgodnie z którym, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

W odpowiedzi wskazano również, że w przypadku wątpliwości co do tożsamości osoby usiłującej pozyskać informacje, powinno się odmówić ich udzielenia, ewentualnie podać informacje ogólne. W takiej sytuacji można w szczególności:

– udzielając informacji osobom, których dane dotyczą, ograniczyć się do przekazywania ogólnych informacji opublikowanych przez administratora na jego stronie internetowej i wysłanych przez niego w formie zawiadomień na indywidualne adresy poczty elektronicznej, lub

– odnosząc się do konkretnej osoby, udzielać informacji o jej kategoriach danych osobowych, których dotyczy naruszenie, ale bez podawania tych konkretnych danych.

Czy IOD może mieć dwóch zastępców?[296]

Odpowiadając na powyższe pytanie Prezes UODO przesądził, że dopuszczalne jest, by administrator wyznaczył dwie osoby zastępujące inspektora ochrony danych. Jedna realizowałaby zadania IOD podczas jego nieobecności, a druga wówczas, gdyby w pracy nie było zarówno IOD, jak i tej pierwszej, zastępującej go osoby. Przyjęcie takiego rozwiązania jest racjonalne, umożliwia bowiem zapewnienie ciągłości wykonywania zadań IOD, a tym samym podnosi standard ochrony danych.

Określenie kwestii zastępstwa IOD (np. w wewnętrznym zarządzeniu) sprzyja dobrej organizacji pracy IOD i uniknięciu sytuacji, w której nie byłoby osoby, która mogłaby wykonywać zadania IOD podczas jego nieobecności. Ważne jest jednak, aby kierownictwo jednostki zadbało nie tylko o przejrzyste określenie systemu zastępstw IOD, ale również jasno określiło podział obowiązków między IOD i jego „zastępców", tak aby nie doprowadzić do ewentualnych konfliktów na tym tle i by wówczas, gdy jednocześnie w pracy będzie obecny inspektor i osoby go zastępujące, nie było wątpliwości, kto za jakie zadania jest odpowiedzialny. Dla wszystkich, zarówno wewnątrz podmiotu będącego administratorem danych, jak w relacjach zewnętrznych, musi być jasne, kto w danym momencie jest odpowiedzialny za monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa.

[296] Newsletter UODO dla IOD Nr 12/2020.

Kto wysyła powiadomienie o odwołaniu inspektora ochrony danych w przypadku likwidacji administratora?[297]

W odpowiedzi na to pytanie wskazano, że powiadomienia Prezesa Urzędu Ochrony Danych Osobowych o odwołaniu dotychczasowego inspektora ochrony danych powinien dokonać podmiot, który go wyznaczył. Obowiązek ten wynika z art. 10 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[298].

W sytuacji zaś, gdy administrator nie zawiadomił Prezesa UODO o odwołaniu IOD, może to zrobić podmiot, który jest jego następcą prawnym, a zatem przejął prawa i obowiązki likwidowanego podmiotu, wstępując tym samym w jego prawa.

Czy kierownik urzędu stanu cywilnego jest administratorem i czy może wyznaczyć IOD?[299]

Wątpliwość IOD powstała w związku z tym, że w jednostce samorządu terytorialnego, w której pełnił on swoją funkcję, burmistrz na stanowisku kierownika urzędu stanu cywilnego zatrudnił inną niż on sam osobę. Dlatego IOD pytał, czy w takiej sytuacji kierownik USC jest administratorem przetwarzanych przez siebie danych osobowych, a jeśli tak, to czy jest on zobowiązany do wyznaczenia inspektora ochrony danych.

Prezes UODO wskazał, że ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego określa wprost, kto realizuje cele z zakresu ustawy, gdyż zgodnie z jej art. 9, do dokonywania czynności z zakresu rejestracji stanu cywilnego został zobowiązany kierownik urzędu stanu cywilnego. Z tego względu należy uznać, iż to kierownik USC jest administratorem, niezależnie od tego, czy w określonej sytuacji faktycznie stanowisko to będzie piastować organ gminy – wójt (burmistrz, prezydent miasta) – czy inna osoba wyznaczona przez niego na podstawie art. 6 ust. 4 lub 5 ustawy Prawo o aktach stanu cywilnego.

Odnosząc się zaś do pytania o ewentualny obowiązek wyznaczenia inspektora ochrony danych przez kierownika USC, Prezes UODO zaznaczył, że wobec brzmienia art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, który ustala kierunek interpretacji w polskim systemie prawnym, użytego w art. 37 ust. 1 lit. a RODO, pojęcia „organ lub podmiot publiczny", nie można przyjąć, aby obowiązek wyznaczenia inspektora ochrony danych dla kierownika USC wynikał z przesłanki wymienionej w art. 37 ust. 1 lit. a RODO. Podkreślił również, że nawet w sytuacji braku

[297] https://uodo.gov.pl/pl/223/1442
[298] Dz. U. z 2019 r. poz. 1781.
[299] https://uodo.gov.pl/pl/223/1443

takiego obowiązku, administrator – kierownik urzędu stanu cywilnego – może dobrowolnie takiego inspektora wyznaczyć.

Organ nadzoru przypomniał jednocześnie, że art. 37 ust. 3 RODO dopuszcza możliwość wyznaczenia przez kilku administratorów jednego inspektora ochrony danych, przy uwzględnieniu jednak ich struktury organizacyjnej i wielkości. Zaznaczył, że skorzystanie z takiego rozwiązania wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora. Wskazał też, jakie czynniki należy wziąć przy tym pod uwagę. Jednocześnie zaznaczył, że więcej informacji na ten temat znaleźć można w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243) oraz na stronie internetowej Urzędu w zakładce Inspektor Ochrony Danych[300].

Organ nadzoru podniósł, że w przypadku, gdyby burmistrz i kierownik USC wyznaczyli na swojego inspektora tę samą osobę, powinni wspólnie określić zasady dotyczące zapewnienia mu wystarczającej ilości czasu na wypełnianie jego obowiązków, pomocy w stworzeniu planu jego pracy, a w razie potrzeby wsparcie jego funkcjonowania zespołem odpowiednich specjalistów. Zwrócił również uwagę, że jeśli kierownik USC decydowałby się na wyznaczenie inspektora, to on jako administrator powinien dokonać tego wyznaczenia, a także zawiadomić Prezesa UODO o jego wyznaczeniu.

Czy dane kontaktowe IOD muszą być łatwo dostępne? W jaki sposób powinny zostać opublikowane na stronie internetowej administratora?[301]

Odpowiadając na to pytanie Prezes UODO wskazał, że celem obowiązku publikowania przez administratora na swojej stronie internetowej imienia i nazwiska oraz adresu poczty elektronicznej lub numeru telefonu inspektora ochrony danych jest zapewnienie, aby osoby, których dane dotyczą, mogły mieć łatwy i bezpośredni kontakt z inspektorem, bez konieczności kontaktowania się z innymi jednostkami podmiotu[302].

Jeśli administrator prowadzi własną stronę internetową, dane o wyznaczonym IOD powinny znaleźć się w łatwo dostępnym miejscu strony, np. w zakładce: „Kontakt", „Inspektor ochrony danych", „RODO" czy „Ochrona danych osobowych". Za niewłaściwe należy natomiast uznać publikowanie tych danych w miejscach wymagających długiego przeszukiwania, takich jak „Aktualności" czy „Polityka prywatności".

[300] np. pod linkiem: https://uodo.gov.pl/pl/223/658
[301] https://uodo.gov.pl/pl/223/1784
[302] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243), str. 13, dostępne na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/10/7.

Zgodnie z RODO jednym z zadań IOD jest pełnienie roli punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą. Unijny prawodawca w art. 38 ust. 4 RODO uprawnił osoby, których dane dotyczą, do kontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Ta rola inspektora jest mocno powiązana z obowiązkami administratora oraz podmiotu przetwarzającego określonymi w art. 12-22 RODO i ma przyczyniać się do skuteczniejszego ich wykonywania.

Jako przykład wskazano sytuację, gdy dochodzi do naruszenia ochrony danych, które może powodować wysokie ryzyko naruszenia praw i wolności. W takim przypadku znaczenie praw osób oraz roli inspektora uwydatnia się w sposób szczególny. Jak należy wnioskować z art. 34 ust. 2 RODO, w przypadkach takich naruszeń, osoby, których to naruszenie dotyczy, powinny mieć możliwość zwrócenia się do IOD lub innego punktu kontaktowego w celu uzyskania dodatkowych informacji, wykraczających poza zakres przekazany im w zawiadomieniu o naruszeniu.

13.2. Wystąpienia

Jak stanowi art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Prezes UODO może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów, wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Zgodnie z ustępem 2 powołanego przepisu, Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

Podmiot, do którego skierowane zostało wystąpienie, jest obowiązany (zgodnie z art. 52 ust. 3) ustosunkować się do niego na piśmie w terminie 30 dni od daty otrzymania.

W ocenie organu właściwego w sprawie ochrony danych osobowych, wystąpienia są ważnym instrumentem w kształtowaniu i podnoszeniu poziomu ochrony danych osobowych. Zawarte w nich wnioski o zmianę obowiązujących regulacji prawnych lub o wprowadzenie nowych norm dotyczących przetwarzania danych osobowych albo wskazujące na konieczność zmodyfikowania praktyk stosowanych w podmiotach, do których są skierowane, wskazują na prawidłowy sposób postępowania i zapewniania zgodności z przepisami RODO.

W 2020 roku Prezes UODO wystosował **366 wystąpień** z określonymi wnioskami do podmiotów administracji publicznej i podmiotów prywatnych działających w różnych sektorach, z czego **346** wiązało się z naruszeniami ochrony danych, zaś **20** wystąpień dotyczyło zagadnień legislacyjnych.

I tak, w związku ze stwierdzonymi **naruszeniami ochrony danych osobowych**, powodującymi wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w 2020 r. Prezes Urzędu skierował **346 wystąpień do administratorów danych** w celu zapewnienia skutecznej ochrony danych osobowych. Głównym przedmiotem wystąpień było zwrócenie się do administratorów danych o zawiadomienie osób, których dane dotyczą, o naruszeniu ich danych osobowych – w przypadku rezygnacji przez administratora z zawiadomienia, lub ponownego zawiadomienia w przypadkach, w których pierwotnie dokonane przez administratora zawiadomienie nie spełniało warunków określonych w ogólnym rozporządzeniu o ochronie danych. Poza rezygnacją z zawiadomienia z powodu błędnie przyjętego poziomu ryzyka, do najczęstszych nieprawidłowości należało: pominięcie lub przekazanie niepełnych informacji wymaganych przepisami art. 34 ust. 2 w zw. z art. 33 ust. 3 lit. b, lit. c i lit. d rozporządzenia 2016/679, np. opisu okoliczności wystąpienia naruszenia, poprzez brak wskazania lub wskazanie niepełnych kategorii danych, które uległy naruszeniu; brak opisu możliwych konsekwencji naruszenia ochrony danych; brak opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych; czy brak wskazania imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji. Równie częstymi nieprawidłowościami, stanowiącymi o konieczności ponownego zawiadomienia osób, których dane dotyczą, o naruszeniu ich danych osobowych, było wskazanie przez administratorów danych w zawiadomieniu opisu możliwych konsekwencji poprzez posługiwanie się ogólnymi, lakonicznymi sformułowaniami, takimi jak „uszczerbek fizyczny", „strata finansowa", czy „kradzież tożsamości" lub wskazywanie możliwych konsekwencji, które nie odpowiadały proponowanym środkom minimalizującym ewentualne konsekwencje naruszenia dla osoby, której dane dotyczą, podczas gdy opis możliwych konsekwencji powinien odzwierciedlać ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych.

Natomiast impulsem do przygotowania **20 wystąpień** dotyczących zagadnień legislacyjnych były zarówno prowadzone analizy obowiązujących lub projektowanych aktów prawnych, jak i wpływające do Prezesa UODO sygnały czy pytania prawne, a także doniesienia medialne.

Szczególnie istotne były te sprawy, które wpływały na ochronę danych osobowych lub prywatność dużych grup osób, odnosiły się do wykorzystania nowoczesnych technologii, w tym zautomatyzowanego przetwarzania danych oraz monitorowania osób, a także przetwarzania szczególnych kategorii danych osobowych, jak np. dane o stanie zdrowia.

Poniżej przedstawione zostały wybrane przykłady wystąpień Prezesa UODO.

Przetwarzanie danych osobowych na portalu internetowym GEOPORTAL2 (geoportal.gov.pl)

W związku z otrzymaniem sygnałów o upublicznianiu informacji o numerach ksiąg wieczystych na portalu internetowym GEOPORTAL2 (*www.geoportal.gov.pl)*, Prezes UODO zwrócił się do Głównego Geodety Kraju o podjęcie stosownych działań mających na celu zapewnienie odpowiedniej ochrony danych osobowych[303]. Dostrzegając konieczność realizowania przez Głównego Geodetę Kraju tak istotnych zadań publicznych, jakimi są zadania związane z tworzeniem i utrzymaniem geoportalu infrastruktury informacji przestrzennej, organ właściwy w sprawie ochrony danych osobowych zwrócił uwagę na to, iż działania odnoszące się do udostępniania informacji z ewidencji gruntów i budynków muszą być także zgodne z zasadami ochrony danych osobowych wynikającymi z RODO, m.in. z zasadą legalności, rzetelności, przejrzystości czy minimalizacji danych.

W świetle definicji danych osobowych zawartej w RODO, numer księgi wieczystej nieruchomości stanowi daną osobową jej właściciela. Jest to bowiem informacja, za pośrednictwem której możliwe jest zidentyfikowanie – w sposób pośredni – osoby fizycznej, będącej właścicielem tej nieruchomości. Numer księgi wieczystej jest daną osobową, ponieważ prowadzi do identyfikacji określonej osoby fizycznej, jeżeli taka osoba jest właścicielem nieruchomości opisanej w księdze wieczystej lub przysługują jej ujawnione w księdze ograniczone prawa rzeczowe względem nieruchomości. W odniesieniu do właściciela, księgi wieczyste zawierają dane nie tylko o jego imieniu i nazwisku czy numerze PESEL, ale także informacje o jego zobowiązaniach finansowych czy o sposobie pozyskania tytułu prawnego do nieruchomości.

Prezes UODO wskazał, że zakwalifikowanie numerów ksiąg wieczystych jako danych osobowych nie budzi wątpliwości zarówno w przyjętych przez organ ochrony danych osobowych

[303] ZSPU.070.1.2019.

jednolitych stanowiskach w doktrynie[304], jak i w orzecznictwie sądów administracyjnych. Przykładowo WSA w Lublinie orzekł wprost, że za dane osobowe w rozumieniu ustawy o ochronie danych osobowych (aktualnie RODO) należy uznać numery ksiąg wieczystych i zbiorów dokumentów, skoro w tych księgach i zbiorach są ujawnione podmioty będące właścicielami nieruchomości, dla których księgi te lub zbiory są prowadzone[305]. Co prawda z przepisów ustawy Prawo geodezyjne i kartograficzne wynika, że informacje zawarte w operacie ewidencyjnym są jawne (art. 24 ust. 2), niemniej jawność ta ograniczona jest – w świetle przepisów o ochronie danych osobowych – do informacji, które nie stanowią danych osobowych właścicieli nieruchomości. Na gruncie obowiązującego prawa nie istnieje bowiem wyraźna podstawa prawna dla szerokiego udostępniania informacji o numerach ksiąg wieczystych w systemie takim jak geoportal.

Prezes UODO zwrócił uwagę na zagrożenia płynące z faktu upublicznienia numerów ksiąg wieczystych, wskazując, że w połączeniu z innymi danymi osobowymi, dostępnymi potencjalnie w innych rejestrach publicznych (np. krajowym rejestrze sądowym oraz danymi z oświadczeń majątkowych osób pełniących funkcje publiczne) mogą utworzyć zbiór danych dostarczających wielu informacji o zidentyfikowanej osobie fizycznej. Tym sposobem mógłby powstać publiczny zbiór, dający dostęp do szerokich informacji o określonych osobach fizycznych, mogący naruszać ich prywatność, poprzez wykorzystywanie tych danych motywowane względami nie tylko ekonomicznymi, ale także ciekawością.

Prezes UODO zwrócił się do Głównego Geodety Kraju o wypracowanie takich rozwiązań, które z jednej strony umożliwią realizację zadań w zakresie utworzenia i utrzymania geoportalu infrastruktury informacji przestrzennej, a z drugiej strony ograniczą dostęp do zbyt szerokiego zakresu danych osobowych zawartych w księgach wieczystych.

W odpowiedzi na powyższe Główny Geodeta Kraju przedstawił swoje stanowisko, w którym nie zgodził się ze zgłoszonymi uwagami. W związku z brakiem zmiany tej kwestionowanej przez organ nadzoru praktyki, rodzącej **zagrożenie spowodowania poważnych i trudnych do usunięcia skutków,** wobec Głównego Geodety Kraju z urzędu wszczęte zostało postępowanie w sprawie

[304] O. Legat, M. Orkusz (red.), Zasady udostępniania danych zawartych w księgach wieczystych w kontekście rozwiązań prawa krajowego i prawa europejskiego – analiza komparatystyczna, uwagi *de lege lata* i wnioski *de lege ferenda*, Warszawa 2019.

[305] Wyrok WSA w Krakowie z 14 maja 2014 r. sygn. akt II SA/Kr 126/14; wyrok NSA z 18 lutego 2014 r. sygn. akt I OSK 1839/12.

naruszenia przepisów o ochronie danych osobowych, dotyczące udostępniania bez podstawy prawnej na portalu internetowym GEOPORTAL2 (geoportal.gov.pl) numerów ksiąg wieczystych[306].

Zakres danych pozyskiwanych przez gminy w deklaracjach śmieciowych

W związku z zaobserwowaną praktyką rad gmin, które określając wzór deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, wymagają podania szerszego zakresu danych niż ten określony przepisami ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, Prezes UODO zwrócił się do **Ministra Spraw Wewnętrznych i Administracji** o uczulenie na tę kwestię właściwych podmiotów nadzorczych w tym zakresie tak, by przyjmowane w uchwałach rozwiązania nie prowadziły do nakładania na właścicieli nieruchomości obowiązków niewynikających z ustawy[307].

Wskazał, że artykuł 6m ust. 1b ustawy o utrzymaniu czystości i porządku w gminach wprost stanowi, podania jakich danych osobowych można w tej sytuacji wymagać. Oznacza to, że gminy nie są uprawnione do pozyskiwania szerszego niż określony w tym przepisie zakresu danych osobowych właściciela nieruchomości, który jest zobowiązany do złożenia deklaracji śmieciowej, a tym bardziej do pozyskiwania danych osobowych osób zamieszkujących daną nieruchomość. Nie mogą więc żądać podania przez właściciela nieruchomości np. daty urodzenia czy imion ojca oraz matki, jak również danych osób zamieszkujących w danym lokalu mieszkalnym, czy ich numeru PESEL, co potwierdza także orzecznictwo[308].

W odpowiedzi resort wskazał, że przekazał wystąpienie Prezesa UODO do wszystkich prezesów regionalnych izb obrachunkowych (RIO), które są organem właściwym do oceny uchwał dotyczących określenia wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanej przez właścicieli nieruchomości[309].

Przyjętą przez Prezesa UODO wykładnię potwierdza najnowsze orzecznictwo sądów administracyjnych. Przykładowo Wojewódzki Sąd Administracyjny w Olsztynie w wyroku z 7 października 2020 r.[310] wskazał, że sformułowanie w deklaracji śmieciowej obowiązku podawania danych współmałżonka stanowi wyjście poza granice upoważnienia wynikającego

[306] https://uodo.gov.pl/pl/138/1483
[307] DOL.413.4.2020.
[308] m.in. wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z 12 stycznia 2017 r. sygn. akt I SA/Po 1459/16.
[309] Jednocześnie dla upowszechnienia właściwego podejścia w tym zakresie temat ten poruszony został w Newsletterze UODO dla IOD nr 3/2020.
[310] Wyrok Wojewódzkiego Sądu Administracyjnego w Olsztynie, sygn. akt I SA/Ol 405/20, opubl. LEX nr 3077728.

z ustawy o utrzymaniu czystości i porządku w gminach. Nie zawsze bowiem zaistnieje nawet możliwość skierowania egzekucji do małżonka składającego deklarację.

Przyjęcie zaś w tym zakresie uniwersalnego założenia, ewentualności wykorzystania takich danych i gromadzenia ich niejako „na wyrost", uznane musi być za praktykę niedającą się pogodzić z zasadą legalizmu działań organów administracji publicznej.

Innowacyjne rozwiązania w sektorze rolniczym a ochrona danych osobowych rolników

W związku z pojawieniem się na stronie internetowej **Agencji Restrukturyzacji i Modernizacji Rolnictwa (ARiMR)** komunikatu informującego o rozpoczęciu przez nią współpracy z Narodowym Centrum Badań i Rozwoju na rzecz wykorzystania innowacyjnych rozwiązań w sektorze rolniczym, Prezes UODO wyraził swoje wątpliwości, czy w procesie tym zapewniona zostanie odpowiednia ochrona danych osobowych. Zgodnie z tym komunikatem współpraca ta miałaby polegać na wdrożeniu nowoczesnych rozwiązań informatycznych do przetwarzania dużej ilości danych (tzw. big data) w zakresie przyznawania i obsługi dopłat obszarowych dla rolników, wykorzystania automatycznych narzędzi do oceny niektórych zobowiązań beneficjentów oraz wykorzystania bezzałogowych systemów latających (drony) do robienia zdjęć terenu w bardzo wysokiej rozdzielczości, a następnie ich analizy. Miały to być tylko niektóre z wielu innych rozwiązań technologicznych, które zostałyby udostępnione ARiMR dla realizacji jej zadań.

W związku z tym organ właściwy w sprawie ochrony danych osobowych wystąpił do Prezesa ARiMR o podjęcie stosownych działań, mających na celu zapewnienie odpowiedniej ochrony danych osobowych przetwarzanych przez ARiMR[311].

Zwrócił przede wszystkim uwagę na konieczność przeprowadzenia w takiej sytuacji oceny skutków dla ochrony danych, zgodnie z art. 35 RODO, oraz zadeklarował swoje wsparcie przy wyjaśnianiu wątpliwości, jakie mogłyby się pojawić podczas takiej oceny.

W odpowiedzi na wystąpienie organu nadzorczego Prezes Agencji Restrukturyzacji i Modernizacji Rolnictwa poinformował, że co prawda proces przetwarzania jakichkolwiek danych w tym projekcie jeszcze się nie rozpoczął, ale przyjął zgłaszane przez organ nadzorczy postulaty za słuszne i konieczne podczas analizy rozwiązań technologicznych w zakresie procesów przetwarzania danych.

[311] DOL.413.2.2020.

