SPRAWOZDANIE Z DZIAŁALNOŚCI PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH W ROKU 2021

SPRAWOZDANIE Z DZIAŁALNOŚCI PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH w ROKU 2021

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 2021 r. do 31 grudnia 2021 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 2021. 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 dotyczące zrealizowanych 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 2021 r. minął trzeci pełny rok kalendarzowy bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych w polskim porządku prawnym. To 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 2021, 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 roku 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 miały ją wdrożyć do 6 maja 2018 r. W polskim systemie prawnym ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości została uchwalona 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].

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

[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.

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. 57 RODO Prezes Urzędu Ochrony Danych Osobowych:

1. monitoruje i egzekwuje stosowanie ogólnego rozporządzenia o ochronie danych;
2. upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienia tych zjawisk (szczególną uwagę poświęcając działaniom skierowanym do dzieci);
3. 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 danych;
4. upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy RODO;
5. udziela osobom, których dane dotyczą, na ich żądanie, informacji o wykonywaniu praw przysługujących im na mocy RODO, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich UE;
6. rozpatruje skargi wniesione przez osoby, których dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80 RODO, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje Skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym;
7. współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami oraz świadczy wzajemną pomoc, w celu zapewnienia spójnego stosowania i egzekwowania RODO;

[11] tj. Dz. U. z 2016 r. poz. 922 z późn. zm.
[12] Wskazane przepisy obowiązywały do 5 lutego 2019 r.

8. prowadzi postępowania w sprawie stosowania RODO, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
9. monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;
10. przyjmuje standardowe klauzule umowne, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d) RODO;
11. ustanawia i prowadzi wykaz operacji podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4 RODO;
12. udziela zaleceń, o których mowa w art. 36 ust. 2 RODO, dotyczących operacji przetwarzania danych;
13. zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1 RODO, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5 RODO;
14. zachęca 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 zatwierdza kryteria certyfikacji zgodnie z art. 42 ust. 5;
15. gdy ma to zastosowanie – zgodnie z art. 42 ust. 7 RODO – dokonuje okresowego przeglądu udzielonych certyfikacji;
16. opracowuje i publikuje wymogi akredytacji podmiotów monitorujących kodeksy postępowania na mocy art. 41 oraz podmiotów certyfikujących na mocy art. 43;
17. akredytuje podmiot monitorujący kodeksy postępowania zgodnie z art. 41 oraz podmiot certyfikujących na mocy art. 43;
18. wydaje zezwolenia na klauzule umowne i przepisy, o których mowa w art. 46 ust. 3 RODO;
19. zatwierdza wiążące reguły korporacyjne na mocy art. 47 RODO;
20. bierze udział w pracach Europejskiej Rady Ochrony Danych;
21. prowadzi wewnętrzny rejestr naruszeń ogólnego rozporządzenia o ochronie danych i działań podjętych zgodnie z art. 58 ust. 2 RODO;
22. wypełnia inne zadania związane z ochroną danych osobowych.

Wraz z powyższymi zadaniami Prezesowi UODO przysługuje wiele **uprawnień**. Na mocy art. 58 ogólnego rozporządzenia o ochronie danych należą do nich: uprawnienia w zakresie

prowadzonych postępowań, uprawnienia naprawcze, uprawnienia w zakresie wydawania zezwoleń oraz uprawnienia doradcze.

Uprawnienia w zakresie prowadzonych postępowań obejmują (art. 58 ust.1):

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 przyznanych na mocy art. 58 ust. 2 RODO 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 niniejszym ustępie, 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 w zakresie wydawania zezwoleń i uprawnienia doradcze (art. 58 ust. 3):

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.

Z chwilą rozpoczęcia obowiązywania od 25 maja 2018 r. ogólnego rozporządzenia o ochronie danych oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych[13], 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 2021, w tym w szczególności zgłaszanych skarg i pytań prawnych oraz naruszeń, które wpływały do organu w wyniku zgłoszeń dokonywanych przez administratorów, pozwoliła na zidentyfikowanie problemów związanych z ochroną danych osobowych w związku ze stosowaniem RODO – problemów, które pojawiały się zarówno po stronie podmiotów danych, jak i administratorów.

2. Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych, zwany dalej „Urzędem", zapewnia wykonanie zadań wynikających z kompetencji Prezesa Urzędu Ochrony Danych Osobowych, określonych 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 uchylenia dyrektywy 95/46/WE[14], ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych[15], a także w innych przepisach powszechnie obowiązującego prawa.

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:

- ww. rozporządzenia 2016/679;
- dyrektywy 2016/680[16];

[13] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2019 r. poz. 1781).
[14] Dz. U. UE. L. z 2016 r. Nr 119 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2.
[15] Dz. U. z 2018 r. poz. 1000.
[16] 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

- rozporządzenia 2016/794[17].

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 Nowych Technologii (DNT), 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 czterech 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: Wydział Kontroli i Wydział Naruszeń, 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, natomiast w Departamencie Współpracy Międzynarodowej i Edukacji: Wydział Współpracy Międzynarodowej i Wydział Edukacji.

Wdrożone zmiany pozwoliły skutecznie i szybko 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

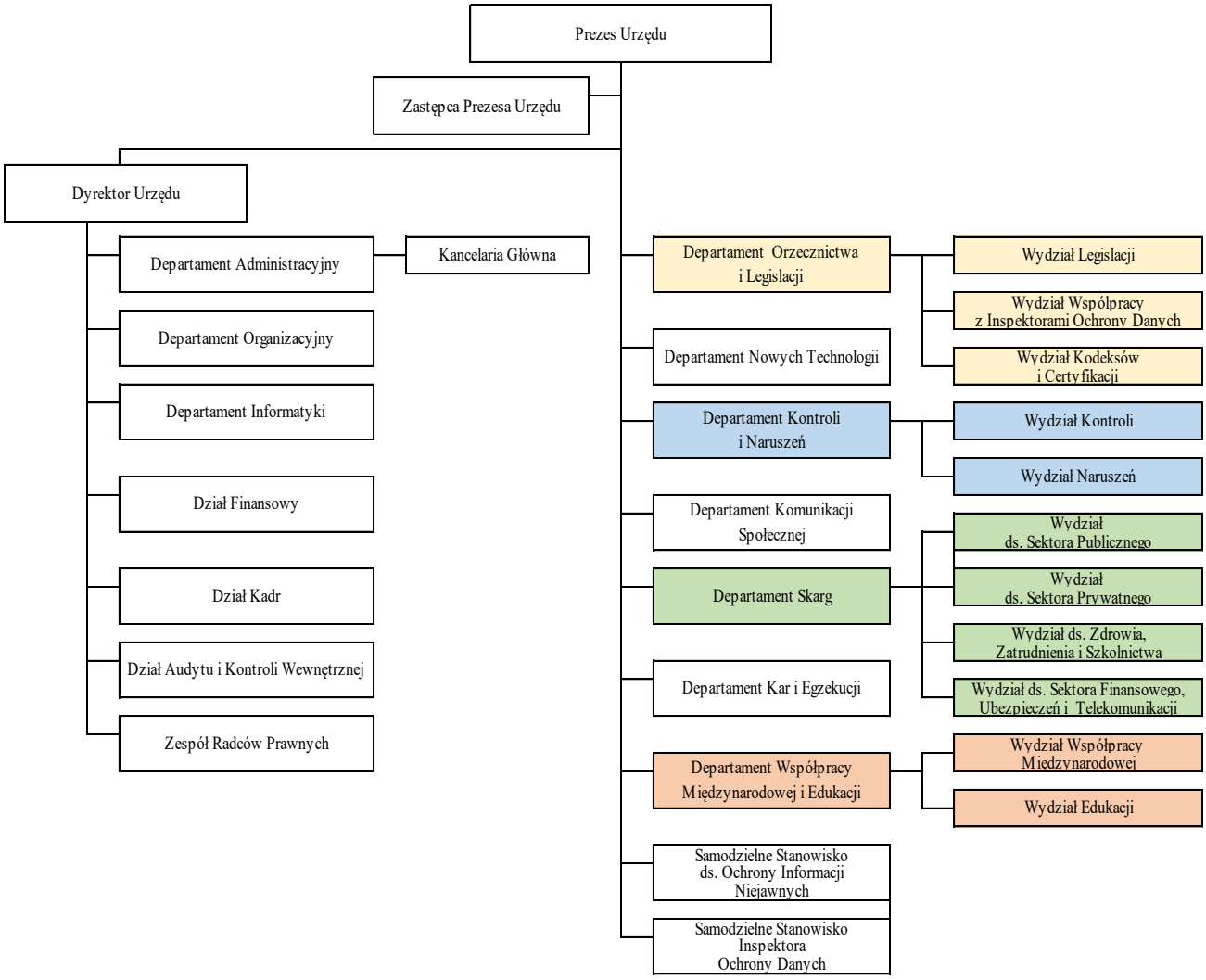
Organizację i zasady działania UODO określa statut stanowiący załącznik do zarządzenia nr 19/2019 Prezesa Urzędu Ochrony Danych Osobowych z 6 listopada 2019 r. w sprawie nadania statutu Urzędowi Ochrony Danych Osobowych[18].

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. Urz. UE L 119, z 4.5.2016, s. 89–131), zwana dalej dyrektywą 2016/680 lub dyrektywą policyjną.

[17] 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.

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

Strukturę organizacyjną Urzędu Ochrony Danych Osobowych przedstawia poniższa ilustracja:



Na mocy Zarządzenia nr 4/2021 Prezesa Urzędu Ochrony Danych Osobowych z dnia 24 lutego 2021 r. w statucie Urzędu, stanowiącym załącznik do Zarządzenia nr 19/2019 Prezesa UODO z dnia 6 listopada 2019 r., wprowadzone zostały zmiany, w oparciu o które w 2021 roku w Urzędzie Ochrony Danych Osobowych powstał Departament Nowych Technologii (DNT).

2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2021 r. w przeliczeniu na pełne etaty wynosił 270 etatów (tj. 274 osoby). Natomiast zatrudnienie w UODO na dzień 31 grudnia 2021 r. wynosiło 262 etaty (tj. 267 osób). Na koniec 2021 r. na stanowiskach

merytorycznych zatrudnionych było 236 osób, a na stanowiskach pomocniczych 31 osób. Wyższe wykształcenie posiadało 240 pracowników, w tym 154 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2021 r. przedstawiała się następująco:

1) Dyrektor Urzędu – 1 osoba,
2) 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),
3) Departament Współpracy Międzynarodowej i Edukacji – 14 osób (13,5 etatu), w tym:
   - Wydział Edukacji – 6 osób (6 etatów)
   - Wydział Współpracy Międzynarodowej – 6 osób (5,5 etatu)
4) Departament Kontroli i Naruszeń – 49 osób (49 etatów) w tym:
   - Wydział Kontroli – 18 osób (18 etatów),
   - Wydział Naruszeń – 24 osoby (24 etaty),
5) Departament Komunikacji Społecznej – 16 osób (15,3 etatu),
6) Departament Skarg – 87 osób (86,5 etatu), w tym:
   - Wydział ds. Sektora Publicznego – 17 osób (17 etatów),
   - Wydział ds. Sektora Prywatnego – 26 osób (26 etatów),
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 19 osób (19 etatów),
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 18 osób (18 etatów),
7) Departament Kar i Egzekucji – 9 osób (9 etatów),
8) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,33 etatu),
9) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba (1 etat),
10) Departament Administracyjny – 25 osób (24 etaty),
11) Departament Organizacyjny – 7 osób (7 etatów),
12) Departament Informatyki – 8 osób (7,42 etatu),
13) Dział Finansowy – 5 osób (5 etatów),
14) Dział Kadr – 4 osoby (4 etaty),

15) Dział Audytu i Kontroli Wewnętrznej – 1 osoba (0,5 etatu),
16) Zespół Radców Prawnych – 3 osoby (3 etaty),
17) Radca – 1 osoba (0,8 etatu).

2.3. Budżet Urzędu Ochrony Danych Osobowych za 2021 r.

Budżet UODO ustalony w ustawie budżetowej na 2021 r. wynosił: 39 246 tys. zł, w tym:

- wynagrodzenia 25 340 tys. zł
- pochodne od wynagrodzeń 4 954 tys. zł
- wydatki majątkowe 1 607 tys. zł
- pozostałe wydatki 7 345 tys. zł

Wydatki zrealizowane przez UODO w 2021 r. w kwocie 38 531 tys. zł, w tym:

- wynagrodzenia 25 248 tys. zł
- pochodne od wynagrodzeń 4 625 tys. zł
- wydatki majątkowe 1 554 tys. zł
- pozostałe wydatki 7 104 tys. zł

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI

1. Wprowadzenie

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

Za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest taka, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden

bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

RODO stosuje się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz w przypadku przetwarzania w sposób inny niż zautomatyzowany, np. w formie tradycyjnej – papierowej, jeżeli dane stanowią lub mogą stanowić część zbioru[19].

Dane osobowe dzielą się na trzy kategorie:

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

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

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (**zgodność z prawem, rzetelność i przejrzystość**);
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz 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**);

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

- prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (**prawidłowość**);
- przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane (**ograniczenie przechowywania**);
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (**integralność i poufność**).

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

Należy podkreślić, że RODO nie powstało w próżni normatywnej. Ponad 20 lat doświadczeń w stosowaniu dyrektywy 95/46/WE – zarówno przez administratorów danych, jak i podmioty danych, ale także niezależne organy nadzorcze – stało się podwaliną nowego prawa ochrony danych w UE. Rozporządzenie 2016/679 opiera się na podstawowych wartościach tego istniejącego już systemu, utrzymując zasady ochrony danych oraz podstawy prawne przetwarzania danych, poddając je jedynie niezbędnym modyfikacjom.

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

Istotnym uprawnieniem osoby, której dane dotyczą, jest wynikające z art. 15 RODO prawo dostępu do tych danych. Zgodnie ze wskazanym przepisem osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz do następujących informacji:

- cele przetwarzania;

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

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

2. Zadania jednostek organizacyjnych UODO

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

aktów prawnych w zakresie ochrony danych osobowych danego sektora (np. prywatnego, publicznego, zdrowia, zatrudnienia i szkolnictwa, 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.

Jak już wcześniej wspomniano, na mocy Zarządzenia nr 4 Prezesa Urzędu Ochrony Danych Osobowych z dnia 24 lutego 2021 r. w sprawie zmiany statutu Urzędu Ochrony Danych Osobowych,

stanowiącego załącznik do Zarządzenia nr 19/2019 Prezesa UODO z dnia 6 listopada 2019 r., w Urzędzie powstał Departament Nowych Technologii.

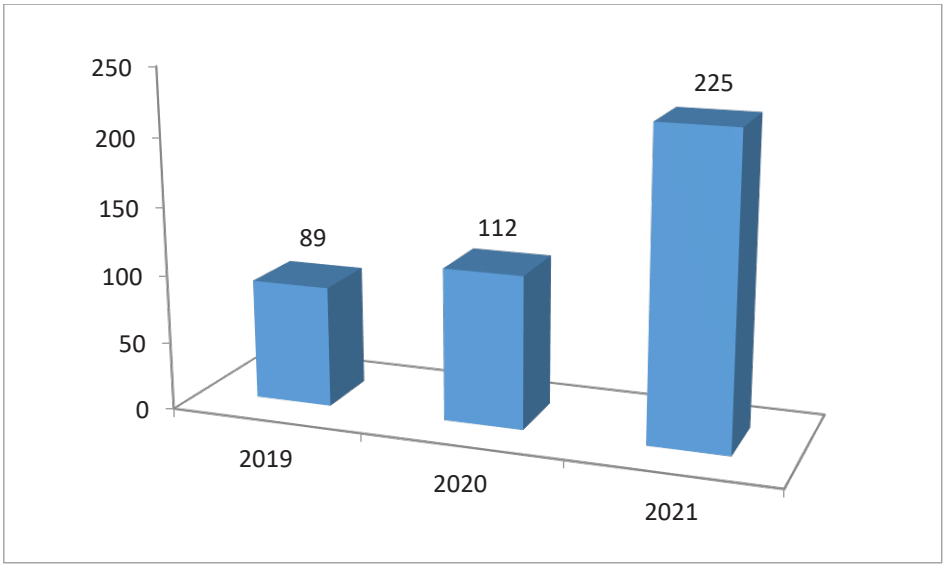
Do zadań nowo powstałego Departamentu należy w szczególności:

1) przygotowywanie opinii dotyczących nowych rozwiązań technologicznych w zakresie ich wpływu na bezpieczeństwo przetwarzania danych osobowych;
2) analiza i współudział w opracowywanych w ramach zespołów międzynarodowych opinii i dokumentów w zakresie rozwiązań technologicznych oraz ich wpływu na ochronę danych osobowych;
3) sporządzanie opinii i udzielanie bieżących konsultacji komórkom organizacyjnym UODO w ramach prowadzonych przez nie spraw, dotyczących przetwarzania danych osobowych w systemach informatycznych;
4) przygotowywanie opinii w zakresie zagadnień odnoszących się do przetwarzania danych osobowych w systemach informatycznych;
5) bieżące monitorowanie nowych rozwiązań technologicznych w zakresie przetwarzania danych i informowanie o nich komórek organizacyjnych UODO[20].

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

W 2021 roku wniesiono do Wojewódzkiego Sądu Administracyjnego w Warszawie **225 skarg** na decyzje lub postanowienia Prezesa UODO. Dla porównania – w 2020 roku skarg tych było 112.

[20] § 36 Regulaminu Organizacyjnego Urzędu Ochrony Danych Osobowych, stanowiącego załącznik do statutu Urzędu Ochrony Danych Osobowych.



Wykres 1: **Zestawienie liczby decyzji Prezesa UODO zaskarżonych do WSA w Warszawie w latach 2019–2021.**

Z ogólnej liczby 225 decyzji organu nadzorczego zaskarżonych do WSA w Warszawie, 49 decyzji zaskarżono do Naczelnego Sądu Administracyjnego. W sumie, w 2021 roku przed sądami administracyjnymi toczyły się **274 sprawy.** Poniżej przytoczono przykłady kilku wybranych skarg.

W jednej ze spraw Wojewódzki Sąd Administracyjny w Warszawie, wyrokiem z 12 lipca 2021 roku[21], oddalił skargę na decyzję Prezesa UODO z 21 grudnia 2020 roku[22], dotyczącą udostępnienia przez Burmistrza podczas sesji rady miejskiej – w związku z podejmowaniem uchwały w sprawie wygaśnięcia mandatu Skarżącego (będącego radnym) – danych osobowych Skarżącego, zawartych w akcie notarialnym sprzedaży nieruchomości oraz w oświadczeniu Skarżącego zawierającym zgodę na wykonanie prac budowlanych na tej działce. W uzasadnieniu tego wyroku Sąd podzielił przedstawione przez Prezesa UODO w zaskarżonej decyzji stanowisko, że dokumenty przedstawione na sesji rady miejskiej w formie prezentacji w wersji zanonimizowanej (udostępniono tylko dane osobowe Skarżącego w zakresie imienia i nazwiska, adresu zamieszkania oraz numeru działki ewidencyjnej do niego należącej) stanowiły dowody potwierdzające okoliczności będące przesłanką wygaśnięcia mandatu Skarżącego, polegającą na naruszeniu przez niego zakazu prowadzenia działalności gospodarczej z wykorzystaniem mienia komunalnego gminy, w której radny uzyskał mandat, o której jest mowa w art. 24f ust. 1 ustawy o samorządzie gminnym[23] i art. 383 § 1 pkt 5

[21] Sygn. akt II SA/Wa 685/21.
[22] Sygn. akt DS.523.214.2020.
[23] Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz. U z 2022 r. poz. 559.

ustawy Kodeks wyborczy[24]. Sąd podzielił również zdanie Prezesa UODO, że przetwarzanie tych danych było niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych, a tym samym znajdowało oparcie w art. 6 ust. 1 lit. c RODO. Sąd wskazał, że według art. 24f ust. 1 ustawy o samorządzie gminnym, radni nie mogą m.in. prowadzić działalności gospodarczej z wykorzystaniem mienia komunalnego gminy, w której uzyskali mandat. W przypadku naruszenia tego zakazu rada, w drodze uchwały, stwierdza wygaśnięcie mandatu radnego (art. 383 § 1 pkt 5 i § 2 Kodeksu wyborczego). Ustalenie tych okoliczności, stanowiących podstawę uchwały rady o wygaśnięciu mandatu radnego, nie należy bezpośrednio do rady, lecz do organu wykonawczego gminy. Przepis art. 30 ust. 2 pkt 1 ustawy o samorządzie gminnym stanowi bowiem, że do zadań wójta należy przygotowywanie projektów uchwał rady gminy. Wójt posługuje się w tym zakresie aparatem administracyjnym, co wynika z regulaminu organizacyjnego urzędu gminy. Zdaniem Sądu Burmistrz miał prawo i obowiązek ustalić, a następnie przedstawić radzie miejskiej, wszystkie okoliczności istotne dla podjęcia uchwały o stwierdzeniu wygaśnięcia mandatu radnego po to, aby uchronić się od ewentualnego zarzutu błędnych ustaleń faktycznych.

Organ właściwy do spraw ochrony danych osobowych odnotował również skargi dotyczące przetwarzania danych osobowych przez komorników sądowych. Przedmiotem jednej z takich skarg było udostępnienie przez Komornika danych osobowych w postaci informacji o prowadzonym przeciwko Skarżącemu postępowaniu egzekucyjnym, poprzez umieszczenie na kopercie skrótów nazw pism zawartych w przesyłce skierowanej do tej osoby, za pośrednictwem publicznego operatora pocztowego.

Prezes UODO stwierdził, że umieszczone na kopercie imię, nazwisko i adres Skarżącego, sygnatura postępowania egzekucyjnego, nazwa organu prowadzącego oraz skróty nazw pism zawartych w przesyłce, czyli: *„opis czynności Wezwanie do złożenia wykazu majątku, zaw. o wszcz. + TW, Zajęcie US EPUPE, Zawiadomienie o zajęciu rachunku KM, Zawiadomienie o zajęciu rachunku KM, Zaw. o zajęciu rachunku – p.p.”,* są informacjami identyfikującymi Skarżącego i tym samym stanowią dane osobowe w rozumieniu art. 4 pkt 1 RODO.

Uznał też, że ujawnienie na kopercie skrótów pism kierowanych do Skarżącego nie było niezbędne do skutecznego doręczenia korespondencji, a zatem miało charakter nadmiarowy i nieadekwatny do celu przetwarzania danych osobowych i odbywało się z naruszeniem przepisów art. 6 ust. 1 RODO w zw. z § 17 ust. 3 rozporządzenia Ministra Sprawiedliwości. Prezes Urzędu

[24] Ustawa z dnia 5 stycznia 2011 r. Kodeks wyborczy, Dz. U. z 2020 r. poz. 1319 z późn. zm.

Ochrony Danych Osobowych udzielił Komornikowi upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych[25].

Komornik od ww. rozstrzygnięcia złożył skargę do Wojewódzkiego Sądu Administracyjnego[26]. Sąd Administracyjny w Warszawie wyrokiem z dnia 1 września 2021 r. oddalił skargę, w pełni podzielając stanowisko zawarte w uzasadnieniu zaskarżonej decyzji. Sąd ten stwierdził, że umieszczenie na kopercie skrótów nazw pism kierowanych do dłużnika nie było niezbędne do skutecznego doręczenia mu korespondencji, miało charakter nadmiarowy i nieadekwatny do celu przetwarzania jego danych osobowych oraz nie znajdowało oparcia w żadnym z przywołanych w skardze przez Komornika przepisów. Nie było również niezbędne do osiągnięcia celu przetwarzania, ani nie miało umocowania w żadnej z przesłanek z art. 6 ust. 1 RODO.

Do Urzędu Ochrony Danych Osobowych wpłynęła skarga, w której Skarżący podniósł między innymi, że Spółdzielnia Mieszkaniowa udostępniła na swojej stronie internetowej imię, nazwisko, adres oraz podpis Skarżącego, zawarte w jego korespondencji do Spółdzielni dotyczącej zmian w uchwałach Walnego Zgromadzenia Spółdzielni. Skarżący złożył do Spółdzielni wniosek o zmianę porządku obrad wraz z projektami dwóch uchwał oraz poprawki do projektów uchwał Walnego Zgromadzenia Spółdzielni. Projekty uchwał zostały udostępnione na stronie internetowej Spółdzielni, w części dostępnej wyłącznie dla członków Spółdzielni, oraz wyłożone w siedzibie Spółdzielni, również do wglądu wyłącznie dla członków Spółdzielni.

Spółdzielnia jest zobowiązana do udostępnienia – zgodnie z art. 18 ust. 2 pkt 2 Prawa spółdzielczego[27], art. 8^1 ust. 1 oraz 8^1 ust. 3 ustawy o spółdzielniach mieszkaniowych[28] – wskazanych w niniejszych przepisach dokumentów członkom Spółdzielni, a także posiada powinność udostępnienia części z nich na swojej stronie internetowej. Determinuje to przyjęcie przez nią określonych rozwiązań technicznych, które zapewnią dostęp do tych dokumentów w formie elektronicznej tylko osobom uprawnionym, tj. członkom Spółdzielni. Zgodnie z art. 8^3 ust. 10 ustawy o spółdzielniach mieszkaniowych, projekty uchwał i żądania zamieszczenia oznaczonych spraw w porządku obrad walnego zgromadzenia lub jego wszystkich części mają prawo zgłaszać: zarząd, rada nadzorcza i członkowie. Projekty uchwał, w tym uchwał przygotowanych w wyniku tych żądań, powinny być wykładane na co najmniej 14 dni przed terminem walnego zgromadzenia lub jego

[25] DS.523.1377.2020.
[26] Sygn. akt II SA/Wa 642/21.
[27] Ustawa z dnia 16 września 1982 r. Prawo spółdzielcze, Dz.U. z 2021 r. poz. 648.
[28] Ustawa z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych, Dz.U. z 2021 r. poz. 1208.

pierwszej części. W ust. 11 wskazano, że członkowie mają prawo zgłaszać projekty uchwał i żądania, o których mowa w ust. 10, w terminie do 15 dni przed dniem posiedzenia walnego zgromadzenia lub jego pierwszej części. Zgodnie z ust. 13, zarząd jest zobowiązany do przygotowania pod względem formalnym i przedłożenia pod głosowanie na walnym zgromadzeniu projektów uchwał i poprawek zgłoszonych przez członków spółdzielni.

Prezes UODO uznał, że udostępnienie przez Spółdzielnię Mieszkaniową danych osobowych Skarżącego w zakresie jego imienia, nazwiska, adresu oraz podpisu, zawartych w jego korespondencji dotyczącej zmian w uchwałach Walnego Zgromadzenia Spółdzielni, na stronie internetowej Spółdzielni (w części dostępnej po zalogowaniu tylko dla jej członków), znajdowało oparcie w art. 6 ust. 1 lit. c RODO w zw. z art. 8^3 ust. 10 ustawy o spółdzielniach mieszkaniowych. Spółdzielnia bowiem była zobowiązana do przedłożenia jej członkom projektów uchwał i żądań zamieszczenia oznaczonych spraw w porządku obrad walnego zgromadzenia lub jego wszystkich części. Prawo zapoznania się z ww. dokumentami przysługuje członkom spółdzielni, którzy zostali wpisani do rejestru członków prowadzonego przez zarząd spółdzielni (na podstawie art. 30 ww. ustawy), a Spółdzielnia umieściła ww. dokumenty w sekcji strony internetowej dostępnej wyłącznie dla członków Spółdzielni, po uprzednim zalogowaniu się indywidualnie określonym loginem i hasłem.

Niniejszą decyzję Skarżący zaskarżył do Wojewódzkiego Sądu Administracyjnego w Warszawie, który wyrokiem z dnia 22 września 2021 r. oddalił skargę[29]. Sąd podzielił stanowisko Prezesa UODO, iż udostępnienie przez spółdzielnię mieszkaniową danych osobowych Skarżącego w zakresie jego imienia, nazwiska, adresu oraz podpisu, zawartych w jego korespondencji dotyczącej zgłoszonych poprawek w uchwałach Walnego Zgromadzenia Spółdzielni, na stronie internetowej Spółdzielni (w części dostępnej po zalogowaniu tylko dla członków Spółdzielni), znajdowało oparcie w art. 6 ust. 1 lit. c RODO w zw. z art. 8^3 ust. 10 ustawy o spółdzielniach mieszkaniowych.

W kolejnej opisywanej sprawie, Wojewódzki Sąd Administracyjny w Warszawie poparł stanowisko Prezesa Urzędu Ochrony Danych Osobowych o niedopuszczalności przetwarzania przez administratora, będącego operatorem telekomunikacyjnym, danych osobowych zawartych w kopii dowodu osobistego w zakresie: obywatelstwa, nazwiska rodowego, imion rodziców, daty i miejsca urodzenia, płci, wzrostu w centymetrach, koloru oczu, nazwy organu wydającego dowód osobisty, daty wydania i terminu ważności, serii i numeru dowodu osobistego oraz wizerunku twarzy i wzoru

[29] Wyrok WSA w Warszawie z dnia 22 września 2021 r. II SA/WA 397/21.

podpisu. Przytaczając przepis art. 161 ust. 2 ustawy Prawo telekomunikacyjne[30] (w brzmieniu obowiązującym od dnia 4 maja 2019 r.), Wojewódzki Sąd Administracyjny w Warszawie uznał stanowisko organu, że cofnięcie przez osobę, której dane dotyczą, zgody na wykonanie kopii dowodu osobistego, wyrażonej w związku w zawarciem umów o świadczenie usług, a wcześniej na podstawie art. 161 ust. 2 ustawy Prawo telekomunikacyjne (w brzmieniu sprzed nowelizacji), oznacza, że przetwarzanie danych osobowych zawartych w wykonanej kopii dokumentu staje się niedopuszczalne. Sąd pokreślił, że proces przetwarzania danych osobowych musi być zgodny z zasadą minimalizacji danych, ustanowioną w art. 5 ust. 1 lit. c RODO, tj. dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Ograniczenie do danych niezbędnych oznacza takie ukształtowanie zakresu przetwarzania danych, aby przetwarzać tylko takie dane, bez których nie da się osiągnąć celu. Sąd uznał za uzasadnione stwierdzenie Prezesa Urzędu Ochrony Danych, że do realizacji umów o świadczenie usług telekomunikacyjnych zawartych z klientem (art. 6 ust. 1 lit. b rozporządzenia RODO) niezbędne jest wyłącznie imię, nazwisko, adres zameldowania oraz numer PESEL. Natomiast pozostałe dane zawarte w dowodzie osobistym (wizerunek i rysopis) nie służą w żaden sposób wykonaniu umowy o świadczenie usług telekomunikacyjnych (niezależnie od charakteru tej umowy) oraz że przetwarzanie tych spornych danych nie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO).

Zdaniem Sądu nieuprawnione było powoływanie się przez Operatora telekomunikacyjnego na wymóg zachowania szczególnej staranności przy weryfikacji tożsamości osoby zawierającej umowę o świadczenie usług telekomunikacyjnych, w związku z przypadkami nadużyć związanych z wykorzystywaniem danych osobowych osób trzecich do zaciągania zobowiązań w imieniu klientów oraz potrzebą kontroli nieuczciwych pracowników salonów firmowych Operatora. Nie istnieje bowiem prawnie uzasadniony interes administratora, przetwarzania danych osobowych strony umowy o świadczenie usług telekomunikacyjnych, takich jak: obywatelstwo, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, płeć, wzrost, koloru oczu, nazwa organu wydającego dowód osobisty, data wydania i termin ważności, seria i numer dowodu osobistego oraz wizerunek twarzy i wzór podpisu.

Wojewódzki Sąd Administracyjny w Warszawie wskazał również, że dyscyplinowanie własnych pracowników to kwestia wewnętrzna pracodawcy i nie ma żadnych podstaw, aby czynić to

[30] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. z 2021 r. poz. 576.

kosztem uprawnień klientów korzystających z usług administratora. Sąd wskazał, że weryfikacja tożsamości klienta możliwa jest poprzez okazanie przez klienta dokumentu ją potwierdzającego. Dla celów dowodowych i archiwizacyjnych związanych z potwierdzeniem faktu zawarcia umów oraz ustalenia, obrony i dochodzenia roszczeń (windykacji), wystarczające są imię, nazwisko, adres zameldowania oraz numer PESEL strony umowy. Wspomniane cele mogą być osiągnięte bez potrzeby przetwarzania innych danych zawartych w dowodzie osobistym. W ocenie Sądu nie zmienia powyższego również fakt, że od końca 2018 r. wykonując kserokopie dowodu osobistego, administrator używał tzw. nakładek anonimizacyjnych, a obraz dokumentu tożsamości nie był zapisywany w pamięci urządzenia, na którym była wykonywana kserokopia dokumentu.

Wojewódzki Sąd Administracyjny w Warszawie jednoznacznie wskazał też, że przepis art. 6 ust.1 lit. f RODO dotyczy sytuacji już istniejącej, w której celem wynikającym z prawnie uzasadnionych interesów administratora danych była konieczność udowodnienia potrzeby dochodzenia lub obrony przed roszczeniem już istniejącym, nie zaś sytuacji, gdy dane są przetwarzane w celu zabezpieczenia się przed ewentualnym przyszłym roszczeniem. Innymi słowy, przetwarzania danych osobowych nie uzasadnia jedynie potencjalność nieuczciwego zachowania się przez drugą stronę umowy w przyszłości. Administrator nie wykazał, że z chwilą wykonania kopii dowodu osobistego, zachowanie osoby, której dane dotyczą, rodzi obawę niewykonania przez nią zobowiązania wynikającego z podpisanej ze Spółką umowy oraz aby skierowała ona wobec administratora jakiekolwiek roszczenia[31]. Sąd potwierdził również prawidłowość zastosowania przez Prezesa Urzędu Ochrony Danych Osobowych środka naprawczego w postaci upomnienia w sprawie, w której ustały kwestionowane w skardze nieprawidłowości w procesie przetwarzania danych osobowych. Zdaniem Sądu w takiej sytuacji organ może skorzystać z przysługujących mu uprawnień naprawczych (w tym poprzez zastosowanie środka z art. 58 ust. 2 lit. b RODO). Nie jest wymagane, aby stan naruszenia był kontynuowany w dacie wydania rozstrzygnięcia, wystarczy bowiem samo ustalenie, że naruszenie takie zaistniało[32]. Ma to istotne znaczenie z perspektywy prowadzonych postępowań przez Prezesa UODO, ponieważ skarżone podmioty niejednokrotnie zarzucały, że zakończenie kwestionowanego procesu przetwarzania danych pozbawia organ nadzorczy możliwości zastosowania środków naprawczych przewidzianych w art. 58 ust. 2 RODO.

[31] Wyrok z dnia 5 maja 2021 r. Wojewódzkiego Sąd Administracyjnego w Warszawie, sygn. akt II SA/Wa 2014/20.
[32] Wyrok z dnia 24 marca 2021 r. Wojewódzkiego Sądu Administracyjnego w Warszawie, sygn. akt II SA/Wa 1336/20 (dot. ZSPR.440.394.2019).

W orzecznictwie warto również zauważyć ugruntowanie poglądu o braku kompetencji Prezesa UODO w rozstrzyganiu wniosków do organu o nakazanie udostępnienia danych osobowych na gruncie przepisów rozporządzenia 2016/679.

Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę w przedmiocie odmowy wszczęcia postępowania w sprawie skargi na odmowę udostępnienia danych osobowych osoby, która naruszyła dobra osobiste Skarżącej w wyniku publikacji reportażu. W treści wniosku do Prezesa UODO Skarżąca wskazała, że dane są jej niezbędne w celu wypełnienia formalnych wymogów pozwu. Spółka, jako pracodawca, odmówiła uwzględnienia żądania udostępnienia tych danych.

Sąd zauważył, że co do zasady uprawnienia proceduralne oraz materialne wynikające z przedmiotowego rozporządzenia przysługują wyłącznie osobom, których dane są objęte ochroną. Celem rozporządzenia 2016/679 jest zagwarantowanie osobie fizycznej odpowiedniej ochrony prawnej, a nie przyznawane uprawnień informacyjnych innym osobom. Co więcej, również Prezes UODO nie może żądać od administratora danych osobowych ujawnienia osobie trzeciej informacji na temat osoby, której dane dotyczą, nawet jeżeli są one potrzebne do wytoczenia powództwa. Tym samym ani art. 6 ust. 1 lit. f rozporządzenia 2016/679 nie stanowi podstawy prawnej do uzyskania takich danych, ani art. 58 tego rozporządzenia nie daje takiego uprawnienia organowi nadzorczemu.

Błędne domniemywanie takiego uprawnienia wynika z poprzedniego stanu prawnego. Na gruncie uchylonej już ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, w przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych, na podstawie art. 18 ust. 1 organ nakazywał przywrócenie stanu zgodnego z prawem, w tym w szczególności nakazywał uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych. Obecnie przepisy nie przewidują takich kompetencji[33].

Orzeczenie stanowi kontynuację linii orzeczniczej w tej materii.

Do Wojewódzkiego Sądu Administracyjnego w Warszawie zaskarżone zostały również decyzje Prezesa UODO nakładające administracyjną karę pieniężną.

Dla przykładu, kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych, dokonana w **ClickQuickNow Sp. z o.o. z siedzibą w Warszawie**[34] w 2019 r., zakończona wydaniem przez Prezesa UODO decyzji stwierdzającej naruszenie przepisów

[33] Wyrok z dnia 11 czerwca 2021 r. Wojewódzkiego Sądu Administracyjnego w Warszawie, sygn. akt II SA/Wa 456/21.
[34] Sygn. ZSPR.421.7.2019.

rozporządzenia 2016/679 i nakładającej administracyjną karę pieniężną w wysokości 201.559,50 zł, została zaskarżona do Wojewódzkiego Sądu Administracyjnego, który oddalił skargę[35].

W uzasadnieniu wyroku Sąd wskazał, że Prezes UODO zasadnie uznał, iż stosowany przez firmę sposób postępowania w procesie odwołania zgody na przetwarzanie uprzednio pozyskanych przez Spółkę danych osobowych, nie spełnia kryteriów prostego i szybkiego odwołania zgody i stanowi naruszenie art. 7 ust. 3, a także art. 12 ust. 2 oraz art. 17 ust. 1 lit. b RODO. Sąd podniósł m.in., że pozyskiwanie przez Spółkę informacji dotyczących przyczyny odwołania zgody było pozbawione podstaw prawnych – było to działanie umyślne, mające na celu utrudnienie, czy wręcz uniemożliwienie realizacji praw osób, których dane dotyczą. Takie działanie stanowiło jednocześnie naruszenie zasady zgodności z prawem, przejrzystości i rzetelności przetwarzania danych, o których mowa w art. 5 ust. 1 lit. a rozporządzenia 2016/679. Na powyższe orzeczenie ClickQuickNow Sp. z o.o. złożyła skargę kasacyjną.

Z kolei kontrola przeprowadzona w 2020 r. u **Głównego Geodety Kraju**[36], zakończona wydaniem przez Prezesa UODO decyzji stwierdzającej naruszenie przepisów rozporządzenia 2016/679153 i nakładającej na ww. podmiot administracyjną karę pieniężną w wysokości 100.000 zł, została również zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie, który oddalił skargę[37].

W uzasadnieniu wyroku Sąd podkreślił, że przenosząc definicję prawną „danych osobowych", o której mowa w art. 4 pkt 1 rozporządzenia 2016/679, na materię zawartości ksiąg wieczystych, podkreślenia wymaga, że podmiotami, których dotyczą poszczególne prawa i obowiązki ujawnione w księgach wieczystych są również osoby fizyczne. Zakres ujawnianych w księdze wieczystej danych osób fizycznych obejmuje m.in. imiona, nazwiska, imiona rodziców, numer PESEL i adres nieruchomości. Na tej podstawie Sąd stwierdził, że podane do publicznej wiadomości (na portalu GEOPORTAL2) numery ksiąg wieczystych pozwalają na identyfikację osób, których dane zawarte były w księdze wieczystej[38]. Posiadanie informacji o numerze księgi wieczystej umożliwia w sposób łatwy i prosty na dostęp do danych podmiotowych osób ujawnionych w księgach wieczystych. Sąd podzielił stanowisko Prezesa UODO, że udostępnienie przez Głównego Geodetę Kraju numerów ksiąg wieczystych na przedmiotowym portalu nastąpiło bez podstawy prawnej, która upoważniałaby

[35] Wyrok WSA w Warszawie z dnia 10 lutego 2021 r. sygn. akt IISA/Wa 2378/20.
[36] Sygn. DKN.5112.13.2020.
[37] Wyrok WSA w Warszawie z dnia 5 maja 2021 r. sygn. akt II SA/Wa2222/20.
[38] por. wyrok Naczelnego Sądu Administracyjnego, sygn. akt I OSK 11/17.

Głównego Geodetę Kraju do pozyskiwania informacji z ewidencji gruntów i budynków (w tym numerów ksiąg wieczystych) prowadzonych przez starostów celem ich publikacji na GEOPORTAL2 (geoportal.gov.pl). Ponadto Sąd zgodził się z Prezesem UODO, że Główny Geodeta Kraju decydując się na publikację na GEOPORTAL2 (geoportal.gov.pl) informacji o numerach ksiąg wieczystych posiadał wiedzę, że w ocenie organu nadzorczego, numer księgi wieczystej podlega przepisom o ochronie danych osobowych i w związku z tym ich przetwarzanie powinno być zgodne z tymi przepisami, co świadczy o umyślności działania ukaranego podmiotu. Na powyższe orzeczenie Główny Geodeta Kraju złożył skargę kasacyjną.

Kontrola przeprowadzona w 2019 r. w **Szkole Głównej Gospodarstwa Wiejskiego w Warszawie (SGGW)**[39], zakończona wydaniem przez Prezesa UODO decyzji stwierdzającej naruszenie przepisów RODO i nakładającej na uczelnię administracyjną karę pieniężną w wysokości 50.000 zł, została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie, który oddalił skargę uczelni[40]. W uzasadnieniu Sąd podzielił stanowisko Prezesa UODO i wskazał, że słusznie SGGW zostało uznane za administratora danych, gdyż uczelnia ta decydowała o celach i sposobach przetwarzania danych osobowych kandydatów na studia, zaś pracownik, któremu skradziono laptopa z danymi, nie był podmiotem, który samodzielnie decydował o celach i sposobach ich przetwarzania. Pracownik ten był osobą działającą w warunkach zależności (podporządkowania) pracodawcy (SGGW), wynikającej ze stosunku pracy łączącego go z uczelnią. Sąd podkreślił, że z istoty stosunku pracy wynika, iż w stosunkach zewnętrznych pracownik – co do zasady – nie występuje jako odrębny podmiot prawa, a jego działania są działaniami pracodawcy i pracodawca ponosi za nie odpowiedzialność, zachowując w stosunku do pracownika *regres* w postaci możliwości egzekwowania od niego odpowiedzialności odszkodowawczej, porządkowej lub dyscyplinarnej.

Sąd zgodził się z Prezesem UODO, iż SGGW naruszyła szereg zasad rozporządzenia 2016/679, w tym m.in. zasadę integralności i poufności, nie przeprowadziła analizy ryzyka i nie oceniła, z jakimi zagrożeniami ma lub może mieć do czynienia. Tym samym nie wdrożyła odpowiednich środków technicznych i organizacyjnych, pozwalających skutecznie zabezpieczyć przetwarzane dane osobowe. Sąd przychylił się do stanowiska Prezesa UODO, że inspektor ochrony danych (IOD) nie był angażowany w proces rekrutacji na studia, nie był włączany przez administratora w sprawy dotyczące ochrony danych osobowych w zakresie podejmowanych rozwiązań technicznych w ramach funkcjonowania systemu informatycznego wykorzystywanego do obsługi procesu

[39] Sygn. akt ZSOSS.421.25.2019, wyrok WSA z dnia z 13 maja 2021 r. sygn. akt II SA/Wa 2129/20.
[40] Wyrok WSA w Warszawie z dnia z 13 maja 2021 r. sygn. akt II SA/Wa 2129/20.

rekrutacji kandydatów na studia, a przy wykonywaniu swoich zadań nie uwzględnił ryzyka związanego z operacjami przetwarzania danych. Sąd podkreślił, że administrator danych jest odpowiedzialny za to, aby inspektor ochrony danych monitorował przestrzeganie przepisów dotyczących przetwarzania danych osobowych oraz polityki administratora w dziedzinie ochrony danych osobowych, przeprowadzał szkolenia personelu uczestniczącego w operacjach przetwarzania oraz audyty, uwzględniając ryzyko związane z operacjami przetwarzania (art. 39 ust. 1 lit. b i art. 39 ust. 2 RODO) oraz był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

Na powyższe orzeczenie SGGW złożyła skargę kasacyjną.

Kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych przeprowadzona w 2020 r. w **Virgin Mobile Polska Sp. z o.o.**[41]**,** zakończona wydaniem przez Prezesa UODO decyzji stwierdzającej naruszenie przepisów rozporządzenia 2016/679 i nakładającej na ww. podmiot karę pieniężną w wysokości 1.968.524,00 zł, została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie, który uchylił decyzję organu.

Zdaniem Sądu organ w sposób dostateczny nie rozważył, przy określaniu wysokości kary pieniężnej, okoliczności podejmowania przez administratora (Spółkę) działań w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą, w tym przede wszystkim w zakresie ich wpływu na zastosowanie ww. sankcji. Sąd zauważył, że w uzasadnieniu zaskarżonej decyzji Prezes UODO nie wskazał też, jaki był tego powód i nie powiązał tej okoliczności z rozmiarem szkody. Sąd natomiast uznał za trafne stanowisko Prezesa UODO, m.in. co do braku w przyjętych przez ww. podmiot procedurach uregulowań zapewniających regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych oraz braku dokonania oceny ryzyka w sposób odzwierciedlający realną sytuację panującą w organizacji i opierającą się przede wszystkim na faktach stwierdzonych podczas badania tej sytuacji, audytu, sprawdzenia bądź na podstawie stwierdzonego stanu faktycznego, co doprowadziło do braku prawidłowej oceny zagrożeń dla procesu przetwarzania danych osobowych. W związku z powyższym wobec wypełnienia przez Prezesa UODO przesłanek zmierzających do należytego ustalenia stanu faktycznego sprawy, dokonanie prawidłowych ocen, co do procesu przetwarzania danych osobowych w tym podmiocie i stosowanych środków technicznych i organizacyjnych, co potwierdził Sąd w przywołanym

[41] Sygn. DKN.5112.1.2020.

uzasadnieniu wyroku, Prezes UODO nie złożył skargi kasacyjnej do Naczelnego Sądu Administracyjnego.

4. Wydawanie decyzji administracyjnych i rozpatrywanie skarg

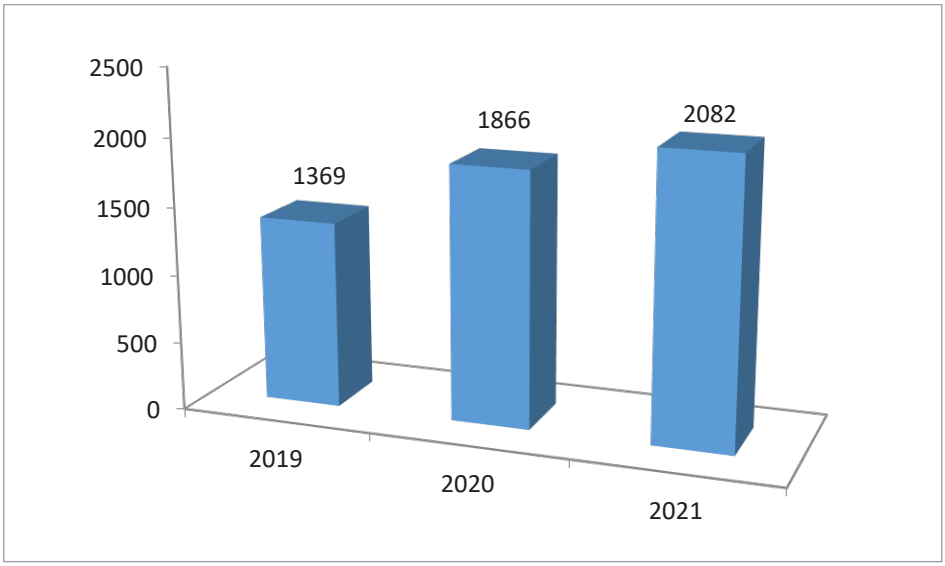
Postępowanie dotyczące naruszenia przepisów o ochronie danych osobowych, wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej, toczy się według przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[42]*. 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.*

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 poprzednich okresach sprawozdawczych, Skarżący wciąż popełniają te same błędy w zakresie wymogów formalnych w składanych przez nich pismach. Najczęściej Skarżący wzywani są do doprecyzowania żądania mieszczącego się w zakresie kompetencji przysługujących Prezesowi UODO, gdyż większość z nich wnosi m.in. o samo wszczęcie postępowania w sprawie, nie wskazując podjęcia jakich działań w sprawie domagają się od Prezesa UODO. Skarżący wnoszą o stwierdzenie, czy doszło do naruszenia ich prawa do ochrony danych osobowych, o przeprowadzenie kontroli w stosunku do skarżonego podmiotu, o nałożenie administracyjnej kary pieniężnej oraz o ustalenie podmiotu, który dopuszcza się naruszenia ich prawa do ochrony danych osobowych, a także wypłaty odszkodowania/zadośćuczynienia. Ponadto wnioskodawcy wzywani są do wskazania pełnej nazwy oraz adresu siedziby albo imienia, nazwiska oraz adresu skarżonego podmiotu oraz do wskazania swojego adresu poczty tradycyjnej,

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

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

W roku 2021 Prezes Urzędu Ochrony Danych Osobowych wydał 2082 decyzje administracyjne, tj. o 216 więcej w stosunku do roku 2020, w którym wydanych było 1866 decyzji.

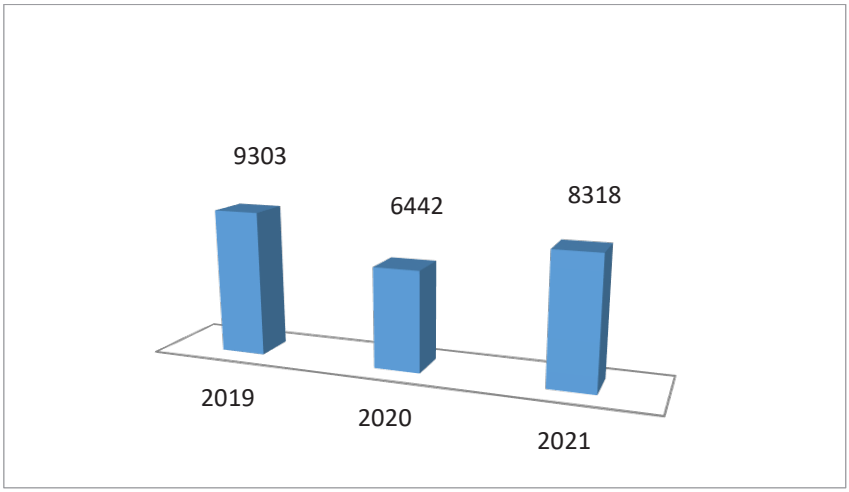


Wykres 2: **Liczba decyzji wydanych przez Prezesa UODO w latach 2019–2021 r.**

4.1. Skargi

Rozpatrywanie skarg jest jednym z głównych zadań organu nadzorczego, zgodnie z art. 57 ust. 1 lit. f RODO. Wpływ skarg do Urzędu Ochrony Danych Osobowych świadczy m.in. o wzroście świadomości obywateli co do przysługujących im praw w zakresie ochrony prywatności i danych osobowych.

W roku 2021 do Urzędu Ochrony Danych Osobowych wpłynęło w sumie **8318 skarg, tj. o 1876 skarg więcej w stosunku do roku 2020.**



Wykres 3: **Liczba skarg, które wpłynęły do UODO w latach 2019–2021 r.**

W roku 2021 do Urzędu Ochrony Danych Osobowych wpłynęło w sumie **8318 skarg (w 2020 – 6442 skargi**). Postępowania zakończono w 6852 sprawach, z czego 1734 zakończono wydaniem decyzji administracyjnej. Jednocześnie do Urzędu wpłynęły 142 skargi, które zostały zakwalifikowane jako transgraniczne.

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

- **1412 skarg na podmioty sektora publicznego;**
- **3486 skarg na podmioty sektora prywatnego;**
- **1445 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa;**
- **1833 skargi na podmioty sektora finansowego, ubezpieczeń i telekomunikacji;**
- **142 skargi na podmioty sektora transgranicznego.**

4.1.1. Sektor publiczny

Spośród 8318 skarg, które w 2021 r. wpłynęły do Urzędu, **1412** z nich dotyczyło podmiotów sektora publicznego. Poniżej omówione zostały przykłady kilku takich skarg.

Udostępnienie na stronie internetowej Biuletynu Informacji Publicznej danych osobowych w związku z publikacją zaleceń pokontrolnych wydanych po przeprowadzonej kontroli

Omawiana skarga dotyczyła udostępniania danych osobowych, w związku z publikacją zaleceń pokontrolnych wydanych po przeprowadzonej kontroli w żłobku przez Wydział Zdrowia i Spraw Społecznych Urzędu Miasta, na podstawie art. 54 i art. 56 w zw. z art. 55 ust. 2 ustawy z dnia 4 lutego 2011 r. o opiece nad dziećmi w wieku do lat 3[43]. Zakres udostępnionych danych osobowych Skarżącej obejmował jej imię i nazwisko oraz obrane określenie prowadzonej działalności gospodarczej (firmę przedsiębiorcy) wraz z nazwą i adresem kontrolowanej placówki.

W myśl art. 3 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[44], prawo do informacji publicznej obejmuje uprawnienia do uzyskania informacji publicznej, w tym uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego (pkt 1), wglądu do dokumentów urzędowych (pkt 2), dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów (pkt 3). Informacje udostępnia się m.in. poprzez ogłaszanie informacji publicznych, w tym dokumentów urzędowych, w Biuletynie Informacji Publicznej (BIP). Obowiązane do udostępniania informacji publicznej są władze publiczne oraz inne podmioty wykonujące zadania publiczne, będące w posiadaniu takich informacji (art. 4 ust. 1 i ust. 3). Zgodnie z art. 6 ust. 1 pkt 4 lit. a ww. ustawy, udostępnieniu podlega informacja publiczna o danych publicznych, w tym treść i postać dokumentów urzędowych, w szczególności: treść aktów administracyjnych i innych rozstrzygnięć (tiret pierwsze); dokumentacja przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających (tiret drugie). W myśl art. 8 ust. 3 tej ustawy, podmioty, o których mowa w art. 4 ust. 1 i 2, obowiązane są do udostępniania w BIP informacji publicznych, o których mowa w art. 6 ust. 1 pkt 1–3, pkt 4 lit. a tiret drugie, lit. c i d i pkt 5. Podmioty, o których mowa w zdaniu pierwszym, mogą udostępniać w BIP również inne informacje publiczne.

Prezes Urzędu Ochrony Danych Osobowych stwierdził, że w przedmiotowej sprawie, przy realizacji przez Prezydenta Miasta obowiązku opublikowania zaleceń pokontrolnych dot. kontroli w żłobku przeprowadzonej przez Wydział Zdrowia i Spraw Społecznych Urzędu Miasta, udostępnienie danych w postaci nazwy firmy Skarżącej oraz adresu prowadzonej działalności gospodarczej było adekwatne do realizowanego celu. Powyższe dane określały bowiem podmiot, który został poddany kontroli. Skarżąca prowadziła żłobek w ramach działalności gospodarczej. Imię i nazwisko Skarżącej oraz obrane określenie prowadzonej działalności gospodarczej[45] stanowiły jej

[43] Dz. U. z 2016 r. poz. 157 z późn. zm. oraz art. 49 ustawy z dnia 6 marca 2018 r. prawo przedsiębiorców, Dz. U. z 2018 r. poz. 646.
[44] Dz. U. z 2020 r. poz. 2176.
[45] Art. 432 w zw. z art. 434 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz. U. z 2020 r. poz. 1740.

firmę. Z ustaleń postępowania wynikało również, że adres placówki poddanej kontroli, którą prowadziła Skarżąca, był tożsamy z jej miejscem zamieszkania. Udostępnienie ww. danych osobowych Skarżącej na stronie internetowej Biuletynu Informacji Publicznej Miasta znalazło zatem oparcie w przesłance określonej w art. 6 ust. 1 lit. c RODO w zw. z art. art. 8 ust. 3 ustawy o dostępie do informacji publicznej w zw. z art. 6 ust. 1 pkt 4 lit. a tiret drugie.

Przy rozpoznawaniu sprawy Prezes UODO oparł się na zasadzie ograniczonego przechowywania danych osobowych określonej w art. 5 ust. 1 lit. e RODO. Zgodnie z nią, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia, w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania"). Wskazać należy, że przepisy ustawy o dostępie do informacji publicznej, a także przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[46], nie precyzują okresu udostępniania informacji w BIP, zarówno minimalnego, jak i maksymalnego. Brak jednak określonych przepisami prawa okresów przetwarzania udostępnionych informacji (zawierających dane osobowe) nie powoduje, że informacje takie można przetwarzać bezterminowo. Zasada ograniczenia czasowego udostępnienia danych osobowych w BIP oznacza, że nawet jeśli określone dane odpowiadają celowi, dla którego są zbierane, to nie powinny być przetwarzane, w tym udostępniane innym podmiotom, bez żadnego czasowego ograniczenia. Czasowym wyznacznikiem powinno być osiągnięcie celu przetwarzania. Opublikowane w BIP informacje, dla których termin publikacji nie wynika z przepisów prawa, powinny zostać poddane ocenie zgodnie z formalną procedurą wprowadzoną przez administratora, zapewniającą usystematyzowane kształtowanie BIP tak, aby wszystkie informacje, dla których cel przetwarzania został osiągnięty, zostały z BIP usunięte.

Prezydent Miasta, jako administrator, był zobowiązany do zapewnienia przejrzystości prowadzonych przez siebie działań, przy jednoczesnym zachowaniu przepisów o ochronie danych osobowych. Spoczywał na nim obowiązek zapewnienia, aby przetwarzanie danych osobowych

[46] Dz. U z 2007 r. Nr 10, poz. 68.

zamieszczonych w BIP było zgodne z przepisami RODO, w tym m.in. z zasadą ograniczenia przechowywania, określoną w art. 5 ust. lit. e RODO.

Wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie (WSA) uchylona została decyzja Samorządowego Kolegium Odwoławczego oraz poprzedzająca ją decyzja Prezydenta Miasta w przedmiocie wykreślenia żłobka z rejestru żłobków i przedszkoli. Natomiast organ nadzorczy został zobowiązany do przeprowadzenia ponownej kontroli w żłobku z uwagi na znaczny upływ czasu od ostatniej udokumentowanej kontroli. Sąd stwierdził, że bez uprzedniego rozpatrzenia przez organ prawidłowo wniesionych zastrzeżeń do sprawozdania z kontroli i rozstrzygnięcia o ich uwzględnieniu bądź nieuwzględnieniu (w całości lub w części) nie będzie możliwe uznanie, iż doszło do wyczerpania procedury weryfikacji ustaleń poczynionych w toku kontroli i do finalnego określenia katalogu nieprawidłowości w działalności kontrolowanego podmiotu. Dopiero tak ustalony katalog nieprawidłowości może, w świetle art. 57 ust. 3 ustawy z 2011 r. o opiece nad dziećmi w wieku do lat 3, stanowić podstawę do formułowania zaleceń pokontrolnych, zamieszczanych w stanowisku organu, o którym mowa w tym przepisie.

Po przeprowadzeniu postępowania wyjaśniającego w niniejszej sprawie, Prezes UODO stwierdził, że cel, dla którego dane osobowe Skarżącej zostały upublicznione w zaleceniach pokontrolnych na stronie internetowej Biuletynu Informacji Publicznej Miasta, został osiągnięty. Tym samym dalsze przetwarzanie danych Skarżącej w powyższy sposób naruszało zasadę ograniczenia czasowego wymienioną w art. 5 ust.1 lit. e RODO. Działając na podstawie art. 58 ust. 2 lit. g RODO, Prezes UODO nakazał Prezydentowi Miasta usunięcie danych osobowych Skarżącej z ww. zaleceń pokontrolnych, znajdujących się na stronie internetowej BIP Miasta, w zakresie imienia, nazwiska i adresu[47].

Udostępnienie na stronie internetowej Biuletynu Informacji Publicznej danych osobowych w związku z publikacją informacji o sesji rady miejskiej oraz uchwale rady miejskiej

Do Prezesa Urzędu Ochrony Danych Osobowych wpłynęła skarga, w której został podniesiony zarzut udostępnienia przez organ administracji publicznej na stronie internetowej BIP danych osobowych Skarżącej, w zakresie jej imienia i nazwiska, zawartych w informacji o zwołaniu sesji rady miejskiej oraz uchwale rady miejskiej podjętej po rozpatrzeniu skargi Skarżącej na Burmistrza.

W postępowaniu wyjaśniającym Prezes UODO uznał, że dla spełnienia obowiązku wynikającego z art. 4 ust. 1 pkt 1 ustawy o dostępie do informacji publicznej, nie było niezbędne

[47] DS.523.3685.2020.

ujawnienie na stronie internetowej BIP imienia i nazwiska osoby wnoszącej skargę na Burmistrza. Nie było również niezbędne upublicznienie na stronie internetowej Urzędu Miasta danych osobowych Skarżącej zawartych w informacji o zwołaniu sesji rady miejskiej. Przy upublicznieniu w celu informacyjnym informacji o zwołaniu sesji rady miejskiej oraz o podjętej uchwale w związku z wniesioną skargą, zbędne było (nieadekwatne do celu) ujawnianie imienia i nazwiska Skarżącej. Publikacja dokumentu, który zawiera dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych, zgodnie z zasadą minimalizacji danych, określoną w art. 5 ust. 1 lit. c RODO. Z ustaleń postępowania nie wynikało również, aby Skarżąca składając skargę na Burmistrza, pełniła funkcję publiczną lub zrezygnowała z prawa do prywatności, wobec tego nie można było zastosować zwolnienia z ograniczenia prawa do informacji publicznej wynikającego z art. 5 ust. 2 ustawy o dostępie do informacji publicznej. W ocenie Prezesa UODO publikacja na stronie internetowej, w informacji o sesji oraz w uchwale rady miejskiej, powinna była nastąpić po usunięciu danych osobowych Skarżącej z tych dokumentów.

Wydając rozstrzygnięcie w przedmiotowej sprawie Prezes UODO stwierdził, że przetwarzanie przez organ administracji publicznej danych osobowych Skarżącej w postaci imienia i nazwiska poprzez ich udostępnienie w Biuletynie Informacji Publicznej w informacji o sesji i uchwale podjętej przez radę miejską po rozpatrzeniu jej skargi na Burmistrza, nie znajdowało uzasadnienia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO. Biorąc pod uwagę, że dane osobowe Skarżącej zawarte w informacji o sesji oraz uchwale zostały zanonimizowane, Prezes UODO uwzględniając wagę i charakter stwierdzonego naruszenia, udzielił administratorowi danych upomnienia za stwierdzone naruszenie[48].

Przetwarzanie danych osobowych w BIP i na sesjach rad miejskich

Przedmiotem jednego z postępowań był zarzut przetwarzania przez Starostwo na stronie internetowej Biuletynu Informacji Publicznej danych osobowych Skarżącej bez podstawy prawnej oraz z naruszeniem obowiązku informacyjnego.

Organ nadzorczy ustalił, że dane osobowe (zarówno zwykłe, jak i szczególnej kategorii, tj. imię, nazwisko, dane dotyczące zdrowia, obejmowane stanowisko, podstawa zmiany warunków zatrudnienia) Skarżącej zostały udostępnione w formie elektronicznej na stronie internetowej BIP. Działanie to wynikało z realizacji przez Starostę ciążącego na nim obowiązku przewidzianego

[48] DS.523.5134.2020.

obowiązującymi przepisami prawa, w tym ustawy o dostępie do informacji publicznej[49]. Przepisy te nie precyzują okresu udostępniania informacji w BIP, zarówno minimalnego, jak i maksymalnego. Jednak brak określonych przepisami prawa okresów przetwarzania udostępnionych w ten sposób informacji (zawierających dane osobowe) nie powoduje, że można je przetwarzać bezterminowo. Starosta, zgodnie z zasadą ograniczenia przechowywania wynikającą z art. 5 ust. 1 lit. e RODO, stanowiącego, że dane osobowe muszą być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane, przy ustalaniu okresu retencji, powinien kierować się przepisami innych aktów prawnych, z których wynika czas, przez jaki może przetwarzać dane osobowe. W przypadkach, w których prawo nie reguluje okresu retencji danych, po przeprowadzeniu analiz, powinien określić ten okres tak, aby przetwarzanie danych było zgodne z celami, z którymi je pozyskano.

W związku z brakiem opracowanych i wdrożonych procedur w tym zakresie, co potwierdzał zgromadzony materiał dowodowy, na stronie BIP Starostwa dokumenty zawierające dane osobowe publikowane były przez okres dłuższy, niż jest to niezbędne do celów, w których dane były przetwarzane. Skutkiem powyższego było umożliwienie dostępu do nich nieograniczonej liczbie użytkowników Internetu. Ponad dwuletni okres publikacji danych osobowych Skarżącej na stronie internetowej BIP w treści uchwały Starostwa, zdaniem Prezesa UODO był okresem wystarczającym, bowiem podstawowym celem BIP jest powszechne informowanie o sprawach publicznych, celem publikacji zaś była możliwość zapoznania się z treścią uchwały przez społeczność lokalną, a publikacja danych osobowych Skarżącej w dalszym okresie niż wskazany nie miała już charakteru informacyjnego, a sam cel został zrealizowany. Każda informacja zamieszczana w BIP powinna być analizowana przez administratora pod kątem jej aktualności i celowości dalszej publikacji. Starosta – jako administrator – nie może zakładać automatyzmu przy publikacji danych osobowych w BIP, tj. upublicznienia wszelkich danych osobowych i ich dalszego nieograniczonego w czasie przetwarzania. Jest on bowiem zobowiązany do każdorazowego dokonania stosownej oceny tak zasadności upublicznienia danych osobowych konkretnej osoby, jak i określenia końca ich retencji. Należy również podkreślić, iż funkcja informacyjna na stronach BIP zachowuje swój charakter nawet w momencie usunięcia danych osobowych osób wskazanych w treści publikowanych dokumentów. W związku z powyższym Prezes UODO w swojej decyzji[50] nakazał usunięcie danych osobowych Skarżącej z BIP.

[49] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. z 2020 r. poz. 2176.
[50] ZSPU.440.732.2018.

Przedmiotem innego postępowania prowadzonego przez organ właściwy w sprawie ochrony danych osobowych był zarzut nieprawidłowego przetwarzania danych osobowych Skarżących przez Radę Miejską (wymienienie ich imion i nazwisk na sesji Rady transmitowanej na żywo).

Na obradach Rady Miejskiej, które były transmitowane online oraz nagrywane (nagranie udostępniono następnie na YouTube) przedstawiciel komisji ds. skarg, wniosków i petycji przedstawił stanowisko tej komisji w sprawie rozpatrzonej przez nią skargi, które następnie zostało skomentowane przez jedną z radnych. I to ona w swojej wypowiedzi udostępniła dane osobowe Skarżących. Organ nadzorczy podkreślił, że informacje ujawnione przez Radną pozwalały pośrednio zidentyfikować Skarżących bez nadmiernych wysiłków i kosztów. Udostępnienie to nastąpiło bez podstawy prawnej, tj. nie miało oparcia w którejkolwiek z przesłanek przetwarzania danych osobowych określonych w art. 6 ust. 1 lit. a–f RODO. Stosownie do przepisów ustawy o samorządzie gminnym[51] oraz postanowień statutu miasta, skarga złożona przez Skarżącego do Rady Miejskiej powinna być przedmiotem obrad jedynie komisji skarg, wniosków i petycji, nie zaś obrad rady miejskiej. Z drugiej strony zaś, ustawowy obowiązek udostępnienia transmisji oraz nagrania z obrad rady gminy, m.in. w BIP, nie oznacza, że w ramach tej transmisji organy gminy mogą w sposób dowolny udostępniać dane osobowe osób fizycznych, zwłaszcza jeżeli osoby te nie pełnią żadnych funkcji publicznych. W ocenie Prezesa Urzędu, zaskarżony proces przetwarzania danych osobowych nie miał oparcia zarówno w przepisach ustawy o samorządzie gminnym, jak i ustawy o dostępie do informacji publicznej, a więc nastąpił bez podstawy prawnej w rozumieniu art. 6 RODO.

Prezes UODO w wydanej w tej sprawie decyzji[52] udzielił Radzie upomnienia w związku z naruszeniem zasady legalności (art. 5 ust. 1 lit. a RODO) oraz zasady rozliczalności (art. 5 ust. 2 RODO).

Przedmiotem innej skargi było nieprawidłowe przetwarzanie danych osobowych Skarżących przez Burmistrza i Radę Miasta. Podczas jednej z sesji Rady miejskiej, na której radni mieli ustosunkować się do skargi złożonej na Burmistrza do kuratorium, przewodniczący Rady, rozpoczynając ten punkt programu, odczytał treść skargi wraz z imionami i nazwiskami osób ją składających. Sesja Rady była transmitowana na żywo online, a jej nagranie zostało następnie udostępnione w Internecie. Ustalono, że dane osobowe Skarżących były przez Radę przetwarzane w związku z rozpatrywaniem skargi złożonej na Burmistrza i w tym zakresie to Rada była administratorem ich danych osobowych. Z kolei Burmistrz oświadczył, że zgodnie

[51] Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz. U. z 2021 r. poz. 1372.
[52] ZWOS.440.5580.2019.

z postanowieniami statutu miasta, obsługę sesji Rady zapewnia Urząd Miasta, którego kierownikiem jest Burmistrz, a zatem to on realizuje transmisję posiedzeń Rady. Przyznał, że nie opracował jednak wewnętrznych uregulowań określających szczegółowe zasady tej transmisji.

Biorąc pod uwagę powyższe ustalenia, obowiązujące przepisy, incydentalny charakter naruszenia oraz fakt, że udostępnione w sieci nagranie sesji Rady zostało zanonimizowane, Prezes UODO wydał decyzję[53] udzielającą upomnienia[54]:

- Radzie miejskiej za odczytanie przez jej przewodniczącego pełnej treści skargi wraz z danymi osobowymi osób ją wnoszących, podczas gdy dane te nie były niezbędne do jej rozpatrzenia, co stanowiło naruszenie zasady minimalizacji danych wyrażonej w art. 5 ust. 1 lit. c RODO,
- Burmistrzowi za niezapewnienie odpowiedniego bezpieczeństwa danych osobowych podczas transmisji online w Internecie oraz poprzez zamieszczenie niezanonimizowanego nagrania z obrad sesji rady miejskiej, co stanowiło naruszenie zasady integralności i poufności danych wyrażonej w art. 5 ust. 1 lit. f w zw. z art. 24 ust. 1 i art. 32 ust. 1 lit. a RODO.

Spełnienie obowiązku informacyjnego, o którym mowa w art. 13 RODO oraz przetwarzanie danych osobowych po wycofaniu zgody

W analizowanym 2021 roku odnotowano skargi dotyczące braku spełnienia obowiązku informacyjnego przez administratora danych osobowych wobec osoby, której dane dotyczą, a także skargi w przedmiocie przetwarzania danych osobowych przez administratora, mimo wycofania zgody na ich przetwarzanie.

Przedmiotem jednej ze skarg było niespełnienie przez Burmistrza wobec Skarżącego obowiązku informacyjnego wynikającego z art. 13 RODO w związku z pozyskaniem jego danych osobowych podczas nagrywania rozmowy w czasie spotkania w urzędzie miejskim. Przed rozpoczęciem nagrywania przebiegu spotkania odebrano od Skarżącego zgodę na nagrywanie. Niemniej kolejnego dnia Skarżący wycofał swoją zgodę, a mimo to jego dane osobowe nadal były przetwarzane przez Burmistrza w przedmiotowym nagraniu.

Ponadto Burmistrz nie spełnił obowiązku informacyjnego względem Skarżącego w związku z nagrywaniem ww. rozmowy. Zgodnie z art. 13 ust. 1 RODO obowiązek podania osobie, której dane dotyczą, informacji, o których mowa w art. 13 ust. 1 i ust. 2 RODO, spoczywa na administratorze danych w momencie pozyskiwania danych osobowych od osoby, której dane dotyczą.

[53] ZSPU.440.1176.2019.
[54] Upomniane podmioty odwołały się od tej decyzji organu nadzorczego do Wojewódzkiego Sądu Administracyjnego w Warszawie, lecz ich skargi zostały oddalone, zob. wyrok z 25 stycznia 2022 r. sygn. akt II SA/Wa 1855/21.

Obowiązek informacyjny przy gromadzeniu danych od osoby, której dane dotyczą, o którym mowa w komentowanym przepisie, powinien być realizowany w sposób zindywidualizowany wobec konkretnej osoby, której dane administrator gromadzi. Oznacza to, że przekazanie informacji tej osobie nie powinno być zastępowane komunikatami kierowanymi do ogółu osób zainteresowanych (np. na stronie internetowej). Nie można także uznać, że samo poinformowanie osoby, której dane dotyczą, o zamiarze nagrywania rozmowy, stanowi spełnienie obowiązku informacyjnego wynikającego z art. 13 ust. 1 i ust. 2 RODO, ponieważ informacja ta nie zawiera wymaganych tym przepisem elementów.

W przedmiotowej sprawie Prezes UODO uznał, że Burmistrz nie dysponował zgodą Skarżącego na przetwarzanie jego danych osobowych zawartych w nagraniu ww. rozmowy i że nie została spełniona żadna z przesłanek legalności przetwarzania danych osobowych określonych w art. 6 ust. 1 RODO.

Prezes UODO, uwzględniając wagę i charakter stwierdzonego naruszenia, udzielił Burmistrzowi upomnienia na podstawie art. 58 ust. 2 lit. b RODO za naruszenie art. 13 ust. 1 i ust. 2 RODO z uwagi na niespełnienie wobec Skarżącego obowiązku informacyjnego wynikającego z art. 13 ust. 1 i ust. 2 RODO w zw. z nagrywaniem rozmowy odbytej podczas spotkania w urzędzie miejskim oraz na podstawie art. 58 ust. 2 lit. g RODO nakazał Burmistrzowi usunięcie z nagrania rozmowy danych osobowych Skarżącego, pozyskanych podczas spotkania Skarżącego w urzędzie miejskim[55].

Wykorzystanie numeru telefonu przez organ administracji publicznej w celach informacyjnych

Tematem kolejnej skargi było wykorzystanie przez Ministra Cyfryzacji numeru telefonu – podanego przez Skarżącego w procesie zakładania profilu zaufanego – do przesyłania informacji o możliwości logowania na stronie internetowej „pacjent.gov.pl" za pomocą profilu zaufanego. W ocenie Skarżącego przesłana do niego informacja o możliwości zalogowania się na stronie „pacjent.gov.pl" miała charakter marketingowy.

Zasady świadczenia usługi profilu zaufanego określa ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[56]. Art. 20ad tej ustawy wskazuje, że profil zaufany zawiera dane identyfikujące osobę fizyczną obejmujące: imię (imiona), nazwisko, datę urodzenia i numer PESEL. Na podstawie delegacji ustawowej zawartej w art. 20d,

[55] DS.523.382.2021.
[56] Dz. U. z 2020 r. poz. 346 z późn. zm.

rozporządzeniem Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego[57], rozszerzono ww. katalog o następujące dane: identyfikator użytkownika, identyfikator profilu zaufanego, czas potwierdzenia, termin ważności, adres poczty elektronicznej, numer telefonu komórkowego, wykorzystywane czynniki uwierzytelniania, o których mowa w ust. 4 (§10).

Serwis pacjent.gov.pl jest dedykowanym pacjentom serwisem informacyjnym Ministerstwa Zdrowia, administrowanym przez Centrum Systemów Informacyjnych Ochrony Zdrowia (aktualnie Centrum e-Zdrowia), udostępniającym Internetowe Konto Pacjenta (IKP), umożliwiające użytkownikom dostęp do najważniejszych informacji z zakresu ochrony zdrowia (zob. „Warunki korzystania z serwisu pacjent.gov.pl"). Zalogowanie (tj. uwierzytelnienie usługobiorcy) do Internetowego Konta Pacjenta możliwe jest m.in. dla posiadaczy profilu zaufanego. Posiadanie profilu zaufanego pozwala logować się do IKP bezpośrednio, tj. bez podejmowania dodatkowych działań i spełnienia dodatkowych warunków.

Postępowanie wyjaśniające wykazało, że celem przesyłania informacji o możliwości zalogowania się na stronie pacjent.gov.pl za pomocą profilu zaufanego było poinformowanie o nowej usłudze publicznej świadczonej przez Ministra Zdrowia na rzecz osób fizycznych, która w szczególności pozwala na zapoznanie się posiadacza profilu zaufanego z realizowanymi na jego rzecz świadczeniami zdrowotnymi.

Motyw 45 RODO wskazuje, że jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Ponadto wskazane w nim jest, że „rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne (…), a prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania. Ponadto prawo to może doprecyzowywać ogólne warunki określone w rozporządzeniu dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania.

Zgodnie z art. 15b ust. 1 ww. ustawy, podmiot publiczny w celu ochrony interesu prawnego lub faktycznego osoby fizycznej, w szczególności w związku z realizowanymi na jej rzecz usługami,

[57] Dz.U. 2020 poz. 1194.

może wykorzystywać jej dane kontaktowe gromadzone w rejestrze publicznym lub systemach teleinformatycznych. Brak odpowiedzi osoby fizycznej na próbę nawiązania przez podmiot publiczny kontaktu z wykorzystaniem danych kontaktowych nie może negatywnie wpłynąć na jej sytuację prawną lub faktyczną.

W przedmiotowej sprawie stwierdzono, że wiadomości SMS o kwestionowanej przez Skarżącego treści, wysyłane były w ramach akcji poinformowania użytkowników profilu zaufanego o możliwości zalogowania się przez ten profil do świadczonej na ich rzecz nowej usługi publicznej. Dzięki tej usłudze, wykorzystującej sieć teleinformatyczną, posiadacz profilu zaufanego ma możliwość m.in. zapoznać się z realizowanymi na jego rzecz świadczeniami zdrowotnymi. Przy tym brak odpowiedzi Skarżącego na próbę nawiązania z nim przez podmiot publiczny kontaktu z wykorzystaniem jego danych, nie miał negatywnego wpływu ja jego sytuację prawną lub faktyczną. Jednocześnie sam Skarżący nie podnosił takiej okoliczności, wskazując jedynie na brak jego zgody na wykorzystanie jego danych osobowych w celu innym niż obsługa profilu zaufanego. W ocenie Prezesa UODO powyższe działanie mieściło się w kategorii przetwarzania „niezbędnego do wykonania zadania realizowanego w interesie publicznym", a tym samym znajdowało oparcie w przesłance określonej w art. 6 ust. 1 lit. e RODO w zw. z art. 15b ust. 1 ww. ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[58]. Wobec powyższego Prezes UODO w wydanej decyzji odmówił uwzględnienia wniosku Skarżącego. Skarżący wniósł skargę do Wojewódzkiego Sądu Administracyjnego w Warszawie na ww. decyzję Prezesa UODO. Wyrokiem z dnia 22 września 2021 r. sąd ten oddalił skargę na ww. rozstrzygnięcie[59].

Udostępnienie danych osobowych zawartych w treści pisma na tablicy ogłoszeń

W analizowanym okresie sprawozdawczym Prezes UODO rozstrzygał skargę dotyczącą udostępnienia na tablicy ogłoszeń danych osobowych pracownika (egzaminatora) przez Wojewódzki Ośrodek Ruchu Drogowego.

Ustalono, że na tablicy w pokoju, w którym egzaminatorzy dokonują losowania osób egzaminowanych, została wywieszona kopia pisma osoby egzaminowanej adresowanego do marszałka województwa za pośrednictwem dyrektora Wojewódzkiego Ośrodka Ruchu Drogowego. W treści tego pisma zostało wskazane imię i nazwisko Skarżącego oraz ocena jego zachowania podczas przeprowadzania egzaminu.

[58] ZSPU.440.568.2019.
[59] sygn. akt II SA/Wa 871/21.

Wojewódzki Ośrodek Ruchu Drogowego w zakresie ww. udostępnienia danych osobowych Skarżącego wyjaśnił, że celem wywieszenia tego pisma była prezentacja pozytywnej opinii o innym niż Skarżący egzaminatorze. Postępowanie administracyjne wykazało również, że dostęp do pomieszczenia, w którym wywieszone było pismo mieli egzaminatorzy, pracownicy koordynacji i nadzoru nad egzaminami oraz osoby sprzątające. Pracownik Ośrodka odpowiedzialny za wywieszenie pisma został pouczony przez inspektora ochrony danych, a następnie zdyscyplinowany przez dyrektora Ośrodka. Ponadto przedmiotowe pismo zostało usunięte z tablicy ogłoszeń po zwróceniu się przez organizację związkową z wezwaniem o jego usunięcie z tej tablicy.

W swoim rozstrzygnięciu Prezes UODO wskazał, że udostępnienie danych osobowych Skarżącego przez Wojewódzki Ośrodek Ruchu Drogowego naruszyło przepisy art. 6 ust. 1 RODO, bowiem nie znajdowało ono oparcia w żadnej z przesłanek wskazanych w tym przepisie.

Mając na uwadze powyższe, uwzględniając wagę i charakter stwierdzonego naruszenia oraz fakt, że Ośrodek zaprzestał udostępniania danych osobowych Skarżącego w kwestionowany przez niego sposób, Prezes UODO uznał za zasadne skorzystanie w sprawie z instrumentu o charakterze naprawczym przewidzianego w art. 58 ust. 2 lit. b RODO i udzielił Ośrodkowi upomnienia w związku z zaistniałym naruszeniem art. 6 ust. 1 RODO[60].

Umożliwienie osobom nieuprawnionym dostępu do danych osobowych osadzonego znajdujących się w „zeszycie spostrzeżeń"

Organ właściwy do spraw ochrony danych osobowych odnotował skargi dotyczące kwestii udostępniania danych osobowych osób osadzonych w zakładach karnych. Przedmiotem jednej ze skarg było udostępnienie przez Dyrektora zakładu karnego danych osobowych Osadzonego, znajdujących się w dokumencie o nazwie „zeszyt spostrzeżeń", innym osobom osadzonym.

Jak zostało ustalone, w zakładzie karnym funkcjonariusz działu ochrony pozostawił bez bezpośredniego nadzoru dokumentację o nazwie „zeszyt spostrzeżeń", która zawierała m.in. dane osobowe Skarżącego. Ww. dokumentacja stanowiła dokumentację wewnętrzną jednostki i była prowadzona w celu sprawnego przekazywania między funkcjonariuszami uwag i informacji mogących wpłynąć na ochronę i bezpieczeństwo jednostki. Przeprowadzone postępowanie wykazało, że „zeszyt spostrzeżeń" został zabrany przez osadzonych zakładu karnego. Z analizy monitoringu wizyjnego funkcjonującego w zakładzie karnym wynikało, że przedmiotowy zeszyt był w posiadaniu osadzonych przez kilka minut. Powyższe zdarzenie skutkowało możliwością zapoznania się z danymi

[60] DS.523.5947.2020.

osobowymi Skarżącego znajdującymi się w „zeszycie spostrzeżeń" przez innych osadzonych, tj. osoby do tego nieupoważnione.

Dla rozstrzygnięcia przedmiotowej sprawy znajdowały zastosowanie przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[61]. Powołana ustawa stwarza prawne podstawy stosowania ochrony państwowej w sytuacjach niezgodnego z prawem przetwarzania danych osobowych obywateli, poprzez określenie zasad i warunków ochrony danych przetwarzanych przez właściwe organy, które dokonują przetwarzania danych osobowych w celu określonym w art. 1 ust 1 ustawy z dnia 14 grudnia 2018 r., tj. 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.

Prezes Urzędu Ochrony Danych Osobowych stwierdził, że umożliwienie dostępu do danych osobowych Skarżącego znajdujących się w „zeszycie spostrzeżeń" innym osadzonym naruszyło obowiązujące przepisy o ochronie danych osobowych – nie znajdowało bowiem oparcia w żadnej z przesłanek określonych w art. 13 ustawy z 14 grudnia 2018 r. Umożliwienie dostępu do danych osobowych Skarżącego było przy tym zdarzeniem jednorazowym i miało charakter nieodwracalny[62].

4.1.2. Sektor prywatny

Spośród 8318 skarg, które w 2021 r. wpłynęły do Urzędu, **3486** z nich dotyczyło podmiotów sektora prywatnego. Poniżej omówione zostały przykłady kilku takich skarg.

Obowiązek informacyjny

Jedna ze skarg[63] dotyczyła **przetwarzania danych osobowych Skarżącego w zakresie numeru telefonu.** Skarżący zwrócił się do Przedsiębiorcy o realizację obowiązku informacyjnego, o którym mowa w art. 15 ust. 1 rozporządzenia 2016/679, jednakże nie otrzymał żadnej odpowiedzi. Na stronie internetowej prowadzonej przez Przedsiębiorcę jako telefon do składania zamówień został opublikowany numer telefonu Skarżącego. Skarżący przedstawił wydruk ze strony. Ustalono, że Skarżący błędnie stwierdził, że jego dane osobowe są przetwarzane przez Przedsiębiorcę. Błąd wynikał z korzystania przez Skarżącego z programu lub funkcji dostarczonej przez podmiot trzeci, który automatycznie tłumaczy tekst strony na język angielski. W wyniku tłumaczenia nastąpiło

[61] Dz. U. z 2019 r. poz. 125.
[62] DS.523.3300.2020.
[63] Decyzja z dnia 3 września 2021 r. sygn. DS.523.772.2021.

przestawienie cyfr w numerze telefonu. Ponadto Przedsiębiorca wyjaśnił, że stronę prowadzi w języku polskim, a przedstawiony przez Skarżącego wydruk był automatycznym przetłumaczeniem jego strony na język angielski, którego on nie dostarcza. Przedsiębiorca wyjaśnił również, że po otrzymaniu wniosku Skarżącego o spełnienie obowiązku informacyjnego ustalił, że nie przetwarza jego numeru telefonu i uznał to wezwanie za bezpodstawne. Tym samym odstąpił od udzielania odpowiedzi. Zgodnie z art. 15 rozporządzenia 2016/679, osoba, której dane dotyczą, jest uprawniona nie tylko do uzyskania od administratora informacji na temat przetwarzania jego danych osobowych, ale przede wszystkim potwierdzenia, czy jego dane są przetwarzane. Obowiązek informacyjny realizowany na wniosek jest najważniejszym środkiem pozwalającym na realizację prawa jednostki do kontroli przetwarzania jej danych osobowych. Warunkiem udzielenia stosownych informacji jest weryfikacja osoby, która zwraca się z wnioskiem oraz potwierdzenie (stwierdzenie), że dane tej konkretnej osoby są przetwarzane, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu oraz informacji na ich temat. W każdej sytuacji, tj. zarówno, gdy dane są lub nie są przetwarzane, powinna nastąpić rzetelna i przejrzysta komunikacja w tym zakresie, zgodnie z zasadami określonymi w art. 12 rozporządzenia 2016/679. Nawet ewidentny błąd lub pomyłka po stronie podmiotu danych nie pozbawia go prawa do uzyskania stosownych informacji na temat przetwarzania (w tym przykładzie – o ich nieprzetwarzaniu). Brak jasnej i rzetelnej odpowiedzi, czy dane osobowe Skarżącego są przetwarzane przez Przedsiębiorcę, spowodował skierowanie przeciwko niemu skargi, której mógł uniknąć, gdyby poinformował Skarżącego o swoich ustaleniach. Prezes UODO umorzył postępowanie w zakresie bezpodstawnego przetwarzania danych Skarżącego i upomniał za niespełnienie obowiązku informacyjnego z art. 15 ust. 1 w zw. z art. 12 rozporządzenia 2016/679.

W kolejnej ze spraw[64] przedmiotem postępowania Skarżąca uczyniła **przetwarzanie danych osobowych bez podstawy prawnej oraz niespełnienie obowiązku informacyjnego, o którym mowa w art. 14 ust. 1 i 2 rozporządzenia 2016/679.** Przepis ten określa obowiązek informacyjny administratora spełniany bez wezwania, w przypadku pozyskania danych osobowych w sposób inny niż od osoby, której dane dotyczą. Skarżąca wskazała, że otrzymała list od Fundacji zachęcający do przekazania 1% procentu podatku na jej działania statutowe. Skarżąca nie zna tej Fundacji, nie udzielała jej zgody na przetwarzanie danych osobowych, ani nie wie skąd zostały przez nią pozyskane. W toku postępowania ustalono, że Fundacja przejęła majątek innej fundacji, wstępując w jej prawa i obowiązki. Fundacja przejmowana pozyskała dane osobowe Skarżącej w zakresie

[64] Decyzja z dnia 22 grudnia 2021 r. sygn. ZSPR.440.783.2019.

imienia, nazwiska i adresu, od Ministerstwa Finansów w ramach bazy podatników przekazujących jej 1% swojego rocznego podatku. Skarżąca zaznaczyła odpowiednie pole wyrażenia zgody na kontakt przez Fundację przejmowaną. Zgodnie z art. 5 ust. 1 lit. a rozporządzenia 2016/679, dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Przestrzeganie przez administratora danych tej zasady sprowadza się m.in. do zapewnienia przez niego należytego stopnia dokładności i staranności podczas procesu przetwarzania, w tym do sumiennego i terminowego wykonywania spoczywających na nim obowiązków. Zasada przejrzystości przetwarzania ma zastosowanie nie tylko w chwili zbierania danych osobowych, ale przez cały czas przetwarzania, bez względu na przekazywane informacje lub komunikację. Ma to miejsce np. przy zmianie tożsamości administratora, zmianie treści dotychczasowych oświadczeń o ochronie prywatności lub zmianie celu przetwarzania danych. Administratorzy powinni uwzględnić wpływ tych zmian na zdolność osób, których dane dotyczą do wykonywania swoich praw, a także na ile zmiana ta będzie dla nich niespodziewana lub zaskakująca. Jak wynikło z zebranego materiału dowodowego, list otrzymany przez Skarżącą zawierał jedynie wzmiankę o połączniu się Fundacji, wyrażoną wyłącznie jednym zdaniem, bez konkretnego rozróżnienia podmiotu przejmującego oraz podmiotu przejmowanego, a co za tym idzie – bez dostatecznie wyraźnego wskazania nowych danych teleadresowych, w tym w szczególności adresu strony internetowej z polityką prywatności oraz klauzulą informacyjną. W następstwie przejęcia Fundacji dokonały się istotne zmiany organizacyjne oraz prawne po stronie administratora danych, co miało znaczący wpływ na proces przetwarzania danych osobowych Skarżącej. Skarżąca przed momentem otrzymania od Fundacji korespondencji nie miała żadnej wiedzy ani o fakcie przetwarzania jej danych osobowych przez Fundację, ani tym bardziej o źródle pochodzenia jej danych osobowych w zasobach Fundacji, jak również podstawach prawnych ich przetwarzania czy też o danych do kontaktu z administratorem. Prezes UODO uznał, że Fundacja nie dopełniła wobec Skarżącej obowiązku informacyjnego wynikającego z art. 14 ust. 1 i 2 rozporządzenia 2016/679 i nakazał jego spełnienie.

W innej sprawie[65] Skarżący złożył **skargę na przetwarzanie jego danych osobowych w postaci nagrania rozmowy telefonicznej bez podstawy prawnej**. Wskazał, że nie wypełniono wobec niego obowiązku informacyjnego w żądanym zakresie oraz nie spełniono jego żądania, co do usunięcia tego nagrania. W przedmiotowej sprawie strony postępowania zawarły umowę dotyczącą

[65] Decyzja z dnia 27 grudnia 2021 r. sygn. DS.523.1470.2021.

sprowadzenia samochodu z zagranicy. W trakcie realizacji umowy doszło do rozbieżności w zakresie zleconej usługi, a w konsekwencji kosztów jej wykonania. Przedsiębiorca udostępnił nagranie Skarżącemu w celu udowodnienia ustalonych pierwotnie warunków umowy oraz należności za wykonaną usługę. Po odsłuchaniu nagrania Strony doszły do konsensusu odnośnie należnej przedsiębiorcy kwoty. Tym samym nagranie rozmowy stanowiło dowód w sporze. Ostatecznie Przedsiębiorca usunął przedmiotowe nagranie.

W toku postępowania Przedsiębiorca wyjaśnił, że w odpowiedzi na żądanie Skarżącego wykonał połączenie telefoniczne i w rozmowie wyjaśnił, że nagranie było przechowywane wyłącznie w celu zabezpieczenia interesów Przedsiębiorcy (art. 6 ust. 1 lit. f rozporządzenia 2016/679). Nagranie nie było udostępniane innym podmiotom. Samo nagrywanie odbywało się w sposób jawny, o czym Skarżący został poinformowany przy pierwszym kontakcie. Przedsiębiorca wyjaśnił również, że praktykę tę stosuje wyłącznie do nowych klientów, zgłaszających pierwsze zamówienie, ze względu na związane z tym ryzyko biznesowe. Prezes UODO wyjaśnienia w zakresie uprzedniego poinformowania Skarżącego o nagrywaniu rozmowy uznał za fakt udowodniony. Odnosząc się natomiast do realizacji wniosku Skarżącego, Przedsiębiorca co prawda je spełnił, jednak informacji tej nie przekazał w takiej samej formie, w jakiej się do niego o to zwrócono, tj. w formie elektronicznej. Doszło zatem do naruszenia wymogów dla udzielanych informacji określonych w art. 12 ust. 1 rozporządzenia 2016/679. Zgodnie z tym przepisem administrator udziela informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie, a jeżeli osoba, której dane dotyczą tego zażąda, informacji można udzielić ustnie[66]. Jednocześnie należy zauważyć, że niezachowanie trybu wykonywania praw osoby, której dane dotyczą w trakcie udzielania informacji, spowodowało niemożność wykazania przestrzegania jego praw (art. 5 ust. 2 rozporządzenie 2016/679). Przedsiębiorcę upomniano za naruszenie ww. przepisów.

Podobne zagadnienie zostało poruszone **w skardze[67] na udostępnienie danych osobowych w postaci numeru telefonu na rzecz firmy kurierskiej.** Skarżący chciał wykonać przysługujące mu prawo do zwrotu zakupionego towaru i korzystając z możliwości wskazania danych osoby trzeciej, w tym jej numer telefonu, od której miał on zostać odebrany, podał je Spółce. Spółka uruchomiła procedurę zwrotu towaru i przekazała przewoźnikowi dane osoby trzeciej, od której towar zwracany przez Skarżącego miał zostać odebrany. Z uwagi na to, że numer telefonu osoby trzeciej podany przez

[66] W tym zakresie również motyw 59 rozporządzenia 2016/679 oraz wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 z 29 listopada 2017 r.
[67] Decyzja z dnia 19 listopada 2021 r. sygn. DS.523.152.2020.

Skarżącego nie był widoczny w formularzu zwrotu, system Spółki automatycznie „zaciągnął" numer telefonu Skarżącego, jako osoby, która dokonała zamówienia, w związku z czym został on przekazany na liście przewozowym przewoźnikowi.

W ocenie organu, Spółka nie legitymowała się podstawą prawną uprawniającą ją do przekazania przewoźnikowi numeru telefonu. Skarżący wskazał Spółce dane osoby trzeciej, w tym jej numer telefonu, od której zwracany przez niego towar miał zostać odebrany. Jednocześnie nie wyraził zgody na przetwarzanie jego danych do ww. celu. Spółka posiadała dane niezbędne do realizacji żądania Skarżącego, w tym numer telefonu konieczny do kontaktu z osobą wydającą towar, ponieważ Skarżący przekazał je Spółce. Spółka nie wprowadziła do systemu zwrotu towaru wszystkich danych wskazanych przez Skarżącego, w szczególności wskazanego numeru telefonu, tym samym doprowadziła do sytuacji, w której numer telefonu Skarżącego z zamówienia został automatycznie dopisany do formularza zwrotu wbrew jego woli, a następnie przekazany na rzecz przewoźnika. W ocenie organu, udostępnienie ww. danych Skarżącego nie było również niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Spółkę i przewoźnika. Skarżący zwrócił się również do Spółki z żądaniem wypełnienia wobec niego obowiązku informacyjnego w zakresie wskazania mu, jakie jego dane i jakim odbiorcom Spółka przekazała w związku z realizacją usługi zwrotu towaru. Spółka wskazała, że nie udostępniła jego danych na rzecz podmiotu nieuprawnionego i przesłała mu wyciąg z systemu zwrotów, zawierający dane osoby trzeciej, które wskazał Skarżący. Nie był na nim jednak widoczny numer telefonu Skarżącego. Skarżący kontynuował korespondencję. Spółka po analizie korespondencji przyjęła, że wniosek Skarżącego nie stanowił żądania realizacji prawa określonego w art. 15 ust. 1 rozporządzenia 2016/679, a jedynie próbę wyjaśnienia, jakie jego dane i komu zostały przekazane w związku z realizacją usługi zwrotu towaru. Spółka uznając roszczenie Skarżącego za bezpodstawne zaniechała wobec niego udzielenia dalszej informacji. Powyższe nie wyłączało jednak uprawnienia Skarżącego do uzyskania stosownych i pełnych informacji na temat przetwarzania jego danych osobowych. Brak jasnej i rzetelnej odpowiedzi Spółki w zakresie tego, jakie dane skarżącego i jakim odbiorcom zostały udostępnione spowodowało, że Skarżący nie wiedział, czy Spółka nie uwzględniła lub zignorowała jego żądanie, co zmusiło go do egzekwowania swoich praw poprzez złożenie skargi do organu nadzorczego. Powodowało to niepewność podmiotu, co do okoliczności przetwarzania jego danych osobowych. Brak pełnej odpowiedzi na wniosek Skarżącego takiej niepewności nie usuwał. W ocenie organu, Spółka nie zrealizowała w pełni prawa dostępu do danych. Natomiast powinna udzielić Skarżącemu informacji zgodnie z obowiązkiem określonym w art. 15 ust. 1 lit. b oraz

c rozporządzenia 2016/679. Zgodnie z tym przepisem osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora m.in. informacji o przetwarzanych kategoriach odnośnych danych osobowych oraz informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych. Prezes UODO nakazał Spółce wypełnienie obowiązku informacyjnego z art. 15 ust. 1 lit. b i c rozporządzenia 2016/679 oraz udzielił upomnienia w związku z udostępnieniem numeru telefonu bez podstawy prawnej na rzecz podmiotu nieuprawnionego.

W innym postępowaniu Prezes UODO analizował **spełnienie obowiązku informacyjnego przez Inspektora Nadzoru Budowlanego**. W sprawie tej nie podzielił argumentów Inspektora, że skoro Skarżąca jest stroną wielu postępowań administracyjnych, to musi posiadać informacje o podstawie prawnej, zakresie i celu przetwarzania jej danych osobowych. Nie można bowiem uznać, że z samego faktu, iż Skarżąca otrzymuje od organu pisma w toczących się postępowaniach administracyjnych zawierające podstawy, cel i zakres przetwarzania danych, posiada wiedzę w zakresie art. 13 ust. 1 i ust. 2 RODO. Samo oświadczenie Inspektora, że obowiązek informacyjny w inspektoracie realizowany jest poprzez umieszczenie klauzuli informacyjnej dla interesantów na tablicach informacyjnych znajdujących się w budynku urzędu oraz na stronie internetowej, nie może być uznane za wystarczające do uznania jego dopełnienia wobec Skarżącej. Nie przedstawiono bowiem treści tej klauzuli, nie udało się jej też odnaleźć na stronie internetowej.

W związku z tym organ nadzorczy wydał decyzję[68] nakazującą spełnienie obowiązku informacyjnego.

Pozyskiwanie danych osobowych na potrzeby dochodzenia praw przed sądem

W 2021 roku organ nadzorczy prowadził też postępowanie administracyjne zainicjowane skargą osoby, która domagała się nakazania Firmie prowadzącej portal internetowy udostępnienia na rzecz Wnioskującej danych osobowych użytkowników tego portalu, posługujących się określonymi w piśmie nickami, w zakresie ich imion, nazwisk, adresów e-mail, adresów zamieszkania i zameldowania oraz numerów IP urządzeń, za pomocą których osoby te łączyły się z Internetem i umieszczały wpisy na ww. stronie internetowej. Pełnomocnik Wnioskującej podnosił, że nieprawdziwe informacje zawarte w postach zamieszczonych przez te osoby poniżają w oczach

[68] ZSPU.440.50.2019.

opinii publicznej prowadzoną przez Wnioskującą działalność, jak również narażają ją na utratę zaufania publicznego.

Prezes UODO uznał, że wniosek o udostępnienie danych osobowych w zakresie adresów e-mail i adresów IP użytkowników portalu internetowego, którzy zamieścili wpisy będące przedmiotem wniosku, znajdował uzasadnienie prawne w art. 6 lit. f RODO, i jako taki powinien zostać przez podmiot uwzględniony. Wnioskodawca uzasadnił bowiem wniosek potrzebą dochodzenia swoich praw w związku z pomówieniem, utratą zaufania publicznego i ochroną swoich dóbr osobistych. Zgodnie zaś z treścią art. 24 Kodeksu cywilnego[69] ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny (§ 1). Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych (§ 2). W związku z tym Prezes UODO uznał, że zindywidualizowanie autorów kwestionowanych wpisów stanowi niezbędny warunek dochodzenia przeciwko nim roszczenia związanego z zarzucaną bezprawną ingerencją w sferę dóbr osobistych Skarżącej.

Nie budziła wątpliwości niezbędność dysponowania przez Wnioskodawcę informacjami indywidualizującymi osoby, przeciwko którym chce dochodzić swoich praw. W sytuacji, gdy nie dysponuje zasadniczo żadnymi informacjami o osobach, które zamieściły wpisy będące przedmiotem skargi, wyłącznie poza tymi, które wynikały z ich opublikowania (tj. – oprócz daty, godziny, treści publikacji), którymi posłużyły się te osoby w celu ukrycia swojej tożsamości, zasadne jest przyjęcie, że podejmowane przez Wnioskodawcę działania służą ustaleniu tożsamości tych osób, w celu pociągnięcia ich do odpowiedzialności cywilnej w związku z treścią publikacji i mieszczą się w pojęciu prawnie usprawiedliwionego celu. Oczywiste jest, że pozyskanie (przetwarzanie) danych osobowych w ww. celu w każdym przypadku zostanie uznane przez osoby, których dane te dotyczą, za sprzeczne z ich interesem. Okoliczność ta – zwłaszcza mając na uwadze prawne gwarancje obrony przed roszczeniami strony przeciwnej – nie świadczy jednak o naruszeniu ich praw i wolności. Przyjęcie przeciwnego stanowiska skutkowałoby bezzasadną ochroną tego, kto mógł dopuścić się

[69] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, t.j. Dz.U. z 2020 r. poz. 1740.

bezprawnej ingerencji w sferę prawnie chronionych interesów innej osoby (zwłaszcza przekonany o anonimowości, jaką gwarantuje mu sieć Internet) przed ewentualną odpowiedzialnością za jego działania.

W ocenie Prezesa UODO, Firma bezpodstawnie odmówiła Wnioskodawcy udostępnienia wnioskowanych danych w zakresie adresów poczty e-mail oraz adresów IP, którymi posługiwali się autorzy przedmiotowych wpisów. Tym samym uniemożliwiła mu podjęcie dalszych działań, które pozwolą na skuteczne zainicjowanie przeciwko tym osobom postępowań sądowych. Dla potwierdzenia słuszności prezentowanego w niniejszej sprawie stanowiska, organ nadzorczy powołał wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie[70], w którym wskazano w szczególności, że: „prawo do swobodnej, anonimowej wypowiedzi nie może chronić osób, które naruszają prawa innych osób, od odpowiedzialności za wypowiedziane słowa. Wprawdzie ustalenie tożsamości danej osoby może być utrudnione, jednak z uwagi na to, że każdy komputer zostawia w Internecie ślad – adres IP, za pomocą którego można ustalić komputer, z którego dokonano wpisu, stwarza to możliwość pośredniego ustalenia tożsamości osoby, która dokonała tego wpisu (…) uczestnik postępowania posiada informacje o dacie logowania, pseudonimach osób dokonujących tej czynności i treści dokonanych wpisów. W ocenie Sądu, powyższe informacje, zestawione z adresami IP, umożliwiają jednoznaczne określenie tożsamości osób, które naruszyły dobra osobiste uczestnika postępowania. (...) żądane przez uczestnika postępowania adresy IP stanowią w niniejszej sprawie dane osobowe w rozumieniu art. 6 ust. 1 ustawy o ochronie danych osobowych, a nakazanie ich udostępnienia stanowi realizację dyspozycji ust. 2 tego przepisu, tzn. stworzy możliwość zidentyfikowania osoby, bądź osób, których tożsamość można określić pośrednio. (...) sam adres IP komputera nie wystarcza do wskazania osoby, która z niego korzystała, ale w zestawieniu z innymi informacjami pozwala przypuszczać, że jej tożsamość można ustalić. W ocenie Sądu, identyfikacja tej osoby nie musi być związana z nadmiernymi kosztami, czasem lub działaniami (…)".

Prezes UODO w swojej decyzji[71] nakazał udostępnienie na rzecz Wnioskodawcy danych osobowych autorów kwestionowanych wpisów w zakresie, w jakim podmiot tymi danymi dysponował – tj. informacji o adresach e-mail i adresach IP tych osób.

Przedmiotem kolejnej sprawy była **odmowa udostępnienia przez podmiot prowadzący portal danych osobowych osoby posługującej się określonym nickiem** Spółce, która chciała

[70] Wyrok WSA w Warszawie z 3 lutego 2010 r. sygn. akt II SA/Wa 1598/09.
[71] ZAS.440.32.2019.

dochodzić przed sądami powszechnymi ochrony swoich praw, naruszonych w związku z zamieszczonymi pod artykułem prasowym wpisami.

W ocenie organu nadzorczego, wniosek Skarżącej firmy o udostępnienie danych osobowych w zakresie adresu IP użytkownika portalu, który zamieścił wpisy będące przedmiotem skargi, znajdował uzasadnienie prawne w art. 6 ust. 1 lit. f RODO, i powinien zostać przez podmiot uwzględniony. Skarżący bowiem podjął odpowiednie kroki prawne w celu wiarygodnego uzasadnienia potrzeby posiadania wnioskowanych danych, a mianowicie na podstawie art. 488 § 1 Kodeksu postępowania karnego[72] złożył pisemną skargę do odpowiedniej komendy policji z wnioskiem o wykrycie sprawcy przestępstwa pomówienia oraz o przekazanie powyższej skargi sądowi rejonowemu celem rozpoznania sprawy. Sąd zaś zwolnił pracowników portalu internetowego z zachowania tajemnicy służbowej, celem ustalenia tożsamości sprawcy oraz numeru IP komputera użytkownika, który zamieszczał wpisy na portalu. Ponadto Firma wykazała niezbędność żądanych danych z punktu widzenia możliwości dochodzenia wobec tej osoby roszczeń na drodze sądowej o ochronę swoich dóbr osobistych, a zindywidualizowanie autorów kwestionowanych wpisów stanowi niezbędny warunek dochodzenia przeciwko nim roszczenia związanego z zarzucaną bezprawną ingerencją w sferę dóbr osobistych Firmy.

Prezes UODO, w wydanej w tej sprawie decyzji[73], nakazał podmiotowi prowadzącemu portal udostępnienie na rzecz Skarżącej danych osobowych autora kwestionowanych wpisów w zakresie, w jakim podmiot tymi danymi dysponuje, tj. informacji o adresie IP tego użytkownika.

Marketing

Częstym tematem skarg było **przetwarzanie danych osobowych w celach marketingowych** – głównie w zakresie nierealizowania obowiązków informacyjnych albo nieuwzględnienia sprzeciwu osoby, której dane dotyczą.

W jednej ze spraw[74] Skarżący złożył skargę na Spółkę, która **wysyłała do niego liczne wiadomości e-mail i SMS o charakterze marketingowym, pomimo że od 2016 roku nie był związany ze Spółką żadną umową.** Skarżący wniósł o usunięcie jego danych osobowych. W toku

[72] Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, t.j. Dz.U. z 2021 r. poz. 534.
[73] ZWAD.440.95.2019.
[74] Decyzja z dnia 2 grudnia 2021 r. sygn. ZSPR.440.1748.2019.

postępowania ustalono, że Spółka pierwotnie przetwarzała dane Skarżącego w celu realizacji umowy, której Skarżący był stroną oraz – w celu marketingu bezpośredniego – zgodnie ze swoim prawnie uzasadnionym interesem. Po wygaśnięciu umowy Spółka dalej przetwarzała jego dane przesyłając wiadomości o charakterze marketingowym informujące o aktualnej ofercie. Kwestionowane zaś przez Skarżącego przetwarzanie miało miejsce kilka lat po rozwiązaniu umowy. Pomiędzy stronami postępowania nie zachodził już żaden rodzaj powiązania i nie było podstaw, w oparciu o które Skarżący mógł spodziewać się przetwarzania jego danych w tych celach przez Spółkę. Przetwarzanie danych osobowych Skarżącego w celach marketingowych po wygaśnięciu umowy łączącej strony, byłoby dopuszczalne jedynie w sytuacji, gdyby Skarżący wyraził na to zgodę. Skarżący takiej zgody jednak nie wyraził.

Przetwarzanie danych osobowych dla celów marketingu bezpośredniego może odbywać się na podstawie zgody podmiotu danych. Rozporządzenie 2016/679 dopuszcza także możliwość prowadzenia marketingu bezpośredniego na podstawie prawnie uzasadnionych interesów administratora. Zgodnie z motywem 47 rozporządzenia 2016/679, cyt.: „Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu”. Prezes UODO uznał za uzasadnione udzielenie Spółce upomnienia w zakresie stwierdzonego naruszenia przepisów art. 6 ust. 1 rozporządzenia 2016/679. Od dnia wygaśnięcia ww. umowy zawartej pomiędzy Spółką a Skarżącym, podmiot ten wysyłając do Skarżącego kwestionowane wiadomości o treści marketingowej, nie posiadał podstawy prawnej. Między stronami nie zachodziło również żadne aktualne powiązanie pozwalające przetwarzać dane osobowe Skarżącego na podstawie uzasadnionego interesu.

W innej ze spraw[75] poruszono często występujące zagadnienie **zlecania akcji marketingowych.** Skarżący złożył skargę na przetwarzanie jego danych osobowych w celach marketingowych, pomimo wniesionego żądania zaprzestania ich przetwarzania w tym celu. Spółka pozyskała dane osobowe bezpośrednio od Skarżącego w związku ze świadczonymi usługami

[75] Decyzja z dnia 8 listopada 2021 r. sygn. ZSPR.440.1216.2018.

serwisowymi i przetwarzała pozyskane dane w celach marketingowych na podstawie udzielonej przez Skarżącego zgody. Wskazana w treści skargi korespondencja elektroniczna o charakterze marketingowym realizowana była przez podmiot trzeci, działający na zlecenie administratora. Choć podmiot ten realizował zleconą przez Spółkę usługę przeprowadzenia akcji marketingowej, to jednak podmiot ten – jako administrator – nie udostępniał podmiotowi trzeciemu żadnych danych osobowych swoich klientów. Realizował wysyłki ofert marketingowych do podmiotów, których dane osobowe zebrał samodzielnie i których sam był administratorem.

Wobec powyższego stwierdzono, że Spółka nie pełniła żadnej roli w procesie przetwarzania danych osobowych Skarżącego w odniesieniu do korespondencji wskazanej w skardze. Korespondencja ta nie była realizowana przez Spółkę. Spółka wypełniła przesłanki legalności przetwarzania danych Skarżącego w celach marketingowych z uwagi na dysponowanie zgodą Skarżącego w tym zakresie. W powyższym zakresie organ nadzorczy nie dopatrzył się zatem nieprawidłowości i odmówił uwzględnienia skargi.

Monitoring

W jednej ze spraw[76] Skarżący podniósł, że teren jego posesji był monitorowany przez kilkanaście kamer należących do jego sąsiada, który nie reaguje na wezwania dotyczące zaprzestania prowadzenia ww. monitoringu.

Ustalono, że zamontowane przez Skarżonego kamery obejmowały swym zasięgiem teren jego posesji, drogę publiczną oraz część posesji należącej do Skarżącego. Skarżony wskazał, że zainstalował monitoring wizyjny w celu zapewnienia bezpieczeństwa oraz ochrony osób i mienia w związku z incydentami sąsiedzkimi oraz że spełnił obowiązek informacyjny wynikający z art. 13[77] ust. 1 i 2 rozporządzenia 2016/679, zamieszczając na elewacji nieruchomości tablicę informacyjną, na której znalazły się: dane administratora, podstawa prawna przetwarzania danych, cel przetwarzania danych osobowych, obszar monitorowany, okres przechowywania nagrań pochodzących z monitoringu, pouczenie o możliwości wniesienia skargi do organu nadzorczego i przysługującym prawie dostępu do danych i ograniczeniu ich przetwarzania. Skarżony wskazał również, że Skarżący nigdy nie zwracał się do niego z wnioskiem o usunięcie jego danych osobowych.

[76] Decyzja z dnia 19 listopada 2021 r. sygn. DS.523.1605.2020.PR.KM.

[77] Zgodnie z art. 13 rozporządzenia 2016/679, jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie przewidziane w niniejszym artykule informacje.

W przedmiotowej sprawie Prezes UODO uwzględnił treść wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 11 grudnia 2014 r. w sprawie C-212/13 František Ryneš przeciwko Úřad pro ochranu osobních údajů Ryneš, zgodnie z którym cyt.: „wykorzystywanie systemu kamer przechowującego zapis obrazu osób na sprzęcie nagrywającym w sposób ciągły, takim jak dysk twardy, zainstalowanego przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, który to system monitoruje również przestrzeń publiczną, nie stanowi przetwarzania danych w trakcie czynności o czysto osobistym lub domowym charakterze", a w takim przypadku proces przetwarzania danych osobowych za pomocą monitoringu wizyjnego podlega normom przepisów prawa o ich ochronie".

Prezes UODO uwzględnił także stanowisko wyrażone przez Europejską Radę Ochrony Danych w wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo[78] i stwierdził, że zasadnym jest przyjęcie, że prawnie uzasadniony interes Skarżonego, o którym mowa w art. 6 ust. 1 lit. f[79] rozporządzenia 2016/679, którym w tym przypadku jest zapewnienie bezpieczeństwa oraz ochrony osób i mienia, ma charakter nadrzędny w stosunku do praw i wolności Skarżącego, także w odniesieniu do prowadzenia monitoringu wizyjnego wykraczającego poza granice nieruchomości Skarżonego, tj. obejmującego drogę publiczną. Prezes UODO zajął powyższe stanowisko ze względu na fakt, iż nagrania, na których utrwalony został wizerunek Skarżącego, ukazujące moment napaści na Skarżonego na drodze publicznej, wykorzystane zostały jako materiał dowodowy w postępowaniu sądowym, zakończonym prawomocnym wyrokiem skazującym. Jednocześnie Prezes UODO wskazał, że opisane przez Skarżonego incydenty sąsiedzkie, w związku z którymi zainstalował monitoring wizyjny, miały miejsce na terenie jego posesji oraz w miejscu publicznym, natomiast nie dochodziło do nich na prywatnej posesji Skarżącego. Skarżony nie wykazał zatem legalnej przesłanki uprawniającej go do przetwarzania danych osobowych Skarżącego pochodzących z nagrań monitoringu wizyjnego obejmującego swoim zasięgiem część należącej do Skarżącego nieruchomości.

[78] Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo przyjęte zostały 29 stycznia 2020 r.

[79] 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.

W związku z powyższym Prezes UODO nakazał[80] zaprzestania przetwarzania danych osobowych Skarżącego pochodzących z nagrań z monitoringu wizyjnego obejmującego swoim zasięgiem należącą do niego nieruchomość. W odniesieniu do kwestii realizacji obowiązku informacyjnego Prezes UODO stwierdził, że Skarżony nie zrealizował w pełni obowiązku informacyjnego określonego w art. 13 ust. 2 lit. b rozporządzenia 2016/679, tj. nie poinformował Skarżącego o przysługującym mu prawie żądania usunięcia danych oraz wniesienia sprzeciwu wobec ich przetwarzania. Prezes UODO nakazał zatem Skarżonemu dostosowanie[81] operacji przetwarzania do przepisów rozporządzenia 2016/679 w tym zakresie. Prezes UODO stwierdził jednocześnie, że nie ma podstaw do zastosowania art. 58 ust. 2 rozporządzenia 2016/679 w związku z monitoringiem wizyjnym obejmującym swoim zasięgiem część drogi publicznej.

Internet, media społecznościowe

Kolejna sprawa[82] dotyczyła **wtyczki zamieszczonej przez administratora strony internetowej**, na którą wszedł Skarżący. Jego zdaniem podmiot Skarżony udostępnił bez zgody: część jego historii przeglądania stron internetowych, adres IP jego urządzenia oraz sztucznie nadane ID w cookie podmiotowi trzeciemu, tj. administratorowi serwisu społecznościowego Twitter. Skarżący zażądał usunięcia jego danych osobowych. Podmiot Skarżony wskazał natomiast, że nie pozyskał żadnych danych osobowych Skarżącego, nie pobierał jego adresu IP, historii przeglądania czy ID pliku cookie, a adres IP Skarżącego został automatycznie pobrany przez widget firmy Twitter znajdujący się na prowadzonej przez podmiot Skarżony stronie internetowej.

W przedmiotowej sytuacji Prezes UODO wskazał – powołując się na wyrok[83] Naczelnego Sądu Administracyjnego – że informacje, które wiążą się z określoną osobą – choćby pośrednio – niosą pewien komunikat o niej. Dlatego też informacją dotyczącą osoby będzie zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, z których korzysta. Poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio będą stanowiły one informację także o niej samej. Adres IP (Internet Protocol Address) jest unikatowym numerem przyporządkowanym urządzeniom sieci komputerowych. Jest zatem

[80] Zgodnie z art. 58 ust. 2 lit. c każdemu organowi nadzorczemu przysługuje uprawnienie naprawcze: nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia.
[81] Zgodnie z art. 58 ust. 2 lit. d rozporządzenia 2016/679, każdemu organowi nadzorczemu przysługuje uprawnienie naprawcze: nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu.
[82] Decyzja z dnia 20 kwietnia 2021 r. sygn. DS.523.5776.2020.PR.KM.
[83] Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r. sygn. akt I OSK 1079/10.

informacją dotyczącą komputera, a nie konkretnej osoby fizycznej, zwłaszcza wtedy, gdy możliwe jest użyczenie jednego adresu IP wielu użytkownikom w ramach sieci lokalnej. Tam, gdzie adres IP jest na dłuższy okres lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że jest on daną osobową. Jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej.

Prezes UODO powołał się również na wyrok[84] Trybunału Sprawiedliwości Unii Europejskiej, w którym stwierdzono, że poprzez umieszczenie wtyczki społecznościowej (w przypadku omawianego wyroku – przycisku „Lubię to" Facebooka) w swojej witrynie internetowej, administrator w decydujący sposób wpływa na gromadzenie i przekazywanie danych osobowych osób odwiedzających wspomnianą witrynę na rzecz dostawcy wspomnianej wtyczki. Samo zamieszczenie wtyczki umożliwia bowiem uzyskiwanie danych osób odwiedzających stronę internetową administratora przez dostawcę wtyczki bez względu na to, czy są one członkami serwisu społecznościowego, którego wtyczkę zamieszczono, czy w tę wtyczkę kliknęły lub też czy wiedziały o takiej operacji. W wyroku tym jasno wskazano, że niezależnie od tego, czy administrator strony internetowej ma dostęp do danych osobowych gromadzonych i przekazanych dostawcy wtyczki społecznościowej czy nie, nie stoi to na przeszkodzie, by przysługiwał mu przymiot administratora danych.

Prezes UODO uznał Skarżonego za administratora danych. Za pośrednictwem swojej strony internetowej ujawnił on dane osobowe Skarżącego poprzez ich transmisję do dostawcy wtyczki, tj. administratora serwisu Twitter. Wobec powyższego Prezes UODO wydał decyzję upominającą[85] w zakresie udostępnienia danych osobowych Skarżącego podmiotowi trzeciemu bez podstawy prawnej. Uznał też, że nakazanie usunięcia danych osobowych Skarżącego nie jest konieczne, ponieważ nie przetwarza on danych, które mogą być usunięte. Jak ustalono, dane osobowe Skarżącego przetwarzane były wyłącznie w czasie, kiedy odwiedzał on stronę internetową.

W kolejnej sprawie[86] Prezes UODO rozstrzygał **kwestię przetwarzania danych osobowych Skarżącej w zakresie imienia, wizerunku jej i innych członków rodziny, prywatnej korespondencji, nazwy zamieszkiwanej przez nią miejscowości oraz dojazdu do jej**

[84] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 29 lipca 2019 r. C-40/17 Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV.

[85] Zgodnie z art. 58 ust. 2 lit. b rozporządzenia 2016/679 każdemu organowi nadzorczemu przysługuje uprawnienie naprawcze: udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania.

[86] Decyzja z dnia 30 lipca 2021 r. sygn. ZSPR.440.1443.2019.PR.MSO.

nieruchomości, opublikowanych w materiale wideo zamieszczonym w serwisie YouTube. Powagi całej sprawie dodawał fakt, że opublikowany materiał dotyczył śmierci człowieka i sugerował, iż Skarżąca mogła dokonać jego zabójstwa.

W sprawie tej brak było odpowiedzi serwisu YouTube na korespondencję od Prezesa UODO, wobec czego wydana decyzja w tej sprawie opierała się na materiale dowodowym zebranym w formie oświadczenia Skarżącej zawartego w jej skardze, pisma uzupełniającego oraz na przedstawionych przez nią dowodach. W ocenie Prezesa UODO zakres informacji dotyczących Skarżącej umożliwiał jej zidentyfikowanie chociażby przez mieszkańców miejscowości, w której Skarżąca mieszkała, bez ponoszenia przez nich nadmiernych kosztów i czasu. Pozostałe informacje, jak wizerunek jej i członków jej rodziny, zostały w ww. materiale zanonimizowane. Prezes UODO uznał, że przetwarzanie danych osobowych Skarżącej nie znajduje prawnego uzasadnienia w przepisach rozporządzenia 2016/679 w związku z czym doszło do naruszenia art. 6 ust. 1[87] i 17 ust. 1[88] rozporządzenia 2016/679.

Prezes UODO wydał decyzję nakazującą usunięcie danych osobowych Skarżącej z materiału wideo zamieszczonego w serwisie YouTube. W związku z żądaniem Skarżącej dotyczącym nałożenia na skarżony podmiot kary finansowej, Prezes UODO wskazał, że organ nie podejmuje tego rodzaju działań na żądanie osoby składającej skargę.

Kolejna ze spraw dotyczyła posłużenia się danymi osobowymi Skarżącego w zakresie imienia i inicjału nazwiska w odpowiedziach na opinie wystawione przez użytkowników jednej ze stron internetowych – w kontekście opinii zamieszczonej tam także przez Skarżącego[89].

Jak ustalono, w ramach prowadzonej działalności gospodarczej pozyskiwane były dane osobowe Skarżącego, w związku z zawarciem z nim umowy o świadczenie usługi w postaci kursu języka obcego. Skarżący zamieścił negatywny komentarz na temat działalności osoby Skarżonej na stronie opinii Google. Prezes UODO wskazał, że Skarżona, jako administrator danych, nie może posłużyć się informacjami pozyskanymi w ramach realizacji umowy w innym celu niż ten, do którego zostały zebrane, w sytuacji kiedy nie ma ku temu podstawy prawnej, i wydał decyzję powołując się

[87] Zgodnie z art. 6 ust. 1 rozporządzenia 2016/679 przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z przewidzianych w tym artykule warunków.

[88] 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.

[89] Decyzja z dnia 23 września 2021 r. sygn. ZSZZS.440.202.2019.PR.AKR.

m.in. na art. 4 pkt. 1[90] rozporządzenia 2016/679. Skarżący podniósł, że jego dane osobowe (imię i inicjał nazwiska) zamieszczone zostały tuż nad wystawioną przez niego opinią, gdzie podpisany był pełnym imieniem i nazwiskiem. Zależność tę wyraźnie widać podczas sortowania opinii od najnowszych. Prezes UODO uznał, że w powyższych okolicznościach informacje w zakresie imienia i inicjału nazwiska, w połączeniu z zamieszczoną na stronie opinią Skarżącego, należy uznać za dane osobowe ze względu na możliwość łatwego zidentyfikowania podmiotu danych.

W opinii Prezesa UODO doszło do naruszenia art. 5 ust. 1 lit. b[91] w zw. z art. 6 ust. 1 rozporządzenia 2016/679. W związku z powyższym nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 poprzez usunięcie danych osobowych Skarżącego w zakresie imienia i inicjału nazwiska z odpowiedzi na opinie wystawione przez użytkowników na jednej ze stron internetowych.

4.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa

Spośród **8318 skarg,** które w 2021 r. wpłynęły do Urzędu, **1445** z nich dotyczyło podmiotów działających w obszarze zdrowia, zatrudnienia i szkolnictwa. Poniżej omówione zostały przykłady kilku takich skarg.

Przetwarzanie danych osobowych w sektorze zdrowia

Częstymi skargami, które w 2021 roku, jak i w latach ubiegłych, wpłynęły do Prezesa Urzędu Ochrony Danych Osobowych, były skargi na uzyskiwanie przez lekarzy dostępu do danych osobowych Skarżących przetwarzanych w systemach ZUS. Jedna z takich spraw dotyczyła **wykorzystania bez wiedzy osoby dotyczących jej danych osobowych do wystawienia recepty oraz udostępnienia tych danych w przedmiotowej recepcie pracownikowi apteki.**

Osoba Skarżąca udała się do apteki nie posiadając wystawionej recepty, z prośbą o sprzedanie jej przyjmowanych na stałe leków potrzebnych do codziennego funkcjonowania. Zobowiązała się

[90] Zgodnie z art. art. 4 pkt. 1 rozporządzenia 2016/679 „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.

[91] Zgodnie z art. 5 ust. 1 lit. b rozporządzenia 2016/679 dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu").

niezwłocznie dostarczyć receptę w późniejszym terminie, czego jednak nie uczyniła. Osoba ta była pacjentką Przychodni, która przetwarzała jej dane osobowe w celu świadczenia na jej rzecz usług medycznych. Pracownik apteki nie uzyskał od Skarżącej recepty na sprzedane leki, więc zwrócił się bezpośrednio do Przychodni o wystawienie recepty na konkretne leki na nazwisko Skarżącej. Lekarz świadczący usługi w Przychodni posłużył się danymi osobowymi Skarżącej w celu wpisania w dokumentacji medycznej teleporady, która się faktycznie nie odbyła oraz wystawienia recepty, którą następnie przekazał pracownikowi apteki. Przychodnia oświadczyła, że działanie to wynikało z troski o Skarżącą, której wydano leki zażywane przez nią na stałe, a jedynym celem takiego działania – pomoc pacjentowi.

Dokonując oceny legalności wskazanych procesów przetwarzania danych osobowych Skarżącej przez Przychodnię, organ stwierdził, że Przychodnia nie dopełniła obowiązków, które ciążą na niej jako administratorze. Umożliwiła bowiem dostęp do danych osobowych Skarżącej osobom nieuprawnionym. Przychodnia we wskazanych procesach przetwarzania nie spełniła żadnej z przesłanek określonych w art. 9 ust. 2 RODO, co stanowiło naruszenie art. 9 ust. 1 RODO, a także art. 5 ust. 1 lit. a RODO. Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b RODO, Prezes Urzędu Ochrony Danych Osobowych udzielił Przychodni upomnienia za naruszenie art. 5 ust. 1 lit. a oraz art. 9 ust. 1 i 2 RODO poprzez bezprawne przetwarzanie danych osoby Skarżącej w celu wystawienia recepty i bezprawne udostępnienie danych osobowych zawartych w przedmiotowej recepcie na rzecz pracownika apteki.

Omyłkowe udostępnienie danych osobowych pacjenta na rzecz nieuprawnionej osoby trzeciej w związku z błędnie wystawioną receptą było tematem innej skargi z tego obszaru.

Skarżąca logując się na swoje internetowe konto pacjenta zwróciła uwagę, że na jej dane osobowe została wystawiona recepta, choć nie korzystała tego dnia z usług medycznych administratora. Ustalono, że dane osobowe Skarżącej zawarte na recepcie zostały ujawnione na rzecz nieuprawnionej osoby trzeciej przez pracownika, który przez pomyłkę wystawił przedmiotową receptę dla innej osoby. Dokonując oceny legalności przetwarzania danych osobowych Skarżącej przez podmiot medyczny organ ustalił, że w omawianej sprawie doszło do naruszenia ochrony danych osobowych Skarżącej. Administrator danych osobowych nie legitymizował się żadną z przesłanek określonych w art. 6 ust. 1 RODO, uprawniających go do udostępnienia danych tej osoby. Prezes Urzędu uznał również, że przedmiotowe zdarzenie naruszyło zasadę określoną w art. 5 ust. 1 lit. c RODO, który nakazuje, by przetwarzane dane – zgodnie z zasadą minimalizacji danych

– były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

W związku ze stwierdzonym naruszeniem Prezes Urzędu, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b RODO, udzielił administratorowi upomnienia za naruszenie art. 5 ust. 1 lit. c oraz art. 6 ust. 1 RODO.

Odmowa nakazania usunięcia danych osobowych, pozyskanych w celu realizacji świadczeń opieki zdrowotnej przez podmiot medyczny, to kolejny przykład skargi z sektora zdrowia[92].

Osoba Skarżąca, jako pacjent korzystający z usług medycznych podmiotu medycznego, zarejestrowała się na wizytę specjalistyczną. Zaplanowane świadczenie zdrowotne nie zostało jednak zrealizowane w wyniku złożonego przez osobę Skarżącą wniosku o usunięcie jej danych osobowych i rezygnacją z dalszego świadczenia wobec niej usług medycznych przez podmiot medyczny.

Z kolei podmiot medyczny oświadczył, że odmówił spełnienia ww. wniosku Skarżącej, z uwagi na to, że spoczywa na nim – jako administratorze danych osobowych – obowiązek prawny wynikający z art. 6 ust. 1 lit. c, art. 9 ust. 2 lit. h oraz lit. i RODO oraz art. 25 oraz art. 29 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[93], polegający na przetwarzaniu danych osobowych pacjentów również w sytuacji, gdy ostatecznie nie dojdzie do realizacji umówionego świadczenia zdrowotnego.

W sprawie tej organ stwierdził, że podmiot prowadzący działalność leczniczą zgodnie z art. 3 ust. 1 i 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[94], jest uprawniony do przetwarzania danych osobowych w zakresie niezbędnym do udzielenia świadczeń zdrowotnych. W kwestii rejestracji Skarżącej na wizytę – zgodnie z art. 20 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[95] – świadczeniodawca zobowiązany jest prowadzić listy oczekujących na świadczenia, które stanowią część harmonogramu przyjęć. Zgodnie z art. 19a ust. 6 przywołanej ustawy, harmonogram przyjęć stanowi integralną część dokumentacji medycznej prowadzonej przez świadczeniodawcę. Zakres danych zawartych na liście oczekujących na świadczenia, zgodnie z art. 20 ust. 2 pkt 3 i 4 ww. ustawy, obejmuje wyszczególnione w tym przepisie dane. Zakres danych niezbędnych przy rejestracji i prowadzeniu listy oczekujących oraz zasady przetwarzania danych, w tym skreślenia z listy oczekujących,

[92] DS.523.1020.2020.
[93] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Dz. U. z 2020 r. poz. 849.
[94] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, Dz. U. z 2021 r. poz. 711.
[95] Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Dz. U z 2021 r. poz. 1285.

szczegółowo określa również rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2019 r. w sprawie zakresu niezbędnych informacji przetwarzanych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych[96].

Prezes Urzędu zwrócił również uwagę, że zgodnie art. 24 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w przedmiotowej ustawie oraz w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[97]. Zgodnie z art. 29 ust. 1 przywołanej ustawy, podmiot udzielający świadczeń zdrowotnych przechowuje dokumentację medyczną przez okres dwudziestu lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem sytuacji w tym przepisie opisanych, tj. m.in. skierowań na badania lub zleceń lekarza, które są przechowywane przez okres: a) pięciu lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza, b) dwóch lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku, gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie.

Tym samym, organ stwierdził, że aktualne przetwarzanie danych osobowych Skarżącej przez administratora było uzasadnione art. 6 ust. 1 lit. c, art. 9 ust. 2 lit. h oraz lit. i RODO w związku z art. 25 i art. 29 ustawy z dnia 6 listopada 2008 r. ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

Przetwarzanie danych osobowych w sektorze zatrudnienia

Sprawy z sektora zatrudnienia, które rozpatrywał w 2021 r. Prezes Urzędu Ochrony Danych Osobowych, dotyczyły bardzo różnorodnych zagadnień, a same postępowania często były wielowątkowe. Spośród przeprowadzonych postępowań na uwagę zasługują m.in. te, których przedmiot dotyczył przedstawionych poniżej przykładów kilku skarg.

Ujawnienie przez pracodawcę informacji o pozytywnym wyniku testu na COVID-19 pracownika na rzecz pozostałych współpracowników[98]

Pracodawca za pomocą wiadomości e-mail rozesłał wśród swoich pracowników informację, że pracownik o konkretnym imieniu i nazwisku uzyskał pozytywny wynik testu na COVID-19. Wyjaśnił

[96] Dz. U. z 2019 poz. 1207
[97] Dz. U. z 2016 r. poz. 1535 z późn. zm.
[98] DS.523.1627.2021

przy tym, że działanie takie było konieczne z uwagi na zapewnienie bezpiecznych i higienicznych warunków pracy w zakładzie pracy oraz w celu weryfikacji przez pracowników i współpracowników, czy mieli bezpośredni kontakt z osobą Skarżącą. Pracodawca wskazał, że wszyscy pracownicy i współpracownicy pracują w tzw. open space, nie posiadają osobnych pomieszczeń do wykonywania powierzonych im obowiązków, zaś Skarżący poruszał się między piętrami biura i korzystał z pomieszczeń wspólnych.

Pracodawca, przed skierowaniem wiadomości mailowej do pracowników z informacją o pozytywnym wyniku testu na COVID-19 osoby Skarżącej, ustalił już osoby mogące mieć z nią bezpośredni kontakt i zgłosił je do Sanepidu. Wbrew twierdzeniom Pracodawcy z treści wysłanej wiadomości e-mail nie wynikało, aby Pracodawca poszukiwał innych osób, które miały kontakt z osobą Skarżącą w okresie poprzedzającym otrzymanie przez nią pozytywnego wyniku testu na COVID-19, a jedynie informował pracowników o zachorowaniu (pozytywnym wyniku testu osoby Skarżącej), podjętych działaniach i konieczności zachowania odpowiednich środków ostrożności.

Prezes UODO wskazał, że w celu poinformowania o konieczności zachowania odpowiednich środków bezpieczeństwa w związku z pandemią COVID-19, nie było niezbędne wskazanie danych osobowych Skarżącego jako osoby, która otrzymała pozytywny wynik testu na COVID-19. W ocenie Prezesa UODO, udostępnienie przez Pracodawcę informacji o pozytywnym wyniku testu uzyskanym przez Skarżącego nie miało oparcia w żadnej z przesłanek legalizujących przetwarzanie danych szczególnej kategorii zawartych w art. 9 ust. 2 RODO, a tym samym nastąpiło z naruszeniem art. 9 ust. 1 RODO oraz zasad zawartych art. 5 ust. 1 lit. a i lit. c RODO.

Udostępnienie przez pracodawcę danych osobowych pracownika w zakresie informacji o stanie zdrowia psychicznego na rzecz lekarza medycyny pracy[99]

Sprawa dotyczyła udostępnienia przez Pracodawcę danych wrażliwych Skarżącej, w zakresie informacji, że leczy się ona psychiatrycznie, lekarzowi medycyny pracy. Pracodawca po powrocie Skarżącej z urlopu rodzicielskiego i zwolnienia lekarskiego skierował ją na kontrolne badania lekarskie celem zweryfikowania, czy nie istnieją przeciwskazania do dalszego jej zatrudniania. Oprócz wystawienia skierowania na badania kontrolne, Pracodawca przekazał do lekarza medycyny pracy pismo, w którym poinformował, że Skarżąca leczyła się psychiatrycznie. Wskazał w nim jednocześnie na zachowania, które dyskwalifikują ją jako pracownika na zajmowanym dotychczas

[99] ZSZZS.440.1161.2019.

stanowisku oraz zawnioskował o niedopuszczenie jej do pracy. Pracodawca załączył jednocześnie do tego pisma zaświadczenie o niezdolności do pracy Skarżącej wystawione przez lekarza psychiatrę.

Pracodawca wskazał, że w okresie zatrudnienia osoba Skarżąca – pracując na stanowisku spedytora, które wymaga skupienia, spokoju i koncentracji uwagi – zaczęła zachowywać się w sposób nieodpowiedzialny i niejako nieadekwatny w stosunku do sytuacji. Pracodawca wyjaśnił również, że zachowanie Skarżącej, w korelacji z przedkładanymi zaświadczeniami lekarskimi, których wystawcą był lekarz psychiatra, wzbudziło u niego uzasadnione podejrzenie, że zasadnym wydaje się, aby przy przeprowadzaniu badań kontrolnych lekarz medycyny pracy rozszerzył zakres badania o dodatkowe specjalistyczne badania konsultacyjne i badania dodatkowe. Pracodawca wyjaśnił, że jego intencją było uzyskanie informacji, czy dotychczasowy stan zdrowia pozwala pracownikowi na dalsze zatrudnienie na dotychczasowym stanowisku pracy. Jako podstawę prawną udostępnienia danych osobowych w zakresie informacji o stanie zdrowia psychicznego osoby Skarżącej wskazał art. 111 w zw. z art. 1832, art. 207 § 2, art. 212 pkt 6 Kodeksu pracy[100], a także § 2 ust. 2 rozporządzenia Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r. w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy[101] oraz załącznik nr 1 do tego rozporządzenia, zawierający wskazówki metodyczne w sprawie przeprowadzania badań profilaktycznych pracowników, a dokładnie pkt V tabeli, w którym zawarte zostały zalecenia dla lekarza medycyny pracy, celem sprawdzenia stanu psychicznego pracownika przed wydaniem stosownej treści orzeczenia. Jako podstawę prawną Pracodawca wskazał również art. 9 ust. 1 i 2 lit. b oraz lit. h RODO.

Prezes Urzędu nie podzielił stanowiska Pracodawcy. Uznał, że Pracodawca, stosownie do treści art. 229 Kodeksu pracy, zobowiązany był jedynie do wystawienia osobie, której dane dotyczą, skierowania na badania kontrolne zgodnie z wzorem określonym w załączniku nr 3a ww. rozporządzenia. Wypełniając skierowanie na badania lekarskie mógł określić, zgodnie z treścią załącznika nr 1 rozporządzenia, jakie badanie profilaktyczne powinno zostać przeprowadzone i w jakim zakresie. Natomiast decyzję o tym, jakim badaniom specjalistycznym będzie podlegała osoba kierowana na badania profilaktyczne, podejmuje wyłącznie lekarz medycyny pracy, wykorzystując do tego celu określone w załączniku nr 1 rozporządzenia „Wskazówki metodyczne w sprawie przeprowadzania badań profilaktycznych pracowników". Prezes Urzędu wskazał również

[100] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, t.j. Dz. U. z 2020 r. poz. 1320 z późn. zm.
[101] Dz. U. z 2016 r. poz. 2067.

na wyrażony przez doktrynę pogląd, zgodnie z którym „o ile pracodawca przesądza o rodzaju badania profilaktycznego, to nie decyduje on o zakresie badań medycznych łączących się z tym badaniem, bo to należy do prerogatyw lekarza profilaktyka”[102]. Lekarz medycyny pracy w oparciu o rozmowę z pracownikiem, przeprowadzoną w trakcie badania, może zdecydować o ewentualnym rozszerzeniu zakresu badań, które mogą wynikać z konieczności potwierdzenia lub negacji potwierdzenia schorzenia. Wskazówki zawarte w załączniku nr 1 do rozporządzenia stanowią wytyczne dla lekarza, który samodzielnie podejmuje decyzję o zakresie i częstotliwości badania.

Prezes Urzędu stwierdził, że udostępnienie przez Pracodawcę lekarzowi medycyny pracy informacji, że Skarżąca leczy się psychiatrycznie, nie znajdowało uzasadnienia w przepisach obowiązującego prawa, nie tylko w zakresie praw pracowniczych wynikających z Kodeksu pracy czy rozporządzenia, ale przede wszystkim z przepisów kształtujących zasady i legalność przetwarzania danych osobowych określonych w RODO. Informacje przekazane przez pracodawcę lekarzowi medycyny pracy stanowiły – zgodnie z art. 9 ust. 1 RODO – szczególną kategorię danych, których legalności przetwarzania, w oparciu o przesłanki legalizujące wskazane w art. 9 ust. 2 RODO, przeprowadzone postępowanie nie wykazało. W związku z powyższym Prezes UODO udzielił Pracodawcy upomnienia za naruszenie art. 9 ust. 2 RODO, polegające na udostępnieniu danych osobowych Skarżącej dotyczących zdrowia bez podstawy prawnej.

Przetwarzanie danych osobowych pracownika przez pracodawcę za pośrednictwem kamery monitoringu wizyjnego ukrytej w miejscu pracy[103]

Pracodawca, z uwagi na kradzieże drogiego alkoholu, do których dochodziło w zakładzie pracy, bez wiedzy pracowników zainstalował w magazynie kamerę, celem wykrycia sprawców.

Prezes Urzędu, biorąc pod uwagę art. 6 i art. 13 RODO oraz art. 22^2 Kodeksu pracy, określający warunki, które musi spełnić pracodawca, aby wprowadzić w zakładzie pracy monitoring wizyjny i legalnie przetwarzać dane osobowe za pośrednictwem tego narzędzia, nie uznał argumentacji Pracodawcy odnośnie podstaw przetwarzania danych osobowych pracownika z wykorzystaniem ukrytej kamery i rozstrzygnął, że działanie Pracodawcy stanowiło naruszenie ochrony danych osobowych. Prezes Urzędu zwrócił w szczególności uwagę na art. 22^2 § 9 Kodeksu pracy, który

[102] K.W. Baran, Komentarz do rozporządzenia w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy. [w:] Prawo pracy. Rozporządzenia. Komentarz. Wolters Kluwer Polska, 2020.
[103] DS.440.330.2019.

obliguje Pracodawcę do niezwłocznego oznaczenia pomieszczeń i terenu monitorowanego w przypadku wprowadzenia monitoringu wizyjnego w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych. W związku ze stwierdzonymi nieprawidłowościami, Prezes Urzędu nakazał Pracodawcy usunięcie nielegalnie zgromadzonych za pośrednictwem ukrytej kamery danych osobowych Skarżącego.

Udostępnienie przez pracodawcę (dyrektora szkoły) informacji o przynależności pracownika (nauczyciela) do organizacji związkowej podczas posiedzeń rady pedagogicznej szkoły[104]

Przedmiotem sprawy było dwukrotne udostępnienie przez administratora – Dyrektora szkoły – będącego jednocześnie pracodawcą Skarżącej, jej danych osobowych w zakresie imienia, nazwiska oraz informacji o przynależności do organizacji związkowej, podczas posiedzeń rady pedagogicznej szkoły.

Organ właściwy do spraw ochrony danych osobowych negatywnie ocenił działania administratora, który stał na stanowisku, że podstawa prawna takiego przetwarzania opierała się na art. 6 ust. 1 lit. c RODO i art. 9 ust. 2 lit. b RODO w zw. z art. 70 ust. 2 Ustawy prawo oświatowe[105] i § 17 ust 3 rozporządzenia Ministra Edukacji Narodowej z dnia 28 lutego 2019 r. w sprawie szczegółowej organizacji publicznych szkół i publicznych przedszkoli[106]. Administrator wyjaśnił, że ujawnienie na posiedzeniu rady pedagogicznej danych osobowych w kwestionowanym przez osobę Skarżącą zakresie, było przejawem wykonywania przez niego swoich obowiązków i było niezbędne w sytuacji sporządzania arkusza organizacyjnego pracy szkoły i jego aneksów, która to czynność wymagała zaopiniowania przez radę pedagogiczną. Tłumaczył również, że pozyskał dane osobowe nie ze swojej inicjatywy, tylko związku zawodowego, który przedłożył Dyrektorowi szkoły uchwałę dotyczącą osób objętych ochroną i w ten sposób pozyskał dane osobowe Skarżącej należące do szczególnych kategorii. Od momentu pozyskania wiedzy o osobach posiadających prawo do ochrony pracy był zobligowany do podjęcia działań zapewniających przestrzeganie praw tym osobom przysługujących. Zdaniem administratora, na dyrektorze ciążył obowiązek wyjaśnienia wszystkim członkom rady pedagogicznej obiektywnych przyczyn ograniczeń wymiaru zatrudnienia bądź rozwiązania stosunku pracy z poszczególnymi pracownikami. Niewyjaśnienie tych okoliczności stanowiłoby powód kierowania przez pozostałych nauczycieli wobec niego zarzutów braku obiektywizmu przy podejmowaniu decyzji w zakresie zatrudnienia. Dyrektor wskazał, że do jego

[104] ZSZZS.440.746.2019.
[105] Ustawa z 14 grudnia 2016 r. - Prawo oświatowe, Dz.U. z 2021 r. poz. 182.
[106] Dz.U. z 2019 r. poz. 502.

obowiązków należy poinformowanie uczestników posiedzenia rady pedagogicznej, dlaczego dany pracownik otrzymał określone godziny pracy w miejsce innego pracownika, a wobec tego konieczne było wskazanie pracowników objętych ochroną. Dyrektor jako podstawy prawne swoich obowiązków wskazał art. 70 ust. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe i § 17 ust. 3 ww. rozporządzenia.

Organ nie podzielił stanowiska administratora. Dokonał analizy ww. przepisów, na które ten się powołał, które jednak nie pozwoliły organowi nadzorczemu na uznanie, iż stanowiły one podstawę do zgodnego z prawem przetwarzania danych osobowych Skarżącej w kwestionowany przez nią sposób. Rada pedagogiczna w zakresie uprawnień, na które powołał się Dyrektor szkoły, nie posiada prawa do opiniowania jego stanowiska co do wskazania osób, którym zamierza wypowiedzieć stosunek pracy. Równocześnie w przywołanych przepisach brak było takiego, który obligowałby radę pedagogiczną do posiadania wiedzy, co do których osób (nauczycieli), Dyrektor szkoły ma ograniczone możliwości rozwiązania stosunku pracy ze względu na szczególną ich ochronę. Organ nadzorczy dokonał również analizy przepisów szczególnych dotyczących arkusza organizacji szkoły i przedszkola, tj. art. 110 Prawa oświatowego. Z ust. 3 przywołanego przepisu wynika, że to nie dyrektor szkoły, tylko organ prowadzący – np. powiat – przedkłada radzie pedagogicznej arkusz organizacji szkoły do zatwierdzenia. Wobec czego wyjaśnienia Dyrektora szkoły, iż był on zobligowany do takiego działania, nie znajdowały podstaw w obowiązujących przepisach. Dopiero z ust. 4 przywołanego przepisu, na podstawie zatwierdzonego arkusza organizacji szkoły, dyrektor szkoły – z uwzględnieniem zasad ochrony zdrowia i higieny pracy – ustala tygodniowy rozkład zajęć określający organizację zajęć edukacyjnych.

Wobec powyższych ustaleń organ nadzorczy uznał, że administrator naruszył przepisy o ochronie danych osobowych, tj. art. 5 ust. 1 lit. b w zw. z art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. b RODO i upomniał za to naruszenie. Przetwarzanie danych osobowych Skarżącej polegające na udostępnieniu jej danych osobowych w zakresie imienia i nazwiska oraz informacji o podleganiu szczególnej ochronie trwałości stosunku pracy nastąpiło bez podstawy prawnej.

Przetwarzanie danych osobowych przez komendę policji oraz organ prowadzący szkołę

Przedmiotem postępowania prowadzonego przez organ właściwy w sprawie ochrony danych osobowych były zgłoszone skargą nieprawidłowości w przetwarzaniu danych osobowych Skarżących przez Komendanta Policji oraz Prezydenta Miasta.

W związku z interwencją policji w jednej ze szkół Prezydent Miasta – jako organ prowadzący szkołę – wszczął postępowanie kontrolne w zakresie prawidłowości działań podjętych przez Skarżącą

będącą dyrektorem szkoły oraz odnośnie do zatrudnienia w niej Skarżącego, do czego – na mocy obowiązujących przepisów – miał prawo. Nie miał jednak uprawnień do przetwarzania danych Skarżącego w zakresie skazań. Zarówno przepisy Prawa oświatowego[107], jak i Karty Nauczyciela[108], nie uprawniają dyrektora szkoły do żądania od pracowników innych niż nauczyciele, przedstawienia informacji o karalności, a więc tym bardziej takich uprawnień nie miał Prezydent, nawet prowadząc działania mające na celu kontrolę pracy dyrektora. Zgodnie z art. 10 RODO, przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 RODO, wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Prezydent, przetwarzając dane osobowe Skarżącego, nie legitymował się podstawą prawną wynikającą z prawa Unii lub prawa krajowego ani nie dokonywał tego pod nadzorem odpowiednich władz publicznych. Tym samym naruszył zasadę legalności, o której mowa w art. 5 ust. 1 lit. a RODO. Zasadę zgodności z prawem Prezydent naruszył także w związku z czynnościami dokonanymi przez jego zastępcę na spotkaniu dotyczącym zaistniałej sytuacji, na którym zastępca odczytał skierowane do niego wyjaśnienia Skarżącej oraz notatkę służbową policji, a także zapoznał zebranych z informacjami o Skarżącym dotyczącymi skazań. Ustalono też, że zastępca Prezydenta Miasta kierował do Skarżącej korespondencję służbową zawierającą m.in. informacje na temat jej zdrowia, na skrzynkę elektroniczną e-mail, do której dostęp mieli, oprócz Skarżącej, również pracownicy szkolnej administracji. Zgodnie z art. 9 ust. 1 RODO, dane dotyczące zdrowia należą do danych osobowych szczególnych kategorii, których przetwarzanie dopuszczone jest tylko w wyjątkowych sytuacjach, wskazanych w art. 9 ust. 2 RODO. Prezydent – jako wykonujący czynności w sprawach z zakresu prawa pracy wobec Skarżącej – posiadał wprawdzie podstawę prawną do przetwarzania informacji o jej zdrowiu w związku z jej niezdolnością do pracy, jednak jego obowiązkiem jako administratora było zapewnienie, by nie miały do nich dostępu osoby nieuprawnione. Prezes UODO ustalił także, że zaniechania Prezydenta w zakresie wprowadzonych procedur i środków w celu utrzymania integralności i dostępności do danych osobowych, choćby poprzez tworzenie kopii zapasowych zawartości służbowych kont pocztowych, stanowiły naruszenie zasady przetwarzania, o której mowa w art. 5 ust. 1 lit. f RODO. Komendant policji działał niezgodnie z prawem. Nie miał bowiem podstawy prawnej do udostępnienia Prezydentowi danych osobowych

[107] Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe, t.j. Dz. U. z 2021 r. poz. 1082.
[108] Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela , t.j. Dz. U. z 2021 r. poz. 1762.

dotyczących skazań Skarżącego. Prezydent w piśmie do Komendanta nie podał ani dokładnego celu, w jakim miałyby być przekazane te informacje, ani przepisu, który wskazywałby na prawo Prezydenta do ich przetwarzania. Podstawy do tak szerokiego udostępnienia danych nie dawał także wskazany przez Komendanta art. 11 ust. 1 ustawy o Policji[109], który stanowi, że wójt (burmistrz, prezydent miasta) lub starosta może żądać od właściwego komendanta policji przywrócenia stanu zgodnego z porządkiem prawnym lub podjęcia działań zapobiegających naruszeniu prawa, a także zmierzających do usunięcia zagrożenia bezpieczeństwa i porządku publicznego. Komendant zobowiązany jest do przetwarzania danych osobowych wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 13 ust. 1 DODO[110]), a ich przetwarzanie w innych celach niż określone w art. 1 pkt 1 ww. ustawy dopuszczalne jest, jeżeli przepisy prawa na to zezwalają (art. 13 ust. 3 DODO). W omawianej sytuacji nie istniały regulacje umożliwiające udostępnienie Prezydentowi danych osobowych Skarżącego.

Prezes UODO w swojej decyzji[111] udzielił upomnienia Prezydentowi Miasta za naruszenie przepisów RODO polegające na niezgodnym z prawem przetwarzaniu danych osobowych Skarżącego dotyczących popełnionych przez niego czynów zabronionych oraz udostępnieniu tych danych na spotkaniu z rodzicami i pracownikami urzędu miasta, a także naruszeniu zasady poufności poprzez przesłanie danych osobowych Skarżącej dotyczących stanu jej zdrowia na ogólnodostępną skrzynkę odbiorczą poczty elektronicznej szkoły oraz niezapewnieniu procedur i środków w celu utrzymania integralności i dostępności danych osobowych zawartych na służbowym koncie poczty elektronicznej wiceprezydenta miasta. Organ nadzorczy stwierdził ponadto, że udostępnienie przez Komendanta danych Skarżącego dotyczących skazań stanowiło naruszenie przepisów o ochronie danych osobowych. Ze względu jednak na niemożność przywrócenia stanu zgodnego z prawem, niemożliwe było zastosowanie przez Prezesa UODO przepisu art. 8 ust. 2 DODO. W związku z powyższym wystosował on do Komendanta wystąpienie[112], w którym zwrócił się o podjęcie stosownych czynności w celu zapewnienia w przyszłości zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, a w szczególności wprowadzenia stosownych rozwiązań organizacyjnych celem rozpatrywania wniosków o udostępnienie danych osobowych w zgodzie z przepisami.

[109] Ustawa z dnia 6 kwietnia 1990 r. o Policji, t.j. Dz. U. z 2021 r. poz. 1881.
[110] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
[111] DS.523.941.2020.
[112] DOL.413.10.2021.

Przetwarzanie danych osobowych w sektorze szkolnictwa

Tematyka skarg na przetwarzanie danych osobowych przez podmioty prowadzące placówki oświatowe wiązała się najczęściej z realizacją nauczania w szczególnych warunkach pandemii, publikacją danych osobowych na prowadzonych przez nie stronach internetowych lub na portalach społecznościowych.

Publikowanie danych osobowych uczniów na portalu społecznościowym placówki oświatowej[113]

Przedmiotem oceny Prezesa Urzędu Ochrony Danych Osobowych była m.in. skarga na udostępnienie danych osobowych małoletnich osób, w tym ich wizerunku, na fanpage'u szkoły – na portalu Facebook.

Zdjęcia, na których znajdował się wizerunek osób, których dane dotyczą, pochodziły z konkursu, którego szkoła była organizatorem. Osobami odpowiedzialnymi za jego organizację byli wychowawcy świetlicy szkolnej, w tym jeden z opiekunów prawnych małoletnich. Szkoła powołała się na postanowienia regulaminów konkursów, zgodnie z którymi przystąpienie uczestnika do konkursu oznaczało zaakceptowanie regulaminu oraz zgodę na publikację wizerunku uczestnika i jego pracy na stronie internetowej szkoły oraz fanpage'u. Ponadto opiekunowie prawni podpisali oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych zawartych w zgłoszeniu dzieci do szkoły, a także ich wizerunków. Zgoda miała obejmować przetwarzanie wizerunku w kronice szkolnej oraz na stronie internetowej szkoły. Organ ochrony danych osobowych zwrócił w decyzji uwagę, że zgodnie z art. 7 ust. 1 i 2 RODO, jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Jeżeli osoba, której dane dotyczą, wyraziła zgodę w pisemnym oświadczeniu, które dotyczyło także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia, nie jest wiążąca. Jak ustalono, ww. oświadczenia opiekunów prawnych o wyrażeniu zgody na przetwarzanie danych osobowych

[113] DS.523.2688.2021.

zawartych w zgłoszeniu dzieci do szkoły, nie obejmowały zgody na przetwarzanie ich wizerunków na portalu społecznościowym Facebook. W przedstawionej przez szkołę dokumentacji szkolnej, w tym w regulaminach do poszczególnych konkursów, zgoda na publikację wizerunku nie została wyodrębniona spośród innych postanowień zawartych w tych dokumentach, w sposób umożliwiający zarówno wyrażenie zgody, jak i jej odmowę w tym konkretnym celu.

W ocenie Prezesa UODO, szkoła nie zapewniła Skarżącej swobody w kwestii wyrażenia zgody na publikację wizerunku ich małoletnich dzieci na stronach internetowych szkoły. Szkoła nie dysponowała więc zgodą opiekunów prawnych, o której mowa w art. 7 RODO, na publikację danych osobowych, w tym wizerunku małoletnich na fanpage'u, czym naruszyła art. 5 ust. 1 lit. a w zw. z art. 6 ust. 1 RODO. Przedmiotowe udostępnienie nastąpiło więc bez podstawy prawnej.

Mając na uwadze, że szkoła niezwłocznie po otrzymaniu skargi usunęła kwestionowane dane, Prezes Urzędu, na podstawie art. 58 ust. 2 lit. b RODO, zastosował wobec szkoły środek naprawczy w postaci upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych.

Pogodzenie prawa do ochrony danych osobowych pracownika szkoły z realizacją nauczania w trybie zdalnym w czasie ograniczonego funkcjonowania placówek oświaty, spowodowanego stanem epidemii COVID – 19[114]

Przedmiotem omawianej sprawy była skarga nauczyciela jednej ze szkół podstawowych, w której nauczyciel ten zgłosił nieprawidłowości w procesie przetwarzania jego danych osobowych, związane z udostępnieniem imienia, nazwiska oraz daty urodzenia na rzecz podmiotu zapewniającego dostarczanie usług platformy edukacyjnej, pozwalającej na realizację procesu nauczania z wykorzystaniem metod i technik kształcenia na odległość. Prezes UODO wziął pod uwagę okoliczności dotyczące wolumenu danych udostępnionych przez szkołę i ich niezbędności do założenia indywidualnego konta na platformie usług udostępnianych przez podmiot przetwarzający i w ten sposób późniejszej realizacji zadań edukacyjnych w trybie zdalnym. Wskazał też, że przetwarzanie danych osobowych w ramach procesu edukacyjnego realizowane było przez szkołę na podstawie art. 6 ust. 1 lit. c RODO, z uwagi na niezbędność przetwarzania dokonywanego w celu zrealizowania obowiązku szkoły wynikającego z przepisu prawa. Natomiast aktem prawnym regulującym m.in. kwestie realizacji procesu edukacyjnego, związanego z zapewnieniem przez placówki edukacyjne bezpiecznych i higienicznych warunków nauki, wychowania i opieki, jest

[114] DS.523.3915.2020.

ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe. Z treści art. 30b tej ustawy wynika, iż w przypadkach uzasadnionych nadzwyczajnymi okolicznościami zagrażającymi życiu lub zdrowiu dzieci i młodzieży, minister właściwy do spraw oświaty i wychowania, w drodze rozporządzenia, może czasowo ograniczyć lub czasowo zawiesić funkcjonowanie jednostek systemu oświaty na obszarze kraju lub jego części, uwzględniając stopień zagrożenia na danym obszarze. Zgodnie natomiast z treścią art. 30c Prawa oświatowego, w przypadku, o którym mowa w art. 30b, minister właściwy do spraw oświaty i wychowania, w drodze rozporządzenia, może wyłączyć stosowanie niektórych przepisów niniejszej ustawy, ustawy o systemie oświaty oraz ustawy o finansowaniu zadań oświatowych w odniesieniu do wszystkich lub niektórych jednostek systemu oświaty, o których mowa w przepisach wydanych na podstawie art. 30b, w szczególności w zakresie przeprowadzania postępowania rekrutacyjnego, oceniania, klasyfikowania i promowania uczniów, przeprowadzania egzaminów, organizacji roku szkolnego i organizacji pracy tych jednostek, a także wprowadzić w tym zakresie odrębne unormowania tak, aby zapewnić prawidłową realizację celów i zadań tych jednostek. W treści decyzji podkreślono, że istotnym aspektem przetwarzania danych osobowych w ramach stosowania technik nauczania w trybie zdalnym jest treść § 1 ust. 1 pkt 2, 3 i 13 rozporządzenia 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[115]. W treści tego aktu prawnego wskazano, że w okresie ograniczenia funkcjonowania jednostki systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, dyrektor jednostki systemu oświaty odpowiada za organizację realizacji jej zadań, w tym zajęć z wykorzystaniem metod i technik kształcenia na odległość lub innego sposobu realizacji tych zajęć. W szczególności ustala, we współpracy z nauczycielami, technologie informacyjno-komunikacyjne wykorzystywane przez nauczycieli do realizacji zajęć, określa zasady bezpiecznego uczestnictwa w zajęciach w odniesieniu do ustalonych technologii informacyjno-komunikacyjnych, ustalonych przez dyrektora; przekazuje uczniom, rodzicom i nauczycielom informację o sposobie i trybie realizacji zadań tej jednostki, a więc np. o serwisach informatycznych używanych do prowadzenia zdalnego nauczania. W przepisach wspomnianego rozporządzenia wskazano, że wszelkie ustalenia w tym zakresie pozostają wyłącznie w gestii dyrektora szkoły, który powinien je wprowadzić w drodze zarządzenia, co też w omawianej sprawie ustalono. Prezes UODO stwierdził, że działania szkoły dotyczące

[115] Dz. U. poz. 493 z późn. zm.

udostępnienia danych osobowych Skarżącej celem organizacji zadań edukacyjnych w formie nauczania zdalnego, znajdują uzasadnienie w treści art. 6 ust.1 lit. e RODO, ale jedynie w odniesieniu do danych dotyczących imienia i nazwiska Skarżącej. Działania szkoły nie znajdowały natomiast uzasadnienia w przedmiocie udostępnienia daty urodzenia Skarżącej. Okoliczność ta podyktowana jest określoną w treści art. 5 ust.1 lit. c RODO zasadą minimalizacji danych osobowych. Przywołany art. 5 ust. 1 lit. c stanowi bowiem, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"). Adekwatność – to gromadzenie danych w zakresie wystarczającym do realizacji celu danego przetwarzania. W myśl tej zasady do przetwarzania danych osobowych musi dochodzić z maksymalnym ograniczeniem ingerencji w sferę prywatności. Przetwarzanie niezbędne, rozumiane w kontekście przepisów chroniących dane osobowe, to czynności koniecznie potrzebne dla osiągnięcia wskazanych celów. Nie ma usprawiedliwienia dla zbierania informacji na zapas, bez wyraźnego i dającego się usprawiedliwić powodu. Jeśli osiągnięcie określonego celu jest możliwe z wykorzystaniem mniejszej ilości informacji, gromadzenie dodatkowych danych może zostać uznane za złamanie zasady adekwatności. Prezes Urzędu stwierdził, że udostępnienie danych osobowych Skarżącej w zakresie jej daty urodzenia, nie znajduje podstaw w przepisach prawa z uwagi na brak niezbędności tych danych do założenia konta pozwalającego na realizację nauczania w trybie zdalnym. Tym bardziej, że podmiotowi przetwarzającemu udostępniono szeroki zakres innych danych wystarczających do założenia takiego konta. Za powyższe naruszenie Prezes Urzędu, korzystając z uprawnienia przewidzianego w art. 58 ust 2 lit. b, upomniał szkołę za naruszenie art. 5 ust. 1 lit. c oraz art. 6 ust. 1 RODO z uwagi na brak podstawy prawnej dla takiego procesu przetwarzania danych osobowych.

Relacja między obowiązkiem realizacji prawa dostępu do danych a obowiązkiem informacyjnym z art. 13 RODO, udostępnienie adresu e-mail na skutek braku ukrycia jego odbiorców, przetwarzanie danych przez podmioty współpracujące (powierzenie przetwarzania danych) – były tematem skargi na nieprawidłowości w procesie przetwarzania danych osobowych Skarżącej i jej małoletniego dziecka przez przedszkole[116].

Skarżąca zarzuciła administratorowi nieprawidłowości polegające na braku realizacji obowiązku informacyjnego w zakresie informacji o źródle i zakresie pozyskanych jej danych

[116] DS.523.3847.2020.

osobowych, bezprawnemu udostępnieniu danych jej oraz jej małoletniego dziecka (w tym w zakresie wizerunku dziecka) na rzecz konkretnych podmiotów współpracujących z przedszkolem (takich jak animatorzy i nauczyciele prowadzący zajęcia w ramach swoich działalności gospodarczych), usługodawcy komunikatora internetowego i podmiotu świadczącego usługi cateringowe oraz bezprawnemu udostępnieniu jej adresu e-mail na rzecz osób trzecich.

Odnosząc się do pierwszego zarzutu, organ stwierdził, że pomimo skierowania przez Skarżącą wniosku odpowiadającego dyspozycji art. 15 ust. lit. b i g RODO, administrator nie udzielił żądanych informacji. Fakt wypełnienia obowiązku informacyjnego z art. 13 RODO nie zwalniał z obowiązku udzielenia wnioskodawcy odpowiedzi na zadane pytanie. Istotą obowiązku informacyjnego z art. 15 RODO jest przejrzysta i rzetelna komunikacja z podmiotem danych, zaś z treści wniosku wynikało, że Skarżąca nie wie, skąd administrator pozyskał jej dane i w jakim zakresie. Tym samym po stronie administratora powstał obowiązek udzielenia żądanych informacji na rzecz wnioskodawcy w terminie określonym w art. 12 ust. 3 RODO. Organ stwierdził, że administrator naruszył art. 12 ust. 3 oraz art. 15 ust. 1 RODO poprzez brak spełnienia obowiązku informacyjnego w zakresie informacji o kategoriach danych osobowych i źródle ich pozyskania.

Natomiast w temacie skargi na udostępnienie adresu e-mail organ stwierdził, że administrator ujawnił dane osobowe Skarżącej na rzecz osób nieuprawnionych poprzez przesłanie dwóch e-maili w tzw. otwartej kopii (bez zakrycia adresatów wiadomości). Organ ocenił, że udostępniając dane osobowe w ww. zakresie administrator nie legitymował się żadną z przesłanek określonych w art. 6 ust. 1 RODO, czym naruszył ww. przepis w zw. z art. 5 ust. 1 lit. a RODO.

W zakresie zarzutu bezprawnego udostępnienia danych osobowych Skarżącej i jej małoletniego dziecka na rzecz osób i podmiotów, z którymi administrator współpracuje, organ stwierdził, że do czasu rozpoczęcia nauki zdalnej, spowodowanej obostrzeniami związanymi z COVID-19, osoby te przetwarzały dane na podstawie stosownych upoważnień do przetwarzania danych osobowych zgodnie z art. 29 RODO i świadczyły pracę stacjonarnie, w siedzibie przedszkola. Natomiast po wprowadzeniu przepisów dotyczących nauki zdalnej, jedynie jedna ze wskazanych osób przetwarzała dane osobowe dziecka, które to przetwarzanie miało miejsce poza siedzibą przedszkola. Ze wskazanym podmiotem zawarta została umowa powierzenia przetwarzania danych osobowych zgodnie z art. 28 ust. 3 RODO. Ponadto osoba ta prowadziła zajęcia przy wykorzystaniu komunikatora internetowego i na tę okoliczność otrzymała od przedszkola pisemną zgodę na dalsze powierzenie przetwarzania danych przez usługodawcę tego komunikatora.

Organ ocenił, że nie doszło tu do bezprawnego udostępnienia danych osobowych Skarżącej oraz jej małoletniego dziecka. Administrator przetwarzał dane osobowe na podstawie umowy o kształcenie w oparciu o art. 6 ust. 1 lit. b RODO. Natomiast w przypadku przekazywania danych na rzecz nauczycieli, innych osób współpracujących w zakresie kształcenia dzieci oraz podmiotów przetwarzających, udostępnienie odbywało się na podstawie umowy łączącej podmioty danych z administratorem. Wobec powyższego organ odmówił uwzględnienia wniosku w zakresie zarzutu bezprawnego udostępnienia danych osobowych na rzecz konkretnych podmiotów współpracujących z przedszkolem (takich jak animatorzy i nauczyciele prowadzący zajęcia w ramach swoich działalności gospodarczych) oraz usługodawcy komunikatora internetowego, ponieważ przetwarzanie to odbywało się na podstawie art. 6 ust. 1 lit. b RODO.

Odnośnie podmiotu świadczącego usługi cateringowe dla przedszkola organ ocenił, że podmiot ten nie otrzymywał od skarżonego podmiotu danych osobowych, wobec tego kwestionowany proces przetwarzania danych osobowych nie zaistniał, i w tym zakresie umorzył podstępowanie ze względu na jego bezprzedmiotowość.

Po zebraniu i rozpatrzeniu całego materiału dowodowego organ wydał decyzję, mocą której:

1. nakazał administratorowi spełnienie obowiązku z art. 15 ust. 1 RODO poprzez udzielenie informacji o kategoriach pozyskanych danych osobowych oraz informacji o źródle ich pozyskania;
2. udzielił upomnienia za naruszenie art. 6 ust. 1 w zw. z art. 5 ust 1 lit. a RODO polegające na udostępnieniu przez administratora danych osobowych w zakresie adresu e-mail na rzecz osób trzecich, bez podstawy prawnej;
3. odmówił uwzględnienia wniosku w zakresie zarzutu bezprawnego udostępnienia danych osobowych, w tym w zakresie wizerunku dziecka, dotyczących osoby Skarżącej oraz jej małoletniego dziecka na rzecz osób współpracujących z przedszkolem oraz usługodawcy komunikatora internetowego;
4. w pozostałym zakresie umorzył postępowanie.

4.1.4. Sektor finansów, telekomunikacji i ubezpieczeń

Spośród 8318 skarg, które w 2021 r. wpłynęły do Urzędu, **1833** z nich dotyczyło podmiotów sektora banków i instytucji finansowych, telekomunikacji i ubezpieczeń. Poniżej omówione zostały wybrane przykłady kilku takich skarg.

Przetwarzanie danych osobowych w sektorze finansowym

Przetwarzanie danych osobowych przez banki w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, a także ocena procesów przetwarzania danych kontynuowanych po wygaśnięciu zobowiązań wynikających z umów, to przykład jednej z wielu skarg dotyczących tego obszaru.

W tej kwestii niezbędne były rozważania dotyczące art. 105a ust. 1 Prawa bankowego[117], zgodnie z którym przetwarzanie przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów, instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, a także instytucje utworzone na podstawie art. 105 ust. 4 Prawa bankowego, informacji stanowiących tajemnicę bankową i informacji udostępnionych przez instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim[118], w zakresie dotyczącym osób fizycznych może być wykonywane, z zastrzeżeniem art. 104, art. 105 i art. 106–106d, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Zgodnie zaś z art. 105a ust. 4 Prawa bankowego, banki oraz instytucje, o których mowa w art. 105 ust. 4, mogą przetwarzać stanowiące tajemnicę bankową informacje dotyczące osoby fizycznej po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów, bez zgody osoby, której informacje dotyczą, do celów stosowania metod wewnętrznych oraz innych metod i modeli, o których mowa w części trzeciej rozporządzenia CRR[119]. Stosownie zaś do art. 105a ust. 5 Prawa bankowego, przetwarzanie informacji stanowiących tajemnicę bankową w przypadku, o którym mowa w ust. 4, przez okres 12 lat od dnia wygaśnięcia zobowiązania.

Wskazać należy, że do przetwarzania danych na podstawie art. 105a ust. 1 Prawa bankowego, zgoda osoby, której dane są przetwarzane, nie jest wymagana. Powołany przepis prawa nie ustanawia takiego wymogu. O zgodzie na przetwarzanie danych stanowiących tajemnicę bankową mowa dopiero w art. 105a ust. 2 Prawa bankowego, tj. po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów[120].

[117] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz. U. z 2021 r. poz. 2439.
[118] Ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim, Dz. U. z 2022 r. poz. 246.
[119] Rozporządzenia Parlamentu Europejskiego i Rady nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012, Dz. Urz. UE L 2013 Nr 176, str. 1.
[120] ZSPR.440.1707.2019.

Zgodnie z art. 70 ust. 1 Prawa bankowego, bank uzależnia przyznanie kredytu od zdolności kredytowej kredytobiorcy. Przez zdolność kredytową rozumie się zdolność do spłaty zaciągniętego kredytu wraz z odsetkami w terminach określonych w umowie. Kredytobiorca jest obowiązany przedłożyć na żądanie banku dokumenty i informacje niezbędne do dokonania oceny tej zdolności. Powyższe przepisy mają istotne znaczenie z perspektywy przetwarzania zapytań kredytowych przez banki, które nie zakończyły się zawarciem z nimi umowy. W takim przypadku bank jest wprawdzie uprawniony, na podstawie art. 105 a ust. 1 Prawa bankowego w zw. z art. 70 ust. 1 tej ustawy, do przetwarza danych wnioskującego o udzielenie kredytu w celu oceny zdolności kredytowej. Jednakże przesłanka uzasadniająca powyższy proces traci na znaczeniu, w momencie gdy nie dochodzi do zawarcia umowy. Warunki określone w art. 105a Prawa bankowego dotyczą przetwarzania informacji objętych tajemnicą bankową w okresie przed powstaniem zobowiązania, w trakcie jego trwania oraz po wygaśnięciu zobowiązania. Gdy pomiędzy bankiem a osobą ubiegającą się o kredyt nie doszło do nawiązania stosunku zobowiązaniowego, który stosownie do art. 105 a ust. 1–6 Prawa bankowego dawałby podstawę do dalszego przetwarzania danych osobowych wynikających z przedmiotowego zapytania, nie można uznać, że bank jest uprawniony do kontynowania procesu przetwarzania tych danych osobowych na powyższej podstawie prawnej[121].

Kwestie przetwarzania danych po wygaśnięciu zobowiązania wynikającego z umowy regulowane są odpowiednio w art. 105a ust. 2, 3 i ust. 4 Prawa bankowego. Przepis art. 105a ust. 2 Prawa bankowego uzależnia legalność tego procesu od zgody osoby, której informacje dotyczą z zastrzeżeniem, że zgoda ta może być w każdym czasie odwołana. Zgodnie z art. 105a ust. 3 Prawa bankowego banki, instytucje oraz podmioty, o których mowa w ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową i informacje udostępnione przez instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy o kredycie konsumenckim, dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z zawartej z tymi podmiotami umowy, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z tej umowy, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby o zamiarze przetwarzania dotyczących jej informacji, bez jej zgody. Zgodnie natomiast z art. 105a ust. 4 Prawa bankowego, banki oraz instytucje, o których mowa w art. 105 ust. 4, mogą przetwarzać stanowiące tajemnicę bankową informacje dotyczące osoby fizycznej po wygaśnięciu zobowiązania wynikającego z umowy zawartej

[121] ZSPR.440.1658.2019, wyrok Naczelnego Sądu Administracyjnego z dnia 27 sierpnia 2019 r. sygn. akt I OSK 2567/17.

z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów bez zgody osoby, której informacje dotyczą, do celów stosowania metod wewnętrznych oraz innych metod i modeli, o których mowa w części trzeciej rozporządzenia CRR. Przetwarzanie informacji stanowiących tajemnicę bankową w przypadkach, o których mowa w ust. 3 może być wykonywane przez okres nie dłuższy niż 5 lat, natomiast w przypadkach, o których mowa ust. 4, może być wykonywane przez okres nie dłuższy niż 12 lat od dnia wygaśnięcia zobowiązania (art. 105a ust. 5 Prawa bankowego).

W kontekście powyższej regulacji Prezes Urzędu Ochrony Danych Osobowych podkreślił, że posiadanie kopii korespondencji oraz zwrotnego potwierdzenia odbioru korespondencji stanowi dostateczny dowód dotyczący spełnienia przesłanki poinformowania dłużnika o zamiarze przetwarzania jego danych osobowych po wygaśnięciu zobowiązania na podstawie art. 105a ust. 3 Prawa bankowego[122]. W ocenie Prezesa UODO, sporządzenie i wysłanie pisma nie jest jednak równoznaczne z udowodnieniem prawidłowego doręczenia, skutkującego poinformowaniem dłużnika o zamiarze przetwarzania danych stanowiących tajemnicę bankową, bez jego zgody, na podstawie art. 105a ust. 3 Prawa bankowego. Samo oświadczenie o wysłaniu korespondencji nie stanowi dowodu na jej dostarczenie lub poinformowanie adresata o jej treści. W tym miejscu należy wskazać, że przepisy powszechnie obowiązujące nie formułują obowiązku wysyłania informacji, o której mowa w art. 105a ust. 3 Prawa bankowego, w szczególnej formie. To do podmiotu informującego należy wybór formy przekazania odbiorcy komunikatu o zamiarze przetwarzania danych osobowych bez jego zgody. Jednocześnie to podmiot informujący wywodzi z powyższego skutki prawne i to on musi wykazać, że poinformował dłużnika o zamiarze przetwarzania danych stanowiących tajemnicę bankową, bez jego zgody, na podstawie art. 105a ust. 3 Prawa bankowego[123].

W innej rozpatrywanej sprawie Prezes UODO stanął na stanowisku, że wymogi przewidziane w przywołanych powyżej przepisach prawa odnoszą się również do osób fizycznych prowadzących działalność gospodarczą. W art. 4 ust. 1 Prawa przedsiębiorców[124] wskazano, że przedsiębiorcą jest osoba fizyczna, osoba prawna lub jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną, wykonująca działalność gospodarczą. Osobą fizyczną w świetle orzecznictwa nie jest wyłącznie konsument[125]. W konsekwencji powyższego Prezes Urzędu Ochrony Danych Osobowych podkreślił, że przetwarzając dane na podstawie prawnej wynikającej z art. 105a

[122] ZWOS.440.5973.2019.
[123] ZSPR.440.324.2019.
[124] Ustawa z dnia 6 marca 2018 r. Prawo przedsiębiorców, Dz. U. 2021 r. poz. 162.
[125] Wyrok Wojewódzkiego Sądu Administracyjnego z dnia 12 czerwca 2017, sygn. akt II Sa/Wa 1991/16.

Prawa bankowego, bank musi spełnić wszystkie wskazane w tym przepisie przesłanki legalizujące przetwarzanie danych osobowych w taki sposób, a nie wykorzystywać je wybiórczo[126].

Z przepisów regulujących uprawnienie banków do przetwarzania danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego nie wynika, zdaniem organu, uprawnienie do pozyskania numeru telefonu. Prezes Urzędu Ochrony Danych Osobowych podkreślił, że bank nie może w dowolny sposób decydować o czynnikach, a zatem także o zakresie danych osobowych koniecznych do przeprowadzenia oceny zdolności kredytowej klienta, ponieważ prowadziłoby to do uznania, że bank na potrzeby oceny zdolności kredytowej klienta może przetwarzać nieograniczony katalog danych osobowych tego klienta, w szczególności, gdy dane w zakresie numeru telefonu zostały pozyskane pierwotnie w innym celu[127].

Przetwarzanie danych osobowych przez banki w bazach zewnętrznych utworzonych na podstawie przepisów ustawy Prawo bankowe

Duża liczba skarg indywidualnych, które wpłynęły do Urzędu w 2021 roku dotyczyła udostępniania przez banki danych na rzecz instytucji utworzonych na podstawie art. 105 ust. 4 Prawa bankowego[128].

Co do zasady, podstawą prawną przetwarzania danych osobowych klientów przez bank w instytucjach, o których mowa w art. 105 ust. 4 Prawa bankowego, może być art. 6 ust. 1 lit. f RODO, gdy przetwarzanie to jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. W poprzednim stanie prawnym podstawą prawną ww. procesu przetwarzania był natomiast przepis art. 23 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[129]. Wskazania ponadto wymaga, że przetwarzanie danych osobowych klientów banku przez powyższe odbywa się na podstawie umowy zawartej z bankiem będącym administratorem[130].

Jedna ze skarg dotyczyła kwestii przekazania do instytucji, o której mowa w art. 105 ust. 4 Prawa bankowego, danych klienta z naruszeniem zasady, o której mowa w art. 5 ust. 1 lit. d RODO. Zgodnie z powyższą zasadą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle

[126] ZWOS.440.5973.2019.
[127] ZSPR.440.726.2018.
[128] ZSPR.440.753.2019.
[129] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2016 r. poz. 922.
[130] ZSPR.440.753.2019.

celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"). Na podstawie art. 16 RODO 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[131].

Powyższe przepisy administrator, będący wierzycielem, powinien uwzględnić, gdy dłużnik składa wniosek o sprostowanie danych osobowych w zakresie np. informacji o historii spłaty kredytu hipotecznego, jak również, gdy dłużnik żąda dokonania korekty w zakresie jego danych osobowych przekazanych do instytucji, o której mowa w art. 105 ust. 4 Prawa bankowego[132]. Do realizacji powyższego żądania sprostowania danych znajduje zastosowanie zasada określona w art. 12 ust. 3 RODO, zgodnie z którą administrator ma obowiązek udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem, bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania, przy czym w razie potrzeby termin ten może być przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, o czym należy powiadomić wnioskodawcę, jeżeli taka sytuacja zachodzi, podając przyczyny opóźnienia[133].

W ocenie Prezesa Urzędu Ochrony Danych Osobowych do nieprawidłowości w zakresie braku sprostowania danych osobowych udostępnionych przez bank na rzecz instytucji, o której mowa w art. 105 ust. 4 Prawa bankowego, nie będzie natomiast dochodziło w przypadku żądania zmiany wartości zobowiązania z waluty obcej na walutę polską, gdy umowa, z której ono wynika, zawarta została w tej walucie obcej. Będzie to miało miejsce w sytuacji, gdy kredytobiorcy zawarli z bankiem umowę kredytu, którego wartość wyrażona została w walucie obcej, kredyt został uruchomiony w walucie polskiej i zgodnie z postanowieniami umownymi spłata rat kredytu następuje w walucie polskiej, ale po przeliczeniu według kursu wymiany walut obowiązującego w banku na dzień spłaty. Bank jest zobligowany przesyłać do ww. instytucji informacje, które odzwierciedlają rzeczywisty stan kredytu zaciągniętego przez dłużnika w walucie obcej. Podkreślić należy, że prawo do żądania od administratora sprostowania danych osobowych przysługuje w sytuacji, gdy dane te są nieprawidłowe, co w powyższej sytuacji nie miało miejsca. Okoliczność czy umowa stanowiła *de facto* zaciągnięcie zobowiązania w walucie polskiej, czy w walucie obcej, może być przedmiotem oceny sądu powszechnego, w ramach dokonywania oceny prawidłowości zawarcia stosunku

[131] ZSPR.440.753.2019.
[132] ZSPR.440.753.2019.
[133] ZSPR.440.753.2019.

zobowiązaniowego i jego elementów, natomiast Prezes Urzędu Ochrony Danych Osobowych nie jest do tego rodzaju ocen uprawniony[134].

Wydanie kopii danych osobowych przez bank na żądanie osoby, której dane dotyczą

Liczne skargi indywidualne kierowane do Prezesa Urzędu Ochrony Danych Osobowych dotyczyły sposobu realizacji obowiązku informacyjnego wynikającego z art. 15 ust. 3 RODO, tj. realizacji uprawnienia do uzyskania kopii danych osobowych przetwarzanych przez administratora.

W stosunku do żądań kierowanych do banków o wskazanie adresów IP innych osób, z których nastąpiły błędne logowania na rachunek wnioskującego klienta banku, Prezes Urzędu Ochrony Danych Osobowych wskazał, że w jego ocenie przekracza to ramy obowiązku informacyjnego, o którym mowa w art. 15 RODO. W przypadku, gdy administrator przetwarza dane osoby, która występuje z żądaniem informacyjnym, powinien on udostępnić tej osobie dane na jej temat. Z uprawnienia tego może skorzystać każda osoba, która chce uzyskać informacje na swój temat, natomiast uprawnienie to nie rozciąga się na ujawnianie informacji na temat innych osób[135].

Prezes Urzędu Ochrony Danych Osobowych rozpatrywał również skargi, w których osoby je wnoszące żądały udostępnienia na podstawie art. 15 ust. 3 RODO przez bank, kopii dokumentacji zawierającej ich dane osobowe. Zgodnie z art. 15 ust. 3 RODO, obowiązek udostępnienia kopii danych osobowych nie jest równoznaczny z obowiązkiem udostępnienia kopii dokumentacji dotyczącej zawartych umów. Administrator nie ma obowiązku udostępnienia osobie zainteresowanej kopii nośnika, na którym przetwarzane są jej dane osobowe. Powyższe oznacza, że realizując obowiązek wynikający z art. 15 ust. 3 RODO, administrator może poprzestać na wskazaniu treści danych dotyczących osoby wnioskującej. Wykonanie obowiązku określonego w art. 15 ust. 3 RODO może być także realizowane poprzez sporządzenie kopii lub odpisu dokumentu (nośnika) zawierającego dane osobowe. Jednak w przypadku zwrócenia się do administratora o kopię przetwarzanych danych osobowych, administrator każdorazowo podejmuje decyzję, w jaki sposób zrealizuje to uprawnienie. Zatem to administrator, a nie osoba, której dane dotyczą, może dokonać wyboru, czy udostępnia kopię dokumentów, czy też udostępnia kopię danych zawartych w tych dokumentach[136].

[134] DS.523.2532.2020.
[135] ZSPR.440.1751.2019.
[136] DS.523.4531.2020.

Wskazać należy także, że uprawnienie wynikające z art. 15 RODO realizowane jest wyłącznie na wniosek osoby uprawnionej i brak takiego wniosku oznacza, że po stronie administratora nie powstaje skorelowany z nim obowiązek. Realizacja uprawnień określonych w art. 15 RODO, w odróżnieniu od prawa do informacji zagwarantowanego w art. 13 czy 14, wymaga inicjatywy podmiotu danych[137]. W ocenie Prezesa Urzędu Ochrony Danych Osobowych osoba, której dane dotyczą, wprawdzie nie musi obligatoryjnie powoływać się w swych wnioskach na przepisy art. 15 ust. 3 RODO, niemniej jednak, jeżeli domaga się realizacji praw przysługujących jej w oparciu o ww. przepis, powinna wskazać administratorowi, że domaga się przekazania kopii jej danych osobowych[138]. Administrator musi odróżniać wniosek o wydanie kopii nośnika danych (dokumentacji, nagrania rozmowy) od wniosku o kopie danych osobowych zawartych na tym nośniku. Prezes Urzędu Ochrony Danych Osobowych przyjął stanowisko, że dopuszczalny jest w ramach uprawnienia, o którym mowa w art. 15 ust. 3 RODO, wniosek o wydanie kopii wzoru podpisu, gdyż nie jest to tożsame z wnioskiem o wydanie kopii dokumentacji w zakresie kopii karty wzoru podpisu osoby wnioskującej. Jednocześnie organ zauważył, że to na banku – jako administratorze – spoczywa ciężar dowodu w zakresie wykazania, iż żądanie miało ewidentnie nieuzasadniony lub nadmierny charakter[139].

Na podstawie art. 15 ust. 3 RODO, osoba może również uzyskać swoje dane osobowe zawarte w nagraniu rozmowy telefonicznej. W przypadku danych osobowych utrwalonych na nagraniu, administrator może dokonać wyboru, czy udostępni kopię nagrania, czy też udostępni kopię danych zawartych w tym nagraniu[140]. Podczas realizacji takiego wniosku należy mieć na uwadze ograniczenia wynikające m.in. z art. 15 ust. 4 RODO. W przypadku takiego żądania przesłanie kopii w formie tekstowej jest niewystarczające. Bank przy wyborze sposobu realizacji ww. obowiązku informacyjnego musi uwzględnić okoliczność, że przetwarza on dane osobowe w zakresie głosu w wyniku przechowywania nagrania rozmowy telefonicznej[141]. Udostępnienie kopii danych osobowych zawartych w rozmowie telefonicznej, nie narusza obowiązku zachowania tajemnicy bankowej. Zgodnie z art. 104 ust. 3 Prawa bankowego, banku nie obowiązuje, z zastrzeżeniem ust. 4 i 4a, zachowanie tajemnicy bankowej wobec osoby, której dotyczą informacje objęte tajemnicą[142].

[137] DS.523.4531.2020, ZSPR.440.562.2019.
[138] DS.523.725.2021.
[139] ZSPR.440.1686.2018.
[140] DS.523.1694.2021.
[141] DS.523.1694.2021.
[142] DS.523.1694.2021.

Spełnienie powyższego obowiązku przez bank powinno nastąpić z poszanowaniem praw innych osób, w tym prawa do ochrony danych osobowych tych osób, tj. w sposób nie przekraczający ram obowiązku informacyjnego z art. 15 ust. 3 RODO[143].

Podkreślenia wymaga, że nie zawsze bank będzie obowiązany do spełnienia obowiązku informacyjnego, o którym mowa w art. 15 RODO. Wspomniany powyżej art. 23 ust. 1 RODO stanowi, że prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym m.in. zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom. Jak natomiast stanowi art. 106e Prawa bankowego, do przetwarzania danych osobowych przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, instytucje pożyczkowe, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy o kredycie konsumenckim, przepisu art. 15 RODO nie stosuje się w zakresie, w jakim jest to niezbędne dla prawidłowej realizacji zadań dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zgodnie z art. 106, oraz zapobiegania przestępstwom, zgodnie z art. 106a i art. 106d. Oznacza to, że w przypadku przetwarzania danych osobowych w powyższych celach bank będzie zwolniony z obowiązku informacyjnego, o którym mowa w art. 15 RODO[144].

W jednej ze spraw Prezes Urzędu Ochrony Danych Osobowych, rozpatrując skargę na sposób realizacji z art. 15 ust. 1 RODO przez bank, wskazał, że spełnił on wniosek jedynie częściowo, udzielając odpowiedzi wyłącznie w formie elektronicznej, pomijając realizację żądania przesłania odpowiedzi również na adres poczty tradycyjnej. Zgodnie z brzmieniem art. 12 ust. 1 RODO, informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie, a jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Stosownie do treści art.

[143] DS.523.1694.2021.
[144] ZSPR.440.1541.2019,

12 ust. 3 RODO, jeśli osoba ta przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. We wniosku zawarto żądanie przekazania Wnioskującemu informacji na adres elektroniczny (e-mail) oraz w formie pisemnej na wskazany adres poczty tradycyjnej. W takiej sytuacji bank powinien był spełnić ww. żądanie poprzez udzielenie odpowiedzi na żądanie w formie pisemnej, zaś formę elektroniczną potraktować jako tę dodatkową, od której ewentualnie, po uzasadnieniu takiego działania, mógłby odstąpić[145].

Inne żądania z rozdziału III RODO kierowane do banków

W roku 2021 Prezes Urzędu Ochrony Danych Osobowych rozpatrywał liczne skargi na banki dotyczące nieprawidłowego rozpatrzenia wniosków o sprostowanie danych osobowych na podstawie przywołanego wcześniej art. 16 RODO.

W pierwszej kolejności podkreślenia wymaga, że Wnioskujący powinien dochować należytej staranności w zakresie prawidłowego złożenia wniosku o sprostowanie. Brak złożenia takiego wniosku do podmiotu będącego administratorem może skutkować uznaniem późniejszej skargi indywidualnej wniesionej do Prezesa Urzędu Ochrony Danych Osobowych za przedwczesną. Taka sytuacja może mieć miejsce, gdy osoba wnioskująca złoży żądanie do innego podmiotu z zaznaczeniem, że żądanie dotyczy też banku będącego administratorem. W sytuacji braku złożenia osobnego wniosku o sprostowanie danych osobowych do banku może dojść do sytuacji, że bank nie zostanie poinformowany o żądaniu np. aktualizacji danych. Ma to istotne znacznie również z tej perspektywy, że bank nie może czynić samodzielnie ustaleń w zakresie prawidłowości podanego w trakcie zawierania umowy adresu do korespondencji. To obowiązkiem osoby, której dane osobowe są przetwarzane przez bank, jest poinformowanie banku o zmianie tego adresu[146].

Warto wskazać, że Prezes Urzędu Ochrony Danych Osobowych wypowiedział się również w kontekście przetwarzania nieaktualnych danych kontaktowych (numeru telefonu) przez bank w przypadku braku możliwości nawiązania kontaktu z wykorzystaniem aktualnego adresu wskazanego przez klienta we wniosku o aktualizację jego danych w tym zakresie. Prezes Urzędu Ochrony Danych Osobowych stanął na stanowisku, że przetwarzanie danych osobowych dłużników

[145] ZSPR.440.1395.2019.
[146] DS.523.5600.2020, DS.523.5599.2020.

w celach windykacyjnych nie może odbywać się z naruszeniem ich praw[147], w tym również prawa do aktualizacji danych osobowych[148].

Kwestia aktualności danych osobowych w zakresie danych kontaktowych przetwarzanych przez bank i brak dbałości w tym zakresie przez osoby, których dane osobowe są przetwarzane przez bank, może mieć też istotne znaczenie z perspektywy zarzutu udostępnienia danych osobowych osobom nieuprawnionym. Organ nadzorczy rozpatrywał skargę na udostępnienie danych osobowych dłużnika przez bank podczas połączenia telefonicznego z osobami trzecimi. Bank kontaktował się na numer telefonu wskazany we wniosku o udzielenie kredytu oraz z numerami telefonu związanymi z działalnością gospodarczą dłużnika. Pracownicy banku usiłowali uzyskać połączenie telefoniczne z dłużnikiem. W przypadku odebrania połączenia telefonicznego przez inną osobę, pozostawiali wiadomość z numerem telefonu i informacją, aby dłużnik pod tym numerem skontaktował się z bankiem. W tej sytuacji Prezes Urzędu Ochrony Danych Osobowych stanął na stanowisku, że powyższe działania banku nie mogą być postrzegane jako naruszające prawa i wolności dłużnika. Celem banku było skontaktowanie się z dłużnikiem, który powinien liczyć się z tym, że bank może telefonować pod podany przez niego numer telefonu. W przypadku, gdy dłużnik przekazał swój numer telefonu innej osobie i nie chciał, aby bank kontaktował się z nim pod tym numerem, powinien o tym poinformować bank. Wskazania również wymaga, że pracownicy banku, dzwoniąc pod numery telefonu związane z działalnością gospodarczą dłużnika, mogli przypuszczać, że rozmawiają z osobami upoważnionymi do odbierania połączeń telefonicznych w imieniu dłużnika[149].

Instytucje pożyczkowe i przetwarzanie danych osobowych pożyczkobiorców

Skargi wniesione w 2021 r. do Prezesa Urzędu Ochrony Danych Osobowych dotyczyły również nieprawidłowości polegających na udostępnieniu danych osobowych dłużników osobom nieuprawnionym w trakcie prowadzenia terenowych czynności windykacyjnych przez instytucje pożyczkowe i osoby działające w ich imieniu.

W jednej ze spraw Instytucja pożyczkowa, prowadząc czynności windykacyjne, w niezabezpieczonym wezwaniu do zapłaty z oznaczeniem „Dłużnik", udostępniła osobom nieuprawnionym dane osobowe dłużnika w zakresie imienia, nazwiska, adresu zamieszkania oraz informacjami o zadłużeniu. Wezwanie umieszczone zostało na skrzynce pocztowej oraz drzwiach

[147] Wyrok Naczelnego Sądu Administracyjnego z dnia 5 stycznia 2010 r. sygn. akt I OSK 399/09.
[148] ZSZZS.440.542.2019.
[149] ZSPR.440.707.2018.

wejściowych do mieszkania dłużnika. Dodatkowo w treści wezwania widniały informacje o zobowiązaniu wraz z numerem konta skarżonego podmiotu. W ocenie Prezesa Urzędu Ochrony Danych Osobowych stanowiło to naruszenie przepisów o ochronie danych osobowych[150].

Inna ze skarg dotyczyła kontaktu Instytucji pożyczkowej z rodzicem dłużnika w celu wyjaśnienia zadłużenia. W sprawie tej kwestionowana była zgoda wyrażona przez rodzica dłużnika na przetwarzanie jego danych osobowych. W przedmiotowej sprawie Prezes Urzędu Ochrony Danych Osobowych stanął na stanowisku, że jednorazowy kontakt telefoniczny mający wyjaśnić sprawę zadłużenia dłużnika, nie może być rozumiany jako zgoda na dalsze przetwarzanie danych osobowych jego rodzica, z którym odbyła się ta rozmowa. Ponadto instytucja pożyczkowa nie wykazała, że rodzic był uprawniony do reprezentacji dłużnika wobec ww. podmiotu. Takie przetwarzanie w przypadku braku powyższego umocowania było niedopuszczalne, w szczególności, że rodzica dłużnika nie łączył z pożyczkodawcą żaden stosunek cywilno-prawny, a ponadto dane rodzica dłużnika od początku były identyfikowane przez pożyczkodawcę jako dane osoby trzeciej. Podkreślenia wymaga, że w świetle art. 7 ust. 1 RODO, to na administratorze spoczywa ciężar dowodowy w zakresie wykazania udzielenia zgody[151]. Prezes Urzędu Ochrony Danych Osobowych podkreślił, że powoływane przez instytucję pożyczkową przepisy ustawy z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmiot rynku finansowego i o Rzeczniku Finansowym[152], nie uzasadniają przetwarzania danych osoby trzeciej w ramach czynności windykacyjnych, niezwiązanych z żadnym stosunkiem cywilno-prawnym z pożyczkodawcą. Art. 5 tejże ustawy określa tryb postępowania z reklamacją złożoną przez klienta danego podmiotu. Natomiast opisana powyżej osoba nie mieści się w katalogu wskazanym w definicji ustawowej „klienta", zawartej w art. 2 pkt 1 ww. ustawy[153].

Odnośnie skarg na udostępnienie danych osobowych przez instytucję pożyczkową na rzecz innego podmiotu warto wskazać, że w 2021 r. organ właściwy do spraw ochrony danych osobowych rozpatrywał skargę na udostępnienie przez instytucję pożyczkową danych pożyczkobiorcy w zakresie jego zobowiązania na rzecz pracodawcy. Instytucja pożyczkowa posiadała podpisane przez pożyczkobiorcę pisemne oświadczenie o wyrażeniu zgody na dobrowolne potrącenie

[150] ZSPR.440.448.2019.
[151] DS.523.4528.2020.
[152] Ustawa z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmiot rynku finansowego i o Rzeczniku Finansowym, Dz.U. 2019 poz. 2279.
[153] DS.523.4528.2020.

należności z wynagrodzenia, o którym mowa w art. 91 § 1 Kodeksu pracy[154]. Prezes UODO wskazał, że jeśli były spełnione wymogi formalne dotyczące pisemności oświadczenia, pracownik miał świadomość wysokości długu i przesłanek co do swojej odpowiedzialności, a wyrażenie zgody nie było dorozumiane[155], to takie udostępnienie danych osobowych pracodawcy pożyczkobiorcy ma oparcie w przesłance z art. 6 ust. 1 lit. a RODO[156].

Dochodzenie wierzytelności przez podmioty działające w imieniu funduszy inwestycyjnych

W przypadku funduszy inwestycyjnych pozyskiwanie danych osobowych dłużników, wobec których podmiot taki prowadził postępowania windykacyjne, odbywało się na podstawie art. 509 Kodeksu cywilnego[157], w ramach umowy cesji wierzytelności zawartej przez taki fundusz z poprzednim wierzycielem. W myśl powyższego przepisu wierzyciel może bez zgody dłużnika przenieść wierzytelność na osobę trzecią (przelew), chyba że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania (§ 1). Wraz z wierzytelnością przechodzą na nabywcę wszelkie związane z nią prawa, w szczególności roszczenie o zaległe odsetki (§ 2).

Prezes Urzędu Ochrony Danych Osobowych poruszając temat cesji na gruncie ustawy z dnia 29 sierpnia 1997 r. wskazał, że nie można też tak rozumieć przepisów powyższej ustawy, że udostępnienie danych osobowych dłużnika w celu windykacji należności narusza dobro tej osoby, gdyż byłoby to niczym nieuzasadnione jej uprzywilejowanie. Zawierając umowę cywilnoprawną, należy liczyć się z jej konsekwencjami, a także z tym, że obowiązek wykonania umowy dotyczy jednej i drugiej strony, nawet jeżeli jedna z nich jest konsumentem. Ochrona dóbr jednych nie może się odbywać kosztem naruszania praw innych, co można pośrednio bądź bezpośrednio wywieźć z wielu przepisów Konstytucji RP[158].

Odnosząc się do przetwarzania danych osobowych w celach windykacyjnych, Prezes Urzędu Ochrony Danych Osobowych stoi na stanowisku, że przetwarzanie danych osobowych dłużnika w celu dochodzenia od niego zaspokojenia roszczeń, stanowi prawnie usprawiedliwiony cel, o którym mowa w art. 6 ust. 1 lit. f RODO. Przetwarzanie danych osobowych dłużnika przez fundusz

[154] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz. U. z 2020 r. poz. 1320.
[155] Naczelny Sąd Administracyjny w wyroku z dnia 21 grudnia 2005 r. sygn. akt I OSK 461/05.
[156] DS.440.355.2019.
[157] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz. U. z 2019 r. poz. 1145.
[158] ZSPR.440.105.2019, wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 21 września 2005 r. sygn. akt II SA/WA 1443/05.

w celu dochodzenia roszczeń, nie może być postrzegane jako naruszające prawa i wolności dłużników[159].

Gdyby każdy przypadek przetwarzania danych osobowych dłużnika uznać za godzący w jego prawa i wolności, to doszłoby z jednej strony do niczym nieusprawiedliwionej ochrony podmiotów niewywiązujących się ze swoich zobowiązań, z drugiej natomiast do naruszenia zasady swobody działalności gospodarczej. Dłużnik musi liczyć się z tym, że popadając w zwłokę w spełnianiu zobowiązania, jego prawo do prywatności może zostać ograniczone ze względu na roszczenia dochodzone przez wierzyciela[160]. W pojęciu „dochodzenia roszczeń" mieszczą się zarówno sądowe, jak i pozasądowe działania zmierzające do zaspokojenia wierzytelności przez wierzyciela, w granicach obowiązujących przepisów[161]. Obowiązujące przepisy prawa nie określają katalogu, który przewidywałby możliwe sposoby postępowań służących dochodzeniu roszczeń[162]. Nie budzi również wątpliwości, że w pojęciu „dochodzenia roszczeń" mieści się windykacja należności[163]. Rolą Prezesa Urzędu Ochrony Danych Osobowych nie jest jednak rozstrzyganie sporów wynikających z umów – może on oceniać wyłącznie proces przetwarzania danych osobowych związany z prowadzeniem czynności windykacyjnych wobec dłużnika[164].

W aspekcie działalności funduszy inwestycyjnych w zakresie windykacji nabytych przez nie wierzytelności, istotnym jest, że administrator danych osobowych nie musi osobiście wykonywać czynności związanych z przetwarzaniem danych osobowych. Może w tym celu skorzystać z usług wyspecjalizowanych podmiotów zewnętrznych, zlecając im wykonywanie w tym zakresie, bądź całego procesu przetwarzania danych osobowych, bądź tylko pewnych czynności np. samo zbieranie bądź przechowywanie[165]. Zgodnie z art. 192 ustawy o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[166], zarządzanie sekurytyzowanymi wierzytelnościami funduszu sekurytyzacyjnego przez podmiot inny niż towarzystwo, wymaga uzyskania przez ten podmiot zezwolenia Komisji. Zezwolenie na zarządzanie sekurytyzowanymi wierzytelnościami oznacza także zezwolenie na zarządzanie pulą wierzytelności (ust. 2). Zgodnie zaś z treścią ust. 3

[159] ZSPR.440.1833.2018.
[160] ZSPR.440.1833.2018, ZSPR.440.1849.2019, Naczelny Sąd Administracyjny w wyroku z 21 lutego 2014 r. sygn. akt I OSK 2463/12.
[161] ZSPR.440.1833.2018, ZSPR.440.1849.2019, Naczelny Sąd Administracyjny w wyroku z 10 listopada 2015 r. sygn. akt I OSK 1210/14.
[162] ZSPR.440.1833.2018, ZSPR.440.1849.2018.
[163] ZSPR.440.105.2019, wyrok NSA z dnia 18 marca 2008 r. sygn. akt I OSK 454/07.
[164] ZSPR.440.1849.2019.
[165] ZSPR.440.105.2019.
[166] Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, Dz. U. z 2021 r. poz. 605.

zezwolenie jest udzielane na wniosek podmiotu, o którym mowa w ust. 1. Wskazać również należy, iż przepisem szczególnym regulującym kwestię powierzenia danych osobowych jest art. 193 ww. ustawy. Zgodnie z jego treścią, fundusz sekurytyzacyjny oraz podmiot, z którym towarzystwo zawarło umowę o zarządzanie sekurytyzowanymi wierzytelnościami, mogą zbierać i przetwarzać dane osobowe dłużników sekurytyzowanych wierzytelności jedynie w celach związanych z zarządzaniem wierzytelnościami sekurytyzowanymi[167].

Zgłaszane nieprawidłowości w procesie przetwarzania danych osobowych przez firmy windykacyjne

Skargi na firmy windykacyjne dotyczyły m.in. zasadności pozyskania danych osobowych dłużników. Należy tutaj wskazać, że firma windykacyjna, oprócz działania w imieniu wierzyciela, jako podmiot przetwarzający może sama nabyć wierzytelność w ramach cesji od poprzedniego wierzyciela na podstawie art. 509 Kodeksu cywilnego[168]. Odmienna sytuacja będzie wtedy, gdy firma windykacyjna prowadzi działania windykacyjne na zlecenie innego podmiotu będącego wierzycielem. Wtedy najczęściej firma windykacyjna działa jedynie jako podmiot przetwarzający w oparciu o umowy z wierzycielem, które spełniają wymóg z art. 28 ust. 3 RODO[169].

Skargi na firmy windykacyjne dotyczyły także procederu pozyskiwania przez firmy windykacyjne danych osobowych osób trzecich w celu podejmowania czynności windykacyjnych względem swoich dłużników. Przykładem była sprawa, w której jeden ze skarżonych podmiotów powiadomił małżonkę dłużnika o zamiarze podjęcia czynności względem nieruchomości objętej współwłasnością małżeńską. W przedmiotowej sprawie zawiadomienie to nie było niezbędne z perspektywy dalszych czynności windykacyjnych. Firma windykacyjna również nie przedstawiła uzasadnienia takiego działania, które w ocenie Prezesa Urzędu Ochrony Danych Osobowych stanowiło naruszenie przepisów o ochronie danych osobowych[170].

Za niedopuszczalne Prezes Urzędu Ochrony Danych Osobowych uznał pozyskanie danych osobowych w zakresie numeru telefonu córki dłużnika w celu kontaktu z nim. Firma windykacyjna już w momencie pozyskania numeru telefonu wiedziała, że należy on do osoby trzeciej. Pozyskanie danych osobowych córki dłużnika, z którą firma windykacyjna nie miała żadnych relacji, tylko po to,

[167] ZSPR.440.105.2019.
[168] ZSPR.440.281.2019.
[169] DS.523.480.2020.
[170] ZSPR.440.1432.2019.

by za jej pośrednictwem kontaktować się z dłużnikiem, stanowi nadmierną ingerencję w prawo do prywatności w stosunku do celu, w jakim firma windykacyjna pozyskała dane osobowe[171].

W przedmiotowej sprawie Prezes Urzędu Ochrony Danych Osobowych wskazał ponadto, że przetwarzanie danych w celu realizacji zasady rozliczalności, pozostające w oderwaniu od zasad wskazanych w art. 5 ust. 1 RODO, stanowi w rzeczywistości przetwarzanie w celu obrony przed ewentualnymi roszczeniami, co w ocenie organu stanowi niedopuszczalne przechowywanie danych osobowych „na zapas"[172].

Przykładem innej sprawy było przetwarzanie numeru telefonu przez firmę windykacyjną, pozyskanego od osoby, wobec której nie były prowadzone żadne działania windykacyjne. W ocenie Prezesa Urzędu Ochrony Danych Osobowych w momencie pozyskania przedmiotowego numeru telefonu firma windykacyjna powinna była zbadać, czy numer ten identyfikuje osobę dłużnika, w stosunku do którego prowadzone były czynności windykacyjne. W powyższej sprawie podmiot skarżony z tego obowiązku się nie wywiązał, tj. nie dokonał weryfikacji tożsamości potencjalnego dłużnika, czego skutkiem było bezprawne pozyskanie danych osobowych oraz dalsze ich przetwarzanie. Należy zaznaczyć, że to na firmie windykacyjnej, będącej administratorem danych, spoczywa obowiązek podjęcia odpowiednich działań i wdrożenia mechanizmów identyfikacji, które zagwarantują prawidłowość przetwarzanych danych, oraz zapobiegną pozyskiwaniu danych osób trzecich o tożsamych danych osobowych[173]. W ocenie Prezesa Urzędu proces przetwarzania numeru telefonu przez firmy windykacyjne staje się niedopuszczalny w momencie pozyskania przez nie informacji, iż stanowi on dane osobowe osoby trzeciej, niebędącej dłużnikiem[174].

Za dopuszczalne w świetle przepisów o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych uznał udostępnienie danych osobowych dłużników przez firmy windykacyjne w ramach prowadzonych względem nich czynności windykacyjnych na stronach internetowych w ramach tzw. giełd wierzytelności. Przetwarzanie to ma oparcie w art. 6 ust. 1 lit. f RODO[175] i jest dopuszczalne, np. w przypadku zawarcia pomiędzy firmą windykacyjną a podmiotem prowadzącym stronę internetową umowy spełniającej wymogi z art. 28 ust. 3 RODO[176]. Dłużnik musi liczyć się z tym, że popadając w zwłokę w spełnieniu zobowiązania, jego prawo do prywatności może zostać

[171] DS.523.3803.2020.
[172] DS.523.3803.2020.
[173] DS.523.1123.2020.
[174] DS.523.657.2020.
[175] ZWOS.440.4801.2019.
[176] ZSPR.440.536.2019.

ograniczone ze względu na dochodzenie przez wierzyciela należnych mu kwot. W przeciwnym przypadku mogłoby dojść do sytuacji, w której dłużnik, powołując się na prawo do ochrony danych osobowych (prawo do prywatności), skutecznie uchylałby się od spoczywającego na nim obowiązku spełnienia świadczenia i w konsekwencji ograniczyłby (wyłączył) prawo wierzyciela do uzyskania należnej mu zapłaty. Powołanie się na prawo do ochrony danych osobowych ograniczałoby też przewidziane szczególnymi przepisami prawo do zbycia wierzytelności czy podejmowania dalszych działań w sprawie ich odzyskania[177]. Dodatkowo ujawnienie na stronie internetowej danych osobowych dłużnika w zakresie jego imienia i nazwiska oraz nazwy ulicy i miejscowości, lecz bez numeru nieruchomości oraz wysokości zadłużenia, stanowiło ujawnienie jedynie części jego danych osobowych niezbędnych do skonkretyzowania wierzytelności w celu jej sprzedaży. Takie działanie należy uznać za zgodne z określoną w art. 5 ust. 1 lit. c RODO zasadą minimalizacji[178].

W przypadku, jeśli firma windykacyjna, udostępniając dane osobowe na rzecz podmiotu prowadzącego stronę internetową, sama działa jako podmiot przetwarzający, należy również uwzględnić art. 28 ust. 4 RODO. Zgodnie z jego brzmieniem, jeżeli do wykonania – w imieniu administratora – konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym[179].

Inne zgłaszane nieprawidłowości w procesie przetwarzania danych osobowych przez podmioty sektora finansowego oraz podmioty z nim związane

Prezes Urzędu Ochrony Danych Osobowych rozpatrywał również skargę na udostępnienie danych podmiotowi celem zawarcia umowy leasingu.

Organ stanął wówczas na stanowisku, że do legalnego przetwarzania danych osobowych w związku z zawarciem takiej umowy może dochodzić wyłącznie w przypadku, gdy przyszła strona umowy jednoznacznie wyrazi chęć jej zawarcia. W rozpatrywanej sprawie Prezes Urzędu Ochrony Danych Osobowych uznał, że zawarcia umowy w zakresie poszukiwania ofert umowy leasingu nie

[177] DS.523.1276.2020.
[178] DS.523.1276.2020.
[179] DS.523.1267.2020.

można uznać za jednoznaczne z wyrażeniem woli zawarcia umowy o leasing z konkretnym podmiotem oferującym tę usługę[180].

Przetwarzanie danych osobowych w sektorze telekomunikacji

Udostępnienie danych osobowych podmiotom nieuprawnionym w wyniku incydentów bezpieczeństwa

Przedmiotowe udostępnienie zachodziło najczęściej w wyniku błędów administratorów[181] lub na skutek ataków hackerskich[182].

Powyższe błędy polegały m.in. na: 1) wprowadzeniu w systemie adresu poczty elektronicznej osoby Skarżącej do niewłaściwego konta; 2) wprowadzeniu w systemie, w miejscu przeznaczonym na adres, oprócz adresu także serię i numer dowodu osobistego osoby Skarżącej, co skutkowało nadrukowaniem na kopercie zawierającej korespondencję listowną także ww. danych osobowych; 3) wprowadzeniu dyspozycji karty SIM na koncie Skarżącej, zamiast na koncie abonenta obsługiwanego bezpośrednio po osobie Skarżącej; 4) błędnym zweryfikowaniu osoby podającej się za Skarżącą. W powyższych postępowaniach organ udzielił administratorom upomnień.

Realizacja przez podmioty sektora telekomunikacyjnego obowiązku informacyjnego, wynikającego z art. 15 RODO

W jednej z rozpatrywanych skarg Skarżący, powołując się na swoje imię i nazwisko oraz wskazując numer PESEL, zażądał spełnienia wobec niego ww. obowiązku informacyjnego. Operator telekomunikacyjny nie spełnił tego żądania uznając, że złożony przez Skarżącego wniosek nie zawierał danych umożliwiających weryfikację klienta, tj. numeru telefonu lub numeru klienta oraz hasła do usług. W przedmiotowej sprawie Prezes Urzędu Ochrony Danych Osobowych wyraził pogląd, że operator telekomunikacyjny dysponował jednak danymi pozwalającymi na zidentyfikowanie Skarżącego (imię, nazwisko i numer PESEL) i w związku z powyższym administrator nie mógł odmówić spełnienia wobec Skarżącego obowiązku informacyjnego, wynikającego z art. 15 RODO[183].

Nowym trendem w analizowanym okresie sprawozdawczym, który pojawił się w analizowanym 2021 roku, były sprawy dotyczące żądań przez osoby Skarżące od operatorów

[180] ZSPR.440.564.2018.
[181] DS.523.3967.2020, DS.523.3541.2020, DS.523.1991.2020, ZSPR.440.1867.2019, DS.523.1415.2020, DS.523.2705.2020.
[182] DS.523.62.2020, DS.523.63.2020, DS.523.793.2020, DS.523.930.2020.
[183] ZSPR.440.1421.2018.

telekomunikacyjnych spełnienia obowiązku wynikającego z art. 15 ust. 3 RODO w zakresie udostępnienia kopii dynamicznego adresu IP.