Monitoring wizyjny w mieszkaniu rodziny sprawującej pieczę zastępczą

Procedury związane z wykorzystaniem monitoringu wizyjnego przez osoby sprawujące pieczę zastępczą, tj. opiekę nad dziećmi w przypadku niemożności zapewnienia jej przez rodziców, nie są jednolite i budzą wiele wątpliwości. Prezes Urzędu Ochrony Danych Osobowych skierował wystąpienie do **Ministra Rodziny, Pracy i Polityki Społecznej** w sprawie uregulowania tej kwestii[312].

Wskazał w nim, że przetwarzanie danych osobowych z wykorzystywaniem monitoringu wizyjnego powinno odbywać się z poszanowaniem zasad wynikających z RODO. Osoby sprawujące pieczę zastępczą nie są wyłączone ze stosowania przepisów tego rozporządzenia. W ich przypadku nie można zastosować wyłączenia, które dotyczy sytuacji, gdy dane osobowe przetwarza osoba fizyczna w ramach czynności o osobistym lub domowym charakterze (art. 2 ust. 2 lit. c RODO). Organ nadzorczy dostrzegł potrzebę stworzenia przepisów prawa, które określiłyby jednolite zasady wykorzystywania monitoringu wizyjnego w pieczy zastępczej, w tym m.in.: obszary w placówkach, które mogłyby zostać objęte monitoringiem, cel wykorzystywania monitoringu czy okres przechowywania zgromadzonego z nagrań materiału. Pozwoliłoby to rozwiać wątpliwości podmiotów sprawujących tego typu formę pomocy rodzinie, co do legalności i możliwego zakresu stosowania tego narzędzia.

Także Rzecznik Praw Dziecka zwrócił uwagę na problem związany ze stosowaniem monitoringu wizyjnego w pieczy zastępczej. Zauważył on, że wykorzystywanie monitoringu wizyjnego w mieszkaniu niezawodowej rodziny zastępczej może stanowić bezprawną ingerencję w życie dziecka, o której mowa w art. 4 pkt 7 ustawy o wspieraniu rodziny i systemie pieczy zastępczej.

Wystąpienie Prezesa UODO spotkało się z aprobatą ze strony Ministra Rodziny, Pracy i Polityki Społecznej. Prezes UODO zadeklarował swoją pomoc i merytoryczne wsparcie, oczekując na zaangażowanie organu w dalsze prace legislacyjne nad projektem w zakresie ochrony danych osobowych.

Wzory kart profilaktycznego badania lekarskiego ucznia

W 2020 r. Prezes UODO skierował też wystąpienie do **Ministra Zdrowia**[313]. Dotyczyło ono niezgodności wzorów kart profilaktycznego badania lekarskiego ucznia, dostępnych na stronie

[312] DOL.411.2.2020.
[313] DOL.413.19.2020.

internetowej Ministerstwa Zdrowia, z przepisami rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

Z otrzymanej przez organ nadzorczy korespondencji wynika, że podmioty lecznicze stosują wzór karty profilaktycznego badania lekarskiego ucznia, który jest dostępny na stronie internetowej Ministerstwa Zdrowia w dokumencie: „Profilaktyczne badania lekarskie i inne zadania lekarza w opiece zdrowotnej nad uczniami. Poradnik dla lekarzy".

W opinii organu nadzorczego, poprzez takie określenie treści dokumentu, naruszona została zarówno zasada legalizmu, wynikająca z art. 5 ust. 1 lit. a RODO (poza regułami prawa krajowego kształtowany jest zakres ingerencji w prawo do prywatności), jak również zasada minimalizacji danych, stanowiąca, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c RODO). Administrator powinien pozyskiwać dane jedynie w niezbędnym i prawnie uzasadnionym zakresie. Stosownie zaś do zasady ograniczenia celu (art. 5 ust. 1 lit. b RODO) dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Prezes UODO wskazał również, że zgodnie z motywem 35 RODO, do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Ogólne rozporządzenie również w motywie 53 wskazuje, że szczególne kategorie danych osobowych zasługujące na większą ochronę powinny być przetwarzane do celów zdrowotnych wyłącznie w przypadkach, gdy jest to niezbędne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa.

W opinii organu nadzorczego, zakres danych osobowych zawartych w stosowanych kartach profilaktycznego badania lekarskiego ucznia jest niezgodny z ww. zasadą minimalizacji danych, bowiem jest on szerszy niż zakres danych określony w § 64 rozporządzenia Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania. Ponadto ujednolicone wzory kart powinny znajdować się w przedmiotowym rozporządzeniu (jako odrębne załączniki do ww. aktu prawnego).

W odpowiedzi na to wystąpienie Minister Zdrowia wskazał m.in., że Poradnik dla lekarzy podstawowej opieki zdrowotnej pt. „Profilaktyczne badania lekarskie i inne zadania lekarza w opiece zdrowotnej nad uczniami", pomimo iż jest dostępny na stronie internetowej Ministerstwa Zdrowia,

nie stanowi źródła prawa. Korzystanie z wszelkiego rodzaju wzorów dokumentacji medycznej, zamieszczanych na stronach internetowych, w tym także dostępnych na stronie internetowej Ministerstwa Zdrowia, każdorazowo wymaga od korzystającego weryfikacji pod względem ich zgodności z aktualnie obowiązującymi przepisami prawa. Dodał też, że w związku z wydaniem nowego rozporządzenia Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobów jej przetwarzania[314], które zastąpiło uprzednio obowiązujące rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, zmienił się zakres informacji, jakie powinny znaleźć się w karcie profilaktycznego badania ucznia. W związku z tym Ministerstwo Zdrowia we wrześniu 2020 r. rozesłało do wszystkich placówek podstawowej opieki zdrowotnej pisemną informację w przedmiotowej sprawie, co należy uznać za dobry krok w kierunku podnoszenia standardów ochrony danych.

Przechowywanie dokumentacji dotyczącej uczestników i byłych uczestników warsztatów terapii zajęciowej

W 2020 r. podmioty prowadzące warsztaty terapii zajęciowej (WTZ) sygnalizowały Prezesowi UODO, że przepisy regulujące ich działalność, tj. ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 25 marca 2004 r. w sprawie warsztatów terapii zajęciowej, nie wskazują, jak długo mają one przechowywać dokumentację dotyczącą uczestników i byłych uczestników warsztatów.

Licząc się m.in. z możliwością kontroli ze strony PCPR czy NIK, przez lata warsztaty terapii zajęciowej gromadziły i przechowywały bardzo dużo takich dokumentów, tym samym przetwarzając wiele danych osobowych. Z uwagi na to, że w obowiązujących przepisach prawa kwestia przechowywania danych zawartych na ww. nośnikach nie jest uregulowana, powodowało to dużą rozpiętość przyjmowanych przez administratorów rozwiązań.

Luka prawna w obszarze archiwizacji dokumentacji wytwarzanej w ramach warsztatów terapii zajęciowej, nie sprzyja poszanowaniu zasad ochrony danych osobowych, w szczególności zasady ograniczenia celu przetwarzania i przechowywania danych (art. 5 ust. 1 RODO). Przykładowo, realizując tożsame cele przetwarzania, administratorzy przyjmują bardzo zróżnicowane okresy przechowywania danych.

[314] Dz.U. poz. 666 z późn. zm.

Problem ten Prezes UODO zasygnalizował **Ministrowi Rodziny, Pracy i Polityki Społecznej,** wnosząc o rozważenie wprowadzenia jasnych standardów prawnych w tym obszarze[315]. W odpowiedzi na wystąpienie przedstawiciel resortu wskazał, że zmianą w ustawie z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych polegającą na dodaniu art. 2b, określono zasady dotyczące przetwarzania, zabezpieczenia, a także przechowywania danych osobowych. Zgodnie z ust. 7 tego przepisu pracodawcy (o których mowa w ust. 1), a także podmioty i osoby realizujące zadania wynikające z ustawy o rehabilitacji, przechowują dane osobowe wyłącznie przez okres nie dłuższy niż jest to niezbędne i w zakresie koniecznym do realizacji celów przetwarzania danych osobowych oraz dokonują przeglądu przydatności przetwarzania danych osobowych nie rzadziej niż co 5 lat. Organizowanie warsztatów terapii zajęciowej jest jednym z zadań określonych w ustawie o rehabilitacji. Oznacza to, że podmioty, które to zadanie realizują, zobowiązane są do przechowywania dokumentacji osobowej związanej z warsztatami terapii zajęciowej przez okres ustalony według ww. przepisu art. 2b ust. 7 ustawy o rehabilitacji. Poinformowano, że w toku prac legislacyjnych w kierunku zmiany przepisów zawartych w ustawie o rehabilitacji, brane będą pod uwagę wszystkie wpływające postulaty i propozycje. Rozważona zostanie również kwestia dotycząca okresu przechowywania dokumentacji osobowej, przetwarzanej w związku z prowadzeniem warsztatów terapii zajęciowej.

Prezes UODO oczekuje zatem na zaangażowanie go w przyszły proces legislacyjny, zmierzający do udoskonalenia obowiązujących przepisów.

Wzór zawiadomienia do Wojskowego Komendanta Uzupełnień

Impulsem do skierowania przez Prezesa UODO wystąpienia do **Szefa Kancelarii Prezesa Rady Ministrów**[316] były wpływające do Urzędu sygnały i wyrażane przez administratorów wątpliwości dotyczące przekazywania danych osobowych pracowników szpitala do wojskowych komisji uzupełnień.

Z informacji przekazywanych Prezesowi UODO wynikało, że pracodawcy wyrażali wątpliwość, czy przetwarzanie wszystkich danych osobowych pracownika, określonych w rozporządzeniu Rady Ministrów z dnia 15 czerwca 2004 r. w sprawie zawiadamiania wojskowych komendantów uzupełnień o osobach podlegających obowiązkowi czynnej służby wojskowej, oraz wydawania przez pracodawców, szkoły i inne jednostki organizacyjne zaświadczeń w sprawach

[315] DOL.413.26.2020.
m[316] DOL.413.10.2020.

powszechnego obowiązku obrony, jest – biorąc pod uwagę przepisy o ochronie danych osobowych – konieczne. Zgodnie z rozporządzeniem, pracodawca w zawiadomieniu do wojskowego komendanta uzupełnień podaje takie dane dotyczące pracownika, jak imię i nazwisko oraz imię ojca, data i miejsce urodzenia oraz numeru PESEL.

W ocenie organu nadzorczego przetwarzanie zarówno imienia ojca, daty i miejsca urodzenia oraz numeru PESEL w zawiadomieniu było – biorąc pod uwagę przepisy o ochronie danych osobowych – nadmiarowe z uwagi na to, że numer PESEL jednoznacznie identyfikuje osobę fizyczną. Prezes UODO wskazał, że konieczne jest ponowne przeanalizowanie przepisów rozporządzenia pod kątem adekwatności zakresu przetwarzanych danych do określonych celów i rozważenie jego ograniczenia do imienia i nazwiska, miejsca urodzenia oraz numeru PESEL, a tym samym zrezygnowanie z danych w postaci daty urodzenia pracownika i imienia jego ojca.

Z odpowiedzi Ministerstwa Obrony Narodowej na to wystąpienie wynikało, że w jego efekcie resort planuje podjąć prace legislacyjne w zakresie zmiany rozporządzenia.

Zakres danych przetwarzanych przez Głównego Inspektora Transportu Drogowego w związku z ujawnianiem naruszeń przepisów ruchu drogowego za pomocą stacjonarnych urządzeń rejestrujących

W wystąpieniu do **Ministra Infrastruktury**[317] o podjęcie prac legislacyjnych mających na celu uregulowanie zakresu danych przetwarzanych przez Głównego Inspektora Transportu Drogowego w związku z ujawnianiem za pomocą stacjonarnych urządzeń rejestrujących naruszeń przepisów ruchu drogowego – przekraczania dopuszczalnej prędkości i niestosowania się do sygnałów świetlnych – oraz ściganiem i karaniem ich sprawców, Prezes Urzędu Ochrony Danych Osobowych stwierdził, iż na Inspekcję Transportu Drogowego, reprezentowaną w tej kwestii przez Głównego Inspektora Transportu Drogowego, zostało nałożone powyższe zadanie, dla realizacji którego Główny Inspektor Transportu Drogowego (dalej GITD) jest uprawniony do: rejestrowania obrazów naruszeń przepisów ruchu drogowego – przekraczania dopuszczalnej prędkości i niestosowania się do sygnałów świetlnych, zwanych dalej „naruszeniami", przetwarzania obrazu pojazdu, którym dokonano danego naruszenia, jego numeru rejestracyjnego, wizerunku kierującego pojazdem, danych właściciela, posiadacza lub kierującego pojazdem oraz danych dotyczących okoliczności (daty, czasu, miejsca i rodzaju) naruszenia[318]. Po ujawnieniu naruszenia GITD, zgodnie z art. 129g ust. 2

[317] DOL.413.1.2020.WL.TG.
[318] art. 129g ust. 2 pkt 1 lit. a-d w zw. z ust. 3 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym.

pkt 2 Prawa o ruchu drogowym (P.r.d.) w postępowaniach w sprawach o wykroczenia prowadzi czynności wyjaśniające w rozumieniu działu VII ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (K.p.s.w.), kieruje do sądu wniosek o ukaranie w rozumieniu art. 57 § 1 K.p.s.w., oskarża przed sądem oraz wnosi środki odwoławcze – w trybie i na zasadach określonych w tym akcie prawa.

Organ właściwy w sprawie ochrony danych osobowych zauważył, że choć w związku z realizacją zadań, o których mowa w art. 129g ust. 1 i ust. 2 pkt 1 i 2 P.r.d., Główny Inspektor Transportu Drogowego przetwarza dane osobowe na dużą skalę, to – poza unormowaniami zamieszczonymi w art. 129g ust. 2 pkt 1 P.r.d. i art. 129g ust. 2 pkt 2 P.r.d. w zw. z K.p.s.w. – przetwarzanie danych osobowych przez GITD w wyżej wskazanych celach nie jest uregulowane, a z przepisów prawa nie wynika w sposób jednoznaczny zakres danych, które GITD może w tych celach przetwarzać. W praktyce skutkowało to wysyłaniem przez GITD, do osób podejrzewanych o popełnienie naruszeń, formularzy nakładających na te osoby obowiązek przekazania GITD szeregu danych osobowych, które to formularze są stosowane bez podstawy wynikającej z jakiegokolwiek aktu prawnego.

Zdaniem Prezesa UODO sytuacja powyższa może być konsekwencją braku wykonania delegacji ustawowej z art. 129g ust. 5 P.r.d., zaś uregulowanie w przepisach kwestii zakresu danych, które GITD może przetwarzać w związku z ujawnianiem za pomocą stacjonarnych urządzeń rejestrujących zainstalowanych w pasie drogowym naruszeń, oraz ściganiem i karaniem ich sprawców, zapewni realizację zasad przetwarzania danych osobowych określonych w art. 4 ust. 1 dyrektywy 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 uchylającej decyzję ramową Rady 2008/977/WSiSW, implementowanym do polskiego porządku prawnego przez art. 31 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Prezes UODO zwrócił się do Ministra Infrastruktury, jako organu upoważnionego w art. 129g ust. 5 P.r.d. do wydania rozporządzenia oraz sprawującego nadzór nad GITD, o wprowadzenie przepisów, w których zostanie prawidłowo unormowany zakres danych przetwarzanych przez GITD w celu realizacji wskazanych wyżej zadań. W przypadku opracowania projektu tych przepisów organ nadzorczy wniósł o ich przesłanie celem zaopiniowania.

W odpowiedzi na wystąpienie Prezesa UODO Minister Infrastruktury stwierdził, iż przetwarzanie przez GITD danych osobowych w związku z realizacją zadań określonych w art. 129g P.r.d., w zakresie ujawniania za pomocą stacjonarnych urządzeń rejestrujących zainstalowanych w pasie drogowym dróg publicznych naruszeń, odbywa się na podstawie i w granicach prawa powszechnie obowiązującego, z tym że regulacje odnoszące się do przetwarzania poszczególnych danych zawarte są w różnych aktach prawnych. Minister Infrastruktury zwrócił w tym kontekście uwagę na art. 55a oraz art. 56a ustawy z dnia 6 września 2001 r. o transporcie drogowym, rozporządzenie Prezesa Rady Ministrów z dnia 22 lutego 2002 r. w sprawie nakładania grzywien w drodze mandatu karnego oraz rozporządzenie Prezesa Rady Ministrów z dnia 29 czerwca 2011 r. w sprawie nadania inspektorom Inspekcji Transportu Drogowego oraz pracownikom Głównego Inspektoratu Transportu Drogowego uprawnień do nakładania grzywien w drodze mandatu karnego.

W sprawach wykroczeń prowadzonych przez Centrum Automatycznego Nadzoru nad Ruchem Drogowym GITD (CANARD) zastosowanie znajdą również przepisy K.p.s.w. oraz ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (K.p.k.). Przepisy tych dwóch kodeksów szczegółowo określają wymogi wszelkich pism procesowych stosowanych w sprawach o wykroczenia, a na podstawie tych regulacji formułowane są wszelkie pisma procesowe aktualnie stosowane przez CANARD.

Minister Infrastruktury wyjaśnił także, iż w celu realizacji upoważnienia zawartego w art. 129g ust. 5 P.r.d. w resorcie prowadzone były prace nad projektem rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej w sprawie wzorów dokumentów stosowanych przez Głównego Inspektora Transportu Drogowego w postępowaniu w sprawach o wykroczenia. W toku prac legislacyjnych ww. projektu, Rządowe Centrum Legislacji wskazało wątpliwości natury konstytucyjnej i systemowej, w zakresie regulacji dotyczących postępowania w sprawach o wykroczenia ujawnione za pomocą stacjonarnych urządzeń rejestrujących zainstalowanych w pasie drogowym dróg publicznych.

Ze względu na przywołane zastrzeżenia Rządowego Centrum Legislacji, przez kierownictwo ówczesnego resortu transportu, budownictwa i gospodarki morskiej podjęta została decyzja o niewydawaniu rozporządzenia Ministra Transportu, Budownictwa i Gospodarki Morskiej w sprawie wzorów dokumentów stosowanych przez Głównego Inspektora Transportu Drogowego w postępowaniu w sprawach o wykroczenia.

Następnie Ministerstwo Infrastruktury wielokrotnie prowadziło prace legislacyjne zmierzające do uchylenia art. 129g ust. 5 P.r.d. Prace te, oparte na założeniu, że przepisy K.p.s.w. oraz K.p.k.

w wystarczającym stopniu szczegółowo określają wymogi pism procesowych stosowanych w sprawach wykroczeń prowadzonych przez GITD, nie zostały dotychczas sfinalizowane, m.in. z powodu nieuchwalenia przez Sejm Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw.

Minister Infrastruktury poinformował też organ właściwy w sprawie ochrony danych osobowych o trwających w resorcie infrastruktury pracach analityczno-legislacyjnych dotyczących wdrożenia regulacji prawnych obejmujących zmianę trybu odpowiedzialności za naruszenia. W związku z tymi pracami – w opinii Ministra Infrastruktury – podjęcie prac nad projektem rozporządzenia w brzmieniu wynikającym z dotychczasowej delegacji ustawowej z art. 129g ust. 5 P.r.d. byłoby niezasadne.

Jako przykłady innych wystąpień Prezesa UODO wskazać można:

- wystąpienie do Ministra Sprawiedliwości o podjęcie prac legislacyjnych mających na celu doprecyzowanie zasad postępowania z dokumentacją dotyczącą wykonywania nieodpłatnej, kontrolowanej pracy skazanych na cele społeczne[319],
- wystąpienie do Ministra Spraw Wewnętrznych i Administracji dotyczące potrzeby stworzenia przepisów regulujących kwestie postępowania z danymi osobowymi utrwalonymi na zagubionych nośnikach[320].

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 danych oraz rozumieniem tych zjawisk, ze szczególnym uwzględnieniem działań skierowanych do dzieci[321];*
- *upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO[322];*

[319] Opisane w Newsletterze UODO dla IOD 10/2020.
[320] Opisane szerzej na stronie internetowej UODO w materiale dostępnym pod linkiem https://uodo.gov.pl/pl/138/1595.
[321] Art. 57.1.b RODO.
[322] Art. 57.1.d RODO.

- *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*[323].

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 zewnętrzne

W ramach prowadzonej działalności edukacyjnej w 2020 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 przepisy o ochronie danych osobowych w praktyce organów administracji publicznej i innych podmiotów.

W sumie w 2020 r. przeprowadzono **6 szkoleń podmiotów zewnętrznych.**

Jedno z takich szkoleń zorganizowane zostało przez Departament Zdrowia MSWiA dla kadry zarządzającej podmiotami leczniczymi (10.02.2020). Było to kolejne z cyklu szkoleń zorganizowanych z myślą o dyrektorach i kadrze zarządzającej Samodzielnymi Publicznymi Zakładami Opieki Zdrowotnej MSWiA. Tematyka wystąpienia przedstawiciela UODO podczas tego szkolenia uwzględniała zagadnienia zapewnienia skutecznej ochrony danych osobowych w sektorze zdrowia, w kontekście analizy przypadków najczęstszych uchybień w zakresie ich przestrzegania.

Wśród innych podmiotów, które w 2020 r. zwróciły się do Urzędu Ochrony Danych Osobowych z prośbą o przeprowadzenie szkolenia znalazły się Warszawski Uniwersytet Medyczny oraz szkoły i inne placówki oświatowe – wśród nich te, które przystąpiły do programu edukacyjnego TDTS.

[323] Art. 57.1.e RODO.

Wychodząc naprzeciw zapotrzebowaniu na edukację, która od marca 2020 r. za pośrednictwem Internetu przeniosła się ze szkół czy biur do domów ze względu na pandemię koronawirusa, Urząd Ochrony Danych Osobowych zorganizował szereg inicjatyw online w celu wyjaśnienia bieżących problemów związanych ze stosowaniem przepisów RODO w sektorze oświaty. Poniżej przedstawiono wybrane przykłady takich szkoleń.

- **„Praca zdalna nauczycieli a ochrona danych osobowych – porady dla nauczycieli" – (webinarium dla nauczycieli z Polski)[324], 20.05.2020 r.**

Szkolenie odbyło się przy współpracy z Fundacją Rozwoju Systemu Edukacji w ramach platformy eTwinning.