W sprawach tych Prezes UODO twierdził, że dynamiczny numer IP stanowi dane osobowe w myśl art. 4 pkt 1 RODO i w związku z tym osoba, której dane dotyczą była uprawniona do otrzymania kopii numeru IP w trybie art. 15 ust. 3 RODO. W żadnym z prowadzonych przed Prezesem Urzędu Ochrony Danych Osobowych postępowań operatorzy telekomunikacyjni nie zrealizowali w terminie określonym w art. 12 ust. 3 RODO żądań osób Skarżących dot. spełnienia wobec nich obowiązku informacyjnego, wynikającego z art. 15 ust. 3 RODO w zakresie udostępnienia dynamicznego adresu IP. Ww. podmioty spełniły powyższy obowiązek dopiero na skutek złożenia skarg do Prezesa Urzędu Ochrony Danych Osobowych w powyższym zakresie – z naruszeniem terminu wskazanego w art. 12 ust. 3 RODO. W związku z powyższym we wszystkich tych postępowaniach Prezes UODO udzielił upomnień operatorom telekomunikacyjnym za spełnienie ww. obowiązku z naruszeniem art. 12 ust. 3 RODO[184].

Przetwarzanie danych osobowych w sektorze ubezpieczeniowym

Udostępnienie przez brokera ubezpieczeniowego danych osobowych podmiotowi nieuprawionemu w celu przyznania odszkodowania

Opisana poniżej skarga dotyczyła wykorzystania przez brokera ubezpieczeniowego danych osobowych Skarżącej pozyskanych w związku ze zgłoszeniem szkody[185].

Osoba wnosząca skargę przekazała urzędowi miasta pismo dotyczące zwrotu poniesionych przez nią kosztów leczenia doznanych na ciele urazów, które poniosła przebywając w miejscach, nad którymi nadzór techniczny sprawuje gmina. Urząd miasta poinformował Skarżącą, że najpierw jej dane osobowe przekazane zostały Brokerowi ubezpieczeniowemu, a następnie właściwemu ubezpieczycielowi. Ustalono, że przedmiotowe dane zostały przekazane przez brokera zakładowi ubezpieczeniowemu, z którym w okresie powstania szkód urząd miasta nie miał zawartej umowy. W związku z tym doszło do nieuprawnionego udostępnienia danych osobowych. Broker

[184] DS.523.5497.2020; DS.523.5701.2020; DS.523.5838.2020; DS.523.6073.2020; DS.523.5698.2020; DS.523.5445.2020; DS.523.5536.2020; DS.523.5425.2020; DS.523.6303.2020.
[185] DS.523.4148.2020.

usprawiedliwiał swoje działanie koniecznością realizacji powinności brokerskich spoczywających na brokerze ubezpieczeniowym, uregulowanych ustawą o dystrybucji ubezpieczeń, a także koniecznością uczynienia zadość obowiązkom kontraktowym, nałożonym na podmiot umową serwisu brokerskiego zawartą z gminą. Wątpliwości dotyczyły ustalenia polisy właściwej w zakresie likwidacji szkody.

Dla rozstrzygnięcia tej sprawy zasadnicze znaczenie miał również fakt, że skarżony podmiot był brokerem ubezpieczeniowym, czyli – stosownie do treści art. 4 ust. 4 ustawy o dystrybucji ubezpieczeń[186] – wykonywał czynności w zakresie dystrybucji ubezpieczeń w imieniu lub na rzecz klienta. W myśl art. 4 ust. 1 pkt 3 ww. ustawy, dystrybucja ubezpieczeń oznacza działalność wykonywaną wyłącznie przez dystrybutora ubezpieczeń, która polega m.in. na udzielaniu pomocy przez pośrednika ubezpieczeniowego w administrowaniu umowami ubezpieczenia lub umowami gwarancji ubezpieczeniowych i ich wykonywaniu, także w sprawach o odszkodowanie lub świadczenie. Broker pozyskał dane osobowe Skarżącej w związku z wystąpieniem przez nią o odszkodowanie z polisy odpowiedzialności cywilnej (OC) gminy, na rzecz którego to podmiotu broker wykonywał czynności brokerskie w oparciu o zawartą umowę serwisu brokerskiego. Powyższe okoliczności pozwoliły na uznanie brokera za administratora.

Przetwarzanie nieprawidłowych danych osobowych w zakresie adresu do korespondencji

Prezes Urzędu Ochrony Danych Osobowych prowadził postępowania administracyjne w sprawach skarg na podmioty zajmujące się działalnością ubezpieczeniową, w których zarzucano dokonanie wysyłki korespondencji na błędny adres[187].

Organ uznał, że skuteczność zarzutu kierowania korespondencji na nieprawidłowy adres uzależniona była od wcześniejszego wystąpienia z żądaniem sprostowania danych, o którym mowa w art. 16 RODO. Ubezpieczyciel nie może czynić samodzielnie ustaleń w zakresie prawidłowości podanego w trakcie zawierania umowy adresu do korespondencji. Obowiązek poinformowania o zmianie adresu spoczywa na osobie, której dane w tym zakresie dotyczą.

Przekazanie danych osobowych na rzecz nieuprawnionej osoby trzeciej

Prezes Urzędu Ochrony Danych Osobowych stanął na stanowisku, zgodnie z którym przekazanie informacji na temat wysokości odszkodowania na rzecz osoby trzeciej, która zbyła

[186] Ustawa z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń, Dz. U. z 2019 r. poz. 1881.
[187] DS.523.5592.2020, DS.523.5593.2020, DS.523.5594.2020, DS.523.5595.2020, DS.523.5597.2020.

wierzytelność wynikającą ze szkody zgłoszonej ubezpieczycielowi w drodze umowy cesji wierzytelności, nie znajduje uzasadnienia w żadnej z przesłanek z art. 6 ust. 1 RODO[188].

W toczącym się postępowaniu Prezes UODO uznał, że informacje o wysokości przyznanej przez ubezpieczyciela kwoty odszkodowania stanowią dane osobowe. Skarżący, na skutek umowy zawartej na podstawie art. 509 § 1 Kodeksu cywilnego, wstąpił w prawa zbywcy wierzytelności, a zatem, zdaniem organu, stał się jedyną osobą występującą z roszczeniem w postępowaniu likwidacyjnym w sprawie szkodowej. Od momentu zawarcia umowy cesji był więc osobą, w majątku której doszło do powstania szkody. Organ uznał, że powoływane w toku postępowania – jako podstawa przekazania danych zbywcy wierzytelności przepisy, tj. art. 14 ust. 3 ustawy o ubezpieczeniach obowiązkowych[189] i art. 29 ust. 5 ustawy o działalności ubezpieczeniowej[190] – nie zastrzegają, aby zakład ubezpieczeń był zobowiązany do informowania właściciela uszkodzonego pojazdu o wysokości przyznanego odszkodowania. Przepisy te wskazują jedynie, że informację taką należy przekazać osobie występującej z roszczeniem. Taką osobą zaś, z uwagi na przedmiot umowy cesji wierzytelności w postępowaniu likwidacyjnym dotyczącym szkody, był wyłącznie Skarżący. Udostępnienie informacji o przyznanej wysokości odszkodowania na rzecz właściciela samochodu w badanej przez organ sprawie uznane zostało za proces niezgodny z prawem.

4.1.5. Postępowania transgraniczne

Prezes Urzędu Ochrony Danych Osobowych w swojej działalności w 2021 roku prowadził nie tylko postępowania krajowe, ale również uczestniczył w prowadzeniu postępowań we współpracy z organami nadzorczymi państw członkowskich Unii Europejskiej. W analizowanym 2021 roku rozpatrzono **142 skargi na podmioty sektora transgranicznego**. Przedmiotem tych postępowań były m.in. sprawy dotyczące przetwarzania danych osobowych przez następujących administratorów:

WhatsApp Ireland Limited

W roku 2021 Prezes Urzędu brał udział w charakterze organu, którego sprawa dotyczy, w wydawaniu decyzji w sprawie WhatsApp Ireland Ltd. przez irlandzki organ nadzorczy – DPC.

Sprawa dotyczyła postępowania z urzędu zainicjowanego przez DPC na skutek licznych sygnałów dotyczących podejrzenia naruszeń RODO przez WhatsApp. Naruszenia dotyczyły m.in. niewypełniania obowiązku informacyjnego wobec osób, których dane dotyczą, przetwarzania

[188] DS.523.3479.2020.
[189] Ustawa z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych, Dz. U. z 2021 r. poz. 854.
[190] Ustawa o działalności ubezpieczeniowej i reasekuracyjnej z dnia 11 września 2015 r., Dz. U. z 2020 r. poz. 895.

numerów telefonu osób, które nie są użytkownikami aplikacji w przypadku, gdy użytkownik aplikacji pozwolił jej na dostęp do kontaktów na swoim urządzeniu, sposobu zabezpieczenia i anonimizacji przetwarzanych danych oraz dzielenia się przez WhatsApp danymi użytkowników z Facebookiem.

DPC wydał w sprawie WhatsAppa decyzję, która nie uwzględniała szeregu mających znaczenie dla sprawy i uzasadnionych sprzeciwów do decyzji, wniesionych przez organy nadzorcze właściwe dla: Niemiec (organ federalny), Badenii-Wirtembergii, Francji, Węgier, Włoch, Niderlandów, Polski oraz Portugalii. Na skutek tego doszło do sporu pomiędzy DPC a ww. organami nadzorczymi. Przedstawiciel Prezesa UODO brał udział w procedurze rozstrzygania tego sporu przez Europejską Radę Ochrony Danych (EROD), w wyniku której doszło do wydania wiążącej decyzji w tej sprawie.

EROD nakazała DPC zmianę decyzji w odniesieniu do zidentyfikowanych naruszeń, obliczania wysokości kary pieniężnej oraz okresu realizacji nakazu przestrzegania przepisów. Zidentyfikowała też dodatkowe braki w informacjach przekazywanych osobom, których dane dotyczą, a które wpływały na ich zdolność zrozumienia, jakie prawnie uzasadnione interesy były realizowane w związku z przetwarzaniem. Wobec powyższego EROD nakazała DPC uwzględnienie w swojej decyzji stwierdzenia naruszenia art. 13 ust. 1 lit. d RODO.

Ponadto EROD wyjaśniła, że doszło do naruszenia zasady przejrzystości zapisanej w art. 5 ust. 1 lit. a RODO, chociaż podkreślono także, że nie każde naruszenie art. 12, 13 lub 14 RODO musi pociągać za sobą naruszenie wspomnianej zasady art. 5 ust. 1 lit. a RODO.

W odniesieniu do gromadzenia przez WhatsApp danych osób niebędących użytkownikami – gdy użytkownicy decydują się na korzystanie z funkcji synchronizacji kontaktów – EROD stwierdziła, że procedura lossy-hashingu stosowana przez WhatsApp nie prowadziła do anonimizacji zgromadzonych danych osobowych, a jedynie do ich pseudonimizacji i jest ona odwracalna, przez co WhatsApp przetwarza dane osób, które nie są użytkownikami jego aplikacji.

W odniesieniu do nałożonej kary pieniężnej i jej obliczenia, DPC uwzględnił tylko obroty WhatsAppa, przez co wysokość kary była znacząco zaniżona. W tym przypadku EROD stwierdziła, że przy obliczaniu podstawy dla wymierzenia administracyjnej kary pieniężnej należy uwzględnić skonsolidowany obrót wszystkich Spółek wchodzących w skład jednolitej jednostki gospodarczej (w tym przypadku Facebook Inc.) w rozumieniu art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej, a także należy wziąć pod uwagę datę wydania ostatecznej decyzji, jako podstawę wyznaczenia poprzedniego roku obrotowego, mającego znaczenie dla kalkulacji administracyjnej kary pieniężnej. EROD stwierdziła również, że DPC musi podczas kalkulacji administracyjnej kary pieniężnej uwzględnić wszystkie naruszenia, nie tylko naruszenie najpoważniejsze. Nakazała więc

DPC oszacować ponownie pieniężną karę administracyjną i zwiększyć jej wysokość tak, aby była ona skuteczna, proporcjonalna i odstraszająca. Po zmianie wysokości administracyjnej kary pieniężnej, wyniosła ona ostatecznie 225 milionów EUR.

W odniesieniu do terminu wyznaczonego dla WhatsAppa na dostosowanie się do treści decyzji, EROD stwierdziła, że najważniejsze jest zapewnienie zgodności z wymogami w zakresie przejrzystości w możliwie najkrótszym czasie. W związku z tym DPC musiał zmienić wyznaczony wcześniej termin sześciomiesięczny na okres trzech miesięcy.

Wiążąca decyzja została skierowana do organów nadzorczych, których sprawa dotyczyła, a DPC – jako organ wiodący – przyjął swoją krajową decyzję na podstawie decyzji EROD. Decyzja krajowa, wraz z załączoną do niej decyzją EROD, została WhatsApp doręczona.

Facebook Ireland Limited (obecnie Meta Platforms Ireland Limited)

Prezes UODO za pośrednictwem systemu IMI[191] uczestniczył w opiniowaniu projektów irlandzkiego organu nadzorczego – DPC, dotyczących różnego rodzaju naruszeń ochrony danych osobowych przez Facebook Ireland Limited (obecnie Meta Platforms Ireland Limited) z siedzibą w Dublinie, jako administratora danych związanego z platformą Facebook oraz Instagram, w ramach mechanizmu współpracy pomiędzy organami nadzorczymi państw członkowskich Unii Europejskiej.

Projekty decyzji przekazywane były zainteresowanym organom nadzorczym w ramach sformalizowanej procedury. Przedstawiono w nich uwagi i w stosownych przypadkach zgłoszenia mające znaczenie dla sprawy i uzasadnione sprzeciwy wobec proponowanej decyzji irlandzkiego organu nadzorczego w danej sprawie. Sprawy dotyczyły zarówno postępowań skargowych, jak i postępowań wszczętych z urzędu.

Prezes UODO otrzymał w 2021 roku projekt decyzji irlandzkiego organu nadzorczego w związku z prowadzonym dochodzeniem wszczętym z urzędu. Dotyczyło ono stwierdzonych 12 naruszeń ochrony danych osobowych spowodowanych różnego rodzaju błędami w oprogramowaniu, zgłoszonych w okresie od 7 czerwca 2018 r. do 4 grudnia 2018 r. W projekcie decyzji zawarte zostały informacje z przeprowadzonego dochodzenia przez irlandzki organ nadzorczy wraz z dokładnym opisem każdego z 12 naruszeń bezpieczeństwa danych, które łącznie dotyczyły 4.750,279 użytkowników z całej Unii Europejskiej (w tym także polskich użytkowników).

[191] IMI – system wymiany informacji na rynku wewnętrznym.

Zakres dochodzenia obejmował badanie zgodności naruszeń z art. 5, 24, 25, 28, 29, 32, 33 i 34 RODO. Z tytułu naruszenia art. 5 ust. 2 RODO, irlandzki organ nadzorczy zaproponował nałożenie na Facebook Ireland Limited grzywny administracyjnej w wysokości nie mniejszej niż 9 mln EUR i nie większej niż 17 mln EUR. Zdaniem DPC, taka wysokość spełniłaby wymóg zawarty w art. 83 ust.1 RODO, aby każda grzywna była skuteczna, proporcjonalna i odstraszająca w każdym indywidualnym przypadku.

W związku z powyższym, Prezes Urzędu Ochrony Danych Osobowych 15 września 2021 r. wniósł mający znaczenie dla sprawy i uzasadniony sprzeciw (łącznie 4 sprzeciwy) do projektu decyzji dotyczącej naruszeń ochrony bezpieczeństwa danych przez Facebook Ireland Limited.

Sprzeciwy dotyczyły następujących kwestii:

1. stwierdzenia jednego zbiorczego naruszenia w okresie od 7 czerwca do 4 grudnia 2018 r. zamiast stwierdzenia naruszenia w odniesieniu do każdego z naruszeń ochrony danych z osobna (wraz z wskazaniem okresu trwania tego naruszenia);
2. niestwierdzenia naruszeń RODO (dot. art. 25 ust. 2, art. 32 ust. 1 i ust. 2, art. 33 ust. 1);
3. wysokości administracyjnej kary pieniężnej;
4. braku informacji o prawie do skutecznego środka ochrony prawnej.

Irlandzki organ nadzorczy, za pośrednictwem IMI w ramach dobrowolnej wzajemnej pomocy, odniósł się do sprzeciwów wniesionych przez Prezesa UODO wyjaśniając, że zmiana decyzji w zakresie stwierdzenia podnoszonych przez polski organ nadzorczy naruszeń tj. (art. 25 ust. 2, art. 32 ust. 1 i ust. 2, art. 33 ust. 1 RODO) nie jest możliwa ze względów proceduralnych oraz ze względu na zakres prowadzonego przez irlandzki organ nadzorczy dochodzenia. Dotyczyło to również sprzeciwu wobec administracyjnej kary pieniężnej, której proponowany zakres zdaniem irlandzkiego organu jest skuteczny, proporcjonalny i odstraszający w odniesieniu do indywidualnych okoliczności tego konkretnego dochodzenia. Irlandzki organ nadzorczy podkreślił również, że nie jest w stanie zmienić projektu decyzji w kwestii stwierdzenia każdego z naruszeń z osobna, ponieważ faktycznie wymagałoby to całkowitej restrukturyzacji i przeredagowania projektu decyzji. Irlandzki organ nadzorczy odniósł się także do sprzeciwu polskiego organu nadzorczego dotyczącego braku odniesienia do skutecznego środka odwoławczego od decyzji i poinformował, że przekazuje tę informację adresatowi lub adresatom swoich decyzji w drodze korespondencji towarzyszącej decyzji.

Inne organy nadzorcze również brały udział w opiniowaniu niniejszego projektu decyzji, np. niemiecki organ nadzorczy właściwy dla kraju związkowego Hamburg, który 15 września 2021 roku wniósł również mający znaczenie dla sprawy i uzasadniony sprzeciw do omawianego projektu decyzji wydanej przez Irlandię. Warto również wspomnieć o Holandii, Węgrach oraz Francji, które zgłosiły uwagi w komentarzu lub poprosiły o dodatkowe wyjaśnienia od irlandzkiego organu nadzorczego.

Prezes UODO uznał, że polubowne rozstrzygnięcie sprawy i niezgłaszanie tym samym żadnych dalszych uwag będzie uzasadnione. Irlandzki organ nadzorczy przekazał szczegółowe wyjaśnienia na podniesione w sprzeciwie polskiego organu nadzorczego wątpliwości. Brak akceptacji stanowiska irlandzkiego organu nadzorczego skutkowałby koniecznością zainicjowania sporu z irlandzkim organem nadzorczym do rozstrzygnięcia przed EROD, co w niniejszej sprawie nie było koniecznym i uzasadnionym rozwiązaniem.

Irlandzki organ ochrony danych wszczął postępowanie z urzędu i prowadził dochodzenie w ramach mechanizmu współpracy pomiędzy organami nadzorczymi państw członkowskich Unii Europejskiej, uczestniczących w procesie zmierzającym do wydania ostatecznej decyzji.

Vinted UAB

Prezes Urzędu Ochrony Danych Osobowych otrzymał w 2021 roku wiele sygnałów (skarg, zawiadomień i połączeń na infolinię) dotyczących wymagania przez operatora vinted.pl (platformy oraz powiązanej z nią aplikacji), którym jest Vinted UAB, przesłania zeskanowanego dowodu tożsamości, pod rygorem zablokowania konta z płatnościami. Sygnały te odnosiły się również do nieprawidłowości związanych z uzyskiwaniem informacji o podstawie prawnej gromadzenia tych dokumentów i innych informacji wymaganych przepisami rozporządzenia 2016/679. Wyrażano również wątpliwości, co do sposobu ich przekazywania i zapewnienia ochrony danych.

W związku z powyższym Prezes UODO złożył wniosek do litewskiego organu nadzorczego, za pośrednictwem systemu IMI, o wzajemną pomoc w sprawie wszczęcia postępowania z urzędu w sprawie Vinted UAB. Wniosek zawierał informacje o nieprawidłowościach oraz wskazanie o podjęcie działań co najmniej w zakresie:

1) ustalenia podstawy prawnej przetwarzania danych osobowych przez operatora platformy/aplikacji vinted.pl, w szczególności zawartych w polskich dowodach osobistych, tj. imię, nazwisko, nazwisko rodowe, wizerunek, imiona rodziców, podpis, data urodzenia, płeć, numer i seria dowodu, PESEL, miejsce urodzenia, adres zameldowania (w przypadku starszych dokumentów), kolor oczu, wzrost;

2) zbadania zakresu i rodzaju przetwarzanych danych osobowych, a także sposobu oraz celu zbierania i udostępniania danych osobowych;

3) ustalenia sposobu dopełnienia obowiązków administratora wynikających z art. 12, art. 13 ust. 1 i 2 oraz art. 14 ust. 1, 2 i 3 rozporządzenia 2016/679;

4) zbadania sposobu realizacji praw osób, których dane dotyczą, wynikających z art. 15–22 rozporządzenia 2016/679;

5) zbadania, czy administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych objętych ochroną (art. 32, art. 24 ust. 1 i 2 rozporządzenia 2016/679).

Wniosek o wzajemną pomoc został zaakceptowany przez litewski organ nadzorczy. Prezes UODO kontynuował wymianę informacji dotyczących praktyk Spółki Vinted UAB z litewskim organem nadzorczym. W związku z otrzymaniem znacznej liczby skarg dotyczących serwisu sprzedażowego ubrań online vinted.com, prowadzonego przez Spółkę Vinted UAB, organy nadzorcze z Francji, Litwy i Polski podjęły współpracę w celu zbadania zgodności tej strony z przepisami rozporządzenia 2016/679. Utworzono w tym celu specjalny zespół zadaniowy, wspierany przez Europejską Radę Ochrony Danych, którego pierwsze spotkanie odbyło się 8 listopada 2021 r.

Celem powołanego specjalnego zespołu zadaniowego jest przede wszystkim wsparcie litewskiego organu nadzorczego i pomoc w wypracowaniu wspólnej praktyki w zakresie skarg na nieprawidłowości w procesie przetwarzania danych osobowych przez litewską Spółkę Vinted UAB. Organy ochrony danych koncentrują się w szczególności na następujących kwestiach: wymaganiu przez operatora strony internetowej przesłania skanu dowodu tożsamości w celu odblokowania środków otrzymanych ze sprzedaży na koncie użytkownika oraz związanej z tym podstawie prawnej, a także na procedurze i kryteriach blokowania konta oraz odpowiednich okresach przechowywania danych.

Wymiana informacji i wzajemna pomoc

W ramach prowadzonych postępowań transgranicznych, Prezes Urzędu Ochrony Danych Osobowych często zobowiązany był do wielokrotnej wymiany informacji i stanowisk celem doprowadzenia do zakończenia prowadzonych spraw.

Przykładem opisującym taką współpracę i wymianę informacji, w toku rozpatrywania spraw między zaangażowanymi w sprawę organami nadzorczymi, była skarga dotycząca niedopełnienia obowiązku informacyjnego oraz przetwarzania nadmiernej ilości danych w postaci kopii dowodu

osobistego przez administratora z siedzibą w Republice Czeskiej i żądanie ustalenia, w jaki sposób administrator zabezpiecza dane osobowe, wezwanie do usunięcia danych osobowych Skarżącego (w tym utrwalonej kopii jego dowodu osobistego) oraz wezwanie do zaprzestania naruszania przepisów RODO.

Prezes UODO przekazał skargę czeskiemu organowi nadzorczego za pośrednictwem IMI, który w odpowiedzi poinformował, iż przesłał do administratora pismo o potencjalnym naruszeniu RODO i przeprowadził kontrolę w jego siedzibie. Ponadto czeski organ nadzorczy poinformował, iż skarga pochodząca od obywatela polskiego wydaje się być indywidualna, a świadczenie usług przez administratora nie jest celowo ukierunkowane na obcokrajowców. Przetwarzanie odbywa się w całości w Czechach, dlatego czeski organ nadzorczy uznał, że sprawa nie ma charakteru transgranicznego, ponieważ nie wpływa znacznie na osoby, których dane dotyczą, poza Czechami.

W reakcji na powyższe stanowisko, Prezes UODO stwierdził, że jeżeli administrator przetwarzał lub nadal przetwarza dane obywateli polskich i stosuje ten sam sposób przetwarzania wobec obywateli innych państw członkowskich (np. obywateli Czech), to przetwarzanie ma charakter transgraniczny, ponieważ znacznie wpływa na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim. W odpowiedzi czeski organ nadzorczy poinformował, że administrator w tym przypadku działał tylko w jednym państwie członkowskim i nie oferował swoich usług w innych państwach członkowskich. Nie był więc spełniony warunek znacznego wpływu na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim (art. 4 pkt 23 lit. b RODO). RODO nie mówi o wpływie na osoby z innego państwa członkowskiego, ale o wpływie na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, co stanowi różnice.

W odpowiedzi Prezes UODO podniósł, że ponieważ dane Skarżącego były przetwarzane przez administratora po jego powrocie na terytorium Polski, przetwarzanie miało jednak charakter transgraniczny – odbywało się w ramach działalności pojedynczej jednostki organizacyjnej administratora w Unii Europejskiej i znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą w więcej niż jednym państwie członkowskim. Prezes UODO zaproponował, aby rozpatrzyć tę skargę jako sprawę lokalną zgodnie z art. 56 ust. 2 RODO, mając na uwadze fakt, że przetwarzanie w tej konkretnej sprawie może znacznie wpływać wyłącznie na Skarżącego.

W odpowiedzi czeski organ nadzorczy przedstawił protokół kontroli stwierdzający, co następuje: (1) administrator nie uzyskiwał od swoich klientów pisemnej zgody na przetwarzanie ich danych osobowych otrzymanych w wyniku skanowania dokumentu tożsamości; (2) poprzez skanowanie dokumentów tożsamości administrator naruszył w art. 7 ust. 1 RODO i przetwarzał dane

osobowe niezgodnie z prawem, ponieważ nie był w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na takie przetwarzanie; (3) administrator naruszył art. 5 ust. 1 lit. c RODO; (4) administrator naruszył art. 13 rozporządzenia 2016/679, ponieważ nie udowodnił, że poinformował swoich klientów o przetwarzaniu ich danych osobowych na piśmie w swojej siedzibie lub na swojej stronie internetowej; (5) ze względu na fakt, że nie poinformował klientów o możliwości złożenia takich żądań w związku z przetwarzaniem ich danych osobowych, czeski organ nadzorczy stwierdził, że administrator naruszył swoje obowiązki wynikające z art. 15–21 RODO; (6) administrator prawidłowo zabezpieczał dane klientów.

Na podstawie dokonanych ustaleń czeski organ nadzorczy wydał rozstrzygnięcie, w ramach którego nałożył na administratora karę pieniężną w wysokości 10 000 CZK oraz skorzystał z następujących środków naprawczych: (1) wydał nakaz zapewnienia zgodności operacji przetwarzania danych z RODO; (2) oraz nakaz usunięcia wszystkich skanów dokumentów tożsamości klientów, chyba że administrator jest w posiadaniu odpowiednio udzielonej zgody.

Czeski organ nadzorczy nadal podtrzymał, iż przetwarzanie nie miało charakteru transgranicznego. Transgraniczne przetwarzanie musi ze względu na swój charakter znacząco wpływać, z terytorium Republiki Czeskiej, na osoby, których dane dotyczą, w innym państwie członkowskim i musi być przetwarzaniem, które nie polega jedynie na wizycie w innym państwie oraz jednorazowym skorzystaniu z usług.

W ramach postępowania z urzędu przeprowadzonego przez czeski organ nadzorczy ustalono, że administrator zrealizował wszystkie żądania Skarżącego zawarte w treści skargi.

Prezes UODO przyjął interpretację czeskiego organu nadzorczego, iż przetwarzanie nie ma charakteru transgranicznego, przez co do niniejszej sprawy nie ma zastosowania mechanizm wzajemnej współpracy przewidziany w art. 60 RODO. Sprawę zakończono pismem do osoby Skarżącej informującym o efektach rozpatrywania skargi przez czeski organ nadzorczy zgodnie z art. 77 ust. 2 RODO.

4.2. Zawiadomienie o podejrzeniu popełnienia przestępstwa

W analizowanym 2021 roku Prezes Urzędu Ochrony Danych Osobowych skierował do organów powołanych do ścigania przestępstw **2 zawiadomienia o podejrzeniu popełnienia przestępstwa przez podmioty odpowiedzialne za przetwarzanie danych osobowych[192].**

[192] DS.523.6635.2020 (zakończona jako sprawa o sygnaturze DOL.023.91.2021), DS.523.3336.2021.

Jedno z tych zawiadomień dotyczyło podejrzenia popełnienia przestępstwa polegającego na niedopuszczalnym przetwarzaniu danych osobowych, poprzez zamieszczenie przez użytkownika serwisu społecznościowego Facebook na łamach tego portalu prywatnych adresów miejsca zamieszkania osób pełniących funkcje publiczne, tj. przestępstwa określonego w art. 107 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[193].

Dane osób pełniących funkcje publiczne lub działających w przestrzeni publicznej, w określonym zakresie (imię i nazwisko) są jawne. Jednak informacje o miejscu ich zamieszkania należą już do sfery ich prywatności, co potwierdza orzecznictwo sądów administracyjnych[194]. Udostępnienie w mediach społecznościowych adresów zamieszkania ww. osób było działaniem nie tylko naruszającym ich prywatność, ale przede wszystkim rodzącym ryzyko naruszenia elementarnych interesów życiowych ich rodzin, poprzez chociażby możliwe akty przemocy i agresji wymierzone w ich życie i zdrowie.

Wobec braku ustawowych przesłanek do ujawniania danych o miejscu zamieszkania, uznano takie działanie za niedopuszczalne i ingerujące w sferę prywatności ww. osób, jak również osób z nimi zamieszkujących. Zgodnie z art. 107 ust. 1 ustawy o ochronie danych osobowych, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Działanie użytkownika serwisu społecznościowego Facebook polegające na udostępnieniu na łamach ww. portalu prywatnych adresów miejsca zamieszkania osób pełniących funkcje publiczne, należy uznać za bezprawne, co wyczerpuje znamiona czynu zabronionego, o którym mowa w art. 107 ustawy o ochronie danych osobowych.

Z kolei skarga z dnia 24 maja 2021 r. stanowiła zawiadomienie o nieprawidłowościach w procesie przetwarzania danych osobowych klientów jednego z podmiotów sektora finansowo-ubezpieczeniowego, których dokumenty znalazł na swojej posesji Skarżący.

Skarżący wskazał, że w trakcie prac porządkowych na swojej posesji znalazł dokumenty należące do ww. podmiotu, tj. kserokopie formularzy zeznań podatkowych, umowy leasingu, oświadczenie o stanie zobowiązań, faktury VAT, dokumenty skierowane do ww. podmiotu lub wystawione przez ten podmiot. Skarżący twierdzi, że dokumenty te pozostawiła osoba będąca pracownikiem ww. podmiotu.

[193] Dz. U. z 2019 r. poz. 1781.
[194] Zob. wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 13 maja 2019 r. II SA/Kr 97/19, LEX nr 2684058.

W związku z tym, w dniu 3 grudnia 2021 r. Prezes Urzędu Ochrony Danych Osobowych skierował zawiadomienie do Prokuratury Rejonowej w Końskich o możliwości popełnienia przestępstwa z art. 276 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny[195]. W dniu 3 lutego 2022 r. do UODO wpłynęło postanowienie Prokuratury Rejonowej w Końskich o odmowie wszczęcia dochodzenia wskazujące, że w poniższej sprawie doszło do przedawnienia karalności.

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[196]. 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 2021 r. Prezes Urzędu Ochrony Danych Osobowych (UODO) przeprowadzał czynności kontrolne w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych **w dwudziestu dwóch 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)[197]. Kontrole były przeprowadzane w rezultacie powzięcia przez Prezesa UODO informacji o występujących nieprawidłowościach oraz w ramach kontroli okresowych, wynikających z realizacji obowiązków ustawowych.

Ze względu na sytuację epidemiczną, która wystąpiła na początku 2020 r. i trwała również w 2021 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[198], działania Prezesa UODO o charakterze kontrolnym musiały uwzględniać wyżej wskazane okoliczności. Zaistniała sytuacja determinowała zatem liczbę i sposób prowadzenia kontroli.

[195] Dz. U. z 2020, poz. 1444 z późn. zm.
[196] Dz. U. z 2019 r. poz. 1781.
[197] Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.
[198] Dz. U. z 2021 r. poz. 2095 z późn. zm.

W analizowanym 2021 roku przeprowadzone zostały czynności kontrolne przestrzegania przepisów dotyczących ochrony danych osobowych między innymi w jednostkach organizacyjnych samorządu terytorialnego – jak urzędy miasta, uczelni wyższej, Krajowej Izbie Rozliczeniowej, fundacji; w podmiotach sektora prywatnego, w tym bankach, podmiotach oferujących usługi poczty elektronicznej za pośrednictwem portali internetowych, podmiotach świadczących usługi pocztowe – operatorzy pocztowi.

5.1. Jednostki organizacyjne samorządu terytorialnego

Prezes UODO przeprowadził dwie kontrole w zakresie przetwarzania danych osobowych w związku ze stosowaniem przez urzędy miasta aplikacji wykrywającej rozbieżności w deklaracjach określających wysokość opłaty za gospodarowanie odpadami komunalnymi[199]. Powyższe kontrole miały na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Czynności kontrolne koncentrowały się na weryfikacji sposobów, w jaki administratorzy danych osobowych zapewniają zachowanie poufności danych oraz ustaleniu, czy nie wykorzystują ich w innych celach, niż te, dla których zostały zebrane. Zakres przeprowadzonych kontroli obejmował m.in. podstawę prawną przetwarzania danych osobowych, źródło ich pozyskania, zakres i rodzaj przetwarzanych danych osobowych, sposób wypełnienia obowiązków administratora danych wynikających z art. 13 i art. 14 rozporządzenia 2016/679. Ponadto dokonano kontroli systemów informatycznych wykorzystywanych do przetwarzania danych osobowych, w tym w związku ze stosowaniem aplikacji wykrywającej rozbieżności w deklaracjach określających wysokość opłaty za gospodarowanie odpadami komunalnymi oraz ustalono, w jakim zakresie dane były pozyskiwane, gdzie je przekazywano i jak długo archiwizowano. Dokonane w toku kontroli ustalenia były następnie analizowane pod kątem oceny zgodności przetwarzania danych z przepisami rozporządzenia 2016/679.

W analizowanym okresie sprawozdawczym, Prezes UODO, działając w oparciu o art. 58 ust. 1 lit. a i lit. e rozporządzenia 2016/679, na podstawie zgłoszenia nieprawidłowości, zwrócił się także do Prezydenta jednego z miast o złożenie wyjaśnień w sprawie nieprawidłowości związanych z przetwarzaniem danych osobowych mieszkańców i innych osób występujących w bazach danych

[199] Sygn. akt DKN.5112.4.2021, DKN.5112.3.2021.

urzędu miejskiego[200]. Zasygnalizowane nieprawidłowości odnosiły się do funkcjonowania systemu teleinformatycznego służącego do prowadzenia ewidencji ludności i polegały na braku zapewnienia rozliczalności przy wykonywaniu operacji przetwarzania danych osobowych, w szczególności zaś przy przeglądaniu danych osobowych mieszkańców przez pracowników zatrudnionych w tym urzędzie.

W oparciu o nadesłane wyjaśnienia Prezes UODO poczynił ustalenia, że dostęp do systemu teleinformatycznego, o którym wyżej mowa, oraz do bazy PESEL posiadali wyłącznie uprawnieni pracownicy, którym zostały udzielone upoważnienia do przetwarzania danych osobowych, zgodnie z zakresem obowiązków. Czynności wykonywane w systemie teleinformatycznym, w tym polegające na wyszukiwaniu, wynikały z zakresu obowiązków i musiały być wykonywane na formalny wniosek osób, których dane dotyczą, stosownie do treści art. 11 ustawy z dnia 24 września 2010 r. o ewidencji ludności[201]. Ponadto ustalono, że użytkownicy mieli przydzielone imienne loginy, hasła do komputerów oraz zabezpieczenia zgodne z wdrożoną polityką bezpieczeństwa. Każdy użytkownik systemu teleinformatycznego posiadał imienny identyfikator, hasło i przydzielone uprawnienia, zgodnie z zakresem obowiązków. Dostęp do bazy PESEL, tj. części ogólnopolskiego Systemu Rejestrów Państwowych (SRP) mieli jedynie użytkownicy z imiennymi kartami dostępu. Karty te były wydawane na pisemny wniosek kierowany do Kancelarii Prezesa Rady Ministrów. Każdy z użytkowników Systemu SRP posiadał nadane uprawnienia zgodne z zakresem obowiązków.

Prezydent Miasta, jako administrator danych osobowych, prowadzi rejestr czynności przetwarzania danych osobowych, stanowiący załącznik do obowiązującej w urzędzie miejskim polityki ochrony danych osobowych. Na podstawie nadesłanych do UODO wyjaśnień ustalono, że przeprowadzona została analiza ryzyka w związku z przetwarzaniem danych osobowych, w tym także w systemie teleinformatycznym służącym do prowadzenia ewidencji mieszkańców. W systemie tym odnotowywane były informacje dotyczące daty, opisu czynności oraz użytkownika dokonującego modyfikacji danych. Przy przeglądaniu karty osobowej danego mieszkańca widoczna była również historia zmian danych z określeniem daty, zakresu zmian oraz użytkownika, który tych zmian dokonał. Dodatkowo w systemie uruchomiona została funkcjonalność rejestrowania czynności przeglądania karty mieszkańca. Rejestr ww. czynności zawierał login użytkownika oraz datę przeglądania karty mieszkańca. W świetle dokonanych ustaleń brak było podstaw do wszczęcia postępowania administracyjnego.

[200] Sygn. DKN. 5110.15.2021.
[201] Dz. U. z 2021 r. poz. 510 z późn. zm.

5.2. Uczelnia wyższa

Prezes UODO przeprowadził kontrolę przetwarzania danych osobowych w związku ze zgłoszonym przez uczelnię wyższą naruszeniem ochrony danych osobowych[202].

Naruszenie to polegało na odblokowaniu dostępu zdalnego (poprzez wyszukiwarkę Google) do struktury katalogowej serwera realizującego aplikacyjne wsparcie dla administracji uczelni[203]. W wyniku błędu automaty indeksujące wyszukiwarki Google mogły zaindeksować wszystkie dostępne pliki obecne na serwerze. Zaistniały błąd był wynikiem awarii serwera, zaś usuwanie awarii w okresie nasilonych prac, wynikających z końca roku akademickiego i obsługi trwającego procesu rekrutacji, miało wpływ na zaistnienie krytycznego błędu ludzkiego. W wyniku zaistniałego zdarzenia doszło do naruszenia poufności i integralności danych osobowych takich jak: imię i nazwisko, data urodzenia, numer rachunku bankowego, adres zamieszkania, numer ewidencyjny PESEL, adres e-mail, seria i numer dowodu osobistego, numer telefonu. Kategoria osób, których dotyczyło naruszenie, to: pracownicy, studenci, kandydaci na studia, klienci podmiotu publicznego. Zakresem kontroli objęto przede wszystkim okoliczności zgłoszonego naruszenia ochrony danych osobowych, podjęte działania po wykryciu naruszenia, zaimplementowanie odpowiednich środków technicznych i organizacyjnych, przeprowadzoną ocenę skutków dla ochrony danych oraz analizę ryzyka naruszenia praw lub wolności osób fizycznych, których danych dotyczyło to naruszenie. Przeprowadzono kontrolę systemów informatycznych, w tym pomieszczeń serwerowni, sprawdzając również zabezpieczenia fizyczne pomieszczeń strategicznych dla bezpieczeństwa danych osobowych. W postępowaniu kontrolnym w niniejszej sprawie nie stwierdzono naruszenia przepisów dotyczących zabezpieczenia danych osobowych.

5.3. Krajowa Izba Rozliczeniowa S.A.

Prezes UODO, w ramach wypełniania nałożonych obowiązków wynikających z art. 119 zg ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa[204], przeprowadził okresową kontrolę przetwarzania danych osobowych przez Krajową Izbę Rozliczeniową S.A. w związku z realizacją zadań, o których mowa w dziale IIIB Ordynacji podatkowej.

Zasadniczym celem kontroli była analiza i porównanie stanu faktycznego do okresu, w którym Prezes UODO przeprowadził poprzednią kontrolę w Krajowej Izbie Rozliczeniowej S.A. w zakresie

[202] Sygn. akt DKN.5130.9331.2021.
[203] Sygn. akt DKN.5112.33.2021.
[204] Dz. U. z 2021 r. poz. 1540.

ochrony danych osobowych przy wypełnianiu wspomnianych wyżej obowiązków[205]. Ustalono, że Krajowa Izba Rozliczeniowa S.A. w ramach przetwarzania danych osobowych wypełnia obowiązki administratora nałożone przepisami rozporządzenia 2016/679, w tym wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami tego aktu prawnego. W ramach funkcjonowania systemu teleinformatycznego izby rozliczeniowej (STIR) dokonywane były okresowe przeglądy i aktualizacje zabezpieczeń. Osobom, które mają dostęp do danych osobowych przetwarzanych w STIR, zostały nadane odpowiednie uprawnienia systemowe oraz upoważnienia do przetwarzania danych. Powyższe działania odbywały się w oparciu o przyjęte w Krajowej Izbie Rozliczeniowej S.A. procedury. Ponadto ustalono, że Krajowa Izba Rozliczeniowa S.A. wypełniała obowiązki, o których mowa w rozporządzeniu 2016/679, w szczególności poprzez wdrożenie odpowiednich polityk ochrony danych, zawieranie umów powierzenia przetwarzania danych z podmiotem przetwarzającym, prowadzenie rejestru naruszeń w oparciu o przyjęte w podmiocie procedury i zasady postępowania z incydentami bezpieczeństwa oraz naruszeniami ochrony danych osobowych oraz poprzez wyznaczenie inspektora ochrony danych i wskazanie jego danych do kontaktu.

W związku z powyższymi ustaleniami brak było podstaw do wszczęcia postępowania administracyjnego.

5.4. Podmiot sektora bankowego

W 2021 roku Prezes UODO przeprowadził kontrolę w obszarze sektora bankowego w zakresie przetwarzania danych osobowych w związku ze stosowaniem odręcznego podpisu biometrycznego[206].

W toku kontroli ustalono, że potencjalni klienci banku mogli złożyć wniosek o zawarcie umowy na produkty bankowe również drogą elektroniczną (online). W takich przypadkach, w celu podpisania umowy, stosowany był przez bank odręczny podpis biometryczny. Podpis biometryczny był odręcznie składany za pomocą rysika na urządzeniu typu tablet. Na podstawie internetowego e-wniosku klientom oferowane było zawarcie umowy konta osobistego oraz umowy usługi online dla klientów indywidualnych i umowy o debetową kartę płatniczą.

Klientami banku, którzy zawierali umowy z użyciem podpisu biometrycznego były osoby fizyczne oraz osoby fizyczne prowadzące działalność gospodarczą na podstawie wpisu do ewidencji

[205] Sygn. DKN.5110.2.2021.
[206] Sygn. DKN.5112.29.2021.

działalności gospodarczej. Natomiast podpisem biometrycznym nie były podpisywane umowy zawierane z klientami będącymi osobami prawnymi. Do zawarcia umowy za pośrednictwem tego kanału dystrybucji (online) dochodziło bez fizycznej obecności klienta w banku.

Kontrola wykazała, że w procesie składania e-wniosku bank pozyskiwał m.in. zdjęcia twarzy osoby składającej wniosek oraz zdjęcia (lub skan) jej dowodu tożsamości, w celu potwierdzenia tożsamości. W ocenie banku w ten sposób realizowane były środki bezpieczeństwa finansowego w celu poprawnej identyfikacji klienta i weryfikacji jego tożsamości.

W dodatkowych wyjaśnieniach do protokołu kontroli bank wskazał, że podstawą prawną przetwarzania danych osobowych klientów i potencjalnych klientów banku, w związku z zawieraniem i wykonaniem zawartych umów, stanowi art. 6 ust. 1 lit. b RODO, który stanowi, że przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. W przypadku osób, z którymi zawierane były umowy przy użyciu podpisu biometrycznego, podstawę prawną stanowił art. 9 ust. 2 lit. a rozporządzenia 2016/679 tj. zgoda osoby, której dane dotyczą, wyrażona w celu jednoznacznego zidentyfikowania osoby fizycznej. Klauzula zgody zamieszczona była w formularzu weryfikacyjnym danych osobowych na tzw. checkliście.

Ponadto zaznaczył, że podstawę prawną przetwarzania danych osobowych przez bank stanowił również art. 6 ust. 1 lit. c RODO w zw. m.in. z art. 725 ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny[207], art. 49 ust. 1 pkt 1 i 2 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu[208], art. 74 ust. 2 pkt 8 ustawy z 29 września 1994 r. o rachunkowości[209] w zw. z art. 26 i art. 27 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[210] oraz z § 9 i § 49 ust. 1 i 2 rozporządzenia Ministra Finansów z dnia 1 października 2010 r. w sprawie szczególnych zasad rachunkowości banków (w przypadku powstania dowodów księgowych w toku wykonywania umowy).

Bank podkreślił, że zobowiązany był do stosowania przepisów ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, tj. jej art. 33–37, a w szczególności: art. 34 ust.1 pkt. 1, w myśl którego środki bezpieczeństwa finansowego obejmują identyfikację klienta oraz weryfikację jego tożsamości; art. 34 ust. 3, zgodnie z którym instytucje obowiązane dokumentują zastosowane środki bezpieczeństwa finansowego oraz wyniki bieżącej analizy przeprowadzanych transakcji.

[207] Dz. U. z 2020 r. poz. 1740.
[208] Dz. U. z 2021 r. poz. 1132.
[209] Dz. U. z 2021 r. poz. 217.
[210] Dz. U. z 2020 r. poz. 764.

Na żądanie organów, o których mowa w art. 130 ww. ustawy, instytucje obowiązane wykazują, że przy uwzględnieniu poziomu rozpoznanego ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z danymi stosunkami gospodarczymi lub transakcją okazjonalną, zastosowały odpowiednie środki bezpieczeństwa finansowego; art. 34 ust. 4 ww. ustawy, zgodnie z którym 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.

Oceniając ustalenia dokonane w toku kontroli wątpliwości Prezesa UODO wzbudziły kwestie związane z zasadnością pozyskiwania zdjęć twarzy osób składających online wnioski oraz zdjęć (lub skanów) ich dowodów tożsamości, a także zasadnością używania podpisu biometrycznego (tj. podpisu składanego na tablecie za pomocą rysika) przy zawierania przez bank umów z klientami, w świetle obowiązujących przepisów prawa. Wykorzystywanie podpisu biometrycznego tym bardziej budzi zastrzeżenia, biorąc pod uwagę treść § 2 pkt 1 rozporządzenia Rady Ministrów z dnia 9 marca 2020 r. w sprawie dokumentów związanych z czynnościami bankowymi, sporządzanych na informatycznych nośnikach danych[211] i wynikające z niego wątpliwości interpretacyjne, co do zakresu pojęciowego „innego podpisu elektronicznego zgodnego z umową stron, a w przypadku dokumentów wewnętrznych Banku, zgodnego z jego przepisami wewnętrznymi".

W zakresie interpretacji przepisów, o których mowa powyżej, Prezes UODO wystąpił do Przewodniczącego Komisji Nadzoru Finansowego o wyjaśnienie, co należy rozumieć pod pojęciem „inny podpis elektroniczny zgodny z umową stron". W związku z powyższym postępowanie kontrolne w niniejszej sprawie nie zostało zakończone, a sprawa podlega dalszej analizie.

5.5. Pozostałe podmioty sektora prywatnego

W 2021 r. Prezes UODO przeprowadził także jedenaście (11) kontroli w podmiotach z sektora prywatnego.

W związku z kontrolą przeprowadzoną w Miejskim Przedsiębiorstwie Komunikacyjnym i dokonanymi tam ustaleniami, że płatności za bilety uprawniające do przejazdu środkami lokalnego transportu zbiorowego dokonywane były m.in. za pomocą terminala płatniczego PayEye (E POS),

[211] § 2. *Ilekroć w rozporządzeniu jest mowa o: 1) podpisie elektronicznym – należy przez to rozumieć kwalifikowany podpis elektroniczny albo inny podpis elektroniczny zgodny z umową stron, a w przypadku dokumentów wewnętrznych banku, zgodny z jego przepisami wewnętrznymi*, Dz. U. poz. 476.

który do akceptacji płatności wykorzystuje biometrię tęczówek oczu, Prezes UODO przeprowadził również kontrolę w podmiocie udostępniającym innym podmiotom do stosowania terminal PayEye, w celu obsługi płatności za usługi świadczone przez te podmioty (lub w zakresie udostępniania do stosowania terminalu PayEye do obsługi płatności za usługi świadczone przez dane podmioty)[212]. Wykorzystywanie tęczówki oka w procesie obsługi płatności odnieść należy do art. 4 pkt 14 rozporządzenia 2016/679, który zawiera definicję danych biometrycznych, czyli danych osobowych, które wynikają ze specjalnego przetwarzania technicznego[213] oraz zasady minimalizacji określonej w art. 5 ust. 1 lit. c przywołanego rozporządzenia 2016/679.

W związku z powyższym Prezes UODO powziął wątpliwość w zakresie przetwarzania przez Spółkę biometrycznych danych osobowych (tęczówek oczu) za pomocą urządzeń służących do dokonywania płatności za zakup biletów uprawniających do przejazdu środkami lokalnego transportu zbiorowego, w kontekście niezbędności i proporcjonalności identyfikacji za pomocą danych biometrycznych do celów uwierzytelniania. Sprawa jest wciąż przedmiotem analizy Prezesa UODO.

Prezes UODO wykonywał również czynności wyjaśniające w odniesieniu do spółki prawa handlowego, w toku których ustalono, że w spółce miał miejsce incydent stanowiący naruszenie ochrony danych pracownika w związku z zagubieniem jego świadectwa pracy, sporządzonego przez poprzedniego pracodawcę[214].

Przedmiotowy incydent nie został zgłoszony Prezesowi UODO, gdyż – jak uznał administrator danych – brak było ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Według oświadczenia spółki, jej pracownik został poinformowany o incydencie niezwłocznie po jego ustaleniu. Jednakże wobec braku przedstawienia przez spółkę dowodu potwierdzającego powyższe, wątpliwości Prezesa UODO wzbudziła możliwość uznania samego oświadczenia o zawiadomieniu o naruszeniu, jako dowodu wypełniającego wymagania związane z zasadą rozliczalności określoną w art. 5 ust. 2 RODO.

Na podstawie zebranego materiału dowodowego Prezes UODO wszczął postępowanie administracyjne w sprawie. W związku z brakiem zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych pracownika oraz biorąc pod uwagę zakres danych zawartych

[212] Sygn. DKN.5112.34.2021.
[213] Art. 4 pkt 14 rozporządzenia 2016/679: „*dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.*
[214] Sygn. DKN.5110.12.2021.

w świadectwie pracy[215], 6 czerwca 2022 r. wydana została decyzja o nałożeniu na spółkę administracyjnej kary pieniężnej w wysokości 15 994 zł za niezgłoszenie do UODO naruszenia ochrony danych osobowych, polegającego na utracie przez ten podmiot świadectwa pracy pracownika[216].

Prezes UODO przeprowadził również kontrolę przetwarzania danych osobowych klientów i potencjalnych klientów wspólników spółki cywilnej, której działalność polegała m.in. na świadczeniu pomocy prawnej w zakresie reprezentowania klientów poszkodowanych (głównie w wypadkach komunikacyjnych) przed towarzystwami ubezpieczeniowymi, przed sądami, a także innymi podmiotami, w celu uzyskania na ich rzecz odszkodowań, zadośćuczynienia i rent, a także zwrotu kosztów leczenia i rehabilitacji[217]. W ramach kontroli zbadano także podstawy prawne przetwarzania danych osobowych – art. 5 ust. 1 lit. a oraz art. 6 ust. 1 lit. a oraz lit. b rozporządzenia 2016/679.

W przedmiotowej sprawie wątpliwości Prezesa UODO wzbudził proces pozyskiwania zgody na przetwarzanie danych osobowych od potencjalnych klientów Spółki oraz informacji o ich stanie zdrowia. Ustalono, że wspólnicy spółki uzyskiwali od klientów, tj. osób, do których wspólnicy kierowali ofertę w przedmiocie świadczonych przez nich usług, i z którymi nie zostały jeszcze zawarte umowy, zgodę na przetwarzanie ich danych osobowych jedynie w formie ustnej. Wobec powyższego Prezes UODO wszczął postępowanie administracyjne.

W sprawie tej Prezes UODO wysunął zastrzeżenia natury prawnej w odniesieniu do przetwarzania danych osobowych potencjalnych klientów wspólników spółki, w tym danych dotyczących ich stanu zdrowia, bez uzyskania w tym celu ich zgody, zgodnie z art. 6 ust. 1 lit. a rozporządzenia 2016/6791 oraz art. 9 ust. 2 lit. a w związku z art. 9 ust. 1 rozporządzenia 2016/679, sposobu realizacji przez wspólników w ramach prowadzonej przez nich działalności w ramach spółki cywilnej, tzw. obowiązku informacyjnego wynikającego z art. 12, art. 13 ust. 1 i ust. 2 oraz art. 14 ust. 1, ust. 2 i ust. 3 rozporządzenia 2016/679 oraz zakresu informacji o operacjach wykonywanych w ramach danej czynności zamieszczanych w rejestrze czynności przetwarzania danych osobowych.

Wobec powyższych ustaleń, Prezes UODO prowadzi dalsze czynności w ramach wszczętego postępowania administracyjnego w tej sprawie.

---

[215] § 2 ust. 1 rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 30 grudnia 2016 r. w sprawie świadectwa pracy.
[216] https://www.uodo.gov.pl/decyzje/DKN.5110.12.2021
[217] Sygn. DKN.5112.5.2021.

5.6. Portale internetowe

Prezes UODO w 2021 roku przeprowadził cztery (4) kontrole w podmiotach oferujących usługi poczty elektronicznej za pośrednictwem portali internetowych.

Zakres kontroli obejmował głównie zbadanie wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z ogólnym rozporządzeniem o ochronie danych oraz z uwzględnieniem charakteru, zakresu, kontekstu, celów przetwarzania i ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te były w razie potrzeby poddawane przeglądom i uaktualniane (art. 32 i art. 24 RODO). W zainteresowaniu kontrolujących pozostawały w szczególności: a) elementy bezpieczeństwa wykorzystywane w celu ochrony infrastruktury usługi poczty z uwzględnieniem mechanizmu tworzenia i weryfikacji kopii zapasowych oraz systemów antywirusowych/antyspamowych, b) sposób realizacji dostępu administracyjnego do zbiorów danych osobowych użytkowników usługi poczty, c) sposoby stosownego logowania oraz korelowania zdarzeń z usługi poczty, d) sposób realizowania dostępu do skrzynki pocztowej dla potencjalnego użytkownika (z uwzględnieniem mechanizmów zapewniających poufność, integralność, dostępność).

Jak ustalono, podmioty kontrolowane wdrożyły środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych objętych ochroną. Zostało to zrealizowane m.in. poprzez opracowanie i wdrożenie polityk bezpieczeństwa, stosowanie odpowiednich polityk haseł, stosowanie środków kryptograficznych, ciągłe monitorowanie bezpieczeństwa systemów teleinformatycznych, stosowanie systemów antyspamowych i antywirusowych, przeprowadzanie okresowych testów bezpieczeństwa, szyfrowanie plików i nośników, monitorowanie przepływu danych z i na nośniki, stosowanie dwuskładnikowego uwierzytelnienia. Do ochrony przed atakami z sieci publicznej zastosowane zostały systemy bezpieczeństwa (np. system zapór sieciowych, system wykrywania oraz reagowania na zagrożenia) oraz systemy zapewniające rozliczalność operacji wykonywanych na danych osobowych. Dużą wagę podmioty kontrolowane przykładały do dostępności swoich usług dla użytkowników, stosując w tym zakresie szereg rozwiązań technicznych. Ponadto podmioty kontrolowane, jako administratorzy danych, w sposób prawidłowy wywiązywały się także z innych obowiązków, tj. prowadziły dokumentację opisującą sposób przetwarzania danych oraz wdrożyły polityki ochrony danych, wyznaczyły i zgłosiły inspektorów ochrony danych, podjęły działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora, która ma dostęp do danych osobowych, przetwarzała je na polecenie

administratora, dokumentowały naruszenia ochrony danych osobowych oraz prowadziły rejestry czynności przetwarzania danych.

W świetle dokonanych ustaleń brak było podstaw do wszczęcia postępowania administracyjnego.

5.7. Operatorzy pocztowi

W związku ze skierowanym do Prezesa Urzędu Ochrony Danych Osobowych przez Rzecznika Praw Obywatelskich wnioskiem o zbadanie sprawy dotyczącej przetwarzania danych osobowych w związku ze stosowaniem odręcznego podpisu biometrycznego, działając na podstawie art. 58 ust. 1 lit. a i lit. e RODO, Prezes UODO zwrócił się do trzech (3) operatorów pocztowych o wyjaśnienie: podstawy prawnej przetwarzania danych osobowych w związku ze stosowaniem odręcznego podpisu elektronicznego, kategorii osób, których te dane dotyczą (rodzaju usług i klientów, których te dane dotyczą oraz od jak dawna podpis jest stosowany), zakresu i rodzaju przetwarzanych danych osobowych, w szczególności jakie cechy fizyczne osoby podpisującej zapisywane były w procesie odręcznego podpisu biometrycznego, czy wdrożono środki techniczne i organizacyjne w celu zapobiegania nieuprawnionemu użyciu (w innym celu, niż realizowany przez osobę podpisującą) odręcznego podpisu biometrycznego w momencie jego składania, czy została przeprowadzona ocena skutków dla ochrony danych w związku ze stosowaniem odręcznego podpisu biometrycznego, jak długo i w jakiej formie przetwarzane były dane osobowe pozyskane w związku ze stosowaniem podpisu biometrycznego oraz innych obowiązków administratorów danych związanych z bezpieczeństwem przetwarzanych danych.

Z nadesłanych wyjaśnień wynikało, że nie w każdym przypadku, gdy składany jest podpis na urządzeniu elektronicznym, mamy do czynienia z podpisem biometrycznym – zależy to od rodzaju świadczonych usług. Podpis składany przez odbiorcę przesyłki na urządzeniu elektronicznym jako pokwitowanie z kopią (obrazem podpisu odbiorcy) wygenerowaną po dokonanej transmisji danych, zastąpił papierowe pokwitowanie doręczenia. Wyżej wskazane odwzorowanie podpisu nie jest uważane za podpis własnoręczny[218], gdyż jest wyłącznie jego kopią, a wykorzystywane przez operatora urządzenia nie korzystają z metod technicznych umożliwiających przetwarzanie cech fizycznych, fizjologicznych lub behawioralnych osoby składającej taki podpis. Dane biometryczne w postaci podpisu mogą być zbierane w przypadku świadczenia specjalnych usług (np. gdy operator pośredniczy w zawieraniu umów), na rzecz innych podmiotów, z którymi zawierane są umowy

[218] Por. uchwała Sądu Najwyższego z dnia 20 grudnia 2006 r. sygn. I KZP 29/06.

powierzenia przetwarzania danych. Operator pocztowy realizuje wówczas swoje obowiązki jako podmiot przetwarzający.

Podpis biometryczny jest również wykorzystywany przy potwierdzaniu odbioru przesyłek w ramach świadczenia usług przez operatora pocztowego, wyznaczonego w szczególności na rzecz organów wymiaru sprawiedliwości. W ten sposób w przypadku pokwitowania odbioru na urządzeniu mobilnym odnotowywane są parametry, takie jak: współrzędne x i y punktu, czas zaznaczenia punktu, siła i nacisk oraz przybliżone dane geolokalizacyjne.

Wykorzystywanie przez ww. podmioty podpisu biometrycznego budzi szereg wątpliwości, ponieważ stanowi on szczególny rodzaj danych, których przetwarzanie jest możliwe po spełnieniu jednego z warunków wskazanych w art. 9 ust. 2 rozporządzenia 2016/679. Powoływane przez Operatorów przepisy prawa pocztowego[219], przewozowego[220], czy też przepisy wykonawcze dotyczące świadczenia przez operatora wyznaczonego usług powszechnych[221], czy doręczania pism procesowych[222], nie zawierają takich podstaw. Sprawa ta jest wciąż przedmiotem analizy organu.

5.8. Fundacja

Prezes UODO przeprowadził również kontrolę przetwarzania danych osobowych w ramach świadczonej przez fundację pomocy w zakresie jej zadań statutowych, a w szczególności pomocy osobom pokrzywdzonym przestępstwem lub osobom im najbliższym oraz pomocy udzielanej świadkom i osobom im najbliższym.

Wątpliwości Prezesa UODO wzbudził stosowany przez fundację formularz zgody na przetwarzanie danych osobowych osób ubiegających się o pomoc fundacji, pod kątem spełniania wymogów rozporządzenia 2016/679. W szczególności art. 5, art. 7 ust. 2 oraz art. 9 – biorąc pod uwagę także przetwarzanie przez fundację danych szczególnej kategorii, tj. m.in. informacji o niepełnosprawności, chorobie, informacji zawartych w wyrokach skazujących, itp.

Ustalono, że przedmiotowy formularz wskazywał jedynie, iż podmiotem, który przetwarza dane osobowe jest Ministerstwo Sprawiedliwości, a nie tylko fundacja. W treści formularza dokonano połączenia dwóch rodzajów treści, tj. klauzuli informacyjnej oraz zgody na przetwarzanie danych,

[219] Ustawa z dnia 23 listopada 2012 r. Prawo pocztowe, Dz. U. 2020 r. poz. 1041 z późn. zm.
[220] Ustawa z dnia 15 listopada 1984 r. Prawo przewozowe, Dz. U. 2020 r. poz. 8.
[221] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 29 kwietnia 2013 r. w sprawie warunków wykonywania usług powszechnych przez operatora wyznaczonego, Dz. U. 2020 r. poz.1026.
[222] Rozporządzenie Ministra Sprawiedliwości z dnia 6 maja 2020 r. w sprawie szczegółowego trybu i sposobu doręczania pism sądowych w postępowaniu cywilnym (Dz.U. 2020 r. poz. 819), Rozporządzenie Ministra Sprawiedliwości z dnia 10 stycznia 2017 r. w sprawie szczegółowych zasad i trybu doręczania pism organów procesowych w postępowaniu karnym (Dz. U. 2018 r. poz. 553 z późn. zm.).

która została umieszczona na stronie drugiej formularza, na samym jego końcu, pod klauzulą informacyjną, co sugerowało, że zgoda jest jednocześnie oświadczeniem wiedzy, że osoba ubiegająca się o pomoc zapoznała się z klauzulą informacyjną. Ponadto treść klauzuli informacyjnej oraz oświadczenia o udzieleniu zgody na przetwarzanie danych nie obejmowały informacji o przetwarzaniu danych przez podmioty współpracujące z fundacją, tj. prawników, psychologów, psychiatrów, itp.

Prezes UODO ustalił także, że treść umów zawieranych przez fundację z ww. specjalistami nie zawierała postanowień odnoszących się do obowiązków specjalistów w zakresie przetwarzania danych osobowych osób korzystających z pomocy świadczonej przez fundację. Brak w niej było określenia zakresu, w którym dany specjalista może przetwarzać dane, sposobu przechowywania i przesyłania dokumentacji zawierającej dane, itd.

Prezes UODO ustalił także, że fundacja korzystając z usług Google w zakresie bezpłatnego konta, tj. z usługi bezpłatnej poczty elektronicznej oraz z usługi tzw. chmury, polegającej na możliwości korzystania z wirtualnego dysku służącego do przechowywania plików elektronicznych, powierzyła przetwarzanie danych osobowych osób ubiegających się o pomoc innemu podmiotowi. Fundacja nie była w stanie wykazać się odpowiednimi dokumentami potwierdzającymi zawarcie umowy powierzenia przetwarzania danych osobowych z uwzględnieniem wszystkich niezbędnych elementów jej treści (art. 28 ust. 3 i ust. 9 rozporządzenia 2016/679), co wzbudziło zastrzeżenia Prezesa UODO.

W przedmiotowej sprawie Prezes UODO ustalił, iż doszło do niedopełnienia obowiązku, o którym mowa w art. 29 w zw. z art. 5 ust. 1 lit. f RODO, tj. dopuszczenie do przetwarzania danych osobowych osób wykonującym obowiązki służbowe przy obsłudze wniosków, osób ubiegających się o pomoc fundacji, bez stosownych upoważnień.

Ponadto wątpliwości Prezesa UODO dotyczyły środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych poprzez fundację, m.in. z powodu braku aktualnej bazy istniejących zagrożeń, wygaśnięcia licencji na oprogramowanie antywirusowe, w odniesieniu do obowiązku zapewniania przez administratora wymaganego poziomu poufności, integralności i odporności systemów (zasobów) informatycznych zawierających dane osobowe, w zw. z art. 5 ust. 2 statuującym zasadę rozliczalności.

Stwierdzoną w toku kontroli nieprawidłowością był także brak zgłoszenia przez fundację Prezesowi UODO danych do kontaktu z inspektorem ochrony danych, w zw. z treścią art. 37 ust. 7 rozporządzenia 2016/679.

5.9. Decyzje administracyjne w postępowaniach kontrolnych

W 2021 roku Prezes UODO, po przeprowadzeniu postępowań administracyjnych dotyczących przetwarzania danych osobowych, wydał sześć (6) decyzji. W pięciu (5) decyzjach postępowanie administracyjne w całości zostało umorzone, zaś w jednej (1) decyzji udzielił upomnienia, a w pozostałej części postępowanie administracyjne zostało umorzone.

Poniżej przykład decyzji Prezesa UODO po przeprowadzeniu postępowania kontrolnego w przedmiocie przetwarzania danych osobowych przez spółkę prowadzącą działalność w zakresie wesołego miasteczka[223]. Na skutek stwierdzenia naruszenia przepisów rozporządzenia 2016/679 wydana została decyzja nakazująca ww. podmiotowi dostosowanie operacji przetwarzania danych osobowych do przepisów RODO poprzez podjęcie odpowiednich środków, 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 rozporządzenia 2016/679, zakreślając 30 dniowy termin.

W toku kontroli ustalono, że dokument pod nazwą Polityka Prywatności, który był dostępny w punkcie obsługi klienta oraz na stronie internetowej spółki, nie został przedstawiony w zwięzłej formie. Zawierał bowiem informacje dotyczące przetwarzania danych osobowych wielu różnych osób, tj. osób poszukujących pracy, pracowników, dostawców i innych osób, osób odwiedzających stronę internetową, poprzez którą zapisywane są na jej komputerze pliki cookies, akcjonariuszy, wspólników, organów statutowych, osób korzystających z parku rozrywki oraz innych klientów.

Na skutek stwierdzonych nieprawidłowości w procesie przetwarzania danych osobowych przez spółkę, Prezes UODO wydał decyzję, w uzasadnieniu której wskazał, że Polityka Prywatności jest dokumentem zawierającym informacje, które warunkują prawidłowe spełnienie obowiązku wynikającego z art. 13 lub 14 rozporządzenia 2016/679. Podkreślił, że Polityka Prywatności powinna zawierać informacje związane z przetwarzaniem danych osoby, której dane dotyczą, w innym przypadku dokument taki nie spełnia warunku przejrzystości i konieczne jest wyszukiwanie informacji i dopasowywanie do procesu przetwarzania danych, w którym osoba, której dane dotyczą, bierze udział. Prezes UODO nadmienił także, że ważna jest nie tylko treść, ale również forma i sposób, w jaki informacje powinny być przekazane osobie, której dane dotyczą. W ocenie Prezesa UODO zastosowane przez spółkę rozwiązanie nie spełniało wymogów określonych w art. 5 ust. 1 lit.

[223] Decyzja z 23 lutego 2021 r.: ZSPR.421.20.2019.11.31.80.

a oraz 12 ust. 1 rozporządzenia 2016/679, co skutkowało wydaniem przedmiotowej decyzji. Postępowanie w niniejszej sprawie zostało zakończone, a decyzja wykonana.

5.10. System Informacyjny Schengen, Wizowy System Informacyjny

W związku z wykorzystaniem przez właściwe organy wielkoskalowych systemów informatycznych odbyły się dwie (2) kontrole w Komendzie Głównej Policji. Stanowiły one obowiązkowe, przeprowadzane co cztery lata, audyty operacji przetwarzania danych, w ramach zgodnego z międzynarodowymi standardami audytu, o których mowa w art. 60 Decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II)[224], art. 44 ust. 2 Rozporządzenia (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II)[225] oraz art. 41 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych[226].

Przedmiotem obydwu kontroli był sposób realizacji obowiązków administratora przez Komendę Główną Policji (Centralny Organ Techniczny Krajowego Systemu Informatycznego), a w przypadku SIS II również zadań Biura SIRENE. W szczególności badane były kwestie zastosowanych środków organizacyjnych i technicznych mających zapewnić przestrzeganie właściwych przepisów o ochronie danych, w tym m.in. ich bezpieczeństwa, realizację praw osób, których dane dotyczą, legalności tworzonych wpisów oraz dokonywania do nich wglądu.

Realizując zadania nadzorcze nad przetwarzaniem danych osobowych za pośrednictwem wielkoskalowych systemów informatycznych, Prezes Urzędu Ochrony Danych Osobowych, działając na podstawie art. 11 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[227], wystąpił do inspektorów ochrony danych wytypowanych dziesięciu jednostek policji o dokonanie sprawdzenia operacji zgodności przetwarzania danych dotyczących wpisów w Systemie Informatycznym Schengen, dokonywanych na podstawie art. 36 ust. 1 Decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II)[228] oraz art. 3 ust. 1 pkt 6 lit. a i b ustawy z dnia 24 sierpnia 2007

[224] Dz. U. UE. L 205 z 7.8.2007 r. str. 63–84.
[225] Dz.U. UE L 381 z 28.12.2006 r. str. 4–23.
[226] Dz.U. UE L 218 z 13.8.2008 r. str. 60–81.
[227] Dz. U. z 2018 r. poz. 125.
[228] Dz.U.UE.L.2007.205.63.

r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[229] oraz właściwych aktów wykonawczych, w tym m.in. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 kwietnia 2013 r. w sprawie dokonywania wpisów danych SIS oraz aktualizowania, usuwania i wyszukiwania danych SIS poprzez Krajowy System Informatyczny[230] z właściwymi przepisami o ochronie danych osobowych. Powyższe zagadnienie było również przedmiotem kontroli Prezesa Urzędu Ochrony Danych Osobowych, która odbyła się w Komendzie Stołecznej Policji. W toku kontroli nie stwierdzono uchybień w zakresie dokonywania ww. operacji przetwarzania danych.

6. Egzekucja administracyjna – zapewnienie wykonania decyzji

Prezes Urzędu Ochrony Danych Osobowych, na podstawie art. 1a pkt 13 w zw. z art. 2 § 1 pkt 12 oraz art. 20 § 2 ustawy o postępowaniu egzekucyjnym w administracji[231], jest wierzycielem i organem egzekucyjnym w odniesieniu do egzekucji obowiązków o charakterze niepieniężnym z zakresu ochrony danych osobowych. Dzięki temu Prezes UODO może prowadzić czynności mające na celu 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 naczelnik właściwego urzędu skarbowego. 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% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

[229] Dz. U. z 2021 r. poz. 1041.
[230] Dz.U. z 2020 r. poz. 1126.
[231] Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, Dz. U. z 2020 r. poz. 1427 z późn. zm.

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

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

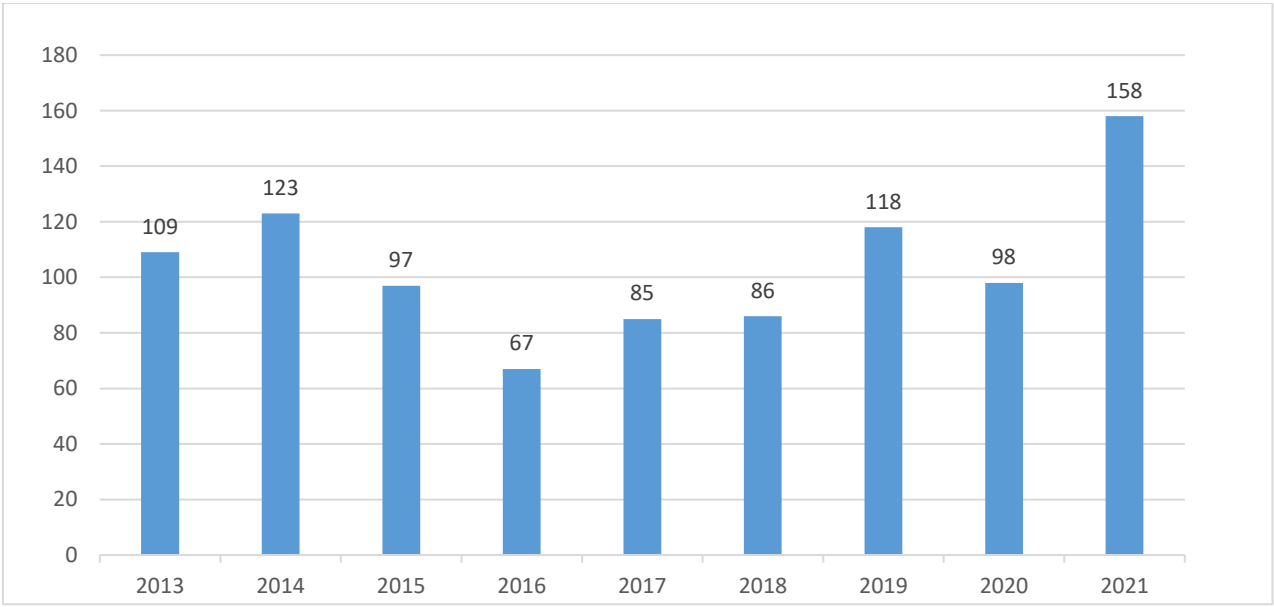
a) obowiązek (nakaz) do wykonania, które były ostateczne oraz te, którym nadano rygor natychmiastowej wykonalności. Jeżeli decyzja administracyjna zawiera postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlega egzekucji administracyjnej dopiero po upływie tego 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) 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% 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 do 10 000 zł.

Egzekucja obowiązków o charakterze niepieniężnym (nakazów decyzji)

Prezes UODO prowadził w 2021 roku **działania egzekucyjne w stosunku do 158 decyzji administracyjnych**, które zawierały nałożony na strony określony nakaz do wykonania. Jest to najwyższa liczba decyzji, które zostały przekazane do egzekucji od momentu powstania komórki egzekucyjnej w Urzędzie Ochrony Danych Osobowych, tj. od 2013 roku i ponad 60% wzrost

w stosunku do roku 2020, w którym działania egzekucyjne prowadzone były wobec 98 decyzji Prezesa UODO zawierających nakaz.

Na poniższym wykresie przedstawiono liczbę decyzji zawierających nakaz, które przekazane zostały do egzekucji w latach 2013–2021.

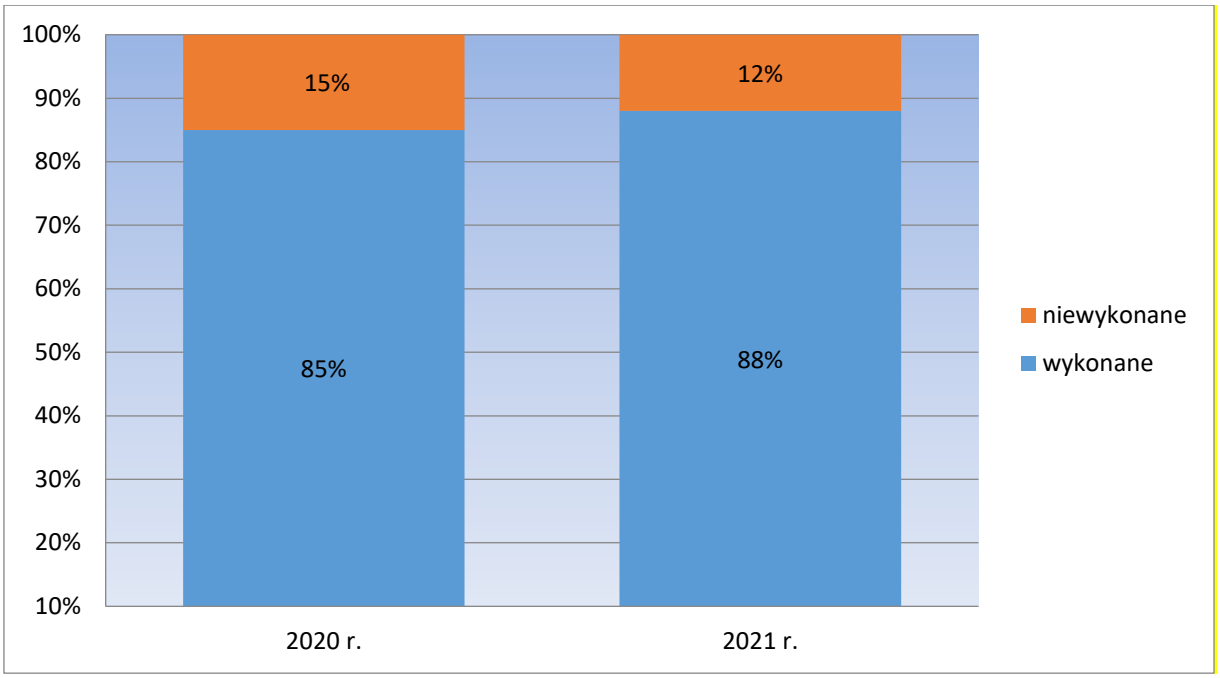


Wykres 4: **Zestawienie decyzji organu z nakazem, przekazane do egzekucji administracyjnej w latach 2013–2021.**

Efektywność prowadzonych przez komórkę egzekucyjną działań egzekucyjnych mających na celu wykonanie przez zobowiązanych obowiązków nałożonych na nich nakazami decyzji administracyjnych w 2021 roku przedstawia się następująco: spośród 158 decyzji **wykonanych zostało przez zobowiązanych 139 decyzji**, natomiast 19 decyzji pozostało niewykonanych. Decyzje te w dalszym ciągu objęte są działaniami egzekucyjnymi.

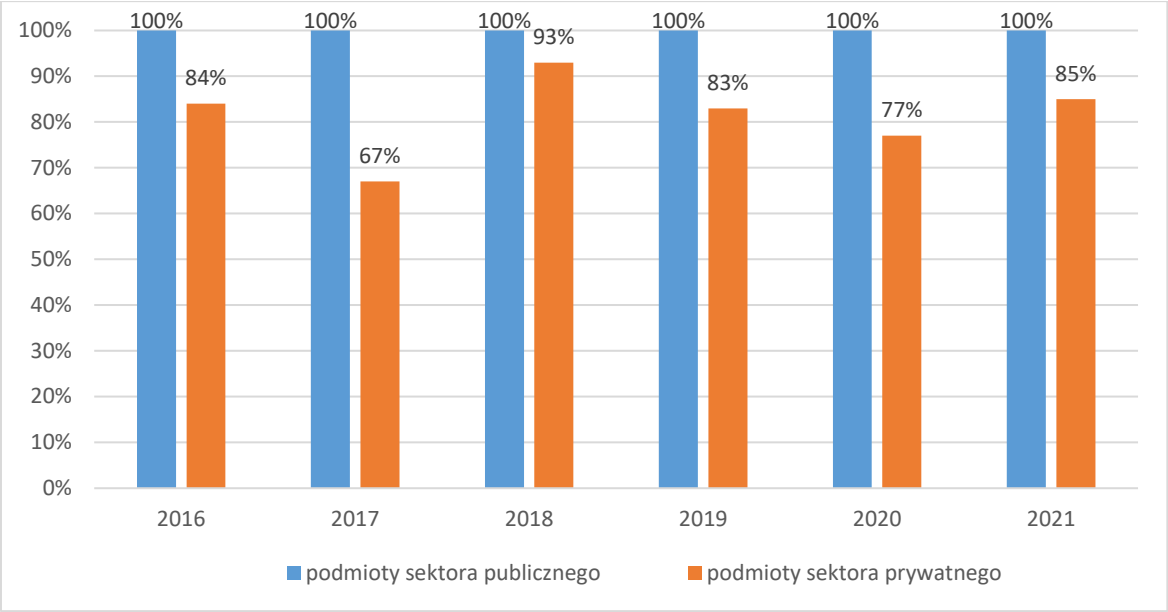
Procentowy wskaźnik efektywności działań egzekucyjnych w odniesieniu do wszystkich decyzji administracyjnych przekazanych w 2021 roku do egzekucji wynosił **88%**.

Porównując efektywność działań egzekucyjnych organu prowadzonych w 2021 roku do efektywności działań prowadzonych w roku 2020, która wynosiła 85%, można zauważyć, że mimo dużego wzrostu liczby decyzji (ponad 60% więcej niż w roku poprzedzającym), wobec których prowadzone były działania egzekucyjne, komórce egzekucyjnej UODO udało się podwyższyć efektywność o 3%, co przedstawia poniższy wykres.



Wykres 5: **Zestawienie procentowej efektywności działań egzekucyjnych organu w 2020 i 2021 r.**

Działania egzekucyjne podejmowane przez Prezesa UODO w 2021 r. dotyczyły decyzji skierowanych w 79% przypadków do podmiotów z sektora prywatnego oraz w 21% przypadków do podmiotów z sektora publicznego. Podobnie jak w roku 2020 i latach wcześniejszych, wszystkie niewykonane decyzje dotyczyły podmiotów z sektora prywatnego. Analizując na przestrzeni kilku lat efektywność działań egzekucyjnych organu ze względu na przynależność zobowiązanych do sektora publicznego i sektora prywatnego w latach 2016–2021 można zaobserwować trend polegający na stale utrzymującej się **100% efektywności w odniesieniu do podmiotów publicznych**.

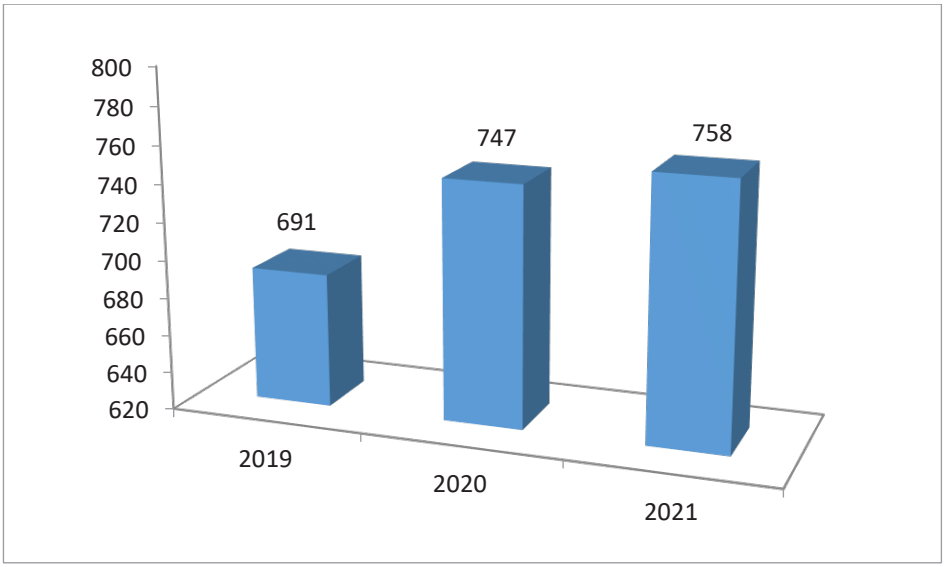


Wykres 6: **Zestawienie efektywności prowadzonych działań egzekucyjnych w odniesieniu do podmiotów sektora publicznego i sektora prywatnego w latach 2016–2021.**

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

Jednym z zadań organu nadzorczego jest opiniowanie projektów aktów prawnych. W 2021 r. zadanie to realizowane było poprzez analizę projektowanych lub nowelizowanych przepisów pod kątem zapewnienia przez projektodawców zgodności treści nowych regulacji z przepisami RODO. Organ nadzorczy opiniował także projekty dotyczące przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

W 2021 roku organ nadzorczy zaopiniował **758 projektów aktów prawnych** (zarówno na poziomie regulacji krajowych, jak i międzynarodowych). Dla porównania: w 2019 roku zaopiniowanych zostało 691 projektów, a w 2020 roku – 747, co przedstawia poniższy wykres.



Wykres 7: **Liczba zaopiniowanych projektów aktów prawnych, które wpłynęły do Urzędu Ochrony Danych Osobowych w latach 2019–2021.**

W odniesieniu do projektów aktów europejskich, Prezes UODO wydawał do nich stanowiska na takich samych zasadach, jak w przypadków projektów krajowych. Projekty te badane były m.in. pod kątem zgodności z zasadami dotyczącymi przetwarzania danych wynikającymi z RODO, przyjęcia właściwych podstaw przetwarzania danych, zakresów danych podlegających przetwarzaniu oraz celów przetwarzania (art. 5, 6 i 9) oraz określenia ról podmiotów w procesie przetwarzania danych osobowych. Organ nadzorczy zwracał uwagę na to, czy projektodawca dokonał analizy wpływu przyjmowanych w przepisach rozwiązań na prywatność osób, których dane mają być przetwarzane – testu prywatności, czy uwzględnił zasadę ochrony danych w fazie projektowania, czy w uzasadnionych przypadkach dokonał oceny skutków dla ochrony danych (art. 25 i 35). Analizowane były także sposoby przetwarzania danych zarówno w systemach teleinformatycznych czy na potrzeby wykonywania operacji przetwarzania danych zdalnie, jak również cele przetwarzania danych oraz okresy retencji danych.

Przedmiotem wnikliwego zainteresowania organu nadzorczego były takie zagadnienia, jak:

- ocena skutków dla ochrony danych,
- kwestie związane z wyłączaniem/ograniczaniem stosowania RODO w projektowanych przepisach,
- zagadnienie otwartych danych,
- wykorzystywanie nowych technologii w procesach przetwarzania danych,

- przetwarzanie danych osobowych szczególnych kategorii.

Przedkładanie aktów prawnych do zaopiniowania organowi nadzorczemu

Zgodnie z art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[232] w związku z art. 57 ust. 1 lit. c RODO[233], założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych. Obowiązek ten jest realizowany przede wszystkim przez ministrów kierujących poszczególnymi działami administracji rządowej i kierowane przez nich ministerstwa prowadzące konkretny proces legislacyjny. Przedkładają oni projekty aktów normatywnych do organu nadzorczego na etapie prac Rządu nad projektem, odpowiednio do § 38 ust. 1 pkt 3 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów.

Niestety niektóre organy publiczne, poprzez pominięcie procesu uzgodnień i opiniowania, nie przekazywały istotnych projektów aktów normatywnych dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie do oceny organu nadzorczego. Zdarzało się również, że na wskazanych etapach prac nad projektem pomijany był, wbrew przepisom, organ nadzorczy. W części przypadków projekty te są konsultowane przez Rządowe Centrum Legislacji (na etapie komisji prawniczej) oraz Kancelarię Sejmu, które przekazują część tych projektów do Prezesa UODO, na właściwych dla tych podmiotów etapach procesu legislacyjnego. Jako przykład wskazać można rządowy **projekt ustawy o służbie zagranicznej**[234], który został przekazany przez Kancelarię Sejmu do UODO w dniu, w którym w Sejmie RP projekt ten był procedowany (odbywało się pierwsze czytanie). Organ nadzorczy nie miał wówczas możliwości zaopiniowania projektu ustawy w wymaganym czasie. Praktyki takie, jak wskazana powyżej naruszają przepisy RODO oraz ustawy o ochronie danych osobowych.

Na wniosek Kancelarii Sejmu czy Kancelarii Senatu są też opiniowane poselskie (rzadziej senatorskie) projekty ustaw. W ten sposób Urząd Ochrony Danych Osobowych realizuje zadanie wspomagania i doradztwa na rzecz Parlamentu RP w sprawie projektowanych przez to ciało aktów prawnych. Jako przykłady wskazać można projekty opiniowanych ustaw: **o zmianie ustawy**

[232] Art. 51 ustawy o ochronie danych osobowych stanowi, że założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu.
[233] Art. 57ust. 1. lit. c RODO stanowi, że 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.
[234] DOL.401.23.2021.

o Państwowej Inspekcji Pracy oraz niektórych innych ustaw, o Funduszu Wzajemnej Pomocy w Stabilizacji Dochodów Rolniczych, o zmianie ustawy o ochronie zwierząt oraz niektórych innych ustaw, o zmianie ustawy o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt oraz niektórych innych ustaw.

7.1. Ocena skutków dla ochrony danych

Art. 35 RODO reguluje obowiązek dokonania – m.in. w związku z tworzeniem przepisów regulujących operację lub zestaw operacji przetwarzania – oceny skutków dla ochrony danych, tj. wpływu projektowanych rozwiązań na prawo do prywatności oraz prawo do ochrony danych osobowych (art. 35 ust. 10). Obowiązek dokonania takiej oceny nie wynika wprost z obowiązujących przepisów, nie jest też wymagany wytycznymi[235] do jej przeprowadzenia, jednak zaistnienie okoliczności wskazanych w art. 35 uzasadnia jej dokonanie. Taka ocena skutków dla ochrony danych powinna być dokonywana ze względu na rodzaj przetwarzania, w szczególności następujący przy użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania, z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób. Należy wykazać niezbędność przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i zakresie. Uzasadnione jest, by ocena skutków dla ochrony danych była dokonywana już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych.

Z wielu przedkładanych organowi nadzorczemu do zaopiniowania projektów nie wynikało, aby ocena taka została przeprowadzona. Co więcej, projektodawcy bardzo często nie dostrzegali potrzeby jej dokonania. Analiza przedstawianych projektów prowadzi do wniosku, że wykonanie testu prywatności w postaci takiej oceny pozwoliłoby na wyeliminowanie wielu niedoskonałości projektowanych przepisów czy uniknięcie ryzyk związanych z proponowanym w przepisach przetwarzaniem danych osobowych w kontekście istoty i celów przyjmowanych rozwiązań oraz stosowanych technik przetwarzania danych, w szczególności z użyciem nowych technologii. Poprawnie przeprowadzona ocena skutków powinna wskazywać związek pomiędzy operacjami wykonywanymi na danych osobowych, z konkretnym celem ich przetwarzania. Cel przetwarzania musi być określony w podstawie prawnej, gdy są nią przepisy prawa powszechnie obowiązującego (art. 6 ust. 3 rozporządzenia 2016/679). Podstawa prawna może zawierać przepisy szczegółowe

[235] Wytyczne do przeprowadzania oceny przewidywanych skutków społeczno-gospodarczych zgodnie z § 24 ust. 3 uchwały nr 190 Rady Ministrów z 29 października 2013 r. – Regulamin pracy Rady Ministrów.

dostosowujące stosowanie przepisów niniejszego rozporządzenia, jak i inne elementy, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX.

W tym miejscu wskazać należy na **projekt ustawy o badaniach klinicznych stosowanych u ludzi (UC63)**[236], który będzie nową regulacją w krajowym porządku prawnym, dotyczącą badań klinicznych. Badania kliniczne są uregulowane w rozporządzeniu 563/2014[237], które w zakresie ochrony danych osobowych odwołuje się do nieobowiązującej już dyrektywy 95/46/WE[238]. Dlatego do materii objętej projektowaną ustawą zastosowanie będą miały przepisy rozporządzenia 2016/679. W związku z tym, zarówno rozporządzenie 563/2014, jak i rozporządzenie 2016/679 będą musiały zostać – w zakresie wprost nieuregulowanym w tych przepisach – odzwierciedlone w przepisach prawa krajowego. Z tej perspektywy przepisy prawa krajowego muszą być dostosowane do wskazanych wyżej rozporządzeń oraz respektować zasady wynikające z ogólnego rozporządzenia o ochronie danych. Natomiast z dokumentów przedstawionych do zaopiniowania nie wynikało, by projektodawca wykonał taką analizę i ocenę skutków dla ochrony danych. W efekcie wyważył on wpływ planowanego przetwarzania danych osobowych na prywatność osób, których te dane dotyczą, i zaproponował rozwiązania odpowiadające poszanowaniu zasad przetwarzania danych osobowych, co organ nadzorczy uznał za wysoce pożądane.

Opiniując **projekt ustawy o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (UC95)**[239], organ nadzorczy zwrócił uwagę na zasadność projektowania ochrony danych osobowych już na etapie tworzenia prawa, w tym przeprowadzenia oceny skutków dla ochrony danych. Wskazał, że pozwoliłaby ona na prawidłową ocenę statusu podmiotów uczestniczących w realizacji programów finansowanych z unijnych funduszy. Biorąc zaś pod uwagę ogromną liczbę przetwarzanych na te potrzeby danych osobowych, w tym danych z art. 9 i 10 RODO, organ nadzorczy zaznaczył, że dokonanie takiej analizy

[236] DOL.401.196.2021.
[237] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE.
[238] Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych Dz.U.UE.L.1995.281.31.
[239] DOL.401.446.2021.

i wykorzystanie jej wyników przy tworzeniu analizowanych przepisów jest wysoce pożądane. W odpowiedzi na zgłaszane uwagi projektodawca wskazywał, że przy projektowaniu przepisów dedykowanych perspektywie finansowej na kolejny okres, analiza procesów oraz ocena skutków dla ochrony danych będą przeprowadzone. Pomimo złożonej deklaracji jednak nie przedłożył jej, przedstawiając projekt do zaopiniowania.

Jako przykład innego istotnego projektu, na potrzeby którego ocena skutków dla ochrony danych osobowych również nie została przeprowadzona – pomimo postulatu organu – wskazać trzeba **projekt ustawy o zmianie ustawy Prawo lotnicze**[240]. Warto jednak odnotować, że niektóre resorty dokonywały oceny skutków dla ochrony danych. Dostrzegały jej wagę, choć nadal były to działania podejmowane głównie po zwróceniu uwagi na ten aspekt przez organ nadzorczy, a zatem w toku opiniowania, a nie w czasie koncepcyjnych prac resortowych.

Projektodawcy niejednokrotnie wskazywali, że to wykonawcy norm przeprowadzą stosowne analizy z zakresu oceny skutków dla ochrony danych, nie bacząc na to, że taka ocena, wykonana po ustaleniu norm prawnych, może być działaniem zbyt późnym, jeśli chodzi o ustalenie zagadnień o charakterze podstawowym. Jako przykład wskazać można odpowiedź projektodawcy w sprawie dotyczącej **prac nad wdrożeniem Zintegrowanej Platformy Analitycznej**, w toku której do zaopiniowania przekazano **projekt rozporządzenia Rady Ministrów w sprawie zakresu danych i wykazu rejestrów publicznych i systemów teleinformatycznych, z których udostępniane są dane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej**[241].

Korzystnie należy natomiast ocenić, że projektodawca – zgodnie z postulatami i uwagami organu w tym zakresie – w związku z tworzeniem przepisów regulujących funkcjonowanie krajowego rejestru maszynistów i prowadzących pojazdy kolejowe oraz rejestru egzaminatorów przedłożył taką ocenę wykonaną do **rządowego projektu ustawy o zmianie ustawy o transporcie kolejowym**[242] oraz zapowiedział przeprowadzenie ponownej analizy wraz z wdrażaniem systemów teleinformatycznych, wspólnie z ich wykonawcami. Dokonanie takiej oceny, uwzględnienie jej wyników w treści projektowanych (stanowionych) przepisów prawa oraz zawarcie informacji o jej wynikach, w ocenie skutków projektowanej regulacji lub w uzasadnieniu do projektowanej regulacji było niezwykle pomocne – zarówno dla projektodawcy tworzącego przepisy z zakresu przetwarzania danych osobowych na potrzeby konkretnej regulacji i jej celów, jak i wykonawców ustanawianych

[240] DOL.401.51.2021; ustawa została uchwalona 19 września 2021 r. Tekst ogłoszony w Dzienniku Ustaw poz. 1898.
[241] DOL.401.624.2021.
[242] DOL.401.358.2021.

norm prawnych, celem stworzenia przepisów zapewniających stosowanie przepisów rozporządzenia 2016/679.

Jako inny przykład projektu, na potrzeby którego wykonana została ocena skutków dla ochrony danych, wskazać także można **projekt rozporządzenia Ministra Zdrowia w sprawie kredytów na studia medyczne**[243].

7.2. Wyłączenia bądź ograniczenia praw osób, których dane dotyczą

W przekazywanych do organu nadzorczego do zaopiniowania projektach pojawiały się przepisy związane z ograniczeniami bądź wyłączeniami stosowania niektórych przepisów RODO. Niestety, w niewielu z analizowanych przypadków spełnione zostały wymogi przewidziane przepisami RODO. W związku z powyższym niezbędne było wskazywanie na konieczność rozróżnienia wyłączeń od ograniczeń, a także na warunki przewidziane w art. 23 RODO oraz informowanie, że nie mogą być one rozumiane jako wyłączenia spod regulacji RODO (wyłączenia przewidziane są bowiem jedynie w treści art. 13, 14 i 17 rozporządzenia). Wielu projektodawców nie wykazywało dostatecznej wiedzy w tym zakresie, nie wie, że ewentualne ograniczenia stosowania RODO mogą następować w dość szerokim, ale nie pełnym zakresie oraz tylko o ile spełnione zostaną warunki z art. 23, w szczególności dla zapewnienia poważnych celów, o których stanowi art. 23 ust. 1. Niezbędne było zatem zwracanie uwagi na to, że zgodnie z art. 23 ust. 1 (prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający) może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym np. bezpieczeństwu narodowemu. Niezbędne było też wskazywanie projektodawcom, iż ograniczenie praw osób, których dane dotyczą, możliwe jest jedynie po spełnieniu następujących przesłanek:

1. odpowiednio skonstruowane powinny być przepisy aktu prawnego – może ograniczać ściśle określony wskazanymi przepisami rozporządzenia 2016/679 zakres praw i obowiązków, tj. tych, które przewidziane są w art. 12–22 i w art. 34 oraz art. 5 rozporządzenia 2016/679;

[243] DOL.401.582.2022.

2. akt prawny ograniczający w ww. zakresie prawa i obowiązki musi zawierać przepisy odpowiadające prawom i obowiązkom przewidzianym w art. 12–22 rozporządzenia 2016/679;
3. wprowadzane w ww. sposób ograniczenie nie może naruszać istoty podstawowych praw i wolności;
4. wprowadzane w ww. sposób ograniczenie musi być w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym;
5. ograniczenie służyć może jednemu z celów przewidzianych w art. 23 ust. 2 lit. a–j rozporządzenia 2016/679. Dodatkowo, niezbędne jest – dla wprowadzania zgodnego z przepisami RODO ograniczenia praw – aby akt prawny, o którym mowa w art. 23 ust. 1 rozporządzenia 2016/679, zawierał szczegółowe przepisy przynajmniej w stosownym przypadku o:
    a. celach przetwarzania lub kategorii przetwarzania;
    b. kategoriach danych osobowych;
    c. zakresie wprowadzonych ograniczeń;
    d. zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
    e. określeniu administratora lub kategorii administratorów;
    f. okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;
    g. ryzykach naruszenia praw lub wolności osoby, której dane dotyczą;
    h. prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Organ nadzorczy zwrócił uwagę na treść wytycznych 10/2020 w sprawie ograniczeń na podstawie art. 23 rozporządzenia 2016/679. Celem tych wytycznych jest wskazanie warunków stosowania ograniczeń z art. 23 rozporządzenia 2016/679 w świetle przepisów Karty praw podstawowych UE i rozporządzenia 2016/679. Dokument zawiera dokładną analizę kryteriów stosowania ograniczeń; ocen, których należy dokonywać, a odnoszących się do tego, jak osoby, których dane dotyczą, mogą wykonywać swoje prawa po zniesieniu ograniczeń oraz konsekwencji naruszeń art. 23 rozporządzenia 2016/679. Ponadto w wytycznych dokonana została analiza, w jaki sposób środki prawne określające ograniczenia, muszą spełniać wymóg przewidywalności oraz

analiza podstaw ograniczeń wymienionych w art. 23 ust. 1 rozporządzenia 2016/679. Wskazano również obowiązki i prawa, które mogą zostać ograniczone. Wytyczne opisują test „niezbędności i proporcjonalności", któremu ograniczenia muszą zostać poddane i następnie go spełnić w oparciu o art. 23 ust. 1 rozporządzenia 2016/679. Podkreślono w nich, że art. 23 ust. 1 RODO wymienia szereg wymagań. Muszą one zostać spełnione wszystkie, aby można było zgodnie z prawem powołać się na dany środek. W wytycznych wskazano również, że zgodnie z zasadą proporcjonalności, treść środka prawnego ograniczającego prawa nie może wykraczać poza to, co jest ściśle niezbędne do ochrony celów wymienionych w art. 23 ust. 1 lit. a–j rozporządzenia 2016/679. EROD w omawianym dokumencie podkreśliła, 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 przepisów Karty (art. 7 i 8) lub innych gwarancji w niej zawartych. Możliwość wprowadzenia ograniczeń, przyznana państwom członkowskim na mocy art. 23 ust. 1 RODO, może być realizowana wyłącznie z poszanowaniem zasady proporcjonalności, zgodnie z którą odstępstwa i ograniczenia w odniesieniu do ochrony danych osobowych muszą mieć zastosowanie tylko w takim zakresie, w jakim jest to bezwzględnie konieczne. Organ nadzorczy wskazywał, że niezbędne jest – o ile ograniczenie odpowiada warunkom z art. 23 ust. 1 rozporządzenia 2016/ 679 – wyznaczenie, stosownie do art. 23 ust. 2 RODO, przepisów odpowiadających prawom i obowiązkom przewidzianym w art. 12–22 rozporządzenia 2016/679.

Jako przykład projektów aktów prawnych przekazanych do organu nadzorczego i analizowanych również w kontekście ograniczeń czy wyłączeń praw z RODO, wymienić można **projekt ustawy o ochronie osób zgłaszających naruszenia prawa**[244] (tzw. sygnalistów), w uwagach do którego organ nadzorczy wskazał na możliwość szczególnego rozwiązania, jakim jest odłożenie w czasie realizacji obowiązku informacyjnego z art. 14 ust. 1 RODO w zakresie źródła danych. Jest to specyficzny przykład i szczególna sytuacja dotycząca przepisów, w których należy pogodzić prawo do informacji osoby dopuszczającej się naruszenia, a której dane dotyczą, z dobrem prowadzonego postępowania sprawdzającego sygnalizowane zgłoszenie oraz z przyjmowaniem zgłoszeń naruszeń.

[244] DOL.401.512.2021.

Jako inny przykład można wskazać także **projekt ustawy o badaniach klinicznych produktów leczniczych stosowanych u ludzi**[245] (w konsekwencji projektodawca zrezygnował z art. 7, który dotyczył tych kwestii).

7.3. Precyzyjne określenie ról podmiotów w procesie przetwarzania danych

Do Urzędu Ochrony Danych Osobowych wpływa bardzo duża liczba sygnałów świadczących o wątpliwościach różnych podmiotów, co do ich ról w procesie przetwarzania danych osobowych. Wnioskować można, że przyczyną tych wątpliwości było nieumiejętne tworzenie regulacji prawnych, tj. takich, które uwzględniałyby przewidziane przepisami RODO możliwości (administrowanie, współadministrowanie, powierzenia przetwarzania). Organ wskazywał projektodawcom na konieczność kształtowania przepisów odpowiadających rzeczywistym potrzebom i celom tworzonych regulacji prawnych. W drugiej połowie roku sprawozdawczego, w uzasadnionych przypadkach, odwoływał się wprost do przyjętych 7 lipca 2021 r. przez Europejską Radę Ochrony Danych wytycznych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego. Wskazywał, że na gruncie RODO pojęcie administratora jest pojęciem funkcjonalnym i ma na celu podział odpowiedzialności, zgodnie z rzeczywistymi rolami w procesach przetwarzania danych. Oznacza to, że status prawny podmiotu, jako administratora, musi zasadniczo być określany przez jego rzeczywistą działalność w określonej sytuacji – w tym przypadku projektowaną przepisami i poprzedzoną oceną skutków.

Jako przykład opiniowanego przez organ nadzorczy projektu, w którym podział ról podmiotów przetwarzających dane (w powstającym rejestrze) nie został przejrzyście ukształtowany, wymienić można **projekt ustawy o zmianie ustawy o wspieraniu rodziny i systemie pieczy zastępczej oraz niektórych innych ustaw**[246]. W związku z tym w odnoszącym się do niego stanowisku organ nadzorczy wskazał, że skoro jeden rejestr będzie prowadzić wiele podmiotów, to z projektowanych przepisów powinny wynikać zasady ich odpowiedzialności za przetwarzane dane. Nie będzie to możliwe, jeżeli dla każdego z podmiotów precyzyjnie nie zostaną ukształtowane wszystkie cele przetwarzania danych w rejestrze. To bowiem z przepisów prawa powinno wynikać, w jakim celu określone podmioty będą pozyskiwać i dalej przetwarzać dane osobowe oraz jakim podmiotom je udostępniać w tak określonych zasobach.

[245] DOL.401.196.2021.
[246] DOL.401.497.2021.

Kilkukrotnie organ nadzorczy zwracał uwagę na brak przejrzystości w ukształtowaniu statusu tzw. administratora systemu w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[247], gdyż takiego pojęcia nie ma w rozporządzeniu 2016/679. Opiniując **projekt ustawy o zmianie ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi oraz niektórych innych ustaw**[248], organ nadzorczy podkreślił, że rozporządzenie 2016/679 nie zna pojęcia „administratora systemu", posługuje się natomiast pojęciem administratora. Projektowana regulacja powinna więc zostać odpowiednio zmodyfikowana tak, aby odpowiadać terminologii rozporządzenia 2016/679, a status podmiotów przetwarzających dane ukształtować w taki sposób, aby zadośćuczynić zasadzie rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679). Za konieczne Prezes UODO uznał także odpowiednie ukształtowanie relacji pomiędzy podmiotami wskazywanymi jako „administrator" oraz „administrator systemu" tak, aby nie dochodziło do osłabiania standardów ochrony danych osobowych, w tym danych szczególnych kategorii. Wskazał przy tym, że istotne jest, czy dane będą pomiędzy tymi podmiotami przekazywane, czy podmioty te będą nimi współadministrować, a jeżeli tak, należy zawsze precyzyjnie określać wszystkie procesy przetwarzania i podstawy prawne dla ich realizacji.

Podobne spostrzeżenia zostały sformułowane w związku z opiniowaniem **projektu ustawy o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027 (UC95)**[249]. Organ nadzorczy zauważył, że przepisy projektowanej ustawy powinny szczegółowo regulować kwestie podziału ról w procesach przetwarzania danych osobowych. Brak doprecyzowania zadań podmiotów i celów przetwarzania danych w przepisach powszechnie obowiązujących często prowadzi do zawierania umów powierzenia w sytuacjach, w których podmioty realizują odrębne zadania. Organ nadzorczy w przekazanej projektodawcy opinii zwrócił uwagę na konieczność ustalenia ról odpowiednio do rzeczywistego przetwarzania danych osobowych. Ma to kluczowe znaczenie z punktu widzenia odpowiedzialności za realizację praw i obowiązków wynikających z przepisów o ochronie danych osobowych. Projektodawca powinien uwzględnić, że budowane normy powinny być przejrzyste także pod kątem ustalenia odpowiedzialności podmiotów realizujących w ich oparciu procesy przetwarzania danych, aby wyeliminować wszelkie ryzyka związane z niewłaściwą ich interpretacją. Konsekwencją przyjmowania takich niedoskonałych przepisów jest naruszanie zasad dotyczących przetwarzania

[247] Dz. U. z 2021 r. poz. 666 z późn. zm.
[248] DOL.401.403.2021.
[249] DOL.401.446.2021.

danych osobowych i narażenie wykonawców norm na działania na danych niezgodne z rozporządzeniem 2016/679. Status prawny podmiotu jako „administratora" musi zasadniczo być określany, przypisywany przez pryzmat jego rzeczywistych działań (realnej działalności) w określonej sytuacji przetwarzania danych osobowych. Określanie administratora nie może i nie powinno polegać jedynie na formalnym jego wyznaczeniu, nazwaniu go tak w przepisach. Oznacza to, że podział ról zwykle powinien wynikać z analizy elementów faktycznych potrzeb i celów przetwarzania danych osobowych lub okoliczności sprawy i jako taki nie podlega negocjacjom. Należy uwzględnić fakt, iż koncepcja administratora odnosi się do wpływu administratora na przetwarzanie poprzez wykonywanie uprawnień decyzyjnych. Administrator to podmiot (organ), który decyduje o kluczowych elementach dotyczących przetwarzania. Organ nadzorczy od wielu lat postulował wprowadzenie przepisów odpowiadających zasadom ochrony danych osobowych we wskazanym obszarze.

Innym przykładem opiniowanego przez organ nadzorczy projektu, w którym nie określono precyzyjnie ról podmiotów w procesie przetwarzania danych osobowych, był **rządowy projekt ustawy o zmianie ustawy o efektywności energetycznej oraz niektórych innych ustaw (druk nr 957)**[250]**,** który dotyczył prowadzenia przez Instytut Ochrony Środowiska – Państwowy Instytut Badawczy, centralnego rejestru oszczędności energii finalnej. Organ nadzorczy zwrócił uwagę na konieczność doprecyzowania w niniejszym projekcie ról i obowiązków podmiotów odpowiedzialnych za cele i sposoby przetwarzania danych osobowych oraz ewentualnie czerpiących dane osobowe z systemu teleinformatycznego oraz zasilających system danymi osobowymi. W związku z wyznaczaniem osób upoważnionych do wprowadzania danych do systemu organ nadzorczy wskazał, że uwzględnić należy role poszczególnych podmiotów w procesach przetwarzania danych osobowych (administrowanie/współadministrowanie). Wskazane role powinny odzwierciedlać rzeczywiste przetwarzanie danych, które projektodawca uznał mocą tych przepisów za dozwolone.

7.4. Otwarte dane

W 2021 roku kontynuowane były prace nad **projektem ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego**[251], która implementuje do polskiego porządku prawnego dyrektywę 2019/1024/UE Parlamentu Europejskiego i Rady z dnia 20

[250] DOL.401.75.2021.
[251] DOL.401.398.2020.

czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, a przy tym nowelizowała przepisy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wprowadzając instytucję prawną zintegrowanej platformy analitycznej.

Organ nadzorczy przekazał liczne opinie dotyczące tego projektu, zarówno na rządowym etapie prac legislacyjnych, jak i po przekazaniu projektu do Sejmu RP i Senatu RP. Zgłaszane uwagi dotyczyły m.in. art. 6 ust. 2 projektu dotyczącego ponownego wykorzystania danych osobowych osób pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji. Organ nadzorczy na każdym z etapów prac legislacyjnych wskazywał, aby przepisy projektu dedykowane ponownemu wykorzystaniu danych osobowych osób pełniących funkcje publiczne (w szczególności art. 6 ust. 2 projektu) – jak również odpowiadająca temu przepisowi projektu regulacja w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[252] dotycząca udostępniania danych osobowych osób pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w trybie dostępu do informacji publicznej (art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej) – zostały uzupełnione o wynikający z RODO mechanizm **ważenia wartości.** Ma to szczególnie istotne znaczenie dla systemu ochrony danych osobowych w Polsce i dla zgodnego z przepisami RODO przetwarzania danych osobowych ww. osób. Istotna kwestia, na którą także zwracał uwagę organ nadzorczy, to zasadność wprowadzenia przepisami opiniowanego projektu (poprzez nowelizację ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[253]) rozwiązania organizacyjno-technicznego o nazwie „zintegrowana platforma analityczna". Organ nadzorczy wskazywał, że zintegrowana platforma analityczna – w formie zaproponowanej w rozdziale 3b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne – to rozwiązanie, które wiązać się będzie z przetwarzaniem danych osobowych obywateli na wielką skalę, w tym w zakresie szczególnych kategorii danych. Co więcej, zaproponowane rozwiązanie (narzędzie) tylko wówczas mogłoby być wykorzystywane w sposób zaplanowany przez projektodawcę, gdyby przepisy prawa krajowego (ustawy sektorowe) wprowadzały obowiązek realizacji określonych procesów przetwarzania przez konkretnych administratorów, w określonych celach (art. 6 ust. 3 rozporządzenia 2016/679), z wykorzystaniem zintegrowanej platformy analitycznej. Zaproponowane i wprowadzone do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne rozwiązanie

[252] Dz. U. z 2020 r. poz. 2176.
[253] Dz. U. z 2021 r. poz. 670, 952 i 1005.

dotyczące ZPA (Zintegrowana Platforma Analityczna) jest niewystarczające, zaś konieczne było dokonanie wnikliwego przeglądu i odpowiedniego dostosowania obowiązujących przepisów (ustaw sektorowych), które jednak nie nastąpiło. Wskazano, że taki przegląd i dostosowanie przekracza ramy niniejszego projektu i dlatego organ nadzorczy powtórzył postulat – zgłaszany na rządowym etapie prac legislacyjnych oraz w toku prac legislacyjnych prowadzonych przez Sejm Rzeczypospolitej Polskiej – by zintegrowana platforma analityczna stała się przedmiotem odrębnego procesu legislacyjnego, w czasie którego przeprowadzone zostaną niezbędne analizy i konsultacje.

W tym miejscu wskazać należy na opiniowany **projekt rozporządzenia Rady Ministrów w sprawie wykazu rejestrów publicznych i systemów teleinformatycznych, z których udostępniane są dane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej**[254]. W stanowisku do tego projektu organ nadzorczy wskazał, że rozwiązania dotyczące przetwarzania danych osobowych na potrzeby analiz w zintegrowanej platformie analitycznej są kluczowe dla systemu ochrony danych osobowych i mają istotny wpływ na realizację prawa do prywatności przez osoby, których dane dotyczą, w skali całego kraju.

W 2021 roku kontynuowane były też prace **nad projektem rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi i zmiany rozporządzenia (UE) 2018/1724 (akt o zarządzaniu danymi)**[255]. Organ nadzorczy, wyrażając stanowisko do kolejnych wersji tego projektu, finalnie pozytywnie ocenił kierunek zmian, zwracając jednocześnie uwagę na kwestie, które nie zostały przez projektodawcę uwzględnione. Dotyczyły one m.in. przepisu projektu zakładającego włączenie, będących w posiadaniu organów sektora publicznego, danych chronionych na podstawie poufności informacji statystycznych, do kategorii danych, które mogą być objęte ponownym wykorzystaniem (re-use). W opinii organu nadzorczego rozwiązanie to może prowadzić do naruszenia zasady, zgodnie z którą dane osobowe zebrane do celów statystycznych mogą być wykorzystywane wyłącznie do tego celu. Udostępnianie lub wykorzystywanie tych danych dla innych celów niż podane w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej jest zabronione. Organ nadzorczy wyjaśnił także, że na zasadzie tej opiera się cała konstrukcja tajemnicy statystycznej w prawie polskim nadając tej tajemnicy charakter absolutny.

[254] DOL.401.624.2021.
[255] DOL.401.660.2020.

7.5. Informatyzacja, nowe technologie, łączenia zbiorów danych

Rok 2021 to kontynuacja daleko posuniętej automatyzacji procesów decyzyjnych wobec osób fizycznych oraz wielkoskalowe przetwarzanie informacji o osobach przy wykorzystaniu systemów teleinformatycznych. Przedkładane projekty w dużym stopniu dotyczyły przetwarzania przez podmioty publiczne danych osobowych przy wykorzystaniu różnych aplikacji mobilnych. Jako przykład wskazać można projekt **rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie leczenia krwią i jej składnikami w podmiotach leczniczych wykonujących działalność leczniczą w rodzaju stacjonarne i całodobowe świadczenia zdrowotne**[256]**.** Odnosząc się do koncepcji pozostawienia wykonawcom norm zupełnej dowolności przy dokonywaniu wyboru odpowiednich środków technicznych i organizacyjnych, w tym rodzajów aplikacji mających służyć prowadzeniu kontroli, organ nadzorczy wskazał, że rozwiązania w tym zakresie powinny zostać określone w przepisach prawa, jako wiążące podmioty wypełniające zadania z zakresu publicznej służby krwi. Przepisy prawa powinny określać dopuszczalne formy i narzędzia przeprowadzania kontroli w sposób zdalny, gdyż pozostawienie wyboru w tym zakresie centrom krwiodawstwa powoduje ryzyko korzystania z rozwiązań niedających gwarancji bezpieczeństwa, w tym także w odniesieniu do danych szczególnej kategorii z art. 9 ust. 1 rozporządzenia 2016/6791, tj. danych o stanie zdrowia. Nie każda dostępna na rynku aplikacja umożliwiająca komunikację zdalną, w pełni odpowiada wymogom przepisów RODO, w tym jego art. 24 i 32. Organ nadzorczy podkreślił, że przyjmowanie rozwiązań dowolnych nie może prowadzić do przetwarzania danych osobowych, w tym o stanie zdrowia, z narażeniem na ryzyko braku podlegania przepisom RODO czy przetwarzania ich w państwie trzecim bez zachowania jego wymogów. Trudno zaakceptować sytuację, gdy w każdym centrum krwiodawstwa kontrola – będąca obowiązkiem wynikającym z przepisów prawa – przeprowadzana będzie za pomocą różnych, w tym niezaufanych narzędzi czy aplikacji. Organy zarówno publiczne, jak i niepubliczne, ale realizujące zadania publiczne, powinny być wyposażone przy realizacji takich zadań w instrumenty precyzyjnie określone w przepisach prawa. Za określeniem chociażby minimalnych standardów bezpieczeństwa przetwarzania danych w przypadku takich podmiotów, przemawia charakter realizowanych przez te podmioty zadań publicznych (kontrole) i spoczywającej na nich z tego tytułu odpowiedzialności. Dlatego to ustawodawca, wdrażając właściwe przepisy prawa, powinien zadbać o wskazanie co najmniej kryteriów wymaganych dla zapewnienia odpowiednich gwarancji dla praw i wolności osób, których

[256] DOL.401.231.2021.

dane osobowe będą przetwarzane w ramach takiej kontroli, co pozwoli zarówno kontrolującym, jak i kontrolowanym zapewnić należytą ochronę danych osobowych dla realizacji celów wskazanych w przepisach.

W tym kontekście wskazać także należy na **projekt ustawy o zmianie ustawy Prawo lotnicze**[257], który przewidywał wprowadzenie procedury opartej na składaniu wniosków o sprawdzenie, które miałyby być przekazywane za pośrednictwem dedykowanej w tym celu „aplikacji dostępowej" pn. Weryfikacja negatywnych przesłanek – Straż Graniczna (aplikacja WNP-SG). Organ podkreślił, że żaden z przepisów projektu nie przewiduje regulacji dotyczących aplikacji WNP-SG, w tym nie definiuje jej, nie wskazuje praw i obowiązków organów związanych z jej prowadzeniem, funkcjonowaniem i wykorzystywaniem, zwłaszcza dla celów przetwarzania danych osobowych. Organ nadzorczy wskazał, że przepisy powszechnie obowiązującego prawa nie określają zatem, w jakich celach, jakie podmioty, na jakich zasadach – stosownie do przepisów rozporządzenia 2016/679 – mogą przetwarzać dane osobowe z użyciem tej aplikacji.

Innym przykładem zastosowania bliżej nieokreślonej aplikacji był poselski **projekt ustawy o szczególnych rozwiązaniach zapewniających możliwość prowadzenia działalności gospodarczej w czasie epidemii COVID-19 (druk nr 1846)**[258]. Jeden z projektowanych przepisów wskazywał, że do weryfikacji danych zawartych w unijnym cyfrowym zaświadczeniu COVID oraz wizerunku twarzy, stosuje się aplikację mobilną, udostępnioną przez jednostkę podległą ministrowi właściwemu do spraw zdrowia, właściwą w zakresie systemów informacyjnych ochrony zdrowia. Organ nadzorczy zwrócił uwagę, że projektowany przepis ma charakter blankietowy – nie określa bowiem, czym ma być aplikacja oraz w jaki sposób ma zapewnić przetwarzanie danych osobowych odpowiadające zasadom określnym w art. 5 rozporządzenia 2016/679, w szczególności zasadzie zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a), oraz zasadzie integralności i poufności (art. 5 ust. 1 lit. f). Wykorzystywanie technologii mobilnych, zwłaszcza mających bliżej nieokreślony dostęp do rejestrów publicznych, a tym bardziej aplikacji niedookreślonych oraz niezweryfikowanych pod względem ich zgodności z przepisami RODO, jest – jak ocenił Prezes UODO – obarczone znacznym ryzykiem spowodowania naruszenia bezpieczeństwa czy naruszenia innych przepisów rozporządzenia 2016/679, które jest tym bardziej dotkliwe, jeśli dotyczy danych sensytywnych (w tym danych o stanie zdrowia z art. 9 ust. 1 RODO). Wykorzystanie nowoczesnych

[257] DOL.401.51.2022.
[258] DOL.401.601.2021.

technologii jest jednym z aspektów wpływających na zasadność wykonania oceny skutków i analizy ryzyk takiego przetwarzania danych osobowych, a tym bardziej należących do kategorii szczególnie chronionych. Jednocześnie organ nadzorczy wskazał, że przy konstruowaniu tego typu rozwiązań warto oprzeć się również na wytycznych EROD 04/2020 przyjętych 21 kwietnia 2020 r. w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19.

Wskazać także należy na opiniowany przez organ nadzorczy rządowy **projekt ustawy o zmianie ustawy o Karcie Dużej Rodziny, ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawy o opiece nad dziećmi w wieku do lat 3**[259]. Kwestia oprogramowania dedykowanego dla urządzeń mobilnych, zawierającego usługi ułatwiające korzystanie z przyznanych uprawnień, udostępnionego przez ministra właściwego do spraw rodziny, została uregulowana ustawą z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw[260]. Oprogramowaniem dedykowanym dla urządzeń mobilnych jest Aplikacja mKDR, która wskazywana jest w informacji zamieszczonej na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw rodziny. Organ nadzorczy zauważył także, że odpowiedzi na powyższe kwestie częściowo można znaleźć jedynie w klauzuli informacyjnej zamieszczonej w Biuletynie Informacji Publicznej Ministerstwa Rodziny i Polityki Społecznej, gdyż w zakładce strony internetowej tego Ministerstwa dedykowanej tej aplikacji nie można odnaleźć regulaminu określającego jej działanie. Organ nadzorczy wskazał także, iż nie jest jasne, jaki system teleinformatyczny umożliwia obsługę funkcjonalności związanych z kartami elektronicznymi, które pozwalają na potwierdzenie uprawnień członków rodzin wielodzietnych oraz zapewniają usługi ułatwiające korzystanie z uprawnień przyznanych na podstawie Karty Dużej Rodziny. Dla porównania organ nadzorczy wskazał, jak szczegółowo – w stosunku do Aplikacji mKDR – uregulowane zostało działanie publicznej aplikacji mobilnej (mObywatel) w art. 19e i następnych ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[261], która również będzie pozwalać na obsługę elektronicznych Kart Dużej Rodziny. Ustawa o KDR wymaga zatem, w opinii Prezesa UODO, zapewnienia w treści jej przepisów kompleksowej regulacji doprecyzowującej kwestię przetwarzania danych w Aplikacji mKDR pod kątem zasad dotyczących przetwarzania danych osobowych.

[259] DOL.401.81.2021.
[260] Dz. U. z 2018 r. poz.1544 z późn. zm.
[261] Dz. U. z 2020 r. poz. 346 z późn. zm.

Kolejnym przykładem regulacji dotyczącej przetwarzania danych osobowych w systemach teleinformatycznych jest **projekt ustawy o zmianie ustawy o cudzoziemcach oraz niektórych innych ustaw**[262]. Organ nadzorczy zwrócił uwagę na rozwiązanie, w którym Straż Graniczna miałaby samodzielnie pozyskiwać z systemu teleinformatycznego Zakładu Ubezpieczeń Społecznych objęte tajemnicą dane płatników, którzy w ostatnim kwartale zgłosili do ubezpieczeń społecznych co najmniej jednego cudzoziemca, a także dane ubezpieczonego cudzoziemca. Miałoby się to odbywać z wykorzystaniem bliżej niesprecyzowanych, własnych lub innych, systemów teleinformatycznych. Wątpliwości pod kątem zgodności z zasadami ochrony danych osobowych wzbudził także przepis, który uprawniałby Szefa Urzędu do Spraw Cudzoziemców oraz wojewodę do pozyskiwania z systemu teleinformatycznego Straży Granicznej dowolnych danych (w tym danych osobowych) i to z wykorzystaniem bliżej niesprecyzowanych, własnych lub innych, systemów teleinformatycznych, a Straż Graniczna (administrator tych danych osobowych) nie miałaby możliwości sprawowania jakiejkolwiek kontroli nad tym procesem. Ponadto organ nadzorczy zauważył, że projektowana regulacja nie przewiduje uprawnienia dla Straży Granicznej (administratora) do kontrolowania spełniania wskazanych warunków dopuszczalności pozyskiwania przez Szefa Urzędu do Spraw Cudzoziemców oraz wojewodę danych z systemu teleinformatycznego Straży Granicznej, co istotnie utrudni Straży Granicznej sprawowanie kontroli nad wykorzystaniem danych, których ta formacja jest administratorem.

Wskazać w tym miejscu należy również na opiniowany **projekt ustawy o niektórych umowach zawieranych elektronicznie (UD230)**[263], który dotyczył rozwiązań wiążących się z przetwarzaniem na dużą skalę w centralnym systemie teleinformatycznym danych osobowych wszystkich osób aktywnych zawodowo, w tym również danych o charakterze prywatnym, jak adres poczty elektronicznej i numer telefonu. Organ nadzorczy zwrócił uwagę na brak wskazania w przepisach sposobów zabezpieczenia danych przetwarzanych na dużą skalę w systemie obejmującym dane wszystkich osób aktywnych zawodowo, co jest niezgodne z zasadami przetwarzania danych osobowych z art. 5 RODO. Dodatkowo Prezes UODO wskazał, że koncepcja przetwarzania danych osobowych dla celów statystycznych powinna oznaczać wykonywanie operacji na danych anonimowych albo spseudonimizowanych, a nie zindywidualizowanych.

[262] DOL.401.271.2021.
[263] DOL.401.595.2021.

W kontekście postępującej informatyzacji nie można pominąć systemu **„elektroniczne zarządzanie dokumentacją w administracji publicznej" EZD RP,** prowadzonego przez Kancelarię Prezesa Rady Ministrów i ministra właściwego do spraw informatyzacji, który ma na celu udostępnienie jednolitego i bezpłatnego narzędzia do elektronicznego zarządzania dokumentacją w administracji publicznej – systemu EZD RP. Realizacja tak istotnego projektu, dla którego mają być przetwarzane na masową skalę dane osobowe, w tym dane szczególnych kategorii i dane z art. 10 rozporządzenia 2016/679, w ocenie organu nadzorczego wymagało rozważenia, wybrania i zastosowania najlepszych rozwiązań organizacyjno-prawnych, zwłaszcza tych, przewidzianych w RODO. W ramach konsultacji wdrażania systemu EZD RP został upubliczniony i poddany konsultacji dokument Strategia dystrybucji, wdrażania i utrzymania EZD RP od 2022 r. – projekt (Dokument wdrażania EZD RP1), w związku z którym organ nadzorczy skierował do KPRM **wystąpienie, w którym zwrócił uwagę na kwestie związane z zapewnieniem ochrony danych przetwarzanych z wykorzystaniem tego narzędzia**[264]. Projektowany system dotyczy podmiotów publicznych dla realizacji ich zadań, w ramach których mają być przetwarzane dane objęte tajemnicami prawnie chronionymi. Natomiast w dokumencie wdrażania EZD RP nie zostały zawarte regulacje dotyczące przetwarzania danych osobowych.

Zwrócono uwagę, że dokument wdrażania EZD RP nie zawiera żadnych informacji o implementacji, wynikających z rozporządzenia 2016/679, procedur i czynności niezbędnych do tworzenia nowego systemu teleinformatycznego. Tymczasem kluczowe znaczenie, oprócz oceny skutków dla ochrony danych, powinien mieć także mechanizm uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych, gdyż projektowany system EZD RP wiąże się z tworzeniem nowych baz i systemów teleinformatycznych, w których przetwarzane będą dane osobowe na wielką skalę. W ocenie organu nadzorczego wdrożenie wymienionych zasad umożliwi wykazanie zgodności planowanego przedsięwzięcia z przepisami o ochronie danych osobowych, a także pozwoli zweryfikować, czy dla jego realizacji jest niezbędne nowe ukształtowanie norm prawa krajowego, które wraz z rozporządzeniem 2016/679 stworzą spójny system ochrony danych osobowych.

UODO zwrócił uwagę, że projektując założenia systemu EZD RP należy także dokonać oceny, jakie podmioty i na jakiej podstawie prawnej będą miały dostęp do danych osobowych różnych kategorii zawartych w tym systemie. Zasadne jest rozważenie, czy będzie dochodzić do powierzenia

[264] DOL.413.5.2021.

przetwarzania danych osobowych zewnętrznym podmiotom i czy takie rozwiązanie jest bezpieczne z punktu widzenia dostępu do tych tajemnic, jak również szeregu zagrożeń związanych m.in. z cyberbezpieczeństwem. Konieczne jest także rozważenie, czy taka konstrukcja pozwala na bezpieczne i zgodne z RODO przetwarzanie danych w chmurze i przekazywanie danych do krajów trzecich. Ma to szczególne znaczenie w świetle wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie C-311/18 – Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillianowi Schremsowi. Zwrócono uwagę, że w tym kontekście istotny jest sposób, zakres i forma partycypacji podmiotów zewnętrznych dla realizacji procesów przetwarzania danych w EZD RP. Wiele wątpliwości wyeliminowałoby przyjęcie instrumentu prawnego spełniającego wszystkie wymogi zawarte w art. 28 ust. 3 rozporządzenia 2016/679.

Na wyrok w sprawie C-311/18 organ nadzorczy powoływał się w 2021 roku, opiniując projekty aktów prawnych oraz umowy międzynarodowe z państwami trzecimi, które wiążą się z przekazywaniem danych osobowych do państwa trzeciego. Wskazać należy, że na podstawie orzeczenia TSUE w sprawie Schrems II (C-311/18) EROD wydała zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych z dnia 10 listopada 2020 r. oraz wytyczne 2/2020 z 15 grudnia 2020 r. w sprawie art. 46 ust. 2 lit. a i art. 46 ust. 3 lit. b rozporządzenia 2016/679 dotyczące przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG, które mają na celu przedstawienie oczekiwań EROD co do zabezpieczeń, które należy wprowadzić za pomocą prawnie wiążącego i egzekwowalnego instrumentu między podmiotami publicznymi lub pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego za pomocą uzgodnień administracyjnych między podmiotami publicznymi[265].

Nawiązując do pojawiającego się przy opiniowaniu wielu projektowanych przepisów problemu wykorzystywania nowych technologii na potrzeby wykonywania operacji na danych osobowych, należy także zwrócić uwagę na wspieranie działań państwa z zakresu m.in. **technologii FinTech** i współpracy m.in. z UKNF w tym zakresie. Wprawdzie organ nadzorczy nie posiada inicjatywy ustawodawczej, to w korespondencji prowadzonej z UKNF[266] każdorazowo podkreśla, że UODO niezmiennie deklaruje wsparcie eksperckie przy wypracowaniu przepisów prawa krajowego

[265] Jako przykład wskazać można Umowę między Ministrem Edukacji i Nauki Rzeczypospolitej Polskiej a Ministrem Edukacji i Szkolnictwa Wyższego Państwa Kataru o współpracy w dziedzinie szkolnictwa wyższego i nauki, DOL.401.515.2021.
[266] np. DOL.071.44.2021.

z zakresu FinTech, których celem byłoby zachowanie testu równowagi pomiędzy prawem do ochrony prywatności a poszanowaniem innych praw, w przypadku przedstawienia do zaopiniowania konkretnych propozycji zmian legislacyjnych. Jako przykłady aktów prawnych, w których wskazuje się bariery związane z ww. technologią wskazać można na przepisy ustawy Prawo bankowe (dotyczące analizy zdolności kredytowej) czy ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych (w zakresie umożliwienia BIG-om dostępu do Rejestru Ksiąg Wieczystych poprzez API).

7.6. Łączenie baz danych

Łączenie baz danych to kolejne zagadnienie będące przedmiotem szczególnego zainteresowania organu nadzorczego, który w swoich opiniach zwracał uwagę, że żądanie ujawnienia danych osobowych, z którym występują organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Organy publiczne powinny przestrzegać przepisów o ochronie danych i przetwarzać dane zgodnie z celami, dla których zostały pozyskane. W opiniach dotyczących zagrożeń wynikających z łączenia baz danych, organ nadzorczy zwracał uwagę na wytyczne motywu 31 RODO, z którego wynika, że ujawnianie danych podmiotom publicznym powinno mieć co do zasady charakter wnioskowy. Organ nadzorczy, opiniując projekty dotyczące łączenia baz danych, wskazywał na wyrok TSUE C-201/14 w sprawie Smaranda Bara[267], w którym Trybunał orzekł, że odrębne organy w ramach administracji publicznej należy traktować jako odrębnych administratorów z własnymi przesłankami. W konsekwencji oznacza to, że organ, któremu w ramach administracji przekazuje się dane osobowe, jest odbiorcą. Jako przykład wskazać należy na opiniowany **projekt ustawy o zmianie ustawy o wspieraniu rodziny i systemie pieczy zastępczej oraz niektórych innych ustaw**[268], jak również **projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie wzmocnienia stosowania zasady równości wynagrodzeń dla kobiet i mężczyzn za taką samą pracę lub pracę o takiej samej wartości, za pośrednictwem mechanizmów przejrzystości wynagrodzeń oraz mechanizmów egzekwowania COM (2021) 93**[269].

[267] Wyrok Trybunału (trzecia izba) z dnia 1 października 2014 r.(wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Curtea de Apel Cluj – Rumunia) – Smaranda Bara i in./Casa Naţională de Asigurări de Sănătate, Preşedintele Casei Naţionale de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF).
[268] DOL.401.497.2021.
[269] DOL.401.98.2021.

Również **projekt ustawy o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw**[270] dotyczył zagadnienia związanego z łączeniem baz danych – pozyskiwania przez ministra właściwego do spraw oświaty i wychowania z bazy danych systemu informacji oświatowej (bazy danych SIO), danych osobowych nauczycieli i przekazanie tych danych Zakładowi Ubezpieczeń Społecznych w celu przeprowadzania analizy przyczyn nieobecności nauczycieli w pracy z powodu urlopu macierzyńskiego lub czasowej niezdolności do pracy wskutek choroby – w tym także monitorowania przyczyn, skali oraz cykliczności nieobecności. Umożliwiłoby to Zakładowi Ubezpieczeń Społecznych przygotowywanie – na potrzeby własne lub ministra właściwego do spraw oświaty i wychowania – badań, prognoz lub opracowań dotyczących nieobecności nauczycieli w pracy wskutek choroby, a także szacowania skutków finansowych zmian przepisów z zakresu ubezpieczeń społecznych.

Dostęp do danych osobowych z rejestrów publicznych za pośrednictwem systemów teleinformatycznych w formie teletransmisji był również przedmiotem zainteresowania organu nadzorczego w przypadku opiniowania **projektu ustawy o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw**[271]. Rozwiązania techniczne prowadzące do nieograniczonego w czasie sięgania przez sądy do danych zgromadzonych w rejestrach, bazach i ewidencjach publicznych, takich jak: Baza Usług Stanu Cywilnego, rejestr danych kontaktowych oraz ewidencja gruntów i budynków, na potrzeby prowadzonych postępowań nieprocesowych, zasadniczo zmieniają dotychczasowy model przetwarzania danych osobowych w trakcie procesu cywilnego. Dostęp do danych osobowych z rejestrów publicznych za pośrednictwem systemów teleinformatycznych w formie teletransmisji, generuje bowiem wiele ryzyk związanych w szczególności z koniecznością zachowania poufności i integralności tych danych, a także w kontekście i zakresie cyberbezpieczeństwa. Wprowadzenie rozwiązania, zgodnie z którym w trakcie postępowania cywilnego można w nieograniczony sposób w formie teletransmisji pozyskiwać dane osobowe z rejestrów publicznych, wymaga głębokiej analizy i refleksji w kontekście wprowadzenia odpowiednich procedur uwzględniających możliwe ryzyka dla przetwarzania w tej formie wymienionych danych osobowych. Podmioty zobowiązane do udostępniania sądom w drodze teletransmisji dostępu do prowadzonych przez siebie rejestrów i baz, nie przestają być administratorami zgromadzonych tam danych osobowych i cały czas ponoszą odpowiedzialność za legalność, celowość i proporcjonalność ich udostępniania. A zatem, celem uniknięcia ryzyka łączenia

[270] DOL.401.370.2021.
[271] DOL.401.605.2021.

zbiorów danych lub też przekazywania danych niezgodnie z celami, projektodawca powinien – w opinii Prezesa UODO – rozważyć wprowadzenie rozwiązań, które z jednej strony przyczynią się do usprawnienia procesów przetwarzania danych przez sądy w ramach sprawowania wymiaru sprawiedliwości, a z drugiej ograniczą ryzyka związane z tym przetwarzaniem, a także zapewnią administratorom tych zbiorów i baz danych realną kontrolę nad tym procesem wynikającym z ich statusu. Na aspekt przetwarzania danych w trybie teletransmisji pod kątem stworzenia dodatkowych gwarancji normatywnych, w związku z koniecznością realizacji zasady rozliczalności przez administratora udostępniającego, organ nadzorczy wielokrotnie zwracał uwagę w swoich opiniach legislacyjnych, a także w związku z doświadczeniami kontrolnymi.

7.7. Numer PESEL

Wykorzystywanie numeru PESEL to kolejne z zagadnień będące przedmiotem szczególnego zainteresowania UODO. PESEL jest bowiem unikatowym identyfikatorem o zasięgu ogólnym, zawierającym wiele dodatkowych informacji, m.in. o wieku i płci. Używa się go wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności podmiotu danych przewidzianych w RODO, oraz dla którego państwa członkowskie mogą określić szczególne warunki przetwarzania (art. 87). Przy opiniowaniu projektów przepisów, w których wykorzystywany ma być numer PESEL, myślą przewodnią organu nadzorczego jest wskazanie ustawodawcy, by w przepisach prawa używał wyłącznie rozwiązań gwarantujących zachowanie odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, jakie przewidują przepisy ogólnego rozporządzenia o ochronie danych. Niezwykle istotne jest to, że numer PESEL jest numerem referencyjnym, właściwie niezbywalnym i niezmienialnym, służącym do identyfikacji osoby w bardzo wielu sytuacjach. Ujawnienie numeru PESEL może rodzić ryzyko kradzieży tożsamości. Z kolei gdy staje się on daną powszechnie dostępną może być zestawiany z innymi danymi i wykorzystywany w innych celach niż pierwotnie zakładany i dla którego został pozyskany. Dlatego opiniując projekty aktów prawnych zakładających wykorzystywanie numeru PESEL, organ nadzorczy zawsze zwraca uwagę projektodawców na potrzebę uzasadnienia niezbędności jego przetwarzania. Jest to szczególnie istotne przy ocenie operacji związanych z wykorzystaniem numeru PESEL na dużą skalę, z użyciem nowych technologii, na odległość, w powiązaniu z innymi danymi, w tym szczególnych kategorii, przy czynieniu tych danych jawnymi, powszechnie dostępnymi czy używanymi przez wiele organów/podmiotów.

Pozytywnie należy ocenić prace nad **projektem rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie świadectw, dyplomów państwowych i innych**

druków[272], który dotyczył m.in. usunięcia numeru PESEL z legitymacji szkolnych. Kontynuując zapoczątkowane wiele lat temu podejście, także teraz, opiniując wymieniony projekt, organ nadzorczy zwrócił uwagę na kwestię niezbędności zamieszczania numerów PESEL na legitymacjach szkolnych. Po raz kolejny wskazał projektodawcy, jakim jest resort edukacji, że numer PESEL posiadacza legitymacji nie jest warunkiem koniecznym do identyfikacji ucznia, że za wystarczające dla celów, którym służy legitymacja szkolna, uznać należy pozostawienie w jej treści takich danych jak: wizerunek (zdjęcie) posiadacza, jego imię i nazwisko, data urodzenia, numer legitymacji. Te dane, w powiązaniu z adresem szkoły, numerem legitymacji i potwierdzeniem jej wydania przez dyrektora w postaci jego podpisu z datą albo nadruku imienia i nazwiska z datą wydania dokumentu, będą bezpośrednio identyfikowały danego ucznia. Przyjęcie takiego rozwiązania będzie zgodne z zasadą minimalizacji danych zawartą w art. 5 ust. 1 lit. c RODO. Organ nadzorczy wskazał, że projektodawca powinien wziąć pod uwagę to, że dane osobowe wpisane w legitymacjach staną się przedmiotem obrotu prawnego w związku z posługiwaniem się ww. dokumentami w różnych sytuacjach (np. przy potwierdzaniu prawa do ulgi za przejazd środkami transportu miejskiego), a nie w celach wyłącznie prywatnych. Po wymianie korespondencji pomiędzy Ministerstwem Edukacji i Nauki a organem nadzorczym, MEiN, które przez długi czas powoływało się na konieczność pozostawienia w legitymacjach numeru PESEL na potrzeby weryfikacji uprawień niepełnoletnich uczniów do korzystania ze świadczeń zdrowotnych, bez związku z celami szkolnymi/edukacyjnymi, przyznało rację organowi i zapowiedziało, że zaproponuje stosowne zmiany w przepisach prawa.

Numer PESEL był także przedmiotem zainteresowania organu nadzorczego w przypadku opiniowania **projektu rozporządzenia Ministra Sprawiedliwości w sprawie sposobu przeprowadzenia sprzedaży nieruchomości w drodze licytacji elektronicznej oraz sposobu uwierzytelniania użytkowników systemu teleinformatycznego obsługującego licytację elektroniczną**[273]. Zgodnie z projektowanymi przepisami rozporządzenia imiona, nazwisko oraz numer PESEL podlegają automatycznej weryfikacji w rejestrze PESEL, natomiast ani projektowane rozporządzenie, ani Kodeks postępowania cywilnego nie regulują, w jaki sposób system teleinformatyczny obsługujący licytację elektroniczną będzie połączony z rejestrem PESEL. Organ nadzorczy zauważył, że zgodnie z motywem 31 rozporządzenia 2016/679, ujawnianie danych podmiotom publicznym powinno mieć co do zasady charakter wnioskowy (odbywać się w formie pisemnej, być uzasadnione i mieć charakter wyjątkowy). Dlatego też przepisy powszechnie

[272] DOL.401.132.2021.
[273] DOL.401.393.2021.

obowiązujące powinny określać sposób teletransmisji danych pomiędzy rejestrem PESEL a systemem teleinformatycznym obsługującym licytację elektroniczną, tak by zachowane zostały zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679). W opinii Prezesa UODO nie powinno dochodzić do sytuacji udostępnienia danych bez zachowania kontroli uprzedniej przez administratora rejestru PESEL.

Opiniując **projekt ustawy o zawodzie ratownika medycznego oraz samorządzie ratowników medycznych**[274], organ nadzorczy wskazał zbędność przetwarzania jednocześnie numeru PESEL oraz daty urodzenia w celu identyfikacji ratownika medycznego. Wyjaśnił, że wystarczające wydaje się identyfikowanie ratownika poprzez numer prawa wykonywania zawodu (ewentualnie datę urodzenia), z wyłączeniem numeru PESEL. Tożsama kwestia była sygnalizowana przez organ nadzorczy w przypadku opiniowania **poselskiego projektu ustawy o zmianie ustawy o kombatantach oraz niektórych osobach będących ofiarami represji wojennych i okresu powojennego**[275] oraz **projektu rozporządzenia Ministra Zdrowia w sprawie szczegółowego wzoru zamówienia indywidualnego na produkty krwiopochodne, rekombinowane koncentraty czynników krzepnięcia oraz desmopresynę**[276], jak również **projektu ustawy o zmianie ustawy o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych oraz niektórych innych ustaw**[277].

Na nieuzasadnione przetwarzanie numeru PESEL, mogące prowadzić do nadmiernej ingerencji w prywatność osoby, której ta dana dotyczy, organ nadzorczy zwrócił uwagę, opiniując **projekt rozporządzenia Ministra Klimatu i Środowiska w sprawie rejestru magazynów energii elektrycznej**[278]. Zagadnienie numeru PESEL było również wskazywane przez organ nadzorczy w opiniowanym **projekcie ustawy o badaniach klinicznych produktów leczniczych stosowanych u ludzi**[279]. Uwagi odnosiły się tu do braku wykazania przez projektodawcę niezbędności przetwarzania tej danej osobowej przez Naczelną Komisję Bioetyczną.

[274] DOL. 401.380.2021.
[275] DOL.401.461.2021.
[276] DOL.401.354.2021.
[277] DOL.401.334.2021.
[278] DOL.401.312.2021.
[279] DOL.401.196.2021.

7.8. Dane osobowe szczególnych kategorii, pandemia, zatrudnienie

Organ nadzorczy, opiniując poselski **projekt ustawy o szczególnych rozwiązaniach zapewniających możliwość prowadzenia działalności gospodarczej w czasie epidemii COVID-19 (druk nr 1846)**[280], zwrócił uwagę projektodawcy na cele, dla których można przetwarzać dane zawarte w unijnym cyfrowym zaświadczeniu COVID[281]. Wskazał, że przepisy rozporządzania 2021/953 nie przewidują możliwości zmiany i rozszerzenia określonych nimi celów, nie może to następować zatem w drodze przepisów krajowych, gdyż będzie prowadziło do naruszenia zasady ograniczenia celu (art. 5 ust. 1 lit. b rozporządzenia 2016/679). Rozporządzenie nie przewiduje również przetwarzania wizerunku twarzy posiadacza zaświadczenia. Organ nadzorczy wyjaśnił, że projektodawca nie wykazał niezbędności pozyskiwania takich danych dla realizacji celów nią przewidzianych, a ponadto takie rozwiązanie prowadzi do rozszerzenia zamkniętego katalogu danych określonych w załączniku do ww. rozporządzenia UE, co powinno być przedmiotem szczególnie pogłębionej analizy pod kątem zgodności z zasadami przetwarzania danych osobowych. Prezes UODO wskazał również na konieczność zapewnienia ochrony praw i wolności osób, które nie mogą skorzystać z prawa do zaszczepienia się, zwłaszcza ze względu na przeciwskazania do zaszczepienia. Zwrócił uwagę też na kwestię zabezpieczeń, jakie gwarantuje projektodawca przy zachowaniu poszanowania praw i wolności osób, których dane dotyczą. Chodzi tu o uniknięcie pozyskiwania i dalszego przetwarzania przez pracodawcę danych osobowych, w tym o stanie zdrowia, podawanych przez pracownika celem wyjaśnienia przyczyny niezaszczepienia się, co nie zostało uregulowane w projekcie ustawy.

W opiniowanych przepisach także w zakresie zmian w **ustawie o systemie informacji w ochronie zdrowia**[282] planowano przetwarzanie wizerunku twarzy usługobiorcy, pobieranego z Rejestru Dowodów Osobistych, co wymagało zwrócenia uwagi projektodawcy na to, że w tym przypadku – ze względu na specjalne przetwarzanie techniczne wizerunku – dochodzi do przetwarzania danych biometrycznych, które są zaliczane do szczególnej kategorii danych (art. 9 ust. 1 RODO). Wskazano na brak określenia sposobu, w jaki będzie następowała migracja danych

[280] DOL.401.601.2021.
[281] Unijne cyfrowe zaświadczenie COVID uregulowane zostało w art. 2 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/953 z dnia 14 czerwca 2021 r. w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID) w celu ułatwienia swobodnego przemieszczania się w czasie pandemii COVID-19. Cele, dla których można przetwarzać dane zawarte w ww. certyfikacie są ściśle ograniczone, co oznacza, że dane te można przetwarzać jedynie w celach określonych wprost w art. 10 ust. 2 ww. rozporządzenia, tj. dla ułatwienia korzystania z prawa do swobodnego przemieszczania się w obrębie Unii w czasie pandemii COVID-19.
[282] W zakresie zmian w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

w postaci wizerunku twarzy z Rejestru Dowodów Osobistych do Centralnego Wykazu Usługobiorców oraz na brak gwarancji, że projektowane rozwiązanie ma charakter epizodyczny. Mogłoby to skutkować przetwarzaniem tych danych również po ustaniu epidemii COVID-19. Organ postulował zatem, aby kwestia ta podlegała powtórnej analizie i weryfikacji zasadności pozostawiania takich rozwiązań w systemie prawa po ustaniu stanu epidemii i szczególnych zagrożeń. Problematyka ta jest tym bardziej istotna, że projektodawca nie wskazał również celu przetwarzania wizerunku twarzy usługobiorcy, co czyniło to rozwiązanie nadmiarowym dla celów projektowanej ustawy i wymagającym zdecydowanie pogłębionej refleksji w zakresie poszanowania praw i wolności osób, których wizerunki miałyby być w ten sposób przetwarzane.

Rozważenia wymagało również przyjęcie odpowiednich rozwiązań w przepisach dotyczących prowadzenia akt pracowniczych. Projektowane przepisy nie odnosiły się do tej kwestii. Tymczasem niezwykle istotne było wyznaczenie wyczerpujących i jednoznacznych reguł dotyczących bezpieczeństwa przetwarzania w aktach pracowniczych, w czasie obowiązywania i stosowania opiniowanych przepisów, informacji takich jak „(…) wynik testu diagnostycznego w kierunku SARS-CoV-2 wykonanego nie wcześniej niż 48 godzin przed jego okazaniem, zaświadczenia o przebytej infekcji wirusa SARS-CoV-2 lub certyfikatu o zaszczepieniu przeciwko COVID-19" oraz ewentualnie innych informacji dotyczących, np. przeciwskazań do zaszczepienia oraz wszelkich informacji z tym związanych. Przepisy takie powinny zostać ustalone jako epizodyczne i obowiązujące jedynie „W okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19" (art. 2 ust. 1).

Na zagadnienie związane z przetwarzaniem na dużą skalę danych osobowych szczególnych kategorii, organ nadzorczy zwrócił również uwagę, opiniując **projekt ustawy o ekonomii społecznej (UD185)**[283]. Projekt ten wymagał przyjęcia kompleksowych, wyczerpujących, przejrzystych i precyzyjnych regulacji, uwzględniających wszelkie aspekty i całość wykonywania operacji przetwarzania danych tak, by zapewniona została zgodność z przepisami RODO, a jednocześnie możliwa była realizacja celów, dla których powstała projektowana ustawa. Tymczasem w projekcie ustawy nie określono celu, w jakim konkretne dane mogą być wykorzystywane oraz w jaki sposób i z jakich źródeł następować miałoby ich pozyskiwanie. Projektowana norma w sposób zbyt ogólny wskazywała, że w zakresie i celu niezbędnym do realizacji ustawy przetwarzane mają być dane osobowe, w tym dane szczególnych kategorii z art. 9 ust. 1 i dane z art. 10 RODO. Przyjmowane

[283] DOL.401.290.2021.

rozwiązanie nie zostało poprzedzone testem prywatności i nie odpowiadało wymogom art. 6, 9 czy 10 RODO. Jednocześnie projektodawca nie wskazał w projektowanych przepisach katalogu danych osobowych, które mają być przetwarzane dla realizacji zakładanych celów ustawy, spełniającego kryterium niezbędności. Brak wskazania katalogu danych osobowych, nieprzypisanie katalogów danych precyzyjne do celów ich przetwarzania i kategorii osób, których dane mają być przetwarzane, w przepisach rangi ustawy, może prowadzić do pozyskiwania i dalszego przetwarzania przez podmioty ekonomii społecznej danych osobowych wielu osób[284], nieadekwatnie i nadmiarowo do celów. Skoro ze względu na cele projektowanej ustawy dochodzić ma do przetwarzania danych osobowych szczególnych kategorii, to dane tego rodzaju, mocą przepisów rozporządzenia 2016/679, poddane muszą być szczególnemu reżimowi przetwarzania, z poszanowaniem warunków wynikających z art. 9 i 10 rozporządzenia 2016/679. Szczególny reżim przetwarzania wymaga uwzględnienia w przepisach nakładających obowiązek przetwarzania danych i zapewnienia nie tylko rzetelności i przejrzystości, ograniczenia celu, niezbędności, minimalizacji (art. 5 rozporządzenia 2016/679), ale i uwzględnienia elementów wynikających z art. 6 ust. 3 rozporządzenia 2016/679, warunków odpowiednich zabezpieczeń praw podstawowych i interesów osoby, której dane dotyczą, konkretnych środków ochrony praw i wolności osób (art. 9 rozporządzenia 2016/679) oraz warunków dokonywania operacji na danych z art. 10 wyłącznie pod nadzorem władz publicznych (art. 10 rozporządzenia 2016/679). Organ nadzorczy wskazał, że należy rozważyć przyjęcie odpowiednich przepisów stanowiących kompetencje określonych podmiotów tak, aby obowiązki i uprawnienia nałożone na nie mocą tych przepisów mogły być realizowane, a jednocześnie uzasadniały przypadki przetwarzania danych dotyczących wyroków skazujących i naruszeń prawa. Rozwiązania projektowane niniejszą regulacją dotyczą bardzo szerokiego katalogu wrażliwych informacji o osobach, głęboko dotykających ich prywatności, intymności. Ujawniają bowiem pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dotyczą przetwarzania danych genetycznych i danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub też orientacji seksualnej osoby – bo taki jest zakres danych osobowych z art. 9 ust. 1 rozporządzenia 2016/679. Katalog danych wrażliwych obejmuje także dane osobowe z art. 10 rozporządzenia 2016/679 dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, których przetwarzania wolno dokonywać wyłącznie pod

[284] Tj. osób zagrożonych wykluczeniem społecznym, członków przedsiębiorstwa ekonomii społecznej i jego organów, a także osób zatrudnionych w takim przedsiębiorstwie.

nadzorem władz publicznych oraz jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego, przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. W opiniowanych przepisach wątpliwości organu wzbudziło zwłaszcza przetwarzanie danych członków przedsiębiorstwa ekonomii społecznej, członków jego organów, w tym także zatrudnionych w przedsiębiorstwie społecznym osobach zagrożonych wykluczeniem społecznym, w zakresie danych np. ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, czy danych genetycznych oraz danych biometrycznych – są to kategorie danych, których przetwarzanie ze względu na ich szczególny charakter musi podlegać wyjątkowemu reżimowi przetwarzania. Organ nadzorczy wskazał, że tak sformułowane przepisy ustawy budzą wątpliwości i pozostawiają zbyt duży margines swobody dla wykonawców norm, stwarzając niebezpieczeństwo nadużyć, przyjmowania rozwiązań dowolnych, nieadekwatnych, nadmiarowych. Organ nadzorczy zauważył, że nawet Najwyższa Izba Kontroli[285] i dokonujący kontroli jej przedstawiciele, w zakresie danych ujawniających poglądy polityczne, przekonania religijne lub światopoglądowe, jak również danych genetycznych, o nałogach, o seksualności lub o orientacji seksualnej, nie mają tak szerokiego zakresu uprawnień, jaki proponowany jest w art. 10 ust. 1 projektu ustawy. Przepisy z zakresu prawa pracy, w tym Kodeksu pracy, również wprowadzają ograniczone katalogi przetwarzania danych osobowych w stosunku do ściśle określonych celów.

Przetwarzanie danych szczególnych kategorii (także w dokumentacji medycznej) było przedmiotem zainteresowania Prezesa UODO podczas opiniowania **projektu ustawy o modernizacji i poprawie efektywności szpitalnictwa**[286]. Wątpliwość wzbudziła kwestia tego, czy w trakcie wykonywania projektowanych przepisów dochodzić będzie do przetwarzania danych osobowych pacjentów, zawartych w ich dokumentacji medycznej. Jeśli miałoby to mieć miejsce, to wskazane jest, aby projektodawca wykonał w tym zakresie test prywatności, ocenę skutków i wpływu przyjmowanego rozwiązania na ochronę danych osobowych i prywatność podmiotów danych. Projekt ustawy dopuszcza bowiem stosowanie komunikacji pomiędzy podmiotami za pomocą środków komunikacji elektronicznej, której potencjalnie mogłoby podlegać również przetwarzanie danych osobowych pacjentów, zawartych w dokumentacji medycznej. W ocenie organu nadzorczego kwestie te wymagają wyjaśnienia przez projektodawcę. Uzasadnione wydaje się też rozważenie wprowadzenia w przepisach ustawy ograniczeń co do przekazywania tą drogą dokumentacji medycznej pacjenta, w tym także danych dotyczących zdrowia, a więc należących do szczególnych

[285] Art. 29 ust. 1 pkt 2 lit. i ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, Dz. U. z 2020 r. poz. 1200.
[286] DOL.401.625.2021.

kategorii, o których mowa w art. 9 ust. 1 RODO. Co do tych danych przepisy rozporządzenia 2016/679 określają szczególny reżim wykonywania na nich operacji przetwarzania.

W 2021 r. jednym z opiniowanych projektów związanych z przetwarzaniem szczególnych kategorii danych osobowych był **projekt ustawy o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw (pierwotny tytuł: projekt ustawy o zmianie ustawy – Kodeks pracy oraz ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi; UD211)**[287]. Dotyczył rozwiązań, w których na dużą skalę mają być przetwarzane szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO. Projektodawca zaproponował, aby szczegółowy katalog danych osobowych pracownika został określony w rozporządzeniu wykonawczym. Przy czym nie uzasadnił tego rozwiązania – nie przedstawił powodów i argumentów, dla których przetwarzanie danych osobowych szczególnej kategorii, ujawniających informacje wrażliwe dotyczące stanu zdrowia czy uzależnień pracowników, miałoby odbywać się na podstawie aktu niższego rzędu. W projekcie rozporządzenia w sprawie badań na obecność alkoholu lub środków działających podobnie do alkoholu w organizmie pracownika, zawarto katalogi danych osobowych pozyskiwane w czasie prowadzonych badań trzeźwości oraz badań na obecność środków działających podobnie do alkoholu, a także dane, które osoba sama musi ujawniać w formie oświadczenia na potrzeby tych badań (m.in. dane antropometryczne czy informację o chorobach). Organ nadzorczy zwrócił uwagę, że przepisy projektowanego rozporządzenia w istocie miałyby zobowiązywać pracowników do przekazywania i ujawniania na podstawie aktu rangi wykonawczej, danych osobowych, w tym danych szczególnie chronionych. Organ nadzorczy zwrócił uwagę, iż zgodnie z wytycznymi zawartymi w delegacji do wydania proponowanego aktu wykonawczego, w projektowanych przepisach Kodeksu pracy niezbędne jest wzięcie pod uwagę dostępnych metod przeprowadzania takich badań, konieczności zapewnienia ochrony życia i zdrowia pracowników lub innych osób czy ochrony mienia, a także sprawne przeprowadzanie badań i zagwarantowanie wiarygodności ich wyników, przy jednoczesnym poszanowaniu godności oraz innych dóbr osobistych pracownika, a także ochrony danych osobowych. W wytycznych tych projektodawca zbyt ogólnie wskazuje na zagadnienie ochrony danych osobowych – zabrakło odniesienia do konieczności zapewnienia rozwiązań gwarantujących integralność i poufność danych przetwarzanych w czasie badań, celem zapewnienia stosowania zasady poufności i integralności wynikającej z art. 5 ust. 1 lit. f rozporządzenia 2016/679. Proponowane w projekcie rozporządzenia katalogi danych osobowych

[287] DOL.401.237.2021.

pozyskane w czasie prowadzonych badań trzeźwości pracownika oraz badań na obecność środków działających podobnie do alkoholu, nie są tożsame z danymi, które pracodawca przetwarza na podstawie § 6 projektu ustawy (odnoszącymi się do informacji o dacie, godzinie i minucie badania oraz jego wyniku, wskazującym na stan po użyciu alkoholu albo stan nietrzeźwości). Organ nadzorczy wskazał na konieczność zawarcia w projektowanych przepisach rozwiązań dotyczących okresów przechowywania, tj. retencji danych osobowych zawartych w tych katalogach i badaniach, celem zapewnienia stosowania zasady ograniczenia przechowania określonej w art. 5 ust. 1 lit. e rozporządzenia 2016/679.

Warto zaznaczyć, że opiniowane w 2021 roku zmiany Kodeksu pracy dotyczyły nie tylko zagadnienia związanego z badaniem trzeźwości, ale również kwestii związanych z pracą zdalną. Zawierał je **projekt ustawy o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw**[288]. W opinii organu nadzorczego charakter wprowadzanych projektem rozwiązań dotyczących pracy na odległość (pracy zdalnej) oznaczał dopuszczalność prowadzenia nieograniczenie szerokiego spektrum operacji lub zestawów operacji przetwarzania danych osobowych w tym trybie, co wiązało się z przetwarzaniem na szeroką skalę ogromnej ilości danych osobowych. Podkreślił, że ogólne sformułowania przepisów, które mają być wprowadzone, nie wykluczają przetwarzania na odległość także danych szczególnych kategorii z art. 9 czy danych objętych reżimem przetwarzania wyznaczonym mocą art. 10 RODO. Zgodnie z projektowanymi przepisami Kodeksu pracy, pracodawca określa procedury ochrony danych osobowych przyjmowanych przez pracodawcę na potrzeby wykonywania pracy zdalnej oraz przeprowadza, w miarę potrzeb, instruktaż i szkolenie w tym zakresie. Przyjmuje się, że pracownik wykonujący pracę zdalną potwierdza, w postaci papierowej lub elektronicznej, zapoznanie się z procedurami, oraz jest obowiązany do ich przestrzegania. Z projektowanych zmian wynikają uprawnienia pracodawców (administratorów) do przeprowadzenia kontroli wykonywania pracy przez pracownika, w tym w zakresie bezpieczeństwa i higieny pracy. Nie wynika z tego jednoznacznie, czy wskazane uprawnienie pracodawcy dotyczy również obowiązków pracownika związanych z przestrzeganiem procedur ochrony danych osobowych. Dlatego też projektowana regulacja wzbudziła wątpliwości organu nadzorczego, który wskazał, że wymaga doprecyzowania w taki sposób, aby z przepisów jednoznacznie wynikało ww. uprawnienie pracodawcy do kontroli przestrzegania przez pracownika przyjętych procedur ochrony danych osobowych. Organ nadzorczy podkreślił, że rozwiązanie takie leży w interesie pracodawcy

[288] DOL.401.219.2021.

– administratora, na którym spoczywa szereg obowiązków, w tym ochrony i bezpieczeństwa przetwarzania danych osobowych, co przy wykonywaniu obowiązków przez pracowników w trybie zdalnym jest tym bardziej istotne.

Pozytywnie należy ocenić wypracowane podczas prac legislacyjnych ustalenia pomiędzy organem nadzorczym a projektodawcą (w chwili pisania sprawozdania na poziomie komisji prawniczej w RCL) w następującym zakresie:

1. projektodawca doprecyzował przepisy dotyczące okresu przechowywania przez pracodawcę informacji o przeprowadzonym w ramach kontroli trzeźwości badaniu, które potwierdziło stan po użyciu alkoholu albo stan nietrzeźwości pracownika;
2. projektodawca przeniósł do projektu ustawy katalog danych osobowych zawartych w protokole badania stanu trzeźwości pracownika, przeprowadzonego albo zleconego przez uprawniony organ powołany do ochrony porządku publicznego;
3. do projektu ustawy przeniesiony został katalog danych osobowych zamieszczonych w protokole badania pracownika na obecność w jego organizmie środka działającego podobnie do alkoholu, stanu trzeźwości pracownika, przeprowadzonego albo zleconego przez uprawniony organ powołany do ochrony porządku publicznego.

Zagadnienie związane z pracą zdalną było także przedmiotem opinii organu nadzorczego dotyczącej **projektu dyrektywy Parlamentu Europejskiego i Rady ws. poprawy warunków pracy platformowej**[289]. W opinii organu nadzorczego przyjęcie i transponowanie do krajowego porządku prawnego tego aktu prawnego może się znacznie przyczynić do wzrostu poziomu ochrony danych osobowych w związku z wykonywaniem tzw. pracy zdalnej i perspektywę taką należałoby oceniać pozytywnie. Projektowana dyrektywa doprecyzowuje takie kwestie, jak realizacja obowiązku informacyjnego, w szczególności w odniesieniu do art. 13 ust. 2 lit. f, art. 14 ust. 2 lit. g i art. 15 ust. 1 lit. h rozporządzenia 2016/679 (motyw 31 projektu dyrektywy), czyli informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu. Doświadczenie polskiego organu nadzorczego pokazuje, że wprowadzenie regulacji precyzyjnych i wyczerpująco odnoszących się do wszystkich aspektów przetwarzania danych osobowych oraz dedykowanych poszczególnym zagadnieniom, jak w tym przypadku regulacje dotyczące pracy zdalnej, przyczynia się do lepszego realizowania wymogów ochrony danych.

[289] Dokument oznaczony jako COM (2021)762 final, DOL.401.606.2021.

Kwestia przeprowadzania szkoleń w formie zdalnej była zagadnieniem analizowanym w związku z opiniowaniem **projektu rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie szkolenia pielęgniarek i położnych dokonujących przetaczania krwi i jej składników**[290]. Organ nadzorczy zwrócił uwagę projektodawcy na proponowane w projekcie rozwiązanie w zakresie prowadzenia szkoleń w formie zdalnej z wykorzystaniem środków komunikacji elektronicznej pozwalających na przesyłanie obrazu i dźwięku oraz umożliwiających dwukierunkową łączność w czasie rzeczywistym pomiędzy uczestnikami szkolenia i wykładowcą. Jest to ważne z uwagi na różnorodność uwarunkowań technicznych (np. rodzaj aplikacji) stosowanych przez administratorów podczas takich szkoleń. Wskazał również na aspekt kategorii/rodzaju danych, jakie przy użyciu „komunikacji na odległość" mogą być przetwarzane, a mianowicie, że taki sposób przetwarzania danych może oznaczać nie tylko przetwarzanie wizerunku czy głosu, ale również potencjalne przetwarzanie szczególnych kategorii danych osobowych, tj. dotyczących zdrowia, pochodzenia rasowego czy etnicznego (czyli danych szczególnie chronionych z art. 9 RODO).

7.9. Profilowanie

Profilowanie to forma zautomatyzowanego przetwarzania danych osobowych, polegającego na ocenie niektórych czynników osobowych osoby fizycznej, np. jej osobistych preferencji, sytuacji ekonomicznej, zdrowia, zainteresowań, wiarygodności czy zachowania. Profilowanie było przedmiotem analizy organu nadzorczego m.in. w związku z **pracami nad wdrożeniem zintegrowanej platformy analitycznej i przekazaniem do zaopiniowania projektu rozporządzenia Rady Ministrów w sprawie wykazu rejestrów publicznych i systemów teleinformatycznych, z których udostępniane są dane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej**[291].

Organ nadzorczy wskazał, że nowe przepisy nie mogą negować istoty przetwarzania danych na podstawie innych ustaw, jak i odrębności zbiorów oraz odrębności celów i zakresów przetwarzania danych. Ustawowe przepisy powinny także zawierać postulowane przez organ nadzorczy dodatkowe gwarancje zakazujące używania ZPA do profilowania indywidualnych osób oraz zautomatyzowanego podejmowania decyzji, oraz dawać gwarancje, że dane nie będą

[290] DOL.401.1.2021.
[291] DOL.401.624.2021.

wykorzystywane do innych celów niż dokonywanie konkretnej analizy. Obecnie obowiązujące przepisy dotyczące ZPA – przyjęte wbrew negatywnej opinii organu nadzorczego – w praktyce wyłączają jakiekolwiek realne gwarancje i ograniczenia państwa do pozyskiwania i przetwarzania danych osobowych dotyczących osób podlegających tym przepisom. Przesłany do zaopiniowania projekt rozporządzenia, pomimo że z zgodnie z delegacją ustawową ma także gwarantować zgodność udostępniania danych z przepisami o ochronie danych osobowych, w praktyce nie zawierał żadnych rozwiązań dedykowanych temu zagadnieniu. Ograniczony został do wskazania zakresu danych, wykazu rejestrów publicznych i systemów teleinformatycznych, z których udostępniane są dane na potrzeby prowadzenia analiz ZPA oraz podmiotów je prowadzących, które są obowiązane do przekazywania danych pochodzących z tych rejestrów i systemów.

Do kwestii profilowania odnosiło się także **wystąpienie Prezesa UODO w sprawie EZD**[292]. Organ nadzorczy wskazał, że przepisy prawa powinny jednoznacznie określać, czy za pośrednictwem systemu EZD RP będzie dokonywane profilowanie osób (zautomatyzowane podejmowanie decyzji w indywidualnych sprawach) – przy uwzględnieniu warunków dozwolonych przepisami rozporządzenia 2016/679. Odniósł się także do zagrożeń związanych z wykorzystaniem algorytmów do profilowania osób, zwracając uwagę na wytyczne Grupy Roboczej Art. 29 w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679 przyjętych w dniu 3 października 2017 r. W dokumencie tym podkreślono, że profilowanie dotyczy również procesów decyzyjnych, które nie przebiegają wyłącznie w sposób zautomatyzowany. Wytyczne z wyżej wskazanego dokumentu powinny, w opinii organu nadzorczego, znaleźć odzwierciedlenie w Dokumencie wdrażania EZD RP tak, aby system EZD RP nie zawierał rozwiązań umożliwiających profilowanie osób, niezgodne z przepisami rozporządzenia 2016/679.

Na zagadnienie profilowania organ nadzorczy zwrócił uwagę opiniując **projekt ustawy o zmianie ustawy – Prawo budowlane oraz ustawy o samorządach zawodowych architektów oraz inżynierów budownictwa**[293]. Wskazał, że przepis, który pozwala udostępniać książki obiektu budowlanego zawierające dane osobowe nieograniczonej liczbie, niesprecyzowanych, dowolnych osób, które zarejestrują się i założą konto w systemie EKOB (Elektroniczna Książka Obiektu Budowlanego), spowoduje potencjalne zagrożenia dla tych danych. Projektowana regulacja zezwala na nieograniczone dysponowanie nimi przez osoby, których te dane nie dotyczą. Fakt założenia konta

[292] DOL.413.5.2021.
[293] DOL.401.138.2021.

w systemie EKOB nie powinien być samoistną przesłanką do udostępnienia danych osobie zalogowanej do każdej książki obiektu budowlanego. Gromadzenie danych pochodzących z EKOB, w tym łączonych z innymi informacjami, powoduje potencjalne zagrożenie profilowania osób, których dane figurują w księgach. Ważnym aspektem jest także to, jak długo będą przechowywane dane osób zalogowanych, które chcą mieć dostęp do książki obiektu budowlanego, oraz czy o dostęp do tych danych będzie trzeba wnioskować indywidualnie, czy będą one dostępne dla innych podmiotów korzystających z systemu. Wskazano ponadto, że należy również rozważyć zasady retencji „historii logów" osób korzystających z systemu EKOB. W ocenie organu nadzorczego wskazane zagrożenia powinny zostać podane szczególnie wnikliwej analizie w ramach oceny skutków dla ochrony danych w trybie art. 35 RODO, pod kątem zasad dotyczących przetwarzania danych osobowych, w tym zasady poufności i integralności oraz przepisów dotyczących profilowania.

7.10. Inne projekty aktów prawnych

Wyżej wskazane zagadnienia nie wyczerpują całego katalogu spraw legislacyjnych, jakimi w 2021 roku zajmował się organ nadzorczy. Wśród projektów aktów normatywnych, które wpłynęły do zaopiniowania organu nadzorczego, było również **Rozporządzenie w sprawie prywatności i łączności elektronicznej ePrivacy**[294].

Organ nadzorczy z zadowoleniem przyjął uwzględnienie w styczniu 2021 roku większości zgłaszanych uwag w zakresie m.in.: wskazania prymatu zgody użytkownika nad ustawieniami oprogramowania, co ma szczególnie istotne znaczenie w przypadku instalacji plików „cookies", dostosowania brzmienia przesłanki „obowiązku prawnego" do wymogów RODO; wskazania wprost na instytucję sprzeciwu w odniesieniu do przetwarzania plików „cookies", a także na wymóg uprzedniości zgody w odniesieniu do marketingu bezpośredniego. Jednocześnie Prezes UODO zwrócił uwagę, że w przypadku, gdy wskazane w przepisie podmioty[295] nie mają siedziby w Unii, wyznacza on na piśmie, w terminie jednego miesiąca od rozpoczęcia swojej działalności, przedstawiciela w Unii i wskazuje to właściwemu organowi nadzorczemu. Art. 3 ust. 2a projektu stanowi zaś, że wymogi określone w ust. 2 nie mają zastosowania, jeżeli działania wymienione

[294] Rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE – kontynuacja prac nad projektem (DOL.401.292.202).
[295] Tj. dostawca usługi łączności elektronicznej, dostawca publicznie dostępnego spisu numerów lub osoba korzystająca z usług łączności elektronicznej do wysyłania komunikatów do celów marketingu bezpośredniego, lub osoba korzystająca z możliwości przetwarzania i przechowywania danych lub gromadząca informacje przetwarzane przez urządzenie końcowe użytkowników końcowych lub przez nie przechowywane.

w ust. 1 są sporadyczne i ze względu na ich charakter, kontekst, zakres i cel jest mało prawdopodobne, że spowodują ryzyko dla praw podstawowych użytkowników końcowych. Organ nadzorczy zwrócił uwagę, że ww. przepis projektu ma charakter nieostry i może powodować problemy interpretacyjne co do tego, w jakiej sytuacji właściwemu organowi nadzorczemu należy przekazać informacje o przedstawicielu dostawcy usług spoza UE. Wskazał, że zarówno sporadyczność działań, jak i kryterium ryzyka naruszenia praw osób, są pojęciami nieostrymi, a ich użycie w komentowanym przepisie może doprowadzić do sytuacji, kiedy dostawca usług spoza UE, uznając dyskrecjonalnie, że jego działalność jest okazjonalna lub nie rodzi ryzyk dla praw podstawowych użytkowników, nie będzie informował właściwego organu nadzorczego o swoim przedstawicielu, mimo że takie powiadomienie byłoby zasadne. Dlatego wskazane aspekty powinny zostać doprecyzowane w treści projektowanego rozporządzenia – zarówno w przepisach normatywnych, jak i w motywach.

Wątpliwości organu nadzorczego wzbudziły projektowane przepisy dotyczące przesłanek legalności przetwarzania metadanych z komunikacji elektronicznej: dane te mogą być wykorzystywane do celu tworzenia i rozpowszechniania oficjalnych statystyk krajowych i europejskich w zakresie niezbędnym do tego celu. Organ nadzorczy wskazał na dodanie zastrzeżenia w ww. zakresie, że „jeśli w tym celu nie mogą być wykorzystywane dane anonimowe". Część zadań organów statystyki publicznej może być bowiem wykonywanych na danych pozbawionych cech danych osobowych, tym samym nie jest zasadne przekazywanie tym służbom metadanych z komunikacji elektronicznej, jeśli swoje ustawowe cele mogą realizować na danych zanonimizowanych. Zastrzeżenia organu nadzorczego dotyczyły projektowanego przepisu, który wskazywał, że dane osobowe użytkownika końcowego, który jest osobą fizyczną, można umieszczać w publicznie dostępnym spisie abonentów pod warunkiem, że użytkownik końcowy, który jest osobą fizyczną, ma prawo sprzeciwić się takiemu umieszczeniu. W sytuacji, kiedy dane osoby znajdą się w publicznie dostępnym spisie abonentów, który funkcjonuje w sieci Internet, mogą one zostać pobrane i wykorzystane przez potencjalnie nieograniczony krąg odbiorców oraz zarchiwizowane przez roboty internetowe, takie jak Googlebot, natychmiast po opublikowaniu w takim spisie. Tymczasem sprzeciw jest zazwyczaj działaniem następczym, a w konsekwencji nie pozwala na niedopuszczenie przez osobę, której dane dotyczą, do wykorzystania jej danych osobowych. Organ nadzorczy wskazał na konieczność zrezygnowania z takiego rozwiązania. Zgoda osoby, której dane dotyczą, powinna być jedyną przesłanką legalności umieszczenia danych osoby w publicznie dostępnym spisie abonentów. Dodatkowo ten projektowany przepis powinien precyzyjnie określać,

jakie dane osoby znajdą się w publicznie dostępnym spisie abonentów. Przepis ten wymaga zatem doprecyzowania poprzez wskazanie zamkniętego katalogu takich danych.

Prezes UODO w 2021 roku opiniował też **rządowy projekt ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw (druk sejmowy nr 1504)**[296], który dotyczył m.in.: a) rozszerzenia zakresu danych zamieszczanych w centralnej ewidencji kierowców o dane o wysokości grzywien nałożonych w drodze mandatu karnego za naruszenia przepisów ruchu drogowego i o uiszczeniu tych grzywien; b) udostępniania zakładom ubezpieczeń danych o: wykroczeniach lub przestępstwach stanowiących naruszenia przepisów ruchu drogowego, punktach za naruszenie przepisów ruchu drogowego przypisanych za wykroczenia lub przestępstwa stanowiące naruszenia przepisów ruchu drogowego, wysokości grzywien nałożonych w drodze mandatu karnego za naruszenia przepisów ruchu drogowego, uiszczeniu grzywien nałożonych w drodze mandatu karnego za naruszenia przepisów ruchu drogowego, kierowaniu pojazdem w stanie nietrzeźwości, w stanie po użyciu alkoholu lub środka działającego podobnie do alkoholu; c) udostępnianiu zakładom ubezpieczeń danych zgromadzonych w centralnej ewidencji kierowców za pośrednictwem systemu teleinformatycznego obsługującego Ubezpieczeniowy Fundusz Gwarancyjny (UFG). Organ nadzorczy wskazał na niespójność między nowelizowanymi przepisami Prawa o ruchu drogowym oraz nowelizowanymi unormowaniami ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej a ustawy z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych. Zgodnie nowelizacją Prawa o ruchu drogowym, zakładom ubezpieczeń mają być udostępniane z centralnej ewidencji kierowców, do oceny ryzyka ubezpieczeniowego w związku z czynnościami zmierzającymi do zawarcia umowy ubezpieczenia, dane o wysokości grzywien nałożonych w drodze mandatu karnego za naruszenia przepisów ruchu drogowego i o uiszczeniu tych grzywien. Tymczasem w myśl nowelizowanego projektu ustawy o działalności ubezpieczeniowej i reasekuracyjnej, zakłady ubezpieczeń nie mają podstawy prawnej do przetwarzania tych danych w celu dokonania oceny ryzyka ubezpieczeniowego i taryfikacji. Co więcej, dane o wysokości grzywien nałożonych w drodze mandatu karnego za naruszenia przepisów ruchu drogowego i o uiszczeniu tych grzywien, mają być udostępnianie zakładom ubezpieczeń z centralnej ewidencji kierowców za pośrednictwem systemu teleinformatycznego obsługującego Ubezpieczeniowy Fundusz Gwarancyjny, a nowelizowany przepis ustawy o UFG nie przewiduje przetwarzania tych

[296] DOL.401.410.2021.

danych przez wspomniany podmiot. Organ nadzorczy wskazał, że taka niezgodność uregulowań nie tylko rodzi ryzyko naruszenia zasady zgodności z prawem, lecz może być nawet uznana za godzącą w tę zasadę (art. 5 ust. 1 lit. a RODO).

Projektowana regulacja Prawa o ruchu drogowym przewidywała udostępnianie zakładom ubezpieczeń, za pośrednictwem systemu teleinformatycznego obsługującego Ubezpieczeniowy Fundusz Gwarancyjny, zgromadzonych w centralnej ewidencji kierowców danych o wykroczeniach lub przestępstwach stanowiących naruszenia przepisów ruchu drogowego i przypisanych im punktach za to naruszenie – jako dane niezbędne do oceny ryzyka ubezpieczeniowego w związku z czynnościami zmierzającymi do zawarcia umowy ubezpieczenia. Organ nadzorczy zwrócił uwagę na cel udostępniania danych z centralnej ewidencji kierowców i ich przetwarzania przez Ubezpieczeniowy Fundusz Gwarancyjny, a następnie także przez zakłady ubezpieczeń. W opinii Prezesa UODO rozszerzenie celu przetwarzania było wątpliwe z punktu widzenia przepisów rozporządzenia 2016/679. W jego ocenie wysoce nieuzasadnioną była także propozycja nałożenia na prokuratorów, sądy lub organy orzekające w sprawach o naruszenia w postępowaniu dyscyplinarnym, obowiązku przekazywania do centralnej ewidencji kierowców danych o uiszczeniu grzywien nałożonych w drodze mandatu karnego za naruszenia przepisów ruchu drogowego. Projektodawca nie wskazał, z jakiego źródła i na jakiej podstawie prawnej ww. organy miałyby pozyskiwać takie dane. Wobec uzależnienia przez projektodawcę usunięcia z centralnej ewidencji kierowców danych o otrzymanej przez kierowcę lub osobę posiadającą pozwolenie na kierowanie tramwajem, liczbie punktów za naruszenie przepisów ruchu drogowego oraz o popełnieniu przez kierowcę (osobę posiadającą pozwolenie na kierowanie tramwajem) wykroczenia lub przestępstwa stanowiącego naruszenie przepisów ruchu drogowego, od uiszczenia grzywny za naruszenie, niejasna jest kwestia terminu usunięcia z centralnej ewidencji kierowców ww. danych w przypadku przedawnienia wykonania orzeczonej grzywny na podstawie art. 45 § 3 ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń albo art. 103 § 1 pkt 3 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny. Organ nadzorczy wskazał, że w razie zaistnienia przedawnienia wykonania orzeczonej grzywny, przepisy projektu nie określają ani początku biegu terminu usunięcia z centralnej ewidencji kierowców ww. danych, ani okresu, po upływie którego dane te podlegają usunięciu. Nie można jednak zapominać, że chodzi w tym przypadku o dane, o których mowa w art. 10 rozporządzenia 2016/679, podlegające szczególnemu reżimowi przetwarzania.

W 2021 roku Prezes UODO zgłosił również uwagi do projektu **ustawy o zmianie ustawy o utrzymaniu czystości i porządku w gminach oraz niektórych innych ustaw**[297]. Odniósł się w nich do propozycji brzmienia art. 2a: *1. W przypadku, gdy gmina zapewni techniczne możliwości identyfikacji odpadów komunalnych wytwarzanych w poszczególnych lokalach w budynkach wielolokalowych, rada gminy może, w drodze uchwały stanowiącej akt prawa miejscowego, postanowić o składaniu deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi oraz ponoszeniu tej opłaty przez właściciela lokalu lub inną osobę, której służy tytuł prawny do lokalu w budynku wielolokalowym, lub osobę faktycznie zamieszkującą lub użytkującą ten lokal.* W swojej opinii Prezes UODO podniósł, że tak skonstruowany przepis może skutkować kształtowaniem przez gminy rozwiązań niezgodnych z RODO i prowadzić do bezpośredniej identyfikacji właścicieli lokali. Podczas prac legislacyjnych projektodawca uwzględnił tę uwagę poprzez dodanie do przepisu ustępów stanowiących, iż identyfikacja odpadów komunalnych nie może polegać na ujawnianiu danych osobowych. Wskazano jednocześnie, że prawdopodobnie formą identyfikacji odpadów przez gminy będzie naklejanie kodów, a identyfikacji lokalu na podstawie kodu będzie mogła dokonać jedynie uprawniona do tego osoba za pomocą specjalnego czytnika. Decyzję w tym zakresie będą jednak podejmowały same gminy, projektowane przepisy zaś zapewniają ochronę danych osobowych właścicieli lokali.

Finalnie, w ustawie z dnia 13 września 1996 r. o utrzymaniu porządku i czystości w gminie wprowadzone zostały zmiany pozwalające burmistrzowi, wójtowi i prezydentowi miasta na dostęp do baz danych jednostek gminy, w tym przedsiębiorstw kanalizacyjno-wodociągowych. Regulacje w tym zakresie nie były konsultowane z Prezesem Urzędu Ochrony Danych Osobowych. Zgodnie z dodanym do ustawy art. 60 ust. 1a: „1a. Wójt, burmistrz lub prezydent miasta w celu weryfikacji złożonych deklaracji może wykorzystać informacje i dane znajdujące się w jego posiadaniu oraz posiadaniu gminnych jednostek organizacyjnych, w tym przedsiębiorstw wodociągowo-kanalizacyjnych". Wątpliwości organu nadzorczego wzbudził tak ukształtowany przepis, który uprawnia gminy do wykonywania operacji na danych osobowych. Wątpliwości dotyczyły także tego, czy na podstawie ww. przepisu nie będzie dochodzić do zmian celów przetwarzania, automatycznego przetwarzania danych osobowych, nieuprawnionej wymiany danych osobowych pomiędzy bazami lub łączenia baz danych.

[297] DOL.401.7.2021.

Prezes UODO, opiniując **projekt ustawy o dokumentach paszportowych**[298], pozytywnie ocenił rozwiązanie, zgodnie z którym dane biometryczne w postaci odcisków linii papilarnych palców będą przechowywane w Rejestrze Dokumentów Paszportowych jedynie czasowo, tj. do czasu przyjęcia spersonalizowanego dokumentu przez organ paszportowy albo, w przypadku wydania przez organ paszportowy decyzji o odmowie wydania dokumentu paszportowego, do czasu wpisania przez organ do Rejestru Dokumentów Paszportowych informacji o odmowie wydania dokumentu paszportowego. Zaproponowane w art. 82, 83 i 86 projektu rozwiązania dotyczące zapewnienia uprawnionym podmiotom dostępu do danych zgromadzonych w Rejestrze Dokumentów Paszportowych, za pomocą urządzeń w trybie teletransmisji danych, stanowią istotny postęp w stosunku do – kwestionowanych przez organ nadzorczy – unormowań ustawy z dnia 24 września 2010 r. o ewidencji ludności, odnoszących się do udostępniania danych z rejestru PESEL za pomocą urządzeń teletransmisji danych po złożeniu jednorazowego, uproszczonego wniosku i wyrażeniu przez właściwy organ zgody. Nie rozstrzygając na tym etapie opiniowania projektu kwestii faktycznego stosowania powołanych wyżej przepisów (w przypadku uchwalenia ustawy o dokumentach paszportowych w kształcie zaprezentowanym w projekcie), Prezes Urzędu Ochrony Danych Osobowych pozytywnie ocenił: 1. wprowadzenie zamkniętego katalogu podmiotów, które mogą uzyskać dostęp do danych zgromadzonych w Rejestrze Dokumentów Paszportowych, w trybie teletransmisji danych za pomocą urządzeń teletransmisji danych (art. 83 ust. 1 w zw. z art. 82 projektu); 2. nieprzekazywanie z Rejestru Dokumentów Paszportowych danych biometrycznych w postaci odcisków linii papilarnych palców (art. 82 projektu); 3. nałożenie obowiązku odnotowywania w systemie uprawnionego podmiotu za pomocą urządzenia teletransmisji danych celu uzyskania danych (art. 83 ust. 1 pkt 1 projektu), a zwłaszcza 4. nadanie ministrowi właściwemu do spraw informatyzacji realnego uprawnienia do kontrolowania wszystkich podmiotów, które mogą uzyskać dostęp do danych zgromadzonych w Rejestrze Dokumentów Paszportowych, w trybie teletransmisji danych za pomocą urządzeń teletransmisji danych (art. 86 ust. 1, 2, 4 i 5 oraz art. 87 projektu). O to – jak dotąd bezskutecznie – organ właściwy w sprawie ochrony danych osobowych wnosił w odniesieniu do dostępu do rejestru PESEL za pomocą urządzeń teletransmisji danych, po złożeniu jednorazowego, uproszczonego wniosku i wyrażeniu przez właściwy organ zgody[299]. Przy czym niespełnienie tego wymogu może, w myśl art. 83 ust. 3 projektu, skutkować cofnięciem przez ministra właściwego do spraw informatyzacji dostępu do Rejestru Dokumentów Paszportowych,

[298] DOL.401.49.2021.
[299] Art. 48 ust. 1 i art. 51 ust. 1 pkt 1 w zw. z art. 46 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności.

w trybie teletransmisji danych za pomocą urządzeń teletransmisji danych. Kontrola ta, zgodnie z art. 86 ust. 4 pkt 2 i ust. 5 projektu, będzie mogła obejmować także urządzenia służące do teletransmisji danych co do spełniania przez nie wymogów z art. 83 ust. 1 pkt 1 projektu. Powyższe rozwiązania powinny stanowić impuls dla innych projektodawców, by udoskonalić istniejące dotychczas konstrukcje prawne regulujące udostępnianie danych w trybie teletransmisji danych za pomocą urządzeń teletransmisji danych.

Ocenie organu nadzorczego poddany był również **projekt ustawy o wolności słowa w internetowych serwisach społecznościowych**[300]. Ta projektowana regulacja ma na celu wprowadzenie instrumentów prawnych, przewidujących ochronę prawną dla użytkowników portali społecznościowych, niezależnie od stosowanych obecnie przez usługodawców mechanizmów filtrowania publikowanych treści. Zważając na istotność proponowanej regulacji ze względu na ochronę wolności słowa w internetowych serwisach społecznościowych, Prezes UODO w pierwszej kolejności wskazał, iż wszelkie inicjatywy związane z budowaniem podstaw prawnych dla realizacji tego projektu muszą zapewniać stosowanie rozporządzenia 2016/679. Przedstawiony projekt nie zawierał dokonanej w kompleksowy sposób oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Polecił zatem uwadze projektodawcy, aby przy wypracowywaniu przepisów prawa uwzględniać dokonywanie oceny skutków dla ochrony danych, jej wyników i wpływu na kształt i treść określonych regulacji stanowiących o dokonywaniu operacji na danych osobowych. Ponieważ regulacja wprowadza nowe rozwiązania prawne, zasadnicze znaczenie ma przede wszystkim przyjęcie kompletnych i precyzyjnie zdefiniowanych pojęć. Na przykład: „internetowy serwis społecznościowy", przez który rozumie się usługę świadczoną drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Umożliwia ona udostępnianie przez użytkowników dowolnych treści innym użytkownikom lub ogółowi, z której może korzystać w kraju co najmniej milion zarejestrowanych użytkowników. W zaproponowanej definicji internetowego serwisu społecznościowego wprowadzono minimum użytkowników korzystających z usługi w kraju, wynoszące jeden milion. Jednak nie sprecyzowano, w jaki sposób ma odbywać się – potencjalnie związana z przetwarzaniem danych osobowych – weryfikacja użytkowników, którzy są zarejestrowani w Polsce. Prezes UODO zwrócił uwagę, że nie jest jasne, na jakich zasadach, na podstawie jakich kryteriów i przez kogo będzie dokonywana weryfikacja takich użytkowników w celu ustalenia końcowej liczby zarejestrowanych użytkowników w kraju oraz

[300] DOL.401.491.2021.

na jakim podmiocie spoczywa obowiązek ustalenia tej liczby, jej aktualizacji np. na skutek dodawania, usuwania zarejestrowanych kont. Zwrócił uwagę projektodawcy, iż należy doprecyzować wskazane określenie „internetowy serwis społecznościowy" oraz zdefiniować termin „użytkownik zarejestrowany", ponieważ obecna konstrukcja definicji jest niekompletna i pozostawia szereg niedomówień, które uniemożliwiają jej właściwe zrozumienie i stosowanie. Projektowana ustawa przewiduje powstanie nowego organu, jakim będzie Rada Wolności Słowa, która ma stać na straży przestrzegania przez internetowe serwisy społecznościowe wolności wyrażania poglądów, pozyskiwania informacji, rozpowszechniania informacji, wyrażania przekonań religijnych, światopoglądowych i filozoficznych oraz wolności komunikowania się. W projekcie ustawy nie wskazano jednak, co mieści się w pojęciu zadań ustawowych wykonywanych przez Radę. Tymczasem kompetencji organów publicznych czy podmiotów wykonujących zadania publiczne nie powinno się domniemywać, zwłaszcza w związku z przetwarzaniem przez nie danych osobowych. Nie wydaje się jednocześnie, aby wystarczającym uzasadnieniem przyjmowanego rozwiązania było jedynie to, że dane szczególnych kategorii w ogólności są przetwarzane w serwisach społecznościowych. Dane z kategorii wskazanych w art. 9 ust. 1 rozporządzenia 2016/679, to informacje głęboko ingerujące w prywatność, objęte szczególnym reżimem przetwarzania wynikającym z przepisów RODO. Konieczne jest zatem przeprowadzenie testu prywatności w zakresie niezbędności przetwarzania takich danych przez Radę i wprowadzenia w przepisach właściwych mechanizmów ochrony praw i wolności osób, których tej kategorii dane miałyby być przetwarzane dla celów realizacji ustawy dla bliżej niesprecyzowanych zadań ustawowych Rady. Nie bez znaczenia jest także to, że przepisy rozporządzenia 2016/679 stanowią o przetwarzaniu danych osobowych dotyczących wyroków skazujących i czynów zabronionych (art. 10), z zachowaniem przewidzianych tym przepisem warunków. Prezes UODO podniósł, że projektodawca nie odnosi się do tej kategorii danych osobowych, a jednocześnie tego rodzaju informacje także mogą się pojawiać w treściach zamieszczanych w serwisach społecznościowych. Ponadto Prezes UODO zwrócił uwagę, że zgodnie z projektem ustawy obsługę merytoryczną, administracyjną i biurową Rady zapewnia Urząd Komunikacji Elektronicznej (UKE). Z projektowanej ustawy nie wynika jednak, jak następować ma przetwarzanie danych osobowych na potrzeby obsługi merytorycznej, administracyjnej i biurowej, realizowanej na rzecz Rady przez Urząd Komunikacji Elektronicznej. Tymczasem wymaga tego wzgląd na zasady: legalizmu i zgodności z prawem, rzetelności i przejrzystości. Regulacje te powinny być wprowadzane mocą przepisów ustawy, a nie wewnętrznego regulaminu określonego w drodze zarządzenia. Nie jest jasna również

rola, jaką wykonuje UKE w zakresie regulowanej przepisem obsługi merytorycznej, administracyjnej i biurowej w kontekście przetwarzania danych osobowych, zwłaszcza szczególnych kategorii. Wątpliwości budzi także to, czy projektodawca przeanalizował wszystkie aspekty związane z procesami przetwarzania danych, w szczególności te, związane z podziałem ról w procesach przetwarzania danych i w związku z realizacją obowiązków wynikających z rozporządzenia 2016/679 pomiędzy Radą a UKE. Dodatkowo projektowana ustawa ma na celu wprowadzenie zmian w ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[301]. Wątpliwości organu nadzorczego wzbudził proponowany zakres danych koniecznych do złożenia pozwu (wskazania danych pozwanego określonych w art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną), bowiem zawiera on szeroki katalog danych osobowych, w tym np. dane służące do weryfikacji podpisu elektronicznego usługobiorcy. W związku z tym organ właściwy w sprawie ochrony danych osobowych zwrócił uwagę, iż istotne jest ponowne rozważenie przez projektodawcę, czy wszystkie informacje objęte zakresem analizowanego przepisu są niezbędne i konieczne do przeprowadzenia postępowania o ochronę dóbr osobistych przeciwko osobom o nieustalonej tożsamości. Obecnie trwają dalsze prace nad projektem ustawy.

Zdarzają się sporadycznie sytuacje, w których projektodawcy uznają, że mogą wprowadzić do przepisów regulacje opierające przetwarzanie danych osobowych na przesłance zgody, co – jak podkreślał wielokrotnie organ nadzorczy – jest błędnym rozwiązaniem. Opiniując **projekt ustawy o fundacji rodzinnej**[302], organ nadzorczy zwrócił uwagę, że proponowana konstrukcja zgody (wyrażonej przez beneficjenta na przetwarzanie jego dodatkowych danych osobowych) powoduje wątpliwości na gruncie przepisów rozporządzenia 2016/679[303]. W ocenie organu proponowane brzmienie przepisu będzie powodowało, iż fundacja rodzinna będzie mogła jednocześnie żądać danych osobowych beneficjenta oraz przetwarzać te dane osobowe na podstawie zgody, co oznaczałoby nieakceptowalne przetwarzanie danych osobowych na podstawie pozornej zgody, pozbawionej niezbędnej cechy dobrowolności. Przyjęcie proponowanego rozwiązania oznaczałoby, że brak przekazania danych przez beneficjenta będzie się wiązał z potencjalnymi negatywnymi skutkami, tj. nieuzyskaniem świadczeń i jego konsekwencjami. W wytycznych Grupy Roboczej Art.

[301] Dz. U. z 2020 r. poz. 1575, 1578 i 2320 oraz z 2021 r. poz. 11.
[302] DOL.401.120.2022.
[303] Zgodnie z art. 4 pkt 11 rozporządzenia 2016/679 „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.

29 dotyczących zgody na mocy rozporządzenia 2016/679[304] wskazano, że co do zasady zgoda może być właściwą, zgodną z prawem podstawą wyłącznie wówczas, gdy osobie, której dane dotyczą, zapewnia się kontrolę oraz rzeczywistą możliwość wyboru w odniesieniu do przyjęcia lub odrzucenia zaoferowanych warunków lub odrzucenia ich bez niekorzystnych konsekwencji. Projektowane przepisy nie spełniają jednak tych warunków i wymagają zmiany przez projektodawcę. W opinii organu w miejsce rozwiązań opartych na zgodzie, jako warunku przetwarzania danych osobowych uzasadnione byłoby przyjęcie w przepisach projektowanej ustawy rozwiązania dopuszczającego przetwarzanie innych danych osobowych niż wymienione w projektowanym przepisie, ze wskazaniem celu i warunku niezbędności takiego przetwarzania nierozerwalnie związanych z profilem fundacji, jak i wsparciem beneficjenta znajdującego się w konkretnej sytuacji uzasadniającej przetwarzanie takich danych osobowych.

7.11. Podsumowanie

Wyżej wskazane zagadnienia nie wyczerpują całego katalogu spraw legislacyjnych, którymi w roku 2021 zajmował się organ nadzorczy. Wśród projektów aktów normatywnych, które wpłynęły do zaopiniowania, były także inne akty, zarówno prawa krajowego, jak i prawa wspólnotowego, opiniowane w ramach prac na poziomie Unii Europejskiej czy także umowy międzynarodowe nieujęte w niniejszym sprawozdaniu. Wśród zagadnień, które od lat znajdują się w kręgu zainteresowań organu nadzorczego znajdują się sprawy dotyczące sektora bankowego i ubezpieczeniowego, sytemu ochrony zdrowia czy przetwarzania danych przez organy ścigania.

Analiza projektów aktów prawnych w 2021 roku wskazuje na występowanie podobnych zjawisk, jak w roku 2020. Projektodawcy ze wszystkich sektorów nadal m.in.:

- nie wykonują testu prywatności, oceny wpływu planowanych w przepisach rozwiązań na ochronę danych, a w konsekwencji 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 – zwłaszcza nieprzejrzyste kształtowanie procesów przetwarzania danych wymaganych przepisami oraz niewyznaczanie celów lub wszystkich celów przetwarzania – zwiększają ryzyko przetwarzania w sposób nieodpowiadający zasadom wynikającym z RODO;

[304] WP259 rev.01.

- popełniają błąd nakładania obowiązków na podmioty biorące udział w procesach przetwarzania danych osobowych niezgodnie z rolami wyznaczonymi przepisami rozporządzenia 2016/679;
- nie zachowują hierarchii aktów prawnych i kształtują prawa i obowiązki związane z przetwarzaniem danych osobowych w przepisach wykonawczych, podczas gdy nie przewidują tego przepisy ustawowe albo też kształtują przepisy ustawowe z brakiem poszanowania warunków wynikających z norm RODO, dopuszczających wyjątki/ograniczenia;
- nie uwzględniają w projektowanych regulacjach prawnych konieczności stosowania zasad dotyczących przetwarzania danych osobowych określonych w RODO, zwłaszcza zasady zgodności z prawem, minimalizacji czy retencji danych, co przekłada się na problem niemożności wypełnienia zasady rozliczalności przez wykonawców norm;
- nie określają w ogóle albo błędnie bądź niewyczerpująco ról poszczególnych podmiotów i/lub organów biorących udział w procesach przetwarzania danych, zwłaszcza odpowiednio do celów przetwarzania danych czy przewidując rozwiązania stanowiące w swej istocie współadministrowanie danymi osobowymi;
- określają kwestie przekazywania informacji, udostępniania danych i dokumentów zawierających dane osobowe w sposób zbyt ogólny, niejednoznaczny, a przez to budzący wątpliwości interpretacyjne;
- niezbyt chętnie proponują – powołując się na ogólne przepisy rozporządzenia 2016/679 i brak szczegółowych wymogów – szczególne rozwiązania zmierzające do realizacji zasady poufności i integralności, wskazują ogólnie na konieczność przestrzegania bezpieczeństwa danych osobowych, zezwalają na stosowanie bliżej nieokreślonych aplikacji, systemów czy funkcjonalności, zwłaszcza na potrzeby zdalnego przetwarzania danych osobowych, a więc w sytuacjach wprowadzania rozwiązań z zakresu nowych technologii czy potrzeb wynikających z okoliczności pandemicznych;
- 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. W 2021 roku coraz częściej dopiero na etapie prac RCL lub sejmowego czy senackiego procesu legislacyjnego organ nadzorczy miał okazję wyrazić

swoje eksperckie stanowisko odnośnie do regulacji kształtujących przetwarzanie danych osobowych.

Z zadowoleniem należy natomiast przyjąć, że w roku sprawozdawczym 2021, podobnie jak w minionym roku 2020:

- Niektórzy projektodawcy – przyjmując wcześniejsze eksperckie wskazówki organu – wykonywali w toku procesu legislacyjnego ocenę wpływu planowanych rozwiązań na ochronę danych – test prywatności, a w uzasadnionych przypadkach ocenę skutków dla ochrony danych, doceniają bowiem, iż proces ten 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 skłaniali się ku konsultacjom przepisów dotyczących przetwarzania danych osobowych w ustaleniach roboczych, po skierowaniu przez organ pisemnego stanowiska do projektu;
- Coraz częściej projektodawcy wykazywali zrozumienie, że konstrukcja tworzonych przez nich przepisów dotyczących przetwarzania danych z uwzględnieniem przepisów RODO spotyka się nie tylko z pozytywną oceną organu nadzorczego, 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;
- Zjawiskiem stosunkowo nowym i pozytywnie rokującym było coraz częstsze poświęcanie odrębnych części lub wręcz rozdziałów projektowanych regulacji zagadnieniu przetwarzania danych osobowych – wprawdzie nie jest to rozwiązanie wymagane i nie zawsze jest konieczna taka konstrukcja aktu prawnego, niemniej przyjmowanie takich rozwiązań wskazuje na świadomość istoty tych regulacji oraz na troskę o ich kompleksowość także pod względem problematyki przetwarzania danych osobowych;
- Coraz rzadziej (choć nie jest to zjawisko całkowicie wyeliminowane) pojawiały się propozycje opierania przetwarzania danych osobowych na wpisanej w projektowane przepisy przesłance zgody;
- Coraz częściej projektodawcy – uwzględniając zasadę minimalizmu – proponowali przetwarzanie danych jedynie w zakresie niezbędnym dla celów regulacji;

- Coraz częściej projektodawcy – uwzględniając zasadę ograniczenia celu – wskazywali w normach prawych 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.

8. Zgłaszanie naruszeń ochrony danych osobowych

Zadaniem Urzędu realizowanym od 25 maja 2018 roku jest przyjmowanie od administratorów zgłoszeń naruszeń o ochronie 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 właściwemu organowi nadzorczemu 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. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[305] w art. 44 również nakłada na administratorów, w przypadku naruszenia ochrony danych osobowych, obowiązek zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Przepisu nie stosuje się, jeżeli nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych. 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[306] 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

[305] Dz. U. z 2019 r. poz. 125.
[306] Dz. U. z 2018 r. poz. 1954.

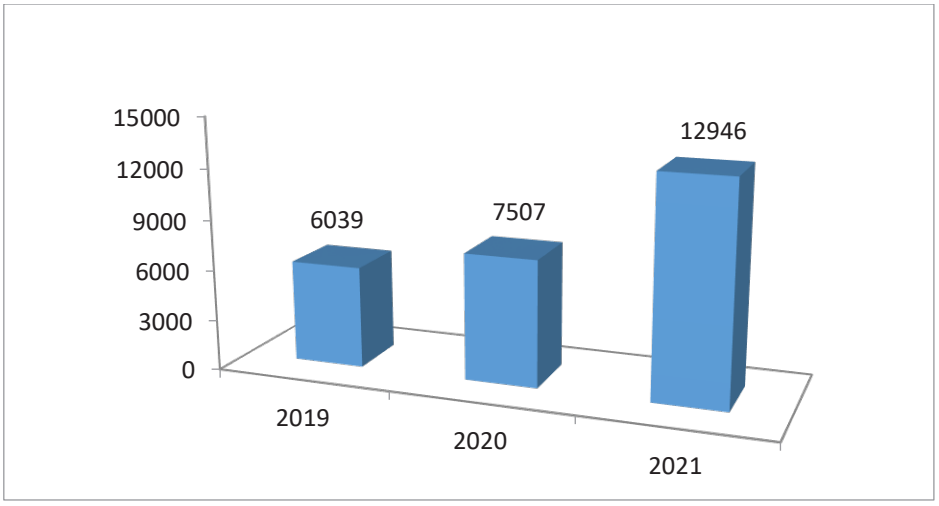
osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej.

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 rozporządzeniu 2016/679, 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 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.

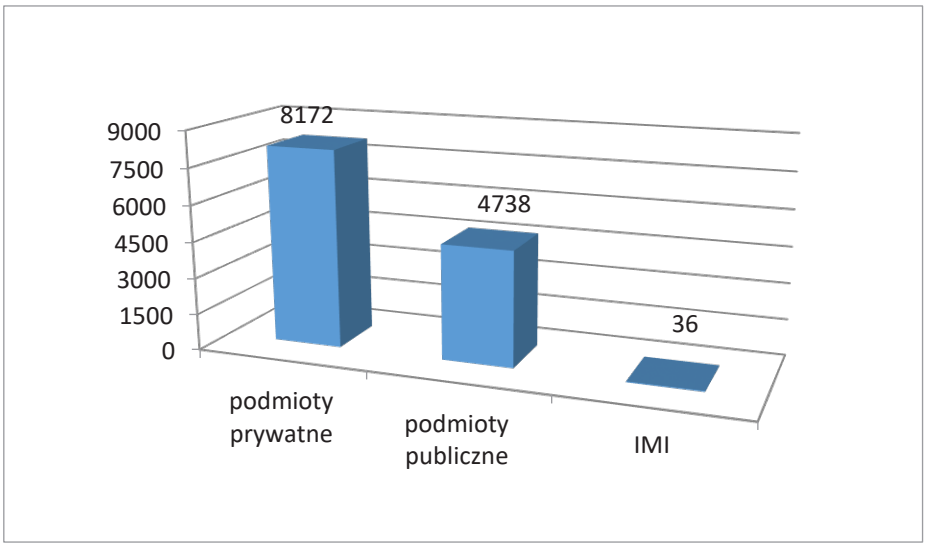
8.1. Statystyka zgłaszanych naruszeń ochrony danych osobowych

W 2021 roku do Urzędu Ochrony Danych Osobowych wpłynęło **12946 zgłoszeń naruszeń.** Porównanie liczby zgłoszeń naruszeń ochrony danych osobowych w latach 2019–2021 przedstawia poniższy wykres:



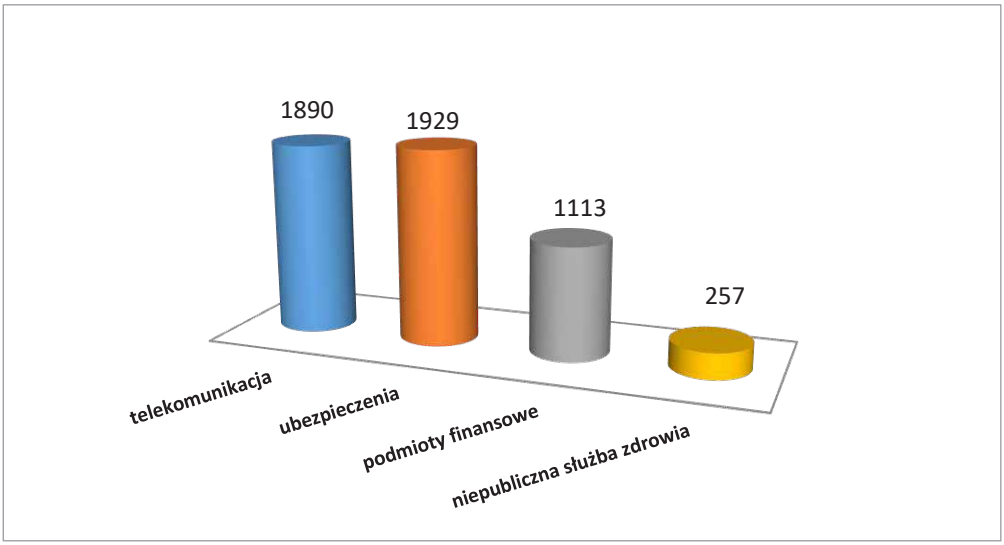
Wykres 8: **Liczba naruszeń ochrony danych osobowych, które wpłynęły do Urzędu Ochrony Danych Osobowych w latach 2019–2021.**

Spośród **12946** zgłoszeń naruszeń, które wpłynęły w 2021 roku, **8172 zostało zgłoszonych przez podmioty sektora prywatnego**, **4738 przez podmioty sektora publicznego**, zaś **36 zgłoszono w międzynarodowym systemie informatycznym (IMI).**



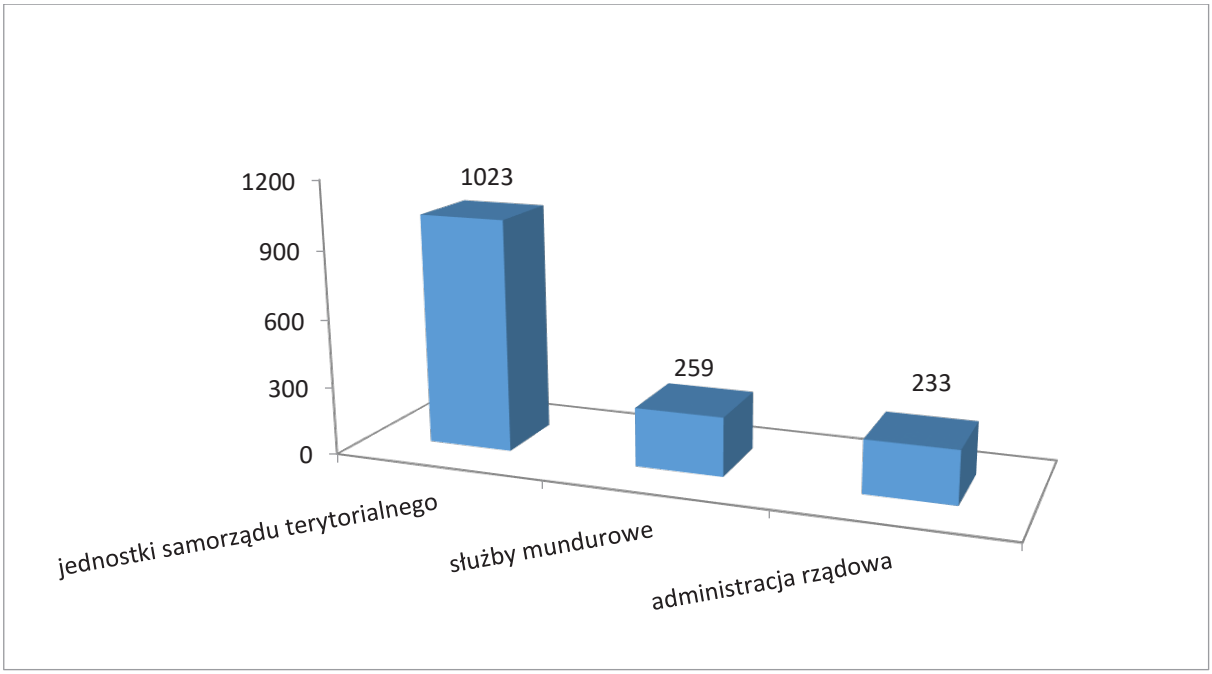
Wykres 9: **Liczba naruszeń ochrony danych osobowych, które wpłynęły do UODO w 2021 roku, z podziałem na sektor prywatny, publiczny oraz zgłoszonych w międzynarodowym systemie informatycznym (IMI).**

W przypadku **sektora prywatnego** najwięcej zgłoszeń napłynęło od podmiotów: telekomunikacyjnych – 1890, ubezpieczeniowych – 1929, banków i podmiotów finansowych – 1113 oraz niepublicznej służby zdrowia – 257.



Wykres 10: **Liczba zgłoszeń naruszeń ochrony danych osobowych od podmiotów prywatnych, które wpłynęły do UODO w 2021 roku.**

W **sektorze publicznym** zawiadomienia o incydentach z danymi osobowymi najczęściej nadsyłały: jednostki samorządu terytorialnego – 1023, służby mundurowe – 259 oraz administracja rządowa – 233.



Wykres 11: **Liczba zgłoszeń naruszeń ochrony danych osobowych od podmiotów publicznych, które wpłynęły do UODO w 2021 roku.**

Dla porównania w 2020 roku do Urzędu Ochrony Danych Osobowych wpłynęło **7507** notyfikacji naruszeń, w tym 4661 zostało zgłoszonych przez podmioty sektora prywatnego, 2691 przez podmioty sektora publicznego, zaś 155 zgłoszonych w międzynarodowym systemie informatycznym (IMI).

Należy podkreślić, że zgłoszenia naruszeń ochrony danych osobowych dokonywali zarówno sami administratorzy, osoby, których danych osobowych naruszenie dotyczyło, jak i osoby nieuprawnione, które w sposób niezamierzony weszły w posiadanie danych dla nich nieprzeznaczonych.

Wzrost liczby zgłoszeń naruszeń ochrony danych osobowych w 2021 roku 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.

8.2. Naruszenia a stan zagrożenia epidemiologicznego

Dodatkowo w roku 2021 do Prezesa UODO zgłaszano naruszenia związane z zagrożeniem epidemiologicznym, które wymogło na administratorach danych podejmowanie

dodatkowych środków w celu ochrony danych osobowych osób w sferach, które nie były wcześniej poddawane szczegółowej analizie pod kątem wystąpienia możliwych zagrożeń i podatności. Należy podkreślić, że skutkiem tych incydentów było naruszenie prawa do prywatności osób, których zdarzenie dotyczyło.

Jedno ze zgłoszonych naruszeń dotyczyło wysłania błędnego pliku, zawierającego formularz z danymi osób mających kontakt z osobami zakażonymi COVID-19 do Stacji Sanitarno-Epidemiologicznej. Błąd polegał na przypisaniu niewłaściwego numeru PESEL do danych innego dziecka z klasy. Spowodowało to, że inny rodzic dziecka z klasy otrzymał informację od Stacji Sanitarno-Epidemiologicznej o skierowaniu dziecka na kwarantannę. Za pomocą systemu telefonicznego (automatyczne telefoniczne powiadamianie o objęciu kwarantanną) poinformowano niewłaściwego rodzica także o imieniu i nazwisku tego dziecka. W ten sposób niewłaściwi rodzice mogli otrzymać informacje w zakresie imienia i nazwiska innego niż swoje dziecko oraz o nałożeniu na niego kwarantanny. Pośrednio zaś otrzymali informacje o stanie zdrowia tego dziecka – że albo jest ozdrowieńcem lub że nie zostało zaszczepione.