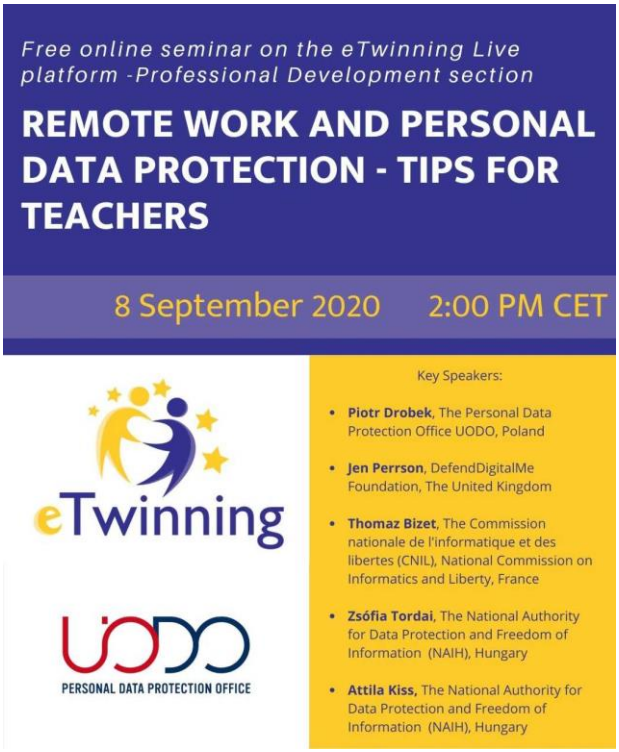
Porady dla nauczycieli w zakresie ochrony danych osobowych podczas wykonywania zdalnej pracy i obowiązki szkoły jako administratora danych były głównym tematem tego szkolenia. Nauczyciele uzyskali wiedzę na temat zasad bezpiecznego przetwarzania danych zawartych w dokumentacji szkolnej (zwłaszcza w sytuacji, gdy nauczyciel korzysta z niej poza szkołą), korzystania z prywatnego sprzętu używanego przez nauczycieli do kontaktu z uczniami, organizowania wideokonferencji, a także ochrony wizerunku jako danej osobowej w kontekście nagrywania przez uczniów i nauczycieli lekcji online. Szkoła reprezentowana przez jej dyrektora jest administratorem w rozumieniu przepisów RODO i to szkoła ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych. Nauczyciele nie są samodzielnymi administratorami danych, a co za tym idzie, nie mogą decydować o celach i sposobach przetwarzania

[324] Szkolenie jest dostępne na stronie internetowej UODO pod adresem: https://uodo.gov.pl/pl/434/1540.

danych. Nauczyciele przetwarzają dane tylko w zakresie realizacji obowiązków służbowych. Realizacja tego wydarzenia odbyła się we współpracy z Krajowym Biurem eTwinning, w ramach akcji „Edukacja zdalna z eTwinning".

- **„RODO w szkolnej ławce – vademecum naruszeń"** – szkolenie zorganizowane 9 czerwca 2020 r. przy współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

- **Praca zdalna a ochrona danych – wskazówki dla nauczycieli (międzynarodowe webinarium online dla nauczycieli z całej Europy), 8.09.2020 r.**



Lekcja została zorganizowana przez UODO we współpracy z Krajowym Biurem eTwinnig oraz z francuskim organem nadzorczym – Krajową Komisją ds. Informatyki i Wolności Obywatelskich (CNIL), węgierskim organem nadzorczym – Krajowym Urzędem Ochrony Danych i Wolności Informacji (NAIH) a także organizacją pozarządową z Wielkiej Brytanii DefendDigitalMe. Wydarzenie poprowadzili: przedstawiciel UODO, przedstawiciel NAIH, przedstawiciel CNIL oraz przedstawiciel brytyjskiej fundacji.

Głównym tematem tego wydarzenia była praca zdalna nauczycieli w kontekście ochrony danych osobowych. Podczas wydarzenia zaprezentowano nauczycielom wymagania dotyczące pracy zdalnej zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO). Ideą inicjatywy była obecna sytuacja, z jaką borykają się kraje europejskie w związku z rozprzestrzenianiem się COVID-19 i nauczaniem zdalnym oferowanym obecnie uczniom. Zadania i obowiązki nauczycieli, uczniów, rodziców oraz inspektora ochrony danych zgodnych z RODO podczas zdalnej edukacji, a także

doświadczenia Węgier, Francji czy Wielkiej Brytanii oraz Polski w tym zakresie były głównymi tematami poruszanymi podczas webinarium.

Szkolenie online dla inspektorów ochrony danych z sektora oświaty, 30.09.2020 r.[325]

W ostatnim czasie pojawiły się liczne pytania dotyczące organizacji nauki zdalnej i zabezpieczenia danych podczas nauki zdalnej. Dlatego Urząd Ochrony Danych Osobowych, wspólnie z Ministerstwem Edukacji Narodowej, zorganizował szkolenie dla inspektorów ochrony danych z sektora oświaty. Było ono uzupełnieniem materiałów opracowanych przez UODO wspólnie z MEN, w których przedstawione zostały zarówno kwestie przetwarzania danych uczniów, ich rodziców czy nauczycieli, jak i praktyczne wskazówki, jak przeprowadzać wideokonferencje, zadbać o sprzęt, na którym pracujemy, itp.

Punktem kulminacyjnym spotkania była debata „E-szkoła na 5! Dobre praktyki zdalnej edukacji". Wzięli w niej udział przedstawiciele UODO, a także specjaliści z zakresu ochrony danych osobowych. Podczas dyskusji zostały przedstawione dobre wzorce nauczania zdalnego oraz zastosowanych rozwiązań. Spotkanie to zainaugurowało cykl szkoleń online, które Urząd Ochrony Danych Osobowych przygotował dla wszystkich zainteresowanych tematyką ochrony danych.

Podkreślenia wymaga, że niektóre szkolenia organizowane przez UODO mają **cykliczny charakter**, jak szkolenie realizowane w ramach XI edycji ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", które online odbyło się w dniach 15-16 października 2020 r.

Ponadto w celu propagowania wiedzy o ochronie danych osobowych prowadzony jest serwis informacyjny **techinfo.uodo.gov.pl**[326], 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.

[325] Szkolenie jest dostępne na stronie internetowej UODO pod adresem: https://uodo.gov.pl/pl/190/1728.
[326] https://techinfo.uodo.gov.pl

1.2. Konkursy

W analizowanym 2020 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 X edycji konkursu dla studentów prawa i administracji na esej dotyczący zagadnień z zakresu ochrony danych osobowych. Jest to kolejna edycja Konkursu dla studentów, który od lat cieszy się niesłabnącym zainteresowaniem.

W kwietniu 2020 r. już po raz X Prezes UODO wraz z partnerem merytorycznym konkursu Kobylańska & Lewoszewski Mednis sp. j. zaprosił studentów kierunków prawa i administracji III-V roku studiów jednolitych oraz I-III roku studiów drugiego stopnia, do udziału w konkursie na esej pt. „*Uzależnienie wykonania świadczenia od wyrażenia zgody na przetwarzanie danych osobowych dla celów marketingowych*". Celem konkursu było propagowanie wiedzy o ochronie danych osobowych i umożliwienie studentom sprawdzenia swojej wiedzy w formułowaniu praktycznych rozwiązań w zetknięciu z realnymi problemami prawnymi. Zadaniem uczestników było przygotowanie rozwiązania kazusu w formie eseju.

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" (TDTS)

W 2020 roku już po raz ósmy 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. Tematem konkursu był spot promujący tematykę ochrony danych osobowych wśród uczniów. Zdobywcą I miejsca i statuetki „Złotego Pióra" Programu została Szkoła Podstawowa im. Króla Jana III Sobieskiego z Puszczy Mariańskiej, nagrodzona za zajęcia edukacyjne pt. „Misio uczy, Misio bawi, Misio dane Ci przedstawi". Jest to pierwsza inicjatywa, która podkreśla wymiar edukacji międzypokoleniowej i prezentuje, jak w ciekawy sposób można wykorzystać tematykę ochrony danych osobowych podczas wydarzeń szkolnych organizowanych z różnych okazji, jednocześnie uświadamiając dzieciom i seniorom znaczenie bezpieczeństwa danych i prywatności w życiu codziennym.

Celem organizowanych konkursów w ramach Programu TDTS jest zachęcenie młodych ludzi do głębszego zainteresowania się problematyką ochrony danych osobowych, promowanie najciekawszych metod edukacji w tym obszarze tematycznym oraz popularyzowanie wiedzy wśród uczniów i nauczycieli.

3) Konkurs Młodych Mistrzów

W ramach 26. Forum Teleinformatyki pt. „System informacyjny państwa wobec globalnej transformacji cyfrowej", które z inicjatywy BizTech Konsulting oraz Polskiej Izby Informatyki i Telekomunikacji odbyło się 24-25.09.2020 r., zorganizowany został konkurs dla studentów i doktorantów polskich uczelni, pod nazwą Konkurs Młodych Mistrzów. Jedną z kategorii Konkursu jest „Najlepsza praca z zakresu ochrony danych osobowych" w dwóch dziedzinach – „Ekonomiczne aspekty informatyzacji Państwa" oraz „Problemy transformacji ustrojowej". Za najlepszą uznana została praca studentki z Politechniki Wrocławskiej pt. „Analiza rozwiązań dla dozorowanego blockchainu, zapewniająca zgodność z RODO".

To kolejna już edycja tego Konkursu, które od kilku lat odbywa się we współpracy z Urzędem Ochrony Danych Osobowych. UODO ma status Partnera i Fundatora Nagrody.

1.3. Projekty i programy

W roku sprawozdawczym 2020 Urząd Ochrony Danych Osobowych kontynuował swój udział w różnego rodzaju projektach. Wśród nich wymienić należy finansowany ze środków Komisji Europejskiej projekt „T4DATA – szkolenie organów ochrony danych i inspektorów ochrony

danych", realizowany w UODO od stycznia 2018 r. oraz 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) T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych

W dniu 8 stycznia 2020 r. zakończył się międzynarodowy projekt **T4DATA – szkolenie organów ochrony danych i inspektorów ochrony danych,** współfinansowany przez Komisję Europejską w ramach Programu „Prawa, równość i obywatelstwo na lata 2016-2020". Celem projektu było wsparcie organów nadzorczych oraz IOD podmiotów publicznych w zakresie szkoleń na temat nowego prawa o ochronie danych osobowych. Prowadzono prace na rzecz jednolitego rozumienia i interpretacji wymogów RODO, a w konsekwencji wzmocnienia 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.

Efektem współpracy w ramach „T4DATA" było opracowanie **„Podręcznika Inspektora Ochrony Danych", który jest zbiorem wytycznych dla IOD dotyczących sposobu zapewnienia zgodności z ogólnym rozporządzeniem o ochronie danych (RODO).** Podręcznik ma zwiększać świadomość i rozumienie roli, kompetencji i głównych obowiązków inspektorów ochrony danych oraz ułatwić tworzenie europejskiej kultury monitorowania, przeglądu i oceny przetwarzania danych. Jest też pomocny w określeniu, jak w kontekście RODO należy patrzeć na status i gwarancje związane z pełnieniem funkcji inspektora. 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 przygotowano jako element materiałów szkoleniowych dla trenerów prowadzących wyżej opisany cykl szkoleń[327].

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. 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[328].

2) **Ogólnopolski program edukacyjny TDTS**

X edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli" w roku szkolnym 2019/2020 oraz rozpoczęcie XI edycji w roku szkolnym 2020/2021.

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 11 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 stanowi doskonałe źródło wiedzy i dobrych praktyk w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty. Rezultatem podejmowanych działań edukacyjnych jest kształtowanie prawidłowych postaw i nawyków wśród dzieci i młodzieży, popularyzacja wiedzy na temat skutecznej ochrony danych

[327] Poradnik jest dostępny na stronie internetowej UODO pod adresem: https://uodo.gov.pl/pl/168/1298.
[328] Platforma jest dostępna na stronie internetowej UODO pod adresem https://t4data.uodo.gov.pl/.

osobowych wśród uczniów i nauczycieli, wzrost zainteresowania tematem oraz współpraca społeczności szkolnej i środowiska lokalnego na rzecz upowszechniania wiedzy o ochronie danych osobowych.

Program „TDTS" – skierowany do szkół podstawowych, ponadpodstawowych oraz ośrodków doskonalenia nauczycieli – jest systemowym projektem edukacyjnym Urzędu Ochrony Danych Osobowych realizowanym na skalę ogólnopolską. Działania w ramach programu są realizowane systemowo, po pierwsze – edukacja dyrektorów szkół i nauczycieli, po drugie – edukacja uczniów i ich środowiska. Atutem jest profesjonalne wsparcie merytoryczne ekspertów UODO oraz organizacja szkoleń i webinariów.

Rocznie w programie bierze udział ponad 45 000 uczniów i ponad 4000 nauczycieli, którzy podejmują różne działania edukacyjne na rzecz upowszechniania wśród uczniów wiedzy o ochronie danych osobowych i prawa do prywatności. Co roku odbywa się ponad 1000 inicjatyw edukacyjnych skierowanych do uczniów, nauczycieli, rodziców, seniorów i środowiska lokalnego.

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 kształtowanie świadomych, odpowiedzialnych i otwartych postaw wśród uczniów w obszarze ochrony danych osobowych. Wspólnie z nauczycielami UODO tworzy ciekawe materiały edukacyjne. W ramach programu Urząd Ochrony Danych Osobowych proponuje atrakcyjne formy i metody pracy z uczniami w różnym wieku, m.in. zabawy, gry edukacyjne, różnorodne zajęcia oraz spotkania i debaty z ekspertami. Praktyczny aspekt edukacji jest tu bardzo ważny. Nie chodzi tylko o nabywanie wiedzy, ale kluczowe jest budowanie świadomości i rozumienie pewnych zjawisk związanych z ochroną prywatności, aby umiejętnie stosować nabytą wiedzę w codziennym życiu. Umiejętności te uczniowie nabywają podczas zajęć lekcyjnych, pozalekcyjnych oraz innych wydarzeń tematycznych organizowanych już lokalnie – w szkołach i placówkach doskonalenia nauczycieli.

W X edycji programu „Twoje dane – Twoja sprawa", organizowanego w roku szkolnym 2019/2020, program realizowało 347 szkół i ośrodków doskonalenia nauczycieli. Największa część uczestników programu to szkoły podstawowe (69 % placówek). Najwięcej szkół jest z województwa mazowieckiego, natomiast najmniej – z województwa opolskiego i podlaskiego.

Do X edycji przystąpiły placówki doskonalenia nauczycieli ze Szczecina, Radomia, Suwałk, Łodzi, Kalisza, Konina, Bydgoszczy, Poznania i Sosnowca, tworząc sieć współpracy w ramach edukacji nauczycieli. 59 % placówek przystąpiło do programu po raz pierwszy. Prawie połowa szkół kontynuuje współpracę z UODO przez kolejne lata, co przyczynia się do utrwalania wiedzy i kształtowania odpowiedzialnych nawyków wśród uczniów.

Od wielu lat program „Twoje dane – Twoja sprawa" cieszy się popularnością i trwale wpisał się w kalendarz szkolnych wydarzeń. Świadczy o tym m.in. liczny udział szkół i placówek w minionych edycjach. W celu utrwalenia tego efektu i wzmocnienia rozpoznawalności programu, od jubileuszowej edycji programu UODO rozpoczął stosowanie nowego systemu identyfikacji wizualnej. Ponadto usprawniono komunikację koordynatorów programu z Urzędem poprzez stworzenie „systemu TDTS", który służy do wymiany informacji oraz materiałów w ramach programu.

Podczas X edycji programu odbyło się **3880 lekcji** poświęconych ochronie danych osobowych i prywatności, w ramach godzin wychowawczych, lekcji informatyki, edukacji wczesnoszkolnej oraz innych lekcji przedmiotowych. **4449 nauczycieli** skorzystało ze szkoleń oferowanych w ramach programu, zaś ok. **1740 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, w których wzięło udział **45 557 uczniów.**

Mimo sytuacji epidemicznej w kraju i edukacji zdalnej, zorganizowano najwięcej, bo **1287 inicjatyw edukacyjnych** skierowanych nie tylko do uczniów i rodziców, ale również do społeczności lokalnej (np. seniorów, przedszkolaków, mieszkańców). A podczas obchodów z okazji **XIV Dnia Ochrony Danych Osobowych (DODO),** który jest obchodzony na świecie 28 stycznia, na przełomie stycznia i lutego 2020 roku we wszystkich województwach odbywały się różne zajęcia oraz wydarzenia tematyczne. W sumie zorganizowano 399 inicjatyw edukacyjnych.

W ramach cyklu konferencji wojewódzkich 28 lutego 2020 r. zorganizowano kolejne spotkanie wojewódzkie pod hasłem **„#RODO w edukacji"**, tym razem w Zamościu. Podczas tego spotkania omówione zostały aktualne aspekty ochrony danych osobowych w sektorze oświaty, przedstawiono założenia programu ze szczególnym uwzględnieniem tematu ochrony danych osobowych osób z niepełnosprawnością i ogromnych potrzeb w tym zakresie. Spotkanie to odbyło się we współpracy

ze Specjalnym Ośrodkiem Szkolno-Wychowawczym w Zamościu, a także Delegatury w Zamościu, Kuratorium Oświaty w Lublinie i Urzędem Miasta Zamość.

W ramach współpracy Ministra Edukacji Narodowej oraz Prezesa Urzędu Ochrony Danych Osobowych powstał **poradnik „Dane osobowe bezpieczne podczas zdalnego nauczania”**, który został rozesłany do szkół oraz udostępniony na stronie internetowej UODO.

Od kwietnia 2020 r. Urząd Ochrony Danych Osobowych rozpoczął cykl porad **„Warto wiedzieć, że…”** dla uczestników programu – uczniów i nauczycieli. Wiele z nich zostało opublikowanych na szkolnych stronach programu oraz wykorzystanych podczas zajęć z uczniami. Porady dotyczyły wielu aspektów związanych m.in. z bezpiecznym użytkowaniem Internetu przez uczniów. Natomiast wyjaśnieniu bieżących problemów związanych ze stosowaniem przepisów RODO w sektorze oświaty w roku szkolnym 2019/2020, poświęcone były szkolenia online, omówione wcześniej w niniejszym sprawozdaniu:

- **„Praca zdalna nauczycieli a ochrona danych osobowych – porady dla nauczycieli”** szkolenie odbyło się 20 maja 2020 r. we współpracy z Fundacją Rozwoju Systemu Edukacji w ramach platformy eTwinning.
- **„RODO w szkolnej ławce – vademecum naruszeń”** – szkolenie zorganizowane 9 czerwca 2020 r. we współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

XI edycja programu „Twoje dane – Twoja sprawa” rok szkolny 2020/2021

Do XI edycji programu TDTS zarejestrowało się ponad **419 placówek oświatowych**. W dniach 15-16 października 2020 r. odbyło się szkolenie online, w którym uczestniczyło 225 koordynatorów ze szkół. W pierwszym dniu szkolenia uczestnicy dowiedzieli się o różnych aspektach ochrony danych w szkołach przedstawionych przez ekspertów UODO, w drugim dniu szkolenia praktyczne aspekty prezentowali przedstawiciele szkół uczestniczących w programie.

W 2020 r. – w obu edycjach tego programu – udział wzięło łącznie 766 placówek (w X edycji – 347 placówek, w XI edycji – 419 placówek).

1.4. Porozumienia o współpracy

Politechnika Warszawska, 11.05.2020 r.

11 maja 2020 r. w Warszawie podpisane zostało porozumienie pomiędzy Prezesem Urzędu Ochrony Danych Osobowych a Rektorem Politechniki Warszawskiej o współpracy w zakresie ochrony prywatności i danych osobowych. Zasadniczym celem podpisanego porozumienia jest świadczenie w tym obszarze pomocy w ramach swoich kompetencji określonych w odpowiednich przepisach. Porozumienie przewiduje, że UODO i PW będą prowadzić wspólne przedsięwzięcia o charakterze naukowo-badawczym, edukacyjnym, organizacyjnym i wydawniczym. W planach jest organizacja seminariów, wykładów, konferencji oraz szkoleń.

Rzecznik Praw Pacjenta, 21.07.2020 r.

Prezes Urzędu Ochrony Danych Osobowych i Rzecznik Praw Pacjenta podpisali porozumienie o współpracy, którego celem jest wzajemne wspieranie się w realizacji ustawowych zadań. Edukacja, współpraca legislacyjna czy wzajemne informowanie o zagrożeniach wymagających wspólnych działań – to obszary, w jakich Prezes UODO i Rzecznik Praw Pacjenta podejmują współpracę. Podpisane pomiędzy nimi porozumienie przewiduje również wzajemne informowanie się w obszarach związanych z realizacją ustawowych zadań obydwu podmiotów, w których obie instytucje przejawiają zainteresowanie bądź posiadają ustawowe kompetencje. Współpraca obu instytucji z pewnością pozwoli lepiej chronić pacjentów, nie tylko poprzez skuteczne reagowanie w sytuacji zagrożenia, ale także poprzez budowanie odpowiedniej świadomości zarówno wśród pacjentów, jak i administratorów danych. Porozumienie ma też za zadanie stworzenie warunków, w których współpraca będzie odpowiednio zorganizowana i nadzorowana przez oba organy. Dlatego też w treści porozumienia zawarto postanowienie o wykorzystaniu potencjału eksperckiego i organizacyjnego obu instytucji.

Pierwszym efektem współpracy w ramach podpisanego porozumienia było wspólne opracowanie „**Wytycznych dotyczących realizacji prawa do informacji przez osoby uprawnione na odległość”**. Problematyka pozyskania informacji o stanie zdrowia pacjenta z wykorzystaniem środków komunikacji na odległość (rozmowy telefoniczne, wideorozmowy) przez osoby uprawnione, w szczególności uwidoczniła się w czasie trwającej epidemii COVID-19. Podmioty lecznicze wprowadziły wówczas ograniczenia osobistego kontaktu pacjenta z osobami bliskimi ze względu na zagrożenie epidemiczne. Nie pozostało to bez znaczenia dla realizacji prawa do informacji o stanie zdrowia pacjenta przez osoby uprawnione, w szczególności z wykorzystaniem możliwości jakie dają nowoczesne technologie.

Wypracowane wytyczne zawierają rekomendowane rozwiązania, które pozwolą na realizację prawa osoby upoważnionej do informacji o stanie zdrowia pacjenta na odległość, z uwzględnieniem praw pacjenta oraz zasad wynikających z regulacji dotyczących ochrony danych osobowych[329].

1.5. Publikacje

Publikacja polskiej wersji wydania z 2018 roku FRA-CoE-EDPS Handbook on European Data Protection Law

W 2020 r. Agencja Praw Podstawowych Unii Europejskiej (FRA) opublikowała polską wersję wydania **FRA-Council of Europe-European Data Protection „Handbook on European Data Protection Law"** z 2018 roku. Z tej okazji, Prezes UODO Jan Nowak otrzymał list od Pana Michaela O'Flaherty z wyrazami podziękowania dla ekspertów Urzędu Ochrony Danych Osobowych, których współpraca z Agencją nad Podręcznikiem była kluczowa dla uzyskania najwyższej jakości tłumaczenia, zarówno z językowego, jak i z koncepcyjnego punktu widzenia.

Sukces wersji angielskiej tej publikacji był dowodem na to, że Podręcznik stanowił ważny punkt odniesienia dla ekspertów i praktyków zajmujących się ochroną danych. Nowa przetłumaczona wersja przyczyniła się do podniesienia świadomości i usprawnienia wdrażania zasad ochrony danych na szczeblu krajowym. Aby kontynuować wspólne wysiłki na rzecz lepszego zrozumienia europejskich przepisów dotyczących ochrony danych, przetłumaczona wersja niniejszego podręcznika została udostępniona na stronie internetowej UODO[330].