Do UODO wpłynęło też wiele zgłoszeń naruszenia ochrony danych osobowych przesyłanych przez Ministra Zdrowia, które dotyczyły w szczególności administrowanego przez Centrum e-Zdrowie systemu rejestracji na szczepienia przeciwko COVID-19 i testy diagnostyczne w kierunku SARS-CoV-2. Centrum e-Zdrowia odpowiada za techniczną obsługę systemu i zapewnia w imieniu Ministra Zdrowia dostęp do systemu podmiotom, którym dane są udostępniane na podstawie rozporządzenia Rady Ministrów z dnia 26 lutego 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[307]. Naruszenia te polegały m.in. na nadawaniu nieupoważnionym osobom uprawnień do edytowania danych, błędnym przypisaniu użytkowników w konsekwencji błędu pracownika, lub przekazaniu danych osobowych do przetwarzania podprocesorowi bez podstawy prawnej. Minister Zdrowia podjął adekwatne środki w celu zminimalizowania ryzyka ponownego wystąpienia tego typu naruszeń. Przykładowo polegały one na: zmianie procedury zakładania kont osób kierowanych na szczepienia i badania, która dotychczas przeprowadzana była przez pracowników Ministerstwa Zdrowia i wymagała podania identyfikatora laboratorium. W nowej zaś formule zapisanie się umożliwione zostało samym pacjentom, od których nie była wymagana znajomość identyfikatora laboratorium; zawarciu przez Ministra Zdrowia stosownej umowy powierzenia przetwarzania danych z podmiotem, który

[307] Dz. U. poz. 367.

dotychczas przetwarzał dane osobowe w jego imieniu i zgodnie z jego zaleceniami, bez podstawy prawnej.

8.3. Najczęściej zgłaszane oraz typowe naruszenia w 2021 r.

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

a) **Nieprawidłowe zaadresowanie lub zapakowanie korespondencji** (w formie tradycyjnej lub elektronicznej) – w konsekwencji tych naruszeń udostępniano dane osobowe osobom nieuprawnionym. Naruszenia te powstawały najczęściej w wyniku błędu pracownika administratora danych i miały z reguły charakter jednorazowego incydentu. Ale źródłem naruszenia stawały się także błędy już na etapie gromadzenia danych adresowych, gdy niedoszli adresaci przesyłek wskazywali administratorom nieprawidłowe adresy do korespondencji. W ramach zastosowanych środków bezpieczeństwa, w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia w przyszłości, administratorzy przeprowadzali dodatkowe szkolenia pracowników, dokonywali aktualizacji baz danych, zobowiązywali osoby nieuprawnione, które weszły w posiadanie dokumentów, do trwałego i bezpowrotnego usunięcia danych i potwierdzenia braku ich nieuprawnionego wykorzystania. Wdrażali też środki bezpieczeństwa w postaci np. wymuszenia dwukrotnego podania adresu do korespondencji w formularzu lub szyfrowania wiadomości. Ponadto do udostępniania danych osobowych niewłaściwym adresatom dochodziło często w konsekwencji wysyłania masowej korespondencji elektronicznej bez ukrycia adresów e-mail innych osób (UDW).

b) **Nieprawidłowa anonimizacja danych lub niezamierzona ich publikacja** – w sektorze publicznym dochodziło do tego typu naruszeń m.in. w Biuletynie Informacji Publicznej i dziennikach urzędowych. W sprawach tego typu naruszeń administratorzy z reguły usuwali nieprawidłowo opublikowane informacje oraz wprowadzali dodatkowe środki bezpieczeństwa, minimalizujące ryzyko powtórzenia się analogicznych nieprawidłowości np. w postaci dodatkowej weryfikacji anonimizacji dokumentów, która miała zmniejszyć ryzyko przeoczenia przez pracownika podobnego błędu w przyszłości.

c) **Udostępnienie danych niewłaściwej osobie** – do tego typu naruszeń dochodziło m.in. w konsekwencji wydawania dokumentów (np. zaświadczeń i deklaracji podatkowych) osobom bez uprawnień do ich otrzymania lub omyłkowych zaksięgowań przelewów.

Administratorzy w celu ograniczenia częstotliwości występowania tego typu naruszeń w przyszłości, podejmowali działania polegające na dyscyplinowaniu pracowników, organizowaniu dodatkowych szkoleń z zakresu ochrony danych osobowych, przeglądzie obowiązujących procedur, a także zwracali się do osób nieuprawnionych o zwrot dokumentów.

d) **Zagubienie korespondencji przez operatora pocztowego lub otwarcie korespondencji przed zwróceniem jej do nadawcy** – w dobie światowej pandemii do naruszeń tego typu dochodziło także w konsekwencji przechowywania korespondencji na „kwarantannie", co uniemożliwiało złożenie reklamacji do operatora pocztowego w terminie i skuteczne ustalenie, na jakim etapie obiegu korespondencji doszło do jej otwarcia lub zniszczenia. W ramach działań naprawczych, po wystąpieniu tego typu naruszeń, administratorzy składali reklamację do operatora pocztowego, dokonywali aktualizacji instrukcji kancelaryjnej oraz zmieniali postanowienia umów zawartych z operatorem pocztowym.

e) **Nieuprawniony dostęp do baz danych** – do tych naruszeń dochodziło wskutek błędów oprogramowania ujawniających się po aktualizacji, braku regularnych testów bezpieczeństwa w kierunku wykrycia podatności systemu oraz nieprawidłowego nadawania uprawnień. W ramach działań naprawczych administratorzy zlecali wykonanie audytów informatycznych firmom zewnętrznym, przeprowadzali testy systemów w środowisku deweloperskim, a także przeprowadzali analizę nadawanych uprawnień.

f) **Zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej** – do tego typu naruszeń dochodziło przeważnie wskutek opieszałości pracowników i miały one z reguły charakter jednorazowych incydentów. Zdarzały się także przypadki pozostawiania dokumentów w ogólnodostępnych lokacjach w celu ograniczenia zagrożenia epidemiologicznego. Chodzi o praktykę „wystawiania" prowizorycznych, niezabezpieczonych pojemników pełniących funkcje skrzynek podawczych służących do składania dokumentów zawierających dane osobowe. W celu obniżenia prawdopodobieństwa wystąpienia tego typu naruszeń w przyszłości, administratorzy danych wdrażali systemy DLP (Data Loss Prevention) oraz przesyłali dokumenty bezpośrednio na skrzynki e-mail pracowników. W przypadku kradzieży dokumentów powiadamiane były organy ścigania. Prowizoryczne rozwiązania w zakresie przyjmowania dokumentów, bez bezpośredniego kontaktu z klientem, zastępowane były innymi, bezpiecznymi rozwiązaniami.

g) **Zagubienie lub kradzież nośnika danych** – do tego typu naruszeń dochodziło w wyniku utraty nośników danych typu laptop lub „pendrive", które często pozostawały w chwili zdarzenia niezaszyfrowane. W celu zminimalizowania prawdopodobieństwa wystąpienia tego typu naruszeń w przyszłości, administratorzy decydowali się na szyfrowanie urządzeń wykorzystywanych do przetwarzania danych osobowych, dokonywali weryfikacji stosowania się przez pracowników do zasady ograniczonego czasu przechowywania danych osobowych, wprowadzali rozwiązania umożliwiające usuwanie danych osobowych z urządzeń na dystans oraz rozpoczęli wykorzystywanie w większym stopniu rozwiązań chmurowych. Kradzieże nośników danych były zgłaszane organom ścigania.

h) **Wykorzystanie złośliwego oprogramowania ingerującego w poufność, integralność lub dostępność danych osobowych** – do tego typu naruszeń dochodziło w wyniku wykorzystania podatności i przełamania zabezpieczeń. W wielu przypadkach podatności systemu były spowodowane brakiem aktualizacji oprogramowania przez administratora. Aby zaradzić tego rodzaju naruszeniom, z reguły przywracano dane osobowe z kopii zapasowych, które nie zawsze były jednak przez administratorów regularnie sporządzane, a w przypadku braku kopii zapasowych, administratorzy zwracali się o pomoc w odszyfrowaniu danych do wyspecjalizowanych w tej dziedzinie podmiotów. W celu eliminowania tego typu naruszeń w przyszłości administratorzy przeprowadzali dodatkowe testy bezpieczeństwa, aktualizowali oprogramowania antywirusowe, podnosili wymogi regularnego testowania, mierzenia i oceniania skuteczności stosowanych środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania, zgłaszali naruszenie organom ścigania oraz Zespołowi CERT Polska.

Analizując **zgłoszenia naruszeń ochrony danych osobowych,** które stwarzają ryzyko dla praw lub wolności osób fizycznych, w 2021 roku – w porównaniu z rokiem poprzednim – **w sektorze prywatnym** nastąpił wyraźny wzrost zgłaszanych naruszeń od podmiotów z sektora ubezpieczeniowego. Najczęściej zgłaszane naruszenia ochrony danych osobowych przez administratorów tego sektora dotyczyły nieprawidłowego zaadresowania korespondencji (zarówno w formie tradycyjnej, jak i elektronicznej), zagubienia dokumentu zawierającego dane osobowe (głównie w formie papierowej) przez operatorów pocztowych lub podmioty świadczące usługi kurierskie, udostępnienie danych w formie papierowej lub elektronicznej osobie nieuprawnionej. W tym ostatnim przypadku do naruszeń poufności danych dochodziło wskutek m.in. wydawania

osobie nieuprawnionej dokumentów (umów, aneksów do umów) zawierających dane osobowe innych osób.

W omawianym 2021 r. nastąpił również wzrost zgłaszanych naruszeń od podmiotów z **sektora publicznego,** w szczególności jednostek samorządu terytorialnego. Najczęściej zgłaszane naruszenia przez tych administratorów dotyczyły publikacji danych osobowych w Biuletynie Informacji Publicznej (BIP) lub na stronie internetowej administratora oraz procesu wysyłania i dostarczania korespondencji. W ramach zastosowanych środków bezpieczeństwa, w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia w przyszłości, administratorzy usuwali treści z witryn internetowych, przeprowadzali dodatkowe szkolenia pracowników i dokonywali aktualizacji baz danych. Ponadto zgłaszane naruszenia dotyczyły zagubienia korespondencji przez operatora pocztowego lub podmiot świadczący usługi kurierskie, a także otwarcia korespondencji przed zwróceniem jej do nadawcy, nieprawidłowej anonimizacji danych, udostępnienia danych niewłaściwej osobie lub wysłania danych do niewłaściwego odbiorcy. Ww. przedmiot zgłaszanych naruszeń miał również charakter dominujący w odniesieniu do pozostałych podmiotów z sektora publicznego.

W okresie sprawozdawczym nastąpił znaczący wzrost zgłaszanych naruszeń ochrony danych osobowych zarówno **w sektorze prywatnym, jak i publicznym**, związanych z atakami z użyciem oprogramowania *ransomware*, które szyfruje zasoby zawierające dane osobowe, uniemożliwiając do nich dostęp, w następstwie czego atakujący oferują klucz deszyfrujący za opłatą. Spełnienie żądania szantażu nie zawsze jednak powodowało odszyfrowanie danych. Niewątpliwie ataki z użyciem ww. oprogramowania miały wpływ na dostępność, a w wielu przypadkach także poufność oraz integralność danych osobowych, a w konsekwencji na ochronę praw lub wolności osób, których dane te dotyczyły. Dlatego też analizując tego typu zgłoszenia, organ nadzorczy zwracał szczególną uwagę, czy zaatakowany podmiot dokonał analizy ryzyka uwzględniającej tego typu zagrożenia dla określonego zasobu bądź zasobów, w szczególności dla systemów informatycznych wykorzystywanych do przetwarzania danych osobowych oraz czy wdrożył odpowiednie środki techniczne i organizacyjne w celu zapewnienia, aby przetwarzanie odbywało się zgodnie z rozporządzeniem 2016/679 i w celu nadania przetwarzaniu niezbędnych zabezpieczeń oraz czy wdrożone środki techniczne i organizacyjne podlegają regularnemu testowaniu, mierzeniu i ocenianiu (chodzi tu np. o wykonywanie testów zabezpieczeń technicznych oraz organizacyjnych w odniesieniu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych), a także dokumentowaniu w określonych przedziałach czasowych. Ponadto zwracał

uwagę, czy podmiot wdrożył i stosuje procedury w zakresie sporządzania kopii zapasowych danych, a w szczególności ich weryfikacji pod kątem zapewnienia spójności danych w przypadku konieczności ich przywrócenia w związku z incydentem technicznym lub fizycznym.

8.4. Wyjaśnienia

Zasadniczym uprawnieniem organu nadzorczego, niezbędnym do prawidłowego prowadzenia czynności w następstwie dokonanego zgłoszenia naruszenia ochrony danych osobowych, jest uprawnienie do nakazania dostarczenia informacji. Prawodawca nadaje te uprawnienia Prezesowi Urzędu w art. 58 ust. 1 lit. a) i e) rozporządzenia 2016/679. Korzystając z uprawnień określonych w ww. przepisie, polegających na nakazaniu administratorom, podmiotom przetwarzającym oraz ich przedstawicielom, zapewnienia dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji jego zadań, Prezes Urzędu wystosował do administratorów danych osobowych dokonujących zgłoszeń naruszeń **1321 pisemnych wezwań do złożenia wyjaśnień lub udzielił pisemnych informacji w związku z przypadkami naruszeń ochrony danych osobowych.**

W większości przypadków wątpliwości Prezesa Urzędu budziły: (i) zastosowane lub proponowane przez administratorów środki bezpieczeństwa w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia; (ii) środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą; (iii) nieprawidłowe oszacowanie poziomu ryzyka naruszenia praw lub wolności osób fizycznych; (iv) nieprawidłowe oszacowanie terminu dokonanego zgłoszenia oraz wyjaśnienia przyczyn opóźnienia powiadomienia organu nadzorczego o naruszeniu; (v) dochowanie obowiązku zawiadomienia osób, których dane dotyczą; (vi) wskazane przez administratorów kategorie i liczba osób oraz danych objętych naruszeniem.

Adresaci pism nie mieli możliwości kwestionowania zakresu żądanych informacji i w większości przypadków podejmowali działania służące zagwarantowaniu odpowiedniego poziomu bezpieczeństwa danych i zminimalizowaniu ryzyka ich przetwarzania w sposób niezgodny z przepisami prawa oraz udzielali organowi oczekiwanych wyjaśnień i informacji.

Z analizy przebiegu obsługi zgłoszeń naruszenia ochrony danych osobowych należy wnioskować, że realizacja kompetencji Prezesa Urzędu w trybie art. 58 ust. 1 lit. a) i e) rozporządzenia 2016/679 pozytywnie wpływała na ochronę danych osobowych. Znacznie bowiem skracała proces przywracania 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 i stosunkowo długim czasem oczekiwania na wydanie decyzji administracyjnej. Podkreślić należy, że cel, jakiemu służy obowiązek zgłaszania naruszeń ochrony danych osobowych i ich kontroli, wymagał wyposażenia Prezesa Urzędu Ochrony Danych Osobowych w instrumenty prawne umożliwiające 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 negatywnymi konsekwencjami naruszenia, zaś administratorzy – niezwłocznie zastosować środki bezpieczeństwa w celu ograniczenia rozmiaru naruszenia i w konsekwencji wyrządzonych szkód.

8.5. Postępowania administracyjne

W 2021 roku Prezes Urzędu wszczął z urzędu **49 postępowań administracyjnych w sprawie naruszenia przepisów o ochronie danych osobowych.** W przypadku niektórych naruszeń podjęta została decyzja o przeprowadzeniu u administratora danych kontroli przestrzegania przepisów o ochronie danych osobowych.

Wątpliwości Prezesa Urzędu w związku z naruszeniami ochrony danych osobowych, które wymagały przeprowadzenia postępowania administracyjnego, dotyczyły w szczególności:

a) przeprowadzonej przez administratorów danych oceny ryzyka naruszenia praw lub wolności osób fizycznych, skutkującej koniecznością zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia osób, których naruszenie to dotyczyło;
b) 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. b) i lit. d) rozporządzenia 2016/679;
c) doboru zabezpieczeń systemu informatycznego oraz testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych

objętych naruszeniem, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia;

d) sposobu realizacji przez podmiot przetwarzający postanowień umowy powierzenia przetwarzania uwzględniającej kryteria zawarte w art. 28 ust. 3 rozporządzenia 2016/679, w szczególności dotyczące spełniania obowiązku przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, podejmowania wszelkich środków wymaganych na mocy art. 32 rozporządzenia 2016/679 oraz – po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych – usuwania lub zwracania administratorowi wszelkich danych osobowych i usuwania wszelkich ich istniejących kopii[308];
e) treści zawiadomienia osób, których dane dotyczą, o naruszeniu ich danych osobowych pod kątem spełniania wymogów określonych w rozporządzeniu 2016/679[309].

8.6. Decyzje administracyjne

Część prowadzonych przez Prezesa Urzędu postępowań administracyjnych została zakończona w 2021 roku, czego konsekwencją było wydanie **36 decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych.**

W dwudziestu jeden (21) decyzjach Prezes UODO udzielił upomnienia administratorowi danych, w tym w trzech (3) decyzjach udzielił upomnienia, a w pozostałej części tych trzech decyzji postępowanie administracyjne zostało umorzone.

W dwóch (2) decyzjach udzielił upomnienia i odpowiednio nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 poprzez: przeprowadzenie analizy ryzyka w celu oszacowania właściwego poziomu ryzyka wiążącego się z przetwarzaniem danych osobowych, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, uwzględniając stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, w tym zagrożenia związane z zainstalowaniem złośliwego oprogramowania ingerującego w dostępność danych oraz

[308] Art. 28 ust. 3 lit. a), c) i g rozporządzenia 2016/679.
[309] Art. 34 ust. 2 w zw. z art. 33 ust. 3 lit. b), c) i d) RODO.

zagrożenia w postaci braku możliwości odtworzenia danych z kopii zapasowej w razie wystąpienia incydentu technicznego lub fizycznego oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

W kolejnych dwóch (2) decyzjach udzielił upomnienia i nakazał zawiadomienie o naruszeniu osób, których dane dotyczą, zaś w pięciu (5) – postępowanie administracyjne w całości zostało umorzone. W przypadku dziesięciu naruszeń Prezes Urzędu Ochrony Danych Osobowych, po przeprowadzeniu postępowań administracyjnych w wydanych decyzjach administracyjnych, zdecydował się nałożyć na administratorów danych administracyjne kary pieniężne[310].

Poniżej przytoczone zostały wybrane przykłady decyzji Prezesa UODO, udzielające upomnienia administratorowi w związku ze stwierdzeniem naruszenia ochrony danych osobowych.

Prezes UODO, wobec stwierdzenia naruszenia przez **Miejski Ośrodek Pomocy Społecznej**[311] przepisów rozporządzenia 2016/679, wydał decyzję, w której udzielił upomnienia Ośrodkowi i nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 poprzez: przeprowadzenie analizy ryzyka w celu oszacowania właściwego poziomu ryzyka wiążącego się z przetwarzaniem danych osobowych oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Naruszenie ochrony danych osobowych polegało na przełamaniu zabezpieczeń systemu informatycznego Ośrodka, wykorzystywanego do przetwarzania danych osobowych pracowników, klientów, dzieci oraz osób o szczególnych potrzebach i następnie zaszyfrowaniu przetwarzanych w nim danych. Naruszenie to dotyczyło łącznie ponad 100 osób. W konsekwencji Ośrodek został pozbawiony dostępu do ww. systemu oraz znajdujących się w nim danych osobowych.

W związku z powyższym, Prezes UODO wszczął postępowanie administracyjne, w którym ustalił, że w przeprowadzonej przez Ośrodek analizie nie uwzględniono zagrożenia w postaci

[310] Opis wspomnianych 10 decyzji nakładających administracyjne kary pieniężne przedstawione są w rozdziale 9 niniejszego *„Sprawozdania…”*.
[311] Sygn. akt DKN.5131.36.2021.

zaszyfrowania danych w wyniku działania złośliwego oprogramowania oraz zagrożenia w postaci niespójności baz danych odtworzonych z kopii zapasowej. W konsekwencji doprowadziło to do niewłaściwego doboru środków bezpieczeństwa i pojawienia się ryzyka polegającego na zaszyfrowaniu danych osobowych przez złośliwe oprogramowanie. Nastąpił również brak możliwości szybkiego przywrócenia dostępności do danych w związku z niespójnością baz danych odtworzonych z kopii zapasowej.

Efektem nieprawidłowo przeprowadzonej analizy ryzyka był również brak właściwych procedur w zakresie sporządzania kopii zapasowych danych, a w szczególności ich weryfikacji pod kątem zapewnienia spójności danych w przypadku konieczności ich przywrócenia w związku z incydentem technicznym lub fizycznym.

Prezes UODO w uzasadnieniu decyzji stwierdził, że Ośrodek nie wykonywał testów zabezpieczeń technicznych oraz organizacyjnych w odniesieniu do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych oraz że środki techniczne i organizacyjne nie były w odpowiedni sposób poddawane przeglądom i uaktualniane. Wykazał też, że Ośrodek przed wystąpieniem naruszenia używał do przetwarzania danych oprogramowania, które utraciło wsparcie producenta. Nie było więc odpowiedniego zabezpieczenia danych przetwarzanych przy jego użyciu, w sytuacji jednoczesnego braku innych środków technicznych i organizacyjnych mających na celu zminimalizowanie ryzyka naruszenia bezpieczeństwa danych. Prezes UODO w wydanej decyzji uznał, że Ośrodek nie wdrożył odpowiednich środków technicznych i organizacyjnych w czasie przetwarzania danych osobowych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem 2016/679, przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem danych osobowych.

Okolicznością przemawiającą za udzieleniem Ośrodkowi upomnienia był brak podstaw do uznania, że osoby, których dane dotyczą, poniosły jakąkolwiek szkodę na skutek tego naruszenia, w związku z czasową niedostępnością systemów informatycznych Ośrodka, zaś zgłoszone naruszenie ochrony danych osobowych miało charakter jednorazowy.

W kolejnej sprawie Prezes UODO stwierdził naruszenie przez administratora, będącego **starostą powiatowym**[312], przepisów rozporządzenia 2016/679, polegające na doborze nieskutecznych zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz braku odpowiedniego testowania, mierzenia i oceniania skuteczności środków

[312] Sygn. akt DKN.5131.9.2021.

technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, a także na niezawiadomieniu osób, których dane dotyczą o tym naruszeniu.

Naruszenie dotyczyło przełamania zabezpieczeń systemu informatycznego, wykorzystywanego do przetwarzania danych osobowych klientów oraz osób figurujących w ewidencji gruntów i budynków powiatu. Zaszyfrowane zostały również kopie zapasowe. Zgodnie ze zgłoszeniem administrator nie stwierdził wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w związku z czym nie zawiadomił osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych.

Zdaniem organu administrator nie dokonał analizy ryzyka związanego ze stosowaniem środków bezpieczeństwa dla danego zasobu, w szczególności nie uwzględnił stosowania mechanizmu Remote Deskop Protocol (RDP) oraz nie zweryfikował, czy oprogramowanie wykorzystane do zdalnego dostępu zapewnia poufność przekazywanych informacji (np. z użyciem szyfrowania). Analiza ta nie uwzględniała również podatności przyjętego przez administratora systemu sporządzania kopii zapasowej na działanie oprogramowania typu *ransomware*. Co więcej, kopie zapasowe systemów, danych i baz danych zapisywane były raz w miesiącu na jeden zewnętrzny dysk, co w przypadku jego uszkodzenia lub awarii uniemożliwiłoby odtworzenie znajdujących się na nim danych.

W ocenie Prezesa UODO administrator w sposób nieprawidłowy przyjął brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, następstwem czego była rezygnacja z zawiadomienia o naruszeniu osób, których dane dotyczą (naruszenie art. 34 ust. 1 i 2 rozporządzenia 2016/679). Jednakże z uwagi na fakt, że dane osobowe objęte niniejszym naruszeniem ochrony zostały odtworzone, a samo naruszenie nie spowodowało naruszenia poufności danych, nakazanie zawiadomienia osób, których dane dotyczą, o naruszeniu zgodnie z art. 34 ust. 1 i 2, nie miało uzasadnienia. W związku z powyższym Prezes UODO uznał, że w ustalonych okolicznościach niniejszej sprawy wystarczającym środkiem było udzielenie administratorowi upomnienia.

Prezes UODO wobec stwierdzenia naruszenia przez **Pomorski Związek Piłki Nożnej**[313] przepisów art. 32 ust. 1 i 2 rozporządzenia 2016/679, polegającego na doborze nieskutecznych zabezpieczeń systemu informatycznego oraz braku odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo

[313] Sygn. akt DKN.5131.28.2021.

przetwarzanych danych osobowych, udzielił upomnienia oraz nakazał dostosowanie operacji przetwarzania do przepisów RODO, przeprowadzenie analizy ryzyka oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Naruszenie ochrony danych osobowych polegało na przełamaniu zabezpieczeń systemu informatycznego wykorzystywanego przez Związek do przetwarzania danych osobowych, a następnie zaszyfrowaniu przetwarzanych w nim danych. Zaszyfrowane bazy obejmowały około 3500 rekordów osób współpracujących ze Związkiem. W konsekwencji Związek został pozbawiony dostępu do znajdujących się w systemie danych osobowych. Administrator nie potrafił odtworzyć danych osobowych znajdujących się na kopiach zapasowych, gdyż poprawność ich zapisu nie była weryfikowana.

Brak rzetelnie przeprowadzonej analizy ryzyka, w połączeniu z brakiem regularnego testowania, mierzenia i oceniania skuteczności wdrożonych środków bezpieczeństwa oraz brakiem wdrożenia adekwatnych środków technicznych (w postaci przede wszystkim prawidłowego systemu tworzenia kopii zapasowych, który umożliwia odzyskanie po utracie lub uszkodzeniu oryginalnych plików i danych utraconych w wyniku m.in. infekcji złośliwym oprogramowaniem) i organizacyjnych (w postaci przeprowadzania regularnych szkoleń pracowników z zakresu ataków phishingowych) mających zapewnić bezpieczeństwo przetwarzania, doprowadziło do naruszenia ochrony danych. Braki te przesądziły również o naruszeniu przez Związek obowiązków spoczywających na administratorze danych, wynikających z art. 32 ust. 1 i 2 rozporządzenia 2016/679.

9. Administracyjne kary pieniężne

W roku sprawozdawczym 2021 Prezes Urzędu Ochrony Danych Osobowych nałożył w sumie **18 administracyjnych kar pieniężnych**, z czego 17 zostało nałożonych na podstawie przepisów RODO, zaś 1 kara na podstawie przepisów Prawa telekomunikacyjnego.

Spośród **18** kar pieniężnych, siedem (7) z nich nałożonych zostało za brak współpracy w związku z nieudzieleniem informacji niezbędnych organowi nadzorczemu do realizacji jego

zadań[314], zaś w jednej (1) sprawie Prezes UODO nałożył administracyjną karę pieniężną za nieprzestrzeganie nakazu decyzji[315].

Natomiast pozostałych **10** kar dotyczyło naruszeń ochrony danych osobowych.

Zestawienie wszystkich administracyjnych kar pieniężnych wymierzonych przez Prezesa Urzędu Ochrony Danych Osobowych w 2021 roku znajduje się w załączniku nr 1.

Egzekucja obowiązków o charakterze pieniężnym

W 2021 roku Prezes UODO podjął działania egzekucyjne wobec 3 decyzji nakładających administracyjne kary pieniężne, w związku z nieuiszczeniem tych kar przez zobowiązane podmioty. Wszystkie powyższe niezapłacone kary zostały nałożone na podmioty prywatne – Spółki prawa handlowego, natomiast ich wysokość stanowi łącznie kwotę 55 632,20 zł, na którą składają się 2 kary po 21 397 zł i 1 kara w kwocie 12 838,20 zł. Jak wyżej wspomniano, w przypadku egzekucji obowiązków pieniężnych wynikających z decyzji administracyjnych Prezes UODO występuje w roli wierzyciela. Dlatego też, po bezskutecznych upomnieniach wzywających do zapłaty powyższych kar, Prezes UODO na podstawie przepisów o postępowaniu egzekucyjnym w administracji wystawił tytuły egzekucyjne i przekazał je Naczelnikom właściwych Urzędów Skarbowych, którzy pełnią rolę organów egzekucyjnych w tych sprawach. Do czasu zakończenia prac nad niniejszym sprawozdaniem, przedmiotowe postępowania egzekucyjne prowadzone przez Naczelników Urzędów Skarbowych były w toku i nie zostały jeszcze zakończone.

Administracyjna kara pieniężna jako środek naprawczy przymuszający do wykonania nakazu decyzji

Nakazy zawarte w decyzjach 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 osobowych. Zadaniem Prezesa UODO jest monitorowanie przestrzegania przepisów o ochronie danych osobowych, w tym także monitorowanie przestrzegania nakazów zawartych w jego decyzjach. Dlatego też Prezes UODO nie może pozwolić na ignorowanie wydawanych przez siebie orzeczeń. Istotnym narzędziem służącym do zapewnienia wykonania

[314] DKE.561.16.2020, DKE.561.25.2020, DKE.561.23.2020, DKE.561.16.2021, DKE.561.13.2021, DKE.561.19.2021, DKE.561.1.2021.
[315] DKE.561.11.2020.

nakazów decyzji jest uprawnienie organu nadzorczego do wszczęcia postępowania w sprawie nałożenia kary za nieprzestrzeganie nakazu, na podstawie przepisu art. 83 ust. 6 RODO. Rok 2021 był kolejnym, w którym Prezes UODO sięgał po ten środek naprawczy i wszczął **3 postępowania w sprawie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazów swoich decyzji.** W jednym przypadku samo wszczęcie postępowania doprowadziło do wykonania nakazu decyzji, w związku z czym Prezes UODO zdecydował się nie nakładać kary na zobowiązanego, a poprzestać jedynie na udzieleniu mu upomnienia. W drugim przypadku postępowanie wykazało, że nakaz decyzji został wykonany przed wszczęciem postępowania, w związku z czym postępowanie należało umorzyć. Trzecie postępowanie nie zostało jeszcze zakończone.

W omawianym roku sprawozdawczym Prezes UODO nałożył jedną (1) administracyjną karę pieniężną[316] za nieprzestrzeganie nakazu decyzji po przeprowadzeniu postępowania wszczętego jeszcze w roku 2020. Kara ta została nałożona na przedsiębiorcę prowadzącego działalność z zakresu ochrony zdrowia i wynosiła **85 588 zł** (20 000 EUR). Przypadek ten charakteryzował się rażącym lekceważeniem przez zobowiązanego obowiązku nałożonego na niego nakazem decyzji administracyjnej i został szerzej opisany w Sprawozdaniu z działalności Prezesa UODO w 2020 roku. Natomiast wartym podkreślenia jest fakt, że w 2021 roku, WSA w Warszawie oddalił skargę ww. przedsiębiorcy na decyzję nakładającą karę, a przedsiębiorca nie złożył skargi kasacyjnej do NSA.

Administracyjna kara pieniężna za uchylanie się od obowiązku współpracy z organem nadzorczym i niezapewnienie dostępu do informacji niezbędnych do realizacji jego zadań

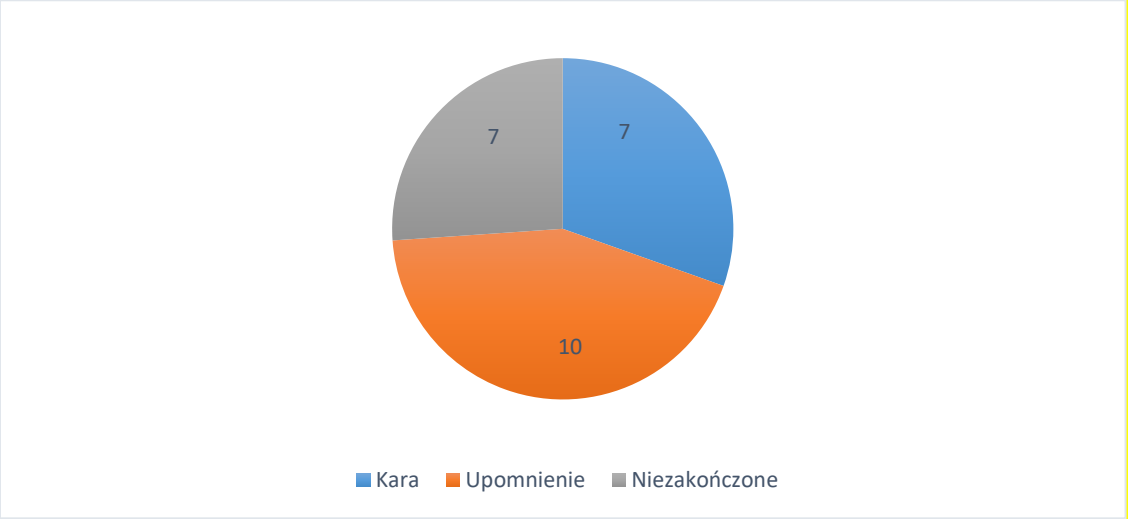
Obowiązkiem Prezesa UODO jest realizowanie zadań związanych z ochroną danych osobowych, w tym egzekwowaniem prawa do tej ochrony. W celu umożliwienia realizacji tych zadań organ nadzorczy wyposażony został w szereg uprawnień kontrolnych, uprawnień umożliwiających prowadzenie postępowań administracyjnych oraz uprawnień naprawczych. Natomiast na administratorów i podmioty przetwarzające nałożone zostały, skorelowane z uprawnieniami organu nadzorczego, określone obowiązki, w tym obowiązek współpracy z organem nadzorczym oraz obowiązek zapewnienia organowi nadzorczemu dostępu do informacji niezbędnych do realizacji jego zadań – określone w art. 31 oraz 58 ust. 1 RODO.

[316] DKE.561.11.2020.

W omawianym roku sprawozdawczym, tak jak w poprzednich latach, Prezes Urzędu Ochrony Danych zmagał się problemem związanym z brakiem współpracy stron postępowań i nieudzielaniem mu informacji niezbędnych do realizacji jego zadań. Do przedmiotowych naruszeń dochodziło zarówno w postępowaniach zainicjowanych skargami osób fizycznych, jak i w postępowaniach prowadzonych z urzędu, w związku z naruszeniami ochrony danych osobowych. Powyższe naruszenia polegały głównie na ignorowaniu pism organu nadzorczego poprzez nieudzielanie odpowiedzi lub na udzielaniu odpowiedzi niepełnych, zbywających, tj. niewystarczających do prowadzenia postępowania. Zachowania takie w sposób znaczący utrudniały pracę organu nadzorczego – wydłużając prowadzone postępowania, a czasem nawet uniemożliwiając ich zakończenie.

W związku z powyższym, w celu przymuszenia stron postępowań do podjęcia współpracy z organem nadzorczym, Prezes UODO w 2021 roku **wszczął z urzędu 24 postępowania** w sprawie nałożenia administracyjnej kary pieniężnej za powyższe naruszenia. W **10** przypadkach wszczęcie postępowania okazało się skuteczne i strony zaczęły współpracować z Prezesem Urzędu, tj. udzieliły żądanych wyjaśnień w sprawach oraz usprawiedliwiły swoje postępowanie, co spowodowało podjęcie przez Prezesa UODO decyzji o nienakładaniu kar i poprzestaniu na udzieleniu im upomnień.

Decyzjami **nakładającymi administracyjne kary pieniężne zakończyło się 7** postępowań, natomiast pozostałe postępowania nie zostały zakończone w 2021 roku.



Wykres 12: **Zestawienie sposobu zakończenia postępowań w sprawie nałożenia kary za brak współpracy w związku z nieudzieleniem Prezesowi UODO informacji niezbędnych do realizacji jego zadań w 2021 r.**

Decyzje Prezesa UODO nakładające na administratorów danych administracyjne kary pieniężne w związku ze stwierdzonym naruszeniem ochrony danych osobowych

Prezes UODO nałożył na **Cyfrowy Polsat S.A.**[317] karę pieniężną w wysokości 1136 975 zł za brak wdrożenia odpowiednich środków technicznych i organizacyjnych przy współpracy z firmą kurierską. Efektem tego były liczne naruszenia identyfikowane z dużym opóźnieniem.

Zdecydowana większość naruszeń była identyfikowana przez Cyfrowy Polsat w czasie przekraczającym 120 dni od daty zdarzenia powodującego naruszenie ochrony danych. Zgubiona korespondencja z danymi osobowymi lub dostarczenie takiej przesyłki do niewłaściwego odbiorcy – to naruszenia, które Spółka często zgłaszała do UODO. W toku postępowania okazało się, że administrator zgłaszał naruszenia, gdy tylko informację o nich otrzymał od firmy kurierskiej, z którą miał podpisaną umowę. Zdaniem UODO, to administrator powinien podjąć skuteczne działania, które po pierwsze zminimalizują skalę naruszeń, a po drugie pozwolą na szybsze identyfikowanie takich incydentów i tym samym powiadamianie o nich osób, których dotyczy dane zdarzenie oraz organu nadzorczego.

Pomimo że naruszenia związane były z nieprawidłowościami po stronie firmy kurierskiej, to właśnie ukarany administrator danych nieprawidłowo realizował nadzór nad egzekwowaniem postanowień umownych, przez co dochodziło do późnej identyfikacji naruszeń. Dopiero w toku postępowania Spółka wdrożyła mechanizmy, które pozwoliły znacznie ograniczyć przypadki wydawania korespondencji nieuprawnionej osobie. Wdrożyła też rozwiązania pozwalające śledzić przesyłki, co umożliwiło szybsze identyfikowanie i zgłaszanie utraty korespondencji z danymi osobowymi. Szybsze identyfikowanie naruszeń, a co za tym idzie zawiadamianie osób, których dane dotyczą, o naruszeniu ich danych osobowych, umożliwia tym osobom podjęcie odpowiednich działań mających na celu zminimalizowanie negatywnych skutków tych naruszeń.

Prezes UODO zdecydował się nałożyć na Spółkę karę za naruszenia przepisów rozporządzenia 2016/679. Uznał bowiem, że zastosowanie innych środków naprawczych nie byłoby proporcjonalne do stwierdzonych nieprawidłowości i nie dawałoby gwarancji, że administrator ten w przyszłości nie dopuści się podobnych zaniedbań.

Powyższa decyzja została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie, który na skutek wydanego orzeczenia uchylił przedmiotową decyzję w zaskarżonej części. W uzasadnieniu sąd wskazał, że Prezes UODO nie wyjaśnił wszystkich istotnych dla

[317] Sygn. akt DKN.5130.3114.2020.

prawidłowego rozstrzygnięcia okoliczności, co miało wpływ na wynik sprawy. Zarzucono organowi brak odniesienia się do statusu prawnego podmiotu świadczącego usługi kurierskie i błędną jego klasyfikację, jako pełniącego rolę podmiotu przetwarzającego w sprawie.

Prezes UODO nałożył na **Bank Millennium S.A.**[318] administracyjną karę pieniężną w wysokości 363 832 zł (80 EUR) za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki oraz niepowiadomienie w sposób prawidłowy o naruszeniu osób, których dane dotyczą. Podstawą powzięcia przez Prezesa UODO wiedzy o naruszeniu była skarga osób na nieprawidłowości w procesie przetwarzania ich danych osobowych przez Bank. Naruszenie polegało na zgubieniu przez firmę kurierską korespondencji z danymi osobowymi Skarżących.

Bank nieprawidłowo określił stopień ryzyka dla osób, których dane dotyczą, przyjmując jego poziom jako średni. W następstwie powyższego nie zgłosił naruszenia do organu nadzorczego. Podkreślić należy, że zgłoszeniu podlegają te z incydentów, w przypadku których istnieje prawdopodobieństwo (wyższe niż małe) szkodliwego (niekorzystnego) wpływu na prawa lub wolności osób, których dane dotyczą. Gdy to ryzyko jest wysokie, to o naruszeniu trzeba także powiadomić osoby, których dane dotyczą.

Prezes UODO podkreślił w uzasadnieniu przedmiotowej decyzji, że nie jest istotne to, czy nieuprawniony odbiorca faktycznie wszedł w posiadanie i zapoznał się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko. Administrator w swoich wyjaśnieniach podkreślał, że z posiadanych przez niego informacji wynika, że dane nie zostały wykorzystane na szkodę osób, których dane dotyczą, ale przewidział jednak, że naruszenie może wiązać się z takim ryzykiem. Świadczy o tym fakt zaproponowania dodatkowej usługi BIK Alert w ramach środków w celu zaradzenia naruszeniu. Zdaniem Banku miałoby to umożliwić podjęcie stosownej reakcji w przypadku, gdyby doszło, jak sam wskazuje, „pomimo niskiego prawdopodobieństwa, do wykorzystania danych Skarżących w systemie bankowym w sposób nieuprawniony".

Powyższa decyzja została zaskarżona przez bank do Wojewódzkiego Sądu Administracyjnego w Warszawie.

[318] Sygn. akt DKN.5131.16.2021.

Na **Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A.**[319] została nałożona administracyjna kara pieniężna w wysokości 159 176 zł za niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, a dodatkowo także za niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki, osoby, której dane dotyczyły. Informacja o naruszeniu ochrony danych osobowych została nadesłana do Prezesa UODO przez podmiot zajmujący się pośrednictwem ubezpieczeniowym.

Naruszenie polegało na wysłaniu pocztą elektroniczną, przez pracownika podmiotu zajmującego się pośrednictwem ubezpieczeniowym, do niewłaściwego odbiorcy analizy potrzeb ubezpieczeniowych oraz oferty ubezpieczenia. Podmiot, który dokonał naruszenia, występował jednocześnie w roli podmiotu przetwarzającego, działającego na polecenie towarzystw ubezpieczeniowych i to on zawiadomił te towarzystwa, jako administratorów danych, o naruszeniu.

W związku z tym incydentem kilka towarzystw ubezpieczeniowych, jako administratorzy danych, dokonało zgłoszenia naruszenia ochrony danych. Zgłoszenia takiego nie odnotowano od Sopockiego Towarzystwa Ubezpieczeń ERGO Hestia S.A.

Administrator potwierdził, że w istocie doszło do naruszenia ochrony danych osobowych, jednak na podstawie wykonanej oceny uznano, iż nie doszło do naruszenia skutkującego koniecznością zgłoszenia naruszenia oraz zawiadomienia osoby, której dane dotyczą. Przeprowadzona przez Spółkę analiza ryzyka wzbudziła wątpliwości organu nadzorczego, który uznał, że dokonana została w sposób nieprawidłowy. Błędy w przeprowadzonej ocenie polegały w szczególności na zaniżaniu wyników w poszczególnych kryteriach, braku uwzględnienia istotnych czynników dla poszczególnych kryteriów, czy uwzględnieniu czynników, które nie powinny mieć zastosowania.

W sprawie doszło do naruszenia bezpieczeństwa, ponieważ dane osobowe zostały udostępnione nieuprawnionemu odbiorcy, którego nie można uznać za „odbiorcę zaufanego", a zakres tych danych przesądza o tym, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Skutkowało to powstaniem po stronie Spółki obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia osoby, której dane dotyczą, o naruszeniu. W decyzji podkreślono, że dla powstania obowiązku zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dane dotyczą, nie jest konieczne zmaterializowanie się negatywnych konsekwencji naruszenia, wystarczająca jest w tym zakresie sama możliwość (ryzyko) wystąpienia

[319] Sygn. akt DKN.5131.3.2021.

takich konsekwencji, które w niniejszej sprawie, w ocenie organu nadzorczego, jest wysokie (art. 34 ust. 1 rozporządzenia 2016/679). Powyższa decyzja została zaskarżona przez Towarzystwo do Wojewódzkiego Sądu Administracyjnego w Warszawie. Na dzień dzisiejszy wyrok w sprawie jeszcze nie zapadł.

Brak zgłoszenia naruszenia ochrony danych osobowych bez zbędnej zwłoki był również powodem nałożenia administracyjnej kary pieniężnej w wysokości ponad 136 000 zł wobec **ENEA S.A. z siedzibą w Poznaniu**[320].

Informacja o naruszeniu ochrony danych osobowych została nadesłana do Prezesa UODO przez osobę, która stała się nieuprawnionym adresatem danych osobowych. Naruszenie to polegało na wysłaniu przez współpracownika ENEA do nieuprawnionego odbiorcy e-maila z załącznikiem zawierającym dane osobowe kilkuset osób w postaci m.in.: imion, nazwisk, adresów e-mail i numerów telefonów. E-mail był niezaszyfrowany i niezabezpieczony hasłem. W związku z powyższym Prezes UODO wszczął wobec ENEA postępowanie administracyjne. W uzasadnieniu decyzji Prezes UODO stwierdził, że powyższe naruszenie miało bezpośredni związek z brakiem wdrożenia lub nieprawidłowym wdrożeniem przez ENEA środków organizacyjnych i technicznych zapewniających bezpieczeństwo przetwarzania danych osobowych, jak np. szyfrowanie plików zawierających dane osobowe przesyłanych w wiadomości elektronicznej. W konsekwencji doszło do naruszenia poufności danych. To z kolei skutkowało powstaniem po stronie ENEA, jako administratora tych danych, obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, możliwie najszybciej, zgodnie z art. 33 ust. 1 rozporządzenia 2016/679. W zgłoszeniu tym powinny się znaleźć informacje określone w art. 33 ust. 3 rozporządzenia 2016/679. ENEA nie dokonała jednak zgłoszenia naruszenia, pomimo powzięcia informacji o zdarzeniu od nieuprawnionego odbiorcy oraz kierowanych do niej pism Prezesa UODO, wskazujących na możliwość zaistnienia w niniejszej sprawie ryzyka naruszenia praw lub wolności osób, których dotyczyło naruszenie.

Powyższa decyzja została zaskarżona przez ENEA do Wojewódzkiego Sądu Administracyjnego w Warszawie, który po rozpoznaniu sprawy wydał wyrok oddalający skargę[321]. W uzasadnieniu orzeczenia Sąd wskazał, że w sprawie nie zaszła przesłanka do wyłączenia stosowania art. 33 ust. 1 RODO – ujawnienie danych nie było mało prawdopodobne, lecz skutkowało

[320] Sygn. akt DKN.5131.7.2020.
[321] Wyrok WSA w Warszawie z dnia 21 stycznia 2022 r. sygn. akt II SA/Wa 1353/21 (nieprawomocny).

ryzykiem naruszenia praw i wolności osób fizycznych, wobec czego naruszenie podlegało obowiązkowi zgłoszenia.

Prezes UODO stwierdził naruszenie przepisów rozporządzenia 2016/679 i nałożył administracyjną karę pieniężną w wysokości 100 000 zł na **Krajową Szkołę Sądownictwa i Prokuratury (KSSiP) z siedzibą w Krakowie**[322] za niezrealizowanie ciążących na niej obowiązków administratora oraz jednocześnie umorzył postępowanie administracyjne wobec podmiotu przetwarzającego eTOP Sp. z o.o. z siedzibą w Warszawie, który przetwarzał dane osobowe w imieniu KSSiP – wobec braku stwierdzenia przez eTOP obowiązków wynikających z rozporządzenia 2016/679.

Postępowanie administracyjne wobec KSSiP zostało wszczęte na skutek zgłoszenia naruszenia ochrony danych osobowych, w związku z powiadomieniem przez Komendę Główną Policji o pojawieniu się w Internecie danych osobowych związanych z domeną kssip.gov.pl. Zgłoszony incydent polegał na uzyskaniu przez nieznane osoby nieupoważnionego dostępu do kopii bazy danych witryny szkoleniowej KSSiP, powstałej w trakcie testowej migracji do nowej platformy szkoleniowej. Naruszenie dotyczyło danych osobowych ponad 50 tys. osób, użytkowników podlegających szkoleniu ustawicznemu, których dane osobowe zgromadzono na platformie szkoleniowej KSSiP. Osoby te piastowały stanowiska m.in. sędziów, asesorów sądowych, prokuratorów i asesorów prokuratury oraz referendarzy sądowych.

Powodem nałożenia na KSSiP kary pieniężnej było niezastosowanie odpowiednich środków technicznych i organizacyjnych, które pozwoliłyby zapewnić poufność usług przetwarzania oraz brak przetestowania i oceny skuteczności środków technicznych i organizacyjnych, a tym samym niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania. W uzasadnieniu decyzji Prezes UODO stwierdził, że KSSiP nie przetestowała i nie dokonała oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej Krajowej Szkoły Sądownictwa i Prokuratury. Ponadto KSSiP powierzył przetwarzanie danych osobowych podmiotowi przetwarzającemu bez umownego zobowiązania go do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie KSSiP.

[322] Sygn. akt DKN.5130.2024.2020.

W uzasadnieniu decyzji Prezes UODO wskazał, że w zasobach informatycznych KSSiP znajdowała się kopia bazy danych, której istnienie i bezpieczeństwo, po wykonaniu czynności migracyjnych, w żaden sposób nie zostało zweryfikowane przez KSSiP, co stanowiło o naruszeniu obowiązków określonych w RODO. KSSiP, w związku ze zmianami w procesie przetwarzania, nie podjęła też wystarczających działań mających na celu zweryfikowanie bezpieczeństwa środowiska przetwarzania przed rozpoczęciem działań migracyjnych, jak i po ich zakończeniu. Weryfikacji tej KSSiP podjęła się dopiero w dniu stwierdzenia naruszenia.

Ponadto w decyzji Prezes UODO wskazał, że doszło do naruszenia przepisów rozporządzenia 2016/679 regulujących kwestię powierzenia przetwarzania danych osobowych, tj. art. 28 ust. 1 oraz art. 28 ust. 3, poprzez brak dookreślenia w treści umowy powierzenia zakresu powierzanych danych, tj. kategorii osób, rodzaju danych osobowych przez wskazanie ich kategorii. Ponadto ukarany podmiot nie zawarł w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, co stanowiło o naruszeniu art. 28 ust. 3 lit. a ww. rozporządzenia.

Powyższa decyzja została zaskarżona przez administratora do Wojewódzkiego Sądu Administracyjnego w Warszawie, który po rozpoznaniu sprawy wydał wyrok oddalający skargę[323]. Sąd w uzasadnieniu wyroku podzielił stanowisko Prezesa UODO, iż zawarta przez KSSiP umowa powierzenia przetwarzania danych nie wypełniała dyspozycji przepisów rozporządzenia 2016/679 w tym zakresie, w szczególności kryteriów zawartych w art. 28 ust. 3 tego aktu prawnego. Ponadto Sąd przyznał, że KSSiP – jako administrator danych osobowych – w sposób niewystarczający dokonywała oceny skuteczności środków technicznych, by zapewnić bezpieczeństwo przetwarzania tych danych i w ten sposób naruszyła przepisy rozporządzenia 2016/679.

Administracyjna kara pieniężna w wysokości 100 000 zł została nałożona na **P4 Sp. z o.o. z siedzibą w Warszawie**[324] za naruszenie przepisów Prawa telekomunikacyjnego oraz rozporządzenia Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. 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

[323] Wyrok WSA w Warszawie z dnia 26 stycznia 2022 r. sygn. akt II SA/Wa 1384/21 (nieprawomocny).
[324] Sygn. akt DKN.5131.10.2020.

elektronicznej[325], polegające na niezawiadomieniu organu nadzorczego w terminie 24 godzin o wykryciu naruszenia danych osobowych. W świetle przepisów Prawa telekomunikacyjnego, przedsiębiorca telekomunikacyjny[326] – administrator danych – nie tylko musi chronić dane osobowe swoich klientów, ale także w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych zobowiązany jest w szczególności powiadomić o tym organ do spraw ochrony danych osobowych w terminie 24 godzin, a także abonenta lub użytkownika końcowego, którego dane zostały naruszone[327].

W związku z powyższym Prezes UODO wszczął postępowanie administracyjne, w toku którego ustalił, że dokonanie zawiadomień o naruszeniu danych osobowych po upływie 24 godzin związane było z nieumyślnym błędem pracowników kancelarii odpowiedzialnych za wysyłkę korespondencji. Błąd ten polegał m.in. na niewpisaniu korespondencji do książki nadawczej, czego efektem był jej zwrot przez operatora pocztowego. W uzasadnieniu decyzji Prezes UODO wskazał, że powtarzające się zgłoszenia naruszenia danych osobowych z przekroczeniem terminu 24 godzin świadczyły o braku zastosowania odpowiednich środków w celu wyeliminowania podobnych zdarzeń w przyszłości. Ponadto zaznaczył, że naruszenie terminu zgłoszenia incydentów bezpieczeństwa ochrony danych nie miało charakteru jednorazowego. Prezes UODO niejednokrotnie też kierował do P4 pisma, w których informował o sposobach zgłaszania naruszeń danych osobowych.

Powyższa decyzja została zaskarżona przez P4 do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Powodem nałożenia na **Politechnikę Warszawską**[328] kary pieniężnej w wysokości 45 000 zł było niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić

---

[325] Art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 – „*Dostawca powiadamia właściwy organ krajowy o przypadku naruszenia danych osobowych nie później niż 24 godziny po wykryciu naruszenia danych osobowych, jeśli jest to wykonalne”.*

[326] Art. 174a ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne – *„dostawca publicznie dostępnych usług telekomunikacyjnych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu danych osobowych w terminie i na zasadach określonych w rozporządzeniu Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. 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 (Dz. Urz. UE L 173 z 26.06.2013, str. 2)”.*

[327] Art. 174a ust. 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne – „*W przypadku, gdy naruszenie danych osobowych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, dostawca publicznie dostępnych usług telekomunikacyjnych niezwłocznie zawiadamia o takim naruszeniu również abonenta lub użytkownika końcowego na zasadach określonych w rozporządzeniu 611/2013, z zastrzeżeniem ust. 5”.*

[328] DKN.5130.2559.2020.

zdolność do ciągłego zapewnienia poufności usług przetwarzania oraz brak regularnego testowania, mierzenia i oceniania skuteczności zastosowanych środków bezpieczeństwa. Politechnika nie uwzględniła również ryzyka związanego z przetwarzaniem danych w aplikacji.

Postępowanie administracyjne wobec administratora zostało wszczęte na skutek zgłoszenia naruszenia ochrony danych osobowych studentów i wykładowców. Jak wskazano w decyzji, osoba nieuprawniona pobrała z zasobów uczelnianej sieci informatycznej bazy danych, zawierające dane osobowe studentów i wykładowców – w sumie ponad 5 tys. osób. Ustalono, że jednostka organizacyjna Politechniki wykorzystywała aplikację opracowaną przez pracowników uczelni, która służyła do zapisywania się na przedmioty oraz pozwalała mieć wgląd w historię nauczania, ocen czy rozliczania opłat. Aplikacja ta była modyfikowana w zależności od potrzeb administratora. Na początku stycznia 2020 roku nieuprawniona osoba wykorzystała funkcjonalność umieszczania plików w aplikacji, dysponując danymi uwierzytelniającymi, a następnie dokonała nieautoryzowanego pobrania danych osobowych wymienionych wyżej osób.

Prezes UODO w uzasadnieniu decyzji podkreślił, że administrator odpowiedzialny jest za wdrożenie odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych osobowych, zgodnie z art. 32 ust. 1 rozporządzenia 2016/679[329]. Politechnika nie przedstawiła dowodów na to, że dokonywała formalnej oceny poziomu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, uwzględniając przy tym kryteria wskazane w art. 32 ust. 1 RODO oraz nie uzasadniła, że stosowane środki techniczne i organizacyjne były odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Politechnika skupiła się jedynie na zabezpieczeniu przed zagrożeniami infrastruktury informatycznej. Nie wzięła jednak pod uwagę zagrożeń związanych z funkcjonowaniem stworzonej przez pracowników aplikacji. Zdaniem Prezesa UODO, zastosowanie środków technicznych bez dokonania uprzedniej analizy ryzyka dla procesu przetwarzania danych osobowych nie może dawać gwarancji, że zastosowane środki będą skuteczne i adekwatne. W uzasadnieniu decyzji Prezes UODO wskazał także, że Politechnika nie dokonywała regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania.

[329] Art. 32 ust. 1 rozporządzenia 2016/679 – administrator jest zobowiązany do zastosowania środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

Na **Śląski Uniwersytet Medyczny**[330] nałożona została administracyjna kara pieniężna w wysokości 25 000 zł za brak zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu bez zbędnej zwłoki oraz zawiadomienia bez zbędnej zwłoki osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. Na Uniwersytecie doszło do naruszenia ochrony danych, o którym administrator powinien powiadomić nie tylko organ nadzoru, ale i osoby, których dotyczył ten incydent. Prezes UODO oprócz nałożonej kary, nakazał również uczelni powiadomienie osób, których dotyczyło naruszenie.

Prezes UODO został poinformowany o naruszeniu przez osoby, których dotyczył incydent – tj. większość uczestniczących w egzaminach studentów. Naruszenie polegało na udostępnieniu na platformie e-learningowej nagrań obrazujących przebieg egzaminów praktycznych z pediatrii, podczas których, w trakcie przystępowania do egzaminu, większość uczestniczących w nim studentów została wylegitymowana legitymacją studencką lub dowodem osobistym. Nagrania z przeprowadzonych egzaminów były dostępne nie tylko dla osób egzaminowanych, ale i dla innych osób mających dostęp do systemu. Wykorzystując bezpośredni link do systemu obsługującego wideokonferencje, bez konieczności logowania na platformie, każda osoba postronna mogła mieć dostęp do nagrań z egzaminów i danych przedstawionych podczas identyfikacji egzaminowanych studentów.

Przedmiotowy incydent nie został zgłoszony Prezesowi UODO, gdyż – jak uznał administrator danych – brak było ryzyka naruszenia praw lub wolności osób, których dane dotyczyły. Uczelnia nie uczyniła tego pomimo otrzymania pisma od Prezesa UODO, wskazującego sytuacje, w których należy dokonać zgłoszenia naruszenia ochrony danych organowi nadzorczemu oraz sytuacje, w których należy powiadomić o naruszeniu osoby dotknięte tym zdarzeniem.

Prezes UODO wszczął postępowanie administracyjne wobec administratora. Ustalono w nim, że do naruszenia doszło, ponieważ jeden z pracowników po zakończonym egzaminie na platformie e-learningowej nie zamknął dostępu do wirtualnego pokoju, w którym odbywał się sprawdzian. Dzięki temu można było pobrać nagrania z przebiegu egzaminu. W związku z tym, że studenci przed przystąpieniem do egzaminu byli identyfikowani na podstawie dowodów osobistych lub legitymacji studenckich, na nagraniach zarejestrowany był szereg ich danych. W zależności od tego, jakim wzorem dowodu osobistego lub legitymacji studenckiej studenci się posługiwali, inny był zakres danych w przypadku poszczególnych osób dotkniętych naruszeniem. W części przypadków były

[330] Sygn. akt DKN.5131.6.2020.

to jednak m.in. wizerunek, nr PESEL, nr dokumentu tożsamości czy albumu, imię i nazwisko oraz adres zamieszkania. Ponadto w wyniku naruszenia osoby nieuprawnione mogły zapoznać się z innymi danymi, jak: rok studiów, grupa, kierunek studiów, informacje o zdawanym przedmiocie czy udzielonych odpowiedziach podczas egzaminu.

W wydanej decyzji Prezes UODO uznał, że Uniwersytet dopuścił się naruszenia zasad ochrony danych osobowych poprzez niewłaściwą ocenę zaistniałego ryzyka dla praw lub wolności dotkniętych nim osób. Nie wdrożył też odpowiednich środków technicznych i organizacyjnych oraz nie dopełnił obowiązków związanych z powiadomieniem o tym fakcie zarówno organu nadzoru, jak i osób, których dotyczyło naruszenie. W konsekwencji doprowadziło to do naruszenia poufności danych osób przystępujących do egzaminów, tj. do naruszenia bezpieczeństwa prowadzącego do przypadkowego, nieuprawnionego ujawnienia danych tych osób.

Prezes Urzędu wymierzając karę za niezgłoszenie naruszenia organowi nadzoru i niepowiadomienie o nim osób, których dotyczył ten incydent, wziął pod uwagę m.in. czas trwania naruszenia, umyślne działanie administratora, który podjął decyzję, by nie zawiadamiać o naruszeniu i nie informować o nim studentów, niezadowalającą współpracę administratora z organem (nie zgłosił naruszenia pomimo wysyłanych pism i wszczętego postępowania).

Powyższa decyzja została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie, który po rozpoznaniu sprawy wydał wyrok oddalający skargę[331]. Sąd nie przyjął argumentacji Skarżącego, że utrwalone na nagraniach dane osobowe były nieczytelne i uznał, że Uniwersytet bezpodstawnie ocenił ryzyko naruszenia praw lub wolności osób jako niskie. W uzasadnieniu orzeczenia Sąd orzekł, że Uniwersytet dopuścił się naruszenia art. 33 ust. 1 i art. 34 ust. 1 rozporządzenia 2016/679. Uniwersytet na powyższe orzeczenie Sądu złożył skargę kasacyjną.

Fundacja Promocji Mediacji i Edukacji Prawnej Lex Nostra z siedzibą w Warszawie[332] została ukarana administracyjną karą pieniężną w wysokości 13 000 zł za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki oraz niezawiadomienie o incydencie osób, których dane dotyczą. Dodatkowo Prezes UODO wyznaczył Fundacji termin 3 dni na zawiadomienie osób, których dane dotyczą, o zaistniałym naruszeniu.

Podstawą powzięcia przez Prezesa UODO informacji o naruszeniu ochrony danych osobowych było nadesłane zawiadomienie o podejrzeniu naruszenia zasad przestrzegania przepisów o ochronie

[331] Wyrok WSA w Warszawie z dnia 22 września 2021 r. sygn. akt II SA/Wa 791/21.
[332] Sygn. akt DKN.5131.11.2020.

danych osobowych przez Fundację, polegające na utracie danych osobowych osób na skutek kradzieży teczek zawierających dane osobowe beneficjentów. Naruszenie dotyczyło 96 osób, ale Fundacja nie była w stanie dokładnie wskazać kategorii danych osobowych zawartych w utraconej dokumentacji. Mogły one obejmować m.in. imię, nazwisko, adres do korespondencji, numer telefonu, a w przypadku kilku osób prawdopodobnie obejmowały także numer PESEL. Przedmiotowy incydent nie został zgłoszony Prezesowi UODO, gdyż – jak uznał administrator danych – brak było ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

W związku z powyższym organ nadzorczy wszczął wobec Fundacji postępowanie administracyjne. W uzasadnieniu decyzji Prezes UODO stwierdził, że naruszenie polegające na kradzieży teczek zawierających dane osobowe beneficjentów Fundacji, z uwagi na zakres danych znajdujących się w utraconej dokumentacji, ma znaczną wagę i poważny charakter. Może bowiem doprowadzić do szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone, a prawdopodobieństwo ich wystąpienia jest wysokie. Wysokie ryzyko wystąpienia negatywnych konsekwencji dla osób, których dane zostały przez Fundację utracone, waga naruszenia, okoliczności zdarzenia, a w szczególności to, że nie było ono przypadkowe, pozwalały na stwierdzenie, że było to celowe działanie osoby lub osób trzecich działających w sposób przestępczy. W konsekwencji Prezes UODO uznał, że wystąpiło naruszenie bezpieczeństwa prowadzące do utracenia oraz nieuprawnionego dostępu do danych osobowych przetwarzanych przez Fundację.

Ponadto Prezes UODO wskazał, iż skoro Fundacja nie posiadała kopii skradzionych dokumentów, ani nie była w stanie ich odtworzyć lub nie przetwarzała ich przy użyciu systemu informatycznego, i tym samym nie była w stanie zidentyfikować osób, których dane dotyczą, to stosownie do art. 34 ust. 3 lit. c rozporządzenia 2016/679, powinna dokonać zawiadomienia tych osób poprzez wydanie publicznego komunikatu lub zastosowanie podobnego środka, aby w równie skuteczny sposób poinformować te osoby o naruszeniu.

Na powyższą decyzję została wniesiona przez Fundację skarga do Wojewódzkiego Sądu Administracyjnego w Warszawie.

W analizowanym 2021 roku nałożona została administracyjna kara pieniężna w wysokości 10 000 zł na **Prezesa Sądu Rejonowego w Zgierzu**[333]. Decyzja ta związana była ze zgłoszeniem zagubienia nieszyfrowanej przenośnej pamięci typu pendrive przez kuratora sądowego. Na nośniku

[333] Sygn. akt DKN.5131.22.2021.

przechowywano dane 400 osób, podlegających nadzorowi kuratorskiemu i objętych wywiadem środowiskowym.

Administrator wdrożył system ochrony danych osobowych w postaci zasad przetwarzania danych osobowych, w którym – zgodnie z obowiązującymi u administratora dokumentami – obowiązek zabezpieczenia nośników spoczywał na użytkownikach. Zdaniem Prezesa UODO, takie podejście jest niewłaściwe, gdyż to administrator danych, a nie pracownik lub osoba wykonująca zadania służbowe, jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z wymaganiami rozporządzenia 2016/679.

Podstawą wdrożenia odpowiednich środków organizacyjnych i technicznych powinna być prawidłowo i rzetelnie uprzednio przeprowadzona analiza ryzyka, w wyniku której powinno nastąpić ustalenie środków mających zaradzić poszczególnym zagrożeniom. Przedstawiona przez administratora analiza ryzyka wskazywała nieadekwatne następstwa naruszenia ochrony danych osobowych oraz przyjmowała niewłaściwe środki bezpieczeństwa z całkowitym pominięciem środków technicznych. Ponadto Prezes UODO stwierdził, iż rozwiązanie przyjęte w tym zakresie przez administratora danych (tylko szkolenia pracowników) podważało skuteczność wdrożonego systemu ochrony danych osobowych, albowiem efektem przeprowadzonej analizy ryzyka winien być odpowiedni dobór środków zarówno technicznych, jak i organizacyjnych. Natomiast pozostawienie doboru i wdrożenia środków zabezpieczających osobie, która otrzymała do użytku niezabezpieczoną pamięć przenośną, oznacza, iż Prezes Sądu pozbawił siebie – jako administratora danych – podstawowych i kluczowych informacji, niezbędnych w kontekście realizacji obowiązków wynikających z art. 32 ust. 2 rozporządzenia 2016/679. Przedstawiona przez administratora dokumentacja ochrony danych nie zawierała uregulowań zapewniających regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych, co również przyczyniło się do wystąpienia naruszenia ochrony danych osobowych. Administrator zobowiązany jest do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania.

Powyższa decyzja została zaskarżona przez administratora do Wojewódzkiego Sądu Administracyjnego w Warszawie, który wydał wyrok oddalający skargę[334]. Sąd w uzasadnieniu

[334] Wyrok WSA w Warszawie z dnia 15 lutego 2022 r. sygn. akt II SA/Wa 3309/21 (nieprawomocny).

wyroku przychylił się do stanowiska Prezesa UODO i podkreślił, że ograniczenie wdrażania zabezpieczeń przez administratora danych osobowych wyłącznie do szkoleń pracowników z pominięciem zabezpieczeń technicznych, z całą pewnością nie może być uznane za wdrożenie odpowiednich środków technicznych czy organizacyjnych w kontekście art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 rozporządzenia 2016/679 – w szczególności w celu zapewnienia zdolności do ciągłego zapewnienia poufności danych. Ponadto Sąd wskazał, że pracownik nie może zastępować administratora danych w realizacji jego zadań wynikających z tych przepisów.

10. 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 rozwiązania przewidzianego w art. 36 RODO. W 2021 roku do Urzędu wpłynęły **trzy (3) wnioski o przeprowadzenie uprzednich konsultacji**. W poprzednim roku sprawozdawczym wpłynęły także 3 takie wnioski, w 2019 roku – 5, a w 2018 roku – 2.

W odniesieniu do poprzednich okresów sprawozdawczych można zaobserwować, że administratorzy coraz lepiej rozumieją cel instytucji uprzednich konsultacji i już nie zwracali się o nie do UODO w sytuacjach innych niż te, o których mowa w art. 36 ust. 1 RODO (przykładowo – poszukując odpowiedzi na pytanie, czy należy udostępnić określone dane osobowe na podstawie prawa dostępu do informacji publicznej albo rozważając, kogo należy uznać za administratora w określonym procesie przetwarzania danych). Niemniej żaden z trzech (3) złożonych w 2021 roku

wniosków nie mógł zainicjować postępowania w sprawie uprzednich konsultacji, gdyż dwa (2) wnioski nie spełniały wymogów określonych w art. 36 ust. 3 RODO, a jeden (1) wniosek nie mógł być przedmiotem uprzednich konsultacji, ponieważ administrator nie legitymował się podstawą prawną do prowadzenia operacji przetwarzania danych, określonych w art. 36 ust. 1 RODO. Organ nadzorczy, uzasadniając powody nieudzielenia konsultacji, wskazywał na konkretne braki, jakimi były obarczone wnioski o uprzednie konsultacje. Żeby je przybliżyć i wyjaśnić, poniżej zostaną one przykładowo omówione.

W jednym z wniosków administrator nie legitymował się podstawą prawną do prowadzenia operacji przetwarzania danych. Organ nadzorczy podkreślił, że administrator planujący określone operacje przetwarzania, przed dokonaniem oceny skutków dla ochrony danych, powinien w pierwszej kolejności przeanalizować, czy istnieje podstawa prawna uprawniająca go do realizacji takiego przetwarzania. Zgodnie bowiem z przepisami RODO, administrator może przetwarzać (w tym pozyskiwać) dane osobowe wyłącznie wtedy, gdy istnieje do tego podstawa prawna.

Z kolei brak spełnienia we wnioskach o uprzednie konsultacje wymogów określonych w art. 36 ust. 3 RODO dotyczył głównie nieprawidłowo przeprowadzonej przez administratora oceny skutków dla ochrony danych:

1) administrator nie wskazał, w jaki sposób dokonał ważenia prawnie uzasadnionego interesu administratora lub strony trzeciej z jednej strony i interesów, podstawowych praw oraz wolności podmiotu danych z drugiej strony (test równowagi), w sytuacji oparcia przetwarzania danych na przesłance z art. 6 ust. 1 lit. f RODO;
2) administrator nie uwzględnił opinii osób, których dane dotyczą, lub ich przedstawicieli, w sytuacji planowanego przetwarzania danych przypadkowych osób, uzasadniając to tym, że w takiej sytuacji zasięgnięcie opinii było niemożliwe;
3) z przedstawionej oceny skutków dla ochrony danych trudno było wywnioskować, w odniesieniu do jakich kategorii danych administrator odnosi poszczególne przesłanki przetwarzania danych, z uwzględnieniem istotnego rozróżnienia na przesłanki dotyczące danych zwykłych i szczególnych kategorii danych. Z oceny skutków nie wynikało też, czy wnioskodawca uwzględnił wszystkie kategorie osób, do których może być adresowana usługa.

W odniesieniu do pkt 1) organ nadzorczy wyjaśnił, że oparcie przetwarzania danych osobowych na przepisie art. 6 ust. 1 lit. f RODO wymaga kumulatywnego spełnienia kilku przesłanek. Po pierwsze, musi występować prawnie uzasadniony interes, który jest realizowany przez administratora

lub przez stronę trzecią. Po drugie, niezbędna jest weryfikacja, czy przetwarzanie danych osobowych było niezbędne dla realizacji celu wynikającego z prawnie uzasadnionych interesów. Następnie należy ocenić, czy nie była spełniona przesłanka o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. W przypadku spełnienia tego warunku nie będzie można powołać się na przepis art. 6 ust. 1 lit. f RODO jako uzasadnienie dla przetwarzania danych osobowych. Stosowanie tej negatywnej przesłanki polega w istocie na wyważeniu dwóch dóbr chronionych prawem, tj. prawnie uzasadnionego interesu administratora lub strony trzeciej z jednej strony i interesów, podstawowych praw oraz wolności podmiotu danych z drugiej.

Co do braku polegającego na nieuwzględnieniu przez administratora opinii osób, których dane dotyczą lub ich przedstawicieli (pkt 2), organ nadzorczy podkreślił, że wyrazem nacisku, jaki RODO kładzie na ochronę praw i wolności osób, których dane dotyczą, było wprowadzenie w art. 35 ust. 9 RODO swoistych konsultacji administratora w sprawie zamierzonego przetwarzania z osobami, których dane dotyczą lub ich przedstawicielami. UODO, przywołując stanowiska doktryny w tym zakresie, wskazał, że stosownymi przypadkami, uzasadniającymi zasięgnięcie opinii podmiotów danych, byłyby więc przypadki planowania takich operacji przetwarzania, które mogłyby znacząco wpłynąć na sytuację lub interesy osób, których dane dotyczą[335]. A zatem chodzi o sytuacje, gdy opinie te mogą mieć istotny wpływ na ocenę skutków dla ochrony danych. W wytycznych dotyczących oceny skutków wskazano ponadto, że jeżeli ostateczna decyzja administratora danych różni się od opinii osób, których dane dotyczą, należy udokumentować powody podjęcia bądź niepodjęcia decyzji[336]. „W praktyce istnieje możliwość zasięgnięcia opinii osób, których potencjalnie dotyczyć będą planowane procesy przetwarzania (np. poprzez badania ankietowe skierowane do osób zainteresowanych) (…). Natomiast w piśmiennictwie wskazuje się także na możliwość uznania, że przedstawicielami takich osób, z którymi mogą zostać przeprowadzone konsultacje, są np. stowarzyszenia konsumentów. (…) Wnioski płynące z konsultacji administrator powinien rozważyć, dokonując oceny skutków dla ochrony danych.”[337]. „Administrator może zastosować formę dowolną,

[335] Edyta Bielak-Jomaa (red.), Dominik Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz do art. 35 RODO w systemie prawniczym LEX.
[336] Wytyczne dot. oceny skutków, str. 18.
[337] Paweł 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 do art. 35 RODO w systemie prawniczym LEX.

odpowiadającą powszechnie przyjętej metodzie kontaktu z klientami, bądź prowadzenia konsultacji w danej branży. Realizując obowiązek określony w art. 35 ust. 9, administrator może kontaktować się bezpośrednio z klientami lub też ograniczyć się do rozmów czy ustaleń np. ze stowarzyszeniami konsumentów czy klientów."[338]

Inny przykład braku, jakim był obarczony wniosek o uprzednie konsultacje (pkt 3), również dotyczył przedłożonej przez administratora oceny skutków dla ochrony danych, z której trudno było wywnioskować, w odniesieniu do jakich kategorii danych administrator odnosi poszczególne przesłanki przetwarzania danych, z uwzględnieniem istotnego rozróżnienia na przesłanki dotyczące danych zwykłych i szczególnych kategorii danych. Z przedstawionej oceny nie wynikało też, czy wnioskodawca uwzględnił wszystkie kategorie osób, do których może być adresowana usługa, ani w jaki sposób będzie weryfikowany wiek osób. Organ nadzorczy podkreślił, że RODO przewiduje szczególne rozwiązania związane z zabezpieczeniem praw dzieci. Należy do nich to przewidziane w art. 8 ust. 1 RODO. Zgodnie z tym przepisem, jeżeli zastosowanie ma zgoda na przetwarzanie danych osobowych, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli natomiast dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

11. Kodeksy postępowania

Na mocy art. 40 RODO wprowadzony został instrument prawny w postaci kodeksu postępowania, którego celem jest doprecyzowanie i pomoc we właściwym stosowaniu przepisów RODO w danej branży. Organ nadzorczy nieustannie zachęca do podjęcia prac w tym zakresie. Kodeksy postępowania mogą być sporządzone, a następnie przedkładane Prezesowi UODO do zatwierdzenia, przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Po otrzymaniu wniosku o zatwierdzenie kodeksu postępowania, organ nadzorczy przeprowadza postępowanie administracyjne w tym zakresie. W jego toku wydaje opinię o zgodności przedłożonego projektu z przepisami o ochronie danych osobowych, a następnie

[338] Edyta Bielak-Jomaa (red.), Dominik Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz do art. 35 RODO w systemie prawniczym LEX.

zatwierdza kodeks postępowania w formie decyzji administracyjnej, o ile uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO.

W 2021 roku do Prezesa UODO wpłynął jeden (1) wniosek o zatwierdzenie kodeksu postępowania[339]. Projekt kodeksu został przedłożony przez Sieć Badawczą Łukasiewicz – PORT Polski Ośrodek Rozwoju Technologii. Dotyczył on przetwarzania danych osobowych dla celów badań naukowych przez biobanki w Polsce. Pod koniec 2021 roku organ nadzorczy wezwał wnioskodawcę do uzupełnienia braków wniosku.

W 2021 roku organ nadzorczy prowadził również postępowania w sprawnie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone wcześniej. Były to:

- dwa kodeksy w służbie zdrowia przygotowane przez Federację Związków Pracodawców Ochrony Zdrowia „*Porozumienie Zielonogórskie" – „Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych*"[340] oraz Polską Federację Szpitali – „*Kodeks postępowania dla sektora ochrony zdrowia*"[341]. Organ nadzorczy pozytywnie zaopiniował obydwa projekty. W 2021 roku odbyło się spotkanie z wnioskodawcami w tej sprawie. Przed zatwierdzeniem tych kodeksów postępowania, wnioskodawcy muszą bowiem jeszcze przedstawić odpowiednie mechanizmy ich monitorowania dla podmiotów publicznych. Podmioty monitorujące muszą natomiast uzyskać akredytację organu nadzorczego;
- „*Kodeks postępowania dla centrów handlowych*"[342]. Na prośbę organu nadzorczego, wnioskodawca – Polska Rada Centrów Handlowych – przedstawił poprawioną wersję kodeksu;
- „*RODO dla bibliotek. Kodeks postępowania wspierający we właściwym stosowaniu RODO*"[343]. Wnioskodawca – Stowarzyszenie Bibliotekarzy Polskich – nie uzupełnił braków wniosku. Pod koniec 2021 roku poinformował również, że zaprzestaje dalszych prac nad kodeksem postępowania. Wniosek o zatwierdzenie ww. kodeksu został pozostawiony przez Prezesa UODO bez rozpoznania, zaś postępowanie w tej sprawie zostało zakończone;
- „*Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez spółdzielnie mieszkaniowe zrzeszone w Związku Rewizyjnym Spółdzielni Mieszkaniowych RP*"[344]. W 2021

[339] DOL.4421.1.2021.
[340] ZAS.070.2.2018.
[341] ZAS.070.4.2018.
[342] DOL.4421.3.2020.
[343] DOL.4421.4.2020.
[344] ZAS.070.5.2019.

roku odbyło się spotkanie przedstawicieli organu nadzorczego i Związku Rewizyjnego Spółdzielni Mieszkaniowych RP będącego wnioskodawcą, podczas którego zostały omówione najważniejsze kwestie dotyczące projektu kodeksu. Pod koniec 2021 roku organ nadzorczy skierował pismo do wnioskodawcy zawierające ocenę zgodności przedłożonego projektu kodeksu postępowania z przepisami o ochronie danych osobowych;

- „*Kodeks postępowania Krajowej Izby Doradców Podatkowych w zakresie ochrony danych osobowych*”[345]. Wnioskodawca – Krajowa Izba Doradców Podatkowych – przedstawił poprawioną wersję kodeksu, który był następnie przedmiotem kompleksowej oceny merytorycznej pod kątem jego zgodności z przepisami o ochronie danych osobowych;
- „*Kodeks postępowania dotyczący przetwarzania danych osobowych przez prywatne agencje badawcze*”[346]. Wnioskodawca, tj. Organizacja Firm Badania Opinii i Rynku, przestawił poprawioną wersję kodeksu, który był następnie przedmiotem kompleksowej oceny merytorycznej pod kątem jego zgodności z przepisami o ochronie danych osobowych;
- „*Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe*”[347]. W 2021 roku odbyły się kolejne spotkania przedstawicieli organu nadzorczego i wnioskodawcy, czyli Związku Banków Polskich. Wobec wycofania wniosku o zatwierdzenie kodeksu postępowania, organ nadzorczy wydał 31 sierpnia 2021 roku decyzję administracyjną umarzającą postępowanie w tej sprawie.

W 2021 roku Prezes UODO prowadził również korespondencję z Ministerstwem Finansów w sprawie wniosku organu nadzorczego – skierowanego na podstawie art. 52 ust. 2 ustawy o ochronie danych osobowych – o podjęcie prac legislacyjnych mających na celu zmianę art. 105 Prawa bankowego, poprzez rozszerzenie katalogu podmiotów, którym udzielane są informacje będące tajemnicą bankową, o akredytowany przez Prezesa UODO podmiot monitorujący kodeks postępowania, o którym mowa w art. 41 RODO[348]. Działania te były prowadzone w związku z rozpatrywaniem wniosku o zatwierdzenie ww. kodeksu postępowania.

W 2021 roku organ właściwy w sprawie ochrony danych osobowych pozostawał również w kontakcie z innymi podmiotami przygotowującymi projekty kodeksów postępowania, które nie złożyły jeszcze wniosków o ich zatwierdzenie.

[345] DOL.4421.1.2020.
[346] DOL.4421.2.2020.
[347] DOL.4421.2.2020.
[348] ZAS.023.1.2019.

Pracownicy Urzędu odbyli **10 spotkań** z przedstawicielami twórców kodeksów postępowania (już złożonych do zatwierdzenia i dopiero przygotowywanych). Ze względu na sytuację pandemiczną spotkania odbyły się głównie w formule online. W czasie kilkugodzinnych spotkań omawiano poszczególne przepisy kodeksów budzące wątpliwości lub dyskutowano o zagadnieniach związanych z ochroną danych w branży objętej kodeksem. Spotkania te pozwalały wyjaśnić poszczególne problemy, które w projektach kodeksów zauważył organ nadzorczy. Były one także okazją do rozmowy m.in. o kwestii monitorowania.

Projektodawcy zgłaszali też różnego rodzaju wątpliwości dotyczące tworzenia projektów kodeksów postępowania. Organ nadzorczy udzielał tym podmiotom stosownych wyjaśnień. Wśród nich znaleźli się:

- Związek Pracodawców Innowacyjnych Firm Farmaceutycznych INFARMA, przygotowujący projekt kodeksu branżowego w zakresie ochrony danych osobowych[349];
- Izba Gospodarcza Wodociągi Polskie, przygotowująca projekt kodeksu postępowania ochrony danych osobowych dla branży wodociągowo-kanalizacyjnej[350];
- Pani Anna Pielok i Pan Piotr Sojka, przygotowujący projekt kodeksu postępowania dla jednostek oświatowych, mający na celu doprecyzowanie stosowania RODO[351];
- Krajowa Rada Regionalnych Izb Obrachunkowych, przygotowująca projekt kodeksu postępowania dla Regionalnych Izb Obrachunkowych[352];
- SO IN LAW Sp. z o.o., przygotowująca projekt kodeksu postępowania dla fotografów[353].

Tak szeroka współpraca z twórcami kodeksów wynikała z faktu, że wnioski o ich zatwierdzenie zostały złożone przed opublikowaniem wytycznych Europejskiej Rady Ochrony Danych nr 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących, zgodnie z rozporządzeniem 2016/679[354]. Zgodnie z pkt 58 wytycznych, „proces oceny nie powinien służyć jako okazja do dalszych konsultacji z właściwym organem nadzorczym w sprawie przepisów przedłożonego kodeksu", dlatego w stosunku do projektów złożonych po opublikowaniu wytycznych (4.06.2019 r.) konsultacje nie były już prowadzone w tak szerokim zakresie, jak poprzednio. Natomiast nowe

[349] DOL.4420.1.2021.
[350] ZAS.071.15.2018.
[351] DOL.4420.1.2020.
[352] DOL.4420.2.2020.
[353] DOL.4420.3.2020.
[354] Wytyczne nr 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, zob. https://uodo.gov.pl/pl/414/1336.

inicjatywy kodeksowe mogą uzyskiwać w toku ewentualnych spotkań informacje o przebiegu procedury, wyjaśnienia dotyczące przepisów ww. wytycznych czy też mających do nich zastosowanie przepisów prawa.

12. Akredytacja podmiotów monitorujących kodeksy postępowania

Za monitorowanie przestrzegania kodeksu postępowania odpowiada niezależny podmiot monitorujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu. Podmiot ten musi zostać akredytowany w tym celu przez organ nadzorczy jeszcze przed zatwierdzeniem kodeksu postępowania.

Jeszcze w 2020 roku Prezes UODO – działając na podstawie art. 41 ust. 3 RODO oraz art. 29 ustawy o ochronie danych osobowych, jak również wytycznych Europejskiej Rady Ochrony Danych nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679[355] – przygotował projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Dokument ten został przetłumaczony przez organ nadzorczy na język angielski, a następnie przekazany do Europejskiej Rady Ochrony Danych w trybie art. 64 RODO[356]. Po otrzymaniu opinii EROD w tej sprawie, Wymogi akredytacji zostały przyjęte i opublikowane w 2021 roku na stronie internetowej UODO[357].

Natomiast 15 lutego 2021 roku zorganizowane zostało webinarium poświęcone m.in. przyjętym wymogom akredytacji podmiotów monitorujących kodeksy[358]. W czasie tego spotkania eksperci UODO przybliżyli słuchaczom przepisy prawa dotyczące kodeków postępowania i podmiotów monitorujących, a także wyjaśnili im wiele wątpliwości związanych ze stosowaniem wyżej wskazanych wymogów.

W 2021 roku do Prezesa UODO wpłynęło 6 wniosków o udzielenie akredytacji do monitorowania kodeksów postępowania. Były to wnioski:

[355] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pl.pdf
[356] DOL.602.4.2020.
[357] https://uodo.gov.pl/pl/138/1861
[358] https://uodo.gov.pl/pl/138/1946

- KPMG Advisory Sp. z o.o. Sp.k.[359] – wniosek został pozostawiony bez rozpoznania, a postępowanie w tej sprawie zakończone w związku z nieuzupełnieniem braków w zakreślonym terminie;
- RS JAMANO Sp. z o.o. Sp.k.[360] – wniosek został pozostawiony bez rozpoznania, a postępowanie w tej sprawie zostało zakończone w związku z nieuzupełnieniem braków w zakreślonym terminie;
- RK RODO Sp. z o.o.[361] – wniosek został poddany ocenie pod kątem formalnym;
- RS JAMANO Sp. z o.o. Sp.k.[362] – wniosek (ponowny) został poddany ocenie pod kątem formalnym;
- Prometriq Akademia Zarządzania Sp. z o.o.[363] – wniosek został poddany ocenie pod kątem formalnym;
- KPMG Advisory Sp. z o.o. Sp.k.[364] – wniosek (ponowny) został poddany ocenie pod kątem formalnym.

W 2021 roku organ nadzorczy udzielał odpowiedzi na napływające do Urzędu zapytania dotyczące kwestii akredytacji podmiotów monitorujących kodeksy postępowania oraz wymogów akredytacji podmiotów monitorujących kodeksy[365].

13. Certyfikacja

Certyfikacja jest nową instytucją prawną, nieznaną w uchylonych w 2018 r. przepisach o ochronie danych osobowych. Zgodnie z RODO, państwa członkowskie, organy nadzorcze, EROD oraz Komisja Europejska zachęcają do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, z uwzględnieniem szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Narzędzia te mają na celu nie tylko zapewnienie dodatkowych gwarancji dla osób, których dane dotyczą, ale również pozwolą tzw. podmiotom zobowiązanym na wdrożenie odpowiednich środków technicznych i organizacyjnych w rozumieniu RODO. Stosownie do art. 12 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, w Polsce certyfikacja będzie dokonywana przez podmioty certyfikujące, które będą

[359] DOL.420.4.2021.
[360] DOL.420.5.2021.
[361] DOL.420.8.2021.
[362] DOL.420.9.2021.
[363] DOL.420.10.2021.
[364] DOL.420.11.2021.
[365] DOL.420.3.2021, DOL.420.7.2021.

posiadać stosowną akredytację udzieloną przez Polskie Centrum Akredytacji (PCA). Akredytacja ta będzie dokonywana m.in. w oparciu o wymogi akredytacji podmiotów certyfikujących, o których mowa w art. 43 ust. 3 RODO, które – stosownie do przepisów RODO i ustawy o ochronie danych osobowych – opracowuje, zatwierdza i podaje do publicznej wiadomości Prezes UODO. W związku z przyjętym w Polsce modelem certyfikacji, zadaniem Prezesa UODO będzie również zatwierdzanie kryteriów certyfikacji, o których mowa w art. 42 ust. 5 RODO.

W 2021 roku organ nadzorczy prowadził prace nad projektem wymogów akredytacji podmiotów certyfikujących. Dokument ten został sporządzony m.in. w oparciu o wytyczne EROD 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679)[366]. W styczniu 2022 roku projekt ten został przedłożony EROD do zaopiniowania w trybie art. 64 RODO[367].

14. 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.

14.1. 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.

Mimo że udzielanie odpowiedzi na pytania prawne nie zostało wprost ujęte wśród kompetencji organu właściwego w sprawach ochrony danych osobowych, to stanowi ważny wyraz jego troski

[366] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_pl
[367] DOL.602.1.2022.

o upowszechnianie i doskonalenie wiedzy w tym zakresie. Jednocześnie problemy podnoszone w pismach z pytaniami stanowią często impuls do podjęcia określonych działań z urzędu (takich jak np. komunikaty, poradniki, wystąpienia). Niejednokrotnie bowiem organowi nadzorczemu w tego typu korespondencji sygnalizowane są problemy wspólne dla różnych grup podmiotów.

W roku 2021 **administratorzy oraz osoby fizyczne skierowali** do Urzędu Ochrony Danych Osobowych łącznie **2141 pism zawierających pytania z zakresu ochrony danych osobowych**. To znacznie mniej niż w roku ubiegłym, kiedy to wpłynęło ich **2774**. Różnica może być spowodowana tym, że wiele kwestii zostało już przez organ nadzorczy wyjaśnionych, np. w komunikatach zamieszczonych na stronie internetowej Urzędu czy w Newsletterze UODO dla IOD.

Łącznie w 2021 roku organ nadzorczy **rozpatrzył 1251** takich pism.

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

W 2021 roku do UODO wpłynęło **301 pytań od inspektorów ochrony danych**. Udzielono zaś **385 odpowiedzi** na pytania od IOD.

14.1.1. Pytania prawne od administratorów i osób fizycznych

Zakres tematyczny zagadnień poruszanych w pytaniach od administratorów i osób fizycznych, dotyczył różnych aspektów przetwarzania danych osobowych oraz stosowania nie tylko przepisów RODO, ale także innych, szczególnych przepisów prawa.

14.1.1.1. Przetwarzanie danych osobowych podczas pandemii COVID-19

Ze względu na trwającą w 2021 roku pandemię COVID-19, podobnie jak w roku ubiegłym, część pytań dotyczyła właśnie tej tematyki. Zauważyć jednak można znaczący spadek ich liczby, szczególnie jeśli chodzi o zapytania z sektora publicznego.

Pozyskiwanie informacji o zaszczepieniu przeciw COVID-19

W związku z tym, że pod koniec 2020 roku rozpoczęły się szczepienia przeciw COVID-19, które były dobrowolne, pojawiły się wątpliwości co do możliwości pozyskiwania informacji o zaszczepieniu danej osoby w świetle obowiązujących przepisów prawa. Najczęściej o zagadnienie to pytano w relacjach pracodawca – pracownik[368]. Pojawiały się też różne interpretacje tej kwestii,

[368] Np. DOL.023.735.2021, DOL.023.497.2021.

m.in. także takie, że skoro pracodawca ma obowiązek zapewnić bezpieczne i higieniczne warunki pracy w zakładzie, to powinien móc pozyskać dane o tym, który z jego pracowników został zaszczepiony, aby zorganizować prace w sposób jak optymalny z punktu widzenia zasad ochrony zdrowia wszystkich zatrudnionych. Wśród wielu podmiotów, które występowały do organu nadzorczego o wskazanie podstawy prawnej przetwarzania danych osobowych pracowników w zakresie szczepień przeciwko COVID-19, były też podmioty publiczne, np. Rządowe Centrum Bezpieczeństwa[369].

UODO wyrażał jednoznaczne stanowisko, że informacje o zaszczepieniu stanowią szczególną kategorię danych osobowych, o której mowa w art. 9 ust. 1 RODO[370]. Przetwarzanie tej kategorii danych jest legalne jedynie po spełnieniu jednej z przesłanek określonych w art. 9 ust. 2 RODO. Szczególną uwagę zwracał na te, które odwołują się do ochrony danych osobowych z zachowaniem odpowiednich, konkretnych środków ochrony praw osób, których dane dotyczą (art. 9 ust. 2 lit. g–i RODO). Powyższe warunki stanowiły o dopuszczalności przetwarzania danych szczególnych kategorii, jednak – jak zauważył organ nadzorczy – w obecnym stanie prawnym brak jest przepisów prawa, które dawałyby pracodawcy podstawy prawne do żądania od pracowników informacji o odbyciu szczepienia ochronnego. Z przepisów prawa pracy takie uprawnienia nie wynikają. Nie zostały one również przyznane pracodawcom mocą przepisów specustawy[371], co pozwalałoby pracodawcy na pozyskiwanie od pracowników danych o odbyciu szczepienia ochronnego przeciwko COVID-19.

Organ nadzorczy nie uznawał także za wystarczającą podstawę prawną do przetwarzania danych osobowych osób zaszczepionych, w tym w relacjach pomiędzy pracodawcami i pracownikami[372], przepisów rozporządzenia Rady Ministrów z 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu

[369] DOL.023.497.2021.

[370] Zgodnie z art. 9 ust. 1 RODO zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

[371] 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 (Dz.U. z 2020 r. poz. 374).

[372] Zgodnie z art. 26 pkt 16, do liczby osób, o której mowa w ust. 10 pkt 1 i ust. 15 pkt. 2 i 3 (tj. imprez i spotkań do 25 osób, które odbywają się w lokalu lub budynku wskazanym jako adres miejsca zamieszkania lub pobytu osoby, która organizuje imprezę lub spotkanie; do limitu osób nie wlicza się osoby organizującej imprezę lub spotkanie oraz osób wspólnie z nią zamieszkujących lub gospodarujących; imprez i spotkań do 150 osób, które odbywają się na otwartym powietrzu albo w lokalu lub w wydzielonej strefie gastronomicznej sali sprzedaży, o których mowa w § 9 ust. 15 pkt 2) nie wlicza się osób zaszczepionych przeciwko COVID-19.

epidemii[373], przyznających osobom zaszczepionym liczne przywileje. Przepisy wskazanego rozporządzenia nie stanowią podstawy żądania danych o stanie zdrowia od osób, których dane dotyczą, na zasadzie obowiązku i dalszego ich przechowywania, tj. nie regulują możliwości żądania udostępnienia od podmiotów danych informacji na temat ich szczepienia – nie określają, kto i na jakich zasadach może weryfikować i w jaki sposób ma być dokonywana weryfikacja, czy dana osoba odbyła szczepienie przeciwko COVID-19. UODO zwracał także uwagę, że przepisy te nie przewidują „konkretnych środków ochrony", o których mowa w art. 9 ust. 2 lit. i RODO, co zgodnie z powołanym przepisem jest niezbędne. Również w rozporządzeniu Rady Ministrów z dnia 4 czerwca 2021 r. zmieniającym rozporządzenie w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[374], brak było przepisów, które mogłyby stanowić podstawę prawną do przetwarzania danych osobowych o zaszczepieniu przez pracodawców.

Organ nadzorczy wielokrotnie wskazywał, że jeżeli pracodawca chce przetwarzać dane osobowe pracowników dotyczące informacji o zaszczepieniu, jedyną uprawniającą go do tego przesłanką może być zgoda osoby, której dane dotyczą (art. 9 ust. 2 lit. a RODO). Jednak pozyskiwanie/udostępnianie takich danych może następować tylko z inicjatywy pracownika. Zgodnie bowiem z art. 22^{1b} § 1 Kodeksu pracy, zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika (…).

W związku z powyższym organ nadzorczy wskazywał, że aby pracodawca mógł żądać od pracownika udostępniania takich danych, powinny zostać wdrożone przepisy prawa gwarantujące odpowiednią ochronę praw osób, których dane dotyczą. Podkreślał także, że nie chodzi tu jedynie o poszanowanie prawa do autonomii informacyjnej, lecz również o spełnienie określonych w RODO warunków pozyskiwania zgody (art. 4 pkt 11 RODO i art. 7 RODO)[375] – zgoda musi być dobrowolna, świadoma, konkretna – wyrażona w formie jednoznacznego okazania woli i możliwa do odwołania w każdym czasie.

[373]Dz.U. z 2021 r. poz. 861.
[374] Dz.U. z 2021 r. poz. 1013.
[375] 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.

Warto dodać, że w analizowanym okresie sprawozdawczym trwały prace legislacyjne mające na celu uregulowanie w przepisach prawa kwestii pozyskiwania przez pracodawców informacji o szczepieniach pracowników, ale ostatecznie żadne regulacje w tym zakresie nie zostały wypracowane.

Wykonywanie testów na COVID-19

W analizowanym 2021 roku pojawiały się także pytania, zwłaszcza od organizacji związkowych, czy pracodawca może zmusić pracownika do wykonywania testu na COVID-19, czy pracownik może odmówić jego wykonania, a także czy pracodawca może żądać przedstawienia wyniku takiego testu[376]. Odpowiadając na nie, organ nadzorczy wyrażał podobne stanowisko, jak w przypadku pozyskiwania informacji o zaszczepieniu, a także odwoływał do stanowisk w zakresie przetwarzania przez pracodawcę danych osobowych dotyczących zdrowia pracowników prezentowanych na stronie internetowej Urzędu Ochrony Danych Osobowych[377].

Certyfikaty szczepień przeciw COVID-19

Osoby fizyczne pytały m.in., czy jakakolwiek instytucja ma prawo żądać od nich przedstawienia certyfikatu szczepienia przeciwko COVID-19 w jakiejkolwiek sytuacji, np. przed wizytą u lekarza czy wejściem do sklepu[378]. Z kolei ze strony podmiotów zobowiązanych do przestrzegania określonego przepisami prawa limitu osób (np. hotele, inne obiekty usługowe) pojawiały się pytania o legalność żądania przedstawienia certyfikatów szczepionkowych[379]. W związku z tym Prezes UODO zamieścił swoje stanowisko w tej sprawie na stronie internetowej Urzędu[380], informując, że przepisy rozporządzenia Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, które określiły m.in. limity osób mogących uczestniczyć w różnych wydarzeniach, nie uprawniają podmiotów zobowiązanych do przestrzegania określonego tymi przepisami limitu osób do żądania od nich udostępnienia informacji o zaszczepieniu przeciwko COVID-19. Ewentualne okazywanie dowodów potwierdzających fakt zaszczepienia może się odbywać z inicjatywy samej osoby zainteresowanej skorzystaniem z usług takiego podmiotu.

Warto dodać, że pod koniec 2021 roku zaczęły obowiązywać zmiany w rozporządzeniu Rady Ministrów z dnia 14 grudnia 2021 r. zmieniającym rozporządzenie w sprawie ustanowienia

[376] DOL.023.973.2021.
[377] Np. https://uodo.gov.pl/pl/138/1516, https://uodo.gov.pl/pl/138/2088
[378] DOL.023.516.2021.
[379] DOL.023.514.2021, DOL.023.665.2021, DOL.023.482.2021.
[380] https://uodo.gov.pl/pl/138/2088

określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, które uregulowały wprost kwestię weryfikowania limitu osób przebywających w różnych obiektach i korzystających z określonych usług. Wskazano, że to do osoby zamierzającej skorzystać z usługi lub uczestniczyć w wydarzeniu należy decyzja, czy chce ona skorzystać z uprawnienia związanego z zaszczepieniem się przeciwko COVID-19 i okazać dokument (cyfrowe zaświadczenie COVID lub zaświadczenie o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19) w przypadku osiągnięcia limitu skutkującego ograniczeniem w dostępie do tej usługi lub wydarzenia[381].

W 2021 roku do UODO wpłynęło też pytanie, kto, w związku z wydanymi przez Ministerstwo Zdrowia *Wytycznymi dla funkcjonowania uzdrowisk w trakcie epidemii COVID-19 w Polsce*, ma prawo do sprawdzania, czy pacjent posiada ważny certyfikat szczepień i kto w takim ośrodku/sanatorium może legalnie wymagać okazania takiego certyfikatu[382]. Organ nadzorczy wskazał, że powołane wytyczne nie określają wprost, kto ma prawo wymagać okazania certyfikatu szczepień, ale należy zauważyć, że zgodnie z zasadami ochrony danych osobowych powinna to być osoba upoważniona przez administratora. Zgodnie bowiem z RODO, podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych, przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego (art. 29). Ponadto UODO zwrócił uwagę, że nie jest właściwy, aby ocenić zasadność wprowadzenia rozwiązań zawartych w *Wytycznych dla funkcjonowania uzdrowisk w trakcie epidemii COVID-19 w Polsce*, przy czym rozwiązania w nich zawarte odzwierciedlały obowiązujące w tym zakresie przepisy prawa[383], które wskazywały wprost, że warunkiem rozpoczęcia rehabilitacji w ramach turnusu

[381] Od 15 grudnia 2021 r. obowiązuje rozporządzenia Rady Ministrów z dnia 14 grudnia 2021 r. zmieniające rozporządzenie w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz. U. z 2021 r. poz. 2311). Zgodnie z jego § 1 pkt 11 (dodającym § 26a w rozporządzeniu Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii) do ustanowionych w rozporządzeniu limitów liczby osób przebywających w pomieszczeniach, budynkach, obiektach, na określonej powierzchni pomieszczeń, budynków lub obiektów lub na otwartej przestrzeni oraz uczestniczących w zgromadzeniach, nie wlicza się osób zaszczepionych przeciwko COVID-19, pod warunkiem okazania przez te osoby unijnego cyfrowego zaświadczenia COVID lub zaświadczenia o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 uznawanego za równoważne z zaświadczeniami wydawanymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/953 z dnia 14 czerwca 2021 r. w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID) w celu ułatwienia swobodnego przemieszczania się w czasie pandemii COVID-19.

[382] DOL.023.514.2021.

[383] Przepisy rozporządzenia Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz. U. z 2021 r. poz. 861).

rehabilitacyjnego jest negatywny wynik testu diagnostycznego w kierunku zakażenia COVID-19 lub zaszczepienie przeciwko COVID-19. Ten sam warunek dotyczył rozpoczęcia leczenia uzdrowiskowego, rehabilitacji uzdrowiskowej lub leczenia sanatoryjnego dzieci. Organ podkreślił także, że z ww. wytycznych wynikało, iż okazanie certyfikatu szczepień jest uprawnieniem pacjenta, a nie obowiązkiem. Jeśli jednak pacjent nie okaże certyfikatu szczepień, to chcąc skorzystać z pobytu w zakładzie lecznictwa uzdrowiskowego, musi spełnić inne warunki, np. poddać się badaniom diagnostycznym w kierunku SARS-CoV-2, którego negatywny wynik będzie mógł być warunkiem przyjęcia do zakładu.

Przekazywanie danych służbom sanitarno-epidemiologicznym przez szkoły

Podobnie jak w roku ubiegłym powtarzały się pytania od rodziców dzieci szkolnych i przedszkolnych, czy szkoła lub inna placówka oświatowa mogą przekazywać dane osobowe dziecka wraz z numerem telefonu kontaktowego służbom sanitarno-epidemiologicznym[384]. Udzielając wyjaśnień w tym zakresie, organ nadzorczy odwoływał się do przepisów prawa, które regulowały zasady odbywania kwarantanny[385] i procedury związane z prowadzonym dochodzeniem epidemiologicznym. Przepisy te uprawniają służby sanitarno-epidemiologiczne do żądania udzielenia informacji o osobach zakażonych lub podejrzanych o zakażenie, chorych lub podejrzanych o chorobę zakaźną, osobach zmarłych z powodu choroby zakaźnej lub osobach, wobec których istnieje takie podejrzenie. Do danych osób, o których mowa wyżej, a które mogą być na te potrzeby pozyskiwane, należą m.in.: imię i nazwisko, data urodzenia, numer PESEL, adres zamieszkania, numer telefonu kontaktowego oraz adres poczty elektronicznej lub innych środków komunikacji elektronicznej. UODO przypominał również, że Główny Inspektor Sanitarny lub działający z jego upoważnienia inny organ Państwowej Inspekcji Sanitarnej może wydawać wielu podmiotom m.in. zalecenia i wytyczne określające sposób postępowania w czasie realizacji zadań w przypadku stanu zagrożenia epidemicznego, stanu epidemii albo w razie niebezpieczeństwa szerzenia się zakażenia lub choroby zakaźnej. Takie wytyczne Głównego Inspektora Sanitarnego zostały wydane dla przedszkoli, oddziałów przedszkolnych w szkole podstawowej i innych form wychowania przedszkolnego oraz instytucji opieki nad dziećmi do lat 3, i były dostępne na stronie Głównego

[384] DOL.023.1043.2021.

[385] 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, ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi oraz rozporządzenie Rady Ministrów w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii.

Inspektora Sanitarnego[386]. Określały one m.in. procedury postępowania w przypadku zakażenia koronawirusem lub zachorowania na COVID-19[387].

Szczepienia nauczycieli a System Informacji Oświatowej

Innym zagadnieniem związanym z kwestią szczepień przeciwko COVID-19 była sprawa zgłoszona Prezesowi UODO przez Rzecznika Praw Obywatelskich dotycząca przekazywania do Systemu Informacji Oświatowej (SIO) przez dyrektorów szkół lub placówek oświatowych danych nauczycieli i innych osób zatrudnionych w szkole chętnych do udziału w szczepieniu, co następowało poprzez wypełnienie specjalnego formularza w SIO[388].

Organ nadzorczy zwrócił się do Ministerstwa Edukacji i Nauki o podanie podstawy prawnej takiego działania. W odpowiedzi MEiN wskazało rozporządzenie z dnia 2 marca 2021 r. zmieniające rozporządzenie z dnia 19 listopada 2020 r. w sprawie szczególnych rozwiązań w zakresie systemu informacji oświatowej w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19[389]. Stanowisko to wzbudziło wątpliwości organu nadzorczego, ponieważ z przepisów ustawy o systemie informacji oświatowej wynika, że baza danych SIO jest szczególnym zbiorem danych, który określa rodzaj i zakres danych w niej gromadzonych, w tym również dane identyfikacyjne i dane dziedzinowe nauczycieli (art. 29). Szczegółowy zakres danych gromadzonych w SIO doprecyzowuje rozporządzenie Ministra Edukacji Narodowej z dnia 28 sierpnia 2019 r. w sprawie szczegółowego zakresu danych dziedzinowych gromadzonych w systemie informacji oświatowej oraz terminów przekazywania niektórych danych do bazy danych systemu informacji oświatowej. Zarówno w ustawie o SIO, jak również w przepisach powołanego aktu wykonawczego, ustawodawca nie wskazał danych o woli wykonania szczepień ochronnych, jako danych przetwarzanych w tej bazie. Jednocześnie katalog danych zawartych w SIO ustawodawca uznał za zamknięty. Organ nadzorczy podkreślał, że rozporządzenie Ministra Edukacji Narodowej z dnia 5 lutego 2021 r. zmieniające rozporządzenie w sprawie szczególnych rozwiązań w zakresie systemu informacji oświatowej w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 – wskazywane jako podstawa

[386] Zob. www.gis.gov.pl.
[387] Można w nich było przeczytać, że „Rekomenduje się ustalenie listy osób przebywających w tym samym czasie w części/częściach podmiotu, w których przebywała osoba podejrzana o zakażenie i zaleca się stosowanie do wytycznych Głównego Inspektora Sanitarnego dostępnych na stronie gov.pl/web/koronawirus/ oraz gis.gov.pl odnoszących się do osób, które miały kontakt z zakażonym".
[388] DOL.023.170.2021.
[389] Dz.U. z 2021 r. poz. 390.

prawna pozyskiwania danych osobowych nauczycieli, którzy wyrazili wolę poddania się szczepieniu ochronnemu przeciwko COVID-19 – choć dopuściło do pozyskiwania tych danych, nie jest podstawą prawną dla ich przetwarzania w SIO, gdyż nie została zmieniona ustawa odnosząca się do zasad przetwarzania danych w tym systemie.

Na skutek działań podjętych przez Prezesa UODO w tej sprawie, Ministerstwo Edukacji i Nauki usunęło przedmiotowe dane z systemu SIO i proces przetwarzania danych osobowych nauczycieli i innych osób zatrudnionych w szkole w zakresie deklaracji chęci odbycia szczepienia przeciwko COVID-19 w SIO nie jest już kontynuowany.