„Poradnik RODO. Ochrona danych osobowych w szkołach i placówkach oświatowych" 2 ed.

W listopadzie 2020 r. rozpoczęte zostały prace nad aktualizacją wydanego w 2018 r. **Poradnika RODO. Ochrona danych osobowych w szkołach i placówkach oświatowych,** który z inicjatywy UODO przygotowany został we współpracy z Ministerstwem Edukacji Narodowej. Poradnik ten był kontynuacją materiału wcześniej publikowanego przez Urząd w ramach Programu Edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Publikacja ta zawiera wskazówki dotyczące przetwarzania danych osobowych dzieci, ich rodziców lub opiekunów prawnych, nauczycieli, a także innych pracowników szkół i placówek oświatowych, opisuje podstawowe zasady, jakich dyrektorzy szkół

[329] https://uodo.gov.pl/pl/138/1787
[330] https://www.uodo.gov.pl/pl/457/1594

i placówek oświatowych powinni przestrzegać przy przetwarzaniu danych osobowych oraz przytacza przepisy RODO i sektorowych aktów prawnych, wskazując ich zastosowanie w konkretnych sytuacjach. Publikacja ta miała pomóc dyrektorom szkół i placówek oświatowych w zapewnieniu właściwego przestrzegania nowych regulacji o ochronie danych osobowych.

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 2020 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. Filmy te zrealizowano w formule debat z udziałem ekspertów i były transmitowane na żywo, za pośrednictwem strony: www.uodo.gov.pl. Pierwszą debatą był zapis **transmisji obrad XIV Dnia Ochrony Danych Osobowych,** dostępny na stronie Urzędu Ochrony Danych Osobowych pod adresem: https://uodo.gov.pl/pl/464/1324 .

Tematyka kolejnych dotyczyła następujących zagadnień:

- ***Najczęstsze problemy w działalności IOD,***
- ***Udostępnianie danych osobowych dzieci w Internecie***

1.7. Konferencje, seminaria, spotkania

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

Od połowy marca 2020 r., z chwilą wybuchu pandemii koronawirusa, wydarzenia te organizowane już były w formule online.

Poniżej przedstawione zostały wybrane przykłady wydarzeń krajowych lub międzynarodowych z udziałem Prezesa UODO bądź jego przedstawicieli, które odbyły się w Polsce w 2020 roku. Ich pełny wykaz zawiera załącznik nr 3.

1) XIV Dzień Ochrony Danych Osobowych – 28 stycznia 2020 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. 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.

W 2020 r. Dzień Ochrony Danych Osobowych koncentrował się na tematyce związanej ze stosowaniem przepisów ogólnego rozporządzenia o ochronie danych w polskim systemie prawnym. **Główne obchody Dnia Ochrony Danych Osobowych – organizowane przez UODO – odbyły się 28 stycznia 2020 r. w Warszawie.** W tym dniu miały miejsce dwie debaty. „Najczęstsze problemy w działalności IOD" – to temat pierwszej debaty, po zakończeniu której wręczone zostały Nagrody im. Michała Serzyckiego, Generalnego Inspektora Ochrony Danych Osobowych III Kadencji, przyznawane za działalność na rzecz edukacji w zakresie ochrony danych osobowych i prywatności[331]. Kolejna debata, pt. „Udostępnianie danych dzieci w Internecie", dotyczyła zagadnień związanych z niebezpieczeństwem nadmiernego udostępniania przez rodziców danych osobowych dzieci i młodzieży, w szczególności na portalach społecznościowych. Wszystkie te wydarzenia były transmitowane na stronie internetowej UODO.

Podczas XIV Dnia Ochrony Danych Osobowych uczniowie jednej ze szkół uczestniczących w Ogólnopolskim programie edukacyjnym „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli" (TDTS), spotkali się z Mirosławem Sankiem, Zastępcą Prezesa UODO oraz wzięli udział w specjalnych zajęciach. Poprowadzona w formule zabawy lekcja była okazją do przybliżenia dzieciom wielu kluczowych aspektów dotyczących ochrony ich danych osobowych i prawa do prywatności – w kontekście codziennych sytuacji, których doświadczają w szkole i w domu[332].

[331] https://uodo.gov.pl/pl/p/nagroda-im-michala-serzyckiego; https://uodo.gov.pl/pl/451/1325.
[332] https://uodo.gov.pl/pl/434/1327

W tym dniu w siedzibie Urzędu odbył się **Dzień Otwarty**, podczas którego eksperci UODO udzielali konsultacji i porad prawnych wskazując, jak poradzić sobie ze stosowaniem przepisów ogólnego rozporządzenia[333].

Wzorem lat ubiegłych w obchody Dnia Ochrony Danych aktywnie włączyły się też uczelnie wyższe, z którymi UODO ma zawarte porozumienie o współpracy. Uczelnie te zaplanowały na ten dzień spotkania i konferencje z udziałem ekspertów Urzędu. Wśród nich znalazły się:

- **Konferencja Naukowa pt. „Cyfrowy bliźniak" na Uniwersytecie Wrocławskim, 10.01.2020 r.**

Głównym tematem tego spotkania było nasilające się zjawisko kradzieży tożsamości, zapewnienie skutecznej ochrony danych osobowych w sieci, w szczególności na portalach społecznościowych, a także zagadnienia monitoringu wizyjnego. Przedstawiciele UODO przedstawili prezentacje o najważniejszych zasadach dotyczących publikacji wizerunku zgodnie z przepisami RODO, uprawnień naprawczych regulatora, w tym kwestie administracyjnych kar finansowych, a także omówili stan realizacji ogólnego rozporządzenia o ochronie danych. Organizatorem Konferencji był Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego we współpracy z UODO.

- **Konferencja Naukowa „Wyzwania ochrony danych" na Uniwersytecie Mikołaja Kopernika w Toruniu, 24.01.2020 r.**

Na spotkaniu tym zaprezentowane zostały kluczowe problemy stosowania RODO w kontekście spraw pracowniczych (ochrona danych osobowych w dokumentacji pracowniczej, badania trzeźwości pracownika w miejscu pracy, dopuszczalność stosowania monitoringu wizyjnego dla wykrywania nadużyć pracowniczych i identyfikacji ich sprawców), a także zagadnienia ogólne związane z doświadczeniami kontrolnymi czy orzecznictwem UODO. Organizatorem tego wydarzenia, które odbyło się na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, było Centrum Badań nad Cyberprzestępczością UMK w Toruniu we współpracy z UODO oraz Towarzystwem Naukowym Organizacji i Kierownictwa w Toruniu.

- **Konferencja pt. „Praktyka wykonywania funkcji Inspektora Ochrony Danych" na Politechnice Warszawskiej, 30.01.2020 r**.

[333] https://uodo.gov.pl/pl/451/1328

Podczas Konferencji zorganizowanej w ramach II Dnia Inspektora Ochrony Danych – IOD oraz XIV Dnia Ochrony Danych Osobowych poruszone zostały głównie zagadnienia związane z właściwym przygotowaniem do pełnienia funkcji IOD. Główny nacisk położony został na posiadanie przez IOD fachowej wiedzy z zakresu ochrony danych i nieustanne podnoszenie swoich kwalifikacji zawodowych w tym obszarze. Niezależność oraz wysokie umiejscowienie w strukturze administratora danych – to fundament, na którym powinna opierać się ochrona danych osobowych w danej organizacji. Organizatorami Konferencji byli: SABI Stowarzyszenie Inspektorów Ochrony Danych oraz Wydział Zarządzania Politechniki Warszawskiej.

- **VI Dzień Otwarty UODO 2020 w Akademii Wyższej Szkoły Biznesu w Dąbrowie Górniczej, 7.02.2020 r.**

Akademia Wyższej Szkoły Biznesu w Dąbrowie Górniczej zorganizowała pod patronatem Prezesa UODO **VI Dzień Otwarty Urzędu Ochrony Danych Osobowych** – konferencję tematyczną połączoną z promocją dobrych praktyk w zakresie ochrony danych osobowych. Podczas tego wydarzenia eksperci UODO przedstawili role i zadania w procesie przetwarzania danych osobowych oraz zagadnienia związane z przetwarzaniem danych osobowych w sektorze medycznym.

2) Konferencja pt. „More Than Just a Game". Warszawa, 28.02.2020 r.

More Than Just a Game (MTJG) to konferencja naukowa poruszająca aspekty prawne i kulturowe przemysłu gier wideo i interaktywnej rozrywki. Konferencja ta to polska edycja serii konferencji z cyklu „Mastering the Game" organizowanych przez Ministerstwo Kultury Wielkiej Brytanii[334]. Linklaters Warsaw wspólnie z Queen Mary University of London zaprosili przedstawiciela UODO do udziału w tym wydarzeniu i przedstawieniu zagadnień związanych z bezpiecznym przetwarzaniem danych osobowych w grach komputerowych, w szczególności w grach mobilnych adresowanych do dzieci.

3) #RODO w edukacji, czyli lubelskie spotkanie z ochroną danych osobowych w szkole. Zamość, 28.02.2020 r.

Aktualne wyzwania związane z edukowaniem dzieci i młodzieży na temat ochrony danych osobowych oraz inne działania edukacyjne prowadzone przez Urząd Ochrony Danych Osobowych były tematem przewodnim spotkania przedstawicieli UODO z dyrektorami szkół i nauczycielami. Spotkanie to było kolejnym wydarzeniem, które odbywało się w ramach cyklu „#RODO w edukacji". Spośród 343 szkół i placówek oświatowych, które przystąpiły do X edycji Programu edukacyjnego

[334] https://www.mtjg.co.uk/

UODO „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", 8 było z województwa lubelskiego. Przedstawiciele Urzędu przedstawili słuchaczom podstawowe zasady przetwarzania danych osobowych w pracy poradni psychologiczno-pedagogicznych, kwestie publikacji wizerunku dzieci w Internecie, a także stosowania monitoringu wizyjnego na terenie placówki oświatowej. Ważnym tematem dyskusji była również sprawa edukowania o sposobach postępowania z danymi osobowymi przez uczniów z niepełnosprawnością intelektualną. Uczestnicy spotkania mieli także możliwość omówić indywidualne problemy z konsultantem UODO. Organizatorem Spotkania był Urząd Ochrony Danych Osobowych.

4) Ogólnopolska Konferencja Naukowa pt. „Drony a prywatność". 8.07.2020 online

Konferencja poświęcona była prawnym aspektom funkcjonowania dronów w przestrzeni publicznej, które – celowo lub mimowolnie – mogą służyć pozyskiwaniu danych osobowych[335]. Dlatego w obszarze tematycznym Konferencji znalazły się kwestie dotyczące certyfikacji i bezpiecznej integracji w przestrzeni powietrznej, a także informatyki śledczej w kontekście funkcjonowania bezzałogowych statków powietrznych. Urząd Ochrony Danych Osobowych, który był organizatorem Konferencji, opracował dokument zawierający zbiór tekstów prelegentów, którzy wystąpili podczas tego wydarzenia. W materiałach pokonferencyjnych poruszane były zagadnienia z zakresu odpowiednich rozwiązań prawnych regulujących korzystanie z dronów, w szczególności kwestie ochrony danych osobowych pozyskiwanych za ich pomocą[336].

5) EIT Health Think Tank Roundtable. 15.09.2020 online

Głównym celem spotkania ekspertów przy Okrągłym Stole było wyznaczenie kierunków w rozwoju sztucznej inteligencji (AI) w opiece zdrowotnej, poprzez określenie wpływu AI na pracowników służby zdrowia oraz wyzwań i konsekwencji wprowadzenia i skalowania AI dla organizacji i systemów opieki zdrowotnej w Europie. Zamierzeniem organizatorów było wypracowanie rekomendacji i planu działania na poziomie krajowym, dotyczących zastosowania AI w sektorze opieki zdrowotnej w 6 obszarach: regulacje i ustawodawstwo, finansowanie, działalność kliniczna, edukacja i nowe kwalifikacje, rola danych: jakość, zarządzanie danymi, bezpieczeństwo i interoperacyjność oraz odpowiedzialność i zarządzanie ryzykiem w obszarze sztucznej inteligencji. EIT Health Think Tank Roundtable to jedno z kilku spotkań poświęconych tematowi sztucznej

[335] Więcej na stronie UODO, organizatora tego wydarzenia: https://uodo.gov.pl/pl/138/1582.
[336] E-book został wydany zarówno w formacie *pdf, jak i *epub, opartym na języku XML, służącym do publikowania elektronicznych książek.

inteligencji w obszarze ochrony zdrowia. Podobne spotkania Okrągłego Stołu odbyły się m.in. w Irlandii, Niemczech, Danii, Holandii i Francji. Wnioski z tych spotkań zostały zebrane w formie lokalnych raportów i przedstawione krajowym interesariuszom i ministerstwom. Na koniec wszystkie raporty zostały zebrane w jeden ogólny dokument ramowy (tzw. white paper), który następnie przedstawiony został Europejskiemu Instytutowi Innowacji i Technologii – EIT oraz Komisji Europejskiej.

6) Ogólnopolska Konferencja Naukowa „Status administratora w sektorze publicznym", 5.11.2020 online

Przedstawiciele UODO wystąpili w sesji poświęconej statusowi administratora danych osobowych w złożonych strukturach administracji publicznej oraz w jednostkach samorządu terytorialnego, gdzie na wybranych przykładach omawiano status administratora w porównaniu do statusu pracodawcy oraz modele regulacji statusu administratora w rejestrach publicznych. Przedstawili także zadania i pozycję administratora w sektorze publicznym w świetle prawa UE. Organizatorem Konferencji był Wydział Prawa i Administracji Uniwersytetu Łódzkiego.

1.8. Internet

W 2020 roku prowadzono liczne prace w zakresie modernizacji istniejących systemów informatycznych oraz tworzeniu nowych, w celu usprawnienia realizacji zadań wynikających z kompetencji Prezesa Urzędu Ochrony Danych Osobowych.

System informatyczny zintegrowany z Elektronicznym Zarządzaniem Dokumentacją

W roku 2020 kontynuowano prace nad stworzeniem systemu informatycznego zintegrowanego z Elektronicznym Zarządzaniem Dokumentacją. W tym celu przeprowadzono postępowanie przetargowe na opracowanie, stworzenie i wdrożenie nowoczesnego, zintegrowanego z systemem Elektroniczne Zarządzanie Dokumentacją (EZD) systemu informatycznego do zarządzania, przetwarzania i gromadzenia danych, powstających w toku realizacji zadań wynikających z kompetencji Prezesa Urzędu Ochrony Danych Osobowych, na podstawie obowiązujących przepisów prawa. Zadaniem Systemu jest usprawnienie i skrócenie realizacji ww. zadań. Realizowane w nim procesy biznesowe uwzględniają możliwość dwustronnej wymiany informacji oraz dokumentów z EZD. W tym celu skonfigurowano m.in. platformę testową systemu w infrastrukturze UODO oraz serwer aplikacyjny (serwer z zainstalowanym systemem Windows Serwer). Utworzono również konto w EZD-TEST dla obsługi modułu IOD. Dokonano konfiguracji

środowisk dla wykonawcy. W środowisku UODO zostały przygotowane maszyny wirtualne dla platformy testowej, szkoleniowej oraz produkcyjnej. Dokonano również wymaganej konfiguracji sieciowej pod realizowany system. Zintegrowany System informatyczny UODO składa się z następujących komponentów:

- Modułu postępowań skargowych;
- Modułu zgłaszania naruszeń;
- Modułu decyzji i postanowień;
- Modułu zgłaszania inspektorów ochrony danych;
- Modułu wspomagającego prowadzenie kampanii edukacyjnych;
- Modułu administracyjnego (dostępnego tylko dla użytkowników zarządzających działaniem systemu).

System informatyczny Baza Wiedzy

Zaprojektowano, oprogramowano i wdrożono wewnętrzny system bazy wiedzy. System ma za zadanie ułatwienie dotarcia pracownikom merytorycznym do dokumentów i spraw za pomocą wydajnej i skutecznej wyszukiwarki. W pierwszych kilku dniach działania systemu zaindeksowano do przeszukiwania ponad 5 tysięcy dokumentów o łącznej długości blisko 100 tysięcy stron. System wykorzystuje silnik potężnej wyszukiwarki EleastiSearch. Wyszukiwarka pozwala na wyszukiwanie odmian wyrazów, np. „decyzji" = decyzje, decyzjom, decyzjami. Posiada personalizowane dla użytkownika wyniki wyszukiwania, np. uwzględniając uprawnienia wyszukującej osoby do dokumentu, w którym znajduje się znaleziona fraza.

Platforma do wideokonferencji

Urząd Ochrony Danych Osobowych podjął również działania mające na celu przygotowanie narzędzia do wideokonferencji. Narzędzie zostało postawione na serwerach Urzędu, co gwarantuje najwyższy poziom bezpieczeństwa i pełną poufność informacji.

Wdrożenie nowego systemu certyfikacji

W grudniu 2020 r. wdrożono i skonfigurowano system uwierzytelnienia kartami inteligentnymi oraz infrastruktury klucza publicznego, urządzenia do programowania, odczytu oraz oprogramowania umożliwiającego dostęp do zasobów wewnątrz organizacji, integracji z Active Directory oraz dostępu do systemu poczty elektronicznej. Dostęp możliwy jest zarówno poprzez klienta Outlook, jak i za pomocą Exchange OWA przy wykorzystaniu przeglądarki wraz

z wymaganym wyposażeniem dodatkowym do programowania i personalizacji kart inteligentnych. Wdrożenie systemu certyfikacji podnosi tym samym bezpieczeństwo danych i infrastruktury w Urzędzie Ochrony Danych Osobowych.

Działania w zakresie tworzenia e-usług na platformie ePUAP oraz biznes.gov.pl

Na Elektronicznej Platformie Usług Administracji Publicznej (ePUAP) oraz serwisie Biznes.gov.pl na bieżąco były tworzone usługi niezbędne do sprawnej obsługi spraw prowadzonych przez Urząd Ochrony Danych Osobowych.

28 października 2020 r. na Elektronicznej Platformie Usług Administracji Publicznej (ePUAP), zostały uruchomione nowe e-usługi umożliwiające przesyłanie w formie elektronicznej do Prezesa Urzędu Ochrony Danych Osobowych skarg oraz zawiadomień o naruszeniu przepisów o ochronie danych osobowych. Obecnie są to:

- zawiadomienie o naruszeniu przepisów o ochronie danych osobowych;
- skarga na naruszenie zasad dotyczących przetwarzania danych osobowych z art. 5 rozporządzenia o ochronie danych osobowych (RODO), w tym na nieuprawnione udostępnienie danych podmiotom trzecim;
- skarga na niedopełnienie obowiązku informacyjnego z art. 13 rozporządzenia o ochronie danych osobowych (RODO) – zbieranie danych osobowych od osoby, której te dane dotyczą;
- skarga na niedopełnienie obowiązku informacyjnego z art. 14 rozporządzenia o ochronie danych osobowych (RODO) – zbieranie danych osobowych w sposób inny niż od osoby, której dane dotyczą;
- skarga na naruszenie prawa z art. 15 rozporządzenia o ochronie danych osobowych (RODO) – prawo dostępu przysługujące osobie, której dane dotyczą;
- skarga na naruszenie prawa z art. 16 rozporządzenia o ochronie danych osobowych (RODO) – prawo do sprostowania danych;
- skarga na naruszenie prawa z art. 17 rozporządzenia o ochronie danych osobowych (RODO) – prawo do usunięcia danych;
- skarga na naruszenie prawa z art. 18 rozporządzenia o ochronie danych osobowych (RODO) – prawo do ograniczenia przetwarzania;
- skarga na naruszenie prawa z art. 20 rozporządzenia o ochronie danych osobowych (RODO) – prawo do przenoszenia danych;

- skarga na naruszenie prawa z art. 21 rozporządzenia o ochronie danych osobowych (RODO) – prawo do sprzeciwu.

2. Działalność informacyjna

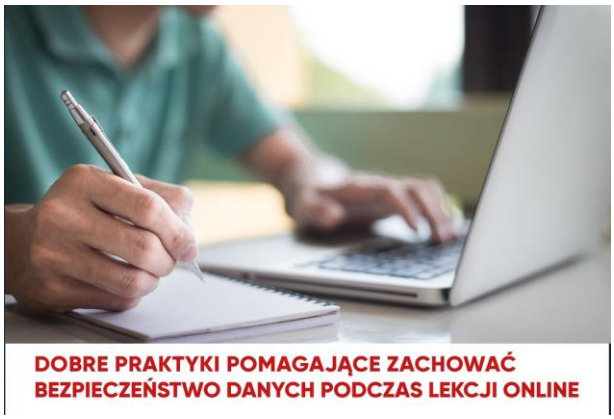
W 2020 r. działalność informacyjna UODO w wielu branżach zdominowana była przez temat pandemii COVID-19 i wynikających z niej skutków dla życia społeczno-gospodarczego. Podobnie jak w latach ubiegłych działalność ta obejmowała wiele obszernych i zróżnicowanych zagadnień tematycznych poświęconych ochronie danych osobowych i zaowocowała inicjatywami służącymi wzmocnieniu bezpieczeństwa danych osobowych w okresie pandemii. W szczególności były to inicjatywy odnoszące się do pracy i nauki wykonywanych w formie zdalnej, a ich adresatami, obok administratorów i inspektorów ochrony danych, były także osoby fizyczne.

Poniżej przedstawiono wybrane materiały graficzne promujące akcje informacyjne Urzędu Ochrony Danych Osobowych w 2020 roku:

Wskazówki dla administratorów (marzec 2020)

Wskazówki dla szkół (marzec 2020)

Wskazówki dla szkół (marzec 2020)



Wskazówki dla administratorów (maj 2020)

Ponadto działania komunikacyjne koncentrowały się na informowaniu o bieżącej działalności organu nadzorczego. Opinia publiczna z dużą uwagą śledziła zwłaszcza informacje dotyczące administracyjnych kar pieniężnych. Wiele uwagi poświęcono także działaniom wspierającym uczestników systemu ochrony danych, a więc w dalszym ciągu UODO skupiało się w sferze informacyjnej na przybliżaniu administratorom i inspektorom ochrony danych zagadnień prawnych dotyczących stosowania RODO.

Wzorem lat poprzednich w 2020 roku działania informacyjne obejmowały:

- współpracę z przedstawicielami mediów,
- prowadzenie działań informacyjno-edukacyjnych poprzez media własne,
- obecność w mediach społecznościowych.

Do głównych działań w sferze informacyjnej, podjętych przez UODO, należały:

- inicjowanie i redagowanie komunikatów oraz tekstów poradniczych udostępnianych na stronie www.uodo.gov.pl i dystrybuowanych do mediów,
- udzielanie odpowiedzi na bieżące zapytania dziennikarzy mediów tradycyjnych i elektronicznych,
- aranżowanie wywiadów z ekspertami UODO i ich wystąpień medialnych,
- obsługa profili UODO w mediach społecznościowych (Twitter, YouTube),
- promocja w mediach programu edukacyjnego „Twoje dane – Twoja sprawa”,
- wsparcie medialne eventów organizowanych przez Urząd lub podmioty zewnętrzne z udziałem jego ekspertów,

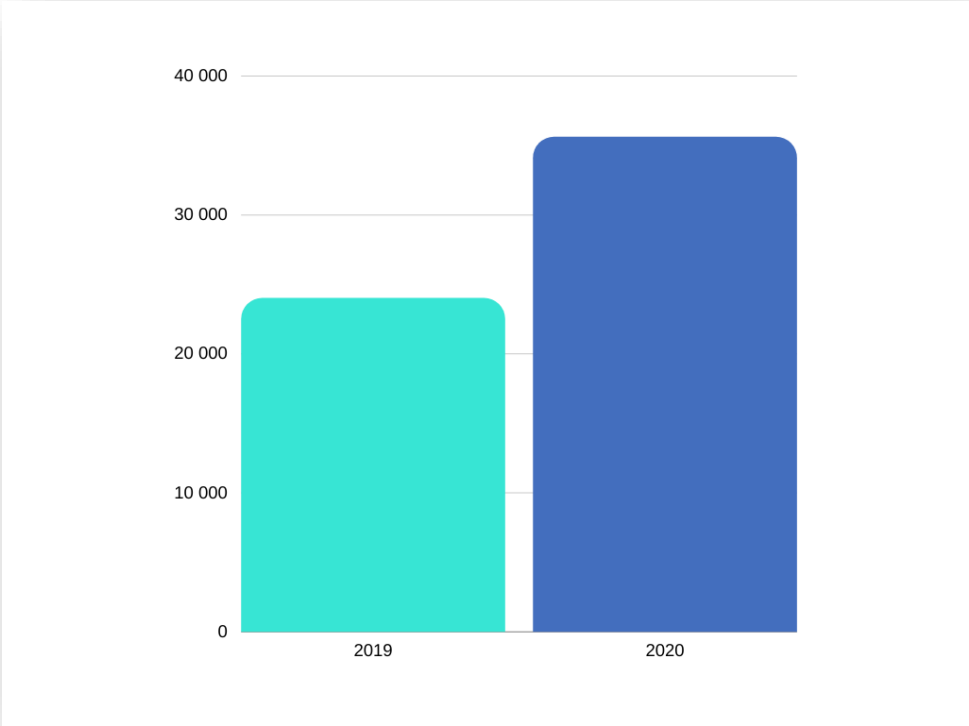
- opracowywanie i cykliczna publikacja „Newslettera UODO dla Inspektorów Ochrony Danych”,
- współtworzenie porad nt. ochrony danych osobowych w publikacjach fachowych,
- produkcja własnych treści wideo.

2.1. Współpraca z mediami

W odniesieniu do stałej współpracy z mediami, w porównaniu do roku 2019 wzrosła liczba opracowanych materiałów dla dziennikarzy, najczęściej w postaci informacji prasowych o tematyce ochrony danych. Przygotowano **169 tego typu opracowań**. Eksperci UODO udzielili blisko **70** wypowiedzi radiowo-telewizyjnych, które w dużej mierze dotyczyły tematów lub były następstwem zdarzeń, wzbudzających zainteresowanie opinii publicznej.

W porównaniu do roku 2019, w analizowanym roku sprawozdawczym odnotowano w mediach wzrost liczby publikacji nt. działalności organu nadzorczego. Łącznie w mediach tradycyjnych i na portalach internetowych ukazało się ponad **36 000** informacji w postaci artykułów (notek) lub wzmianek. Media przede wszystkim prezentowały informacje dotyczące różnorodnych działań związanych z zadaniami i decyzjami Prezesa UODO oraz relacjonowały wydarzenia z udziałem np. Zastępcy Prezesa UODO oraz ekspertów Urzędu. Informowano także o wielu przedsięwzięciach podejmowanych przez UODO.

Dominującym środkiem przekazu nt. działalności UODO, podobnie jak w roku poprzednim, był Internet, co znajduje odzwierciedlenie w liczbie opublikowanych informacji za pośrednictwem mediów internetowych lub internetowych wydań mediów tradycyjnych. Niewiele ponad **34 000** informacji opublikowano na portalach lub w serwisach branżowych wobec **1634** informacji, które ukazały się w prasie drukowanej.



Wykres 10: **Liczba publikacji w mediach na temat działalności UODO w latach 2019-2020.**

W roku sprawozdawczym uwagę mediów zwróciły opublikowane na stronie www.uodo.gov.pl teksty problemowe i poradnikowe. Dużym zainteresowaniem cieszyły się w szczególności wskazówki i rekomendacje Prezesa UODO dotyczące tego, jak należy stosować przepisy RODO i dbać o bezpieczeństwo danych w związku z wyzwaniami, jakie pojawiły się wskutek pandemii COVID-19. Aktywność UODO w tym zakresie miała charakter prewencyjny i obfitowała w akcje informacyjno-edukacyjne, które zostały zauważone zarówno przez media ogólnopolskie i regionalne, jak i lokalne.

Do opracowań najczęściej cytowanych w mediach należały komunikaty poświęcone stanowisku Prezesa UODO odnośnie stosowania przepisów RODO w działaniach służących opanowaniu pandemii oraz w sprawie mierzenia temperatury pracownikom, jako środka zapobiegającego rozprzestrzenianiu się wirusa SARS-CoV-2. Kolejnym tematem, który nawiązywał do trwającej pandemii, a cieszył się niesłabnącym zainteresowaniem mediów, była kwestia zdalnej pracy i nauczania na odległość. Opracowane przez UODO wskazówki dla administratorów stały się tematami głównymi w mediach nie tylko branżowych.

W dalszym ciągu ogromnym zainteresowaniem mediów cieszył się temat badania stanu trzeźwości pracowników przez pracodawców oraz działań zabezpieczających przed utratą danych – zwłaszcza tych, które miały zapobiec kradzieży tożsamości lub stanowiły wskazówkę, jak postępować w przypadku zaistnienia takiego zdarzenia.

W odniesieniu do działań wspierających uczestników systemu ochrony danych, to w obszarze działalności informacyjnej UODO takiemu celowi służyło systematyczne publikowanie wskazówek postępowania odnoszących się do konkretnych sfer działalności administratorów.

Przykładowo, realizowano następujące akcje informacyjne:

W marcu 2020 roku zaprezentowano wskazówki dla właścicieli nieruchomości, którzy zdecydowali się zainstalować monitoring wizyjny na terenie własnych posesji.

W czerwcu 2020 roku UODO opublikowało wskazówki podpowiadające, na co zwrócić uwagę przed zakupem zabawki i jak prawidłowo ją zabezpieczyć, aby nie zagrażała prywatności dziecka.

W lipcu 2020 roku UODO opracowało wskazówki odnoszące się do ochrony danych osobowych podczas wakacji.

Ponadto media informowały o obchodach XIV Dnia Ochrony Danych Osobowych oraz relacjonowały przebieg X i XI edycji programu „Twoje dane – Twoja sprawa". Uwagę mediów przyciągnęły także wydarzenia specjalne, takie jak webinaria tematyczne organizowane przez UODO. Przykładem takiego wydarzenia było szkolenie dla Inspektorów Ochrony Danych z sektora oświaty, zrealizowane 30 września 2020 r.

Plansza tytułowa zapowiadająca szkolenie dla Inspektorów Ochrony Danych Osobowych z sektora oświaty.

Podsumowując, współpraca z mediami była prowadzona zarówno z prasą codzienną o zasięgu lokalnym i ogólnopolskim, jak i ogólnopolskimi pismami branżowymi. Objęła ona także portale internetowe, w tym serwisy tematyczne. Kontynuowana była również współpraca z ogólnopolskimi stacjami telewizyjnymi i radiowymi o profilu informacyjnym oraz społeczno-gospodarczym. Regularna współpraca z czołowymi agencjami informacyjnymi zaowocowała także realizacją wielu

materiałów informacyjnych. Dodatkowo w okresie sprawozdawczym kontynuowano współpracę z redakcjami czasopism fachowych, we współpracy z którymi publikowano cykliczne materiały eksperckie. Efektem współpracy UODO z mediami były patronaty medialne nad wydarzeniami organizowanymi przez Urząd, np. nad XIV Dniem Ochrony Danych Osobowych oraz X edycją programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do szkół i nauczycieli" (TDTS).

2.2. Odpowiedzi na indywidualne pytania dziennikarzy

Szczególne miejsce w realizacji działań informacyjnych zajmuje udzielanie odpowiedzi na indywidualne pytania dziennikarzy. W roku sprawozdawczym 2020 odnotowano **355 pytań** skierowanych do rzecznika prasowego Urzędu, co oznacza **wzrost w stosunku do roku 2019, w którym wpłynęło 340 pytań od dziennikarzy.** Co ważne zaobserwowano bardziej złożony charakter problemów, do których odnosiły się zapytania prasowe. Niejednokrotnie w ramach jednego zapytania prasowego dziennikarze zadawali wiele pytań odnoszących się do różnorodnych aspektów spraw, którymi byli zainteresowani.

Wśród zagadnień, którymi szczególnie interesowali się przedstawiciele mediów były m.in.:

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii, w tym zwłaszcza w odniesieniu do działań związanych z walką lub przeciwdziałaniem rozprzestrzenianiu się wirusa SARS-CoV-2;
- wykorzystywanie danych osobowych na potrzeby marketingu;
- udostępnianie nieznanym podmiotom – przez osoby, których dane dotyczą – szczegółowych informacji na swój temat, sposoby wyłudzania danych i zagrożenia z tym związane;
- odmowa udostępniania informacji publicznej.

Natomiast w odniesieniu do przepisów ogólnego rozporządzenia o ochronie danych, dziennikarze niezmiennie interesowali się zwłaszcza:

- liczbą skarg, pytań oraz zgłoszonych naruszeń,
- nakładaniem kar finansowych na administratorów łamiących zasady ochrony danych osobowych,
- reakcją UODO na wycieki danych,
- przetwarzaniem danych osobowych w związku z organizacją wyborów, w procesie rekrutacji, przez szkoły oraz placówki zdrowia.

2.3. Strona internetowa i media społecznościowe

Rok 2020 był kolejnym, w którym Urząd Ochrony Danych Osobowych koncentrował się na rozwijaniu tzw**. mediów własnych**. Działania informacyjne były prowadzone głównie za pośrednictwem strony internetowej – www.uodo.gov.pl, którą regularnie wzbogacano o liczne materiały informacyjno-edukacyjne z myślą o przedstawicielach różnych systemów ochrony danych. Co miesiąc odnotowywano średnio **150 tys. odsłon**, co świadczy o dużym zainteresowaniu internautów informacjami dostarczanymi opinii publicznej poprzez witrynę internetową Urzędu. Z zasobów strony w roku sprawozdawczym skorzystało **blisko 600 000 użytkowników**, którzy podczas jednorazowego wejścia spędzili na stronie UODO średnio blisko **2 minuty i 40 sekund.** Internauci korzystali z witryny przede wszystkim w dni robocze, a najaktywniej między godzinami 9.00 a 15.00. Większość odwiedzających stronę korzystała z urządzeń desktopowych, a ok. 39% użytkowników witrynę przeglądało na urządzeniach mobilnych.

Istotnym wzmocnieniem działań informacyjnych prowadzonych przez UODO było systematyczne **komunikowanie za pośrednictwem mediów społecznościowych**. Chodzi przede wszystkim o działania informacyjne Urzędu prowadzone w serwisie Twitter. Drugi z profili w mediach społecznościowych – serwis YouTube – został we wrześniu 2020 roku poddany modyfikacji, a dotychczasowy profil zastąpiono nowym.

W 2020 roku UODO prowadził aktywnie działania na swoim profilu Twitter. W 2020 liczba opublikowanych wpisów była o **37%** wyższa niż w 2019 roku. Łącznie pojawiło się **490** tweetów, co spowodowało prawie **2 mln** wyświetleń. Liczba obserwujących profil UODO przekroczyła **4200** użytkowników, z czego dołączyło prawie **1000** nowych „followersów". Informacje o UODO pojawiły się w tym kanale prawie **4300** razy. Na urzędowym profilu Twitter, poza informowaniem o bieżącej działalności organu nadzorczego, została przeprowadzona także kampania edukacyjno-informacyjna Prezesa UODO w związku z drugą rocznicą stosowania w Polsce przepisów RODO. Urząd Ochrony Danych Osobowych promował również w tym medium społecznościowym kampanię informacyjną Europejskiej Rady Ochrony Danych, a także ogólnopolską akcję Prezesa UOKiK „Sprawdzaj, czytaj, pytaj!".

Z kolei nowy kanał UODO na YouTube odnotował w ciągu czterech miesięcy funkcjonowania (między wrześniem a grudniem 2020 r.) ponad 9,1 tys. wyświetleń. Wśród dostępnych materiałów wideo rekordową liczbę odsłon odnotowało nagranie wideo zawierające zapis organizowanego przez Urząd szkolenia dla inspektorów ochrony danych osobowych z sektora oświaty (ponad 3000 wyświetleń).

2.4. Newsletter UODO dla IOD

W 2020 roku kontynuowano wydawanie cyklicznego **„Newslettera UODO dla Inspektorów Ochrony Danych”**. Łącznie w roku sprawozdawczym ukazało się 12 wydań newslettera. O jego popularności świadczy stale rosnąca liczba subskrybentów. Na koniec grudnia 2020 roku newsletter trafiał do **7 565** subskrybentów. To **wzrost o 16%** w porównaniu do analogicznego okresu roku poprzedniego (grudzień 2019 roku – 6501 subskrybentów).

Na ilustracji poniżej przedstawiony został nagłówek tytułowy „Newslettera UODO dla Inspektorów Ochrony Danych”.

W połowie 2020 roku newsletter zmodyfikowano pod względem doboru prezentowanych treści, dostosowując go w większym stopniu do potrzeb czytelników oraz zmieniono jego szatę graficzną. Działanie to było efektem współpracy z samymi czytelnikami, bowiem odpowiedzieli oni na zaproszenie UODO do wzięcia udziału w badaniu ankietowym, w którym poddano ocenie zarówno jakość publikowanych informacji, jaki i sposoby ich prezentacji. Uzyskane odpowiedzi i spostrzeżenia czytelników newslettera posłużyły do ustalenia zakresu zmian, które ostatecznie przeprowadzono.

2.5. Infolinia UODO

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 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.

Ponadto eksperci obsługujący infolinię wskazują osobom poszukującym informacji przydatne opracowania na stronie internetowej UODO lub Europejskiej Rady Ochrony Danych, na których można znaleźć wytyczne i wskazówki z zakresu ochrony danych osobowych. Poprzez infolinię przekazywane były nie tylko informacje związane z działalnością Urzędu, ale także zbierano 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 tych rozmów była bardzo różnorodna. Najczęściej zadawane pytania dotyczyły (oprócz pytań o stan sprawy toczącej się w Urzędzie) następujących zagadnień:

- ochrony danych osobowych podczas pandemii,
- podawania numeru PESEL w punktach sprzedaży węgla,
- legalności kserowania/skanowania dowodów osobistych,
- niechcianego telemarketingu,
- przetwarzania danych osobowych przez pracodawców (także w kontekście pracy poza miejscem jej stałego wykonywania).

Techniczne uwarunkowania infolinii nie pozwalają na przedstawienie dokładnej liczby odebranych połączeń. Niemniej łącznie pracownicy infolinii przeprowadzili w 2020 roku **ponad 13000 rozmów**. Podobnie jak w przypadku indywidualnych pytań od dziennikarzy (patrz pkt. 2.2.) również pytania zadawane za pośrednictwem infolinii odnosiły się do bardzo złożonych problemów. Trzeba mieć też na uwadze, że jedno połączenie, to często kilka pytań od tej samej osoby, dotyczących różnych zagadnień.

W 2020 r. praca ekspertów infolinii została wydłużona o godzinę i obecnie odbywa się od poniedziałku do piątku w godz. 10.00-14.00.

2.6. Inne

W 2020 roku, w ramach prac sieci komunikacyjnej (The EDPB Communications Network), odbyło się 9 spotkań Rzeczników Prasowych organów ochrony danych osobowych.

Grupa ta jest platformą wymiany wiedzy, doświadczeń, działań pomiędzy poszczególnymi członkami Europejskiej Rady Ochrony Danych (dalej także jako: „EROD"). Uczestnicząc w spotkaniach Communications Network, polski organ nadzorczy miał możliwość zapoznania się z działaniami komunikacyjnymi innych organów nadzorczych, z ich interpretacją przepisów oraz z informacjami o nakładanych przez te organy karach. Spotkania poruszały plany działania poszczególnych organów ochrony danych osobowych, a także wspólne działania komunikacyjne w ramach EROD. Każdy komunikat wydawany po posiedzeniach plenarnych Rady był przedmiotem zainteresowań sieci komunikacji Rzeczników Prasowych.

Niemalże cały 2020 rok był związany z walką z rozprzestrzenianiem się COVID-19. Dlatego podczas spotkań Communiactions Netwok temat ten był również wielokrotnie podnoszony. Efektem takich wspólnych prac były np. wytyczne dotyczące pandemii COVID-19, które dotyczyły przetwarzania danych dotyczących zdrowia do celów badań naukowych oraz geolokalizacji i innych narzędzi ustalania kontaktów zakaźnych. Innym, równie istotnym tematem podnoszonym podczas spotkań było przyjęcie przez EROD dokumentu z najczęściej zadawanymi pytaniami, który zawierał wstępne wyjaśnienia i wskazówki w zakresie stosowania instrumentów prawnych do przekazywania danych osobowych do państw trzecich, w tym do Stanów Zjednoczonych (w konsekwencji wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-311/18 Schrems II).

Ponadto w ramach spotkań wspólnie pracowano nad komunikacją w sprawie pierwszej decyzji rozstrzygającej spór na podstawie art. 65 RODO oraz podjęto wspólne działania komunikacyjne dotyczące wydarzeń, takich jak ustalenie przebiegu kampanii z okazji dwulecia stosowania RODO, czy promocja Dnia Ochrony Danych Osobowych.

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. Do zadań Prezesa UODO należy współpraca międzynarodowa z organami nadzorczymi innych państw członkowskich UE oraz wykonywanie obowiązków

wynikających z członkostwa Polski w Unii Europejskiej, w szczególności poprzez współpracę w ramach działań Europejskiej Rady Ochrony Danych (EROD) – ustanowionej ogólnym rozporządzeniem o ochronie danych osobowych (RODO), zastępując Grupę Roboczą Artykułu 29.

W 2020 roku pracownicy UODO brali udział w pracach podgrup eksperckich EROD, które są platformami współpracy organów nadzorczych zrzeszonych w ramach Europejskiej Rady Ochrony Danych, do której należy także Prezes UODO.

Pracownicy UODO uczestniczyli także w obradach **Grup Koordynujących Nadzór nad unijnymi wielkoskalowymi systemami informatycznymi, tj. nad Systemem Informacyjnym Schengen (SIS), Wizowym Systemem Informacyjnym (VIS) oraz Europejskim Zautomatyzowanym Systemem Rozpoznawania Odcisków Palców (EURODAC).** Przedmiotem ich prac była przede wszystkim dyskusja nad funkcjonowaniem systemów w ramach obecnej sytuacji pandemicznej oraz stan prac nad wdrażaniem reformy związanej m.in. z ustanowieniem nowych podstaw prawnych SIS.

1. Współpraca w ramach EROD

EROD jest niezależnym organem europejskim, który działa na rzecz spójnego stosowania zasad ochrony danych w całej Unii Europejskiej, a także promuje współpracę pomiędzy organami nadzorczymi do spraw ochrony danych z UE oraz EOG i EFTA[337].

Do Europejskiej Rady Ochrony Danych należą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego i państw EOG-EFTA lub wspólny przedstawiciel organów nadzorczych, zgodnie z treścią art. 68 ust. 4 RODO, a także Europejski Inspektor Ochrony Danych (dalej także jako: „EIOD") lub przedstawiciele wyżej wymienionych. Komisja Europejska ma prawo uczestniczyć w pracach Rady bez prawa głosu i wyznacza swojego przedstawiciela w Radzie.

Zgodnie z art. 25 Regulaminu wewnętrznego EROD, działa ona poprzez wewnętrzne podgrupy eksperckie, które wspierają Radę w wykonywaniu jej zadań. W spotkaniach podgrup Rady uczestniczą przedstawiciele organów nadzorczych, w tym pracownicy UODO, którzy reprezentują polski organ w 11 grupach z 12 aktualnie istniejących, a także przedstawiciele EIOD i Komisji Europejskiej. Uczestnicząc w pracach podgrup EROD przedstawiciele polskiego organu

[337] Europejskie Stowarzyszenie Wolnego Handlu (EFTA) – międzynarodowa organizacja gospodarcza powstała 3 maja 1960 roku na mocy konwencji sztokholmskiej, mająca na celu utworzenie strefy wolnego handlu artykułami przemysłowymi między państwami członkowskimi drogą redukcji ceł i ograniczeń importowych.

nadzorczego, wraz z reprezentantami pozostałych organów, opracowują: opinie, wytyczne, zalecenia i najlepsze praktyki w celu promowania wspólnego zrozumienia RODO i dyrektywy 2016/680 (tzw. dyrektywy policyjnej), a także biorą udział w doradzaniu Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych w UE. Dokumenty te są następnie przedmiotem dyskusji i zostają przyjmowane podczas comiesięcznych posiedzeń plenarnych EROD, podczas których polski organ nadzorczy reprezentowany jest przez pracowników UODO.

W 2020 roku EROD funkcjonowała w oparciu o przyjęty w 2019 roku program prac na lata 2019-2020. W 2020 roku Rada zorganizowała 27 posiedzeń plenarnych, z czego pierwsze dwa (w styczniu i lutym) odbyły się w siedzibie Rady w Brukseli, która jest jednocześnie głównym miejscem prowadzenia jej działalności. W marcu 2020 r. Światowa Organizacja Zdrowia ogłosiła pandemię COVID-19, w tym też miesiącu Rada nie obradowała. Od kwietnia do końca roku 2020 EROD zbierała się na 25 posiedzeniach plenarnych, obradując w trybie zdalnym. Działając zgodnie z art. 24 Regulaminu wewnętrznego, w związku z zaistniałą sytuacją epidemiczną, EROD podejmowała niektóre decyzje i przyjmowała wybrane, niewymagające dodatkowej dyskusji, dokumenty w trybie procedury pisemnej.

Zgodnie z ustalonym planem oraz w wyniku potrzeby działania *ad hoc* Rada w 2020 roku przyjęła m.in. następujące dokumenty:[338]

- Zalecenia 1/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE – wersja do konsultacji publicznych;
- Zalecenia 2/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru;
- Wytyczne 1/2020 w sprawie pojazdów połączonych i aplikacji związanych z mobilnością – wersja do konsultacji publicznych;
- Wytyczne 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) RODO;
- Wytyczne 3/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19;
- Wytyczne 4/2020 w sprawie wykorzystywania danych dotyczących lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19;
- Wytyczne 5/2020 w sprawie zgody na mocy rozporządzenia 2016/679;

[338] Wszystkie dokumenty przyjęte przez EROD dostępne są na jej stronie internetowej, pod adresem: https://edpb.europa.eu/edpb_pl.