14.1.1.2. Administrator czy podmiot przetwarzający

Mimo że przepisy RODO definiują pojęcie administratora i podmiotu przetwarzającego, to w praktyce pojawiają się wątpliwości, co do statusu danego podmiotu. Analizując i wyjaśniając zgłaszane wątpliwości, organ nadzorczy odwoływał się do opinii Grupy Roboczej Art. 29 przyjętej 16 lutego 2010 r. pn. Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169)[390] oraz do wytycznych 7/2020 Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO.

Dyrektor zakładu karnego a podmiot zatrudniający więźnia

Jako przykład wskazać można sprawę opisywaną w newsletterze UODO dla IOD[391], a dotyczącą oceny statusu dyrektora zakładu karnego i podmiotu zatrudniającego więźnia. UODO wyraził stanowisko, że dyrektor zakładu karnego i podmiot zatrudniający więźnia przetwarzają jego dane osobowe w innych celach, każdy z nich wypełnia odmienne, przewidziane przepisami prawa zadania, a także niezależnie ustala środki przetwarzania danych i sposoby ich zabezpieczania. W związku z tym uznać ich należy za odrębnych administratorów.

Zaznaczył, że zgodnie z art. 121 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (K.k.w.), skazanemu zapewnia się w miarę możliwości świadczenie pracy. Ma to sprzyjać resocjalizacji więźniów. Dyrektor zakładu karnego zawiera z zewnętrznym podmiotem umowę o odpłatne zatrudnienie skazanych, która określa zasady i warunki organizacji świadczenia pracy przez skazanych. Choć ogólnym celem społecznym tej umowy będzie oddziaływanie na życie skazanych poprzez umożliwienie im pełnienia społecznie pożytecznych ról,

[390] Grupa Robocza Art. 29 wskazywała, że pojęcie administratora danych jest pojęciem funkcjonalnym, mającym na celu przypisanie obowiązków tam, gdzie występuje faktyczny wpływ, a zatem raczej w oparciu o analizę okoliczności faktycznych niż o analizę formalną.
[391] Newsletter 12/2021.

to cele przetwarzania danych osobowych przez dyrektora zakładu karnego i podmiot zatrudniający będą odrębne. Dla dyrektora będzie to realizacja zobowiązania, o którym mowa w art. 121 § 1 K.k.w., a dla podmiotu zewnętrznego wykonywanie działalności gospodarczej. Każdy z tych podmiotów wypełnia w związku z tym odmienne zadania przewidziane przepisami prawa, a także niezależnie od siebie ustala środki przetwarzania danych i sposoby ich zabezpieczania. Razem będą jednak przetwarzać dane w związku z odbywaniem kary przez skazanych. Dlatego dyrektor zakładu karnego i zewnętrzny podmiot zatrudniający więźnia będą, każdy w swoim zakresie, oddzielnymi administratorami danych osobowych skazanego świadczącego pracę odpłatną.

Status oferenta (przyszłego cesjonariusza) w procesie przetargu na nabycie wierzytelności

Z kolei Związek Przedsiębiorstw Finansowych w Polsce[392] zwrócił się z prośbą o wsparcie w rozstrzygnięciu statusu podmiotu uczestniczącego w procesie przetargu na nabycie wierzytelności, tj. roli oferenta, jako administratora danych bądź podmiotu przetwarzającego dane w imieniu organizatora przetargu[393]. UODO wyjaśnił, że zasadnicze znaczenie dla rozstrzygnięcia ma kwestia możliwości samodzielnego ustalania celów i sposobów przetwarzania danych. To administrator w momencie przetwarzania danych osobowych decyduje o całym procesie działań podejmowanych na tych danych, a podmiot przetwarzający działa na zlecenie administratora i w zakresie, jaki zostanie przez niego wskazany. Organ przypomniał, że od wielu lat ugruntowane jest stanowisko sądów administracyjnych określających rolę nabywcy wierzytelności – cesjonariusza, jako administratora – co zostało już wyrażone w wyroku Naczelnego Sądu Administracyjnego z dnia 6 czerwca 2005 r.[394] W związku z powyższym organ wskazał, że to oferent (przyszły cesjonariusz) jest samodzielnym administratorem, przetwarzającym udostępnione mu dane we własnym imieniu, we własnym interesie i na własne ryzyko[395].

[392] Związek Przedsiębiorstw Finansowych w Polsce (wcześniej Konferencja Przedsiębiorstw Finansowych w Polsce – Związek Pracodawców) działa na podstawie ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 1991 r. Nr 55, poz. 235), obowiązujących przepisów prawa i postanowień Statutu.
[393] DOL.023.684.2021.
[394] Sygnatura akt I OPS 2/05.
[395] Prezes UODO przypomniał, że w przypadku sprzedaży wierzytelności, firma windykacyjna, która nabyła wierzytelność, staje się administratorem danych osobowych dłużników i zobowiązana jest do przestrzegania obowiązków wynikających z RODO. Całość stanowiska można znaleźć pod linkiem: https://uodo.gov.pl/pl/138/1263.

14.1.1.3. Inne pytania

Weryfikacja przez gminy informacji zawartych w deklaracjach śmieciowych

O ile w roku ubiegłym Prezes UODO rozpatrywał wiele spraw związanych z zakresem danych osobowych pozyskiwanych przez gminy w tzw. deklaracjach śmieciowych[396], to w 2021 roku do UODO wpływały pytania dotyczące różnego sposobu weryfikacji informacji zawartych w tych deklaracjach.

W jednej z takich spraw Miejski Ośrodek Pomocy Społecznej miał wątpliwości, co do udostępnienia urzędowi miasta danych z bazy osób pobierających świadczenia 500+ w zakresie adresu nieruchomości, pod którym zamieszkuje osoba pobierająca świadczenie oraz liczby dzieci, na które pobierane było świadczenie 500+, w celu weryfikacji deklaracji śmieciowych[397].

Organ nadzorczy wyraził stanowisko, że obowiązujące przepisy prawa nie dają podstawy do pozyskiwania przez urząd miasta od innego organu państwowego (np. miejskiego ośrodka pomocy społecznej) informacji z bazy osób pobierających świadczenia 500+ w celu weryfikacji deklaracji śmieciowych. Ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach[398] nakłada obowiązek do złożenia nowej deklaracji śmieciowej w przypadku zmiany danych w niej zawartych jedynie na właściciela nieruchomości. Prezes UODO zwrócił także uwagę, że Miejski Ośrodek Pomocy Społecznej, działając na podstawie ustawy z dnia 12 marca 2004 r. o pomocy społecznej[399], ma obowiązek dbać o dobro osób korzystających z pomocy społecznej i chronić ich dobra osobiste, a także przetwarzać dane osobowe osób, do których stosuje się ustawę, oraz członków ich rodzin w zakresie i celu niezbędnym do realizacji zadań wynikających z ustawy.

Takie samo podejście Prezes UODO prezentował w sprawach żądania przez związek gmin od ośrodków pomocy społecznej informacji o liczbie osób wspólnie zamieszkałych na danej nieruchomości, korzystających z pomocy społecznej oraz świadczeń rodzinnych, wraz z podaniem adresu w celu weryfikacji deklaracji śmieciowych[400].

W związku zaś ze znowelizowaną w 2021 roku ustawą o utrzymaniu czystości i porządku w gminach, zgodnie z którą wójt, burmistrz lub prezydent miasta w celu weryfikacji złożonych deklaracji może wykorzystać informacje i dane znajdujące się w jego posiadaniu oraz posiadaniu

[396] Efektem czego było wystąpienie w tej sprawie 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 (DOL.413.4.2020; opisane w Sprawozdaniu z działalności Prezesa UODO w roku 2020).
[397] DOL.023.501.2021.
[398] t.j. Dz. U. z 2021 r. poz. 888 z późn. zm.
[399] t.j. Dz. U. z 2020 r. poz. 1876 z późn. zm.
[400] DOL.023.503.2021, DOL.023.508.2021.

gminnych jednostek organizacyjnych, w tym przedsiębiorstw wodociągowo-kanalizacyjnych[401], wpłynęło pytanie, czy wprowadzony przepis stanowi podstawę do pozyskiwania przez wójta, burmistrza lub prezydenta miasta wszystkich informacji z baz danych będących w posiadaniu jednostek podległych, ponieważ nie precyzuje, jakie dane i w jakim zakresie mogą zostać udostępnione[402]. Organ nadzorczy zwrócił wówczas uwagę, że wprowadzony przepis należy interpretować w powiązaniu z innymi przepisami. Zgodnie z art. 60 ust. 1 tej ustawy, w razie niezłożenia deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi albo uzasadnionych wątpliwości co do danych zawartych w deklaracji, wójt, burmistrz lub prezydent miasta określa, w drodze decyzji, wysokość opłaty za gospodarowanie odpadami komunalnymi, biorąc pod uwagę dostępne dane właściwe dla wybranej przez radę gminy metody, a w przypadku ich braku – uzasadnione szacunki, w tym w przypadku nieruchomości, na których nie zamieszkują mieszkańcy, średnią ilość odpadów komunalnych powstających na nieruchomościach o podobnym charakterze. Natomiast art. 6m ust. 1a ww. ustawy stanowi, że deklaracja zawiera dane niezbędne do określenia wysokości opłaty za gospodarowanie odpadami komunalnymi oraz wysokość opłaty za gospodarowanie odpadami komunalnymi. Prezes UODO wskazywał, że dopuszczalność wykorzystania możliwości pozyskania danych na podstawie znowelizowanego przepisu art. 6o ust. 1a ustawy uwarunkowana jest przede wszystkim przesłanką w postaci uzasadnionych wątpliwości, co do danych zawartych w deklaracji lub niezłożenia takiej deklaracji w ogóle. A zatem organ właściwy w sprawie ochrony danych osobowych za niedopuszczalne uznał przyjęcie, że wszystkie złożone deklaracje mogą być weryfikowane w sposób określony w tym przepisie, a zatem z założeniem, że wszystkie deklaracje mogą być nierzetelne.

W kontekście zaś zgłoszonych wątpliwości, czy możliwe jest całościowe, globalne przekazanie gminie danych osobowych wszystkich osób będących w ewidencji gminnej jednostki organizacyjnej, czy też weryfikację należy traktować jako czynność dotyczącą indywidualnego przypadku, UODO zwrócił uwagę, że pozyskiwanie przez gminy danych osobowych z innych baz danych powinno odbywać się z poszanowaniem zasad i gwarancji wynikających z RODO. Przepisy wdrażające tego rodzaju rozwiązania powinny szczegółowo określać procedurę, formę, zakres i tryb udostępniania danych osobowych. Przyjmowanie rozwiązań o charakterze blankietowym powoduje brak jasnych podstaw prawnych w zakresie praw i obowiązków, a tym samym zakresów odpowiedzialności

[401] Art. 6o ust. 1a dodany przez art. 1 pkt 16 lit. a ustawy z dnia 11 sierpnia 2021 r. (Dz. U. z 2021 r. poz. 1648) zmieniającej niniejszą ustawę z dniem 23 września 2021 r.
[402] DOL.023.774.2021.

– w tym relacji i ról w zakresie procesów związanych z przetwarzaniem danych osobowych. Przekazywanie danych osobowych pomiędzy podmiotami publicznymi powinno odbywać się w sposób zapewniający bezpieczeństwo tych danych na odpowiednim poziomie, na zasadach ściśle określonych przepisami ustawy. Przekazywanie danych nie może również prowadzić do łączenia zbiorów danych – ustawodawca, przyjmując rozwiązania prawne, powinien zwrócić uwagę na motyw 31 rozporządzenia 2016/679, który stanowi, że organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (…) nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, organy te powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

Udostępnianie danych osobowych pomiędzy podmiotami publicznymi

Podobnie, jak w latach poprzednich, także i w roku 2021 pojawiały się wątpliwości związane z możliwością udostępnienia danych pomiędzy podmiotami publicznymi. Przy czym odnosiły się one do takich sytuacji, gdy jeden z podmiotów publicznych wnioskuje o pozyskanie danych osobowych z bazy danych drugiego podmiotu publicznego. We wszystkich takich sprawach organ przypominał, że w przypadku podmiotów publicznych, co do zasady podstawę prawną przetwarzania danych osobowych (w tym udostępniania danych) powinno stanowić wykonanie obowiązku prawnego ciążącego na administratorze (art. 6 ust.1 lit. c RODO) lub też wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO). Ponadto każdy wniosek o udostępnienie danych osobowych musi wskazywać dokładnie, o jaki zakres danych osobowych chodzi, podstawę prawną oraz cel ich pozyskania. Taki wniosek, ze względu na niezbędność przetwarzania danych w celu wypełnienia obowiązku prawnego ciążącego na administratorze, powinien zawierać dokładne wskazanie, o jaki wynikający z przepisów prawa obowiązek wnioskodawcy chodzi.

Jedna z tego typu spraw dotyczyła wniosku Gminnego Ośrodka Pomocy Społecznej (GOPS) skierowanego do Powiatowego Centrum Pomocy Rodzinie (PCPR) o udzielenie informacji

o przyznanych osobie fizycznej świadczeniach[403]. Jako podstawę prawną wskazano art. 105 ust. 1 ustawy o pomocy społecznej[404], a jako cel – niezbędność do przyznania świadczenia z pomocy społecznej. Przepis ten wymienia, jakie podmioty są zobowiązane do udostępnienia informacji, które mają znaczenie dla rozstrzygnięcia o przyznaniu lub wysokości świadczeń z pomocy społecznej, dla ustalenia wysokości odpłatności za świadczenia z pomocy społecznej lub dla weryfikacji uprawnień do świadczeń z pomocy społecznej, wysokości tych świadczeń lub odpłatności za te świadczenia. Informacji tych udziela się w terminie 7 dni od dnia otrzymania wniosku kierownika ośrodka pomocy społecznej, dyrektora centrum usług społecznych lub pracownika socjalnego.

UODO wyjaśnił, że ostateczna merytoryczna ocena każdego wniosku o udostępnienie danych należy do administratora. Natomiast każdy podmiot wnioskujący powinien wskazać konkretną, szczegółową podstawę prawną swojego żądania o udostępnienie danych, tak aby podmiot mający je udostępnić mógł podjąć merytoryczną decyzję, czy może dane te przekazać, aby nie narazić się na odpowiedzialność z tego tytułu, w szczególności na podstawie RODO. W przypadku braków formalnych we wniosku, celowe jest zwrócenie się do wnioskodawcy o ich uzupełnienie, a także o uzyskanie od niego wyjaśnień lub dodatkowych informacji.

Podobne stanowisko organ nadzorczy prezentował także w innych sprawach, m.in. gdy Starosta wnioskował do Zakładu Ubezpieczeń Społecznych (ZUS) o przekazanie danych dla ustalenia, czy dana osoba (beneficjent otrzymujący ekwiwalent dla właścicieli gruntów rolnych) figuruje w kartotece emerytalno-rentowej, a jeśli tak, to od jakiego terminu[405], czy w sprawie, gdzie zarząd dróg miejskich zwracał się do Narodowego Funduszu Zdrowia o udostępnienie adresów

[403] DOL.023.444.2021.
[404] Jednostki sektora finansów publicznych, w tym sądy, policja, Zakład Ubezpieczeń Społecznych, Kasa Rolniczego Ubezpieczenia Społecznego i organy administracji publicznej, a także kuratorzy sądowi, pracodawcy, podmioty wykonujące działalność leczniczą, przedszkola, szkoły, placówki, poradnie i ośrodki, o których mowa w art. 2 pkt 1–8 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, szkoły wyższe, gminne komisje rozwiązywania problemów alkoholowych, organizacje pozarządowe, o których mowa w art. 3 ust. 2 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie, oraz podmioty wymienione w art. 3 ust. 3 tej ustawy z 2003 r. o działalności pożytku publicznego i o wolontariacie, oraz podmioty wymienione w art. 3 ust. 3 tej ustawy są obowiązani niezwłocznie, nie później jednak niż w terminie 7 dni od dnia otrzymania wniosku kierownika ośrodka pomocy społecznej, dyrektora centrum usług społecznych, o którym mowa w ustawie z dnia 19 lipca 2019 r. o realizowaniu usług społecznych przez centrum usług społecznych, lub pracownika socjalnego udostępnić informacje, które mają znaczenie dla rozstrzygnięcia o przyznaniu lub wysokości świadczeń z pomocy społecznej, dla ustalenia wysokości odpłatności za świadczenia z pomocy społecznej lub dla weryfikacji uprawnień do świadczeń z pomocy społecznej, wysokości tych świadczeń lub odpłatności za te świadczenia.
[405] DOL.023.638.2021.

zamieszkania właścicieli pojazdów w celu skontaktowania się z nimi w związku z koniecznością usunięcia pojazdu z drogi[406].

Inne z pytań dotyczyło tego, czy **Powiatowe Centrum Pomocy Rodzinie (PCPR) na potrzeby prowadzenia czynności monitorujących sytuację rodziny, w której osoba stosująca przemoc domową poddana była oddziaływaniom korekcyjno-edukacyjnym, ma prawo pozyskiwać dane osobowe od Miejskiego Ośrodka Pomocy Społecznej (MOPS).**

Dokonując oceny przedstawionego zagadnienia, pod uwagę należy wziąć wszystkie przepisy, które regulują przedmiotową materię, m.in. ustawę z dnia 12 marca 2004 r. o pomocy społecznej, ustawę z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie oraz rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 22 lutego 2011 r. w sprawie standardu podstawowych usług świadczonych przez specjalistyczne ośrodki wsparcia dla ofiar przemocy w rodzinie, kwalifikacji osób zatrudnionych w tych ośrodkach, szczegółowych kierunków prowadzenia oddziaływań korekcyjno-edukacyjnych wobec osób stosujących przemoc w rodzinie oraz kwalifikacji osób prowadzących oddziaływania korekcyjno-edukacyjne, a także przepisy Kodeksu postępowania administracyjnego[407]. Podczas toczących się postępowań prowadzonych przez PCPR, w czasie których PCPR samodzielnie próbował uzyskać informacje od innych podmiotów, m.in. od MOPS, to osoby, z udziałem których toczyły się te postępowania, powinny również mieć możliwość przedłożenia stosownych dokumentów, a także oświadczeń niezbędnych do zbadania danej sprawy. Osoby te powinny być również informowane o pozyskiwaniu ich danych z innych źródeł. Pamiętać bowiem należy, że w przypadku pozyskiwania danych osobowych w sposób inny niż od osób, których one dotyczą, gdy źródłem danych są inne organy administracji publicznej lub osoby trzecie, wówczas należy poinformować osobę, której dane dotyczą, o źródle pozyskania danych, chyba że przepis szczególny zwalnia z tego obowiązku. Ponadto zakres pozyskiwanych danych osobowych i informacji powinien być ograniczony jedynie do niezbędnego minimum, bez przetwarzania danych nadmiarowych bądź danych niemających znaczenia dla danej sprawy. Dzięki temu przekazywanie danych będzie służyło rozstrzygnięciu konkretnej sprawy i jednocześnie czyniło zadość zasadom

[406] Na podstawie art. 130a ust. 10 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. 2021 r. poz. 450 z późn. zm.). Zgodnie z powołanym przepisem „Starosta w stosunku do pojazdu usuniętego z drogi, w przypadkach określonych w ust. 1 lub 2, występuje do sądu z wnioskiem o orzeczenie jego przepadku na rzecz powiatu, jeżeli prawidłowo powiadomiony właściciel lub osoba uprawniona nie odebrała pojazdu w terminie 3 miesięcy od dnia jego usunięcia (…)", DOL.023.542.2021.

[407] Przepisy Kodeksu postępowania administracyjnego wskazują, że w toku postępowania organy administracji publicznej współdziałają ze sobą w zakresie niezbędnym do dokładnego wyjaśnienia stanu faktycznego i prawnego sprawy, mając na względzie interes społeczny i słuszny interes obywateli oraz sprawność postępowania, przy pomocy środków adekwatnych do charakteru, okoliczności i stopnia złożoności sprawy (art. 7b K.p.a.).

przetwarzania danych określonym w art. 5 RODO (zasadzie zgodności z prawem, ograniczenia celu oraz minimalizacji danych) [408].

Przetwarzanie danych przez placówki oświatowe

W 2021 roku do organu nadzorczego wpływały pytania od dyrektorów i pracowników szkół, co do legalności publikacji danych osobowych absolwentów w księgach pamiątkowych i monografiach poświęconych historii szkoły[409]. Pytający wskazywali na trudności w pozyskaniu zgód od absolwentów na publikację ich imion i nazwisk oraz wizerunku i zastanawiali się nad przesłanką z art. 6 ust. 1 lit. f RODO. Argumentowali, że takie księgi pamiątkowe nie będą podlegały sprzedaży, gdyż będą przeznaczone tylko dla wybranego grona osób związanych z historią placówki. Celem książki będzie zaś upamiętnienie działań, osiągnięć dokonanych przez absolwentów i grona pedagogicznego szkoły.

UODO zwracał wówczas uwagę, że przy spełnieniu określonych warunków w przypadku księgi pamiątkowej można zastanawiać się nad uznaniem, że przetwarzanie danych następuje dla celów działalności literackiej. Chodzi o wyłączenie dotyczące wypowiedzi literackiej i artystycznej przewidziane przez unijnego prawodawcę w art. 85 RODO[410] i mające swoje odzwierciedlenie w art. 2 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[411], zgodnie z którym do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe[412], a także do wypowiedzi w ramach działalności literackiej lub artystycznej, nie stosuje się przepisów art. 5–9, art. 11, art. 13–16, art. 18–22, art. 27, art. 28 ust. 2–10 oraz art. 30 RODO. W związku z powyższym przepisów RODO m.in. o podstawach przetwarzania danych osobowych (określonych w art. 6 i art. 9) nie stosuje się do utworów prasowych, literackich i artystycznych. Zaznaczył jednak, że jeśli planowana publikacja nie będzie spełniać warunków do uznania jej za utwór literacki, to

[408] Więcej na ten temat znajduje się w Newsletterze UODO dla IOD 4/2021.
[409] Np. DOL.023.666.2021, DOL.023.713.2021, DOL.023.808.2021.
[410] Państwa członkowskie przyjmują przepisy pozwalające pogodzić prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej (art. 85 ust. 1). Dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej państwa członkowskie określają odstępstwa lub wyjątki od rozdziału II (Zasady), rozdziału III (Prawa osoby, której dane dotyczą), rozdziału IV (Administrator i podmiot przetwarzający), rozdziału V (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych), rozdziału VI (Niezależne organy nadzorcze), rozdziału VII (Współpraca i spójność) oraz rozdziału IX (Szczególne sytuacje związane z przetwarzaniem danych), jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji (art. 85 ust. 2).
[411] Dz. U. z 2019 r. poz. 1781.
[412] Dz. U. z 1984 r. nr 5, poz. 24 z późn. zm.

przepisy dotyczące przetwarzania danych osobowych, w tym regulujące przesłanki dopuszczalności ich przetwarzania (art. 6 ust. 1 i art. 9 ust. 2) i obowiązek informacyjny (art. 13, art. 14), powinny być stosowane w pełnym zakresie. Jeśli zaś chodzi o zamieszczanie w publikacji książkowej zdjęć uczniów i absolwentów oraz nauczycieli, UODO wskazał, że wizerunek należy do danych osobowych w rozumieniu art. 4 pkt 1 RODO i podlega przepisom RODO. A do legalnego przetwarzania (w tym pozyskiwania czy udostępniania) danych osobowych konieczne jest spełnienie jednej z przesłanek wskazanych w art. 6 ust. 1 RODO. Jedną z nich jest zgoda osoby, której dane dotyczą.

Wątpliwości związane z zawieraniem umów powierzenia

Mimo że na stronie internetowej UODO opublikowano już wiele informacji na temat tego, kiedy i na jakich zasadach powinna być zawierana umowa powierzenia, o której stanowi art. 28 RODO, to w praktyce nadal pojawiają się wątpliwości w tym zakresie. Mają je zarówno podmioty publiczne, jak i te z sektora prywatnego.

Przykładowo pewien organ administracji publicznej zwrócił się do UODO z pytaniem, czy w ramach prowadzonego postępowania administracyjnego, podczas którego konieczne stało się skorzystanie z pomocy tłumacza przysięgłego, powinien zawrzeć z nim umowę powierzenia. UODO w odpowiedzi wskazał, że organ administracji publicznej jest obowiązany w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy (art. 77 ust. 1 K.p.a.). Zatem przedłożenie przed organem administracji publicznej dokumentów w języku obcym jest dopuszczalne i to na tym organie spoczywa obowiązek uzyskania ich tłumaczenia. Organy administracji publicznej, działając na podstawie przepisów prawa, mogą więc zwrócić się do tłumacza przysięgłego o dokonanie takiego tłumaczenia, a tłumacz przysięgły na podstawie art. 15 ustawy z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego, nie może odmówić wykonania takiego tłumaczenia, chyba że zachodzą szczególnie ważne przyczyny uzasadniające odmowę. Jednak ustawa o zawodzie tłumacza przysięgłego w art. 29a–29c kreuje obowiązki tłumacza jako administratora. Dlatego organ administracji publicznej, przekazując w związku z prowadzonym postępowaniem dokumenty do tłumaczenia przez tłumacza przysięgłego, nie musi zawierać z nim umowy powierzania przetwarzania danych osobowych. Mamy tu bowiem do czynienia z udostępnieniem danych innemu administratorowi na podstawie przepisów prawa[413].

[413] Więcej na ten temat znajduje się w Newsletterze UODO dla IOD 7/2021.

W innej sprawie **powiatowy urząd pracy (PUP) chciał zawrzeć umowę powierzenia z bankiem,** przekazując mu listy bezrobotnych, którym miały być wypłacane świadczenia. W takiej sytuacji mamy do czynienia z odrębnymi administratorami, których łączy jedynie umowa o świadczenie usług bankowych i dlatego umowa powierzenia nie powinna być zawierana. PUP przetwarza bowiem dane osób bezrobotnych w związku z realizacją własnych zadań określonych w przepisach prawa. Natomiast w związku z zawartą z bankiem umową o świadczenie usług bankowych, udostępnia bankowi dane bezrobotnych w celu realizacji wypłaty należnych im świadczeń. Z kolei bank w momencie otrzymania od PUP danych osób bezrobotnych, na rzecz których ma być zrealizowana określona w umowie usługa bankowa, staje się administratorem tych danych, który realizuje swoje zadania, samodzielnie określając cele i sposoby przetwarzania danych wynikające z przepisów ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe[414].

Wykorzystywanie numeru PESEL

Jednym z analizowanych zagadnień była też kwestia stosowania numeru PESEL jako loginu do różnych systemów informatycznych. Niektóre podmioty wyrażały dopiero chęć wprowadzenia takich rozwiązań, podczas gdy inne już je stosowały. W związku z tym organ nadzorczy podjął ten temat w newsletterze dla IOD[415], przypominając swoje jednoznaczne stanowisko w tej sprawie, zgodnie z którym numer PESEL nie powinien być wykorzystywany jako login do systemu informatycznego czy portalu. Jednocześnie wskazał przemawiające za tym argumenty i przestrzegał przed skutkami wprowadzania takich rozwiązań.

W analizowanym okresie sprawozdawczym **Rzecznik Praw Obywatelskich** zwrócił się z kolei o zajęcie stanowiska w sprawie funkcjonowania systemu SEPIS[416] pod kątem bezpieczeństwa danych osobowych osób posługujących się Profilem Zaufanym[417]. RPO poinformował, że wpływają do niego skargi pracowników inspekcji sanitarnej, którzy zostali zobowiązani do korzystania z systemu SEPIS przez Profil Zaufany. Ten sam problem zasygnalizowała organowi nadzorczemu także **Sekcja Krajowa Pracowników Stacji Sanitarno-Epidemiologicznych NSZZ „Solidarność”,** która zgłosiła swoje wątpliwości w zakresie legalności działań polegających na nakładaniu na

[414] Informacje na ten temat znajdują się w Newsletterze UODO dla IOD 9/2021.
[415] Newsletter UODO dla IOD 11/2021.
[416] SEPIS jest systemem teleinformatycznym do obsługi procesów przetwarzania danych w Państwowej Inspekcji Sanitarnej (PIS). System ten wykorzystywany jest do zarządzania przez PIS sprawami związanymi z epidemiologią, bezpieczeństwem żywności, wody użytkowej i kranowej. Pracownicy PIS wykorzystują system SEPIS m.in.: do przyjmowania zgłoszeń od obywateli, nakładania kwarantann i izolacji czy też edycji danych związanych z ogniskami epidemii.
[417] DOL.023.363.2021.

pracowników Państwowej Inspekcji Sanitarnej wymogu wykorzystywania Profilu Zaufanego do celów służbowych.

Organ do spraw ochrony danych osobowych, odpowiadając na te sygnały, wskazał, że z punktu widzenia przepisów o ochronie danych osobowych zasadniczym problemem jest wykorzystywanie PESEL w podpisie elektronicznym, a następnie jego udostępnianie. Problem ten ma charakter systemowy i jest od dawna przedmiotem pogłębionej analizy organu nadzorczego, a także wystąpień kierowanych m.in. do resortu cyfryzacji[418] czy ministra sprawiedliwości[419].

PESEL jest unikatowym identyfikatorem osoby zawierającym wiele informacji o niej, w tym m.in. o wieku i płci. Ujawnienie numeru PESEL osobie niepowołanej może rodzić szereg ryzyk, w tym ryzyko kradzieży tożsamości. Wykorzystywanie profilu zaufanego do celów służbowych powinno być dodatkowo przeanalizowane w świetle zasady minimalizacji danych, wyrażonej w art. 5 ust. 1 lit. c RODO[420]. Podstaw prawnych dla ujawniania numeru PESEL pracownika poprzez podpisywanie przez niego dokumentów elektronicznych nie kształtuje także art. 22^1 § 1 Kodeksu pracy. Odnosząc się zaś do kwestii uwierzytelniania w systemie SEPIS , to zakres informacji o osobie fizycznej przetwarzanych w związku z utworzeniem przez nią konta na platformie e-PUAP (na potrzeby posługiwania się podpisem elektronicznym), jest znacznie szerszy niż tylko imię i nazwisko oraz numer PESEL. Obejmuje on bowiem również jej numer telefonu i adres poczty elektronicznej – art. 20ac ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[421]. Z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne nie wynika, aby ktoś poza administratorem – ministrem właściwym do spraw informatyzacji – mógł uzyskać poprzez proces logowania dostęp do danych zawartych w systemie teleinformatycznym zapewniającym obsługę publicznego systemu identyfikacji elektronicznej. Profil Zaufany to bezpłatna metoda potwierdzania tożsamości obywatela w systemach podmiotów publicznych, za pomocą której obywatel może załatwić prywatne sprawy urzędowe. Natomiast dla spraw służbowych, jak np. podpisywanie pism w imieniu urzędu, istnieją inne usługi, w szczególności kwalifikowany podpis elektroniczny czy też pieczęć elektroniczna.

[418] Wystąpienie Prezesa UODO z 17 czerwca 2019 r. do Ministra Cyfryzacji, sygn. ZSPU.023.97.2019.
[419] Wystąpienie Prezesa UODO z 26 kwietnia 2019 r. do Ministra Sprawiedliwości, sygn. ZSPU.023.53.2019.
[420] Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").
[421] Dz. U. z 2020 r. poz. 346 z późn. zm.

Podsumowując tę kategorię pytań prawnych podkreślenia wymaga, że dotyczyły one różnych aspektów przetwarzania danych osobowych – i to nie tylko w zakresie stosowania RODO, ale także innych, szczególnych przepisów prawa.

Przykładowo, **przychodnia weterynaryjna** miała wątpliwości, czy na wniosek policji może udostępnić dane osobowych właściciela/opiekuna psa, gdyż podstawa prawna w nim wskazana nie była precyzyjna. Pomimo bowiem tego, że ustawa z dnia 6 kwietnia 1990 r. o Policji[422] wyraźnie wskazuje na uprawnienia policji do uzyskiwania szeregu informacji od określonych podmiotów[423], to każdy administrator, w tym organy policji, powinien wskazać konkretną, szczegółową podstawę prawną swojego żądania o udostępnienie danych, tak aby administrator mający je udostępnić mógł podjąć właściwą decyzję w tej sprawie, bez narażenia się na odpowiedzialność z tego tytułu, w szczególności na podstawie RODO.

Podobnie jak w latach ubiegłych wpływały też pytania od **spółdzielni i wspólnot mieszkaniowych**, dotyczące m.in. legalności udostępniania danych osobowych członków wspólnoty mieszkaniowej, wykorzystywania mediów społecznościowych do komunikowania się w sprawach dotyczących funkcjonowania wspólnoty mieszkaniowej czy stosowania monitoringu.

Zdarzały się także nadinterpretacje przepisów o ochronie danych osobowych, gdy podmiot – nie chcąc udostępnić określonych informacji – odmowę w tej sprawie uzasadniał ochroną danych osobowych, np. **salon samochodowy** nie chciał udostępnić swojemu klientowi historii serwisowej pojazdu[424]**.** Prezes UODO przypominał wówczas, że – w sytuacji wątpliwości, czy określone informacje stanowią dane osobowe – podmiot mający je udostępnić powinien uwzględnić ochronę danych osobowych w fazie projektowania. RODO przewiduje bowiem tzw. pseudonimizację, która oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Pod warunkiem, że takie dodatkowe informacje będą przechowywane osobno i będą objęte środkami technicznymi

[422] Dz. U. z 2020 r. poz. 360 z późn. zm.
[423] Policja wykonując czynności, o których mowa w art. 14 (czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe) ma prawo m.in. do: żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielenia tej pomocy, w zakresie obowiązujących przepisów prawa oraz ma prawo do zwracania się o niezbędną pomoc do innych przedsiębiorców i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy, w ramach obowiązujących przepisów prawa (art. 15 ust. 1 pkt 6 i 7).
[424] DOL.023.451.2021.

i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 5 RODO).

Z kolei w innej sprawie **Starosta** odmówił deweloperowi farm fotowoltaicznych udostępnienia informacji na temat klasy bonitacyjnej gruntów znajdujących się w obrębie działek ewidencyjnych, uzasadniając to przepisami RODO[425]. Organ wskazywał wówczas, że określona informacja może stanowić daną osobową, jeśli na jej podstawie można zidentyfikować w sposób pośredni konkretną osobę (np. właściciela gruntu). Jeśli zaś taka identyfikacja jest niemożliwa, to analogicznie nie można owej informacji uznać za daną osobową.

Osoby fizyczne pytały, czy **operator telekomunikacyjny** może pozyskiwać ksero ich dowodu osobistego przy zawieraniu umowy o świadczenie usług telekomunikacyjnych. Organ wyjaśniał, że z przepisów ustawy Prawo telekomunikacyjne nie wynika konieczność dokonywania kserokopii dowodów osobistych abonenta, z czym dodatkowo związane jest pozyskanie szerszego zakresu danych osobowych, jak np. wizerunku[426].

Podobnie jak w latach poprzednich Prezes UODO otrzymywał pytania związane **z okresem publikowania wyników naborów w Biuletynie Informacji Publicznej** oraz z **pozyskiwaniem informacji z urzędów gmin w trybie dostępu do informacji publicznej**[427]. Wyrażał też opinię, co do **upublicznienia wizerunku osoby protokółującej obrady rady gminy** zarówno podczas transmisji, jak i na utrwalonym nagraniu posiedzenia. Wskazał, że działanie takie jest zgodne z prawem i nie wymaga wyrażania przez taką osobę zgody[428]. Prezes UODO zajął także stanowisko w sprawie **okresu przechowywania dokumentacji uczestników warsztatów terapii zajęciowej**[429].

Pojawiły się też zagadnienia całkiem nowe, nierozpatrywane wcześniej przez Prezesa UODO, jak np.: 1) sprawa zgłoszona przez Urząd Lotnictwa Cywilnego o wyrażenie opinii, co do sposobu weryfikacji kandydatów na uzyskanie kompetencji pilota bezzałogowego statku powietrznego[430]; 2) procedury zatwierdzania kodeksów postępowania; 3) wiodącego organu nadzorczego dla przedsiębiorców posiadających siedzibę poza UE zainteresowanych przyjęciem wiążących reguł

[425] DOL.023.804.2021.
[426] DOL.023.1052.2021.
[427] Np. DOL.023.45.2021.
[428] Więcej na ten temat w Newsletterze UODO dla IOD 3/2021.
[429] Newsletter UODO dla IOD 3/2021.
[430] DOL.023.15.2021.

korporacyjnych (WRK), czy też wątpliwości w zakresie procedury zatwierdzania WRK i wiele innych.

14.1.2. Pytania prawne od inspektorów ochrony danych

Rola inspektorów ochrony danych ma fundamentalne znaczenie dla budowy systemu skutecznej ochrony danych osobowych. Przejawia się ona m.in. w pełnieniu obowiązków punktu kontaktowego oraz pośrednika pomiędzy administratorem i organem nadzorczym. IOD z jednej strony udziela bowiem fachowego wsparcia administratorowi, co do sposobu wykonania ciążących na nim obowiązków nałożonych przepisami RODO, z drugiej strony – wspomaga go przed organem nadzorczym w wykazaniu zasadności wybranych rozwiązań, np. udzielając określonych informacji na żądanie organu nadzorczego. Jednocześnie IOD ma prawo zwrócić się do organu nadzorczego o udzielenie mu konsultacji nie tylko w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, ale również we wszelkich innych sprawach, co ma istotne znaczenie dla doskonalenia systemu ochrony danych osobowych.

Z tego względu Urząd Ochrony Danych Osobowych od wielu lat przykłada dużą wagę do współpracy z inspektorami ochrony danych, m.in. udzielając im konsultacji i porad. W 2021 roku inspektorzy chętnie korzystali z tej formy współpracy, czego wyrazem były kierowane do UODO liczne pytania związane z napotkanymi przez nich w codziennej pracy problemami, związanymi zarówno ze stosowaniem przepisów o ochronie danych osobowych, jak i innych regulacji prawnych dotyczących przetwarzania danych osobowych. Wątpliwości inspektorów nierzadko dotyczyły ich statusu i sposobu wykonywania zadań określonych w art. 39 RODO. Jednocześnie Urząd Ochrony Danych Osobowych oprócz udzielania odpowiedzi na pytania IOD, na bieżąco – wzorem lat ubiegłych – wzbogacał zakładkę „Inspektor Ochrony Danych" na stronie internetowej UODO (oraz „Newsletter UODO dla IOD") o nowe zagadnienia będące przedmiotem zgłaszanych przez inspektorów wątpliwości. Na stronie internetowej zamieszczane były również komunikaty i wskazówki dotyczące pojawiających się problemów w zakresie obowiązków związanych z wyznaczeniem IOD i jego funkcjonowaniem u administratorów i podmiotów przetwarzających, np. w zakresie wywiązywania się z obowiązku zgłaszania wyznaczenia IOD do Prezesa UODO, czy podawania danych inspektora do wiadomości osób, których dane dotyczą.

W 2021 roku do UODO wpłynęło **301 pytań od inspektorów ochrony danych**, tj. o 37 pytań mniej, niż w 2020 roku, w którym odnotowano 338 takich pytań. Nieznaczny spadek 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 specjalnej zakładce adresowanej inspektorom, stale uzupełnianej o nowe stanowiska przygotowane na podstawie wpływających do UODO pytań od inspektorów ochrony danych, a także w Newsletterze UODO dla IOD. Udzielone w poprzednich latach wyjaśnienia, będące odpowiedziami na pytania inspektorów, wskazywały kierunek i zasady interpretacji przepisów i obecnie posłużyły również jako wskazówki dla rozstrzygania nowych pojawiających się wątpliwości.

Pytania przesyłane przez inspektorów są dla organu nadzorczego bardzo ważne, ponieważ nie tylko dają wiedzę na temat stosowania przepisów prawa w praktyce przez administratora, podmiot przetwarzający i wspierających ich inspektorów ochrony danych, ale też pokazują obszary wymagające podjęcia działań o charakterze systemowym, np. legislacyjnym. Wątpliwości przedstawiane przez inspektorów pokazują m.in., że w niektórych kwestiach brakuje przepisów prawa albo że istniejące przepisy nie zawsze są spójne i jasne. Rozstrzyganie przez UODO wątpliwości pomaga inspektorom w prawidłowym realizowaniu ich obowiązków, zwłaszcza tych dotyczących wspierania administratora i podmiotu przetwarzającego poprzez doradzanie im, udzielanie konsultacji i prowadzenie działań szkoleniowych. To z kolei przyczynia się do wzrostu poziomu przestrzegania przepisów w zakresie ochrony danych osobowych przez administratorów i podmioty przetwarzające.

W 2021 roku wśród najczęściej poruszanych lub szczególnie interesujących zagadnień, na które zwrócili uwagę inspektorzy w przesłanych do Urzędu pytaniach, a które stały się przedmiotem analiz organu, były takie kwestie, jak:

1) określenie statusu podmiotów w procesie przetwarzania danych osobowych,
2) ustalenie przesłanek przetwarzania danych osobowych,
3) okres retencji danych osobowych,
4) obowiązki administratora lub podmiotu przetwarzającego określone w RODO,
5) wyznaczenie inspektora ochrony danych,
6) zawiadomienie Prezesa UODO o wyznaczeniu IOD,
7) status i zadania inspektora ochrony danych.

Określenie statusu podmiotów w procesie przetwarzania danych osobowych

W 2021 roku – podobnie jak w latach poprzednich – wiele wątpliwości przysparzało inspektorom ochrony danych właściwe określenie statusu podmiotów biorących udział w procesie przetwarzania danych osobowych. Ustalenie, czy w danym przypadku mamy do czynienia z administratorem, współadministratorem czy podmiotem przetwarzającym, było kluczowe 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.

Odpowiadając na te pytania, Urząd Ochrony Danych Osobowych powoływał się m.in. na wskazówki zawarte w wytycznych 7/2020 Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego[431]. Niejednokrotnie też wprost wskazywał kryteria pomocne w ostatecznej ocenie statusu i cele, które determinowały określone role. Wątpliwości inspektorów dotyczące właściwego określenia statusu podmiotów biorących udział w procesie przetwarzania danych osobowych dotyczyły zarówno podmiotów z sektora publicznego, jak podmiotów z sektora prywatnego.

14.1.2.1. Pytania IOD dotyczące statusu podmiotów z sektora publicznego

Mimo prezentowanych przez UODO wskazówek odnoszących się do określenia ról podmiotów uczestniczących w procesie przetwarzania danych osobowych, zagadnienie to w dalszym ciągu było często przedmiotem pytań IOD. Można przypuszczać, że wynika to ze sposobu ujęcia terminu „administrator" w przepisach o ochronie danych osobowych i konieczności dokonania szczegółowej analizy konkretnych sytuacji. Sprawy nie ułatwiały zmieniające się i nieprecyzyjne przepisy prawa.

Największe problemy z właściwym określeniem roli w procesie przetwarzania danych dotyczyły podmiotów z sektora publicznego, głównie **jednostek samorządu terytorialnego.**

Zgodnie z przyjętą w RODO definicją, pojęcie administratora ma bardzo szeroki zakres znaczeniowy, gdyż może nim być w zasadzie każdy podmiot, o ile ustala cele i sposoby przetwarzania danych osobowych. W zależności od danych osobowych, podstawy prawnej ich przetwarzania, a także kompetencji poszczególnych podmiotów (organów) do przetwarzania, administratorem może być zarówno organ, np. wójt lub burmistrz (prezydent), rada gminy, gminne jednostki organizacyjne (np. ośrodek pomocy społecznej lub szkoła), a także – w odniesieniu do danych pracowników

[431] Wytyczne po konsultacjach publicznych dostępne są na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/414/1714.

i kandydatów do pracy – gminna jednostka organizacyjna jaką jest urząd gminy. W odpowiedziach na te pytania akcentowano też zasadę legalizmu, zgodnie z którą działania takich podmiotów muszą mieć oparcie w przepisach prawa. Podkreślano, że w celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, czy jednak istnieje konieczność zawarcia umowy powierzenia, należy przede wszystkim dokonać analizy procesu przetwarzania z uwzględnieniem zadań określonych podmiotów wynikających m.in. z przepisów prawa czy z zawartej pomiędzy nimi umowy. Ocena ról w konkretnym przypadku zależy bowiem od tego, o jakie dane osobowe oraz o jakie zadania chodzi. W wielu sytuacjach, gdy następuje przekazanie zadania innemu podmiotowi, który realizuje je (także w zakresie przetwarzania danych) w sposób niezależny, stosując się w tym zakresie do szczegółowych przepisów, uzasadnione było uznanie tego podmiotu za odrębnego administratora. Natomiast powierzenie przetwarzania powinno mieć miejsce wówczas, jeśli zewnętrzny podmiot przetwarza dane w imieniu administratora i na jego polecenie, czyli w celach i w sposób przez niego określony. 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 potrzebna jest zawsze analiza konkretnych przepisów prawa. Poniżej przedstawiono przykłady pytań z tego zakresu.

Jeden z inspektorów zwrócił się z prośbą o udzielenie odpowiedzi na pytanie, **czy w jednostkach organizacyjnych samorządu terytorialnego funkcjonuje kilku odrębnych administratorów?**[432] Zastanawiał się, czy w takiej sytuacji należy opracować oddzielną dokumentację ochrony danych osobowych dla każdego z tych administratorów, czy też powinna to być dokumentacja uwzględniająca współpracę pomiędzy administratorami, a także czy należy powołać inspektora ochrony danych dla każdego z tych administratorów.

UODO, udzielając odpowiedzi na tak postawione pytania, przywołał definicję administratora zawartą w 4 pkt 7 RODO, zgodnie z którą „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. Określając status administratora w odniesieniu do konkretnego przetwarzania, należy uwzględniać element zarówno podmiotowy (tzn. administratorem może być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot), jak i to, że w przypadku podmiotów sektora publicznego (o ile podmiot będący administratorem nie jest wskazany wprost w konkretnym przepisie) najczęściej ma miejsce sytuacja, w której rola ta wynika

[432] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/2018.

z zakresu zadań publicznych, jakie przepisy mu przypisują i dla realizacji których niezbędne jest przetwarzanie danych. Na te elementy wskazywała również Grupa Robocza Art. 29 w Opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"[433] podkreślając, że konkretne stosowanie pojęcia administratora danych staje się obecnie coraz bardziej złożone, ze względu na zróżnicowanie form prawnych oraz organizacyjnych różnych podmiotów, które faktycznie decydują o celach i sposobach przetwarzania.

Taki sposób identyfikowania administratora podpowiadała również Europejska Rada Ochrony Danych w wytycznych EROD 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. Zgodnie z tymi wytycznymi, istnieją przypadki, w których administrator lub kryteria jego wyznaczania są wprost określone w przepisie prawa. Jednak bardziej powszechne są sytuacje, w których status ten wynika z tego, że ustawa nakłada na dany podmiot zadanie lub obowiązek gromadzenia i przetwarzania określonych danych. Wówczas administratorem jest zwykle organ wyznaczony na mocy prawa do realizacji tego zadania publicznego. W takim przypadku prawo, choć pośrednio, określa, kto jest administratorem. Innymi słowy prawo może nakładać na podmioty publiczne lub prywatne obowiązek przetwarzania określonych danych, a podmioty te uznawane są zazwyczaj za administratorów w odniesieniu do przetwarzania, które jest niezbędne do wykonania tego obowiązku (pkt 21–22 ww. wytycznych).

Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy przede wszystkim dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla realizacji których niezbędne jest przetwarzanie danych osobowych. Ocena ta powinna być dokonywana w odniesieniu do konkretnego procesu przetwarzania.

Tytułem przykładu, UODO wskazał, że art. 18 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym stanowi, że do właściwości rady gminy należą wszystkie sprawy pozostające w zakresie działania gminy, o ile ustawy nie stanowią inaczej. Natomiast art. 18 ust. 2 tej ustawy wskazuje na katalog zadań przypisanych do wyłącznej właściwości rady gminy. A zatem, w tych przypadkach, w których przepisy prawa wskazują, że określone zadania należą do właściwości rady gminy i dla ich wykonania niezbędne jest przetwarzanie określonych danych, należy uznać radę gminy za administratora tych danych. W omawianej odpowiedzi organ nadzorczy przypomniał, że takim sposobem identyfikowania administratora na podstawie norm, które określają zadania

[433] Opinia 1/2010 Grupy Roboczej Art. 29 w sprawie pojęć „administrator danych" i „przetwarzający", str. 11, dostępna pod linkiem https://archiwum.giodo.gov.pl/pl/1520057/3595.

podmiotu będącego administratorem, Prezes UODO (wcześniej GIODO) posługiwał się w wielu dotychczasowych decyzjach, ale też we wskazówkach i poradnikach publikowanych na stronie internetowej UODO[434].

Jako przykład podał artykuł „Realizacja autonomicznych uprawnień kontrolnych radnego" zamieszczony w Nr 9 Newslettera dla Inspektorów Ochrony Danych[435], gdzie wskazano, że radny, realizując zadania na rzecz rady gminy, nie będzie administratorem, tylko częścią organu kolegialnego, jakim jest rada. W takim przypadku to ona w związku z wykonywaniem swoich zadań ma status administratora. Natomiast z inną sytuacją mamy do czynienia wówczas, gdy radny wykonuje swoje autonomiczne uprawnienia kontrolne, o których mowa w art. 24 ust. 2 ustawy o samorządzie gminnym. Wówczas radny będzie odrębnym administratorem, gdyż to on będzie ustalał cele i sposoby przetwarzania danych osobowych pozyskanych w związku z tego typu swoją aktywnością.

Funkcjonowanie kilku administratorów w gminie uzasadnia fakt, iż jednostki organizacyjne samorządu terytorialnego i ich organy realizują różne zadania przypisane im na podstawie przepisów prawa. Przykładem takich złożonych sytuacji są np. wybory na ławników, gdzie do przetwarzania danych kandydatów na ławników i ławników – zgodnie z przepisami prawa – uprawnionych jest kilka podmiotów, a zatem wobec tych danych można wskazać kilku administratorów, m.in. radę gminy dokonującą wyboru oraz burmistrza jako organ zapewniający przeprowadzenie tych wyborów.

Organ nadzorczy podobne podejście prezentował również w innych odpowiedziach na pytania inspektorów zamieszczonych na stronie internetowej UODO w zakładce Inspektor Ochrony Danych/Zadania[436] oraz w Newsletterze UODO dla Inspektorów Ochrony Danych[437]. Jednocześnie podniósł, że istnienie w strukturach gminy, powiatu czy województwa więcej niż jednego podmiotu będącego odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych w odrębnych dokumentach dla każdego z administratorów. Jedna dokumentacja

[434] Decyzja w sprawie przetwarzania danych przez Burmistrza Aleksandrowa Kujawskiego dostępna pod linkiem: https://uodo.gov.pl/decyzje/ZSPU.421.3.2019, poradnik „Ochrona danych osobowych w kampanii wyborczej" dostępny pod linkiem: https://uodo.gov.pl/pl/138/497, poradnik „Ochrona danych osobowych w szkołach i placówkach oświatowych" dostępny pod linkiem: https://uodo.gov.pl/pl/201/481.

[435] Newsletter dla Inspektorów Ochrony Danych (wrzesień 2020), str. 7, dostępny pod linkiem: https://uodo.gov.pl/p/archiwum-newslettera-dla-iod.

[436] https://uodo.gov.pl/pl/225/1640, https://uodo.gov.pl/pl/225/1249, https://uodo.gov.pl/pl/225/1720, https://uodo.gov.pl/pl/225/1937.

[437] W Newsletterze UODO dla IOD, Wydanie 2 (maj 2019), str. 2, jako przykład funkcjonowania więcej niż jednego administratora w jednej jednostce organizacyjnej wskazano wojewódzką komisję do spraw orzekania o zdarzeniach medycznych oraz wojewodę, w związku z obsługą wniosków o ustalenie zdarzenia medycznego. Każdy z tych podmiotów uczestniczy w procesie przetwarzania danych osobowych w innym zakresie. W odniesieniu do tej sytuacji UODO wskazywał na współadministrowanie określone w art. 26 RODO.

może bowiem regulować kwestie ochrony danych dotyczące administratorów istniejących w ramach tej samej jednostki. Szerzej na ten temat UODO wypowiedział się w odpowiedzi na pytanie: *Czy kilku administratorów może mieć jedną dokumentację ochrony danych*?[438]

Przechodząc zaś do **obowiązku wyznaczenia inspektora ochrony danych**, np. przez radę gminy, organ nadzorczy wskazał, że na podstawie art. 37 ust. 1 lit. a RODO zobowiązane są do tego organy lub podmioty publiczne, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Natomiast zgodnie z brzmieniem art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych – który to przepis prawa krajowego określa kierunek interpretacji użytego w art. 37 ust. 1 lit. a RODO pojęcia „organ lub podmiot publiczny" – podmiotami zobowiązanymi do wyznaczenia inspektora ochrony danych osobowych są m.in. podmioty i organy publiczne, które są jednostkami sektora finansów publicznych. Zgodnie z art. 9 pkt 1 ustawy o finansach publicznych sektor finansów publicznych tworzą m.in. organy władzy publicznej.

Gdy w ramach danej jednostki organizacyjnej, np. urzędu gminy, działa kilku administratorów zobowiązanych do wyznaczenia IOD, mogą oni wyznaczyć do pełnienia tej funkcji jedną, tę samą osobę. Zgodnie z brzmieniem art. 37 ust. 3 RODO, jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych. Skorzystanie z takiego rozwiązania wymaga dokonania analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora. Jednocześnie przypomniano, że więcej informacji na ten temat zawarto w odpowiedzi na pytanie *Czy kierownik urzędu stanu cywilnego jest administratorem i czy musi wyznaczyć IOD?*[439]

Przykładem zagadnienia z sektora publicznego, które wciąż budziło wątpliwości, była sytuacja, gdy organ publiczny przekazywał swoje zadania innemu podmiotowi. W pytaniu, *czy ze związkiem powiatowo-gminnym należy zawrzeć umowę powierzenia?*[440] inspektor wskazał, że powiat i gminy powiatu utworzyły związek celowy powiatowo-gminny, który realizuje określone przepisami Prawa oświatowego zadanie gminy, polegające na zorganizowaniu bezpłatnego dowożenia dzieci objętych wczesnym wspomaganiem rozwoju i ich opiekunów z miejsca zamieszkania dziecka do szkoły lub placówki. Jego wątpliwości dotyczyły tego, czy w ww. przypadku będzie dochodziło do powierzenia przetwarzania danych osobowych uczniów między gminą i związkiem, czy raczej będzie tu miało

[438] https://uodo.gov.pl/pl/225/1937
[439] https://uodo.gov.pl/pl/223/1443
[440] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/2174.

miejsce udostępnienie danych osobowych. UODO, udzielając odpowiedzi, zwrócił uwagę, że w odniesieniu do opisanej przez inspektora sytuacji należy w pierwszej kolejności odwołać się do przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ponadto stwierdził, że co do zasady, jeżeli w danej jednostce organizacyjnej przekazuje się całość zadania na podmiot upoważniony, wówczas to ten podmiot realizuje to zadanie we własnym imieniu i staje się odrębnym administratorem[441].

14.1.2.2. Pytania IOD dotyczące statusu podmiotów z sektora prywatnego

Wątpliwości inspektorów, co do właściwego określenia statusu podmiotów uczestniczących w procesie przetwarzania danych, dotyczyły też podmiotów z sektora prywatnego, głównie relacji pracodawca a inny podmiot, ale także np. statusu komisji funkcjonujących w strukturze pracodawcy. W przypadku odpowiedzi na pytania o status podmiotów z sektora prywatnego UODO wskazywał przede wszystkim na decydujące znaczenie analizy stanu faktycznego, 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 można wskazać wiele przepisów prawa szczegółowo określających zadania, cele lub sposoby postępowania z danymi osobowymi w poszczególnych dziedzinach działalności zawodowej lub gospodarczej (przepisy branżowe). Takiej właśnie sytuacji dotyczyło pytanie inspektora: *Czy w przypadku PPE pracodawca powinien zawrzeć umowę powierzenia?*[442]

W odpowiedzi wskazano, że zasady tworzenia i działania pracowniczych programów emerytalnych, warunki, które powinny spełniać podmioty realizujące programy, oraz warunki uczestnictwa w tych programach, określone zostały w szczególności w ustawie z dnia 20 kwietnia 2004 r. o pracowniczych programach emerytalnych (ustawa o PPE).

Zgodnie z art. 10 ust. 1 ustawy o PPE program emerytalny tworzy się:

1) przez zawarcie umowy zakładowej albo umowy międzyzakładowej;

2) następnie przez zawarcie umowy z instytucją finansową, z zastrzeżeniem art. 17 ust. 3, albo utworzenie towarzystwa emerytalnego i funduszu emerytalnego albo nabycie przez pracodawcę akcji istniejącego towarzystwa emerytalnego;

3) następnie przez rejestrację programu przez organ nadzoru.

[441] Podobnie UODO wypowiedział się na temat tego zagadnienia w odpowiedzi na pytanie: *Kto jest administratorem danych przetwarzanych w celu wydania karty seniora*? (https://uodo.gov.pl/pl/225/1720).
[442] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1869.

Zgodnie z art. 17 ust. 1 ustawy o PPE, pracodawca zawiera umowę z instytucją finansową, która określa warunki gromadzenia środków i zarządzania nimi. W przypadku programu w formie funduszu emerytalnego, warunki gromadzenia środków i zarządzania nimi określa statut funduszu.

Kwestie dotyczące deklaracji o przystąpieniu do programu uregulowane zostały w art. 18 powyższej ustawy. Zgodnie z ust. 1 tego przepisu, przystąpienie pracownika do programu na warunkach określonych w umowie zakładowej następuje na podstawie deklaracji o przystąpieniu do programu, złożonej w postaci elektronicznej, pozwalającej na utrwalenie jej treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono, po upływie miesiąca od dnia jej złożenia. Chyba że pracodawca potwierdzi w postaci elektronicznej pozwalającej na utrwalenie treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono, przystąpienie do programu w terminie wcześniejszym. Deklaracja zawiera oświadczenie pracownika, że otrzymał kopię umowy zakładowej i zapoznał się z jej treścią, akceptuje jej warunki. Może także zawierać rozrządzenie na wypadek śmierci pracownika (art. 18 ust. 2).

Pracodawca przyjmuje deklarację i potwierdza uczestnikowi jej przyjęcie w postaci elektronicznej pozwalającej na utrwalenie treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono (art. 18 ust. 4). Jeżeli pracownikowi nie przysługuje prawo do uczestnictwa w programie, pracodawca zwraca deklarację wraz z uzasadnieniem odmowy jej przyjęcia w postaci elektronicznej pozwalającej na utrwalenie treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono (art. 18 ust. 5). Zgodnie z art. 20 ust. 1 ustawy o PPE, w sprawach dotyczących programu uczestnik składa oświadczenie woli pracodawcy lub za jego pośrednictwem w postaci elektronicznej pozwalającej na utrwalenie jego treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono.

Powyższe przepisy określają zadania każdego z podmiotów zaangażowanych w realizację programu, w tym zadania pracodawcy. W takiej sytuacji UODO wskazał, że zawieranie umowy powierzenia nie jest konieczne, ponieważ pracodawca realizuje tutaj swoje – określone przez ustawodawcę zadania – i w tym zakresie jest odrębnym administratorem.

Organ nadzorczy podkreślił, że niezależnie od tego w każdej konkretnej sytuacji trzeba analizować, czy w określonych procesach przetwarzania (w konkretnej relacji między pracodawcą a instytucją finansową) realizowane są tylko takie zadania (operacje na danych). Jeśli dane osobowe przetwarzane są również w innych celach, np. marketingowych, wówczas należy dokonać dodatkowo analizy w tym zakresie. Należy przede wszystkim ustalić, jakie dane są w tym celu przetwarzane,

przez które podmioty, a także którego z tych podmiotów cele są realizowane, a w związku z tym, który podmiot decyduje o celach i sposobach przetwarzania tych danych.

Inne pytanie dotyczyło tego, **jaki jest status komisji antymobbingowej?**[443], powołanej przez pracodawcę w myśl przepisów prawa pracy i czy można ją uznać za odrębnego administratora. UODO wskazał, że w celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, należy dokonać analizy konkretnych okoliczności i podstaw prawnych funkcjonowania określonego podmiotu. W pierwszej kolejności należy określić, czy, a jeżeli tak, to w jakich celach, komisja antymobbingowa działająca u pracodawcy przetwarza dane osobowe. W następnym kroku należy ocenić, kto ustala cele i sposoby przetwarzania danych. Należy przy tym wziąć pod uwagę podstawy prawne i zasady działania takiego podmiotu wynikające zarówno z powszechnie obowiązujących przepisów prawa, jak i regulacji wewnętrznych pracodawcy (np. zarządzenia, regulaminy). Jeśli chodzi o przepisy powszechnie obowiązujące, które dotyczą mobbingu, to będą to przepisy ustawy Kodeks pracy. Zgodnie z jej art. 94^3 § 2, mobbing oznacza działania lub zachowania dotyczące pracownika lub skierowane przeciwko pracownikowi, polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu pracownika, wywołujące u niego zaniżoną ocenę przydatności zawodowej, powodujące lub mające na celu poniżenie lub ośmieszenie pracownika, izolowanie go lub wyeliminowanie z zespołu współpracowników. Przeciwdziałanie mobbingowi należy do obowiązków pracodawcy (§ 1ww. przepisu).

Jak wskazano w komentarzu do tego przepisu[444], „co do sposobów realizacji tego obowiązku, to pracodawca może używać środków organizacyjnych i perswazyjnych, a gdy są one nieskuteczne, może stosować sankcje przewidziane w prawie pracy. Jak wynika z wyroku SN z 3.08.2011 r.[445], pracodawca powinien (…) przeciwdziałać mobbingowi, w szczególności szkoląc pracowników – informując o niebezpieczeństwie i konsekwencjach mobbingu czy stosując procedury, które umożliwią wykrycie i zakończenie tego zjawiska. Dobór właściwych środków uzależniony pozostaje od konkretnego pracodawcy, jak na przykład rodzaju środowiska pracy, charakteru i ilości interakcji między pracownikami, grożących wystąpieniem tego negatywnego zjawiska, wpływem rodzaju wykonywanej pracy". Jak zauważył organ nadzorczy, żaden przepis ustawowy nie zobowiązuje pracodawcy do powoływania komisji antymobbingowej, nie określa jej zadań ani sposobu rozpatrywania spraw, a jej powołanie stanowi zazwyczaj element polityki/procedury wewnętrznej

[443] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1938.
[444] Jaśkowski Kazimierz, Maniewska Eliza, Komentarz aktualizowany do Kodeksu pracy, Lex online.
[445] Sygn. akt I PK 35/11, opubl. OSNP 2012/19–20, poz. 238.

pracodawcy. Procedury takie określać mogą sposób zgłaszania niepożądanych praktyk, rozpatrywania skarg, a także organy powołane przez pracodawcę do prowadzenia takich spraw, ich skład i sposób wyboru (np. komisja antymobbingowa, pełnomocnicy, rzecznicy zaufania, mediatorzy). Pracodawcy mają zatem swobodę tworzenia i nazwania organu, który będzie prowadził takie postępowania. Zazwyczaj jest to kilkuosobowy zespół określany jako komisja antymobbingowa. Pracodawca może też zdecydować, czy powołuje komisję stałą czy będzie ona tworzona odrębnie do każdego postępowania wyjaśniającego, czy w składzie komisji będą tylko pracownicy firmy czy także zewnętrzni eksperci.

Dla jednoznacznej oceny, w jakiej roli występuje taka komisja w kontekście przepisów o ochronie danych osobowych, niezbędna jest znajomość konkretnych okoliczności faktycznych i prawnych. Jednak pomocniczo można odwoływać się do orzeczenia Sądu Apelacyjnego w Krakowie z 27 stycznia 2016[446], w którym stwierdzono, że komisje antymobbingowe powoływane każdorazowo przez pracodawcę do zbadania skarg pracowników, realizują w istocie zadania samego pracodawcy i stanowią „ramię" tego pracodawcy[447] w realizacji jego zadań, polegających na przeciwdziałaniu tym negatywnym zjawiskom w stosunkach pracy. Zatem to nie przepisy ustawy czy rozporządzeń wykonawczych, lecz sam pracodawca w uchwale Zarządu Spółki samodzielnie określił zasady, na jakich ma odbywać się przeciwdziałanie tym zjawiskom, określił skład, sposób wyboru członków komisji, wyznaczył jej kompetencję, zwolnił członków komisji z obowiązku świadczenia pracy w czasie jej posiedzeń, określił procedurę dochodzenia do końcowych wniosków, a także konsekwencje tych wniosków w zakresie poszczególnych stosunków pracy „pracowników obwinionych". Działalność tej komisji, cele dla których została powołana i procedura, w którą została wyposażona, stanowią wyłączną domenę pracodawcy, związaną z realizacją obowiązków tego pracodawcy wobec pracowników wynikających z przepisów kodeksowych (…). Podobnie do statusu komisji antymobbingowej odniósł się WSA w Gliwicach w wyroku z 11 grudnia 2019 r.[448] wskazując, że Dyrektor Szpitala Wojewódzkiego w postępowaniu występuje jako pracodawca, a komisja antymobbingowa jest jego ciałem pomocniczym.

Powyższe zatem przemawia za uznaniem, że komisja antymobbingowa samodzielnie nie ustala celów i sposobów przetwarzania danych osobowych, a tym samym nie spełnia kryteriów wymaganych dla kwalifikacji jej jako odrębnego administratora. Zgodnie z przytoczonymi powyżej

[446] Sygn. akt III APa 20/15.
[447] Zob. uchwała SN z 7 stycznia 1992 r. I PZP 62/91.
[448] Sygn. akt III SA/Gl 888/19.

orzeczeniami sądów, komisja taka stanowi organ pomocniczy pracodawcy, powoływany przez pracodawcę w celu realizacji jego zadań.

14.1.2.3. Inne pytania od IOD

Pytania dotyczące przesłanek przetwarzania danych osobowych

Duża cześć pytań wpływających od inspektorów dotyczyła wątpliwości związanych z określeniem właściwej przesłanki przetwarzania, w tym pozyskiwania i udostępniania, danych osobowych. Wskazanie właściwej podstawy prawnej, która odpowiada celowi i istocie przetwarzania ma zasadnicze znaczenie, jest niezbędne do zapewnienia przestrzegania zasady zgodności z prawem, rzetelności i przejrzystości określonej w art. 5 ust. 1 lit. a RODO. Kwestia ta jest również kluczowa z punktu widzenia spełnienia przez administratora innych obowiązków wynikających z przepisów RODO. Jest on bowiem zobowiązany wskazać podstawę prawną przetwarzania danych, nie tylko w związku z realizacją obowiązków informacyjnych z art. 13 i 14 RODO, ale również w prowadzonym przez siebie rejestrze czynności przetwarzania danych osobowych. Wiele pytań IOD dotyczyło określenia podstawy do przetwarzania danych przez pracodawców oraz przez uczelnie. Ich wątpliwości związane były m.in. z udostępnianiem danych osobowych innym podmiotom oraz możliwością powoływania się na przesłankę zgody w przypadku przetwarzania danych osobowych pracowników i studentów.

Pracodawcy często spotykają się z wnioskami o udostępnienie danych osobowych swoich pracowników i w takich przypadkach zobowiązani są do oceny, czy, a jeśli tak, to na podstawie której z przesłanek, powinni te dane udostępnić. Takiej sytuacji dotyczyło przesłane przez inspektora pytanie: *Czy komornikowi należy udostępnić dane w postaci numeru rachunku bankowego pracownika*?[449]

W pytaniu tym inspektor zwrócił się z prośbą o potwierdzenie aktualności stanowiska zawartego na archiwalnej stronie internetowej GIODO, dotyczącego udostępnienia komornikowi sądowemu informacji o numerze rachunku bankowego pracownika, na żądanie wniesione w trybie art. 761 § 1 Kodeksu postępowania cywilnego (K.p.c.). Zgodnie z przepisami RODO, podmiot może przetwarzać (w tym udostępniać) dane osobowe zwykłe po spełnieniu jednej z przesłanek określonych w art. 6 RODO. Jedną z nich jest sytuacja, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO).

[449] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1991.

W takim przypadku – jak stanowi ust. 3 tego artykułu – podstawa przetwarzania musi być określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator.

W przypadku żądania przez komornika określonych danych w toku prowadzonego przez niego postępowania, należy sięgnąć do właściwych przepisów (tu: przepisów prawa krajowego) określających jego uprawnienia. Podstawę prawną do pozyskiwania przez niego danych osobowych dłużnika stanowią przepisy ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, w tym art. 761 § 1^1 K.p.c. – powołany jako podstawa żądania komornika w zasygnalizowanej sytuacji. Przepis ten ustanawia przykładowy, niezamknięty katalog osób i instytucji, do których organ egzekucyjny może zwracać się o udzielenie informacji. Wśród tych podmiotów wskazano „inne instytucje i osoby nieuczestniczące w postępowaniu", do których można zaliczyć pracodawców. Podmioty te, na żądanie organu egzekucyjnego, zobowiązane są udostępnić informacje na temat stanu majątkowego dłużnika lub danych umożliwiających identyfikację składników jego majątku oraz danych adresowych w zakresie niezbędnym do zapewnienia prawidłowego toku postępowania. Do informacji takich może należeć numer rachunku bankowego dłużnika. Ocena, które informacje są niezbędne w konkretnym przypadku, należy do komornika. Zgodnie z art. 222 pkt 8 ustawy o komornikach sądowych, komornik odpowiada dyscyplinarnie za zawinione działania lub zaniechania (przewinienia dyscyplinarne), takie jak m.in. pozyskiwanie informacji z naruszeniem art. 761 § 1 K.p.c.

Od wykonania takiego żądania można uchylić się w takim zakresie, w jakim według przepisów części pierwszej Kodeksu można odmówić przedstawienia dokumentu lub złożenia zeznań w charakterze świadka albo odpowiedzi na zadane pytanie. Informacji udziela się w oparciu o dane przekazane przez organ egzekucyjny, w terminie przez niego wyznaczonym, o ile przepisy szczególne nie przewidują innego terminu (art. 761 § 2 i § 2^1 K.p.c.).

W przekazanych IOD wyjaśnieniach organ nadzorczy podniósł, że powołany w materiale zamieszczonym na stronie archiwalnej GIODO[450] art. 882 § 1 K.p.c. określa obowiązki pracodawcy w związku z zajęciem wynagrodzenia za pracę w ramach egzekucji prowadzonej przez komornika. Celem tego przepisu jest uregulowanie czynności zajęcia wynagrodzenia za pracę. Na podstawie tego przepisu komornik wzywa pracodawcę, aby w ciągu tygodnia: przedstawił za okres trzech miesięcy poprzedzających zajęcie, za każdy miesiąc oddzielnie, zestawienie periodycznego wynagrodzenia dłużnika za pracę oraz oddzielenie jego dochodu z wszelkich innych tytułów. Ponadto wzywa

[450] https://archiwum.giodo.gov.pl/318/id_art/3277/j/pl

pracodawcę, aby podał, w jakiej kwocie i w jakich terminach zajęte wynagrodzenie będzie przekazywane wierzycielowi oraz, w razie istnienia przeszkód do wypłacenia wynagrodzenia za pracę, złożył oświadczenie o rodzaju tych przeszkód, a w szczególności podał, czy inne osoby roszczą sobie prawa, czy i w jakim sądzie toczy się sprawa o zajęte wynagrodzenie i czy oraz o jakie roszczenia została skierowana do zajętego wynagrodzenia egzekucja przez innych wierzycieli. Natomiast po stronie pracodawcy istnieje obowiązek niezwłocznego zawiadomienia komornika oraz wierzyciela o każdej zmianie ww. okoliczności (na podstawie art. 882 § 2 K.p.c.).

Udostępnienie danych komornikowi w powyższych sytuacjach będzie następowało zatem w wykonaniu obowiązku nałożonego na administratora przepisem prawa, a więc na podstawie art. 6 ust. 1 lit. c RODO w połączeniu z właściwym przepisem procedury cywilnej, w zależności od tego, jaki cel lub podstawę prawną powołał komornik. Przy realizacji tego obowiązku należy pamiętać o przestrzeganiu zasady integralności i poufności danych określonej w art. 5 ust. 1 lit. f RODO, czyli 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.

Inne pytanie inspektora, które odnosiło się do wskazania **przesłanki będącej podstawą przetwarzania danych przez pracodawcę stosującego monitoring**[451] również dotyczyło potwierdzenia stanowiska UODO, po zmianie przepisów w 2019 roku, w zakresie podstawy przetwarzania danych osobowych pracownika w związku ze stosowaniem monitoringu w zakładzie pracy. UODO, wyjaśniając to zagadnienie, wskazał, że Kodeks pracy (K.p.) nie nakłada na pracodawcę obowiązku stosowania monitoringu, a jedynie daje mu taką możliwość. Skorzystanie z niej jest jednak obwarowane konkretnymi warunkami i może nastąpić wyłącznie w celach ściśle określonych w tym Kodeksie, a mianowicie:

– w przypadku monitoringu wizyjnego do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę (art. 22^{2} K.p.);
– w przypadku monitoringu poczty elektronicznej i innych form monitoringu do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy (art. 22^{3} § 1–4 K.p).

[451] Pytanie i odpowiedź dostępne pod linkiem: https://uodo.gov.pl/pl/225/2017.

W uzasadnieniu projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 wskazano, że celem wprowadzenia przepisów regulujących monitoring pracowników jest zabezpieczenie interesów pracowników przed dowolnym wykorzystywaniem monitoringu przez pracodawców. Dlatego uregulowano kwestię monitoringu w przepisach prawa oraz ograniczono możliwość wykorzystywania monitoringu do celów wskazanych w przepisach. Za przesłankę przetwarzania danych osobowych pracowników w związku ze stosowaniem monitoringu w powyższych celach i na warunkach określonych w Kodeksie pracy, UODO wskazał art. 6 ust. 1 lit. f RODO. Jednocześnie podkreślił, że powołanie się na tę przesłankę wymaga przeprowadzenia uprzedniej starannej oceny, określanej jako test równowagi. Jej istotą jest ustalenie, czy interes administratora (lub strony trzeciej), przemawiający za przetwarzaniem danych, jest prawnie uzasadniony, czy przetwarzanie jest niezbędne do realizacji celu wynikającego z tego interesu, a następnie rozważenie, czy interesy lub podstawowe prawa i wolności osoby, której dane dotyczą nie przeważają nad prawnie uzasadnionym interesem administratora lub strony trzeciej[452].

Możliwość stosowania monitoringu przez pracodawcę zachodzi wyłącznie, gdy cel przetwarzania nie może być osiągnięty za pomocą innych środków, które są mniej inwazyjne w stosunku do podstawowych praw i wolności osoby, której dane dotyczą. Pracodawca jako administrator powinien być w stanie wykazać zasadność jego stosowania, w tym proporcjonalność tego środka do celu, jakiemu ma on służyć. Powinien wiedzieć, jakie argumenty przeważają, by uznać, że monitoring jest lepszym środkiem niż inne dostępne służące temu samemu celowi oraz czy niepożądane negatywne skutki dla pracowników nie przeważają nad taką formą kontroli. Innymi słowy taka forma nadzoru może być stosowana po upewnieniu się, że inne środki prewencyjne czy ochrony są ewidentnie niewystarczające lub niemożliwe do zastosowania.

W odpowiedzi na zadane pytanie zaznaczono, że do kwestii monitoringu pracowników odnoszą się też inne dokumenty i materiały dostępne na stronie internetowej Urzędu[453].

Przykładem pytania IOD dotyczącego relacji między pracodawcą a pracownikiem było to, **czy pracodawca może pozyskiwać od pracownika informacje na temat powodów odejścia**

[452] Więcej na temat tego testu i materiałów przydatnych w jego przeprowadzeniu m.in. w odpowiedzi na pytanie: *Czy przesłanką przetwarzania przez organy publiczne może być art. 6 ust. 1 lit. f RODO*? (https://uodo.gov.pl/pl/225/2017).
[453] Opinia 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy (https://uodo.gov.pl/pl/10/2010), wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo (https://uodo.gov.pl/pl/414/1332), jak również materiały zmieszczone na stronie internetowej Urzędu: „Przetwarzanie danych osobowych na potrzeby zatrudnienia" – szkolenie dla IOD (https://uodo.gov.pl/pl/138/547). „Montujesz kamery w miejscu pracy. Sprawdź, o czym należy pamiętać" (https://uodo.gov.pl/pl/138/1634).

z pracy?[454] Jak wskazał inspektor ochrony danych, w celu podnoszenia jakości i poprawy warunków pracy oraz zaspokajania potrzeb pracowników, pracodawca chciałby mieć możliwość uzyskiwania od odchodzącego pracownika informacji na temat powodów jego decyzji i na tej podstawie zidentyfikować obszary wymagające poprawy. Wątpliwości inspektora dotyczyły tego, czy dopuszczalne jest pozyskiwanie takich informacji od pracownika oraz czy przetwarzanie takich danych pracowników można oprzeć na przesłance z art. 6 ust. 1 lit. f RODO.

W przedstawionej sytuacji w pierwszej kolejności należy odwołać się do przepisów Kodeksu pracy, ponieważ wskazują one, jakie informacje i w jakich celach pracodawca może pozyskiwać od pracownika. Zgodnie z art. 22^1 § 1 Kodeksu pracy, pracodawca żąda od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko; datę urodzenia; dane kontaktowe wskazane przez taką osobę; wykształcenie; kwalifikacje zawodowe; przebieg dotychczasowego zatrudnienia. Natomiast zgodnie z art. 22^1 § 3, pracodawca żąda od pracownika podania dodatkowo danych osobowych obejmujących: adres zamieszkania; numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość; inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy; wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie; numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych. Natomiast zgodnie z art. 22^1 § 4 Kodeksu pracy pracodawca może żądać podania innych danych osobowych pracownika niż określone w § 1 i 3, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Obowiązek taki może wynikać zarówno z przepisów Kodeksu pracy, jak i z odrębnych przepisów prawnych. Przykładem takiej sytuacji może być przekazanie danych kontaktowych, np. prywatnego adresu e-mail i numeru prywatnego telefonu, w związku z obowiązkiem zawarcia umowy o prowadzenie Pracowniczych Planów Kapitałowych z wybraną instytucją finansową. Pracodawca ma bowiem obowiązek prawny, wynikający z ustawy o pracowniczych planach kapitałowych, przekazania danych osobowych, m.in. w postaci adresu poczty elektronicznej i numeru telefonu od pracownika bez wyrażenia jego zgody do wybranej instytucji finansowej, o ile pracownik takie dane mu udostępni.

[454] Pytanie i odpowiedź dostępne pod linkiem: https://uodo.gov.pl/pl/225/2227.

W Kodeksie pracy uregulowane są również przypadki, gdy zgoda kandydata do pracy lub pracownika pozwala na przetwarzanie innych danych niż wymienione w przepisach Kodeksu pracy, z wyłączeniem danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych (art. 10 RODO). Należy jednak pamiętać, że zgoda taka musi odpowiadać wszystkim wymaganiom przewidzianym zarówno w RODO, jak i w przepisach Kodeksu pracy. W szczególności należy mieć na uwadze, że pracownik ma prawo w dowolnym momencie udzieloną zgodę wycofać. Ponadto brak zgody lub jej wycofanie nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę (22^{1a} § 2 Kodeksu pracy). Zgoda pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 RODO (np. danych dotyczących zdrowia) wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy pracownika (art. 22^{1b} § 1 Kodeksu pracy).

Odnosząc się natomiast do możliwości powołania się na art. 6 ust. 1 lit. f RODO, organ nadzorczy wskazał, że przyjęcie tej przesłanki jako podstawy pozyskiwania od pracowników informacji dotyczących „obiektywnych powodów rozwiązania stosunku pracy", wymagałoby wnikliwego rozważenia. Ponadto pozyskiwane od pracowników informacje mają dotyczyć powodów rozwiązania stosunku pracy, a te mogą być bardzo różne i nie można wykluczyć, że czasami będą one dotyczyć względów pozazawodowych, a zatem dotykać bezpośrednio lub pośrednio sfery życia osobistego pracownika, np. stanu zdrowia. Natomiast ww. przesłanka może być podstawą do przetwarzania wyłącznie tzw. danych osobowych zwykłych.

Podkreślenia wymaga, że w Opinii 2/2017 na temat przetwarzania danych w miejscu pracy[455] Grupa Robocza Art. 29 wskazała, że niekiedy pracodawcy mogą powołać się na uzasadniony interes, wskazując go jako podstawę prawną podejmowanych działań, pod warunkiem, że przetwarzanie danych jest bezwzględnie konieczne ze względów prawnych i zgodne z zasadami proporcjonalności i pomocniczości. A zatem administrator, który zamierza przetwarzać dane osobowe (w tym dane osobowe pracowników), powinien kierować się zasadą minimalizacji (art. 5 ust. 1 lit. c RODO), czyli gromadzić tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Jak wskazano w motywie 39 RODO, dane osobowe powinny być przetwarzane

[455] Opinia dostępna pod linkiem: https://uodo.gov.pl/pl/10/10.

wyłącznie w takich przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Wobec tego administrator, zanim podejmie decyzję o przetwarzaniu danych osobowych, powinien dokonać oceny, czy dane osobowe rzeczywiście są konieczne do osiągnięcia celu, czy nie istnieją inne, mniej inwazyjne, sposoby jego osiągniecia. Przetwarzanie danych w zakresie zbędnym dla osiągnięcia celu będzie sprzeczne z RODO.

Zastosowanie przesłanki z art. 6 ust. 1 lit. f RODO wymaga dokonania wcześniejszej starannej oceny, czy wskazane w niej kumulatywne warunki zostały spełnione. Zgodnie z art. 6 ust. 1 lit. f RODO, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – 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.

Po pierwsze należy ocenić, czy w konkretnej sytuacji występuje prawnie uzasadniony interes, który jest realizowany przez administratora lub przez stronę trzecią. Po drugie, niezbędna jest weryfikacja, czy przetwarzanie danych osobowych jest niezbędne dla realizacji celu wynikającego z prawnie uzasadnionych interesów. Następnie należy ocenić, czy nie jest spełniona przesłanka o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. W przypadku spełnienia tego warunku nie będzie można powołać się na przepis art. 6 ust. 1 lit. f, jako uzasadnienie dla przetwarzania danych osobowych. Stosowanie tej negatywnej przesłanki polega w istocie na wyważeniu dwóch dóbr chronionych prawem, tj. prawnie uzasadnionego interesu administratora lub strony trzeciej z jednej strony i interesów, podstawowych praw oraz wolności podmiotu danych z drugiej.

Zatem aby można było oprzeć się na art. 6 ust. 1 lit. f RODO jako podstawie prawnej przetwarzania, należałoby przeprowadzić ważenie ww. interesów, nazywane też testem równowagi.

Na potrzebę przeprowadzenia takiego testu przed rozpoczęciem przetwarzania oraz udostępnienia jego wyników osobom, których dane dotyczą, wskazywała również Grupa Robocza Art. 29 w wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679 (WP 260)[456]. Wskazano w nich m.in., że w ramach najlepszej praktyki administrator może również przedstawić

[456] Wytyczne dostępne pod linkiem https://uodo.gov.pl/pl/3/1343.

osobie, której dane dotyczą, informacje uzyskane w wyniku testu równowagi, który należy przeprowadzić, aby można było oprzeć się na art. 6 ust. 1 lit. f, jako podstawie prawnej przetwarzania, zanim jakiekolwiek dane osobowe osoby, której dane dotyczą, zostaną zebrane. (…) Jest to istotne dla skutecznej przejrzystości w przypadku, gdy osoby, których dane dotyczą, mają wątpliwości, czy test równowagi przeprowadzono rzetelnie lub chcą złożyć skargę do organu nadzorczego[457].

Inny z inspektorów zwrócił się z kolei z pytaniem, **jaka powinna być podstawa prawna przetwarzania danych osobowych osób wystawiających referencje?**[458] W procesie rekrutacyjnym administrator może otrzymać od kandydata, z jego inicjatywy, dokument referencji, w którym oprócz opinii o kandydacie mogą pojawić się dane osobowe wystawcy referencji, tj. imię, nazwisko, stanowisko, miejsce pracy, ewentualnie adres e-mail i telefon. Administrator nie ma możliwości pozyskania zgody wystawcy referencji, a zatem czy zasadne jest założenie, że przetwarzanie oparte jest na przesłance wynikającej z art. 6 ust. 1 lit. f RODO.

W odpowiedzi UODO poinformował, że w treści pytania słusznie wskazano, że podstawą przetwarzania danych osoby trzeciej udzielającej rekomendacji jest (przy spełnieniu warunków określonych w tym przepisie) art. 6 ust. 1 lit. f RODO. Prawnie uzasadniony interes pracodawcy związany będzie z możliwością wykorzystania informacji zawartych w treści referencji[459].

Jak już zostało wskazane wyżej, również inspektorzy pełniący swoją funkcję w szkołach wyższych zwracali się do UODO z pytaniami dotyczącymi określenia prawidłowej przesłanki przetwarzania. Jeden z nich pytał o to, **jaka jest podstawa przetwarzania danych studentów, którym udziela się pomocy materialnej?**[460] Uczelnia bowiem zamierzała utworzyć Biuro ds. Obsługi Osób Niepełnosprawnych, wspierające studentów w trudnych sytuacjach życiowych, w tym poprzez udzielanie pomocy materialnej bądź pomocy psychologicznej. Wątpliwości inspektora dotyczyły tego, czy w zaistniałych okolicznościach właściwą przesłanką przetwarzania danych osobowych może być zgoda.

---

[457] Również w wytycznych 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z artykułu 25 (https://uodo.gov.pl/pl/414/1331) Europejska Rada Ochrony Danych wskazała, że w przypadku gdy uzasadnione interesy stanowią podstawę prawną, administrator musi przeprowadzić ważenie interesów, ze szczególnym uwzględnieniem nierównowagi władzy, w szczególności dzieci poniżej 18 roku życia i innych grup znajdujących się w trudnej sytuacji. Wskazówki, w jaki sposób należy przeprowadzić test równowagi, znaleźć można m.in. w Opinii 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (https://archiwum.giodo.gov.pl/pl/1520203/7813).

[458] Pytanie i odpowiedź dostępne pod linkiem: https://uodo.gov.pl/pl/225/2051.

[459] Pomocne podpowiedzi związane ze złożeniem przez kandydata do pracy tzw. referencji można znaleźć w komunikacie pt. „ABC rekrutacji" (https://uodo.gov.pl/pl/138/1599).

[460] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/2019.

UODO wskazał, że zgodnie z przepisami RODO podmiot może przetwarzać dane osobowe wyłącznie wtedy, gdy istnieje podstawa prawna przetwarzania danych. Przetwarzanie tzw. danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6 RODO, a w przypadku szczególnej kategorii danych osobowych i danych osobowych dotyczących wyroków skazujących i czynów zabronionych, po spełnieniu przesłanek określonych w art. 9 i 10 RODO.
Jednym z praw studenta jest możliwość ubiegania się o przyznanie pomocy materialnej. W art. 86 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, zostały wskazane formy tej pomocy, tj. stypendium socjalne; stypendium dla osób niepełnosprawnych; zapomoga; stypendium rektora; stypendium finansowane przez jednostkę samorządu terytorialnego; stypendium za wyniki w nauce lub w sporcie finansowane przez osobę fizyczną lub osobę prawną niebędącą państwową ani samorządową osobą prawną. Właściwą przesłanką przetwarzania danych zwykłych w przypadku prowadzenia postępowania w celu przyznania pomocy materialnej studentowi przez uczelnię jest art. 6 ust. 1 lit. c RODO, a w przypadku danych szczególnej kategorii – art. 9 ust. 2 lit. g RODO w powiązaniu z art. 86 ustawy Prawa o szkolnictwie wyższym i nauce.

Odnosząc się zaś do pytania dotyczącego odbierania zgody na przetwarzanie danych osobowych przez Biuro w związku ze świadczeniem pomocy psychologicznej studentom oraz pomagania w trudnych sytuacjach życiowych, organ nadzorczy zaznaczył, że Europejska Rada Ochrony Danych w wytycznych z 4 maja 2020 r. dotyczących zgody[461] wskazała, że administratorzy, chcąc przetwarzać szczególne kategorie danych osobowych, w pierwszej kolejności powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b–j RODO. Jeżeli żaden z nich nie będzie miał zastosowania, wówczas jedyną możliwą przesłanką uprawniającą do przetwarzania takich danych jest uzyskanie wyraźniej zgody, spełniającej przewidziane w RODO warunki.

Wobec powyższego zanim administrator podejmie decyzję, aby opierać przetwarzanie szczególnych kategorii danych na zgodzie, powinien wcześniej dokonać analizy innych przesłanek.

Kolejnym zagadaniem budzącym wątpliwość inspektora pełniącego swą funkcję na uczelni było ustalenie**, jaka jest podstawa przetwarzania danych w przypadku monitoringu karier zawodowych studentów?**[462] Czy w tej sytuacji zastosowanie znajdzie przepis art. 352 pkt 14 ustawy Prawo o szkolnictwie wyższym i nauce, czy też w tym celu należy uprzednio pozyskać stosowne zgody od studentów bądź absolwentów.

[461] Wytyczne dostępne są na stronie Europejskiej Rady Ochrony Danych pod linkiem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl.
[462] Pytanie i odpowiedź są dostępne pod linkiem: https://uodo.gov.pl/pl/225/2138.

UODO przypomniał, że administrator będący podmiotem publicznym, oceniając, czy przetwarzanie danych jest dopuszczalne w określonej sytuacji, powinien przede wszystkim kierować się przepisami prawa odnoszącymi się do jego działalności. Podmioty publiczne, co do zasady, przetwarzają dane na podstawie i w granicach określonych przez przepisy prawa. W przypadku podmiotów publicznych – co do zasady – właściwymi podstawami do przetwarzania danych osobowych powinny być przesłanka określona w art. 6 ust. 1 lit. c i lit. e RODO w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji, a zatem gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Natomiast zgoda osoby, której dane dotyczą, może być odebrana przez podmiot publiczny w sytuacjach przewidzianych w przepisach prawa. Wynika to z zasady praworządności, zgodnie z którą podmioty publiczne działają na podstawie przepisów prawa i w jego granicach.

Tymczasem zgodnie z brzmieniem art. 352 ust. 14 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce „w celu dostosowania programu studiów do potrzeb rynku pracy, uczelnia może prowadzić własny monitoring karier zawodowych swoich absolwentów". Przepis ten nie nakłada na uczelnię obowiązku prowadzenia monitoringu karier, a jedynie daje jej taką możliwość. Wobec tego zasadne jest przyjęcie, że podstawą przetwarzania danych absolwentów uczelni wyższej w związku z monitorowaniem karier zawodowych absolwentów w celu dostosowania programu studiów do potrzeb rynku pracy, nie będzie art. 6 ust. 1 lit. c RODO, lecz art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Okres retencji danych osobowych

Kolejną grupę pytań IOD stanowiły zagadnienia związane z retencją danych. W każdej z udzielanych na nie odpowiedzi UODO wskazywał na zasadę wynikającą z art. 5 ust. 1 lit. e RODO, dotyczącą retencji danych. Wyjaśniał, że określenie terminu przechowania danych determinowane jest celem ich przetwarzania. Z kolei sam okres przetwarzania danych może być określony w przepisach prawa, a w sytuacji gdyby przepisy prawa nie określały okresu przechowywania określonych danych osobowych, administrator powinien stworzyć właściwe procedury określające termin ich usuwania.

Często inspektorzy pytali, **jakie dokumenty i przez jaki okres powinny być publikowane w BIP?**[463] W odniesieniu do wątpliwości, czy wnioski o udzielenie informacji publicznej składane w trybie ustawy o dostępie do informacji publicznej wraz z udzieloną odpowiedzią muszą być umieszczone na stronie urzędu, UODO wskazał, że podmiot zobowiązany do udostępnienia informacji publicznej, rozstrzygając o sposobie udostępnienia określonego zakresu danych w BIP, w pierwszej kolejności powinien ocenić, czy określone informacje mieszczą się w zakresie pojęcia informacji publicznej. Dokonując takiej oceny warto zapoznać się z orzecznictwem sądów administracyjnych, zwłaszcza zaś z wyrokami zawierającymi rozstrzygnięcia dotyczące tego, czy dokument prywatny (np. pismo strony wnoszone w sprawie administracyjnej) jest dokumentem urzędowym. Przykładowo w orzeczeniu I OSK 814/16 z dnia 26 stycznia 2018 r. NSA stwierdził: „zgodzić się należy ze stanowiskiem, że przymiot informacji publicznej bez wątpienia posiadają dokumenty urzędowe organu (będące dowodem tego, co w nich urzędowo stwierdzono, zatwierdzono lub podano), wytworzone w ramach realizacji powierzonych mu zadań, a więc dokumenty powstałe w związku z prowadzeniem konkretnych spraw. Natomiast przymiotu informacji publicznej nie mają dokumenty prywatne, które podmiot kieruje do organu administracji publicznej". Wobec tego w kontekście przepisów ustawy o dostępie do informacji publicznej inaczej należy traktować pismo strony postępowania (np. wniosek o dostęp do informacji publicznej), a inaczej treść dokumentu urzędowego, w rozumieniu art. 6 ust. 2 tej ustawy. Jeśli administrator oceni, że określona informacja stanowi informację publiczną, w następnym kroku powinien ocenić, czy prawo dostępu do takiej informacji nie podlega ograniczeniu, np. z uwagi na prywatność osoby fizycznej. Zgodnie z art. 5 ust. 2 u.d.i.p. prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy jednak informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz w przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. A zatem przepisy ustawy o dostępie do informacji publicznej wskazują na sytuacje oraz kategorie informacji, które mogą bądź muszą być wyłączone z udostępnienia.

Odnosząc się natomiast do kwestii obowiązku publikacji określonych informacji, UODO wskazał, że jedną z form udostępnienia informacji publicznej jest jej ogłaszanie w Biuletynie Informacji Publicznej (BIP), o którym mowa w art. 8 ust. 1 ustawy o dostępie do informacji

[463] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/2199.

publicznej. Katalog informacji podlegających obowiązkowemu udostępnieniu w BIP wskazany został w art. 8 ust. 3 tej ustawy. Niemniej organy władzy publicznej, do których zaliczają się również organy gminy, mogą udostępniać w Biuletynie także inne informacje publiczne, jak np. zarządzenia burmistrza (art. 8 ust. 3 zdanie drugie).

Ponadto prawo do informacji publicznej wynika również z art. 11b ustawy o samorządzie gminnym, który przewiduje jawność działalności organów gminy. Ograniczenia tej jawności mogą wynikać wyłącznie z ustaw (ust. 1). Zgodnie z tym przepisem jawność działania organów gminy obejmuje w szczególności prawo obywateli do uzyskiwania informacji, wstępu na sesje rady gminy i posiedzenia jej komisji, a także dostępu do dokumentów wynikających z wykonywania zadań publicznych, w tym protokołów posiedzeń organów gminy i komisji rady gminy (ust. 2). Zasady dostępu do dokumentów i korzystania z nich określa statut gminy (ust. 3). Jeżeli zatem w statucie gminy przewidziano obowiązek zamieszczania określonych informacji publicznych w BIP (np. zarządzeń burmistrza), to wtedy informacje te podlegają obligatoryjnemu zamieszczeniu na stronie BIP urzędu danej gminy. Opublikowanie przez Urząd określonych informacji powinno być zawsze poprzedzone staranną oceną, czy i w jakim zakresie należy je udostępnić.

Odnosząc się natomiast do kwestii okresu publikacji danych w BIP, organ nadzorczy zaznaczył, że przepisy ustawy o dostępie do informacji publicznej, a także przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej, nie precyzują okresu udostępniania informacji w BIP, zarówno minimalnego, jak i maksymalnego. Brak określonych przepisami prawa okresów przetwarzania (udostępniania) informacji zawierających dane osobowe, nie oznacza, że informacje takie można przetwarzać bezterminowo. Do takich informacji zastosowanie bowiem znajduje zasada ograniczonego przechowywania, wynikająca z art. 5 ust. 1 lit. e RODO. Administrator powinien w tym zakresie kierować się przepisami, z których wynika czas, przez jaki może przetwarzać dane osobowe, a w przypadkach, w których prawo nie reguluje okresu retencji danych, po przeprowadzeniu analiz, określić ten okres tak, aby przetwarzanie danych było zgodne z celami, w których je pozyskano. Stanowisko takie zaprezentowane zostało także w uzasadnieniu wyroku Wojewódzkiego Sądu Administracyjnego w Lublinie z 1 marca 2016 r.[464]: „[z] art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych wynika zasada ograniczenia czasowego udostępnienia danych osobowych w Biuletynie Informacji Publicznej. Zasada ta oznacza, że nawet jeśli określone dane odpowiadają celowi, dla

[464] Sygn. akt II SA/Lu 876/15.

którego są zbierane, to nie powinny być przetwarzane, w tym udostępniane innym podmiotom *ad finitum*. Czasowym wyznacznikiem powinno być natomiast osiągnięcie celu przetwarzania". Wyrok ten zachowuje aktualność także przy obecnie obowiązujących przepisach o ochronie danych osobowych.

Podobnie wypowiedział się WSA w Warszawie w wyroku z 29 stycznia 2020 r.[465], wskazując, że brak regulacji nie oznacza, że dane mogą być publikowane bezterminowo. W takiej sytuacji znajduje bowiem zastosowania art. 5 ust. 1 lit. e RODO, co w konsekwencji nakłada obowiązek dokonania samodzielnej oceny okresu niezbędnego do osiągnięcia celu przetwarzania oraz zakreślenia precyzyjnego terminu usunięcia danych osobowych z BIP.

UODO przypomniał również, że w decyzji z dnia 18 października 2019 r.[466] wskazano, iż w celu zapewnienia przetwarzania danych zgodnie z zasadą ograniczonego przechowywania, administrator powinien stworzyć procedury, z których będzie wynikał termin i sposób usuwania informacji zawierających dane osobowe oraz zasady dokonywania przeglądów przetwarzanych danych w celu weryfikacji, czy określone w ten sposób terminy usuwania danych osobowych są przestrzegane. Innymi słowy, jeżeli w tym zakresie brak jest określonych przepisami terminów, wzorów postępowania, to administrator musi przyjąć konkretne rozwiązania, które potrafi uzasadnić. Wynika to z przyjętej w art. 5 ust. 2 RODO zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych wymienionych w art. 5 ust. 1 RODO i musi być w stanie to wykazać. Zasada rozliczalności wymaga też, aby administratorzy wykazywali logikę, na której opierają swoje decyzje, i potrafili uzasadnić, dlaczego przyjęli określone rozwiązania[467].

Powyższe wyjaśnienia mogą być pomocne również w rozstrzygnięciu wątpliwości dotyczących skarg i wniosków w rozumieniu działu VIII K.p.a. Warto przy tym nadmienić, że problemem zamieszczania na stronie podmiotowej BIP danych osobowych wnoszącego taką skargę, zajął się m.in. Naczelny Sąd Administracyjny w wyroku z 14 marca 2013 r.[468] NSA stwierdził w nim, że „jeżeli celem zamieszczenia informacji publicznej w BIP-ie jest transparentność działalności publicznej rady gminy, w tym treść podejmowanych przez nią uchwał, to cel ten zostaje spełniony

[465] Sygn. akt II SA/Wa 1810/19.
[466] https://uodo.gov.pl/decyzje/ZSPU.421.3.2019
[467] Pomocne informacje dotyczące tego zagadnienia zawierają także odpowiedzi na pytania*: Czy trzeba precyzyjnie określać okres przechowywania danych?* (https://uodo.gov.pl/pl/225/1733), *Jak długo powinny być udostępniane w BIP oświadczenia majątkowe, np. radnego, wójta?* (https://uodo.gov.pl/pl/225/1130).
[468] Sygn. akt I OSK 620/12,

także wówczas, gdy chroniąc sferę prywatności z informacji usunięte zostaną dane dot. osób prywatnych".

Jeśli natomiast chodzi o petycje, to przy określaniu okresu przechowywania zastosowanie znajdą powyższe wskazówki. Nieco inaczej sytuacja wygląda natomiast w zakresie publikacji petycji i danych osobowych osób je wnoszących. Zgodnie bowiem z art. 4 ust. 3 ustawy o petycjach, petycja może zawierać zgodę na ujawnienie na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego danych osobowych podmiotu wnoszącego petycję lub podmiotu, o którym mowa w art. 5 ust. 1 tej ustawy. Zgodnie z art. 8 ust. 1 ww. ustawy, na stronie internetowej podmiotu rozpatrującego petycję lub obsługującego go urzędu, 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 była składana. Z treści powyższych przepisów wynika, że rozpatrujący petycję ma obowiązek zamieszczenia na swojej stronie internetowej informacji zawierającej odwzorowanie cyfrowe petycji, przy czym jeśli składający petycję wyrazi zgodę na ujawnienie jego imienia i nazwiska lub nazwy podmiotu, wówczas publikowana informacja o petycji może zawierać również te dane. Jeśli natomiast składający petycje nie udzieli takiej zgody, wówczas adresat petycji nie może ujawnić jego danych, nie może też żądać wyrażenia takiej zgody. W udzielonej odpowiedzi UODO zaznaczył, że podstawą prawną do ujawnienia danych osobowych osoby składającej petycję na stronie internetowej organu rozpatrującego, będzie zgoda w rozumieniu przepisów o ochronie danych osobowych. Skoro tak, to należy mieć na uwadze wymagania dotyczące zgody wskazane w RODO (art. 4 pkt 11 oraz art. 7–8)[469].

W kolejnej sprawie wątpliwości inspektora ochrony danych dotyczyły tego, **jak prawidłowo usuwać dane pozyskane dla przyznania Karty Dużej Rodziny**[470], w sytuacji gdy dana osoba utraciła prawo do posiadania Karty Dużej Rodziny, z wniosku oraz innych dokumentów potwierdzających jej prawo do przyznania Karty, gdy prawo to utraciła tylko jedna osoba, i czy w takiej sytuacji można dane wymazywać korektorem.

Zgodnie z zasadą ograniczenia przechowywania (retencji) sformułowaną w art. 5 ust. 1 lit. e RODO, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby,

[469] Więcej informacji na temat ww. przesłanki przetwarzania znaleźć można na stronie internetowej UODO, w tym m.in. w materiale *Zgoda nie zawsze jest podstawą przetwarzania danych,* https://uodo.gov.pl/pl/138/16380.
[470] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/2125.

której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których są one przetwarzane. Administrator zobowiązany jest zatem ustalić, przez jaki okres może posiadać dane osobowe przetwarzane w określonym celu oraz jakie czynności musi podjąć po upływie tego okresu. W odniesieniu do niektórych danych kwestia ta wynika wprost z przepisów prawa. Zgodnie z art. 21 ust. 4 ustawy o Karcie Dużej Rodziny, dane osobowe, o których mowa w ust. 1 tego artykułu, są przetwarzane przez okres 1 roku od dnia utraty prawa do korzystania z tego dokumentu, z wyjątkiem informacji dotyczących osób, którym Karta nie została przyznana, które przetwarza się przez okres 1 roku od dnia, w którym decyzja odmawiająca prawa do Karty stała się ostateczna. W myśl art. 21 ust. 5 ww. ustawy, dane osobowe, o których mowa w ust. 1 tego artykułu, wraz z wnioskiem o przyznanie Karty i dokumentami potwierdzającymi prawo do przyznania Karty, usuwa się niezwłocznie po upływie okresów przetwarzania, o których mowa w ust. 4. Odnosząc się do kwestii usuwania danych, wówczas gdy we wniosku o przyznanie karty zawarte byłyby – poza danymi osoby, która utraciła prawo do korzystania z Karty – dane innych osób uprawnionych nadal do korzystania z niej, UODO wskazał, że usuwanie niektórych danych (w tym przypadku danych dotyczących osoby, która utraciła prawo do korzystania z karty) z takiego wniosku, wydaje się działaniem niewłaściwym i wpłynęłoby na integralność tego dokumentu. Organ nie powinien ingerować w treść dokumentów, które otrzymuje od strony lub innego podmiotu. Jeżeli zatem prawo do korzystania z Karty traci jedna z osób ujętych we wniosku, wówczas taki wniosek powinien zostać usunięty dopiero wówczas, gdy wszystkie osoby, których dane ten wniosek zawiera, utracą prawo do korzystania z Karty. Organ nadzorczy zaznaczył też, że każda decyzja podjęta w tej materii przez administratora powinna uwzględniać zasadę rozliczalności sformułowaną w art. 5 ust. 2 RODO, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych określonych w ustępie 1 tego artykułu i musi być w stanie wykazać ich przestrzeganie. Pomocne w przestrzeganiu zasady ograniczenia przechowywania jest opracowanie i wdrożenie odpowiednich procedur związanych z usuwaniem danych osobowych.

Kolejnym zagadnieniem budzącym wątpliwości IOD było określenie okresu przechowywania w systemach informatycznych uczelni danych osób, które zostały przyjęte na studia, ale nie zostały studentami, gdyż nie złożyły ślubowania. W związku z tym IOD zadał pytanie, **jaki jest okres retencji danych zebranych w związku z rekrutacją na uczelnię wyższą?**

Kluczowe dla udzielenia odpowiedzi na tak sformułowane pytanie było określenie, w jakim celu, w systemach informatycznych uczelni, przetwarzane były dane osobowe osób, które

uczestniczyły w procesie rekrutacyjnym, ale nie zostały studentami uczelni. Czy ten cel związany był jedynie z rekrutacją, czy też w grę wchodziły jakieś inne cele. Po ustaleniu, w jakim konkretnie celu określone dane były przetwarzane w systemach informatycznych uczelni, należało dokonać analizy, kiedy ten cel zostanie osiągnięty. Zgodnie z 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; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu"). Określenie celów przetwarzania danych osobowych ma zatem bezpośredni wpływ na zapewnienie zgodności operacji przetwarzania danych z pozostałymi zasadami ochrony danych osobowych, takimi jak chociażby zasada minimalizmu, rzetelności i legalności oraz ograniczenia przechowywania. Z zasady ograniczenia przechowywania (retencji) sformułowanej w art. 5 ust. 1 lit. e RODO wynika natomiast, że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Zasada ta oznacza, że w każdym przypadku administrator musi ustalić, przez jaki okres może przetwarzać określone dane osobowe w określonym celu oraz jakie czynności musi podjąć po upływie tego okresu.

Kwestia ustalenia adekwatnego okresu przetwarzania jest kluczowa również z punktu widzenia spełnienia przez administratora innych obowiązków wynikających z przepisów RODO. Jest on zobowiązany wskazać okres, przez który dane osobowe będą przechowywane, w ramach realizacji obowiązków informacyjnych określonych w art. 13 ust. 2 i art. 14 ust. 2 RODO, oraz wskazać te okresy w prowadzonym przez siebie rejestrze czynności przetwarzania danych osobowych. Administrator powinien dokonać analizy dotyczących jego działalności przepisów prawa, które mogą przewidywać określony termin przechowywania danych do realizacji określonego celu przetwarzania (np. ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, których doprecyzowaniem jest instrukcja kancelaryjna, lub ustawy z dnia 29 września 1994 r. o rachunkowości). W przypadku, gdy prawo nie reguluje okresu przechowywania danych należy, przy uwzględnieniu ogólnych zasad wynikających z RODO, samodzielnie ustalić termin ich przechowywania biorąc pod uwagę cel przetwarzania. Brak określonych przepisami prawa okresów

przetwarzania informacji zawierających dane osobowe nie oznacza bowiem, że informacje takie można przetwarzać bezterminowo[471].