- Wytyczne 6/2020 w sprawie współzależności pomiędzy dyrektywą PSD2 a RODO;
- Wytyczne 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO;
- Wytyczne 8/2020 w sprawie targetowania użytkowników mediów społecznościowych;
- Wytyczne 9/2020 w sprawie pojęcia mającego znaczenie dla sprawy i uzasadnionego sprzeciwu;
- Wytyczne 10/2020 w sprawie ograniczeń praw osób, których dane dotyczą, na podstawie art. 23 RODO;
- Decyzja 01/2020 w sprawie sporu powstałego w związku z projektem decyzji irlandzkiego organu nadzorczego w sprawie Twitter International Company na podstawie art. 65 ust. 1 lit. a) RODO;
- Oświadczenie w sprawie przetwarzania danych osobowych w kontekście pandemii COVID-19 przyjęte 19 marca 2020 r.;
- Oświadczenie EROD dotyczące końca okresu przejściowego Brexitu przyjęte 15 grudnia 2020 r.

2. Współpraca w ramach „Corona Contact Point"

W 2020 roku Urząd Ochrony Danych Osobowych uczestniczył w pracach punktu kontaktowego ds. COVID-19, tzw. „Corona Contact Point", utworzonego podczas pierwszego zdalnego posiedzenia plenarnego EROD, które odbyło się 3 kwietnia 2020 r.

Zadaniem punktu kontaktowego było koordynowanie wymiany informacji w zakresie aktywności organów nadzorczych, m.in. w związku z opracowaniem przez państwa członkowskie specjalnych rozwiązań prawnych związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19. Wymiana tych informacji miała przyczynić się do jednolitego monitorowania i egzekwowania Rozporządzenia 2016/679 w związku z zaistniałą, nadzwyczajną sytuacją związaną z pandemią koronawirusa.

3. Komitet Skoordynowanego Nadzoru – CSC

Jednym z założeń unijnej reformy ochrony danych jest usprawnienie skoordynowanego nadzoru m.in. poprzez ustanowienie spójnego modelu tej formy współpracy organów nadzorczych. Przedstawiciele UODO uczestniczyli w pracach nowoutworzonego Komitetu Skoordynowanego Nadzoru (CSC), którego spotkania organizowane są w ramach Europejskiej Rady Ochrony Danych. Istotnym dokumentem przyjętym przez ww. Komitet był plan prac na lata 2020-2022, w ramach którego wskazano m.in. na konieczność podjęcia działań zmierzających do ułatwienia osobom, których dane dotyczą, możliwości realizacji swoich praw, np. poprzez dokonanie przeglądu dostępnych informacji. W harmonogramie prac ujęto również realizację wspólnych kontroli

i audytów, wymianę doświadczeń w tym zakresie pozyskanych na poziomie krajowym, usuwanie trudności związanych z jednolitą interpretacją przepisów oraz wzajemne przygotowanie organów skupionych w ramach Komitetu do objęcia nadzorem nowych systemów (EES, ETIAS, ECRIS-TCN) i przejęcia zadań od Grupy Koordynacji Nadzoru nad SIS.

W związku z art. 45 rozporządzenia 2016/794 z 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol)[339], Prezes UODO uczestniczy w pracach Rady Współpracy Europolu. W 2020 r. odbyły się dwa spotkania tego organu. Prezes UODO jest – wraz z Europejskim Inspektorem Ochrony Danych – współsprawozdawcą przy aktualizacji podręcznika dla Jednostek Krajowych Europolu (ENU), dotyczącego przetwarzania danych osobowych w systemach Europolu. W toku prac nad aktualizacją podręcznika, Prezes UODO zwrócił się do Komendanta Głównego Policji o informacje na temat problemów i najczęściej pojawiających się wątpliwości dotyczących zgodności przetwarzania danych z przepisami o ochronie danych. Na podstawie uzyskanych informacji Prezes UODO przedstawił swoje stanowisko Europejskiemu Inspektorowi Ochrony Danych, a następnie brał udział w przygotowaniu ankiety dla ENU, która podczas spotkania Rady została zatwierdzona z uwzględnieniem poprawek zgłoszonych przez polski organ nadzorczy.

Ankieta została rozesłana do wszystkich jednostek Europolu w UE za pośrednictwem krajowych organów nadzorczych. Na podstawie uzyskanych informacji Europejski Inspektor Ochrony Danych, przy udziale Prezesa UODO, prowadzi prace nad aktualizacją podręcznika dla krajowych ENU.

4. Sieć Inspektorów Ochrony Danych w ramach EROD

Sieć Inspektorów Ochrony Danych w ramach EROD – DPO Network – ma charakter nieformalnej sieci, mającej na celu wymianę informacji i praktyk pomiędzy inspektorami ochrony danych z poszczególnych organów nadzorczych. Sieć IOD jest niezależna w udzielaniu opinii i porad. Opracowywane w ramach sieci zalecenia są rekomendacjami nieformalnymi, wewnętrznymi i dotyczą wyłącznie organów nadzorczych. W spotkaniach tej grupy uczestniczył Inspektor Ochrony Danych polskiego organu nadzorczego lub jego przedstawiciel.

[339] Dz. Urz. UE L 135/53 z 24.05.2016, str. 53-114.

5. Współpraca w ramach systemu IMI

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 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.

Od 25 maja 2018 r. organy nadzorcze korzystają z systemu wymiany informacji na rynku wewnętrznym – tzw. IMI[340], w celu wymiany, w sposób bezpieczny i ustandaryzowany, informacji niezbędnych dla realizacji mechanizmów współpracy i spójności, przewidzianych w rozdziale VII RODO, i w tym w zakresie prowadzenia postępowań transgranicznych.

System IMI został opracowany przez Dyrekcję Generalną Komisji Europejskiej ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MŚP (DG GROW). Został on dostosowany do potrzeb RODO w ścisłej współpracy z Sekretariatem EROD i organami nadzorczymi. W celu zapewnienia dostosowania systemu do zmieniających się potrzeb organów nadzorczych, w ramach EROD działa specjalna podgrupa ekspercka, która omawia i zatwierdza wszelkie niezbędne zmiany. W ramach systemu IMI organy współpracują, korzystając z procedur uruchamianych na podstawie poniższych przepisów RODO:

- Artykuł 56 – właściwość wiodącego organu nadzorczego (LSA) i organów, których sprawa dotyczy (CSA);
- Artykuł 60 – współpraca między wiodącym organem nadzorczym (LSA) a innymi organami nadzorczymi, których sprawa dotyczy (CSA);
- Artykuł 61 – wzajemna pomoc i dobrowolna wzajemna pomoc;
- Artykuł 62 – wspólne operacje organów nadzorczych;

[340] W języku angielskim: Internal Market Information System – IMI.

- Artykuł 64 – opinia EROD;
- Artykuł 65 – rozstrzyganie sporów przez EROD;
- Artykuł 66 – tryb pilny.

Zgodnie ze statystykami przygotowanymi przez EROD, **od momentu wejścia w życie RODO do 31 grudnia 2020 r.**[341], w rejestrze spraw IMI[342] zarejestrowano **1392** sprawy transgraniczne prowadzone przez organy nadzorcze EOG, z których:

- **1001** zostało zainicjowanych w następstwie wniesionych skarg;
- **391** pochodziło z innych źródeł, takich jak postępowania, inicjatywy organów nadzorczych, zobowiązania prawne, itd.

Z powyższych spraw uruchomiono następujące procedury:

- **361** procedur wzajemnej pomocy (art. 61). Oprócz tego organy uruchomiły **4674** procedury w celu świadczenia sobie dobrowolnej wzajemnej pomocy;
- **512** procedur związanych z mechanizmem kompleksowej współpracy – **One-stop-shop** (art. 60), z których **168** zakończyło przyjęcie ostatecznej decyzji;
- **82** sprawy o charakterze lokalnym (art. 56 ust. 2);
- **1** wspólną operację organów nadzorczych (art. 62);
- **procedury spójności**, w tym: **84** procedury z art. 64 i **1** procedurę z art. 65 zakończoną wydaniem **1** decyzji ostatecznej z art. 65.

Należy przy tym dodać, że po raz pierwszy uruchomiono procedurę z art. 65, czego efektem było przyjęcie 9 listopada 2020 r. przez EROD wspomnianej wcześniej wiążącej Decyzji 01/2020 ws. sporu powstałego w związku z projektem decyzji irlandzkiego organu nadzorczego w sprawie Twitter International Company na podstawie art. 65 ust. 1 lit. a) RODO.

Dodatkowo uruchomiono **2083** procedury w celu zidentyfikowania organów wiodących i organów, których sprawa dotyczy (**183** w toku, 1900 **zakończonych).**

[341] Stan spraw zgodny ze statystykami na dzień 31 grudnia 2020 r., przygotowanymi dla organów nadzorczych przez Helpdesk IMI EROD.

[342] Wpis w rejestrze spraw IMI odnosi się do wpisu w systemie IMI, który umożliwia zarządzanie procedurami współpracy lub spójności od początku do końca. Wpis w rejestrze spraw może polegać na zarządzaniu jedną lub wieloma procedurami związanymi z wpisem do rejestru. Jest to centralny punkt, w którym organy mogą wymieniać się informacjami na temat konkretnych kwestii i wyszukiwać je. Informacje i procedury dotyczące wielu skarg związanych z tym samym przetwarzaniem mogą być połączone w jeden wpis dotyczący jednej sprawy, aby ułatwić wyszukiwanie informacji i spójne stosowanie RODO.

Zgodnie ze statystykami IMI na 31 grudnia 2020 Urząd Ochrony Danych Osobowych:

- był organem wiodącym w **17** sprawach w rejestrze spraw IMI;
- zainicjował łącznie **65** powiadomień, w tym **40** z art. 56 (identyfikacja organu wiodącego i organu, którego sprawa dotyczy), **10** z art. 60 (1 – projekt decyzji, 9 – nieformalne konsultacje), **13** z art. 61 (dobrowolna wzajemna pomoc) i **2** z art. 64 (opinia EROD);
- przesłał łącznie **215** wniosków, w tym: **3** z art. 56 (sprawa lokalna), **74** z art. 61 (wzajemna pomoc), **138** z art. 61 (dobrowolna wzajemna pomoc),
- otrzymał łącznie **69** wniosków, w tym: **1** z art. 56 (sprawa lokalna), **13** z art. 61 (wzajemna pomoc), **54** z art. 61 (dobrowolna wzajemna pomoc), **1** z art. 64 (ostateczna opinia EROD).

6. Pytania prejudycjalne

W ramach współpracy międzynarodowej z organami nadzorczymi innych państw członkowskich UE oraz wykonywania obowiązków wynikających z członkostwa Polski w Unii Europejskiej, Prezes 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 Kancelarię Prezesa Rady Ministrów ze strony Polski odpowiedzi na pytania prejudycjalne TSUE. W 2020 r. Prezes UODO wypowiadał się w tego typu sprawach na różnych etapach postępowań prowadzonych przez TSUE, w tym także w zakresie ewentualnej konieczności zmiany polskiego prawa w wyniku wydania wyroku przez TSUE.

W 2020 r. wpłynęło **13 wniosków o wydanie orzeczeń w trybie prejudycjalnym**[343], co do których Prezes UODO był proszony o wyrażanie swojego stanowiska w zakresie ochrony danych osobowych.

W omawianym okresie sprawozdawczym UODO przygotowywał również informacje mające znaczenie dla stosowania przepisów prawa w Polsce, w kontekście rozstrzygnięcia zapadłego przed Trybunałem EFTA w sprawie E-11/19 Adpublisher w zakresie ochrony danych osobowych w kontekście prawa do wniesienia skargi do organu nadzorczego, rozpoznania skargi przez organ

[343] DOL.0623.2.2020, DOL.0623.5.2020, DOL.0623.9.2020, DOL.0623.11.2020, DOL.0623.14.2020, DOL.0623.19.2020, DOL.0623.17.2020, DOL.0623.21.2020, DOL.0623.23.2020, DOL.0623.24.2020, DOL.0623.29.2020, DOL.0623.30.2020, DOL.0623.32.2020.

nadzorczy bez ujawniania nazwiska i adresu skarżącego oraz zwolnienia z kosztów postępowań odwoławczych[344].

Prezes UODO współpracował także z Zespołem ds. Europejskiego Trybunału Praw Człowieka w Ministerstwie Spraw Zagranicznych, w związku z monitorowaniem spraw, w których zarzucano łamanie prawa do ochronnych danych osobowych przed Europejskim Trybunałem Praw Człowieka[345].

7. Pytania od innych organów nadzorczych

W omawianym okresie sprawozdawczym do Urzędu wpłynęło także **14 pytań od organów nadzorczych innych państw członkowskich**, na które Prezes UODO udzielał odpowiedzi.

Przykładowo francuski organ nadzorczy (CNIL) miał wątpliwości dotyczące krajowych praktyk w zakresie pozyskiwania zgody odnośnie do plików cookies, słowacki organ nadzoru pytał o możliwości wykorzystania danych telekomunikacyjnych do uzyskania informacji o tym, czy obywatele jednego kraju byli w innym państwie (w którym stwierdzono obecność wirusa COVID-19), z kolei pytanie cypryjskiego organu nadzoru dotyczyło krajowych praktyk w zakresie pozyskiwania danych osobowych z wyrzuconych na śmietnik dokumentów, w celu ustalenia sprawcy nielegalnego wyrzucania takich śmieci, odpowiedź dla mołdawskiego organu nadzoru odnosiła się do stosowania systemu monitoringu wizyjnego w zakładach karnych[346], a dla litewskiego organu nadzorczego – polskich przepisów proceduralnych dotyczących kwestii rozpatrywania skarg na przetwarzanie danych osobowych[347]. W 2020 r. Prezes UODO wspomógł także japoński organ nadzorczy w ocenie adekwatności poziomu ochrony danych w UE/EOG w związku z obowiązywaniem decyzji wykonawczej Komisji (UE) 2019/419 z dnia 23 stycznia 2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzającej odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych[348].

Realizując wynikające z art. 61 RODO obowiązki dotyczące wzajemnej pomocy, Prezes UODO wspomógł litewski organ nadzorczy w rozstrzygnięciu kwestii zastosowania wyłączenia, o którym mowa w art. 2 ust. 2 lit. c RODO, do przetwarzania danych osobowych w zamkniętych

[344] DOL.0623.4.2020.
[345] DOL.071.22.2020.
[346] DOL.614.10.2020.
[347] DOL.614.4.2020.
[348] DOL.602.5.2020; https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32019D0419&from=PL

grupach na portalach społecznościowych[349]. W ramach wzajemnej pomocy Prezes UODO odniósł się także do wątpliwości norweskiego organu nadzorczego w zakresie przepisów dotyczących przeciwdziałania praniu pieniędzy w UE oraz przepisów ustanowionych przez amerykańskie Biuro Kontroli Aktywów Zagranicznych (OFAC) w związku z przeglądem wykazu OFAC oraz skonsolidowanego wykazu sankcji OFAC[350]. Polski organ nadzorczy odpowiedział też niemieckiemu organowi nadzorczemu w sprawie ograniczeń w materialnym stosowaniu RODO w zakresie przetwarzania danych osobowych przez polski parlament, jego członków oraz komisje parlamentarne w polskim porządku prawnym.

W 2020 r. Prezes UODO współpracował także z pozostałymi europejskimi organami nadzorczymi w ramach art. 56 RODO w celu ustalenia właściwego wiodącego organu nadzorczego w sprawie wprowadzenia w Europie Facebook Suicide[351]. Prezes Urzędu uczestniczył także – na podstawie art. 60 RODO – w wymianie informacji między wszystkimi europejskimi organami nadzorczymi (One-Stop-Shop Cooperation) w sprawach związanych z aplikacją Facebook Messenger Rooms[352], LinkedIn Supervision[353], oprogramowaniem SIRI[354] oraz planowanych nowych funkcji Facebook[355].

8. Inne sprawy międzynarodowe

Prezes UODO udzielił także odpowiedzi ukraińskiemu Ministerstwu Transformacji Cyfrowej w zakresie polskich unormowań dotyczących obowiązków dostawców usług hostingowych w temacie usuwania nielegalnych treści, w szczególności materiałów przedstawiających seksualne wykorzystywanie dzieci (child sexual abuse material – CSAM), oraz odpowiedzialności za ich nieprzestrzeganie, obowiązku blokowania przez dostawców usług internetowych CSAM hostowanych poza jurysdykcją oraz odpowiedzialności za niezastosowanie się do nich, a także ujawnienia podstawowych informacji o abonencie i danych o ruchu w dochodzeniach dotyczących CSAM.

[349] DOL.614.2.2020.
[350] DOL.614.11.2020.
[351] DOL.612.1.2020.
[352] DOL.614.3.2020.
[353] DOL.614.5.2020.
[354] DOL.614.6.2020.
[355] DOL.614.7.2020.

Prezes UODO opiniował także dokumenty dla Komisji Europejskiej na potrzeby postępowania w sprawie kontroli koncentracji przedsiębiorstw[356]. Przedstawiciel Urzędu uczestniczył również zdalnie w organizowanym przez Komisję Europejską nieformalnym spotkaniu technicznym dotyczącym handlu cyfrowego i przepływu danych.

W roku 2020 UODO udzielił również odpowiedzi na zapytania zawarte w kwestionariuszu zatytułowanym „Badanie dotyczące wymogów lokalizacji danych w transpozycji RODO lub innych wymogów dotyczących danych znajdujących zastosowanie do danych osobowych na poziomie państw członkowskich Unii Europejskiej, które mają wpływ na swobodny przepływ danych osobowych"[357]. Celem tego kwestionariusza było uzyskanie informacji, czy ustawodawstwo niektórych państw członkowskich, wytyczne lub decyzje przewidują postanowienia dotyczące lokalizacji danych, które zakazują lub ograniczają przekazywanie danych osobowych poza ich terytorium lub poza terytorium Unii Europejskiej/EOG. Prezes Urzędu został poproszony o udzielenie odpowiedzi na wszystkie pytania istotne w kontekście krajowego porządku prawnego.

Ze względu na szczególny okres przypadający na rok sprawozdawczy, Prezes UODO opiniował także dokumenty związane z pandemią COVID-19. Przekazywał swoje uwagi do projektu rekomendacji EROD w sprawie wykorzystywania danych lokalizacyjnych i narzędzi śledzenia kontaktów w kontekście wybuchu pandemii COVID-19[358], a także wspomagał Ministerstwo Spraw Zagranicznych w zakresie opiniowania części raportu dotyczącego problematyki wpływu COVID-19 na prawa podstawowe[359]. Przedstawiciel Urzędu brał także udział w webinarium poświęconym wpływowi stanu pandemii na działalność kryminalną na rynku finansowym, organizowanym zdalnie przez organ ds. ochrony danych osobowych w Hong Kongu.

W związku z pracami EROD w 2020 r. Prezes UODO kontaktował się również z Polską Agencją Nadzoru Audytowego (PANA), celem ustalenia w szczególności, czy PANA współpracuje z amerykańską PCAOB, przekazując przy tym dane osobowe, a jeśli tak, to jak jest uregulowana przedmiotowa współpraca[360]. PANA była również informowana przez Urząd m.in. o piśmie do Przewodniczącego Komitetu Europejskich Organów Nadzoru Audytowego (CEAOB) przyjętym podczas 32. Posiedzenia plenarnego EROD, w którym Przewodnicząca EROD wskazała w szczególności, że istnieje możliwość przeprowadzenia wymiany informacji z CEAOB w celu

[356] DOL.0623.25.2020.
[357] DOL.602.1.2020.
[358] DOL.601.2.2020.
[359] DOL.601.7.2020.
[360] DOL.601.6.2020.

wyjaśnienia ewentualnych pytań dotyczących unijnych wymogów w zakresie ochrony danych związanych z opracowywaniem uzgodnień administracyjnych w świetle Wytycznych EROD 2/2020, oraz że do przedmiotowej wymiany mogłaby zostać włączona PCAOB.

W 2020 r. z Prezesem UODO wielokrotnie kontaktowali się przedstawiciele Ministerstwa Rozwoju/Ministerstwa Rozwoju, Pracy i Technologii w związku z pracami nad międzynarodowymi umowami handlowymi, w szczególności w zakresie klauzul dotyczących przepływu danych, ochrony danych osobowych oraz otwartych danych rządowych. Organ nadzorczy przedstawiał w tych kwestiach swoje komentarze[361].

9. Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy

W 2020 r. do Prezesa UODO wpływały zapytania od organów nadzorczych z Europejskiego Obszaru Gospodarczego („EOG") dotyczące wiążących reguł korporacyjnych („WRK") w ponad 50 różnych grupach kapitałowych. Współpraca organów nadzorczych z EOG w toku procedury zatwierdzania WRK odbywa się w eksperckiej podgrupie EROD International Transfers (ITS) z uwzględnieniem mechanizmu spójności przewidzianego w art. 63 RODO i kończy się wydaniem opinii Europejskiej Rady Ochrony Danych.

Zapytania od organów nadzorczych z EOG dotyczyły zgłoszenia ewentualnych zastrzeżeń odnośnie do ustanowienia organu wiodącego w ramach danej procedury zatwierdzania WRK, zmiany organu wiodącego w związku z opuszczeniem przez Wielką Brytanię struktur Unii Europejskiej, ewentualnych komentarzy do projektu konkretnych wiążących reguł korporacyjnych (ich skonsolidowanego projektu, będącego rezultatem współpracy organu wiodącego i pozostałych sprawozdawców) – w przypadku projektów niektórych WRK komentarze do nich były również dyskutowane podczas specjalnych sesji podgrupy ITS dotyczących WRK, w których uczestniczyły inne organy z EOG. W grudniu 2020 r. Prezes UODO podjął się działania w charakterze sprawozdawcy w procedurze zatwierdzania wiążących reguł korporacyjnych prowadzonej przez organ wiodący z EOG.

Jedna grupa przedsiębiorstw wstępnie wyrażała zainteresowanie, aby polski organ nadzorczy działał jako organ wiodący w procedurze dotyczącej zatwierdzenia wiążących reguł korporacyjnych w grupie. Pojawiły się wątpliwości, co do lokalizacji europejskiej siedziby głównej grupy, a tym samym co do ustalenia najbardziej właściwego organu wiodącego. W związku z tym Prezes UODO

[361] DOL.401.234.2020, DOL. 401.364.2020, DOL.401.414.2020.

zwrócił się do grupy z prośbą o informacje, które umożliwią ustalenie organu wiodącego najbardziej właściwego dla dalszego prowadzenia procedury zatwierdzenia WRK w grupie. Jednocześnie grupie zostały zasygnalizowane pewne podstawowe kwestie odnoszące się do przesłanego wstępnego projektu WRK[362].

W innym przypadku prawnik w e-mailu skierowanym do UODO wskazał, że reprezentowany przez niego klient rozważa przeniesienie swojej aplikacji o zatwierdzenie wiążących reguł korporacyjnych do polskiego organu nadzorczego działającego w charakterze organu wiodącego. Polski organ nadzorczy udzielił odpowiedzi na pytania, z którymi zwrócił się wspomniany prawnik[363].

10. Międzynarodowe Warsztaty

1) Warsztaty TAIEX, Kijów 27-28.02.2020 r.

W dniach 27-28 lutego 2020 r. w Kijowie odbyły się Warsztaty poświęcone najlepszym praktykom w zakresie ochrony danych osobowych w Europie. W charakterze krajowego eksperta uczestniczył w nich przedstawiciel UODO. Tematem Warsztatów było przedstawienie informacji na temat przepisów dotyczących ochrony danych osobowych wdrożonych w Unii Europejskiej (rozporządzenie 2016/679) oraz zaznajomienie z decyzjami i procedurami stosowanymi w celu ochrony danych osobowych dla poprawy poziomu bezpieczeństwa, kontroli, regulacji i właściwego przetwarzania danych oraz do wdrożenia tych wymogów do ustawodawstwa ukraińskiego. Warsztaty te były głównym wydarzeniem w ramach prac nad dostosowaniem ukraińskich ram prawnych do standardów europejskich, poprzez wskazanie kwestii praktycznych dotyczących procesu kontroli stanu ochrony danych osobowych podczas ich przekazywania w systemach informacyjnych i telekomunikacyjnych.

Organizatorem Warsztatów był TAIEX we współpracy z Krajową Służbą ds. Specjalnej Komunikacji i Ochrony Informacji Ukrainy (State Service of Special Communication and Information Protection).

2) Warsztaty eksperckie dot. ochrony medycznych danych osobowych, 19.05.2020 r.

Warsztaty eksperckie dotyczące ochrony medycznych danych osobowych to przedsięwzięcie szkoleniowe i konsultacyjne związane z epidemią COVID-19.

[362] DOL.4413.3.2020.
[363] DOL.612.2.2020.

Celem przeprowadzenia warsztatów było zbadanie i przedstawienie przepisów państw członkowskich UE, regulujących przetwarzanie medycznych danych osobowych, z podkreśleniem ewentualnych różnic i zidentyfikowaniem elementów, które mogą mieć wpływ na transgraniczną wymianę tych danych w UE. Podczas dyskusji wskazano, że przetwarzanie medycznych danych osobowych dzieli się na pierwotne i wtórne. W pierwszym przypadku przetwarzanie dotyczy wyłącznie procesu leczenia pacjenta, w drugim zaś dotyczy wszystkich sfer niezwiązanych bezpośrednio z leczeniem, a więc głównie badań naukowych, wymiany informacji dla celów bezpieczeństwa epidemicznego, itd. Konkluzją warsztatów stało się stwierdzenie, iż potrzebne są dalsze prace i konsultacje dla wypracowania wspólnego mechanizmu w UE, regulującego na drodze prawnej zasady dostępu do medycznych danych osobowych.

Organizatorem warsztatów było Konsorcjum EUHealthSupport składające się z: NIVEL (holenderski instytut badań usług zdrowotnych – lider konsorcjum), RIVM (Narodowy Instytut Zdrowia Publicznego i Środowiska Holandii), Infeurope S.A., (AMSE) Stowarzyszenia Szkół Medycznych w Europie e.V, (RCSI) Królewskiej Szkoły Wyższej Chirurgów w Irlandii oraz Leginda GmbH.

3) Warsztaty OECD/GPA z serii COVID-19, 16.09.2020 r.

Wirtualne warsztaty OECD/GPA „The road to recovery: Lessons learned and challenges ahead. *Addressing the data protection and privacy challenges raised by COVID-19"*, poświęcone były zdobytym doświadczeniom i przyszłym wyzwaniom w zakresie ochrony danych i prywatności w związku z pandemią COVID-19. Miały one na celu wymianę dotychczasowych doświadczeń państw na różnych etapach pandemii i posłużyły jako forum dla rządów, organów ochrony danych, pracowników naukowych i innych interesariuszy do dyskusji na temat tego, jak nauka może pomóc w przygotowaniu się państw na przyszłe wyzwania w zakresie ochrony danych i prywatności. Ważna jest tu ocena, czy strategie rządowe ograniczania rozprzestrzeniania się choroby będą skuteczne, niezbędne i proporcjonalne do zagrożenia, oparte na dowodach i czy będą uwzględniały prawa człowieka.

4) Warsztaty EROD nt. prawnie uzasadnionego interesu, 27.11.2020 r.

27 listopada 2020 r. odbyło się online spotkanie interesariuszy EROD nt. prawnie uzasadnionego interesu. Spotkanie miało charakter warsztatów i uczestniczyli w nim, poza przedstawicielami organów nadzorczych, przedstawiciele przedsiębiorstw, organizacji sektorowych,

organizacji pozarządowych, kancelarii prawnych i środowisk akademickich. Celem tego wydarzenia było zebranie opinii i ekspertyz interesariuszy, które miały stanowić pomoc podczas prac EROD nad wytycznymi dotyczącymi prawnie uzasadnionego interesu.

11. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2020 r. Prezes UODO i jego przedstawiciele uczestniczyli online w konferencjach, seminariach i spotkaniach o charakterze międzynarodowym. Wykaz tych wydarzeń znajduje się w załączniku nr 4.

Poniżej przedstawione zostały wybrane przykłady najważniejszych z nich.

1) Spotkanie wirtualne poświęcone pracy zdalnej, 24 i 26.06.2020 r.

Hiszpańskojęzyczna sesja pt. „Nowe modele pracy, nowe zarządzanie", która z udziałem przedstawiciela UODO odbyła się 24 czerwca 2020 r., adresowana była głównie do sektora publicznego. W wystąpieniach podkreślano nie tylko zalety pracy zdalnej, jak jej elastyczność w godzeniu różnych sfer życia czy pozytywny wpływ na zdrowie emocjonalne pracowników. Wskazywano także na potrzebę zapewnienia perspektywy, zgodnie z którą praca zdalna traktowana będzie tak samo, jak inne formy pracy (np. w biurze), bez obaw o dyskryminację osób pracujących zdalnie, np. pod względem rozwoju kariery, niższej płacy, czy też o tzw. oddalenie od środowiska pracy. Moderatorem tej sesji była Hiszpańska Agencja Ochrony Danych (AEPD), która przedstawiła „Program pracy zdalnej" realizowany od 2017 r. na rzecz równości, wspierania godzenia życia osobistego, zawodowego i rodzinnego pracowników.

2) Webinarium „Data protection Views from Strasbourg in Visio", 1-3.07.2020 r.

Biuro Komitetu Konwencji 108 i Jednostka Ochrony Danych w Radzie Europy zorganizowały otwarte webinarium online w celu przedstawienia pracy Komitetu szerszej publiczności, niż delegacjom zwykle uczestniczącym w spotkaniach w Strasburgu. Tematyka sesji została przygotowana specjalnie po to, by uczestnicy mogli dowiedzieć się, co robi Rada Europy w kwestiach związanych z ochroną danych osobowych.

Webinarium *Data protection Views from Strasbourg in Visio*, które z udziałem przedstawiciela UODO odbyło się w dniach 1–3 lipca 2020 r. (daty te zostały pierwotnie zaplanowane na 40. Posiedzenie Plenarne Komitetu, które musiało zostać przełożone w związku z pandemią COVID-19), zostało podzielone na 6 sesji tematycznych. W trakcie obrad uczestnicy zastanawiali się, co zrobić w celu zapewnienia, aby kraje, które zobowiązały się do Konwencji 108+, przestrzegały jej

postanowień. Dyskutowano nad mechanizmem monitorowania i oceny, profilowania, sztucznej inteligencji, prawie do ochrony danych osobowych w środowisku edukacyjnym oraz o programach tożsamości cyfrowej i identyfikacji cyfrowej. Ostatni dzień webinarium poświęcony był zagadnieniom związanym z rozpoznawaniem twarzy oraz kwestiom związanym z ochroną danych osobowych w kampaniach politycznych. Po każdej sesji tematycznej był czas na odpowiedzi na pytania zadawane przez uczestników webinarium, bezpośrednio oraz przez narzędzie pytań i odpowiedzi w formie czatu.

Prezentacje prelegentów dostępne są na stronie internetowej Rady Europy[364].

3) Spotkanie online „Follow the Sun: A Digital Launch of the Data Protection Handbook" (2nd ed.), 1.09.2020 r.

Przedstawiciele Urzędu Ochrony Danych Osobowych wzięli udział w wydarzeniu online, inaugurującym publikację drugiego wydania „Podręcznika o ochronie danych w działaniach humanitarnych" („Handbook on data protection in humanitarian action"). Wydarzenie zostało zorganizowane przez Global Privacy Assembly i Międzynarodowy Komitet Czerwonego Krzyża. Uczestnicy wzięli udział w kilku interesujących panelach dotyczących ochrony danych osobowych w zakresie m.in.: tożsamości cyfrowej i biometrii, Covid-19 i aplikacji do śledzenia kontaktów, korzystania z mediów społecznościowych i aplikacji do przesyłania wiadomości, Blockchain oraz sztucznej inteligencji i uczenia maszynowego[365].

4) EIT Health Think Tank Roundtable, 15.09.2020 r.

Głównym celem spotkania ekspertów przy Okrągłym Stole było wyznaczenie kierunków w rozwoju sztucznej inteligencji (AI) w opiece zdrowotnej, poprzez określenie jej wpływu na pracowników służby zdrowia oraz wyzwań i konsekwencji wprowadzenia i skalowania AI dla organizacji i systemów opieki zdrowotnej w Europie. Zamierzeniem Organizatorów było wypracowanie rekomendacji i planu działania na poziomie krajowym, dotyczących zastosowania AI w sektorze opieki zdrowotnej w 6 obszarach: regulacje i ustawodawstwo, finansowanie, działalność kliniczna, edukacja i nowe kwalifikacje, rola danych: jakość, zarządzanie danymi, bezpieczeństwo i interoperacyjność oraz odpowiedzialność i zarządzanie ryzykiem w obszarze sztucznej inteligencji. EIT Health Think Tank Roundtable to jedno z kilku spotkań poświęconych tematowi sztucznej inteligencji w obszarze ochrony zdrowia. Podobne spotkania Okrągłego Stołu odbyły się m.in.

[364] https://www.coe.int/en/web/data-protection/data-protection-views-from-strasbourg-in-visio-1-3-july.
[365] Link do wydarzenia wraz z programem można znaleźć na stronie Międzynarodowego Komitetu Czerwonego Krzyża: https://www.icrc.org/en/event/data-protection-handbook-launch.

w Irlandii, Niemczech, Danii, Holandii i Francji. Wnioski z tych spotkań zostały zebrane w formie lokalnych raportów i przedstawione krajowym interesariuszom i ministerstwom. Na koniec wszystkie raporty zostały zebrane w jeden ogólny dokument ramowy (tzw. white paper), który następnie przedstawiony został Europejskiemu Instytutowi Innowacji i Technologii – EIT oraz Komisji Europejskiej.

5) 50. Posiedzenie Biura Komitetu Konwencji nr 108 Rady Europy, 28-30.09.2020 r.

W 50. Posiedzeniu Biura Komitetu Konwencji nr 108 spotkało się online ponad 50 ekspertów ds. ochrony danych reprezentujących nie tylko państwa będące stronami Konwencji 108, ale także wielu obserwatorów. W sumie w spotkaniu tym wzięło udział 113 osób.

Uczestnicy kontynuowali dyskusje na priorytetowe tematy Komitetu Konwencji, takie jak rozpoznawanie twarzy, dane osobowe przetwarzane w kontekście systemów edukacji, profilowanie, tożsamość cyfrowa, przetwarzanie danych osobowych w kontekście kampanii politycznych oraz mechanizm monitoringu i oceny Konwencji 108[366].

6) Spotkanie coachingowe EROD, 29.09.2020 r.

W związku z przygotowanym w ramach Europejskiej Rady Ochrony Danych dokumentem dotyczącym strategii EROD, 29 września 2020 r. zorganizowano wirtualne wydarzenie coachingowe, mające na celu przeprowadzenie otwartej i szczerej dyskusji na temat przyszłego kierunku działań EROD. Założeniem nie była dyskusja merytoryczna nad tym dokumentem, lecz skoncentrowanie się na kwestii, w jaki sposób członkowie EROD mogą współpracować, aby osiągnąć cele zakładane w strategii. W wydarzeniu uczestniczyli przewodniczący organów nadzorczych bądź ich przedstawiciele, wśród nich – przedstawiciele polskiego organu nadzorczego.

7) 42. Międzynarodowa Konferencja Global Privacy Assembly, 13-15 października 2020 r.

W dniach 13-15 października 2020 r. – z udziałem przedstawiciela UODO – odbyła się sesja zamknięta Międzynarodowej Konferencji Global Privacy Assembly (GPA), po raz pierwszy w formie online. Gospodarzem wydarzenia był Sekretariat GPA, którego obsługę zapewnia Urząd Rzecznika Informacji Zjednoczonego Królestwa. W tym najważniejszym corocznym spotkaniu Global Privacy Assembly, zrzeszającym m.in. przedstawicieli organów ochrony danych osobowych

[366] Raport z 50. posiedzenia zawierający porządek obrad i dokumenty robocze, można znaleźć tutaj: https://rm.coe.int/t-pd-bur-2020-50rap-en/16809fd6bc.

z całego świata, Europejskiego Inspektora Ochrony Danych i Rady Europy, uczestniczyło ponad 100 członków i obserwatorów GPA[367].

8) Webinarium Światowej Organizacji Handlu, 10.11.2020 r.

10 listopada 2020 r. odbyło się webinarium zorganizowane przez Światową Organizację Handlu (WTO) pt. „Different models to facilitate the cross-border exchange of personal data" („Różne modele służące ułatwieniu transgranicznej wymiany danych osobowych"). Tematem webinarium była analiza wszystkich instrumentów regulujących transgraniczne przepływy danych osobowych pod kątem zagwarantowania poufności, integralności i dostępności danych osobowych. Omówione zostały takie mechanizmy, jak system certyfikacji (np. Transgraniczne Zasady Przekazywania APEC), standardowe klauzule umowne, wiążące reguły korporacyjne czy ocena adekwatności stopnia ochrony. Mówcy przedstawili różne podejścia do ułatwienia transgranicznej wymiany danych osobowych, dążąc w ten sposób do osiągnięcia równowagi między potrzebą zabezpieczenia ochrony prywatności i danych osobowych a rosnącymi możliwościami rynku cyfrowego.

Wydarzenie to wpisało się w cykl organizowanych przez WTO webinariów „Zarządzanie przepływami ochrony danych a handel"[368].

9) 40. posiedzenie plenarne Komitetu Konwencji nr 108 Rady Europy (Komitetu T-PD), 18-20.11.2020 r.

Po 50. posiedzeniu Biura we wrześniu 2020 r. rozpoczęła się trzydniowa 40. sesja plenarna Komitetu Konwencji nr 108. Ponad 100 uczestników ze wszystkich regionów świata połączyło się, aby omawiać różne aktualne tematy dotyczące ochrony danych, finalizować ważne dokumenty i przyczyniać się do opracowywania polityki. Komitet kontynuował prace nad najważniejszymi tematami, jak: rozpoznawanie twarzy, tworzenie profili, ochrona danych dzieci w placówkach edukacyjnych, tożsamość cyfrowa, przetwarzanie danych osobowych przez organizacje odpowiedzialne za kampanie polityczne, itp.[369] W trakcie 40. posiedzenia plenarnego, Komitet Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem

[367] Szczegółowe informacje oraz przyjęte rezolucje dostępne są na stronie UODO: https://uodo.gov.pl/pl/460/1742.
[368] Prezentacje poszczególnych mówców dostępne są w języku angielskim pod adresem: https://www.wto.org/english/res_e/reser_e/tradedialogueslseries_e.htm.
[369] Raport z 40. Posiedzenia Komitetu TP-D, w tym porządek obrad i dokumenty robocze można znaleźć tutaj: https://rm.coe.int/t-pd-2020-40rap-en/1680a07084.

danych, przyjął **Wytyczne dotyczące ochrony danych dzieci w środowisku edukacyjnym**[370]. Wytyczne wyjaśniają kwestie związane z realizacją podstawowych zasad dotyczących praw dziecka w placówkach edukacyjnych w kontekście ochrony danych osobowych. W ocenie autorów Wytycznych, prawo do prywatności i ochrony danych osobowych są prawami komplementarnymi w stosunku do innych praw dziecka, uwzględniającymi jego dobro, zmieniające się możliwości dziecka, prawo do bycia wysłuchanym oraz prawo do niedyskryminacji. Eksperci Urzędu Ochrony Danych Osobowych przygotowali nieoficjalne tłumaczenie Wytycznych na język polski, które zostało opublikowane na stronie internetowej UODO[371].

10) 51. Posiedzenie Biura Komitetu Konwencji nr 108 Rady Europy, 16-18.12.2020 r.

51. Posiedzenie Biura Komitetu Konwencji nr 108 odbyło się z udziałem wielu ekspertów ds. ochrony danych i obserwatorów reprezentujących państwa będące stronami Konwencji 108, w tym przedstawiciela Urzędu Ochrony Danych Osobowych. Uczestnicy spotkania kontynuowali dyskusje na priorytetowe tematy, takie jak: rozpoznawanie twarzy, profilowanie, tożsamość cyfrowa, przetwarzanie danych osobowych w kontekście kampanii politycznych, mechanizm monitoringu i oceny Konwencji 108 oraz transgraniczny dostęp do danych organów ścigania[372].

V. Podsumowanie

Przechodząc do podsumowania niniejszego *Sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2020,* 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

[370] https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b
[371] https://uodo.gov.pl/pl/138/1824
[372] Raport z 51. Posiedzenia Biura Komitetu TP-D, w tym porządek obrad i dokumenty robocze, można znaleźć tutaj: https://rm.coe.int/t-pd-bur-2020-51rap-en/1680a0d004

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 można stwierdzić, że po upływie drugiego roku stosowania nowego prawa o ochronie danych osobowych organowi nadzorczemu udało się 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 był rokiem pierwszego całościowego przeglądu działania przepisów RODO. Zadanie to wynikało 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[373]. Prowadzona była też w Unii Europejskiej dyskusja na temat sektorowych przepisów dotyczących ochrony danych.

Strategia EROD na najbliższe lata ujęta została w 4 podstawowe filary, które zapowiadają wspieranie harmonizacji i ułatwianie przestrzegania przepisów (1. filar), wspieranie skutecznego egzekwowania prawa i skutecznej współpracy między krajowymi organami nadzorczymi (2. filar), podejście do nowych technologii oparte na prawach podstawowych (3. filar) oraz wymiar globalny w odniesieniu do promowania instrumentów transferu danych gwarantujących równorzędny poziom

[373] 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 .

ochrony, w tym współpraca członków EROD z organami nadzorczymi państw trzecich w szczególności w zakresie egzekwowania prawa (4. filar).

Realizacja zadań w ramach tak zakreślonej strategii odbywała się w cieniu pandemii COVID-19, która doprowadziła na całym świecie do przeorganizowania działania instytucji sektora prywatnego i publicznego na niespotykaną dotąd skalę. Pandemia doprowadziła do ogromnej eskalacji i wzrostu ilości przetwarzanych informacji, w tym danych osobowych. W tych warunkach na administratorach danych spoczął szczególny obowiązek, aby tę poszerzoną, także zakresowo, ilość informacji przetwarzać w sposób zgodny z określonymi standardami dotyczącymi zarówno ochrony danych osobowych, jak i z innymi przepisami prawa – chociażby odnoszącymi się do zarządzania kryzysowego, świadczenia usług medycznych lub do walki z cyberprzestępczością. W tych wszystkich procesach wykorzystywane są różnego rodzaje dane, różnych kategorii, w różnym zakresie i odnoszące się do różnych osób.

Przepisy RODO nie zostały zawieszone na czas pandemii. Jak wynika z wytycznych EROD (4/2020), organ ten – wskazując na wykorzystywanie danych osobowych chociażby do lokalizacji i narzędzi do śledzenia kontaktów zakaźnych w czasie pandemii – wyraźnie wskazał **na konieczność poszanowania zasad ochrony danych osobowych w tym czasie, aby zbudować także społeczną akceptację tych rozwiązań, które będą ograniczały sferę decydowania o prywatności obywateli.**

W tym zakresie, w ramach zarządzania danymi w trakcie pandemii, konieczne jest wprowadzenie określonych – przejrzystych i jasnych zasad zarządzania danymi osobowymi. Kluczowe znaczenie dla jednolitego stosowania przepisów ma działalność EROD. Dokumenty przyjmowane przez Radę, takie jak wytyczne, zalecenia i najlepsze praktyki mają na celu zagwarantowanie spójnego podejścia organów nadzorczych. Praktyka administratorów w różnych państwach członkowskich nie musi i nie może, z uwagi na różniące się przepisy krajowe, być identyczna, ale przepisy RODO i wydawane w związku z nimi wskazówki, jak je interpretować, mają zapewnić spójność i jednolitość podejścia do ochrony danych.

Prezes UODO jest członkiem EROD, z tego powodu UODO wnosi wkład i uczestniczy w przygotowywaniu dokumentów EROD.

Podsumowując, w oparciu o analizę zakresu tematycznego pytań prawnych kierowanych do Urzędu 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.

I choć w codziennej praktyce Urzędu zdarzają się problemy z właściwym stosowaniem RODO, to w dużej mierze wynikają one z niespójności lub niejasności przepisów sektorowych. Dlatego Prezes UODO podejmuje działania mające na celu ich eliminację, np. przygotowywanie materiałów informacyjno-edukacyjnych, czy kierowanie wystąpień o rozważenie stosownych zmian prawa. Instrumentem pomocnym w zapewnieniu zgodności z RODO mogą być także wspomniane 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.

Od 1 grudnia 2019 r. w miejsce dotychczasowych Zespołów tematycznych utworzone zostały nowe Departamenty. Nowa struktura Urzędu, porządkująca organizację i podział zadań poszczególnych jednostek organizacyjnych, jasno określa kompetencje organu i ułatwiła realizację zadań wynikających z RODO i ustawy o ochronie danych osobowych.

Jest to szczególnie ważne, gdy weźmie się pod uwagę wciąż rosnące zainteresowanie obywateli problematyką ochrony danych osobowych i działalnością organu nadzorczego. Niejednokrotnie publikowane na stronie internetowej komunikaty Urzędu, informujące np. o wydanych przez Prezesa UODO decyzjach administracyjnych w przedmiocie kar pieniężnych, powodowały wzmożone zainteresowanie zagadnieniami ochrony danych osobowych.

ZAŁĄCZNIKI

Załącznik nr 1

Wykaz administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2020 r.