Zgodnie z art. 70 ust. 1 ustawy z dnia 20 lipca 2018 r. o szkolnictwie wyższym i nauce, uczelnia ustala warunki, tryb oraz termin rozpoczęcia i zakończenia rekrutacji oraz sposób jej przeprowadzenia. Artykuł ten stanowi delegację do określenia w uchwale Senatu uczelni, zasad i trybu rekrutacji, a także terminu rozpoczęcia i zakończenia rekrutacji na studia, jak również sposobu jej przeprowadzenia. Mając na uwadze, że przepisy ustawy nie zawierają szczegółowych regulacji dotyczących okresu przechowywania danych w związku z przeprowadzaną rekrutacją na studia, a jedynie odsyłają do ustalenia przez uczelnię szczegółów dotyczących tego procesu, trzeba samodzielnie określić okres przechowywania danych osobowych, również w odniesieniu do danych przetwarzanych w systemach informatycznych. Konieczne jest uwzględnienie, że w odniesieniu do określonych danych osobowych przetwarzanych przez uczelnię publiczną mogą mieć zastosowanie przepisy o narodowym zasobie archiwalnym i archiwach. Natomiast w sytuacji, gdy kandydat wniósł opłatę rekrutacyjną, przy ustaleniu okresu przechowywania danych należy także uwzględnić przepisy ustawy o rachunkowości (art. 74 tej ustawy).

Pomocne w przestrzeganiu zasady ograniczenia przechowywania jest opracowanie i wdrożenie odpowiednich procedur związanych z usuwaniem danych osobowych. W decyzji z dnia 18 października 2019 r.[472] UODO wskazał, iż w celu zapewnienia przetwarzania danych zgodnie z zasadą ograniczonego przechowywania, administrator powinien stworzyć procedury, z których będzie wynikał termin i sposób usuwania informacji zawierających dane osobowe oraz zasady dokonywania przeglądów przetwarzanych danych w celu weryfikacji, czy określone w ten sposób terminy usuwania danych osobowych są przestrzegane.

Warto wskazać, że UODO nie narzuca określonych wzorów postępowania, ale oczekuje od administratora przedstawienia argumentów, które przemawiają za przyjęciem określonych rozwiązań i wykazania spełnienia wynikających z RODO zasad, takich jak: zgodność z prawem, rzetelność i przejrzystość, celowość, minimalizacja danych, prawidłowość, integralność czy poufność. Powyższe wynika z określonej w art. 5 ust. 2 RODO zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie wymienionych w art. 5 ust. 1 RODO zasad dotyczących przetwarzania danych i musi być w stanie wykazać ich przestrzeganie. Zasada

[471] Tak też wskazano w odpowiedzi na pytanie: *Czy trzeba precyzyjnie określać okres przechowywania danych?* https://uodo.gov.pl/pl/225/1733.
[472] https://uodo.gov.pl/decyzje/ZSPU.421.3.2019

rozliczalności wymaga też, aby administratorzy wykazywali logikę, na której opierają swoje decyzje, i potrafili uzasadnić, dlaczego przyjęli określone rozwiązania.

Obowiązki administratora lub podmiotu przetwarzającego określone w RODO

Jednym z obowiązków administratora jest zapewnienie, aby miał kontrolę (władztwo) nad tym, kto, w jakim zakresie ma dostęp do danych osobowych oraz na jakich zasadach i w jaki sposób je przetwarza (art. 29 i art. 32 ust. 4 RODO). Jednym ze środków organizacyjnych służących temu celowi może być nadawanie upoważnień do przetwarzania danych osobowych.

Odnośnie tego zagadnienia organ nadzorczy wypowiadał się wielokrotnie na swojej stronie internetowej UODO, w specjalnej zakładce dedykowanej inspektorom. Wskazywał w szczególności, że wydawanie upoważnień może być jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem przetwarzania danych osobowych. Niemniej w 2021 roku nadal wpływały do Urzędu kolejne pytania od inspektorów dotyczące tego zagadnienia.

Przykładowo jeden z nich pytał, **czy inspektorowi ochrony danych należy nadawać upoważnienie do przetwarzania danych?** [473] Wskazał, że dostępne opinie na ten temat są sprzeczne. W opiniach opowiadających się przeciwko nadawaniu upoważnień inspektorom pojawiał się argument, że takie upoważnienia są zbędne ze względu na prawo inspektora do właściwego i niezwłocznego włączania go we wszystkie sprawy dotyczące ochrony danych osobowych u administratora oraz z uwagi na jego zadania określone w art. 39 ust. 1 RODO. Udzielając odpowiedzi na to pytanie, UODO wskazał, że przede wszystkim należy wziąć pod uwagę cel, w jakim takie upoważnienia się nadaje. Mogą być one jednym ze środków organizacyjnych, którego celem jest zapewnienie przez administratora odpowiedniej kontroli nad procesem przetwarzania danych.

Przepisy RODO zobowiązują administratora, aby miał kontrolę (władztwo) nad tym, kto, w jakim zakresie ma dostęp do danych osobowych oraz na jakich zasadach i w jaki sposób je przetwarza. Dane osobowe mogą być przetwarzane wyłącznie na polecenie administratora przez osoby działające z upoważnienia administratora lub podmiotu przetwarzającego (art. 29 oraz art. 32 ust. 4). Przyjmowane przez administratora i podmiot przetwarzający środki wobec osób, za których działania administrator i podmiot przetwarzający odpowiadają, powinny służyć m.in. zapobieganiu nieuprawnionemu pozyskiwaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych. Dzięki tym środkom osoby, które zostały

[473] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1939.

dopuszczone do przetwarzania danych, zostają również poinformowane, jaki jest zakres ich uprawnień, co do przetwarzania danych osobowych. Dlatego środek ten należy odróżnić od uprawnienia dostępu do danych osobowych przyznanego określonym funkcjom czy zawodom przez przepisy prawa w związku z wykonywanymi przez nich obowiązkami lub zadaniami. Patrząc z tej perspektywy, jeżeli administrator decyduje się na skorzystanie ze środka, jakim jest nadawanie upoważnień do przetwarzania danych w wykonaniu obowiązków określonych w art. 29 i art. 32 ust. 1 i 4 RODO, to taki środek uzasadniony jest również wobec inspektora ochrony danych, niezależnie od tego, że jego uprawnienie dostępu do danych osobowych wynika z RODO[474].

Wyznaczenie inspektora ochrony danych

W 2021 roku nie wpływały już pytania, czy w danym podmiocie należy wyznaczyć inspektora ochrony danych. Natomiast liczne kierowane do Urzędu pytania dotyczyły wyznaczenia zewnętrznego inspektora ochrony danych. Problematyczne okazało się ustalenie, czy z takim zewnętrznym inspektorem ochrony danych należy zawrzeć umowę powierzenia, oraz to, czy taki zewnętrzny inspektor ochrony danych może świadczyć swoje usługi w banku.

Ze względu na liczne i różne interpretacje prawne dotyczące tego zagadnienia, organ nadzorczy zajął stanowisko w tej materii, udzielając odpowiedzi na pytanie inspektora, **czy z zewnętrznym IOD należy zawrzeć umowę powierzenia?**[475] Wskazał w niej, że wykonywanie zadań IOD przez osobę, która nie jest członkiem personelu administratora, powinno następować na podstawie umowy o świadczenie usług niebędącej umową powierzenia danych. Art. 37 ust. 6 RODO wskazuje wprost, iż inspektor ochrony danych może wykonywać swoje zadania na podstawie umowy o świadczenie usług, czyli nie musi być on pracownikiem administratora. Dopuszczalny jest zatem outsourcing tej funkcji, przy czym przedmiotem umowy z inspektorem nie są zadania administratora, tylko zadania wskazane w art. 39 ust. 1 RODO. Umowa o świadczenie usług, której przedmiotem jest wykonywanie zadań IOD, nie będzie umową powierzenia przetwarzania. Konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator w celu realizacji swoich celów (zadań) związanych z przetwarzaniem danych posługuje się innym, zewnętrznym podmiotem. Innymi słowy, powierzenie przetwarzania powinno mieć miejsce w przypadkach, gdy administrator prowadzący działalność w określonej dziedzinie ma potrzebę

[474] Analogiczne podejście i więcej informacji na temat upoważnień do przetwarzania danych można znaleźć na stronie internetowej UODO w zakładce Inspektor Ochrony Danych/Zadania IOD, m.in. w odpowiedziach na pytania: *Czy administrator powinien nadawać upoważnienia np. sędziom?* (https://uodo.gov.pl/pl/225/1276), *Czy lekarzom należy nadawać upoważnienia?* (https://uodo.gov.pl/pl/225/1578).
[475] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/223/2050.

skorzystania z pomocy zewnętrznych specjalistów, których usługi będą miały charakter pomocniczy, nierzadko techniczny, wspierający działalność główną administratora. Podmiot przetwarzający jest zobowiązany do stosowania się do instrukcji przekazanych przez administratora co najmniej w odniesieniu do celu przetwarzania oraz istotnych elementów sposobu przetwarzania. Najczęściej występujące przykładowe usługi świadczone w modelu powierzenia wskazane zostały w Poradniku: „Wskazówki i wyjaśnienia dotyczące obowiązku z art. 30 ust. 1 i 2 RODO”[476], jako 1) przechowywanie danych klienta (administratora) rozumiane jako udostępnienie zamawiającemu określonej przestrzeni dyskowej w infrastrukturze przetwarzającego na przechowywanie danych, którymi zlecający (administrator) sam zarządza i decyduje o tym, jakie dane tam przechowuje – np. wykonuje kopie zapasowe danych elektronicznych; 2) udostępnianie klientowi (administratorowi) mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej lub innych usług na potrzeby instalacji i eksploatacji usług przetwarzania, którymi zamawiający w pełni zarządza – dostarczanie infrastruktury informatycznej; 3) udostępnienie klientowi (administratorowi) określonej platformy programistycznej (np. serwera www wraz z odpowiednim oprogramowaniem do prowadzenia własnej strony internetowej); 4) wykonywanie na zamówienie klienta (zamawiającego) określonych usług w zakresie konfiguracji sprzętowej, programowej, w tym zabezpieczeń udostępnionych mu serwerów, innych urządzeń komputerowych oraz oprogramowania – usługi administracyjne i konserwacyjne; 5) wykonywanie na zamówienie klienta (zamawiającego) usług programistycznych, w tym aktualizacji oprogramowania na okoliczność zmieniających się przepisów prawnych lub wymagań klienta – usługi programistyczne, itp. 6) samo przechowywanie dokumentacji podatkowej, księgowej, kadrowej i medycznej; 7) prowadzenie dokumentacji podatkowej, księgowej, kadrowej; 8) archiwizacja danych elektronicznych; 9) skanowanie i digitalizacja danych; 10) niszczenie nośników informacji[477].

Natomiast przedmiotem umowy o świadczenie usług, o której mowa w art. 37 ust. 6 RODO, powinny być zadania wskazane w art. 39 ust. 1 RODO, realizowane przy spełnieniu warunków określonych w przepisach tego aktu, w sposób gwarantujący inspektorowi niezależność. Administrator i podmiot przetwarzający mają m.in. obowiązek zapewnić, aby inspektor nie

[476] Poradnik dostępny jest pod linkiem: https://uodo.gov.pl/pl/383/214.

[477] Inne przykłady przypadków uzasadniających skorzystanie z konstrukcji powierzenia przetwarzania danych można znaleźć np. w odpowiedzi na pytanie: *Czy przekazanie dokumentacji do fumigacji powoduje konieczność zawarcia umowy powierzenia?* (https://uodo.gov.pl/pl/225/1467); *Czy w celu wytworzenia legitymacji należy skorzystać z powierzenia przetwarzania?*(https://uodo.gov.pl/pl/225/1642); *Czy po wejściu stosowania RODO CUW może powołać jednego IOD dla wszystkich obsługiwanych jednostek* (https://uodo.gov.pl/pl/225/660); *Czy świadczenie usługi kolokacji implikuje konieczność zawarcia umowy powierzenia?* (Newsletter UODO dla IOD, wydanie 3, marzec 2020, str. 5).

otrzymywał instrukcji dotyczących wykonywania swoich zadań (art. 38 ust. 4 RODO). Dostęp do danych osobowych niezbędnych (zewnętrznemu) IOD do wykonywania jego zadań wynika z przepisów prawa. Art. 38 ust. 2 RODO stanowi, że administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu m.in. dostęp do danych osobowych i operacji przetwarzania. W kontekście dostępu do danych należy podkreślić, że ust. 5 ww. artykułu zobowiązuje IOD do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. Warto pamiętać, że możliwość wykonywania przez osobę, z którą zawierana jest umowa o świadczenie usług, zadań innych niż określone w RODO, ograniczona jest zakazem występowania w tym zakresie konfliktu interesów (art. 38 ust. 6 RODO).

W analizowanej odpowiedzi organ nadzorczy zaznaczył, że Grupa Robocza Art. 29 w wytycznych dotyczących inspektorów ochrony danych (WP 243) podkreśliła, że w przypadku gdy funkcję IOD pełni osoba spoza organizacji administratora – biorąc pod uwagę fakt, iż IOD posiada wiele zadań – administrator albo podmiot przetwarzający musi mieć pewność, że jeden IOD, z zespołem, jeśli jest to niezbędne, pozytywnie wypełni swoje obowiązki pomimo wyznaczenia go dla kilku podmiotów i organów publicznych (str. 11–12 wytycznych). W odpowiedzi na pytanie: *Czy podmioty publiczne mogą powołać jednego IOD poza sytuacją uregulowaną w art. 37 ust. 3 RODO?*[478]*,* UODO wyjaśnił, że skorzystanie z rozwiązania określonego w art. 37 ust. 3 RODO wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora. Trzeba mieć przy tym świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. efektywnej dostępności inspektora dla osób z danej organizacji[479].

Z kolei w odpowiedzi na pytanie inspektora, **czy z zewnętrznym IOD wykonującym zadania dla banku należy zawrzeć umowę powierzenia?[480],** UODO wskazał, że w przypadku gdy administratorem jest bank, w pierwszej kolejności należy mieć na uwadze, że prawidłowe wykonywanie zadań przez IOD wiąże się z zapewnieniem mu dostępu do danych objętych tajemnicą bankową.

[478] https://uodo.gov.pl/pl/223/658
[479] Więcej na ten temat znajduje się pod linkami: https://uodo.gov.pl/pl/223/655, https://uodo.gov.pl/pl/223/658, https://uodo.gov.pl/pl/223/707.
[480] Pytanie i odpowiedź dostępne pod linkiem: https://uodo.gov.pl/pl/223/2091.

Zgodnie z RODO, administrator zobowiązany jest zapewnić, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Musi on również wspierać inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania (art. 38 ust. 1 i 2 RODO). A zatem do prawidłowego wykonywania zadań IOD niezbędny jest dostęp do informacji dotyczących przetwarzania danych osobowych, do samych danych osobowych, jak i operacji przetwarzania. Dlatego warto rozważyć, czy najlepszym rozwiązaniem nie byłoby wyznaczenie do pełnienia funkcji IOD pracownika banku. Jeśli miałaby to być osoba wykonująca obowiązki na podstawie umowy o świadczenie usług, to do umowy takiej zastosowanie powinien mieć art. 6a ust. 1 pkt 2 ustawy Prawo bankowe, który umożliwi zapoznanie się przez IOD z informacjami objętymi tajemnicą bankową. Jak wskazuje art. 104 ust. 2 pkt 2 lit. a Prawa bankowego, obowiązek zachowania tajemnicy bankowej, o którym mowa w art. 104 ust. 1 tej ustawy, nie dotyczy przypadków, w których bank, zgodnie z art. 6a ust. 1 i art. 6b–6d, powierzył wykonywanie, stale lub okresowo, czynności związanych z działalnością bankową. Przy czym podmioty oraz osoby w nich zatrudnione, którym zgodnie z m.in. przepisem art. 104 ust. 2 pkt 2 lit. a Prawa bankowego udzielono lub ujawniono informacje objęte tajemnicą bankową, mogą wykorzystać te informacje wyłącznie w celu zawarcia i wykonania umów, o których mowa m.in. w ust. 2 pkt 2 lit. a Prawa bankowego (art. 104 ust. 5 Prawa bankowego). Ponadto zgodnie art. 38 ust. 5 RODO, inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań zgodnie z prawem Unii lub prawem państwa członkowskiego. Wykonywanie zadań IOD przez osobę, która nie jest członkiem personelu administratora, powinno następować na podstawie umowy o świadczenie usług niebędącej umową powierzenia danych. Art. 37 ust. 6 RODO wskazuje wprost, iż inspektor ochrony danych może wykonywać swoje zadania na podstawie umowy o świadczenie usług, czyli nie musi być on pracownikiem administratora (banku). Dopuszczalny jest zatem outsourcing tej funkcji, przy czym przedmiotem umowy z inspektorem nie są zadania administratora, a zadania wskazane w art. 39 ust. 1 RODO.

Zawiadomienie Prezesa UODO o wyznaczeniu IOD

W 2021 roku do UODO wpływały liczne pytania dotyczące tego, czy administrator skutecznie powiadomił Prezesa UODO o wyznaczeniu IOD. Organ nadzorczy od czasu wejścia w życie przepisów RODO wielokrotnie podkreślał na stronie internetowej Urzędu (w komunikatach czy też w Zakładce IOD), że jedynym prawidłowym i skutecznym sposobem zawiadomienia Prezesa UODO o wyznaczeniu inspektora ochrony danych jest zawiadomienie w postaci elektronicznej (zgodnie

z art. 10 ust. 6 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz z art. 46 ust. 9 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości). W analogiczny sposób należy także przesyłać zawiadomienia dotyczące zastępcy inspektora ochrony danych (art. 11a ust. 3 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz art. 46 ust. 6 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości). Oznacza to, że należy skorzystać z właściwego formularza elektronicznego, tj. dotyczącego IOD bądź zastępcy IOD, jak również uzależnionego od podstawy powołania IOD przez danego administratora. Administratorzy wyznaczający IOD na podstawie art. 37 ust. 1 RODO (częściowo doprecyzowanego w art. 9 ustawy o ochronie danych osobowych) powinni skorzystać z formularzy oznaczonych jako RODO, natomiast administratorzy wyznaczający IOD na podstawie ustawy z dnia 14 grudnia 2018 r. powinni skorzystać z formularzy DODO. Ponadto wypełniony formularz musi zostać opatrzony kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP osoby uprawnionej do reprezentowania administratora. W zawiadomieniu należy podać wszystkie wymagane przepisami prawa informacje. Do zawiadomienia składanego przez pełnomocnika należy załączyć pełnomocnictwo udzielone w formie elektronicznej oraz opłatę skarbową od pełnomocnictwa (chyba że przepisy zwalniają od jej uiszczenia).

Mimo licznych wyjaśnień przedstawianych w tej materii przez organ nadzorczy dostrzec można, że najczęściej popełnianymi błędami przy przesyłaniu zawiadomień dotyczących IOD było:

- przesłanie zawiadomienia w postaci papierowej, np. drogą listowną zamiast w postaci elektronicznej, która jest jedyną prawidłową postacią zawiadomienia, zgodnie z przepisami o ochronie danych osobowych;
- przesłanie pisma przewodniego bez formularza zawiadomienia;
- przesłanie zawiadomienia na niewłaściwym formularzu (np. szkoła przesłała zawiadomienie na formularzu przeznaczonym dla organów przetwarzających dane na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości);
- przesłanie zawiadomienia dotyczącego zastępcy IOD na niewłaściwym formularzu (np. przesłanie zawiadomienia na formularzu dotyczącym IOD);
- nieprzedstawienie pełnomocnictwa bądź załączenie do zawiadomienia pełnomocnictwa bez zachowania jego formy elektronicznej, np. scan pełnomocnictwa nieopatrzony kwalifikowanym

podpisem elektronicznym, podpisanie pełnomocnictwa przez jednego członka zarządu, gdy z reprezentacji w KRS wynika reprezentacja np. dwuosobowa.

W sytuacji gdy zawiadomienie zawiera błędy, konieczne jest jego ponowne przesłanie. Organ nadzorczy dostrzegając pojawiające się błędy, zwłaszcza związane z dokonywaniem zawiadomienia dotyczącego IOD przez pełnomocnika, postanowił jeszcze raz przybliżyć i wyjaśnić zasady prawidłowej realizacji tego obowiązku. Znalazły się one w Newsletterze dla IOD nr 11/2021 w materiale: **„Wielu pełnomocników błędnie, a przez to nieskutecznie, zawiadamia o wyznaczeniu IOD”**[481].

Status i zadania inspektora ochrony danych

Udzielanie odpowiedzi na pytania dotyczące statusu inspektora ochrony danych 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.

UODO zwrócił uwagę na określony w art. 38 ust. 2 RODO obowiązek administratora (podmiotu przetwarzającego) zapewnienia wsparcia IOD poprzez dostarczanie mu niezbędnych zasobów do wykonania jego zadań oraz dostępu do danych osobowych i operacji przetwarzania, a także zasobów niezbędnych do utrzymania jego wiedzy fachowej również w sytuacji, gdy inspektor wykonuje zadania na podstawie umowy o świadczenie usług. Przynosi to niewątpliwe korzyści dla administratorów (podmiotów przetwarzających), którzy – wspierani przez odpowiednio wykwalifikowanego inspektora – są w stanie sprostać wymogom, jakie nakładają na nich przepisy prawa.

Na kwestie dotyczące obowiązku administratora (podmiotu przetwarzającego) do zapewnienia IOD niezbędnych zasobów, UODO zwrócił uwagę w odpowiedzi na pytanie, **czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD?**[482] Podkreślił, że RODO nakłada na administratora (kierownictwo podmiotu będącego administratorem) określone, bardzo konkretne obowiązki wobec funkcjonującego w jego organizacji inspektora ochrony danych, a sposób ich realizacji zależy od specyfiki danego administratora (m.in. jego wielkości, struktury, rodzaju działalności) i prowadzonego przez niego przetwarzania danych (m.in. charakter, zakres, kontekst i cele przetwarzania). W zależności od tych czynników administrator musi zapewnić IOD

[481] Newsletter dla IOD dostępny jest pod linkiem: https://uodo.gov.pl/p/archiwum-newslettera-dla-iod.
[482] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/223/2049.

właściwe warunki funkcjonowania i to administrator odpowiedzialny jest za skuteczne i prawidłowe wykonywanie przez inspektora jego zadań. Takim konkretnym obowiązkiem nałożonym na administratora jest udzielanie IOD wsparcia w wypełnianiu przez niego zadań (o których mowa w art. 39 RODO), zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej zgodnie z art. 38 ust. 2 RODO. Grupa Robocza Art. 29 w wytycznych dotyczących inspektora ochrony danych[483] opowiada się za szerokim rozumieniem zasobów, do których zalicza m.in.: wsparcie kadrowe, np. powołanie zespołu inspektora ochrony danych. Dodać należy, że przez zasoby, które powinien zapewnić administrator można rozumieć również:

– wsparcie IOD ze strony kadry kierowniczej (np. na poziomie zarządu);

– wymiar czasu umożliwiający IOD wykonywanie zadań;

– odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie);

– oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia IOD i poinformowanie o jego zadaniach;

– umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT itd.;

– ciągłe szkolenie. IOD powinien mieć możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Celem powinno być zwiększanie wiedzy IOD i zachęcanie go do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych itd.

Administrator, wyznaczając na inspektora daną osobę, powinien wspólnie z nią określić zasady dotyczące zapewnienia jej wystarczającej ilości czasu na wypełnianie obowiązków IOD, pomocy w stworzeniu planu jego pracy, a w razie potrzeby wsparcie jego funkcjonowania zespołem odpowiednich specjalistów. W celu realizacji wyrażonej w art. 5 ust. 2 RODO zasady rozliczalności, konieczne jest dokonanie starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec administratora. Ocena tej kwestii zależna jest od wielu czynników, w tym m.in. od: dysponowania przez nią ilością czasu odpowiednią do zakresu zadań i specyfiki procesów przetwarzania danych, konieczności unikania konfliktu interesów oraz wielkości i struktury organizacyjnej jednostki będącej administratorem danych. Trzeba mieć przy tym świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania oraz tzw. efektywnej dostępności inspektora dla osób z danej organizacji. Do zadań IOD należy bowiem np. bieżące monitorowanie zgodności przetwarzania danych osobowych

[483] WP243 rev.01. wytyczne te dostępne są pod linkiem: https://uodo.gov.pl/pl/3/1348.

z przepisami prawa oraz udzielanie informacji i rad w zakresie obowiązków wynikających z tych przepisów, a także pełnienie punktu kontaktowego dla osób, których dane dotyczą, oraz dla organu nadzorczego. W skład zespołu IOD wchodzić może osoba (osoby) zastępująca inspektora w czasie jego nieobecności. Możliwość powołania takiej osoby przewiduje art. 11a ust. 1 ustawy o ochronie danych osobowych. W opinii UODO 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[484].

Warto również odnotować pogląd zawarty w „Podręczniku Inspektora Ochrony Danych"[485] (str. 123), dotyczący powołania zespołu IOD w podmiotach publicznych: *„W organach publicznych faktycznie zalecane byłoby stworzenie zespołu. W małych podmiotach publicznych w skład takiego zespołu mogą wchodzić po prostu obecni pracownicy regularnie spotykający się z inspektorem ochrony danych w celu omówienia istotnych spraw i opracowania polityki. W większych – część pracowników może zostać formalnie przypisana do pełnienia funkcji wspierających inspektora ochrony danych na część etatu. W innych konieczne może okazać się mianowanie pełnoetatowych pracowników wspierających inspektora ochrony danych. Jak jasno wynika z wszystkich wytycznych, decyzje w tych sprawach należy podejmować, biorąc pod uwagę (i) złożoność lub wrażliwość operacji przetwarzania danych osobowych oraz (ii) rozmiar i zasoby danego podmiotu. Jednak w końcu zgodnie z RODO zasoby przydzielone inspektorowi ochrony danych (i zespołowi) muszą być odpowiednie do wykonywanych obowiązków".* Wiele informacji na temat obowiązków administratora określonych w art. 37 i 38 RODO można również znaleźć w zakładce IOD na stronie internetowej UODO[486].

W jednym z podmiotów inspektor zastanawiał się, czy w dużej organizacji, zatrudniającej ponad 1000 osób, **inspektor ochrony danych może zaplanować audyt na dwa lub trzy lata.** Odpowiadając na pytanie, **czy IOD powinien sporządzić plan audytów**[487]**,** UODO wskazał, że

[484] Więcej informacji w tym zakresie znajduje się w wydaniu 10 Newslettera UODO dla IOD (październik 2020, str. 2, https://uodo.gov.pl/pl/p/archiwum-newslettera-dla-iod.
[485] Podręcznik dostępny pod linkiem https://uodo.gov.pl/pl/168/1298.
[486] Cennych wskazówek dostarczają też rozstrzygnięcia Prezesa UODO, np. decyzja o sygn. ZSOŚS.421.25.2019 (https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019) i innych organów nadzorczych UE, których zadaniem jest monitorowanie i egzekwowanie przestrzegania ww. przepisów (m.in. poprzez nakładanie na administratorów administracyjnych kar pieniężnych na podstawie art. 83 ust. 4 lit. a RODO, *Czy naruszenie przepisów odnoszących się do inspektora ochrony danych może skutkować administracyjnymi karami pieniężnymi nakładanymi na administratora danych lub podmiot przetwarzający?*(https://uodo.gov.pl/pl/122/198).
[487] Pytanie i odpowiedź dostępne są pod linkiem: https://uodo.gov.pl/pl/225/1870.

w aktualnym stanie prawnym nie ma przepisów, które wprost i jednakowo dla wszystkich wskazywałyby okres, na jaki należy opracować plan audytów. Niemniej, aby prawidłowo realizować zadanie z art. 39 ust. 1 lit. b RODO, warto planować swoje działania, tj. posiadać plan audytów. Zgodnie z powołanym art. 39 ust. 1 lit. b RODO, inspektor odpowiada m.in. za monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk ustanowionych w tym zakresie przez administratora lub podmiot przetwarzający. Realizacja tego zadania przez inspektora nie powinna mieć charakteru jednorazowego, lecz charakter ciągły i długofalowy. Na tę aktywność składa się (jak wyjaśniono w wytycznych dotyczących IOD) zbieranie informacji o prowadzonych procesach przetwarzania; analizowanie i ocena zgodności tego przetwarzania z wymogami oraz informowanie, doradzanie i rekomendowanie określonych działań administratorowi albo podmiotowi przetwarzającemu. Zaplanowanie audytów – zwłaszcza, gdy IOD monitoruje przestrzeganie przepisów w dużej organizacji – pozwoli mu dobrze wywiązywać się z powyższego zadania. Taki plan powinien uwzględniać wiele czynników zależnych od specyfiki danego administratora i prowadzonych przez niego procesów (czynności) przetwarzania danych. Konieczne jest jego dostosowanie do przeprowadzonej w organizacji oceny ryzyka (do tego zobowiązuje IOD art. 39 ust. 2 RODO) i przypisanie wyższego priorytetu obszarom, które mają szczególne znaczenie dla systemu ochrony danych u konkretnego administratora. Pomocny w planowaniu audytów będzie rejestr czynności przetwarzania. Plan ułatwia jak najlepsze i realne wykorzystanie zasobów, którymi IOD dysponuje. Tworzenie planu pomaga ustalić, czy zasoby te są wystarczające, a także czy we wszystkich monitorowanych obszarach IOD ma zapewnione przez administratora współdziałanie ze strony osób przetwarzających dane osobowe i posiadających wiedzę na temat tego przetwarzania.

Sporządzając plan audytów warto przemyśleć takie jego elementy, jak: częstotliwość przeprowadzania, metody, kryteria i zakres poszczególnych audytów (w zależności od obszaru poddawanego ocenie), tryb uruchamiania audytów, zasady i sposób jego dokumentowania (w tym czas przechowywania raportu z audytu), zasady i sposób raportowania jego wyników. Trzeba pamiętać, że – ze względu na podejście oparte na ryzyku i nieprzewidziane zdarzenia, na które należy szybko reagować – plan audytów powinien przewidywać tryb doraźny. Zarówno plan audytów, jak i wyniki z audytów są dla administratora (kierownictwa, kadry zarządzającej) ważnym elementem rozliczalności (art. 5 ust. 2 RODO), sprawowania kontroli, jak wykonywane są obowiązki z zakresu ochrony danych, czy funkcjonujące w podmiocie rozwiązania techniczne i organizacyjne są zgodne z przepisami oraz wewnętrznymi politykami, a także czy zostały skutecznie wdrożone. Mogą

wskazywać, jakie obszary organizacji potrzebują pomocy i wiedzy fachowej, aby prawidłowo wykonywać powierzone zadania.

14.2. 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 zaś obowiązany (zgodnie z art. 52 ust. 3) ustosunkować się do niego na piśmie w terminie 30 dni od daty otrzymania.

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 RODO.

W 2021 roku Prezes UODO wystosował **375 wystąpień** z określonymi wnioskami do podmiotów administracji publicznej i podmiotów prywatnych działających w różnych sektorach, z czego **365** wiązało się z naruszeniami ochrony danych, zaś **10** wystąpień w większości dotyczyło zagadnień legislacyjnych.

I tak, w związku ze stwierdzonymi **naruszeniami ochrony danych osobowych**, powodującymi wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w 2021 roku Prezes Urzędu skierował **365 wystąpień do administratorów danych** w celu zapewnienia skutecznej ochrony danych osobowych. Głównym przedmiotem wystąpień było 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 rozporządzeniu

2016/679[488]. Przykładowe braki w zawiadomieniu polegały na braku informacji co do: imienia i nazwiska inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji, opisu możliwych konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach – środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Natomiast impulsem do sformułowania wniosków w pozostałych **10 wystąpieniach** Prezesa UODO były zarówno analizy obowiązujących lub projektowanych aktów prawnych, jak i wpływające do Prezesa UODO sygnały czy pytania prawne, a także doniesienia medialne. Szczególnie istotne były zaś te sprawy, które wpływały na ochronę danych osobowych lub prywatność dużych grup osób, odnosiły się do wykorzystania nowoczesnych technologii, w tym zautomatyzowanego przetwarzania danych. Poniżej przedstawione zostały wybrane przykłady wystąpień.

Elektroniczne zarządzanie dokumentacją w administracji publicznej

Jednym z ważniejszych wystąpień skierowane było do Kancelarii Premiera Rady Ministrów (KPRM) w związku z tworzeniem jednolitego i bezpłatnego narzędzia do elektronicznego zarządzania dokumentacją w administracji publicznej – systemu EZD RP[489] – wspomnianego wcześniej w niniejszym sprawozdaniu. Miało to być narzędzie, za pomocą którego przetwarzane będą na masową skalę dane osobowe, w tym dane szczególnych kategorii i dane z art. 10 RODO, a także dane objęte tajemnicami prawnie chronionymi. Dlatego tym bardziej istotne było zapewnienie im właściwej ochrony, na co organ nadzorczy zwrócił uwagę w swoim wystąpieniu, obszernie omówionym w części poświęconej opiniowaniu projektów aktów prawnych.

Samospis internetowy

W analizowanym roku sprawozdawczym organ nadzorczy wystąpił do Prezesa GUS o podjęcie stosownych działań, mających na celu wdrożenie odpowiednich narzędzi, które pozwolą na zapewnienie stosowania zasad określonych w art. 5 rozporządzenia 2016/679, w szczególności zasady rzetelności i przejrzystości, w procesie przetwarzania danych osobowych podczas przeprowadzania narodowego spisu powszechnego ludności i mieszkań metodą tzw. samospisu

[488] Art. 34 ust. 1 i art. 34 ust. 2 w zw. z art. 33 ust. 3 lit. b, c i d RODO.
[489] DOL.413.5.2021.

internetowego[490]. Organ nadzorczy nie kwestionował przetwarzania numeru PESEL, natomiast zwrócił uwagę, aby GUS jako administrator danych osobowych przetwarzanych na potrzeby przeprowadzania spisu ludności zapewnił, by dedykowany spisowi internetowemu formularz był przejrzysty dla respondentów w zakresie wskazania podstaw prawnych tego działania.

W odpowiedzi na wystąpienie poinformowano, że w celu zapewnienia większej przejrzystości dotyczącej podstaw prawnych przetwarzania danych osobowych, w tym numeru PESEL, w klauzulach informacyjnych zostały uzupełnione zapisy określające podstawy prawne przetwarzania danych osobowych. Wskazano w nich, że: „Służby statystyki publicznej przetwarzają w celu statystycznym dane osobowe, zgodnie z katalogiem określonym w art. 35b ustawy o statystyce publicznej. Dane osobowe, od momentu ich zebrania od respondentów albo z systemów informacyjnych administracji publicznej i rejestrów urzędowych lub niepublicznych systemów informacyjnych na potrzeby wykonywania zadań określonych w ustawie o statystyce publicznej (w tym prowadzenia spisów powszechnych) stają się danymi statystycznymi i objęte są tajemnicą statystyczną".

Bezpieczeństwo danych osobowych studentów przekazywanych przez uczelnie do GUS

Korzystając ze swoich uprawnień, organ nadzorczy w 2021 roku wystąpił też do Prezesa GUS o podjęcie stosownych działań, mających na celu zapewnienie odpowiedniej ochrony danych osobowych studentów przekazywanych przez uczelnie Głównemu Urzędowi Statystycznemu[491]. Chodziło o podstawy prawne pozyskiwania przez Główny Urząd Statystyczny od uczelni wyższych danych o słuchaczach, uczestnikach kształcenia specjalistycznego czy doktorantach – osobach, które otrzymały świadectwo maturalne lub jego odpowiednik poza Polską.

Prezes Głównego Urzędu Statystycznego przyjął do wiadomości wskazane w ww. wystąpieniu zastrzeżenia organu nadzorczego, co do braku podstawy prawnej do przekazywania przez uczelnie wyższe informacji na temat kraju ukończenia szkoły średniej przez studenta (doktoranta) i zdecydował, że uczelnie wyższe (a także instytuty Polskiej Akademii Nauki i instytuty badawcze) będą zobligowane do przekazania tylko danych w postaci zagregowanej, a nie danych jednostkowych (czyli danych osobowych), i tylko wówczas, gdy dane takie już posiadają. Z przekazanych informacji wynika, że podmioty te zostaną w kolejnych latach zobowiązane do obligatoryjnego przekazywania

[490] DOL.413.4.2022.
[491] DOL.413.7.2021.

zagregowanych danych, ale – jak wskazano w korespondencji – będzie to możliwe po zmianie ustawy Prawo o szkolnictwie wyższym i nauce oraz rozporządzenia dotyczącego systemu POL-on.

Dokumentacja w poradniach psychologiczno-pedagogicznych

Z kolei w wystąpieniu skierowanym do Ministerstwa Edukacji i Nauki (MEiN) organ nadzorczy postulował m.in. rozważenie doprecyzowania przepisów regulujących działalność poradni psychologiczno-pedagogicznych, w zakresie prowadzonej dokumentacji, do przepisów RODO[492]. Wskazał, że przepisy rozporządzenia w sprawie orzeczeń i opinii wydawanych przez zespoły orzekające działające w publicznych poradniach psychologiczno-pedagogicznych, w zakresie dotyczącym wniosku o wydanie orzeczenia lub opinii, zawierają oświadczenie wnioskodawcy o wyrażeniu zgody na przetwarzanie danych osobowych w celu wydania orzeczenia lub opinii. Podstawy prawne przetwarzania szczególnych kategorii danych osobowych w celu wydania orzeczenia lub opinii powinny natomiast wynikać z aktów o randze ustawy, zapewniających odpowiednie gwarancje ochrony, i nie być kształtowane wyłącznie w oparciu o zgodę, o której mowa w art. 9 ust. 2 lit. a RODO, która w każdym momencie może być wycofana, a to powoduje określone konsekwencje prawne.

Uwagi dotyczące braku podstaw do przyjmowania zgody zostały przez projektodawcę uwzględnione – z rozporządzenia usunięto przepis przewidujący wymóg zamieszczania we wniosku o wydanie opinii bądź orzeczenia, o których mowa w tym rozporządzeniu, oświadczenia wnioskodawcy o wyrażeniu zgody na przetwarzanie danych osobowych w celu wydania orzeczenia lub opinii.

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA

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

- *upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumieniem tych zjawisk, ze szczególnym uwzględnieniem działań skierowanych do dzieci[493];*

[492] DOL.413.8.2022.
[493] Art. 57.1.b RODO.

- *upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO*[494]*;*
- *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*[495].

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

Wychodząc naprzeciw zapotrzebowaniu na edukację, która od marca 2020 roku za pośrednictwem Internetu przeniosła się ze szkół czy wielu miejsc pracy do domów ze względu na pandemię koronawirusa, w 2021 roku Urząd Ochrony Danych Osobowych zorganizował szereg inicjatyw online w celu wyjaśnienia bieżących problemów związanych ze stosowaniem przepisów RODO w różnych obszarach życia zawodowego i prywatnego obywateli. Były to nieodpłatne szkolenia, warsztaty czy webinaria z zakresu ochrony danych osobowych, skierowane do instytucji publicznych oraz innych podmiotów zainteresowanych podnoszeniem swoich kwalifikacji w tym obszarze.

1.1. Studium dla IOD w KSAP (online)

Prezes Urzędu Ochrony Danych Osobowych prowadzi działania edukacyjne w ramach podpisanych porozumień o współpracy w zakresie prawa do prywatności i ochrony danych osobowych z licznymi uczelniami i szkołami wyższymi w Polsce. W ramach współpracy Krajowej Szkoły Administracji Publicznej im. Prezydenta RP Lecha Kaczyńskiego (KSAP) i Urzędu Ochrony Danych Osobowych, zapoczątkowanej 7 listopada 2019 r. podpisanym porozumieniem o współpracy w zakresie ochrony prywatności i danych osobowych, w roku sprawozdawczym zrealizowano 5. edycję Studium dla Inspektorów Ochrony Danych. Obszary współpracy obu instytucji obejmują m.in. działalność naukowo-badawczą, działalność edukacyjną, wydawniczą czy organizacyjną.

[494] Art. 57.1.d RODO.
[495] Art. 57.1.e RODO.

W dniu 31 marca 2021 roku odbyło się spotkanie przedstawicieli UODO i KSAP określające główne założenia organizacyjne jak i merytoryczne 5. edycji Studium, która została zrealizowana w maju i czerwcu 2021 r. i objęła 56 godzin dydaktycznych oraz 2 godziny konsultacji. Studium poprowadziło 10 wykładowców, w tym 8 przedstawicieli Urzędu Ochrony Danych Osobowych. Tematyka Studium omawiana przez przedstawicieli UODO koncentrowała się na prawnych aspektach ochrony danych osobowych, takich jak certyfikacja i kodeksy postępowania oraz informacje o organie nadzorczym. Analiza ryzyka i bezpieczeństwo danych osobowych, informacje nt. wyznaczania, statusu czy zadań inspektora ochrony danych, współpraca IOD z UODO, w tym działania edukacyjne UODO adresowane do IOD – były głównymi zagadnieniami prezentowanymi podczas spotkania ze słuchaczami Studium. Na wybranych przykładach przedstawiono naruszenia ochrony danych osobowych oraz czynności kontrolne podejmowane przez Urząd. Omawiano aktualne problemy związane z ochroną danych w sektorze publicznym w kontekście decyzji wydanych przez Prezesa UODO, wybrane zagadnienia sektorowe dotyczące ochrony danych osobowych w związku ze stanem pandemii COVID-19, ochroną danych osobowych w zatrudnieniu oraz w organach publicznych zajmujących się ściganiem sprawców przestępstw i wykroczeń.

1.2. Szkolenia zewnętrzne

Warsztaty dla Dyrektorów Generalnych Służby Cywilnej, 31.05.2021 r. (online)

Celem szkolenia zorganizowanego 31 maja 2021 roku przez KSAP pn. „Zarządzanie i przywództwo", przeznaczonego dla Dyrektorów Generalnych Służby Cywilnej, ministerstw, urzędów centralnych i wojewódzkich, było przedstawienie zagadnień ochrony danych osobowych w związku z sygnalizowanymi przez te podmioty potrzebami i oczekiwaniami wsparcia w zakresie interpretacji przepisów RODO i ich stosowania. Dotyczyło one zwłaszcza analizy pojęcia „administrator", „współadministrator" i „podmiot przetwarzający", a także obowiązku wyznaczania inspektora ochrony danych. Zagadnienia związane z wdrażaniem zasad ochrony danych w organizacji pracy Służby Cywilnej, analiza przyczyn naruszeń ochrony danych na wybranych przykładach i ich możliwe konsekwencje, a także przegląd trzyletniego stosowania RODO – były głównymi tematami wystąpień przedstawicieli UODO podczas tego spotkania.

Webinarium UODO „Zgłaszanie naruszeń ochrony danych osobowych w praktyce", 9.06.2021 r. (online)

Podczas szkolenia eksperci UODO przedstawili praktyczne aspekty zgłaszania naruszeń ochrony danych osobowych, w oparciu o przypadek zaszyfrowania danych złośliwym oprogramowaniem typu *ransomware.* Webinarium służyło omówieniu kluczowych zagadnień dla bezpieczeństwa danych osobowych, którym zagrażają ataki oraz wirusy cyfrowe oraz wyjaśnieniu kwestii związanych z naruszeniami danych osobowych w oparciu o przedstawione przykłady. Wykład adresowany był nie tylko do informatyków lub specjalistów z branży IT, ale i przeciętnego użytkownika nowych technologii – narażonego na wyciek danych osobowych.

Szkolenie „Ochrona danych osobowych w podmiotach kościelnych". Zakopane, 7–9.10.2021 r.

Organizatorem szkolenia, które odbyło się w Centrum Formacyjno-Szkoleniowym „Księżówka", była Konferencja Episkopatu Polski i Kościelny Inspektor Ochrony Danych (KIOD).

Podczas trzydniowego szkolenia odbywały się warsztaty prowadzone przez kanoników, prawników oraz specjalistów z zakresu ochrony danych, pełniących funkcje inspektorów ochrony danych w podmiotach kościelnych. Audytorium mogło wysłuchać wykładów dotyczących praktyki działania IOD w podmiotach kościelnych, o przepisach odnoszących się do regulacji archiwów kościelnych oraz RODO, a także o dobrych praktykach organizacji kancelarii w podmiotach kościelnych. W spotkaniu uczestniczyli przedstawiciele Urzędu Ochrony Danych Osobowych, którzy opowiedzieli zgromadzonym o metodyce prowadzenia kontroli przez organ nadzorczy oraz o perspektywach realizacji porozumienia pomiędzy Prezesem UODO a KIOD, które podpisane zostało 10 maja 2019 roku. Podczas tego warsztatu odbyły się także konsultacje indywidualne z pracownikami Urzędu Ochrony Danych Osobowych.

Było to pierwsze od czasu wystąpienia stanu pandemii stacjonarne szkolenie organizowane przez Kościelnego Inspektora Ochrony Danych. Było ono poświęcone dwóm głównym tematom: kontrolom oraz organizacji kancelarii w podmiotach kościelnych. Zgromadzonych na szkoleniu przywitał ks. Piotr Kroczek, który wprowadził uczestników w tematykę spotkania oraz zasygnalizował bieżące kwestie dotyczące ochrony danych osobowych w Kościele katolickim.

Szkolenia dla pracowników Kancelarii Sejmu RP, 21–22.10.2021 i 4–5.11.2021 r. (online)

Na przełomie października i listopada 2021 roku przedstawiciele Urzędu przeprowadzili cykl szkoleń dla pracowników Kancelarii Sejmu RP oraz legislatorów, przybliżając zagadnienia związane

z ochroną danych osobowych w zarządzaniu tą organizacją oraz rolą, jaką w tym procesie pełni administrator, współadministrator i podmiot przetwarzający.

W ramach szkolenia przedstawiono wpływ ogólnego rozporządzenia o ochronie danych na przepisy krajowe, zasadę poufności w praktyce Kancelarii Sejmu, zasadę *privacy by design* – wdrażanie ochrony danych na etapie projektowania w związku z wypełnianiem zadań związanych z zamówieniami publicznymi czy pracą nad realizacją projektów unijnych – a także tematy związane z obowiązkami pracodawcy w związku z pandemią i pracą zdalną oraz naruszeniami ochrony danych.

Podkreślenia wymaga fakt, że niektóre szkolenia Urzędu Ochrony Danych Osobowych organizowane są w ramach ogólnopolskiego programu edukacyjnego UODO „Twoje dane – Twoja sprawa" i zostaną przedstawione w dalszej części niniejszego sprawozdania w rozdziale poświęconym Programowi 1.4.1. Szkolenia te mają często **cykliczny charakter**. Są to organizowane co roku dwudniowe szkolenia dla koordynatorów Programu – przedstawicieli placówek uczestniczących w tym przedsięwzięciu. Koordynatorzy przekazują zdobytą wiedzę nauczycielom na radach pedagogicznych w swoich szkołach i podczas lekcji z uczniami. Działania te mają na celu upowszechnienie wiedzy na temat bezpiecznego posługiwania się danymi osobowymi w szkole i poza nią. Coroczne, dwudniowe szkolenia to jedno z najważniejszych etapów Programu, dzięki któremu kadra pedagogiczna szkół i placówek doskonalenia nauczycieli zdobywa wiedzę na temat zasad ochrony danych osobowych i prywatności. Szkolenia są również okazją do odpowiedzi na wiele nurtujących pytań oraz wymiany doświadczeń i dobrych praktyk dotyczących organizacji zajęć tematycznych z uczniami.

W celu propagowania wiedzy o ochronie danych osobowych prowadzony jest również serwis informacyjny **techinfo.uodo.gov.pl**[496], 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.

1.3. Konkursy

W analizowanym 2021 roku organ nadzorczy był organizatorem i patronem konkursu z dziedziny prawa do prywatności i ochrony danych osobowych.

[496] https://techinfo.uodo.gov.pl

Konkurs na esej dotyczący zagadnień z zakresu ochrony danych osobowych

Od wielu lat organ ds. ochrony danych osobowych jest organizatorem konkursów dla studentów prawa i administracji, na esej dotyczący zagadnień z zakresu ochrony danych osobowych. Celem konkursów jest propagowanie wiedzy o ochronie danych osobowych i umożliwienie studentom sprawdzenie swojej wiedzy w formułowaniu praktycznych rozwiązań w zetknięciu z realnymi problemami prawnymi. Konkursy te niezmiennie od lat cieszą się niesłabnącym zainteresowaniem.

W kwietniu 2021 r. już po raz XI Prezes UODO 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. „Skanowanie tęczówki oka jako sposób identyfikacji studentów podczas egzaminów".

Partnerem merytorycznym konkursu była kancelaria Kobylańska Lewoszewski Mednis sp. j. W 2021 roku studenci zmierzyli się z kwestiami związanymi z wykorzystywaniem danych biometrycznych. Dane tego typu są łatwe do pozyskania, niezmienne w ciągu życia człowieka i jednocześnie „noszone zawsze przy sobie". Temat konkursu był również związany z aktualną w tamtym czasie sytuacją związaną z rozprzestrzenianiem się wirusa COVID–19 i powszechnie stosowaną edukacją na odległość.

Organizatorzy konkursu zapytali studentów o możliwości dotyczące wykorzystywania danych biometrycznych (tęczówki oka) na potrzeby przeprowadzenia egzaminu w formule zdalnej. Czy uzasadnione może być wykorzystywanie danych w postaci skanowania tęczówki oka studenta, na potrzeby weryfikacji jego tożsamości przy udostępnianiu zadania egzaminacyjnego? Czy uczelnia ma podstawę prawną do przetwarzania danych osobowych wykorzystanych w tak innowacyjnym rozwiązaniu? Jakie główne obowiązki z zakresu ochrony danych osobowych powinna wykonać uczelnia wobec studentów w związku z wprowadzeniem takiej procedury? Zadaniem uczestników było przygotowanie rozwiązania kazusu w formie eseju.

W dniu 8 lipca 2021 roku w siedzibie Urzędu zwycięzcom konkursu wręczono dyplomy oraz nagrody rzeczowe, podczas zorganizowanej ceremonii z udziałem przedstawicieli UODO oraz

partnera merytorycznego konkursu. Dla laureatów przewidziano również nagrody specjalne – praktyki w Urzędzie Ochrony Danych Osobowych[497].

1.4. Projekty i programy

1.4.1. Ogólnopolski program edukacyjny TDTS

W roku sprawozdawczym 2021, Urząd Ochrony Danych Osobowych kontynuował realizację największego ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli" (TDTS), który od 2009 r. nieprzerwanie realizowany jest przez Urząd Ochrony Danych Osobowych.

XI edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa" w roku szkolnym 2020/2021 oraz rozpoczęcie XII edycji w roku szkolnym 2021/2022.

Zgodnie z art. 57 pkt. 1 lit. b rozporządzenia o ochronie danych osobowych (RODO) jednym z zadań Prezesa Urzędu Ochrony Danych Osobowych jest upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumieniem tych zjawisk, ze szczególnym uwzględnieniem działań skierowanych w tym zakresie do dzieci, które są mniej świadome konsekwencji i praw przysługujących im w związku z przetwarzaniem dotyczących ich danych. Wsparciem dla tego zadania jest z powodzeniem realizowany ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa", który cieszy się niesłabnącym zainteresowaniem wśród placówek oświatowych.

Podniesienie kompetencji pedagogów i nauczycieli oraz edukowanie dzieci i młodzieży, w jaki sposób mają chronić dane osobowe zarówno w realnym, jak i cyfrowym świecie, to główne cele tego Programu, prowadzonego od 12 lat przez organ właściwy w sprawie ochrony danych osobowych. Przedsięwzięcie realizowane jest pod honorowym patronatem Ministra Edukacji Narodowej (obecnie Ministra Edukacji i Nauki) oraz Rzecznika Praw Dziecka, przy wsparciu patronów medialnych. W ramach współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie organizowane są webinaria dla uczestników Programu.

[497] Szczegółowe informacje o XI edycji konkursu na esej dla studentów kierunków prawa i administracji są dostępne pod linkiem: https://uodo.gov.pl/pl/20.

Przedsięwzięcie stanowi doskonałe źródło wiedzy i dobrych praktyk dla nauczycieli w zakresie ochrony danych osobowych w szkołach oraz przekazuje informacje na temat realizacji obowiązków wynikających z RODO w sektorze oświaty. Rezultatem podejmowanych działań edukacyjnych jest nabyta wiedza i umiejętności uczniów w zakresie ochrony swojej prywatności i danych osobowych, stosowanie odpowiednich zabezpieczeń oraz świadomość swoich praw i obowiązków wynikających z przepisów prawa. Ochrona danych osobowych jest sednem umiejętności cyfrowych, dlatego też kształtowanie odpowiedzialnych postaw i nawyków wśród dzieci i młodzieży, popularyzacja wiedzy na temat skutecznej ochrony danych osobowych wśród uczniów i nauczycieli, nabrała dużego znaczenia szczególnie w okresie edukacji zdalnej.

Działania w ramach Programu są realizowane dwuetapowo. W pierwszej kolejności w wiedzę o ochronie danych osobowych wyposaża się dyrektorów szkół i nauczycieli, a następnie oni edukacją uczniów i rodziców. Atutem Programu jest profesjonalne wsparcie merytoryczne ekspertów Urzędu Ochrony Danych Osobowych oraz organizacja szkoleń/webinariów.

Od wielu lat program „Twoje dane – Twoja sprawa" cieszy się popularnością i na trwałe wpisał się w kalendarz szkolnych wydarzeń o czym świadczy m.in. liczny udział szkół i placówek w minionych edycjach.

Każdego roku w Programie bierze udział ponad 45 000 uczniów i ponad 4000 nauczycieli, którzy podejmują różne działania edukacyjne na rzecz upowszechniania wiedzy o ochronie danych osobowych i prawa do prywatności wśród uczniów. 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 i odpowiedzialnych postaw wśród uczniów w obszarze ochrony danych osobowych, poprzez realizowane różnorodne zajęcia adekwatnie do wieku uczniów. Praktyczny aspekt edukacji jest 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 lokalnie – w szkołach i placówkach doskonalenia nauczycieli.

XI edycja programu TDTS – rok szkolny 2020/2021

W roku szkolnym 2020/2021, w XI edycji Programu udział wzięło 419 placówek, tj. 289 szkół podstawowych, 120 szkół ponadpodstawowych oraz 10 placówek doskonalenia nauczycieli. Rekrutacja była prowadzona przez cały rok szkolny. Najwięcej szkół przystąpiło z województwa mazowieckiego, łódzkiego oraz śląskiego, natomiast najmniej z województwa warmińsko-mazurskiego, 61% placówek przystąpiło do Programu po raz pierwszy, zaś 39% uczestników kontynuuje z Urzędem współpracę już kolejny rok, co ma duże znaczenie dla utrwalania wiedzy i kształtowania odpowiedzialnych nawyków wśród uczniów.

Szkolenia w ramach XI edycji Programu

Szkolenie inaugurujące XI edycję Programu, ze względu na pandemię COVID-19 odbyło się po raz pierwszy w formule online w dniach 15–16 października 2020 roku. Szkolenie należy do grupy wspomnianych wcześniej w niniejszym sprawozdaniu szkoleń cyklicznych organizowanych przez Urząd. Wydarzenie było okazją do przybliżenia koordynatorom tematyki ochrony danych osobowych w sektorze oświaty, sposobu realizacji Programu, a także wymiany doświadczeń i omówienia dobrych praktyk w edukacji dzieci i młodzieży. Przeszkolonych zostało 225 koordynatorów, którzy następnie organizowali szkolenia rad pedagogicznych w poszczególnych szkołach.

Jak co roku, wsparcie eksperckie przedstawicieli Urzędu zostało zapewnione podczas konsultacji całorocznych (e-mail oraz telefonicznie). Konsultacje w sprawie interpretacji przepisów o ochronie danych osobowych odbywały się pod numerem tel. 606-950-000, konsultacje w sprawie Programu pod numerem tel. 22 531-04-55 oraz e-mail: tdts@uodo.gov.pl.

W ramach XI edycji Programu odbyło się 4398 lekcji poświęconych ochronie danych osobowych i prywatności, prowadzonych podczas godzin wychowawczych, informatyki, w ramach edukacji wczesnoszkolnej oraz innych lekcji przedmiotowych. Ze szkoleń oferowanych w ramach Programu skorzystało 4482 nauczycieli, zaś 2564 nauczycieli aktywnie zaangażowało się w realizację różnorodnych inicjatyw edukacyjnych.

W licznych zajęciach wzięło udział 50861 uczniów. Szkolenia, materiały edukacyjne, webinaria oraz porady przyczyniają się do wzrostu wiedzy oraz podniesienia kompetencji nauczycieli i pedagogów w obszarze ochrony danych osobowych i bezpieczeństwa w Internecie. Z roku na rok coraz więcej nauczycieli zostaje przeszkolonych, coraz więcej uczniów bierze udział w Programie i nabywa wiedzę na temat przysługujących im praw i obowiązków, ryzyka związanego z nierozsądnym udostępnianiem informacji o sobie oraz sposobów skutecznej ochrony siebie. W XI edycji została przeprowadzona rekordowa liczba inicjatyw edukacyjnych: 1778 zajęć lekcyjnych, pozalekcyjnych oraz wydarzeń tematycznych.

Webinaria w ramach XI edycji Programu

Wspomaganiu dzieci i młodzieży w nauce zdalnej a także w ich funkcjonowaniu w społeczeństwie, poprzez przekazanie im (a także rodzicom i nauczycielom) wiedzy, służyły organizowane webinaria. W ramach XI edycji Programu zostały zorganizowane następujące webinaria:

1) „Bezpieczeństwo danych osobowych w okresie kształcenia", 11.03.2021 r. – wydarzenie odbyło się w ramach programu zainicjowanego przez Kuratorium Oświaty w Warszawie „Reaguj i wspieraj. Koalicja na rzecz tworzenia bezpiecznego środowiska nauczania na odległość". Wydarzenie przeznaczone było dla kadry pedagogicznej szkół różnego typu.
2) „Bezpieczeństwo cyfrowe dzieci i młodzieży a odpowiedzialność", 9.04.2021 r. – wydarzenie odbyło się w ramach współpracy z Komendą Stołeczną Policji oraz Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

   Celem spotkania było przybliżenie zasad ochrony danych w Internecie i przedstawienie sposobów na unikanie zagrożeń. Podczas wykładu eksperci odpowiedzieli m.in. na pytania, jak odpowiedzialnie i świadomie korzystać z dostępnych narzędzi w celu ochrony swojego wizerunku i danych osobowych, a także o konsekwencjach nierozważnych decyzji w cyfrowej rzeczywistości. Wykład był okazją dla dyrektorów szkół, nauczycieli, uczniów i ich rodziców do zrozumienia, jak świat nowych technologii wpływa na nawyki młodych ludzi we wszystkich aspektach ich codziennego życia.
3) „RODO w szkolnej ławce. Przetwarzanie danych biometrycznych", 28.04.2021 r.

Wykład był adresowany do przedstawicieli sektora oświaty. Webinarium służyło omówieniu kluczowych zagadnień związanych z przetwarzaniem danych biometrycznych. Eksperci UODO wyjaśnili, dlaczego należy zachować wzmożoną ostrożność przy przetwarzaniu przez szkoły danych osobowych dzieci, które powinny być szczególnie chronione. Na podstawie analizy bieżących spraw oraz przepisów i wytycznych, wskazali, na co zwracać uwagę przy przetwarzaniu danych biometrycznych.

Cykl porad w ramach XI edycji Programu

Równolegle z webinariami i szkoleniami uczestnicy XI edycji programu „Twoje dane – Twoja sprawa" otrzymywali porady edukacyjne z cyklu „Warto wiedzieć". Tematyka porad najczęściej dotyczyła bezpiecznego użytkowania Internetu i ochrony danych osobowych. Porady skupiały się na najbardziej popularnych wśród dzieci i młodzieży szkolnej aspektach ochrony prywatności, m.in. przy korzystaniu z aplikacji czy serwisów społecznościowych. W oferowanych poradach UODO przedstawiał, z jakich ustawień dotyczących ochrony prywatności warto skorzystać w sieci, a także co robić w przypadku wycieku danych w Internecie. Cykl porad spotkał się z zainteresowaniem i aprobatą uczestników Programu. W ocenie uczniów przygotowane materiały były ciekawe i bardzo przydatne. Wiele z nich zostało opublikowanych na szkolnych stronach, wykorzystanych podczas szkolnych zajęć z uczniami, a także w ramach, zorganizowanego przez Radomski Ośrodek Doskonalenia Nauczycieli, Festiwalu wiedzy o ochronie danych osobowych.

Współpraca palcówek doskonalenia nauczycieli w ramach XI edycji Programu

Wzmocnienie pozycji ośrodków w Programie, wsparcie i wymiana doświadczeń – to główne cele nawiązanej po raz pierwszy współpracy placówek doskonalenia nauczycieli w ramach XI edycji programu „Twoje dane – Twoja sprawa".

Radomski Ośrodek Doskonalenia Nauczycieli, który od wielu lat współpracuje z Urzędem Ochrony Danych Osobowych, po raz pierwszy zaplanował cykl trzech spotkań w formule wideokonferencji – dla przedstawicieli placówek doskonalenia nauczycieli ze Szczecina, Radomia, Suwałk, Bydgoszczy, Warszawy, Wrocławia, Gdańska, Białegostoku i Gdyni. Udział w organizowanym przedsięwzięciu pozwolił nie tylko na wymianę doświadczeń, ale stanowił również inspirację do podejmowania kolejnych interesujących działań w ramach programu „Twoje dane – Twoja sprawa".

Konkursy w ramach XI edycji Programu

Już po raz dziewiąty w ramach programu „Twoje dane – Twoja sprawa" został zorganizowany konkurs dla placówek na najciekawszą inicjatywę edukacyjną oraz konkurs dla uczniów – tym razem na najlepszy poradnik dla rodziców pt. „Życie rodzinne online i offline. Porozmawiajmy o ochronie danych osobowych".

Konkursy zostały ogłoszone 28 stycznia 2021 r. podczas Dnia Ochrony Danych Osobowych. Celem konkursów było popularyzowanie wiedzy wśród uczniów i nauczycieli, zachęcenie młodych ludzi do głębszego zainteresowania się problematyką ochrony danych osobowych oraz promowanie najciekawszych metod edukacji w tym obszarze tematycznym. W swoich pracach uczniowie podkreślili istotne aspekty ochrony prywatności w cyfrowym świecie.

Spośród wszystkich prac uczniów, których UODO otrzymał aż 160, zostało nagrodzonych i wyróżnionych 5 prac (I–III miejsce oraz dwa wyróżnienia). Zwycięzcą konkursu został uczeń Szkoły Podstawowej nr 9 im. Władysława Jagiełły w Kutnie, który przygotował wideoporadnik dla rodziców. W jego pracy konkursowej znalazły się praktyczne rymowane podpowiedzi, jak poruszać się w Internecie bez narażania się na utratę kontroli nad własnymi danymi osobowymi.

Specjalne wyróżnienie Prezesa Urzędu Ochrony Danych Osobowych – statuetkę Złotego Pióra – otrzymała Szkoła Podstawowa nr 4 im. Adama Mickiewicza z Lublina za zajęcie I miejsca za najlepszą inicjatywę edukacyjną zrealizowaną w ramach XI edycji programu TDTS. Zwycięska inicjatywa to zajęcia edukacyjne na temat ochrony danych osobowych zorganizowane z okazji Dnia Ochrony Danych Osobowych, które można zrealizować podczas lekcji języka polskiego pt. „DODO Agencja – mitologiczna interwencja". Podczas zajęć, obok motywów z mitologii greckiej, uczniowie rozwiązywali zagadkę detektywistyczną i brali udział w zabawie z zagadnieniami o ochronie danych osobowych.

Ceremonie wręczenia nagród laureatom konkursów

Podobnie jak w ubiegłym roku, przedstawiciele Urzędu Ochrony Danych Osobowych odwiedzili laureatów konkursów w ich placówkach. Uroczyste wręczenie nagród odbyło się 8 czerwca 2021 roku w Szkole Podstawowej nr 9 w Kutnie oraz 21 czerwca 2021 roku w Trybunale Koronnym w Lublinie. Miały miejsce także kameralne ceremonie wręczenia nagród pozostałym laureatom konkursów w siedzibie Urzędu Ochrony Danych Osobowych w Warszawie.

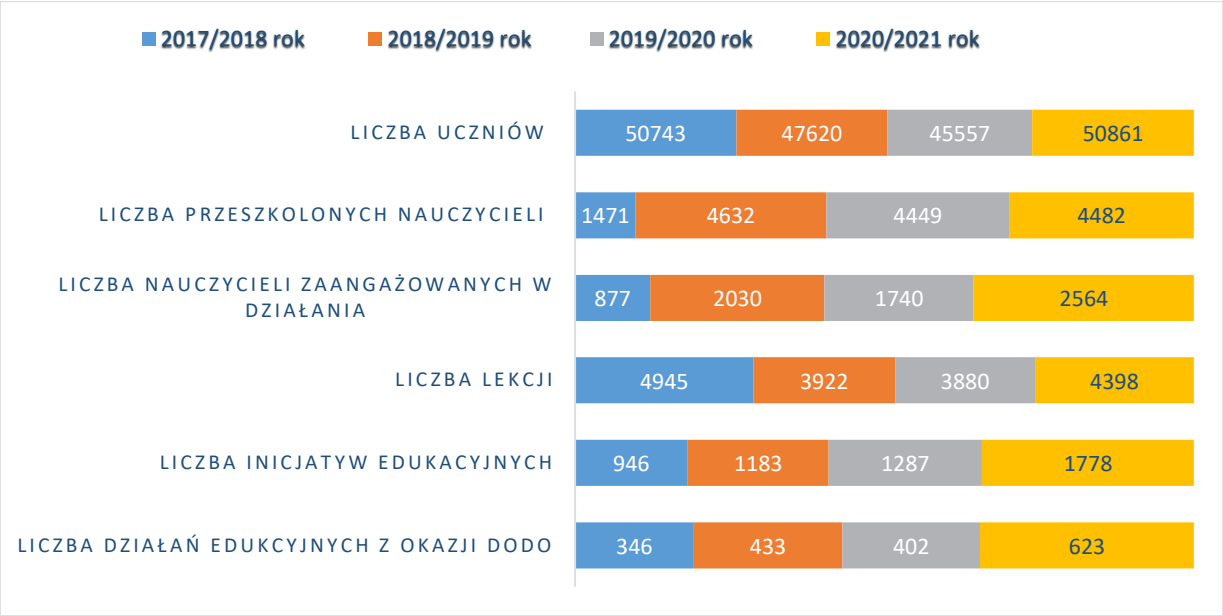
O XI edycji Programu

Do XI edycji Programu zgłosiło się ponad 400 placówek edukacyjnych z całej Polski. O wyjątkowości zakończonej edycji świadczą nie tylko statystyki, ale również to, że pomimo utrudnień i ograniczeń wynikających z pandemii COVID-19 i nauki w trybie zdalnym, uczniowie i nauczyciele chętnie angażowali się w przygotowanie zajęć i wydarzeń tematycznych. Przeprowadzono bardzo dużo inicjatyw edukacyjnych[498]. Powstało wiele ciekawych i cennych przedsięwzięć na rzecz ochrony prywatności uczniów, z których najciekawsze zostały wyróżnione i nagrodzone.

Przygotowane szkolenia, pakiet materiałów edukacyjnych, webinaria, cykl porad i artykuły publikowane na stronie internetowej Urzędu Ochrony Danych Osobowych dla przedstawicieli oświaty stanowią odpowiedzi na wiele istotnych pytań związanych z aktualnymi problemami tego środowiska w zakresie ochrony danych osobowych.

Jak wynika z zamieszczonego poniżej wykresu, w porównaniu do lat ubiegłych można zaobserwować znaczny wzrost przeszkolonych i zaangażowanych w działania w ramach Programu nauczycieli, a także znaczny wzrost liczby zrealizowanych inicjatyw edukacyjnych.

[498] Pełny wykaz inicjatyw został udostępniony na stronie internetowej UODO: https://uodo.gov.pl/pl/458/2132.



Wykres 13: **Liczba inicjatyw edukacyjnych, uczniów, przeszkolonych nauczycieli, zrealizowanych lekcji i działań edukacyjnych z okazji Dnia Ochrony Danych Osobowych w ramach VIII–XI edycji programu TDTS.**

Podobnie jak w poprzednich edycjach Programu, stopień spełnienia oczekiwań uczestników był bardzo wysoki, o czym świadczą oceny dokonane przez realizatorów – uczniów i nauczycieli. Nauczyciele podkreślali konieczność organizowania zajęć w tym obszarze tematycznym, uznając je za niezbędny element zapewnienia bezpieczeństwa w szkole. Wskazywali przy tym na adekwatność tej tematyki do realiów społeczeństwa informacyjnego, uniwersalny zakres merytoryczny oraz duże zainteresowanie jego realizacją.

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 osobowych wśród uczniów i nauczycieli, wzrost zainteresowania tematem oraz współpraca społeczności szkolnej i środowiska lokalnego na rzecz upowszechniania wiedzy o ochronie danych osobowych.

XII edycja programu TDTS – rok szkolny 2021/2022

1 września 2021 roku rozpoczęła się rekrutacja uczestników XII edycji w roku szkolnym 2021/2022. Rekrutacja do Programu jest całoroczna. Niemniej na koniec 2021 roku do XII edycji

TDTS zarejestrowało się 305 placówek oświatowych, z czego 37% placówek przystąpiło do Programu po raz pierwszy, zaś 63% kontynuuje współpracę z UODO. Najwięcej zgłoszeń wpłynęło z województwa mazowieckiego, łódzkiego oraz wielkopolskiego.

Konferencją z cyklu „#RODO w edukacji", zorganizowaną w Szkole Podstawowej Nr 9 im. Władysława Jagiełły w Kutnie, Urząd Ochrony Danych Osobowych uroczyście zainaugurował XII edycję Programu w roku szkolnym 2021/2022. Konferencja miała na celu propagowanie tematyki o ochronie danych osobowych wśród uczniów i nauczycieli, a także podkreślenie istotnej roli tej tematyki w edukacji młodych ludzi. Podczas dwóch paneli tematycznych zostały omówione najważniejsze kwestie związane z realizacją ogólnego rozporządzenia o ochronie danych (RODO) w praktyce szkolnej, a także przykłady dobrych praktyk w działaniach edukacyjnych na rzecz ochrony prywatności dzieci i młodzieży. Przybliżono również kwestie dotyczące Programu skupiając się na jego założeniach oraz harmonogramie bieżącej edycji.

Szkolenia w ramach XII edycji Programu

Jednym z głównych wydarzeń zorganizowanych w ramach XII edycji TDTS, było cykliczne szkolenie online dla koordynatorów, które odbyło się 27 i 28 października 2021 roku. Wydarzenie to było okazją do przedstawienia podstaw prawnych przetwarzania danych osobowych, ze szczególnym uwzględnieniem przepisów odnoszących się do sektora oświaty i problemów zgłaszanych przez szkolnych inspektorów ochrony danych. Służyło także wymianie doświadczeń i omówieniu szczegółów dotyczących realizacji Programu. W drugim dniu szkolenia odbyły się warsztaty, podczas których zaprezentowano przykłady sześciu inicjatyw edukacyjnych zrealizowanych przez placówki oświatowe w czasie XI edycji.

Webinaria w ramach XII edycji Programu

W ramach XII edycji Programu kontynuowany był cykl webinariów z zakresu ochrony danych osobowych. W roku sprawozdawczym zrealizowano webinarium „Klikam z głową – jak chronić swoje dane osobowe", 23.11.2021 roku w formule online. Była to wspólna inicjatywa Urzędu Ochrony Danych Osobowych i Urzędu Komunikacji Elektronicznej (UKE). Wykład poświęcony bezpieczeństwu danych osobowych młodzieży w Internecie. Celem szkolenia było przedstawienie młodym ludziom sposobów na podejmowanie świadomych decyzji dotyczących ujawniania informacji o nich samych, co pozwoli im uniknąć negatywnych konsekwencji nierozważnego

udostępniania danych osobowych. Adresatami wykładu byli uczniowie klas 7. i 8. szkół podstawowych.

1.4.2. Wsparcie programu cyfryzacji w Kirgistanie

W celu upowszechniania wiedzy o ochronie danych osobowych Urząd Ochrony Danych Osobowych angażuje się również w działania związane z realizacją projektów finansowanych ze środków Unii Europejskiej. W okresie od kwietnia 2021 r. do lipca 2021 r. Urząd współpracował z Ministerstwem Funduszy i Polityki Regionalnej, Kancelarią Prezesa Rady Ministrów oraz Centrum Projektów Polska Cyfrowa nad opracowaniem wspólnej oferty w odpowiedzi na fiszkę projektową KG 20 DCI OT 01 21 Support to Digitalisation Agenda in Kyrgyzstan TWINNING REFERENCE NUMBER: KG 20 DCI OT 01 21 (Wsparcie programu cyfryzacji w Kirgistanie). Urząd Ochrony Danych Osobowych, w ramach swoich kompetencji, przygotował wkład do realizacji jednego z komponentów projektu – Umocnienie ochrony danych osobowych i prywatności obywateli Kirgistanu (Citizens privacy and data protection enhanced). W wyniku procedury konkursowej, projekt nie został jednak zakwalifikowany do realizacji.

1.5. Publikacje

E-book „Drony a prywatność".

Efektem Ogólnopolskiej Konferencji Naukowej „Drony a prywatność", która z inicjatywy Urzędu Ochrony Danych Osobowych odbyła się 8 lipca 2020 roku, była publikacja pod tym samym tytułem. Przy współpracy z prelegentami tego wydarzenia, Urząd przygotował e-book z materiałami pokonferencyjnymi w formacie e-pub, umożliwiającym odtworzenie e-booka na dedykowanych urządzeniach. W publikacji tej omówione zostały tematy związane z wykorzystywaniem bezzałogowych statków powietrznych oraz związanych z tym regulacji w zakresie ochrony danych osobowych. Poruszono też kwestie dotyczące odpowiedzialności za naruszenie prywatności za pomocą dronów oraz ich zastosowania w środowisku pracy. Nie zabrakło również zagadnień z obszaru działalności straży gminnych (miejskich) oraz informatyki śledczej.

E-book „Sztuczna inteligencja w kontekście ochrony danych osobowych".

Publikacja ta stanowi podsumowanie panelu dyskusyjnego pt. „Sztuczna inteligencja – w kontekście ochrony danych osobowych", który Urząd Ochrony Danych Osobowych zorganizował online 26 kwietnia 2021 r. Przedstawiono w niej korzyści i zagrożenia, jakie wiążą się z przetwarzaniem danych osobowych przez systemy komputerowe symulujące ludzkie myślenie.

Podkreślano, że postęp związany z innowacjami musi odbywać się z uwzględnieniem zasad określonych w RODO, w tym minimalizacji danych, prawidłowości czy integralności. W tym celu niezbędne jest podjęcie odpowiednich działań i wypracowanie takich rozwiązań, które przyczynią się do zwiększenia bezpieczeństwa oraz świadomości na temat zagrożeń wynikających z dobrodziejstw nowych technologii. W materiałach omówione zostały tematy związane z wykorzystywaniem sztucznej inteligencji w różnych branżach oraz związanych z tym regulacji w zakresie danych osobowych i prywatności.

1.6. 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 roku – z chwilą wybuchu pandemii koronawirusa – przez cały 2021 rok, wydarzenia te organizowane 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 2021 roku. Ich pełny wykaz zawiera załącznik nr 3.

1) XV Dzień Ochrony Danych Osobowych – 28 stycznia 2021 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.

Z okazji Dnia Ochrony Danych Osobowych Prezes UODO zorganizował konferencję online „Realna ochrona danych w zdalnej rzeczywistości", która transmitowana była 28 stycznia 2021 r. za pośrednictwem strony internetowej Urzędu: www.uodo.gov.pl. Wydarzenie było adresowane do wszystkich zainteresowanych tematyką ochrony danych osobowych i cieszyło się bardzo dużym zainteresowaniem. Udział w konferencji był okazją do podjęcia dyskusji na temat aktualnych

wyzwań związanych ze skuteczną ochroną danych osobowych w kontekście współczesnych problemów związanych z zagrożeniem praw i wolności obywatelskich, z rozwojem gospodarki cyfrowej, pandemią wirusa COVID-19, powszechnie stosowanych zdalnych narzędzi komunikacji w pracy czy nauczaniu.

Jak co roku, Dniu Ochrony Danych Osobowych towarzyszyły wydarzenia upowszechniające wiedzę o ochronie danych osobowych, zorganizowane przez podmioty współpracujące z UODO oraz takie, które swoimi działaniami chciały zaakcentować wagę tej tematyki.

Ceremonia wręczenia nagród im. Michała Serzyckiego

Nagroda im. Michała Serzyckiego, którą ustanowiła dr Edyta Bielak-Jomaa, poprzednia Prezes UODO, jest wyróżnieniem dla tych, którzy przyczyniają się do poszerzania świadomości na temat prywatności i roli ochrony danych osobowych w wielu dziedzinach i środowiskach. Od 2018 roku nagroda ta jest wręczana co roku podczas obchodów Dnia Ochrony Danych Osobowych. Termin ten ma wymiar symboliczny, gdyż Polska włączyła się w obchody tego święta w 2007 roku, a więc w czasie, gdy patron nagrody – Michał Serzycki – zajmował stanowisko Generalnego Inspektora Ochrony Danych Osobowych III kadencji. Jednym z rezultatów jego działań było zainicjowanie na szeroką skalę działalności informacyjnej i edukacyjnej organu ds. ochrony danych osobowych.

W 2021 roku po raz czwarty przyznano nagrodę im. Michała Serzyckiego. Wyróżnieni nagrodą zostali: Pani Barbara Grądkowska – dyrektor Specjalnego Ośrodka Szkolno-Wychowawczego w Zamościu, Pani Jen Persson – dyrektor brytyjskiej organizacji pozarządowej DefendDigitalMe i Pan Maciej Gawroński – doświadczony prawnik, ekspert i bardzo dobry praktyk, który od wielu lat aktywnie wspiera ochronę danych osobowych. Nagrodzonych wyróżniono za działania na rzecz edukacji w dziedzinie ochrony danych osobowych. Uroczystość wręczenia nagród odbyła się w Warszawie 27 stycznia 2021 r., w przeddzień obchodów XV Dnia Ochrony Danych Osobowych.

Na coroczne obchody Dnia Ochrony Danych Osobowych składają się także liczne wydarzenia lokalne, podejmowane głównie przez szkoły i placówki doskonalenia nauczycieli uczestniczące w programie edukacyjnym UODO „Twoje dane – Twoja sprawa". W analizowanym 2021 roku uczniowie i nauczyciele przygotowali wiele propozycji, w tym głównie wirtualnych, dostosowując się do pandemicznych realiów, w których bezpieczeństwo danych nabrało szczególnego znaczenia. Quizy, gry i zabawy z wykorzystaniem wirtualnych platform, a także towarzyszące im pogadanki dotyczące ochrony danych osobowych i prywatności – były najpopularniejszymi sposobami

rozpowszechniania wiedzy o ochronie danych w społecznościach szkolnych, w związku z przypadającymi 28 stycznia obchodami XV Dnia Ochrony Danych Osobowych.

XV Dzień Ochrony Danych Osobowych stał się również okazją dla uczniów, aby pokazać swoje talenty, np.:

• pisarskie, tworząc fraszki na temat „Twoje dane – Twoja sprawa" (Szkoła Podstawowa w Nieporęcie, woj. mazowieckie);

• krasomówcze, prowadząc audycje na temat idei Dnia Ochrony Danych Osobowych i programu edukacyjnego UODO za pośrednictwem szkolnego radiowęzła (Szkoła Podstawowa im. płk. Floriana Laskowskiego w Grucie, woj. kujawsko-pomorskie);

• plastyczne, organizując konkurs na znaczek – symbol ochrony danych osobowych (Publiczna Szkoła Podstawowa nr 8 w Brzegu, woj. opolskie), mural (Szkoła Podstawowa z Oddziałami Integracyjnymi nr 87 im. 7 PP AK „Garłuch" w Warszawie, woj. mazowieckie) lub koszulkę z motywem zachęcającym do ochrony danych osobowych (Szkoła Podstawowa im. Henryka Sienkiewicza w Niesułkowie, woj. łódzkie).

Równie ciekawe były inicjatywy, które angażowały dorosłych, jak np. wspólna nauka szyfrowania z udziałem uczniów i nauczycieli (Szkoła Podstawowa w Białołęce, woj. dolnośląskie) czy szkolenie dla rodziców z zakresu ochrony danych osobowych (Zespół Szkół Ekonomicznych w Częstochowie, woj. śląskie).

Wśród zaplanowanych inicjatyw edukacyjnych nie zabrakło także działań wychodzących poza szkolne mury, jak np.:

• wymiana informacji między szkołami za pośrednictwem platformy eTwinning (Organizator: Szkoła Podstawowa nr 5 im. prof. Adama Wodziczki w Swarzędzu, woj. wielkopolskie),

• lekcja otwarta nt. ochrony danych w mediach społecznościowych (Szkoła Podstawowa nr 4 im. Adama Mickiewicza w Lublinie, woj. lubelskie),

• spotkanie z inspektorem ochrony danych, podczas którego uczniowie mieli okazję bliżej poznać zasady przetwarzania danych osobowych oraz dowiedzieć się, jakie umiejętności i kompetencje są potrzebne, aby zostać inspektorem ochrony danych (Szkoła Podstawowa im. Konstytucji 3 Maja w Jaświłach, woj. podlaskie).

Wzorem lat ubiegłych, w obchody Dnia Ochrony Danych Osobowych aktywnie włączyły się też inne podmioty, w tym uczelnie wyższe, z którymi UODO ma zawarte porozumienie o współpracy. Wśród zaplanowanych z okazji Dnia Ochrony Danych Osobowych wydarzeń z udziałem ekspertów Urzędu znalazły się:

- Konferencja „IOD wobec nowych wyzwań w ochronie danych osobowych", 26.01.2021 r. Organizatorem konferencji było SABI – Stowarzyszenie Inspektorów Ochrony Danych[499].

  W programie konferencji przewidziano wystąpienia przedstawicieli różnych organizacji, którzy omówili aktualne problemy związane z wykonywaniem funkcji IOD. Podczas debaty przedstawiciel Urzędu Ochrony Danych Osobowych odniósł się do zagadnień związanych z realizacją przepisów wynikających z ogólnego rozporządzenia o ochronie danych w związku z wykonywaniem zadań przez IOD.
- Konferencja pt. „Ochrona danych osobowych – wyzwania 2021", 27.01.2021 r.

  Organizatorem konferencji była Kancelaria Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp.k.[500] Celem wydarzenia było upowszechnienie wiedzy na temat aktualnych zagadnień związanych z ochroną danych osobowych. W trakcie wydarzenia poruszono tematy dotyczące m.in. transferów danych osobowych do państw trzecich, przetwarzania danych przez sztuczną inteligencję oraz wpływu projektów rozporządzenia ePrivacy oraz ustawy – Prawo komunikacji elektronicznej na ochronę danych osobowych. Przedstawiciel UODO wygłosił prezentację pt. „Główne wyzwania dotyczące stosowania RODO w 2021 r. ze szczególnym uwzględnieniem transferów osobowych do państw trzecich". Przedstawione w prezentacji kwestie były niezwykle istotne dla praktyki prawa ochrony danych osobowych w 2021 roku.
- VII Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej, 3.02.2021 r.[501]

  Dni Otwarte UODO to inicjatywa Prezesa Urzędu Ochrony Danych Osobowych zapoczątkowana w 2012 roku. Co roku w organizację tego wydarzenia aktywnie włącza się Akademia WSB w Dąbrowie Górniczej, organizując w siedzibie Uczelni konferencję tematyczną połączoną z promocją dobrych praktyk w zakresie ochrony danych osobowych. W uroczystości otwarcia konferencji uczestniczył Mirosław Sanek, Zastępca Prezesa UODO. Natomiast eksperci Urzędu wzięli udział w debacie poświęconej skutecznemu administrowaniu bezpieczeństwem naszych danych, w szczególności tych przetwarzanych w systemach informatycznych, w Internecie czy w sektorze zdrowia.
- Międzynarodowa Konferencja zorganizowana przez wydawnictwo Privacy Laws & Business – PL&B, 23–25.02.2021 r.[502]

[499] https://sabi.org.pl/iii-dzien-iod/
[500] https://portalodo.com/konferencja-ochrona-danych-osobowych-wyzwania-2021/
[501] https://wsb.edu.pl/index.php?p=m&idg=Giod,3686
[502] https://www.privacylaws.com/events-gateway/events/poland2021/polandprog/

Wydarzenie to poświęcone było ochronie danych osobowych w Polsce, a jego adresatem – międzynarodowe korporacje prowadzące działalność m.in. w naszym kraju. Podczas konferencji przedstawiciele Urzędu Ochrony Danych Osobowych uczestniczyli w dwóch sesjach: „Przełomowe działania w zakresie egzekwowania RODO w Polsce" oraz „Relacje pracownicze na gruncie RODO i polskiego prawa pracy. Jak polski organ ochrony danych i inne organy regulacyjne podchodzą do COVID-19?". W Polsce konferencja PL&B organizowana była po raz trzeci. We wszystkich edycjach tego wydarzenia prelegentami byli przedstawiciele Urzędu.

2) Ogólnopolska Konferencja Naukowa 7. Forum Prawa Mediów Elektronicznych, 13–14.04.2021 r.

Organizatorami wydarzenia była Okręgowa Izba Radców Prawnych we Wrocławiu, Uniwersytet Wrocławski, Uniwersytet Opolski, Uniwersytet Szczeciński, Currenda sp. z o.o. oraz Ośrodek Naukowo-Szkoleniowy przy Krajowej Radzie Komorniczej. Hasłem przewodnim 7. edycji Ogólnopolskiej Konferencji Naukowej „Forum Prawa Mediów Elektronicznych" było „Prawo nowych technologii w obliczu pandemii COVID-19". Wybuch pandemii zintensyfikował rozważania i prace nad wdrożeniem nowych technologicznych rozwiązań w wielu dziedzinach życia i dlatego zagadnienia te znalazły się w centrum zainteresowania uczestników Forum. Tematyka tego wydarzenia objęła szeroko pojęte prawo nowych technologii, ze szczególnym uwzględnieniem zagadnień związanych z wymiarem e-sprawiedliwości, e-prywatności oraz e-zdrowia. Konferencja miała na celu ich analizę, ocenę z perspektywy upływu czasu oraz wypracowanie miarodajnych postulatów, które mogłyby przyczynić się do efektywnej informatyzacji państwa, przy uwzględnieniu zagrożeń i ograniczeń wynikających z ustawodawstwa krajowego i unijnego.

3) Seminarium Naukowe pt. „Sztuczna inteligencja – w kontekście ochrony danych osobowych", 26.04.2021 r.

Urząd Ochrony Danych Osobowych był organizatorem seminarium naukowego poświęconego tematowi sztucznej inteligencji (AI – z ang. artificial intelligence) i możliwościom wykorzystywania tej technologii w różnych obszarach życia codziennego. Celem tego spotkania było przede wszystkim zwiększenie wiedzy i świadomości na temat nowoczesnych rozwiązań, w które wpisuje się sztuczna inteligencja oraz związanych z nią regulacji w zakresie danych osobowych i prywatności. Prelegenci w swoich wystąpieniach przybliżyli słuchaczom m.in. kwestie zautomatyzowanego podejmowania decyzji, numerów identyfikacyjnych, które niejednokrotnie

stanowią danę osobową, federowanego uczenia maszynowego czy konstruowania humanocentrycznej AI, przybliżając nas tym samym do lepszego zrozumienia zasad działania algorytmów sztucznej inteligencji, w szczególności pod kątem odpowiednich regulacji prawnych, obejmujących zasady ochrony danych osobowych pozyskiwanych za jej pomocą.

4) Konferencja „AI w zdrowiu", 8.06.2021 r.

Organizatorami konferencji, która odbyła się pod patronatem Prezesa UODO byli: Polska Federacja Szpitali, Ambasada Brytyjska, Koalicja AI w Zdrowiu oraz Uniwersytet Medyczny im Piastów Śląskich we Wrocławiu. Konferencja ta była pierwszym ogólnopolskim wydarzeniem poświęconym wyłącznie sztucznej inteligencji w sektorze zdrowia. Przedstawiciel UODO wystąpił w sesji pn. „Obszar prawno-regulacyjny" oraz w panelu dyskusyjnym „Po co krajom strategia AI w zdrowiu?" prezentując, jak dalece zmiany technologiczne w obszarze AI mają wpływ na system ochrony zdrowia, rozwój badań naukowych i opiekę nad pacjentem.

5) XIII Konferencja „Bezpieczeństwo w Internecie – Global Games", 10–11.06.2021 r.

Organ nadzorczy był współorganizatorem wszystkich trzynastu dorocznych edycji konferencji z cyklu „Bezpieczeństwo w Internecie", które przy wsparciu merytorycznym i organizacyjnym UODO odbywały się na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie. Uczestnicy XIII Konferencji debatowali online na temat rynku gier video i e-sportu, grywalizacji, własności intelektualnej w świecie gier, nieuczciwej konkurencji i ochrony konsumenta, analityki danych, ochrony graczy w Internecie, a także o potrzebie wiedzy i umiejętności w zakresie cyberbezpieczeństwa, w tym – wykorzystywania gier i symulatorów w edukacji dla cyberbezpieczeństwa. Podczas tego wydarzenia przedstawiciel Urzędu przedstawił prezentację na temat przejrzystości przetwarzania danych w aplikacjach mobilnych.

6) Konferencja pt. „Szyfrowanie – skuteczny sposób na zabezpieczenie danych?", 19.07.2021 r.

Głównym celem konferencji, organizowanej przez Urząd Ochrony Danych Osobowych, była wymiana wiedzy i doświadczeń oraz próba odpowiedzi na pytanie: Czy korzystając z rozwiązań technologicznych dostępnych na polskim rynku można zwiększyć bezpieczeństwo danych i ograniczyć ryzyko wystąpienia braku zgodności? W wydarzeniu wzięli udział specjaliści z zakresu ochrony danych osobowych, którzy przedstawili rolę szyfrowania w zapewnieniu zgodności z przetwarzaniem danych osobowych. Konferencja odbyła się w formie panelu dyskusyjnego online,

podczas którego analizowano techniczne i formalno-prawne aspekty szyfrowania i uwierzytelniania, w tym zapewnienie bezpieczeństwa w fazie projektowania.

7) Seminarium Naukowe pt. „Sztuczna inteligencja a prawa podstawowe", 20.09.2021 r.

Głównym tematem omawianym podczas wydarzenia organizowanego przez Urząd Ochrony Danych Osobowych była wspólna opinia EROD i EIOD w sprawie wniosku Komisji Europejskiej na temat rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji. Dokument ten został przyjęty 18 czerwca 2021 roku podczas 50. posiedzenia plenarnego EROD. Eksperci udzielili odpowiedzi na pytania: Czy jest możliwy kompromis w sprawie ochrony danych osobowych w systemach AI? Czy sztuczna inteligencja może naruszać prawa podstawowe? Jakie są możliwe interakcje między ochroną danych osobowych a sztuczną inteligencją?

8) Konferencja Cyber24 Day. Warszawa, 12.10.2021 r.

Celem konferencji orgaznizowanej przez Grupę Defence24 było przedstawienie kwestii cyberbezpieczeństwa oraz budowania odporności społeczeństwa na zagrożenia hybrydowe. Podczas tego wydarzenia omówione zostały zagadnienia związane z rozwojem nowoczesnych technologii, cyberedukacji, sztucznej inteligencji (SI) czy komunikacji strategicznej. Dyskutowano m.in. o hakerach i ich znaczeniu, o Big Data jako domenie walki, o tym, jak SI może przeciwdziałać terroryzmowi, o edukacji żołnierzy i społeczeństwa w obronie kraju, o infrastrukturze krytycznej w dobie cyberzagrożeń, komunikacji strategicznej, rozwiązaniach technologii chmurowej, a także o pracy kobiet w branży cyberbezpieczeństwa.

9) Warsztaty UODO z IAB Polska, 20.10.2021 r.

Spotkanie z przedstawicielami IAB Polska miało charakter konsultacyjno-informacyjny, a ich tematem były zagadnienia związane z ochroną danych osobowych zawartych w plikach cookies, w tym m.in. sposobom udzielania zgód czy spełnienia obowiązku informacyjnego. Zaprezentowane zostało stanowisko firm członkowskich działających w ramach Grupy Roboczej IAB zajmującej się zagadnieniami ochrony danych osobowych. Podczas tego spotkania przedstawione zostały treści skarg europejskiej organizacji *NOYB*[503] złożonych na administratorów w związku z ich praktyką dot. stosowania tzw. banerów cookies. Poinformowano także, że podczas 55. posiedzenia plenarnego EROD powołano – w związku ze skargami *NOYB* – grupę zadaniową Cookie Banner Taskforce w ramach EROD, w pracach której uczestniczą przedstawiciele UODO. Zadaniem tej grupy jest ułatwienie komunikacji w zakresie otrzymanych skarg i podjęcie spójnych działań przy

[503] Nazwa *NOYB* pochodzi od „none of your business".

ich rozpatrywaniu. Na spotkaniu z przedstawicielami UODO, IAB Polska złożyła deklarację szybkiego zakończenia prac i złożenia organowi nadzorczemu do zatwierdzenia kodeks postępowania dla pracodawców branży internetowej.

10) Spotkanie w ramach prac przy Polskim Komitecie Normalizacyjnym, 22.10.2021 r.

W spotkaniu w sprawie prac nad uregulowaniem skutków prawnych podpisu biometrycznego uczestniczył przedstawiciel UODO, Polskiego Komitetu Normalizacyjnego (PKN) oraz eksperci współpracujący z Komitetami Technicznymi PKN (KT PKN). Tematem rozmów był stan normalizacji w zakresie projektowanej regulacji w zakresie możliwości składania oświadczeń woli w formie elektronicznej z wykorzystaniem podpisu biometrycznego (w rozumieniu digitalizacji podpisu własnoręcznego na przystosowanym urządzeniu). W szczególności debatowano nad:

– określeniem wymagań technicznych dostępu do danych, urządzeń i programów oraz sposobu składania podpisu biometrycznego w celu zapewnienia przydatności danych biometrycznych podpisów elektronicznych do badań identyfikacyjnych;

– określeniem norm i standardów technicznych podpisu biometrycznego pod elektronicznym oświadczeniem woli oraz sposobu jego przetwarzania.

Podkreślenia wymaga, że przedstawiciel UODO jest wieloletnim członkiem PKN KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych.

11) Spotkanie z przedstawicielami Departamentu Legislacyjnego Prawa Cywilnego Ministerstwa Sprawiedliwości, 22.10.2021 r.

Było to pierwsze z trzech spotkań zorganizowanych w związku z pracami koncepcyjnymi dotyczącymi oceny zasadności zmiany art. 78(1) § 1 Kodeksu cywilnego, prowadzonymi w Departamencie Legislacyjnym Prawa Cywilnego Ministerstwa Sprawiedliwości. Postulowana zmiana dotyczyć miała rozszerzenia o podpis zaufany i podpis osobisty katalogu podpisów umożliwiających zachowanie elektronicznej formy czynności prawnych. Podczas tych spotkań debatowano nad uregulowaniem statusu i skutków prawnych podpisu biometrycznego w kontekście ochrony danych osobowych w procesie składania takiego podpisu. W jednym z tych spotkań dodatkowo uczestniczyli przedstawiciele Grupy Roboczej ds. Rejestrów Rozproszonych i Blockchain, którzy analizowali także propozycje rozwiązań legislacyjnych dotyczących uregulowania w prawie krajowym skutków prawnych posługiwania się kwalifikowaną pieczęcią elektroniczną do składania oświadczeń woli w postaci elektronicznej. Omawiano różne rozwiązania

legislacyjne i możliwe ryzyka dla wprowadzenia nowych regulacji z punktu widzenia bezpieczeństwa obrotu i ochrony danych osobowych.

Terminy pozostałych dwóch spotkań przedstawiciela UODO w Ministerstwie Sprawiedliwości to 8.11.2021 r. i 17.12.2021 r.

12) Konferencja „Kodeks branżowy – Data Driven Marketing", 26.10.2021 r.

Kodeks postępowania to ważne narzędzie zapewniające zgodność działania organizacji z przepisami o ochronie danych osobowych. Dlatego podczas konferencji przedstawione zostały doświadczenia różnych rynków i dobre praktyki w tym zakresie. Przedstawiciel UODO omówił procedurę zatwierdzania kodeksów postępowania przez Prezesa Urzędu Ochrony Danych Osobowych, a także akredytowania podmiotu, który będzie monitorować jego przestrzeganie. Organizatorami wydarzenia byli: Polskie Stowarzyszenie Marketingu Bezpośredniego SMB oraz Wydział Zarządzania Uniwersytetu Warszawskiego.

13) VIII Krajowe Forum Ochrony Infrastruktury Krytycznej, 17.11.2021 r.

Podczas VIII Forum Ochrony Infrastruktury Krytycznej, którego organizatorem było Rządowe Centrum Bezpieczeństwa – RCB. przedstawiony został projekt zmiany ustawy o krajowym systemie cyberbezpieczeństwa oraz projekty dyrektyw: w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii – NIS II oraz odporności infrastruktury krytycznej – CER (Critical Entities Resilience).

W bloku tematycznym poświęconym współpracy administracji publicznej z operatorami IK omówione zostały między innymi kwestie dotyczące implementacji systemu S46 oraz zasad wyznaczania stref zakazu lotów BSP jako formy ochrony obiektów infrastruktury krytycznej. Natomiast tematem wiodącym panelu dyskusyjnego było utrzymanie ciągłości działania w czasie pandemii COVID-19.

14) Konferencja pt. „Nowe technologie w przetwarzaniu danych medycznych", 19.11.2021 r.

Spotkanie było okazją do omówienia najważniejszych wyzwań stojących przed służbą zdrowia w kontekście przetwarzania danych medycznych przez nowoczesne technologie. Głównym celem konferencji była wymiana wiedzy i doświadczeń oraz próba odpowiedzi na pytania: Jakie działania należałoby podjąć, aby podnieść poziom bezpieczeństwa danych medycznych? Jak kształtuje się przyszłość systemu opieki zdrowotnej w dobie zaawansowanych technologii? Organizatorem spotkania był Urząd Ochrony Danych Osobowych.

15) Spotkanie z Profesorem Davidem F. Forte, 15.12.2021 r.

Na zaproszenie Prezesa UODO gościł z wizytą w Polsce Profesor David F. Forte, amerykański prawnik, absolwent Harvardu, Columbii, Manchester University oraz Toronto University, wykładowca Uniwersytetów Cleveland oraz Princeton. Na spotkaniu w siedzibie organu ochrony danych osobowych wygłosił wykład pt. „Natural Law, Positive Law and the Right to Privacy" skierowany do pracowników Urzędu Ochrony Danych Osobowych. Prof. David F. Forte nakreślił podstawowe zagadnienia z zakresu teorii prawa naturalnego i prawa pozytywnego oraz przedstawił je w kontekście prawa do prywatności. Podczas dyskusji poruszono problematykę amerykańskich przepisów w obszarze prawa do prywatności, a także polskich doświadczeń na gruncie RODO.

2. Działalność informacyjna

W 2021 roku, podobnie jak rok wcześniej, działalność informacyjna UODO w wielu branżach zdominowana była przez temat pandemii COVID-19 i wynikających z niej skutków dla życia społeczno-gospodarczego. W analizowanym roku sprawozdawczym działalność informacyjna UODO w dalszym ciągu ukierunkowana była na działania służące ochronie danych osobowych i prywatności w tych obszarach, które pandemia szczególnie dotknęła – ochrona zdrowia, rynek pracy czy oświata. Działania informacyjne UODO dotyczyły także wielu innych zagadnień odnoszących się do ochrony danych osobowych, takich jak: naruszenia ochrony danych, realizacja praw wynikających z RODO, praktyczne aspekty realizacji obowiązków administratorów.

Sporą część działań komunikacyjnych poświęcono informowaniu o bieżącej działalności organu nadzorczego. W dalszym ciągu opinia publiczna z dużą uwagą śledziła zwłaszcza informacje dotyczące administracyjnych kar pieniężnych. UODO skupiało się w sferze informacyjnej również na przybliżaniu administratorom i inspektorom ochrony danych zagadnień prawnych dotyczących stosowania RODO.

Wzorem lat poprzednich w 2021 roku działania informacyjne obejmowały:

- współpracę z przedstawicielami mediów,
- prowadzenie działań informacyjno-edukacyjnych poprzez media własne,
- obecność w mediach społecznościowych,
- współpracę w działaniach komunikacyjnych z Partnerami Urzędu.

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,

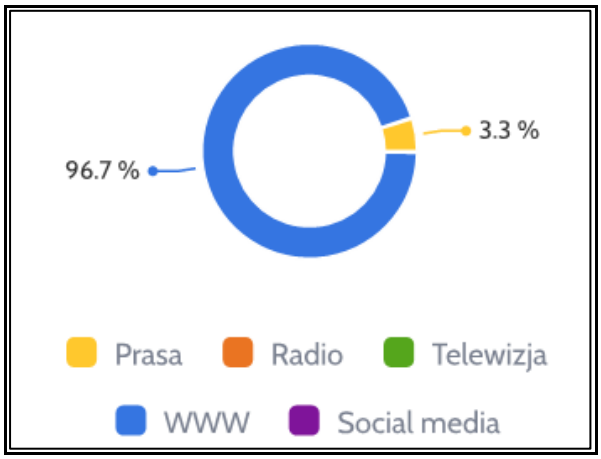
- udzielanie odpowiedzi na bieżące zapytania dziennikarzy mediów tradycyjnych i elektronicznych,
- aranżowanie wywiadów z ekspertami UODO i ich wystąpień medialnych,
- obsługa profili UODO w mediach społecznościowych (Twitter, YouTube),
- promocja w mediach programu edukacyjnego „Twoje dane – Twoja sprawa”,
- 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,
- tworzenie własnych treści wideo o charakterze edukacyjnym lub będących relacjami z wydarzeń organizowanych przez organ nadzorczy.

2.1. Współpraca z mediami

W ramach stałej współpracy z mediami, inspiracją do opracowanych przez dziennikarzy materiałów były informacje prasowe o tematyce ochrony danych i prywatności. Przygotowano **114** tego typu opracowań. Eksperci UODO udzielili blisko **30** wypowiedzi radiowo-telewizyjnych, które w dużej mierze dotyczyły tematów związanych z bieżącą działalnością organu nadzorczego lub były reakcją na zdarzenia wzbudzające zainteresowanie opinii publicznej.

W roku sprawozdawczym ukazało się w mediach tradycyjnych i na portalach internetowych ok. **21,5 tys**. informacji (w postaci artykułów, notek lub wzmianek). Tak wynika z danych zebranych przez Press-Service. Jeśli chodzi o wskaźnik zasięgu informacji[504], to wyniósł on 7,3 mld **potencjalnych kontaktów**, zaś dotarcie informacji[505] wyniosło 159,1 mln **realnych kontaktów**.

[504] Zasięg publikacji jest miarą określającą **liczbę potencjalnych kontaktów odbiorców z przekazem medialnym**. W prasie obliczany jest na podstawie sumy nakładów pisma, w Internecie wyrażany jest przez sumę liczby unikatowych użytkowników danego portalu. Natomiast w radiu i telewizji zasięgiem jest suma oglądalności bądź słuchalności danej stacji. Zasięg wyraża liczbę potencjalnych kontaktów z informacją, a nie liczbę osób, które mogły zetknąć się z nią. Zasięg wyższy niż liczba mieszkańców Polski oznacza, iż każda osoba mogła spotkać się z daną informacją kilkukrotnie.
[505] Dotarcie publikacji jest miarą określającą **liczbę realnych kontaktów odbiorców z przekazem medialnym**. Dotarcie jest przypisane do konkretnej publikacji. Różni się od zasięgu wprowadzeniem zmiennych odnoszących się do realnych zachowań odbiorców – sposobów i częstotliwości korzystania z kanałów przekazu.

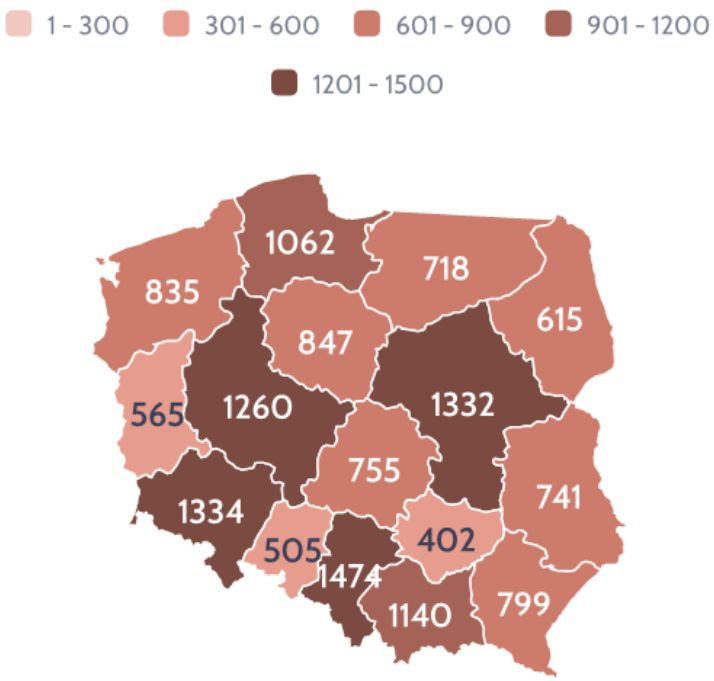


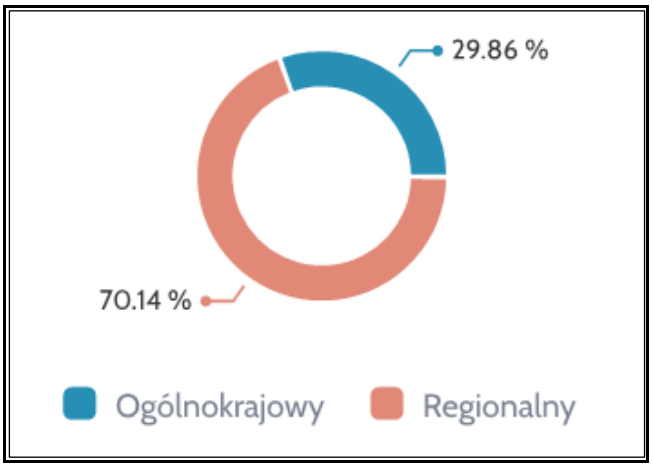
Wykres 14: **Procentowy udział publikacji nt. UODO, które ukazały się w 2021 roku, w podziale na medium.**

Dominującym środkiem przekazu nt. działalności UODO niezmiennie pozostaje Internet, co znajduje odzwierciedlenie w liczbie opublikowanych informacji za pośrednictwem mediów internetowych lub internetowych wydań mediów tradycyjnych.

Zauważalną tendencją było to, że poza prezentowaniem przez dziennikarzy informacji dotyczących różnorodnych działań związanych z zadaniami i decyzjami Prezesa UODO, coraz częściej dziennikarze zwracali się do rzecznika prasowego UODO z pytaniami dotyczącymi bardzo skomplikowanych przypadków. Ponadto media relacjonowały wydarzenia z udziałem ekspertów Urzędu, a także informowały o wielu przedsięwzięciach edukacyjnych podejmowanych przez UODO. Na uwagę zasługuje też fakt, że tematyka ochrony danych osobowych i związana z nią działalność organu nadzorczego w roku sprawozdawczym była często podejmowana przez media regionalne.

Potwierdza to poniższa ilustracja przedstawiająca liczbę informacji na temat UODO, które ukazały się w mediach regionalnych w 2021 roku, z podziałem na województwa oraz wykres przedstawiający procentowy udział aktywności mediów ogólnopolskich i regionalnych w zakresie przekazywania informacji dot. Urzędu.





Wykres 15: **Procentowy podział aktywności mediów ogólnopolskich i regionalnych w 2021 r.**

W roku sprawozdawczym uwagę mediów zwróciły opublikowane na stronie www.uodo.gov.pl m.in. teksty problemowe i poradnikowe oraz te, które zawierały wskazówki lub rekomendacje Prezesa UODO. Szczególnym zainteresowaniem dziennikarzy, zwłaszcza mediów branżowych, cieszyły się porady dla inspektorów ochrony danych dostępne na stronie internetowej Urzędu oraz artykuły publikowane w newsletterze.