L.p.	Data decyzji	Departament prowadzący postępowanie	Sygnatura	Administrator	Wysokość kary w zł
1.	18.02.2020	Departament Skarg	ZSZZS.440.768.2018	Szkoła Podstawowa	20 000,00
2.	20.03.2020	Departament Kontroli i Naruszeń	ZSPR.421.19.2019	Vis Consulting Sp. z o.o.	20 000,00
3.	29.05.2020	Departament Kar i Egzekucji	DKE.561.1.2020	East Power Sp. z o.o.	15 000,00
4.	03.06.2020	Departament Kar i Egzekucji	DKE.561.2.2020	Przedsiębiorca prowadzący przedszkole	5 000,00
5.	02.07.2020	Departament Kar i Egzekucji	DKE.561.3.2020	Główny Geodeta Kraju	100 000,00
6.	21.08.2020	Departament Kontroli i Naruszeń	ZSOŚS.421.25.2019	Szkoła Główna Gospodarstwa Wiejskiego	50 000,00
7.	24.08.2020	Departament Kontroli i Naruszeń	DKN.5112.13.2020	Główny Geodeta Kraju	100 000,00
8.	03.12.2020	Departament Kontroli i Naruszeń	DKN.5112.1.2020	Virgin Mobile Polska Sp. z o.o.	1.968.524,00
9.	09.12.2020	Departament Kar i Egzekucji	DKE.561.13.2020	Smart Cities Sp. z o.o.	12.838,20
10.	09.12.2020	Departament Kontroli i Naruszeń	DKN.5131.5.2020	TUiR Warta S.A.	85.588,00
11.	17.12.2020	Departament Kontroli i Naruszeń	DKN.5130.1354.2020	ID Finance Poland Sp. z o.o. w likwidacji	1.069.850,00

Załącznik nr 2

Wykaz wydarzeń objętych patronatem Prezesa UODO w 2020 r.

1. Konferencja Naukowa pt. „Wyzwania ochrony danych osobowych” zorganizowana w ramach obchodów XIV Europejskiego Dnia Ochrony Danych Osobowych. Organizatorzy: Wydział Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu oraz Towarzystwo Naukowe Organizacji i Kierownictwa w Toruniu. Toruń, 24.01.2020 r.
2. Konferencja z cyklu II Dzień IOD: „Praktyka wykonywania funkcji Inspektora Ochrony Danych Osobowych”. Organizatorzy: SABI – Stowarzyszenie Inspektorów Ochrony Danych, Wydział Zarządzania Politechniki Warszawskiej. Warszawa, 30.01.2020 r.
3. VI Dzień Otwarty UODO w Akademii WSB w Dąbrowie Górniczej, w ramach obchodów XIV Dnia Ochrony Danych Osobowych. Organizator: Akademia WSB w Dąbrowie Górniczej. Dąbrowa Górnicza, 7.02.2020 r.
4. Konferencja Naukowa pt. „Ochrona danych osobowych w zbiorowym prawie pracy”. Organizator: Zakład Prawa Pracy Kolegium Prawa Akademii Leona Koźmińskiego. Warszawa, 3.03.2020 r.
5. X Konferencja Naukowa „Prawo w dobie cyfryzacji”. Organizatorzy: Katedra Teorii Prawa i Państwa WPiA UMK w Toruniu oraz Studenckie Koło Naukowe Prawa Nowych Technologii UMK w Toruniu. Toruń, 24-25.03.2020 r.
6. Konferencja pt. „AI w zdrowiu”. Organizatorzy: Polska Federacja Szpitali oraz Ambasada Brytyjska. Warszawa, 26.03.2020 r.
7. IX Konwent Ochrony Danych Osobowych i Informacji pt. „RODO w praktyce, czyli ochrona danych osobowych na co dzień”. Organizatorzy: Lubasz i Wspólnicy – Kancelaria Radców Prawnych Sp. k. oraz FORSAFE Sp. z o.o. Łódź, 7.10.2020 r.
8. I Kongres Inspektorów Ochrony Danych, organizowany w ramach XVIII Samorządowego Forum Kapitału i Finansów. Organizatorzy: Pismo Samorządu Terytorialnego „Wspólnota” oraz Municipium S.A. Katowice, 7-8.10.2020 r.
9. Ogólnopolska Konferencja Naukowa online, pt. „Status administratora w sektorze publicznym”. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją, działające na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, 5.11.2020 r.

Załącznik nr 3

Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2020 r. w Polsce przez UODO lub inne podmioty

L. p.	Data	Wydarzenie	Miejsce
1.	9.01.2020	Seminarium SABI dot. oceny skutków dla ochrony danych, działalności marketingowej i zarządzania realizacją praw osób. Organizator: SABI – Stowarzyszenia Inspektorów Ochrony Danych.	Warszawa
2.	10.01.2020	Konferencja Naukowa pt. „Cyfrowy bliźniak". Organizatorzy: UODO oraz Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.	Wrocław
3.	24.01.2020	Konferencja Naukowa pt. „Wyzwania ochrony danych" zorganizowana w ramach obchodów XIV Europejskiego Dnia Ochrony Danych Osobowych. Organizatorzy: Centrum Badań nad Cyberprzestępczością, WPiA Uniwersytetu Mikołaja Kopernika w Toruniu oraz Towarzystwo Naukowe Organizacji i Kierownictwa w Toruniu.	Toruń
4.	28.01.2020	XIV Dzień Ochrony Danych Osobowych. Dzień Otwarty Urzędu Ochrony Danych Osobowych. Organizator: UODO.	Warszawa
5.	28.01.2020	Konferencja pt. „More Than Just a Game". Organizator: Koło Naukowe Własności Intelektualnej WPiA, Uniwersytet Warszawski.	Warszawa
6.	30.01.2020	Konferencja „Praktyka wykonywania funkcji Inspektora Ochrony Danych Osobowych" zorganizowana w ramach II Dnia IOD oraz XIV Dnia Ochrony Danych Osobowych. Organizatorzy: SABI – Stowarzyszenie Inspektorów Ochrony Danych, Wydział Zarządzania Politechniki Warszawskiej.	Warszawa
7.	7.02.2020	VI Dzień Otwarty UODO w Akademii Wyższej Szkoły Biznesu w Dąbrowie Górniczej, z okazji XIV Dnia Ochrony Danych Osobowych 2020. Organizator: Akademia WSB w Dąbrowie Górniczej.	Dąbrowa Górnicza
8.	28.02.2020	#RODO w edukacji – lubelskie spotkanie z ochroną danych osobowych w szkole. Organizator: UODO.	Zamość
9.	28.02.2020	Konferencja pt. „More Than Just a Game". Organizatorzy: Queen Mary University of London oraz Linklaters Warsaw, S.k.	Warszawa
10.	3.03.2020	Konferencja Naukowa pt. „Ochrona danych osobowych w zbiorowym prawie pracy". Organizator: Zakład Prawa Pracy Kolegium Prawa Akademii Leona Koźmińskiego.	Warszawa
11.	11.03.2020	Ogólnopolska Konferencja Naukowa pt. „Karne i dyscyplinarne aspekty ochrony danych osobowych". Organizatorzy: Wydział Prawa Kanonicznego Uniwersytetu Papieskiego JPII oraz Kościelny Inspektor Ochrony Danych.	Kraków
12.	16.03.2020	Kongres Konsumentów 2020. Organizator: Federacja Konsumentów.	Warszawa
13.	3.06.2020	Uroczystość wręczenia nagród laureatom konkursu na najlepsze inicjatywy edukacyjne z zakresu ochrony danych osobowych.	Puszcza Mariańska
14.	4.06.2020	Uroczystość wręczenia I nagrody laureatce konkursu na najlepsze inicjatywy edukacyjne z zakresu ochrony danych osobowych.	Piotrków Trybunalski

15.	5.06.2020	VI Kongres Zarządzania Administracją Samorządową. Organizatorzy: Redakcja pisma samorządu terytorialnego „Wspólnota” oraz Municipium.	Wrocław
16.	8.07.2020	Ogólnopolska Konferencja Naukowa pt. „Drony a prywatność”. Organizator: Urząd Ochrony Danych Osobowych.	online
17.	20.07.2020	Spotkanie w UODO z przedstawicielem MEN w ramach X. ed. Programu TDTS.	online
18.	23.07.2020	Spotkanie z przedstawicielami MEN dot. platformy współpracy oraz 2. ed. podręcznika dla szkół.	online
19.	1.09.2020	Konferencja „Follow the Sun: A Digital Launch of the Data Protection Handbook (2nd ed.)”, inaugurująca II wyd. Podręcznika o ochronie danych w działaniach humanitarnych. Organizator: Międzynarodowy Komitet Czerwonego Krzyża (ICRC).	online
20.	15.09.2020	EIT Health Think Tank Roundtable. Organizator: Europejski Instytut Innowacji i Technologii - EIT Health.	online
21.	29.09.2020	Spotkanie z przedstawicielami IAB Polska w sprawie dodatkowych środków uzupełniających.	online
22.	30.09.2020	Szkolenie dla inspektorów ochrony danych sektora oświaty. Organizator: UODO we współpracy z MEN.	
23.	7-8.10.2020	I Kongres Inspektorów Ochrony Danych Osobowych online, organizowany w ramach XVIII Samorządowego Forum Kapitału i Finansów. Organizatorzy: Pismo Samorządu Terytorialnego „Wspólnota” oraz Municipium S.A.	online
24.	15.10.2020	Posiedzenie Komisji Sprawiedliwości i Praw Człowieka, Senat RP.	online
25.	15-16.10.2020	Inauguracja XI edycji Programu „Twoje dane – Twoja sprawa”. Organizator: UODO.	online
26.	23.10.2020	Uroczystości obchodów 75-Lecia Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.	online
27.	24.10.2020	Inauguracja zajęć XX edycji Podyplomowego Studium Ochrony Danych Osobowych w Akademii Leona Koźmińskiego w Warszawie.	online
28.	5.11.2020	Ogólnopolska Konferencja Naukowa pt. „Status administratora w sektorze publicznym”. Organizator: Centrum Ochrony Danych Osobowych i Zarządzania Informacją, działające na WPiA Uniwersytetu Łódzkiego.	online
29.	12.11.2020	I Spotkanie sieci współpracy placówek doskonalenia nauczycieli w ramach Programu „Twoje dane – Twoja sprawa”.	online
30.	16.11.2020	Spotkanie z przedstawicielami Biura Rzecznika Praw Pacjenta w sprawie „Wytycznych dot. realizacji przez osoby uprawnione informacji o stanie zdrowia pacjenta na odległość”.	online
31.	23.11.2020	VI Doroczna Konferencja Wydawnictwa C.H.Beck „Ocena i rewizja RODO po dwóch latach obowiązywania”.	online
32.	8.12.2020	Konferencja pt. „Współczesny wymiar bezpieczeństwa w szkołach i placówkach oświatowych w okresie pandemii”. Organizatorzy: Kuratorium Oświaty w Warszawie, Mazowieckie Samorządowe Centrum Doskonalenia Nauczycieli oraz Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.	online
33.	17.12.2020	Wykład dla studentów Wydziału Farmaceutycznego WUM z zakresu bezpieczeństwa danych osobowych w praktyce aptecznej.	online

Załącznik nr 4

Wykaz wydarzeń międzynarodowych i europejskich, w tym posiedzeń plenarnych EROD i podgrup, z udziałem Prezesa UODO lub jego przedstawicieli, które odbyły się w 2020 r.

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	8.01.2020	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory – SAESG) Europejskiej Rady Ochrony Danych	Bruksela
2.	13.01.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	Bruksela
3.	14-15.01.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
4.	15-16.01.2020	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	Bruksela
5.	28-29.01.2020	17. Posiedzenie plenarne EROD + Dzień ochrony danych osobowych	Bruksela
6.	4.02.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	Bruksela
7.	5.02.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	Bruksela
8.	5.02.2020	Spotkanie Podgrupy Użytkowników IT (IT USERS) Europejskiej Rady Ochrony Danych.	online
9.	6.02.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
10.	6.02.2020	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	Bruksela
11.	7.02.2020	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup – SOCM) Europejskiej Rady Ochrony Danych.	Bruksela
12.	18-19.02.2020	18. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	Bruksela
13.	27-28.02.2020	Workshop on best practices for the protection of personal data in Europe, the introduction of the Regulation (EU) 2016/679.	Ukraina
14.	3-4.03.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
15.	4-5.03.2020	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
16.	24-25.03.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	Bruksela
17.	14.04.2020	21. Posiedzenie plenarne EROD.	online
18.	16.04.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
19.	16.04.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
20.	17.04.2020	22. Posiedzenie plenarne EROD.	online
21.	20.04.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
22.	21.04.2020	23. Posiedzenie plenarne EROD.	online
23.	24.04.2020	24. Posiedzenie plenarne EROD.	online
24.	29.04.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online

25.	5.05.2020	25. Posiedzenie plenarne EROD.	
26.	5-6.05.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
27.	7.05.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
28.	7.05.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
29.	8.05.2020	26. Posiedzenie plenarne EROD.	online
30.	11-13.05.2020	Spotkanie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
31.	12.05.2020	27. Posiedzenie plenarne EROD.	online
32.	13.05.2020	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	
33.	15.05.2020	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup – SOCM) Europejskiej Rady Ochrony Danych.	online
34.	19.05.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
35.	19.05.2020	Warsztaty eksperckie dot. ochrony danych medycznych. Organizator: Konsorcjum EUHealthSupport.	
36.	20.05.2020	28. Posiedzenie plenarne EROD.	online
37.	26.05.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
38.	27.05.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
39.	28.05.2020	29. Posiedzenie plenarne EROD.	online
40.	2.06.2020	30. Posiedzenie plenarne EROD.	online
41.	4.06.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
42.	5.06.2020	Podgrupa ds. Finansowych (Financial Matters Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
43.	8.06.2020	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup – SOCM) Europejskiej Rady Ochrony Danych.	online
44.	8.06.2020	Workshop on Certification Criteria w ramach Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
45.	9.06.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
46.	9.06.2020	31. Posiedzenie plenarne EROD.	online
47.	10.06.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
48.	10.06.2020	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
49.	11.06.2020	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
50.	15.06.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
51.	15.06.2020	Posiedzenie Grupy Koordynującej Nadzór nad Systemem Informacji Celnej (CIS SCG).	online
52.	16.06.2020	Spotkanie Europol Cooperation Board.	online

53.	16.06.2020	32. Posiedzenie plenarne EROD.	
54.	16-17.06.2020	Spotkanie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
55.	17.06.2020	Spotkanie Grupy ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen – SIS II.	online
56.	18.06.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
57.	18.06.2020	Posiedzenie Eurodac SCG.	online
58.	18.06.2020	Communications network – Conference call.	online
59.	18.06.2020	Posiedzenie Podgrupy Użytkowników IT (IT USERS) Europejskiej Rady Ochrony Danych.	online
60.	18.06.2020	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym –VIS SCG.	online
61.	22.06.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
62.	23.06.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
63.	24.06.2020	Annual Conference on European Data Protection Law 2020.	online
64.	24.06.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
65.	24-26.06.2020	Spotkanie wirtualne poświęcone pracy zdalnej pt. „Nowe modele pracy, nowe zarządzanie". Organizator: Hiszpańska Agencja Ochrony Danych.	online
66.	25.06.2020	Posiedzenie Podgrupy ds. Finansowych (Financial Matters Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
67.	29-30.06.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
68.	30.06.2020	EDPS Strategy Launch.	online
69.	30.06.2020	33. Posiedzenie plenarne EROD.	online
70.	1.07.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	
71.	1.07.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
72.	1-3.07.2020	Webinarium dot. przedstawienia pracy Komitetu T-PD „Data Protection Views from Strasbourg in Visio". Organizatorzy: Biuro Komitetu Konwencji 108 i Jednostka Ochrony Danych w Radzie Europy.	online
73.	2-3.07.2020	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
74.	6.07.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
75.	6.07.2020	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
76.	7.07.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
77.	8.07.2020	Spotkanie Komitetu CSC – Coordinated Supervision Committee.	online
78.	8.07.2020	Spotkanie sieci rzeczników prasowych EROD.	online
79.	9.07.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online

80.	9.07.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
81.	13.07.2020	CEH Codes Discussion.	online
82.	13.07.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
83.	14.07.2020	Posiedzenie Enforcement ESG.	online
84.	15.07.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
85.	16.07.2020	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network).	online
86.	17.07.2020	Połączone posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) oraz Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) w sprawie Schrems II.	online
87.	17.07.2020	34. Posiedzenie plenarne EROD.	online
88.	22.07.2020	Spotkanie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych w sprawie kodeksów.	online
89.	22.07.2020	35. Posiedzenie plenarne EROD.	online
90.	23.07.2020	Webinar „Enables and Protectors: the Role of DPAs confronting COVID-19 – contact tracing and the recovery response". Organizator: GPA.	online
91.	23.07.2020	36. Posiedzenie plenarne EROD.	online
92.	26.08.2020	Spotkanie sieci rzeczników prasowych EROD.	online
93.	1.09.2020	Konferencja pt. „Follow the Sun: A Digital Launch of the Data Protection Handbook (2nd ed.). Organizatorzy: Global Privacy Assembly i Międzynarodowy Komitet Czerwonego Krzyża.	online
94.	2.09.2020	37. Posiedzenie plenarne EROD.	online
95.	3.09.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
96.	8-10.09.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
97.	9.09.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
98.	10-11.09.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
99.	14.09.2020	Warsztat Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych w sprawie wymogów certyfikacji.	online
100.	14.09.2020	38. Posiedzenie plenarne EROD.	online
101.	15.09.2020	Spotkanie EIT Health Think Tank Roundtable.	Warszawa
102.	15.09.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
103.	15.09.2020	Posiedzenie podgrupy ds. Finansowych (Financial Matters Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
104.	16.09.2020	Wirtualne warsztaty GPA-OECD COVID-19. Workshop the Road to Recovery.	online
105.	17.09.2020	Spotkanie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych w sprawie kodeksów.	online
106.	17-18.09.2020	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
107.	18.09.2020	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online

108.	22.09.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
109.	25.09.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
110.	28.09.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
111.	28-30.09.2020	50. Posiedzenie Biura Komitetu Konwencji nr 108 Rady Europy.	online
112.	29.09.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
113.	29.09.2020	Coaching Event on EDPB Strategy 2021/2023.	online
114.	30.09.2020	Spotkanie sieci rzeczników prasowych EROD.	online
115.	30.09.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement) Europejskiej Rady Ochrony Danych.	online
116.	5.10.2020	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
117.	6.10.2020	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup – SOCM) Europejskiej Rady Ochrony Danych.	online
118.	7.10.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
119.	7.10.2020	Mini-posiedzenie plenarne EROD dot. przyjęcia opinii w sprawie art. 64.	online
120.	8.10.2020	39. Posiedzenie plenarne EROD.	online
121.	8-9.10.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
122.	13-14.10.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	
123.	13-15.10.2020	Międzynarodowa Konferencja Global Privacy Assembly 2020 Closed Session – At Your Desk.	online
124.	14.10.2020	Posiedzenie Podgrupy Użytkowników IT (IT USERS) Europejskiej Rady Ochrony Danych.	online
125.	14.10.2020	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
126.	15.10.2020	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
127.	20.10.2020	40. Posiedzenie plenarne EROD.	online
128.	21.10.2020	Warsztaty dotyczące zależności pomiędzy Art. 3 a Rozdziałem V RODO.	online
129.	21.10.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
130.	22.10.2020	CIPL's online roundtable on Schrems 2 „The Schrems II Mandate: Do what you can't?".	online
131.	22.10.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
132.	28.10.2020	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
133.	28.10.2020	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
134.	29.10.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
135.	29.10.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online

136.	30.10.2020	Spotkanie Sieci Inspektorów Ochrony Danych EROD (DPO Network).	online
137.	3.11.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
138.	3-4.11.2020	Wideokonferencja „Digital Citizenship Education Days". Organizator: Rada Europy.	online
139.	3-4.11.2020	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
140.	4.11.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
141.	4.11.2020	Spotkanie sieci rzeczników prasowych EROD.	online
142.	5.11.2020	Podgrupa ds. Sektora Finansowego (Financial Matters Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
143.	5.11.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
144.	5.11.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
145.	5-6.11.2020	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
146.	6.11.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
147.	9-10.11.2020	41. Posiedzenie plenarne EROD.	online
148.	10.11.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
149.	10.11.2021	Webinarium „Different models to facilitate the cross-border exchange of personal data". Organizator: Światowa Organizacja Handlu (WTO).	online
150.	17.11.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
151.	18.11.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
152.	18-19.11.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
153.	18-20.11.2020	40. Posiedzenie plenarne Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD).	online
154.	20.11.2020	42. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
155.	23.11.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
156.	24.11.2020	Spotkanie Rady Współpracy Europolu (ECB).	online
157.	24-25.11.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
158.	25.11.2020	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen – SIS II.	online
159.	26.11.2020	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac.	online
160.	26.11.2020	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym – VIS.	online
161.	26.11.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
162.	27.11.2020	Spotkanie interesariuszy dot. uzasadnionego interesu administratora.	online

163.	1.12.2020	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG).	online
164.	2.12.2020	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup – SOCM) Europejskiej Rady Ochrony Danych.	online
165.	2.12.2020	Spotkanie dot. doświadczeń w zakresie szkoleń i potrzeb szkoleniowych Urzędu Rzecznika Informacji Ukrainy, na zlecenie Rady Europy. Organizator: Massey-Consulting.	online
166.	3.12.2020	Posiedzenie Podgrupy Użytkowników IT (IT USERS) Europejskiej Rady Ochrony Danych.	online
167.	3.12.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych – spotkanie z Komisją w sprawie standardowych klauzul umownych.	online
168.	7.12.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
169.	7.12.2020	Spotkanie Grupy zadaniowej ds.101 skarg Noyb (Taskforce 101 Noyb).	online
170.	7-8.12.2020	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
171.	8.12.2020	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
172.	8.12.2020	Posiedzenie Podgrupy International Transfers Subgroup – ITS, Europejskiej Rady Ochrony Danych.	online
173.	9.12.2020	Spotkanie Komitetu Skoordynowanego Nadzoru (Coordinated Superision Committee – CSC).	online
174.	9.12.2020	Posiedzenie Podgrupy ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
175.	10.12.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Europejskiej Rady Ochrony Danych.	online
176.	10.12.2020	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
177.	11.12.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych w sprawie korporacyjnych reguł korporacyjnych.	online
178.	12.12.2020	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network).	online
179.	14.12.2020	Posiedzenie Podgrupy ds. Transferów Danych (International Transfers Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
180.	15.12.2020	43. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
181.	16.12.2020	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
182.	16-18.12.2020	51. Posiedzenie Biura Komitetu Konwencji nr 108 Rady Europy.	online
183.	17.12.2020	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (BTLE) Europejskiej Rady Ochrony Danych.	online
184.	18.12.2020	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG).	online

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
www.uodo.gov.pl