Jeśli chodzi o tematykę, którą dziennikarze byli w ubiegłym roku szczególnie zainteresowani, to nadal popularnością cieszył się temat badania stanu trzeźwości pracowników przez pracodawców. Stanowisko UODO w tej sprawie, z czerwca 2019 roku, było jednym z najczęściej przypominanych,

obok dominującego w mediach wątku weryfikacji przez pracodawców faktu zaszczepienia pracowników. W obu sprawach brakuje bowiem podstaw prawnych do przetwarzania przez pracodawców danych o stanie zdrowia pracowników, na co UODO konsekwentnie zwraca uwagę. Innym tematem, który media często podejmowały w tym kontekście, powołując się na stanowiska lub aktywność organu nadzorczego, były działania zabezpieczające przed utratą danych, zwłaszcza tych, które mają zapobiec kradzieży tożsamości lub stanowią wskazówkę, jak postępować w przypadku zaistnienia takiego zdarzenia. Tematyka ta była podejmowana przez media ogólnopolskie, regionalne i lokalne. Co warto podkreślić, temat ten pojawiał się zarówno w mediach branżowych, jak i w mediach o profilu społeczno-gospodarczym.

Kontynuowana była również współpraca z ogólnopolskimi stacjami telewizyjnymi i radiowymi o profilu informacyjnym oraz społeczno-gospodarczym. Natomiast regularna współpraca z czołowymi agencjami informacyjnymi zaowocowała realizacją wielu materiałów informacyjnych.

W okresie sprawozdawczym kontynuowano współpracę z redakcjami czasopism branżowych, we współpracy z którymi publikowano cykliczne materiały eksperckie. Ponadto współpraca z mediami zaowocowała także patronatami medialnymi nad np. 15. Dniem Ochrony Danych Osobowych oraz XI edycją programu edukacyjnego „Twoje dane – Twoja sprawa".

2.2. Odpowiedzi na indywidualne pytania dziennikarzy

Szczególne miejsce w realizacji działań informacyjnych zajmuje udzielanie odpowiedzi na indywidualne pytania dziennikarzy. W roku sprawozdawczym 2021 odnotowano **278 pytań** skierowanych do rzecznika prasowego Urzędu. Jednocześnie warto podkreślić, że analiza tych pytań odsłoniła ciekawą tendencję – zmniejszyła się liczba zapytań o charakterze ogólnym, przybyło natomiast zapytań odnoszących się do bardzo złożonych problemów. Niejednokrotnie dziennikarze, kierując zapytania, które dotyczyły nt. wycieku danych osobowych czy innych naruszeń ochrony danych, zadawali wiele pytań szczegółowych odnoszących się do różnorodnych zagadnień, które składały się na dany problem. Dlatego w ujęciu ilościowym należy doprecyzować, że w ramach wspomnianych **278 zapytań,** faktycznie udzielono odpowiedzi na **1014 pytań szczegółowych**. Innym, wartym odnotowania spostrzeżeniem nt. zapytań prasowych jest zwrócenie uwagi na to, że media lokalne i regionalne oprócz zainteresowania szczegółami naruszeń ochrony danych, do jakich dochodziło u administratorów działających na danym terenie, przejawiały większą aktywność niż media ogólnopolskie w obszarze edukacji nt. ochrony danych osobowych i prywatności.

Wśród problemów, którymi interesowali się przedstawiciele mediów w 2021 roku były m.in. następujące tematy:

- przetwarzanie danych osobowych z wykorzystaniem nowoczesnych technologii, w tym zwłaszcza w odniesieniu do działań związanych z walką lub przeciwdziałaniem rozprzestrzenianiu się wirusa COVID-19;
- 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.

Jeśli chodzi zaś o RODO, to dziennikarze niezmiennie interesowali się:

- liczbą skarg, pytań oraz zgłoszonych naruszeń;
- korzystaniem przez Prezesa UODO z sankcji, w tym szczególnie nakładanie kar finansowych wobec administratorów łamiących zasady ochrony danych osobowych;
- reakcjami Prezesa UODO na wycieki danych;
- przetwarzaniem danych osobowych w relacjach pracodawca-pracownik, przez szkoły czy placówki zdrowia.

2.3. Strona internetowa i media społecznościowe

Rok sprawozdawczy 2021 był kolejnym, w którym Urząd Ochrony Danych Osobowych koncentrował się na rozwijaniu tzw. mediów własnych. Działania informacyjne prowadzone były głównie za pośrednictwem strony internetowej Urzędu – www.uodo.gov.pl. Z myślą o przedstawicielach różnych środowisk, regularnie publikowane tu były liczne materiały informacyjno-edukacyjne. W sumie zamieszczono **114 komunikatów**, wśród których znalazły się też informacje o konferencjach, webinariach i seminariach.

W roku 2021 strona internetowa organu nadzorczego została poddana modyfikacji w zakresie sposobu redagowania prezentowanych treści. Przede wszystkim dopracowano ją pod kątem wymogów osób ze szczególnymi potrzebami, poprzez zapewnienie dostępności cyfrowej. Zastosowano takie zasady redakcji tekstu oraz materiałów multimedialnych, które umożliwiają zapoznanie się z jej zasobami przez np. osoby niesłyszące czy niedowidzące. Materiały dostępne na stronie często miały postać wideo, co uczyniło je atrakcyjniejszymi w odbiorze i odpowiadało

aktualnym potrzebom komunikacyjnym odbiorców. Łącznie UODO przygotował **19 materiałów filmowych**.

Strona internetowa organu nadzorczego odgrywa bardzo ważną rolę informacyjną i edukacyjną. Wśród publikowanych na niej treści dużym zainteresowaniem opinii publicznej cieszyły się informacje o administracyjnych karach pieniężnych, dotyczące sygnałów, jakie UODO otrzymał od obywateli ws. telefonów od oszustów podających się m.in. za pracowników UODO (proceder ten dotyczy także innych instytucji), którzy prosili o udzielenie odpowiedzi na pytania dotyczące m.in. danych osobowych. UODO ostrzegał przed próbami wyłudzenia danych przez oszustów podszywających się pod pracowników UODO i dzwoniących z numeru telefonu wskazującego na UODO.

Dużą popularnością cieszyły się również komunikaty o charakterze edukacyjnym, przygotowane i opublikowane przez UODO na stronie internetowej, aby wspierać uczestników systemu ochrony danych. Opracowania te miały postać akcji informacyjnych, które dostarczały wielu wskazówek postępowania dla osób fizycznych oraz administratorów.

Dla przykładu, w 2021 roku realizowane były następujące akcje informacyjne:

W maju 2021 roku UODO dokonał podsumowania dotychczasowych doświadczeń w stosowaniu RODO, przeprowadzając akcję informacyjną pt. „Za nami trzy lata RODO”[506].

Początek wakacji to tradycyjnie czas, gdy UODO przypomina o zasadach bezpiecznego przetwarzania danych osobowych podczas wypoczynku. Latem 2021 roku przeprowadzono akcję edukacyjną pod hasłem „UODO radzi, jak zadbać o swoje dane podczas wakacji”[507].

[506] https://uodo.gov.pl/pl/138/2059
[507] https://uodo.gov.pl/pl/138/2101

We wrześniu 2021 roku UODO opublikował wskazówki „Szkolna RODO-wyprawka dla rodziców”[508]. To przygotowany przez UODO miniprzewodnik, który zawierał odpowiedzi na najczęściej zadawane przez rodziców (opiekunów prawnych) pytania o przetwarzanie danych osobowych uczniów.

W październiku 2021 roku UODO przedstawił rekomendacje „Jak efektywnie prowadzić prace nad kodeksem postępowania”[509]. Opracowanie zawierało użyteczne wskazówki przydatne podczas opracowywania kodeksu postępowania.

W listopadzie 2021 roku, w Światowy Dzień Seniora, UODO przedstawił „Kilka porad dla seniora”[510], w których zwrócono uwagę na konieczność rozsądnego posługiwania się np. dokumentem tożsamości, aby nie narażać się na utratę kontroli nad własnymi danymi.

Jak co roku, duże zainteresowanie mediów i opinii publicznej wzbudziły obchody Dnia Ochrony Danych Osobowych – w 2021 roku święto to było obchodzone po raz piętnasty – oraz informacje o programie edukacyjnym „Twoje dane – Twoja sprawa”, którego 11. edycja rozpoczęła się w 2021 roku. Uwagę mediów przyciągnęły także wydarzenia specjalne, takie jak webinaria tematyczne organizowane przez UODO, zwłaszcza te, które zrealizowano na potrzeby programu edukacyjnego „Twoje dane – Twoja sprawa”.

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. Istotnym wzmocnieniem działań informacyjnych

[508] https://uodo.gov.pl/pl/138/2164
[509] https://uodo.gov.pl/pl/426/2308
[510] https://uodo.gov.pl/pl/138/2212

prowadzonych przez UODO było systematyczne **komunikowanie za pośrednictwem mediów społecznościowych**, prowadzone w serwisach Twitter (@UODOgov_pl) oraz YouTube.

Profil UODO na **Twitterze** to dodatkowy kanał komunikacji, który służy do promocji wydarzeń organizowanych przez UODO lub podmioty zewnętrzne z udziałem przedstawicieli Urzędu. Zaletą Twittera jest możliwość bezpośredniej i szybkiej komunikacji z obywatelem. Pozwala to UODO aktywnie i na bieżąco reagować na pojawiające się wątpliwości czy problemy oraz jeszcze lepiej dostosowywać treści przekazów do potrzeb użytkowników.

W 2021 roku w serwisie Twitter UODO opublikował **493 wpisów** – podobnie jak w roku ubiegłym, w którym zamieszczono 490 tweetów. Znajdują się tu wypowiedzi eksperckie pracowników, a także komunikowane są inicjatywy i wydarzenia (szkolenia, debaty, wykłady, webinaria, konferencje czy seminaria naukowe) organizowane przez UODO i inne podmioty, bądź nad którymi Urząd objął patronat honorowy. Publikowane są też relacje z ich przebiegu i udostępniane zapisy nagrań.

W serwisie publikowane były wskazówki i porady dotyczące ochrony danych osobowych i ostrzeżenia przed zagrożeniami. Prowadzone były także działania promocyjne programu TDTS.

Na Twitterze na bieżąco pojawiały się też informacje o kolejnych wydaniach numeru newslettera dystrybuowanego przez UODO i odpowiedzi na pytania IOD. Ponadto w roku 2021 opublikowano tweety zawierające informacje o ofertach pracy i aktualnie trwających rekrutacjach, a także udostępniano niektóre wpisy zamieszczone na profilu EROD.

Profil UODO na Twitterze służy jako dodatkowy kanał komunikacji oraz promocji wydarzeń organizowanych przez UODO i zachęca do udziału w nich. Publikowane na nim treści mają charakter głównie informacyjny i merytoryczny, rzadziej wizerunkowy.

Zaletą Twittera jest możliwość bezpośredniej komunikacji z obywatelem, budowanie zaufania do UODO. Należy też wspomnieć, że korzystając z Twittera, informacje są przekazywane w sposób skuteczny i szybki. Pozwala to UODO aktywnie i na bieżąco reagować na pojawiające się wątpliwości czy problemy oraz jeszcze lepiej dostosowywać treści przekazów do potrzeb użytkowników.

Z kolei treści prezentowane na kanale UODO na **YouTube** mają charakter głównie edukacyjny – prezentują filmy z przygotowanych przez UODO webinariów i konferencji.

Wśród materiałów dostępnych na YouTube rekordową liczbę odsłon odnotowało wideo zawierające instrukcję składania skargi do organu nadzorczego (4,2 tys. wyświetleń) oraz nagranie

wideo zawierające zapis organizowanego przez Departament Komunikacji Społecznej szkolenia dla inspektorów ochrony danych osobowych z sektora oświaty (ok. 4 tys. wyświetleń).

Podsumowując, prawie 100% treści zamieszczanych na oficjalnym profilu Twitterze czy kanale YouTube odsyła na stronę www.uodo.pl, która jest podstawowym źródłem informacji o działalności Urzędu. Warto też dodać, że UODO prowadzi zarówno anglojęzyczną stronę internetową (www.uodo.gov.pl/en) oraz anglojęzyczny profil na Twitterze (@PDPO_Poland), które są wykorzystywane jako kanały komunikacji w ramach współpracy międzynarodowej.

2.4. Newsletter UODO dla inspektorów ochrony danych – IOD

W 2021 roku kontynuowano wydawanie cyklicznego **„Newslettera UODO dla Inspektorów Ochrony Danych”**[511]. W roku sprawozdawczym 2021 ukazało się 12 wydań. O jego popularności świadczy stale rosnąca liczba subskrybentów. Na koniec grudnia 2021 roku newsletter trafił do **8 592** subskrybentów. To **wzrost o 13%** w porównaniu do analogicznego okresu roku poprzedniego (grudzień 2020 roku – 7 565 subskrybentów).

Na ilustracji poniżej przedstawiony został nagłówek tytułowy „Newslettera UODO dla Inspektorów Ochrony Danych”.

„Newsletter UODO dla Inspektorów Ochrony Danych” stanowi cenne źródło informacji o działalności Urzędu. Publikowane tu treści wpisują się w działalność informacyjno-edukacyjną Urzędu. Początkowo powstał z myślą o bieżącym informowaniu inspektorów ochrony danych. Jednak prezentowane w nim materiały okazały się być przydatne każdemu odbiorcy, bowiem w skuteczny sposób przybliżały tematykę ochrony danych osobowych. Duża część subskrybentów to dziennikarze, a także przedstawiciele podmiotów prawnych. Przekazywane materiały odnoszą się do

[511] https://uodo.gov.pl/p/archiwum-newslettera-dla-iod

oficjalnych wystąpień organu nadzorczego, udzielane są ogólne wskazówki o stosowaniu przepisów RODO czy wnioski płynące z decyzji administracyjnych, w szczególności tych, w których nałożono administracyjne kary pieniężne. Newsletter służy też do przedstawiania zaangażowania UODO w prace na arenie międzynarodowej.

Biuletyn ten pozwala organowi nadzorczemu nie tylko na budowanie relacji z wszystkimi osobami, którym bliska jest tematyka ochrony danych osobowych, ale także utrzymuje z nimi stałą, comiesięczną komunikację.

Bazując na przeprowadzonym w 2020 roku badaniu ankietowym wśród czytelników newslettera – którego rezultatem była m.in. zmieniona szata graficzna – w 2021 roku kontynuowano prace nad dostosowaniem prezentowanych treści do potrzeb czytelników.

2.5. Infolinia UODO

Każdego dnia pracownicy infolinii UODO odbierają kilkadziesiąt telefonów od osób fizycznych i podmiotów prawnych, upowszechniając w ten sposób wiedzę o ochronie danych osobowych, skutecznie informując obywateli na temat przysługujących im praw, a także o działalności Urzędu. 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. Pracownicy UODO udzielają informacji również w języku angielskim za pośrednictwem specjalnej infolinii międzynarodowej.

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.

Tematyka pytań kierowanych w 2021 roku do Urzędu za pośrednictwem infolinii była bardzo różnorodna. Najczęściej zadawane pytania dotyczyły (oprócz pytań o stan sprawy toczącej się w Urzędzie) następujących zagadnień:

- ochrona danych osobowych podczas pandemii (jak dbać o bezpieczeństwo swoich danych osobowych w czasie pandemii, co robić, gdy otrzymamy podejrzaną wiadomość od nieznanego adresata z linkiem do łączenia, itd.);

- przetwarzanie danych osobowych przez pracodawców (sprawy z zakresu relacji pracodawca – pracownik, udostępnienie danych pracownika – w tym danych prywatnych – nieupoważnionej osobie, np. współpracownikowi lub klientowi, nadużywanie prywatnego numeru telefonu pracownika przez pracodawcę, przetwarzanie szczególnej kategorii danych osobowych pracowników, w tym danych o stanie zdrowia, w tym zaświadczeń o zaszczepieniu przeciwko COVID-19);
- prawidłowe postępowanie w przypadku naruszeń (jak ustrzec się przed negatywnymi konsekwencjami naruszenia, jakie należy podjąć kroki formalno-prawne, by zapobiec im w przyszłości);
- niechciany telemarketing (identyfikacja nieuczciwych praktyk i przetwarzania danych osobowych w sposób niezgodny z prawem przez niektóre firmy, prawa przysługujące obywatelom na podstawie RODO oraz obowiązki ciążące na administratorach danych, czy numer telefonu stanowi dane osobowe, jakie podjąć działania, by przerwać proceder otrzymywania niechcianych telefonów).

Inne tematy, które pojawiały się podczas rozmów na infolinii, to kwestie związane z monitoringiem wizyjnym, przetwarzaniem danych osobowych we wspólnotach i spółdzielniach mieszkaniowych, a także żądania przesyłania skanów dokumentów tożsamości przez internetowe platformy sprzedażowe w celu odblokowania środków otrzymanych ze sprzedaży na kontach użytkowników.

Techniczne uwarunkowania infolinii nie pozwalają na przedstawienie dokładnej liczby odebranych połączeń. Nie mniej pracownicy infolinii przeprowadzili w 2021 roku łącznie **ok. 17 500 rozmów, co w przybliżeniu stanowi 69 rozmów przeprowadzanych w każdy dzień roboczy**. Pytania zadawane za pośrednictwem infolinii odnoszą się coraz częściej do bardzo złożonych problemów. Trzeba mieć na uwadze, że na jedno połączenie często składało się kilka pytań, dotyczących różnych i skomplikowanych prawnie zagadnień. Na podstawie analizy treści takich pytań tworzone były m.in. komunikaty prasowe i praktyczne wskazówki, będące odpowiedzią na najczęściej sygnalizowane problemy. Pytania te stanowiły także dla UODO ważne źródło wiedzy, z jakimi problemami mierzą się interesanci Urzędu.

2.6. Inne

W 2021 roku, w ramach prac Sieci Komunikacyjnej (The EDPB Communications Network), odbyło się 12 spotkań rzeczników prasowych organów ochrony danych osobowych.

Grupa ta jest platformą wymiany wiedzy, doświadczeń, działań pomiędzy poszczególnymi członkami 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 karach nakładanych przez te organy. Podczas tych spotkań omawiano plany działania poszczególnych organów ochrony danych osobowych oraz wspólne działania komunikacyjne w ramach EROD. Każdy komunikat wydawany po posiedzeniach plenarnych Rady był przedmiotem zainteresowania sieci komunikacji rzeczników prasowych.

Spotkania Communications Network to także współpraca przy okazji ważnych wydarzeń, jak obchody 15. Dnia Ochrony Danych Osobowych. W 2021 roku z okazji obchodów tego dnia przedstawiciele organów nadzorczych wystąpili we wspólnej kampanii wideo. Także trzecia rocznica rozpoczęcia stosowania RODO stała się okazją do podjęcia wspólnych inicjatyw.

W 2021 roku w ramach spotkań rzeczników prasowych, przedstawiciele UODO uczestniczyli w pracach nad następującymi publikacjami:

- „2020 Sprawozdanie Roczne. Zapewnienie Praw Do Ochrony Danych w Zmieniającym Się Świecie – Streszczenie”[512],
- „RODO i przysługujące prawa. Ochrona danych, prawa podstawowe”[513],
- „EROD: gwarantowanie wszystkim takich samych praw”[514].

Rok 2021 zaowocował również działaniami informacyjnymi, które UODO zainicjował i zrealizował we współpracy z innymi podmiotami. Przykładem takiego działania było badanie pt. „Ochrona danych osobowych w czasie pandemii”, przeprowadzone pod patronatem UODO przez serwis ChronPESEL.pl i Krajowy Rejestr Długów.

Poniżej przedstawione zostały grafiki poświęcone publikacjom zawierającym omówienie wspomnianego wyżej badania.

[512] https://edpb.europa.eu/system/files/2021-10/edpb_es_080621_pl.pdf
[513] https://edpb.europa.eu/system/files/2021-04/edpb-leaflet-gdpr_and_your_rights_pl.pdf
[514] 2020_06_22_one-stop-shop_leaflet_pl.pdf (europa.eu)

Młodzi Polacy świadomi zagrożeń i przygotowani do ochrony danych osobowych w czasie pandemii

Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków – raport z badań

Badanie pt. „Ochrona danych osobowych w czasie pandemii" miało charakter ogólnopolski i zostało przeprowadzone w marcu 2021 roku. Wnioski z badania zostały przedstawione w dwuczęściowym raporcie.

Pierwsza część raportu pt. „Młodzi Polacy świadomi zagrożeń i przygotowani do ochrony danych osobowych w czasie pandemii"[515] została opublikowana pod koniec kwietnia 2021 r. Opracowanie to pozwoliło zrozumieć skalę problemu, jakim jest wyłudzanie danych osobowych. Przedstawione wyniki wykazały, że ponad 43 proc. Polaków obawiało się, że w czasie pandemii padnie ofiarą oszustów wyłudzających dane osobowe, a prawie 30 proc. spotkało się już z taką próbą. Ponadto blisko 70 proc. ankietowanych zauważyło większą aktywność oszustów wyłudzających dane osobowe na przestrzeni ostatnich miesięcy.

Z kolei druga część raportu „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków"[516] (opublikowana w maju 2021 r.) zobrazowała stan świadomości Polaków w odniesieniu do zagrożeń związanych z wyłudzaniem danych osobowych czy kradzieży tożsamości. Im większe poczucie zagrożenia, tym Polacy podejmowali większe starania o pogłębienie wiedzy na temat cyberbezpieczeństwa i konsekwencji działań cyberprzestępców. Blisko 2/3 dorosłych Polaków (61,2 proc.) zadeklarowało, że wie, jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych. Prawie 24% ankietowanych wskazało, że podczas rozmowy

[515] https://uodo.gov.pl/pl/138/2021
[516] https://uodo.gov.pl/pl/138/2062

telefonicznej zostali poproszeni o podanie danych osobowych, takich jak: imię, nazwisko i numer PESEL. UODO nieraz przestrzegał przed podawaniem danych np. podczas rozmów telefonicznych, osobom nieznanym, zwłaszcza kiedy nie można zweryfikować, czy są tymi, za których się podają. Ponadto 34,3 proc. ankietowanych wskazało, że sytuacja, w której zostali poproszeni o dane osobowe dotyczyła rozmowy z pracownikiem banku, w którym mieli konto.

Jak wskazują badania, o takie informacje w trakcie rozmowy telefonicznej prosiły również osoby podszywające się m.in. za przedstawicieli firm energetycznych, gazowych i telekomunikacyjnych oraz pracowników banków, w których ankietowani nie mieli konta.

Wyniki raportu „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków" zostały zaprezentowane podczas webinarium połączonego z debatą ekspertów z zakresu ochrony danych osobowych[517]. Podczas tej debaty zaprezentowane zostały działania UODO związane z ochroną numeru PESEL. Eksperci wskazali w niej na brak konsekwencji w działaniach systemowych – z jednej strony zwrócili uwagę, że numer PESEL jest niepowtarzalny i należy go chronić, a z drugiej strony tworzone są rejestry publiczne zawierające numer PESEL, które czynią go powszechnie dostępnym i jednocześnie pozbawionym jakiejkolwiek ochrony.

Opracowany w wyniku badań dwuczęściowy raport miał na celu podniesienie świadomości społeczeństwa w zakresie ochrony danych osobowych. Zaprezentowane publikacje pokazały, że zagadnienia ochrony danych osobowych, w tym problemy, z jakimi polskie społeczeństwo spotkało się w analizowanym okresie marzec 2020 r. – marzec 2021 r., odcisnęły się na jego życiu codziennym. W raporcie zostały opublikowane analizy nt. metod przestępców próbujących wyłudzić dane osobowe, a także komentarze i podpowiedzi ekspertów, jak postępować w sytuacji, gdy już dojdzie do wyłudzenia danych osobowych. Nie zabrakło w nim także porad, które pozwolą Polakom uchronić się od wyłudzenia dotyczących ich danych osobowych.

IV. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych

1. Współpraca w ramach EROD

Jednym z ustawowych zadań organu właściwego w sprawach ochrony danych osobowych jest uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką

[517] https://uodo.gov.pl/pl/138/2062

ochrony danych osobowych. Do zadań Prezesa UODO należy współpraca z organami nadzorczymi innych państw członkowskich UE, w szczególności w ramach działań Europejskiej Rady Ochrony Danych (dalej także „Rada" lub „EROD") ustanowionej ogólnym rozporządzeniem o ochronie danych osobowych (RODO), zastępującej Grupę Roboczą Artykułu 29, do której należy Prezes UODO.

Europejska Rada Ochrony Danych jest organem UE posiadającym osobowość prawną, który wykonuje swoje zadania i korzysta z uprawnień z zachowaniem pełnej niezależności. Zgodnie z zasadą niezależności zapisaną w art. 69 RODO, w toku wypełniania swoich zadań lub wykonywania uprawnień Rada działa w sposób bezstronny i całkowicie niezależny. Rada ma siedzibę w Brukseli, która jest głównym miejscem prowadzenia jej działalności.

EROD 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 Europejskiego Obszaru Gospodarczego (EOG). Europejską Radę Ochrony Danych ustanowiono ogólnym rozporządzeniem o ochronie danych. EROD zapewnia spójne stosowanie RODO, a także realizację zadań wymienionych w dyrektywie 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 (dalej „dyrektywa 2016/680) oraz w innych właściwych instrumentach prawodawczych zgodnie z prawem UE.

W skład Rady wchodzą: 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 („EIOD") lub ich przedstawiciele. W odniesieniu do działań Rady związanych z RODO, organy nadzorcze państw EOG-EFTA mają takie same prawa i obowiązki jak organy nadzorcze państw członkowskich UE, z wyjątkiem prawa do głosowania i do kandydowania w wyborach na przewodniczącego lub wiceprzewodniczących, o ile nie określono inaczej w regulaminie wewnętrznym EROD. Organy te mają prawo wyrażenia swojego stanowiska na temat wszystkich omawianych lub poddanych pod głosowanie kwestii.

Komisja Europejska ma prawo uczestniczyć w pracach Rady bez prawa głosu i wyznacza swojego przedstawiciela w Radzie. Urząd Nadzoru EFTA ma prawo uczestniczyć w działaniach Rady dotyczących RODO bez prawa do głosowania oraz wyznacza swojego przedstawiciela.

Jeżeli w państwie członkowskim za monitorowanie stosowania przepisów RODO oraz dyrektywy 2016/680 odpowiada więcej niż jeden organ nadzorczy, to zgodnie z przepisami prawa krajowego wyznaczony zostaje wspólny przedstawiciel. To samo dotyczy organów nadzorczych państw EOG-EFTA odpowiedzialnych za monitorowanie stosowania przepisów zgodnie z RODO.

EROD działa na podstawie regulaminu wewnętrznego, który określa najważniejsze zasady działania Europejskiej Rady Ochrony Danych[518]. Zasady te dotyczą organizacji Europejskiej Rady Ochrony Danych, wspólnej pracy jej członków, wyboru przewodniczącego i wiceprzewodniczących i metod pracy EROD.

Protokół ustaleń jest porozumieniem, które określa warunki współpracy pomiędzy EROD i EIOD. Ma on również zastosowanie do personelu sekretariatu, którego obsługę zapewnia EIOD w celu wsparcia Europejskiej Rady Ochrony Danych[519].

2. Podgrupy ekspertów EROD

Zgodnie z art. 25 jej regulaminu wewnętrznego, EROD działa poprzez wewnętrzne podgrupy ekspertów, w skład których wchodzą przedstawiciele organów nadzorczych, Europejskiego Inspektora Ochrony Danych i Komisji Europejskiej. Podgrupy ekspertów wspierają Radę w wykonywaniu jej zadań i dążą do osiągnięcia porozumienia w sprawie każdego wniosku przedłożonego Radzie. Rada, działając przez podgrupy ekspertów, realizuje zadania zgodnie z dwuletnim programem prac. Wstępny plan roczny powinien być przygotowany na początku każdego roku przez koordynatora, ze wskazaniem liczby posiedzeń oraz, w miarę możliwości, harmonogramu i zagadnień, które zostaną omówione. Na podstawie art. 70 ust. 1 lit. u) RODO, EROD powołuje również dedykowane grupy zadaniowe, które służą koordynacji działań organów nadzorczych.

W ramach prac podgrup i grup zadaniowych przedstawiciele polskiego organu nadzorczego, wraz z reprezentantami pozostałych organów, opracowują dokumenty EROD, w tym opinie, wytyczne, zalecenia i najlepsze praktyki w celu promowania wspólnego zrozumienia RODO i dyrektywy 2016/680, a także biorą udział w doradzaniu Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych w UE. Dokumenty te są następnie przedmiotem dyskusji

[518] https://edpb.europa.eu/our-work-tools/our-documents/publication-type/rules-procedure_pl
[519] Protokół ustaleń dostępny jest na stronie EROD, pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/memorandum-understanding/memorandum-understanding_pl .

i zostają przyjmowane na comiesięcznych posiedzeniach plenarnych EROD, podczas których polski organ nadzorczy reprezentowany jest przez Prezesa UODO lub jego zastępców.

Poszczególne podgrupy ekspertów koncentrują się na konkretnych obszarach ochrony danych i wspierają EROD w wykonywaniu jej zadań. Poniżej zamieszczony jest wykaz podgrup eksperckich i opis zakresów ich zadań. W 2021 roku pracownicy UODO czynnie reprezentowali polski organ nadzorczy, uczestnicząc w pracach następujących podgrup ekspertów EROD:

1. **Podgrupa Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (ang. Borders, Travel and Law Enforcement Expert Subgroup**), do spraw dotyczących dyrektywy 2016/680 (tzw. dyrektywy policyjnej), transgranicznych wniosków o udostępnienie e-dowodów, decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony danych w państwach trzecich, dostępu do danych przez organy ścigania i krajowych organów wywiadowczych w państwach trzecich (np. działania podjęte w związku z wyrokiem TSUE w sprawie Schrems II), kontroli nad danymi o przelocie pasażera (PNR) i kontroli granicznych;
2. **Podgrupa Ekspertów ds. Zgodności, e-Administracji i Zdrowia (ang. Compliance, e-Government and Health Expert Subgroup)**, która jest właściwa do spraw m.in. kodeksów postępowania, certyfikacji i akredytacji, oceny skutków dla ochrony danych, uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, zgodności z prawem publicznym, administracji elektronicznej, zdrowia i przetwarzania danych osobowych do celów badań naukowych;
3. **Podgrupa Ekspertów ds. Współpracy (Cooperation Expert Subgroup**), która jest właściwa do spraw m.in. procedur współpracy w ramach RODO, międzynarodowej wzajemnej pomocy i innych narzędzi współpracy służącym egzekwowaniu RODO poza UE (art. 50 RODO);
4. **Podgrupa Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup**), która zajmuje się analizą zapotrzebowania na dodatkowe wyjaśnienia lub wytyczne w oparciu o praktyczne doświadczenia związane ze stosowaniem rozdziałów VI, VII i VIII RODO, oceną konieczności aktualizowania narzędzi podgrupy Cooperation, monitorowania postępowań, wytycznych dotyczących praktycznego stosowania rozdziału VII i VIII RODO;
5. **Podgrupa Ekspertów ds. Finansowych (Financial Matters Expert Subgroup**), która jest właściwa do spraw m.in. stosowania zasad ochrony danych w sektorze finansowym, np. przy automatycznej wymianie danych osobowych do celów podatkowych, a także wpływu FATCA na ochronę danych osobowych i wzajemnego oddziaływania dyrektywy w sprawie usług płatniczych i RODO;

6. **Podgrupa Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup**), która jest właściwa do spraw m.in. wytycznych dotyczących rozdziału V RODO, w szczególności przeglądu decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony danych w państwach trzecich, wytycznych dotyczących art. 46 RODO, przeglądu uzgodnień administracyjnych między władzami i organami publicznymi, kodeksów postępowania i certyfikacji, jako narzędzia do przekazywania danych, wytycznych dotyczących zakresu terytorialnego i wzajemnego oddziaływania z Rozdziałem V RODO, wymiany informacji na temat przeglądu wiążących reguł korporacyjnych i klauzul umownych *ad hoc* zgodnie z art. 64 RODO;
7. **Podgrupa Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup**), która opracowuje i testuje narzędzia informatyczne wykorzystywane przez EROD, z naciskiem na kwestie praktyczne, tj. zbieranie informacji zwrotnych na temat systemów informatycznych od użytkowników, w tym przede wszystkim IMI – narzędzia wymiany informacji na rynku wewnętrznym;
8. **Podgrupa Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup)**, opracowująca wytyczne dotyczące podstawowych pojęć i zasad RODO, w tym rozdziału I, II, III, IV oraz IX RODO;
9. **Podgrupa Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup)**, właściwa do analizy usług mediów społecznościowych oraz istniejących i powstających funkcji oferowanych przez nie, w tym leżących u ich podstaw czynności przetwarzania danych i związanych z nimi zagrożeń dla praw i wolności osób fizycznych, opracowywania wytycznych, zaleceń i najlepszych praktyk w odniesieniu do oferowania i korzystania z funkcji mediów społecznościowych;
10. **Podgrupa Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup**), zajmuje się kwestiami strategicznymi, które mają wpływ na całą EROD i wyjaśnianiem kwestii, które nie zostały jednoznacznie rozstrzygnięte w ramach podgrup ekspertów;
11. **Podgrupa Ekspertów ds. Technologii (Technology Expert Subgroup**), która jest właściwa do spraw związanych z technologiami, innowacjami, bezpieczeństwem informacji, poufnością komunikacji, łącznością elektroniczną i prywatnością, szyfrowaniem, powiadamianiem o naruszeniu ochrony danych, geolokalizacją i innymi narzędziami śledzenia w kontekście pandemii COVID-19 oraz audytami aplikacji mobilnych.

3. Grupy zadaniowe EROD

W 2021 r. pracownicy UODO reprezentowali polski organ nadzorczy także 4 grupach zadaniowych, w tym:

1. **Grupie zadaniowej ds. bannerów cookie,** której celem jest koordynowanie działań organów nadzorczych EOG w odpowiedzi na skargi dotyczące bannerów cookie złożonych przez NOYB;
2. **Grupie zadaniowej ds. administracyjnych kar pieniężnych,** której zadaniem jest opracowanie wytycznych w sprawie harmonizacji obliczania przez krajowe organy nadzorcze administracyjnych kar pieniężnych;
3. **Grupie zadaniowej ds. 101 skarg,** która zajmuje się rozpatrywaniem skarg wniesionych przez organizację NOYB, reprezentującą Skarżących. Skargi dotyczą Spółek w 30 państwach członkowskich UE i EOG, związku z korzystaniem przez administratorów z narzędzi, za pomocą których dane przekazywane są do państw trzecich w sposób niezgodny z wyrokiem TSUE w sprawie C-311/18 (Schrems II), który rozstrzygnął, kiedy przekazywanie danych do państw trzecich jest legalne[520];
4. **Grupie zadaniowej ds. środków uzupełniających,** której zadaniem było stworzenie zaleceń pomocnych dla administratorów i podmiotów przetwarzających w wykonywaniu ich obowiązku polegającego na wskazywaniu i wdrażaniu odpowiednich środków dodatkowych w celu zapewnienia należytej ochrony przy przekazywaniu danych do państw trzecich.

4. Sieć Komunikacyjna

Przedstawiciele Departamentu Komunikacji Społecznej Urzędu Ochrony Danych Osobowych uczestniczą w pracach Sieci Komunikacyjnej EROD, zajmującej się przygotowywaniem oświadczeń prasowych i komunikatów Rady, a także wszelką komunikacją EROD z mediami. Sieć Komunikacyjna dba także o to, by w sprawach dotyczących wspólnych działań organów zachować spójną komunikację. Sieć przygotowuje także wspólne działania organów w ramach corocznych obchodów międzynarodowego Dnia Ochrony Danych Osobowych.

5. Sieć Inspektorów Ochrony Danych

Inspektor Ochrony Danych UODO jest członkiem Sieci Inspektorów Ochrony Danych (DPO Network). Sieć IOD została powołana podczas posiedzenia plenarnego EROD w lipcu 2019 roku w celu umożliwienia wymiany najlepszych praktyk pomiędzy inspektorami ochrony danych organów

[520] Więcej informacji na temat tego wyroku znajduje się na stronie UODO: https://uodo.gov.pl/pl/138/1614.

nadzorczych i stworzenia bardziej zharmonizowanego podejścia między nimi. Opracowywane w jej ramach zalecenia są rekomendacjami nieformalnymi, wewnętrznymi i dotyczą wyłącznie organów nadzorczych.

Sieć Inspektorów Ochrony Danych ma charakter nieformalnej sieci, niezależnej w udzielaniu opinii i porad. W jej skład wchodzą wszyscy inspektorzy ochrony danych organów nadzorczych, inspektor ochrony danych EROD oraz inspektor ochrony danych EIOD. Działania niezależnej Sieci IOD pozwalają na lepszą koordynację między EROD, organami i EIOD w zakresie korzystania z narzędzi związanych z ich wspólnymi działaniami (np. IMI).

6. Nadzór nad wielkoskalowymi systemami

Istotnym obszarem działalności Prezesa UODO w 2021 roku pozostawała także współpraca międzynarodowa w ramach zapewnienia skoordynowanego nadzoru nad unijnymi wielkoskalowymi systemami informatycznymi, a także uczestnictwo w Radzie Współpracy Europolu. W ramach realizacji powyższego zadania pracownicy UODO uczestniczyli w posiedzeniach następujących organów: Grupy ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen (SIS II)[521], Grupy ds. Koordynacji Nadzoru nad Systemem Informacji Celnej (CIS)[522], Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS)[523], Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac[524], a także w Radzie Współpracy Europolu[525]. Przedstawiciele UODO uczestniczyli też w pracach Komitetu Skoordynowanego Nadzoru (CSC), o którym mowa poniżej.

Komitet ds. Skoordynowanego Nadzoru („Komitet")[526] zapewnia skoordynowany nadzór organów ochrony danych nad wielkoskalowymi systemami informatycznymi oraz organami, urzędami i agencjami UE objętymi jego zakresem, zgodnie z art. 62 rozporządzenia 2018/1725 lub z aktem prawnym UE ustanawiającym wielkoskalowy system informatyczny lub organ, urząd lub agencję UE[527].

[521] Więcej informacji o SIS II dostępnych jest na stronie UODO: https://uodo.gov.pl/pl/p/schengen.
[522] Więcej informacji o CIS dostępnych jest na stronie UODO: https://uodo.gov.pl/pl/p/wspolny-organ-nadzorczy-ds-celnych.
[523] Więcej informacji o VIS dostępnych jest na stronie UODO: https://uodo.gov.pl/pl/435.
[524] Więcej informacji o Eurodac dostępnych jest na stronie UODO: https://uodo.gov.pl/pl/p/eurodac.
[525] Więcej informacji o Europolu dostępnych jest na stronie UODO: https://uodo.gov.pl/pl/p/europol.
[526] Komitet ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee – CSC).
[527] Dokumenty Komitetu oraz przegląd systemów informatycznych i agencji UE objętych obecnie nadzorem Komitetu znaleźć można w wyodrębnionej części strony internetowej EROD: https://edpb.europa.eu/csc/about-csc/legal-framework-coordinated-supervision-committee_pl.

W ramach swojej misji, polegającej na zapewnieniu skoordynowanego nadzoru nad niektórymi wielkoskalowymi systemami informatycznymi oraz organami, biurami i agencjami UE, Komitet może: wymieniać istotne informacje, pomagać organom nadzorczym w przeprowadzaniu audytów i inspekcji, badać trudności w interpretacji lub stosowaniu aktu prawnego UE ustanawiającego wielkoskalowy system informatyczny lub urząd, organ lub agencję UE podlegające skoordynowanemu nadzorowi, badać problemy związane ze sprawowaniem niezależnego nadzoru lub z wykonywaniem praw osób, których dane dotyczą, opracowywać zharmonizowane propozycje rozwiązań problemów, a także propagować wiedzę na temat prawa ochrony danych.

Co dwa lata Komitet sporządza również sprawozdanie ze swojej działalności w zakresie skoordynowanego nadzoru. Komitet przekazuje to sprawozdanie do EROD w celu przedłożenia go Parlamentowi Europejskiemu, Radzie, Komisji i innym adresatom, jeżeli jest to wyraźnie wymagane w akcie prawnym UE ustanawiającym wielkoskalowy system informatyczny lub organ, urząd lub agencję UE podlegające skoordynowanemu nadzorowi.

Komitet został ustanowiony w ramach EROD, zgodnie z art. 62 rozporządzenia 2018/1725. Komitet korzysta z autonomicznego funkcjonowania i usytuowania, zgodnie z art. 37 ust. 2 regulaminu wewnętrznego EROD. Komitet przyjmuje własny regulamin wewnętrzny i metody pracy.

W ramach prac w Komitecie przedstawiciele UODO brali także udział w pracach nad raportem dotyczącym stopnia i sposobu implementacji przez państwa członkowskie, zasad przetwarzania danych osobowych w systemie wymiany informacji na rynku wewnętrznym (IMI).

7. Punkt kontaktowy EROD ds. pandemii COVID-19

W 2021 roku Urząd Ochrony Danych Osobowych uczestniczył w pracach punktu kontaktowego ds. COVID-19 (ang. *Corona Contact Point*), utworzonego w dniu 3 kwietnia 2020 r. podczas pierwszego zdalnego posiedzenia plenarnego EROD.

Zadaniem punktu kontaktowego jest 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 wywołaną przez pandemię koronawirusa.

8. Grupa ekspertów wspierających EROD

15 grudnia 2020 r. Europejska Rada Ochrony Danych przyjęła Dokument określający zakres zadań grupy ekspertów wspierających EROD (ang. **Support Pool of Experts – SPE**).

Celem SPE jest przyczynianie się do wysokiego i spójnego stopnia ochrony danych osobowych we wszystkich państwach członkowskich EOG poprzez zapewnianie członkom EROD wsparcia materialnego w postaci wiedzy specjalistycznej, przydatnej w postępowaniach i działaniach związanych z egzekwowaniem prawa, będących przedmiotem istotnego wspólnego zainteresowania, a tym samym promowanie lepszej ochrony osób, których dane dotyczą. Ważnym zadaniem jest również wzmacnianie współpracy i solidarności między wszystkimi członkami EROD poprzez dzielenie się i uzupełnianie mocnych stron oraz zaspokajanie potrzeb operacyjnych. Koordynacją tych działań na poziomie krajowym zajmują się punkty kontaktowe powołane w organach nadzorczych.

9. Program prac EROD na lata 2021–2022

W 2021 roku EROD funkcjonowała w oparciu o przyjęty w 2021 roku *Program prac na lata 2021/2022*[528]. Program ten opiera się na czterech filarach:

- Filar I: Wspieranie harmonizacji i ułatwianie zgodności.
- Filar II: Wspieranie skutecznego egzekwowania i efektywnej współpracy między krajowymi organami nadzorczymi.
- Filar III: Podejście do nowych technologii oparte na prawach podstawowych.
- Filar IV: Wymiar globalny.

W 2021 roku Rada zorganizowała 15 posiedzeń plenarnych, z czego jedno (w listopadzie) odbyło się w siedzibie Rady w Brukseli. W związku z ogłoszeniem przez Światową Organizacją Zdrowia w marcu 2020 r. pandemii COVID-19, Rada obradowała głównie 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.

Porządki obrad i protokoły z sesji plenarnych są publikowane na stronie internetowej EROD[529]. Podczas tych posiedzeń EROD przyjęła wytyczne, opinie i inne dokumenty, takie jak oświadczenia

[528] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf
[529] https://edpb.europa.eu/our-work-tools/agenda_en; https://edpb.europa.eu/our-work-tools/our-documents/publication-type/minutes_pl.

lub noty informacyjne, aby doradzać Komisji Europejskiej, krajowym organom nadzorczym i innym zainteresowanym stronom w kwestiach związanych z RODO. W sumie odbyło się 10 spotkań podgrup eksperckich i 10 spotkań w ramach EROD, w tym posiedzeń plenarnych, spotkań podgrup eksperckich i spotkań zespołów redakcyjnych.

Zgodnie z ustalonym planem oraz w wyniku potrzeby działania *ad hoc*, w 2021 roku Rada przyjęła m.in. niżej wymienione dokumenty[530].

Wytyczne

1. Wytyczne 01/2020 w sprawie pojazdów połączonych w wersji po konsultacjach publicznych;
2. Wytyczne 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO, uwzględniające wnioski z konsultacji publicznych;
3. Wytyczne 08/2020 w sprawie targetowania użytkowników mediów społecznościowych, w wersji po konsultacjach publicznych;
4. Wytyczne 9/2020 w sprawie pojęcia mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, w wersji po konsultacjach publicznych;
5. Wytyczne 10/2020 w sprawie ograniczeń praw osób, których dane dotyczą, na podstawie art. 23 RODO, w wersji po konsultacjach publicznych;
6. Wytyczne 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych, w wersji do i po konsultacjach publicznych;
7. Wytyczne 02/2021w sprawie wirtualnych asystentów głosowych, w wersji do i po publicznych konsultacjach;
8. Wytyczne 03/2021 w sprawie stosowania art. 65 ust. 1 lit. a) RODO;
9. Wytyczne 04/2021 dotyczące kodeksów postępowania jako narzędzia przekazywania danych;
10. Wytyczne 05/2021 w sprawie wzajemnych relacji pomiędzy art. 3 i rozdziałem V RODO.

Wspólne Opinie EROD – EIOD

1. Wspólna Opinia 1/2021 w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi;
2. Wspólna Opinia 2/2021 opinię w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich;

[530] Wszystkie dokumenty EROD o charakterze publicznym znajdują się na jej stronie: https://edpb.europa.eu/our-work-tools_pl.

3. Wspólna Opinia 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi);
4. Wspólna Opinia 04/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia, w celu ułatwienia swobodnego przepływu w czasie pandemii COVID-19 (zielone zaświadczenie cyfrowe);
5. Wspólna Opinia 5/2021 w sprawie wniosku dotyczącego rozporządzenia parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji („akt w sprawie sztucznej inteligencji").

Zalecenia

1. Zalecenia 01/2020 w sprawie środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, w wersji po konsultacjach publicznych;
2. Zalecenia 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy 2016/680 (tzw. dyrektywy policyjnej);
3. Zalecenia 02/2021 w sprawie podstawy prawnej przechowywania danych kart kredytowych wyłącznie w celu ułatwienia dokonywania dalszych transakcji online.

Opinie

1. Opinia 01/2021 w sprawie projektu decyzji duńskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych administratora grupy Saxo Bank;
2. Opinia 02/2021 w sprawie projektu decyzji szwedzkiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dotyczących administratorów grupy Elanders;
3. Opinia 03/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych BDO dotyczących administratora BDO;
4. Opinia 04/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dla podmiotów przetwarzających BDO;
5. Opinia 05/2021 EROD w sprawie uzgodnień administracyjnych między amerykańską Radą Nadzorczą Księgowości Spółki Publicznej (PCAOB) a francuskim Komitetem Audytu (H3C);

6. Opinia 06/2021 w sprawie projektu decyzji hiszpańskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dla podmiotów przetwarzających Grupy Kumon;
7. Opinia 07/2021 w sprawie projektu decyzji hiszpańskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dotyczących administratorów Grupy Kumon;
8. Opinia 08/2021 w sprawie projektu decyzji Urzędu Nadzoru Badenii-Wirtembergii w sprawie Wiążących Reguł Korporacyjnych dla podmiotów przetwarzających Grupy Luxoft;
9. Opinia 09/2021 w sprawie projektu decyzji Organu Nadzoru Badenii-Wirtembergii w sprawie Wiążących Reguł Korporacyjnych Administratora Grupy Luxoft;
10. Opinia 10/2021 w sprawie projektu decyzji właściwego organu nadzorczego Węgier w sprawie zatwierdzenia wymogów akredytacji organu monitorującego kodeks postępowania zgodnie z art. 41 RODO;
11. Opinia 11/2021 w sprawie projektu decyzji właściwego organu nadzorczego Norwegii w sprawie zatwierdzenia wymogów akredytacji organu monitorującego kodeks postępowania zgodnie z art. 41 RODO;
12. Opinia 12/2021 w sprawie projektu decyzji właściwego organu nadzorczego Portugalii w sprawie zatwierdzenia wymagań dotyczących akredytacji jednostki certyfikującej zgodnie z art. 43(3) RODO;
13. Opinia 13/2021 w sprawie projektu decyzji właściwego organu nadzorczego Rumunii w sprawie zatwierdzenia wymagań dotyczących akredytacji jednostki certyfikującej zgodnie z art. 43(3) RODO;
14. Opinia 14/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo;
15. Opinia 15/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na podstawie dyrektywy (UE) 2016/680 stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo;
16. Opinia 16/2021 dotycząca projektu decyzji belgijskiego organu nadzorczego w sprawie „Kodeksu postępowania w zakresie ochrony danych UE dla dostawców usług w chmurze" przedłożona przez Scope Europe;
17. Opinia 17/2021 w sprawie projektu decyzji francuskiego organu nadzorczego w sprawie europejskiego kodeksu postępowania złożonego przez dostawców usług infrastruktury chmury (CISPE);

18. Opinia 18/2021 w sprawie projektu standardowych klauzul umownych przedstawionego przez litewski organ nadzorczy (art. 28 ust. 8 RODO);
19. Opinia 19/2021 w sprawie projektu decyzji właściwego organu nadzorczego Węgier w sprawie zatwierdzenia wymogów akredytacji jednostki certyfikującej zgodnie z art. 43(3) RODO;
20. Opinia EROD 20/2021 w sprawie systemu identyfikalności wyrobów tytoniowych;
21. Opinia 21/2021 w sprawie projektu decyzji francuskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych administratora grupy CGI;
22. Opinia 22/2021 w sprawie projektu decyzji francuskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dla podmiotów przetwarzających w grupie CGI;
23. Opinia 23/2021 w sprawie projektu decyzji właściwego organu nadzorczego Republiki Czeskiej w sprawie zatwierdzenia wymogów akredytacji organu monitorującego kodeks postępowania zgodnie z art. 41 RODO;
24. Opinia 24/2021 w sprawie projektu decyzji właściwego organu nadzorczego Słowacji w sprawie zatwierdzenia wymogów akredytacji organu monitorującego kodeks postępowania zgodnie z art. 41 RODO;
25. Opinia 25/2021 w sprawie projektu decyzji właściwego organu nadzorczego Litwy w sprawie zatwierdzenia wymagań dotyczących akredytacji jednostki certyfikującej zgodnie z art. 43(3) RODO;
26. Opinia 26/2021 w sprawie projektu decyzji organu nadzorczego Nadrenii Północnej-Westfalii (Niemcy) w sprawie wiążących reguł korporacyjnych dotyczących administratorów grupy Internet Initiative Japan Group;
27. Opinia 27/2021 w sprawie projektu decyzji organu nadzorczego Nadrenii Północnej-Westfalii (Niemcy) w sprawie wiążących reguł korporacyjnych dla podmiotów przetwarzających Grupy Internet Initiative Japan Group;
28. Opinia 28/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych administratora Spółki Oregon Tool, Inc (dawniej „Blount");
29. Opinia 29/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dla podmiotów przetwarzających w Oregon Tool, Inc (dawniej „Blount");
30. Opinia 30/2021 w sprawie projektu decyzji hiszpańskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dotyczących administratorów Grupy COLT;

31. Opinia 31/2021 w sprawie projektu decyzji hiszpańskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych dla podmiotów przetwarzających w Grupie COLT;
32. Opinia 32/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 stwierdzająca odpowiedni stopień ochrony danych osobowych przez Republikę Korei;
33. Opinia 33/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych przewoźnika administratora Carrier;
34. Opinia 34/2021 w sprawie projektu decyzji belgijskiego organu nadzorczego w sprawie wiążących reguł korporacyjnych firmy Otis;
35. Opinia 35/2021 w sprawie projektu decyzji właściwego organu nadzorczego Belgii w sprawie zatwierdzenia wymagań dotyczących akredytacji jednostki certyfikującej zgodnie z art. 43.3 (RODO);
36. Opinia 36/2021 w sprawie projektu decyzji właściwego organu nadzorczego Norwegii w sprawie zatwierdzenia wymagań dotyczących akredytacji jednostki certyfikującej zgodnie z art. 43.3 (RODO);
37. Opinia 37/2021 w sprawie projektu decyzji właściwego organu nadzorczego Malty w sprawie zatwierdzenia wymogów akredytacji organu monitorującego kodeks postępowania zgodnie z art. 41 RODO;
38. Opinia 38/2021 w sprawie projektu decyzji właściwego organu nadzorczego Łotwy w sprawie zatwierdzenia wymagań dotyczących akredytacji jednostki certyfikującej zgodnie z art. 43.3 (RODO);
39. Opinia 39/2021 w sprawie organów nadzorczych korzystających z art. 58 ust. 2 lit. g) RODO, jako podstawy prawnej do nakazania z urzędu usunięcia nielegalnie przetwarzanych danych osobowych.

Oświadczenia

1. Oświadczenie w sprawie wystąpienia Zjednoczonego Królestwa z Unii Europejskiej, przyjęte 15 grudnia 2020 r., zaktualizowane 13 stycznia 2021 r.;
2. Oświadczenie 02/2021 EROD w sprawie nowych postanowień Konwencji w sprawie cyberprzestępczości;
3. Oświadczenie 03/2021 EROD w sprawie rozporządzenia w sprawie prywatności i łączności elektronicznej;

4. Oświadczenie 04/2021 EROD w sprawie umów międzynarodowych obejmujących przekazywanie danych;
5. Oświadczenie 05/2021 dotyczące aktu w sprawie zarządzania danymi w świetle zmian legislacyjnych;
6. Oświadczenie z dnia 18.11.2021 r. w sprawie pakietu usług cyfrowych i strategii w zakresie danych Komisji Europejskiej;
7. Oświadczenie z dnia 14.12.2021 r. dotyczące współpracy przy opracowaniu wytycznych.

Wkłady

1. Wkład EROD z dnia 4.05.2021 r. w szóstą rundę konsultacji w sprawie projektu Drugiego protokołu dodatkowego do Budapeszteńskiej Konwencji Rady Europy o Cyberprzestępczości;
2. Wkład EROD z dnia 14.12.2021 r. w dokonaną przez Komisję Europejską ocenę dyrektywy 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.

Wiążące decyzje

1. Wiążąca Decyzja EROD 1/2021 w trybie pilnym w sprawie wniosku hamburskiego organu nadzorczego złożonego na podstawie art. 66 ust. 2 RODO o przyjęcie środków o charakterze ostatecznym w odniesieniu do Facebook Ireland Limited;
2. Wiążąca Decyzja 01/2021 rozstrzygającą spór na podstawie art. 65 ust. 1 lit. a) RODO powstałego w wyniku projektu decyzji irlandzkiego organu nadzorczego w sprawie WhatsApp Ireland Limited.

10. Współpraca w ramach IMI

Od 25 maja 2018 roku organy nadzorcze korzystają z systemu wymiany informacji na rynku wewnętrznym – tzw. IMI[531], w celu wymiany, w sposób bezpieczny i ustandaryzowany, informacji

[531] W języku angielskim: Internal Market Information System – IMI.

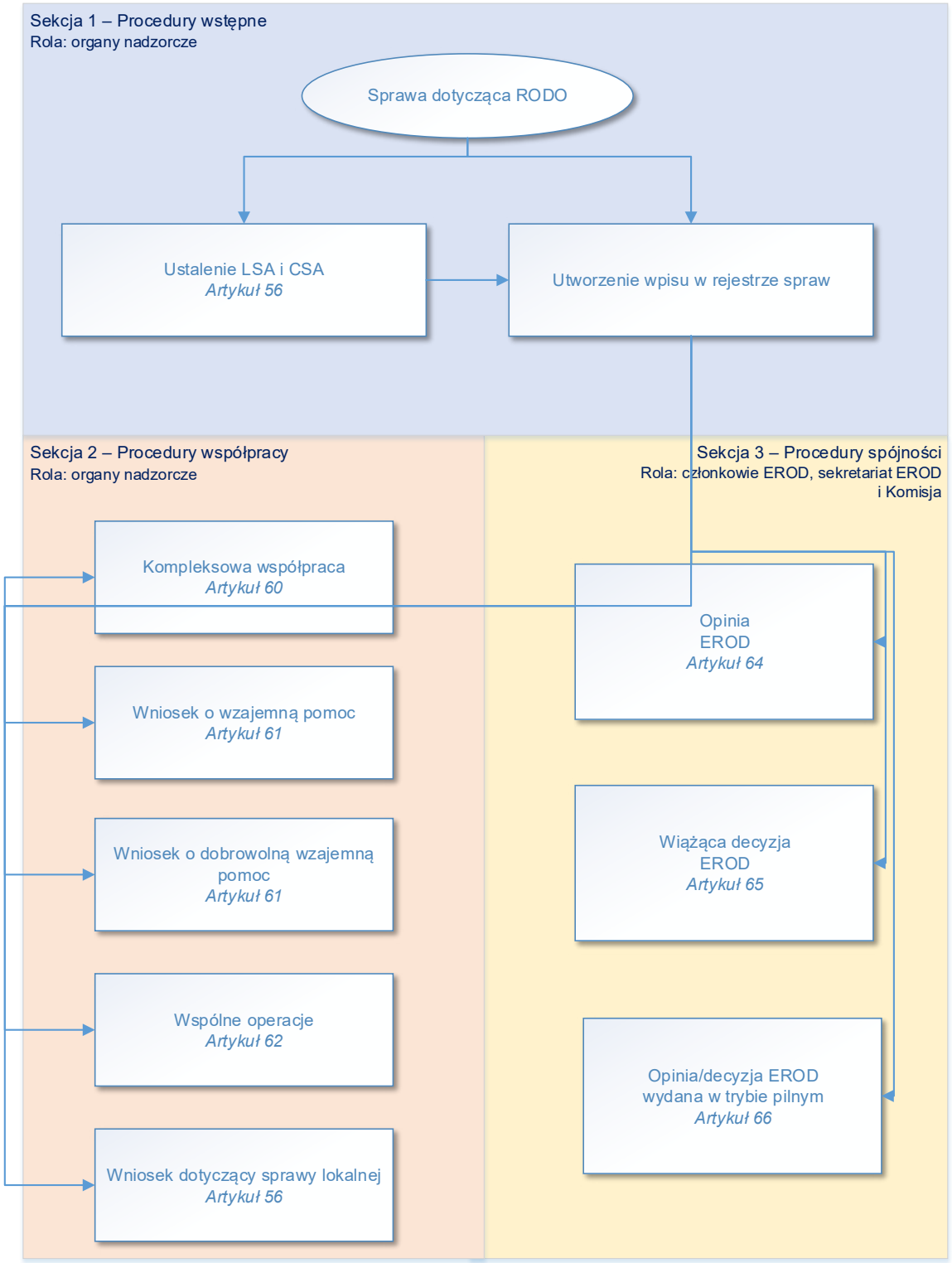
niezbędnych dla realizacji mechanizmów współpracy i spójności, przewidzianych w rozdziale VII RODO, i w tym zakresie prowadzenia postępowań transgranicznych[532].

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 dedykowana temu zadaniu podgrupa ekspercka IT Users, która omawia i zatwierdza wszelkie niezbędne zmiany.

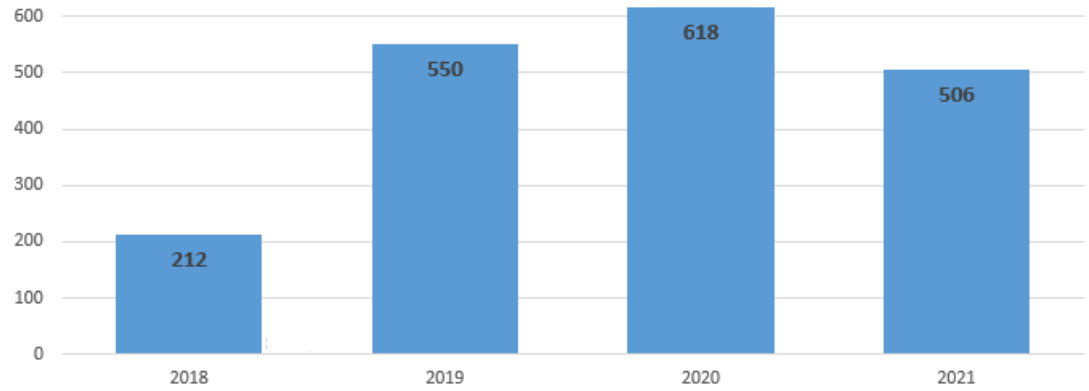
W ramach systemu IMI organy współpracują, korzystając z procedur współpracy i spójności, na podstawie przepisów RODO: Artykuł 56 – ustalenie wiodącego organu nadzorczego i organów, których sprawa dotyczy; wniosek dotyczący sprawy lokalnej), Artykuł 60 – kompleksowa współpraca; Artykuł 61 – wniosek o wzajemną pomoc i dobrowolną wzajemną pomoc; Artykuł 62 – wspólne operacje organów nadzorczych; Artykuł 64 – opinia EROD; Artykuł 65 – wiążąca decyzja EROD; Artykuł 66 –opinia/decyzja EROD wydana w trybie pilnym.

W sposób obrazowy przedstawia to poniższa ilustracja, zaczerpnięta z wewnętrznego podręcznika IMI dla organów nadzorczych, opracowanego przez EROD.

[532] Szczegółowe informacje na temat prowadzonych przez Prezesa UODO postępowań transgranicznych znajdują się w części 4.1.5. niniejszego Sprawozdania „Postępowania transgraniczne".


Sekcja 1 – Procedury wstępne
Rola: organy nadzorcze
Sprawa dotycząca RODO
Ustalenie LSA i CSA
Artykuł 56
Utworzenie wpisu w rejestrze spraw
Sekcja 2 – Procedury współpracy
Rola: organy nadzorcze
Sekcja 3 – Procedury spójności
Rola: członkowie EROD, sekretariat EROD i Komisja
Kompleksowa współpraca
Artykuł 60
Wniosek o wzajemną pomoc
Artykuł 61
Wniosek o dobrowolną wzajemną pomoc
Artykuł 61
Wspólne operacje
Artykuł 62
Wniosek dotyczący sprawy lokalnej
Artykuł 56
Opinia EROD
Artykuł 64
Wiążąca decyzja EROD
Artykuł 65
Opinia/decyzja EROD wydana w trybie pilnym
Artykuł 66

Zgodnie ze statystykami przygotowanymi przez EROD[533], od momentu wejścia w życie RODO do 31 grudnia 2021 roku, w rejestrze spraw IMI[534] utworzono **1886** spraw o charakterze transgranicznym[535].



Wykres 16: **Liczba spraw o charakterze transgranicznym utworzonych w rejestrze IMI w okresie 25.05.2018–31.12.2021.**

1379 spraw zostało zainicjowanych w następstwie wniesionych skarg.

507 pochodziło z innych źródeł, takich jak postępowania, inicjatywy organów nadzorczych, zobowiązania prawne, itd.

Z powyższych spraw uruchomiono następujące procedury:

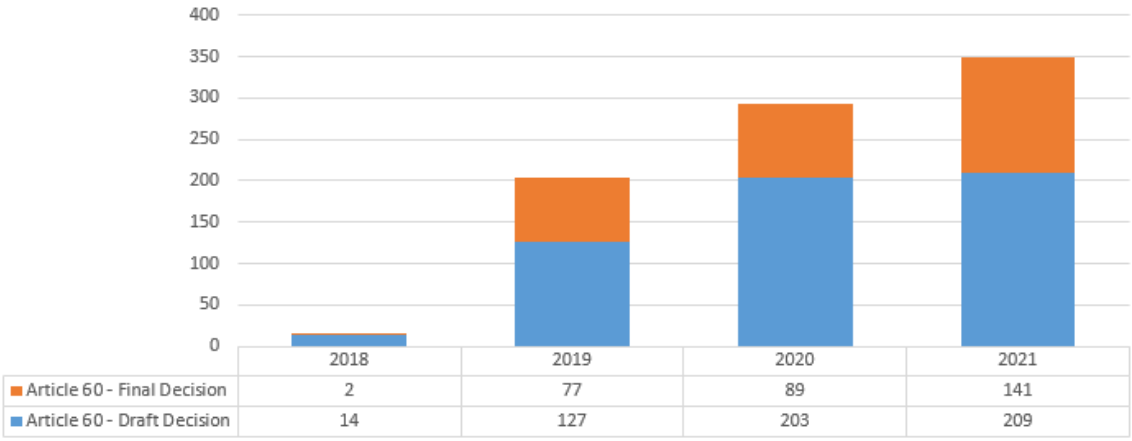
- **602** procedury wzajemnej pomocy (art. 61); oprócz tego organy uruchomiły **7112** procedur w celu świadczenia sobie dobrowolnej wzajemnej pomocy.

[533] Stan spraw zgodny ze statystykami na dzień 31 grudnia 2021 r. przygotowanymi dla organów nadzorczych przez Helpdesk IMI EROD.

[534] 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.

[535] Należy pamiętać, że statystyki te obejmują jedynie sprawy rozpatrywane w ramach mechanizmu One-Stop-Shop z art. 60 RODO. W związku z tym należy wziąć pod uwagę, że: (1) odniesienia do wpisów do rejestru spraw w tych statystykach nie mają korelacji 1 do 1 z liczbą spraw transgranicznych rozpatrywanych w danym kraju, ponieważ wiele spraw może być połączonych w jednym wpisie do rejestru spraw, który w związku z tym może odnosić się do wielu spraw transgranicznych; (2) w zależności od ustawodawstwa państwa członkowskiego, organy nadzorcze mogły rozpatrywać sprawy poza procedurą przewidzianą w art. 60 zgodnie z prawem krajowym.

- **862** procedury związane z mechanizmem kompleksowej współpracy – One-stop-shop (art. 60), z których **309** zakończyło przyjęcie ostatecznej decyzji;



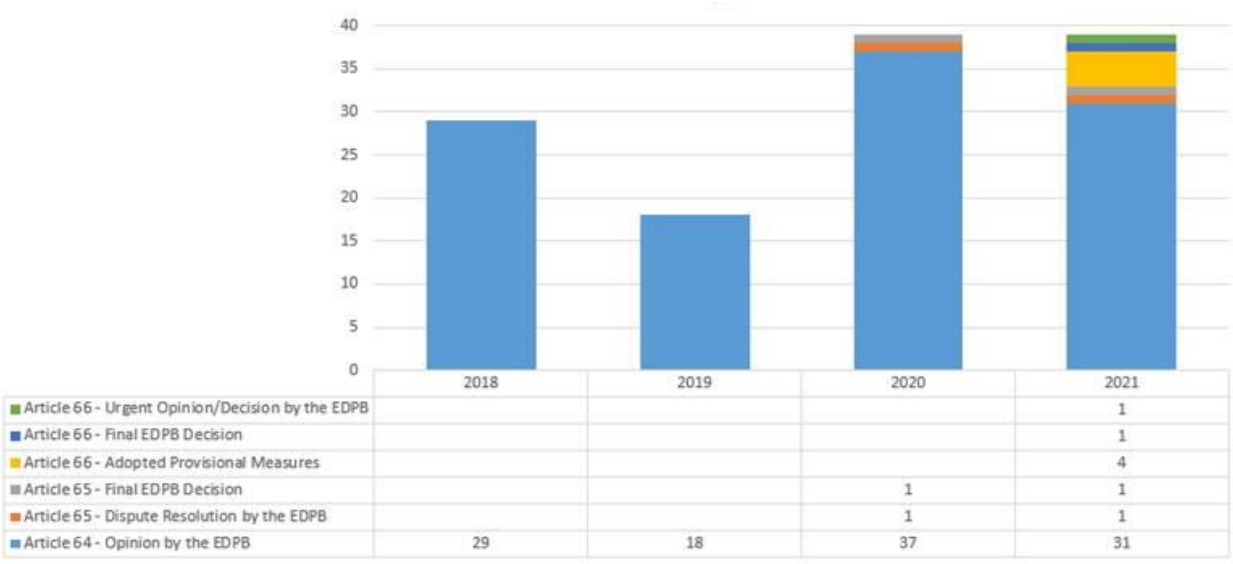
	2018	2019	2020	2021
Article 60 - Final Decision	2	77	89	141
Article 60 - Draft Decision	14	127	203	209

Wykres 17: **Liczba procedur w ramach mechanizmu kompleksowej współpracy utworzonych w rejestrze IMI w okresie 25.05.2018–31.12.2021**[536].

- **98** spraw o charakterze lokalnym (art. 56 ust. 2);
- **1** wspólną operację organów nadzorczych (art. 62);
- procedury spójności, w tym:

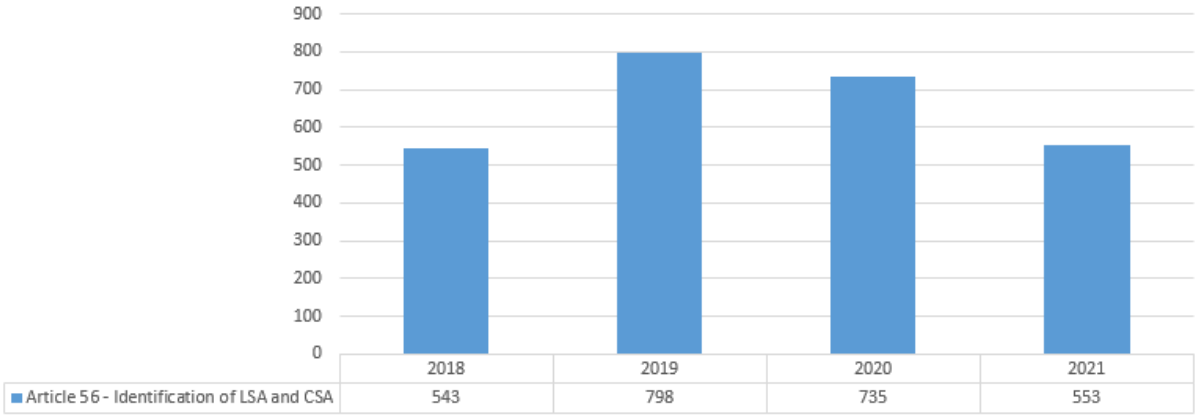
- **115** procedur z art. 64 zakończonych wydaniem **100** ostatecznych opinii z art. 64
- **2** procedury z art. 65 zakończone wydaniem **2** decyzji ostatecznych z art. 65.
- **4** środki tymczasowe z art. 66
- **1** ostateczna decyzja EROD z art. 66
- **1** ostateczna decyzja EROD w trybie pilnym z art. 66

[536] Źródłem grafik do wykresów nr 15, 16 i 17 były wewnętrzne statystyki EROD przygotowywane dla organów nadzorczych przez Helpdesk IMI.



Wykres 18: **Liczba procedur w ramach mechanizmu spójności utworzonych w rejestrze IMI w okresie 25.05.2018–31.12.2021**.

Dodatkowo uruchomiono **2629** procedur wszczętych w celu zidentyfikowania organów wiodących i organów, których sprawa dotyczy, na podstawie art. 56 ust. 1 (**93** procedury w toku, **2536** zakończonych).



Wykres 19: **Liczba procedur wszczętych w celu zidentyfikowania organów wiodących i organów, których sprawa dotyczy (art. 56 ust. 1) utworzonych w rejestrze IMI w okresie 25.05.2018–31.12.2021**.

Zgodnie ze statystykami IMI na dzień 31 grudnia 2021 r. Urząd Ochrony Danych Osobowych:

- był organem wiodącym w **28** sprawach w rejestrze spraw IMI;

- zainicjował łącznie **470** powiadomień, w tym **108** z art. 56 (identyfikacja organu wiodącego i organu, którego sprawa dotyczy), **36** z art. 60 (5 – projekt decyzji, 6 – ostateczna decyzja; 25 – nieformalne konsultacje), **324** z art. 61 (dobrowolna wzajemna pomoc) i **2** z art. 64 (opinia EROD);
- przesłał łącznie **237** wniosków, w tym: **4** z art. 56 (sprawa lokalna), **95** z art. 61 (wzajemna pomoc), **138** z art. 61 (dobrowolna wzajemna pomoc);
- otrzymał łącznie **78** wniosków, w tym: **1** z art. 56 (sprawa lokalna), **21** z art. 61 (wzajemna pomoc), **54** z art. 61 (dobrowolna wzajemna pomoc), **2** z art. 64 (ostateczna opinia EROD).

11. Wnioski prejudycjalne

W ramach współpracy międzynarodowej z organami nadzorczymi innych państw członkowskich UE oraz wykonywania obowiązków wynikających z członkostwa Polski w Unii Europejskiej, Prezes UODO dokonuje analizy wniosków w sprawach prejudycjalnych wniesionych do Trybunału Sprawiedliwości Unii Europejskiej (TSUE), przekazanych przez Kancelarię Prezesa Rady Ministrów (KPRM). Wnioski te dotyczą zagadnień z zakresu ochrony danych osobowych. Organ nadzorczy przygotowuje obszerne stanowiska, których przedmiotem jest rekomendacja w zakresie zasadności udziału Polski w poszczególnych postępowaniach przed TSUE. Stanowiska te przekazywane są do KPRM i służą do przygotowania stanowiska Polski w sprawach postępowań prowadzonych przez TSUE. Prezes UODO przedstawia swoje rekomendacje także na późniejszych etapach postępowań prowadzonych przed TSUE. Po wydaniu wyroku TSUE organ nadzorczy przedstawia swoje stanowisko w sprawie zasadności zmiany polskiego prawa w świetle treści danego orzeczenia.

Organ nadzorczy dokonuje – niezależnie od powyższego – regularnego przeglądu wszystkich postępowań inicjowanych przez TSUE, na podstawie wykazów otrzymanych od KPRM. Bada, czy wszystkie sprawy, których przedmiotem jest ochrona danych osobowych, trafiły do organu nadzorczego i czy zajął on stanowisko co do zasadności udziału Polski w postępowaniu.

W 2021 roku do Prezesa UODO wpłynęło **27 nowych wniosków prejudycjalnych skierowanych do TSUE przez sądy z różnych państw Unii Europejskiej.** Stanowi to znaczny wzrost liczby spraw w porównaniu do lat ubiegłych. Dla porównania, w 2020 r. wpłynęło 13

wniosków o wydanie orzeczeń w trybie prejudycjalnym[537], co do których Prezes UODO był proszony o wyrażanie swojego stanowiska w zakresie ochrony danych osobowych.

Organ nadzorczy dokonał wnikliwej analizy przekazanych przez KPRM wniosków prejudycjalnych, a następnie przedstawił swoje stanowisko co do zasadności udziału Polski w tych postępowaniach z punktu widzenia przepisów o ochronie danych osobowych[538]. W poszczególnych postępowaniach przedstawiał on również dalsze rekomendacje, w tym co do zasadności wnioskowania przez Polskę o przeprowadzenie rozprawy przed TSUE.

W 2021 roku Prezes UODO przedstawiał również swoje stanowiska w ramach postępowań TSUE – na różnych ich etapach – w których wnioski prejudycjalne wpłynęły do organu nadzorczego w poprzednich latach. Przykładowo, Prezes UODO dokonał analizy wpływu wyroku wydanego przez TSUE w sprawie *C-102/20 StWL Städtische Werke Lauf a.d. Pegnitz*, dotyczącej kwestii ochrony danych osobowych w sektorze łączności elektronicznej[539].

W analizowanym 2021 roku Prezes UODO dokonał kompleksowej oceny skutków wyroków TSUE dla polskiego porządku prawnego również w 5 innych zakończonych postępowaniach, tj. w sprawach: *C-746/18 Prokuratuur (d. H. K.)*, *C-505/19 Bundesrepublik Deutschland*, *C-439-19 Latvijas Republikas Saeima*, *C-597/19 M.I.C.M. Mircom International Content Management & Consulting* oraz *C-645/19 Facebook Ireland e.a.* Organ nadzorczy przekazał swoje stanowiska, co do wpływu wyroków w tych sprawach na polski porządek prawny[540].

W 2021 roku Prezes UODO wydawał także rekomendacje w innych postępowaniach – wszczętych przed 2021 rokiem – prowadzonych przez TSUE. Dotyczy to spraw: *C-175/20 Valsts ieņēmumu dienests*, *C-793/19 i C-794/19 i C-140/20 Space Net i in.*, *C-245/20 Autoriteit Persoonsgegevens*, *C-534/20 Leistritz*, *C-817/19 Ligue des droits humains* oraz *C-460/20 Google*. W sprawach tych organ nadzorczy wypowiedział się na różnym etapie postępowania, w tym m.in. w zakresie zasadności udziału Pełnomocnika Polski w rozprawie przed TSUE, czy też potrzeby

[537] 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.

[538] DOL.0623.1.2021, DOL.0623.3.2021, DOL.0623.4.2021, DOL.0623.5.2021, DOL.0623.6.2021, DOL.0623.7.2021, DOL.0623.8.2021, DOL.0623.9.2021, DOL.0623.10.2021, DOL.0623.11.2021, DOL.0623.12.2021, DOL.0623.13.2021, DOL.0623.14.2021, DOL.0623.15.2021, DOL.0623.16.2021, DOL.0623.17.2021, DOL.0623.18.2021, DOL.0623.19.2021, DOL.0623.20.2021, DOL.0623.21.2021, DOL.0623.22.2021, DOL.0623.23.2021, DOL.0623.24.2021, DOL.0623.26.2021, DOL.0623.27.2021, DOL.0623.28.2021, DOL.0623.29.2021.

[539] DOL.0623.9.2020.

[540] ZWME.070.4.2019, DOL.0623.6.2020, ZWME.070.10.2019, DOL.0623.12.2020, DOL.0623.13.2020.

złożenia przez Polskę wniosku o przeprowadzenie rozprawy, jak również przedstawił swoje uwagi do stanowiska Polski, które zostało następnie przedłożone do TSUE[541].

12. Pytania od innych organów nadzorczych

Prezes UODO jest zobowiązany na podstawie przepisów RODO do udzielania odpowiedzi na pytania zadane mu przez inne organy nadzorcze z państw Unii Europejskiej. Obowiązki te realizowane są w oparciu o mechanizmy spójności i współpracy uregulowane w art. 63 i nast. RODO. Zapytania od innych organów nadzoru kierowane są do polskiego regulatora za pośrednictwem Systemu IMI (Internal Market Information System), tj. Systemu Wymiany Informacji na Rynku Wewnętrznym. Tą samą drogą przekazywane są odpowiedzi na przedłożone zapytania.

W 2021 roku do Prezesa UODO wpłynęło **25 zapytań** organów nadzorczych z innych państw. Dla porównania, w 2020 roku takich pytań wpłynęło 14.

W analizowanym roku sprawozdawczym najwięcej pytań wpłynęło od organów nadzorczych Łotwy, Słowenii, Francji, Malty, Węgier, Litwy, Holandii, Bułgarii, Irlandii, Finlandii i Słowacji[542]. Organy nadzorcze zwracały się do Prezesa UODO z różnymi zagadnieniami. Przykładowo, jedno z pytań dotyczyło możliwości przetwarzania danych biometrycznych (danych osobowych szczególnej kategorii) w scentralizowanej bazie danych, przy wykorzystaniu narzędzi, które uniemożliwiają kontrolę przetwarzania danych osobowych przez podmiot danych (przykładowo, w przypadku wykorzystywania tzw. biometrii głosowej do podłączenia do interaktywnego serwera głosowego)[543]. W innej sprawie organ właściwy do spraw ochrony danych osobowych zwrócił się z pytaniem dotyczącym legalności wykorzystywania aplikacji mobilnych, ułatwiających przeprowadzenie badań w zakresie narażenia dzieci i młodzieży na wpływ marketingu niezdrowych żywności i napojów[544].

Pozostałe zapytania organów nadzorczych dotyczyły m.in. kwestii: prowadzenia przez osobę fizyczną monitoringu wizyjnego za pośrednictwem wizjera w drzwiach do mieszkania; dostępu do

[541] DOL.0623.19.2020, DOL.070.2.2019, DOL.0623.24.2020, DOL.0623.32.2020, DOL.0623.33.2020, DOL.0623.2.2020.
[542] DOL.614.2.2021, DOL.614.3.2021, DOL.614.4.2021, DOL.614.5.2021, DOL.614.6.2021, DOL.614.7.2021, DOL.614.8.2021, DOL.614.12.2021, DOL.614.13.2021, DOL.614.14.2021, DOL.614.15.2021, DOL.614.16.2021, DOL.614.17.2021, DOL.614.19.2021, DOL.614.20.2021, DOL.614.21.2021, DOL.614.22.2021, DOL.614.23.2021, DOL.614.24.2021, DOL.614.25.2021, DOL.614.26.2021, DOL.614.27.2021, DOL.614.28.2021, DOL.614.29.2021, DOL.614.30.2021.
[543] DOL.614.4.2021.
[544] DOL.614.17.2021.

danych osobowych przetwarzanych przez profesjonalnych prawników; możliwości zastosowania art. 17 RODO do danych osobowych udostępnionych w wiadomościach opublikowanych na forum internetowym; legalności zastosowania tzw. inteligentnych kamer, tj. urządzeń rejestrujących obraz wykorzystujących sztuczną inteligencję (*artificial intelligence* – AI); legalności wykorzystywania narzędzi do zapewnienia stałej komunikacji między pojazdami; możliwości lokalizowania urządzeń mobilnych przez organy ścigania czy też możliwości realizacji prawa jednostki dostępu do danych w świetle potrzeby ochrony przed potencjalnie szkodliwymi informacjami na temat ich własnego zdrowia.

We wszystkich powyższych sprawach polski regulator przygotował odpowiedzi i przekazał je do adresatów za pośrednictwem systemu IMI.

13. Przekazywanie danych osobowych poza EOG

W 2021 roku do Prezesa UODO wpłynęły zapytania od organów nadzorczych z Europejskiego Obszaru Gospodarczego (EOG) oraz z Sekretariatu EROD dotyczące wiążących reguł korporacyjnych (WRK) w ponad 50 różnych grupach kapitałowych. Współpraca organów nadzorczych z EOG w toku procedury zatwierdzania WRK odbywa się z uwzględnieniem mechanizmu spójności przewidzianego w art. 63 RODO, po zasięgnięciu opinii EROD.

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 tzw. *brexitem*, możliwości podjęcia się przez polski organ nadzorczy działania w charakterze współrecenzenta w procedurze zatwierdzania WRK, ewentualnych komentarzy (w tym w charakterze współrecenzenta) do projektu konkretnych WRK (ich skonsolidowanego projektu, będącego rezultatem współpracy organu wiodącego i współrecenzentów) czy też projektów opinii EROD dot. projektów decyzji odnoszących się do konkretnych WRK. W przypadku projektów niektórych WRK komentarze do nich były również dyskutowane podczas specjalnych sesji dotyczących WRK w ramach podgrupy eksperckiej EROD do spraw przekazywania danych osobowych do państw trzecich (International Transfers Expert Subgroup), w których uczestniczyły także inne organy z EOG.

W 2021 roku, w ramach prac nad decyzją Komisji Europejskiej mającą stwierdzać odpowiedni poziom ochrony danych osobowych w Zjednoczonym Królestwie, Prezes UODO przygotował i przedstawił KPRM analizę projektu decyzji KE, już po przyjęciu przez EROD opinii dotyczącej wcześniejszego projektu decyzji o adekwatności w stosunku do Zjednoczonego Królestwa.

Po analizie najnowszej wersji projektu decyzji, organ właściwy do spraw ochrony danych uznał, że uwagi i rekomendacje zawarte w opinii EROD 14/2021 nie zostały w sposób wystarczający uwzględnione w treści najnowszej wersji projektu decyzji[545]**.** Do organu nadzorczego wpłynęła również informacja o ostatecznych wersjach decyzji KE o adekwatności w stosunku do Wielkiej Brytanii[546].

W 2021 roku Prezes UODO otrzymał zapytanie od Ministerstwa Rozwoju, Pracy i Technologii dotyczące kwestii nowego ujęcia postanowień dotyczących przepływu danych i ochrony danych osobowych w Umowie EU-UK CTA. Organ nadzorczy przygotował i przesłał stanowisko w tej sprawie[547].

W roku sprawozdawczym 2021 przedstawiciele organu nadzorczego uczestniczyli ponadto w spotkaniach podgrupy eksperckiej EROD do spraw przekazywania danych osobowych do państw trzecich (International Transfers Expert Subgroup). Brali udział w przygotowywaniu licznych informacji, które później były przedmiotem dyskusji podczas posiedzeń plenarnych EROD, jak również informacji potrzebnych do oceny projektów opinii EROD, które były poddawane głosowaniom odbywającym się w procedurze pisemnej, w tym zwłaszcza dotyczących projektów decyzji organów nadzorczych odnoszących się do różnych WRK.

14. Inne sprawy

W 2021 roku organ właściwy w sprawie ochrony danych osobowych zajmował się również innymi sprawami – zarówno o zasięgu krajowym, jak i międzynarodowym – dotyczącymi innych kwestii niż te wskazane powyżej.

W 2021 roku Przewodnicząca EROD zwróciła się do organów nadzorczych państw członkowskich Unii Europejskiej, w tym do polskiego regulatora, o udzielenie odpowiedzi na pytania zawarte w kwestionariuszu Komisji Europejskiej dotyczącym oceny implementacji Dyrektywy LED[548]. W Polsce przepisy Dyrektywy LED zostały wdrożone na mocy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku

[545] DOL.401.224.2021.
[546] DOL.412.7.2021.
[547] DOL.401.630.2021.
[548] 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, wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylające decyzję ramową Rady 2008/977/WsiSW.

z zapobieganiem i zwalczaniem przestępczości[549]. Organ nadzorczy zaopiniował przedłożone stanowisko Pełnomocnika RP, które następnie miało być przedstawione podczas posiedzenia Grupy Ekspertów Komisji Europejskiej do spraw RODO i Dyrektywy LED, odbywającego się w związku z pracami Komisji Europejskiej nad ewaluacją Dyrektywy LED[550]. Prezes UODO zaopiniował również stanowisko oraz przygotował wkład do instrukcji dla Pełnomocnika RP na posiedzenie Grupy Roboczej do spraw ochrony danych osobowych Rady (UE), w związku z pracami w sprawie ewaluacji Dyrektywy LED[551].

W 2021 roku Prezes UODO zaopiniował również projekt stanowiska Polski dotyczący postępu prac Komisji Europejskiej nad projektem tzw. decyzji o adekwatności wobec Korei Południowej[552]. Organ nadzorczy otrzymał pismo od południowokoreańskiego stowarzyszenia *Open Net Association*. Pismo zawierało informacje, które w ocenie stowarzyszenia, były istotne dla wydania decyzji o adekwatności wobec Korei Południowej. Prezes UODO – za pośrednictwem tzw. systemu *Confluence* – przekazał swoje stanowisko, zgodnie z którym nie było potrzeby przygotowywania wspólnej odpowiedzi organów nadzorczych na poziomie EROD.

Ponadto do UODO wpłynęło też 12 zapytań zawartych w tzw. kwestionariuszach[553]. Przygotowano stosowne odpowiedzi m.in. do kwestionariuszy dotyczących: podejścia do przetwarzania danych osobowych dzieci; oceny Dyrektywy LED; pytań w sprawie nadzoru nad plikami cookie i podobnymi technologiami; szczególnych ograniczeń w zakresie przetwarzania szczególnych kategorii danych osobowych (biometria) w państwach członkowskich Unii Europejskiej czy też projektu wytycznych EROD w sprawie prawa dostępu do danych.

W 2021 roku Prezes UODO obserwował postępy negocjacji w zakresie umów i porozumień międzynarodowych, które mogły mieć związek z przetwarzaniem danych osobowych. Otrzymał informacje w zakresie:

- przebiegu negocjacji Porozumienia ws. handlu elektronicznego WTO[554],

[549] Dz.U. z 2019 r. poz.125 – ustawa weszła w życie po upływie 14 dni od dnia ogłoszenia (06.02.2019 r.) – z wyjątkiem art. 58 pkt 12, który wszedł w życie z dniem 1 listopada 2019 r.; art. 82 pkt 5 w zakresie art. 25c–25h, które weszły w życie po upływie roku od dnia ogłoszenia (23.01.2020 r.).
[550] DOL.401.560.2021.
[551] DOL.401.485.2021.
[552] DOL.401.498.2021.
[553] DOL.401.604.2021.
[554] DOL.412.5.2021.

- Wspólnej inicjatywie Światowej Organizacji Handlu w sprawie handlu elektronicznego (*Joint Initiative on E-commerce of the World Trade Organisation*)[555],
- przebiegu negocjacji umowy handlowej UE-Indonezja FTA[556].

Dokonał również analizy otrzymanych z KPRM finalnych wersji dwóch decyzji Komisji Europejskiej w sprawie przyjęcia standardowych klauzul umownych (wydanych na podstawie art. 28 i art. 46 RODO) przed ich ostatecznym przyjęciem[557].

W 2021 roku organ nadzorczy przygotował stosowne informacje w zakresie działań podejmowanych przez Prezesa UODO w związku z wyrokiem TSUE z 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Limited, Maximillian Schrems („Schrems II")[558] – o którym była już mowa w innej części niniejszego sprawozdania. Przygotowane materiały miały być wykorzystane podczas spotkania Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), którego przedmiotem miał być m.in. projekt Rezolucji Parlamentu Europejskiego dot. ww. wyroku TSUE. Spotkanie to nie odbyło się w związku ze sprzeciwem irlandzkiego organu nadzorczego na zaproponowaną przez Komisję LIBE formułę spotkania.

W 2021 roku Prezes UODO otrzymał od Ministerstwa Rozwoju, Pracy i Technologii projekt *Memorandum of Understanding,* dotyczącego lokalnych pracowników cywilnych i mającego na celu realizację postanowień umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki o wzmocnionej współpracy obronnej, podpisanej w Warszawie 15 sierpnia 2020 roku[559]. Organ nadzorczy udzielił stosownej odpowiedzi Ministerstwu Rozwoju, Pracy i Technologii, w której zwrócił uwagę na kwestię dotyczącą ochrony danych osobowych rezydentów przebywających na terytorium RP[560]. 6 lipca 2021 roku odbyło się spotkanie w sprawie ww. dokumentu. Wzięli w nim udział m.in. przedstawiciele UODO.

W 2021 roku do organu nadzorczego wpłynęła do zaopiniowania propozycja Unii Europejskiej w zakresie umowy o wolnym handlu UE – Nowa Zelandia. Prezes UODO udzielił w tym zakresie odpowiedzi Ministerstwu Rozwoju i Technologii[561].

---

[555] DOL.412.3.2021.
[556] DOL.055.3.2021.
[557] DOL.601.1.2021.
[558] DWME.602.3.2021.
[559] Dz. U. z 2020 r. poz. 2153.
[560] DOL.401.319.2021.
[561] DOL.412.8.2021.

15. Międzynarodowe Warsztaty

1) Warsztaty ONZ nt. wpływu pandemii COVID-19 na prawo do prywatności i ochrony danych osobowych, 21–23.06.2021 r.

Efektem współpracy i porozumienia Grupy Roboczej OECD ds. Zarządzania Danymi i Prywatności w Gospodarce Cyfrowej (WPDGP), Globalnego Zgromadzenia ds. Prywatności oraz mandatu Specjalnego Sprawozdawcy ONZ ds. Prawa do Prywatności była organizacja dwóch warsztatów z cyklu „back-to-back". Ich głównym celem była analiza wpływu pandemii COVID-19 na prawo do prywatności i zarządzanie danymi osobowymi. Temat tych spotkań stanowił kontynuację dwóch poprzednich warsztatów, które odbyły się w kwietniu 2020 r. i wrześniu 2020 r.

Podczas I sesji warsztatów (21.06.2021 r.) adresowanych do decydentów politycznych i organów regulacyjnych, przedstawione zostały perspektywy różnych ram zarządzania prywatnością i danymi osobowymi. Kolejna sesja (22.06.2021 r.) poświęcona była spostrzeżeniom na temat innowacyjnych planów poszczególnych krajów, dotyczących sposobów powrotu do zdrowia, ze szczególnym uwzględnieniem „Aspektów prywatności danych w miejscu pracy podczas pandemii" oraz „Programów szczepień i paszportów covidowych". Trzeci i ostatni dzień warsztatów – zorganizowany przez specjalnego sprawozdawcę ONZ ds. prawa do prywatności przy wsparciu Global Privacy Assembly (GPA) – skoncentrowany był na pogłębionej ocenie dostępnych dowodów dotyczących wpływu pandemii na prywatność i ochronę danych osobowych na całym świecie.

2) Europejskie Warsztaty Rozpatrywania Skarg, 16–17.11.2021 r.

W dniach 16–17 listopada 2021 r. odbyły się w formule online coroczne warsztaty rozpatrywania spraw, w których uczestniczyli przedstawiciele UODO. Organizatorem wydarzenia był organ nadzorczy Gibraltaru. Tegoroczne warsztaty koncentrowały się na wdrażaniu przepisów RODO dotyczących prowadzenia postępowań w codziennej praktyce organów nadzorczych. W trakcie warsztatów w 2021 roku omówiono kwestie związane z powiadamianiem o naruszeniu ochrony danych, wewnętrznym rozpatrywaniem skarg, działaniami egzekucyjnymi oraz skutkami wyroku Trybunału Sprawiedliwości UE z 16 lipca 2020 r. w sprawie C-311/18 („Schrems II").

Coroczne spotkania dają organom z całej EOG możliwość dzielenia się doświadczeniami w rozpatrywaniu spraw i dobrymi praktykami w zakresie wcześniej ustalonych tematów na otwartym, integracyjnym forum.

16. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2021 r. Prezes UODO i jego przedstawiciele uczestniczyli online w konferencjach, seminariach i spotkaniach o charakterze międzynarodowym, organizowanych przez UODO oraz inne podmioty krajowe i zagraniczne. Wykaz tych wszystkich wydarzeń znajduje się w załączniku nr 4.

Poniżej przedstawione zostały wybrane przykłady najważniejszych z nich.

1) Międzynarodowa Konferencja OECD pt. „OECD International Conference on AI in Work, Innovation, Productivity and Skills", 1–5.02.2021 r.

W dniach 1–5 lutego 2020 r. odbyła się online Międzynarodowa Konferencja OECD pt. „Sztuczna inteligencja w pracy, innowacja, wydajność i umiejętności". Przedstawiciel UODO uczestniczył w dwóch sesjach tego wydarzenia, tj. w sesji pt. „Ramy OECD klasyfikacji systemów AI: postępy, wyzwania i dalsze działania" (2.02.2021 r.) oraz w sesji pt. „Etyka AI w miejscu pracy" 5.02.2021 r.). Wydarzenie to zgromadziło ekspertów w zakresie technologii i polityk w celu omówienia szybko zmieniających się zmian w zakresie możliwości sztucznej inteligencji (AI) i przyjmowania tego typu rozwiązań, a także oceny jej skutków dla rynków pracy i społeczeństw. Wnioski i ustalenia płynące z tego spotkania miały wpłynąć na przyspieszenie debaty politycznej na temat konieczności przyjmowania takich rozwiązań AI w obszarze zatrudnienia, aby były one skuteczne w obszarze pracy, korzystne, skoncentrowane na ludziach i akceptowane przez ludzkość.

2) Konferencja ERA „Responding to Personal Data Breaches in the Post-GDPR era", 24–26.03.2021 r.

To już kolejna edycja konferencji organizowanej przez The Academy of European Law (ERA) z udziałem przedstawiciela UODO. Celem konferencji było dostarczenie wskazówek, jak postępować w przypadku naruszenia danych osobowych. Przedstawiciel UODO wystąpił w panelu dyskusyjnym poświęconym zagadnieniu obsługi naruszeń ochrony danych osobowych na poziomie państw członkowskich. W swoim wystąpieniu przedstawił doświadczenia polskiego organu nadzorczego w obszarze naruszeń danych osobowych, w tym kwestie związane z oceną ryzyka naruszenia praw i wolności oraz stosowaniem zasady rozliczalności w kontekście naruszeń ochrony danych oraz odpowiedzialności.

3) 52. posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108, 24–26.03.2021 r.[562]

W 52. Posiedzeniu Biura T-PD uczestniczyło ponad 100 ekspertów ds. ochrony danych reprezentujących Państwa-Strony Konwencji 108, a także obserwatorzy ze wszystkich regionów świata. W spotkaniu tym wziął udział przedstawiciel Departamentu Współpracy Międzynarodowej i Edukacji, uczestnicząc w dyskusji na temat priorytetowych tematów Komitetu Konwencji, takich jak środki podjęte lub rozważane przez państwa w ramach szczepień przeciwko COVID-19, tożsamość cyfrowa, wymiana danych finansowych, przetwarzanie danych osobowych w kontekście kampanii politycznych oraz mechanizm oceny i działań następczych zgodnie z Konwencją 108+[563].

4) 41. Posiedzenie plenarne Komitetu Konsultacyjnego Konwencji nr 108, 28–30.06.2021 r.

Ponad 150 uczestników z Państw-Stron Konwencji 108 Rady Europy o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych i obserwatorów Komitetu ze wszystkich części świata spotkało się 28–30 czerwca 2021 r. zdalnie, aby dyskutować i pracować nad aktualnymi tematami dotyczącymi ochrony danych. Komitet kontynuował prace nad kluczowymi tematami zawartymi w jego programie prac w zakresie tożsamości cyfrowej, przetwarzania danych

[562] https://www.coe.int/en/web/data-protection/-/52nd-meeting-of-the-bureau-of-the-committee-of-convention-108-was-held-online.
[563] Skrócony raport, porządek obrad i dokumenty robocze są dostępne tutaj: https://rm.coe.int/t-pd-bur-2021-52rap-en/1680a1ea74.

osobowych przez organizacje odpowiedzialne za kampanie polityczne, oraz automatycznego przekazywania danych[564].

5) Spotkanie ekspertów ds. audytów aplikacji mobilnych – Mobile App Audit Exchange, 9.06.2021 r. i 19.11.2021 r.

W analizowanym roku sprawozdawczym odbyły się dwa spotkania ekspertów ds. audytów mobilnych, podczas których omawiano szczegóły dotyczące kierunków ich współpracy. Bundeskartellamt (niezależny organ ochrony konkurencji z siedzibą w Bonn) przedstawił wyniki swojego badania sektorowego dotyczącego aplikacji mobilnych w celu zbadania praw konsumentów. Ponadto zaprezentowano program pracy związany z wymianą ekspertów ds. aplikacji mobilnych, praktyki udostępniania danych w systemach Android, iOS, metodologii ich badania, a także zakreślono możliwości szerszej współpracy i budowania potencjału partnera Europejskiego Inspektora Ochrony Danych w zakresie technologii laboratoryjnej vTrust. Organizatorem spotkania był organ nadzorczy niemieckiego kraju związkowego Badenia Wirtembergia.

6) 53. posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108, 28–30.09.2021 r.

Uczestnicy 53. Posiedzenia Biura T-PD, które z udziałem przedstawiciela UODO odbyło się online w dniach 28–30.09.2021 r., kontynuowali prace z 41. posiedzenia plenarnego Komisji ds. tematów wymienionych w Planie prac na lata 2020–2021. W szczególności skupili się na opracowaniu wytycznych dotyczących tożsamości cyfrowej, międzypaństwowej wymiany danych na potrzeby przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu i celów podatkowych, na zagadnieniach związanych z przetwarzaniem danych osobowych przez organizacje prowadzące kampanie polityczne, na art. 11 Konwencji 108+ oraz na klauzulach umownych w kontekście transgranicznych przepływów danych. Uczestnicy omówili również dokumenty dotyczące przyszłego mechanizmu oceny i przeglądu zmodernizowanej Konwencji 108[565].

7) 43. Międzynarodowa Konferencja Global Privacy Assembly – GPA, 19–22.10.2021 r.

Coroczna międzynarodowa Konferencja GPA poświęcona ochronie danych osobowych, zrzesza organy ochrony danych i prywatności z całego świata. W tegorocznej edycji tego wydarzenia udział wzięło ponad 100 uczestników, w tym przedstawiciele Urzędu Ochrony Danych Osobowych. Konferencja została podzielona na dwie sesje: otwartą i zamkniętą[566].

[564] https://rm.coe.int/t-pd-2021-41rap-en/1680a302b9
[565] https://www.coe.int/en/web/data-protection/-/the-bureau-of-the-committee-of-convention-108-held-its-53rd-session
[566] Poniższe informacje dostępne są na stronie UODO: https://uodo.gov.pl/pl/460/2189.

Wystąpienia wygłoszone podczas **sesji otwartej** (19–20.10.2021 r.) poświęcone były rozwojowi technologii i interwencji ludzkiej w masowe przetwarzanie danych, ochronie prywatności w dobie pandemii COVID-19: paszportów szczepionkowych i innych certyfikatów, przyszłości prywatności i nowych technologii oraz sztucznej inteligencji i wartości demokratycznych. Skoncentrowano się też na temacie promowania etycznego podejścia w organizacjach, ochronie danych osobowych i praw człowieka, na konieczności ustanowienia międzynarodowych standardów na rzecz skutecznej ochrony prawa człowieka, a także na zagadnieniu masowego nadzoru z wykorzystaniem technologii rozpoznawania twarzy i analizy danych. Podczas sesji równoległych dyskutowano m.in. kwestie analityki danych i prywatności użytkowników; Agendy ONZ 2030 w kontekście ochrony danych osobowych; polityki integracyjnej – sektorów ubóstwa i marginalizacji oraz ochrony danych; współpracy regionalnej w kwestiach ochrony danych i prywatności oraz konwersacji międzyregionalnej – skutecznym narzędziom zapewniającym bezpieczny i swobodny przepływ danych. Szczególną uwagę poświęcono tematowi Konwencji 108+ RE i perspektywie Traktatu RE nt. sztucznej inteligencji oraz kwestii tożsamości cyfrowej Na zakończenie ogłoszono, że pierwszym laureatem ustanowionej Nagrody GPA im. Giovanniego Buttarelliego została Shoshana Zuboff, *profesor emeritus* Uniwersytetu Harvarda, w uznaniu jej wyjątkowego wkładu w dziedzinie ochrony danych i prywatności.

W **sesji zamkniętej** Konferencji GPA (21–22.10.2021 r.) uczestniczyło ponad 90 akredytowanych członków – przedstawicieli organów ochrony danych osobowych oraz obserwatorów Konferencji. Podczas sesji tej przyjęto ogółem pięć istotnych rezolucji[567]:

1. Rezolucję w sprawie strategicznego kierunku GPA 2021–2023**;**
2. Rezolucję w sprawie wymiany danych dla dobra publicznego**;**
3. Rezolucję w sprawie praw cyfrowych dzieci**,** której współwnioskodawcą był UODO;
4. Rezolucję w sprawie dostępu rządu do danych, prywatności i rządów prawa: zasady rządowego dostępu do danych osobowych będących w posiadaniu sektora prywatnego do celów bezpieczeństwa narodowego i publicznego;
5. Rezolucję w sprawie przyszłości Konferencji i Sekretariatu**.**

[567] Wszystkie dokumenty przyjęte podczas 43. Międzynarodowej Konferencji Global Privacy Assembly zostaną w najbliższym czasie opublikowane na stronie GPA: https://globalprivacyassembly.org/document-archive/. Oświadczenie prasowe GPA dotyczące sesji zamkniętej Międzynarodowej Konferencji GPA dostępne jest pod adresem: https://globalprivacyassembly.org/highlights-from-the-global-privacy-assembly-closed-session-2021/. Więcej informacji na temat Global Privacy Assembly dostępnych jest w zakładce: https://uodo.gov.pl/pl/459.

8) 42. Posiedzenie plenarne Komitetu Konsultacyjnego Konwencji nr 108, 17–19.11.2021 r.

Komitet Konsultacyjny Konwencji nr 108 Rady Europy o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych, podczas 42. Posiedzenia plenarnego powitał nowo wybraną Specjalną Sprawozdawczynię ONZ ds. Prywatności. Podczas posiedzenia kontynuowana była dyskusja i prace nad aktualnymi tematami dotyczącymi ochrony danych. W szczególności Komitet sfinalizował i przyjął wytyczne w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez i na potrzeby kampanii politycznych[568].

Komitet kontynuował prace nad kluczowymi tematami zawartymi w jego programie prac, w szczególności tożsamością cyfrową, automatycznym przekazywaniem danych, klauzulami umownymi w kontekście transgranicznych przepływów danych, międzypaństwową wymianą danych na potrzeby przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu i celów podatkowych itp. Podczas tego spotkania laureatka Nagrody im. Stefano Rodota w 2020 roku, miała możliwość zaprezentowania Komitetowi pracy, za którą została wyróżniona, a której wcześniej nie umożliwił jej kryzys sanitarny[569].

9) Szczyt cyfrowy ONZ – GF2021 (16th Annual Meeting of the Internet Governance Forum – IGF), 6–8.12.2021 r.

Szczyt Cyfrowy ONZ to jedno z najważniejszych cyfrowych wydarzeń 2021 r. z udziałem m.in. sekretarza generalnego ONZ i wiceprzewodniczącej Komisji Europejskiej, ministrów cyfryzacji z różnych zakątków świata, przedstawicieli biznesu, działaczy organizacji pozarządowych i środowiska naukowego.

Program objął łącznie ponad 300 różnych aktywności, a wśród nich warsztaty, otwarte fora dyskusyjne, sesje grupowe i sesje networkingowe. To także sesje wysokiego szczebla z udziałem przedstawicieli państw i organizacji międzynarodowych, a także sesja parlamentarna.

[568] https://rm.coe.int/t-pd-bur-2021-3rev4-fin-draft-guidelines-political-campaigns/1680a4a36d.
[569] Pełny raport z posiedzenia dostępny jest tu: https://rm.coe.int/t-pd-2021-42-rapabr-en/1680a49798.

10) 21. Spotkanie Grupy Państw Europy Środkowej i Wschodniej, 16–17.12.2021 r.

W dniach 16–17 grudnia 2021 roku odbyło się 21. Spotkanie Grupy Państw Europy Środkowej i Wschodniej (Central and Eastern Europe personal data protection authorities – CEEDPA) zorganizowane w formule online. Wśród uczestników spotkania znaleźli się przewodniczący oraz przedstawiciele organów nadzorczych z państw członkowskich CEEDPA, zarówno należących do Unii Europejskiej, jak i spoza niej.

W roku sprawozdawczym 2021 Grupa Państw Europy Środkowej i Wschodniej obchodziła 20. rocznicę swojej działalności. Uczestnicy w trakcie dwudniowej konferencji dyskutowali przede wszystkim na temat dotychczasowych osiągnięć i dalszych wyzwań, jakie stawia przed organami ochrony danych pandemia COVID-19, wymieniali się doświadczeniami i najlepszymi praktykami dot. skutecznej ochrony danych osobowych. Przedmiotem dyskusji panelowych pierwszego dnia spotkania była kwestia narzędzi rozliczalności (*accountability mechanisms*) i ochrona prywatności w świecie dotkniętym pandemią koronawirusa. Podczas drugiego dnia debatowano nad zagadnieniem wdrażania standardów Unii Europejskiej i Rady Europy dotyczących ochrony danych osobowych oraz potencjalnych wyzwań transgranicznych z tym związanych. Ważnym tematem były także kluczowe kwestie i wyzwania związane z zapewnieniem ochrony danych osobowych dzieci. Dyskusje podczas obu dni spotkania pozwoliły uczestnikom podzielić się dotychczasową praktyką ich organów, a także przedstawić plany i wyzwania na kolejne lata w obszarze ochrony danych

osobowych. Wydarzenie dopełnił film promujący 21. Spotkanie Grupy Państw Europy Środkowej i Wschodniej i całokształt ich 20-letniej współpracy.

Gospodarzem 21. Spotkania Grupy Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej był polski organ nadzorczy. Wybór Urzędu Ochrony Danych Osobowych jako gospodarza spotkania oraz daty konferencji nie był przypadkowy. W 2021 roku CEEDPA obchodziła dwudziestolecie istnienia Grupy. Dwadzieścia lat temu, pod koniec 2001 roku Generalny Inspektor Ochrony Danych Osobowych (GIODO) zainicjował międzynarodową współpracę między organami ochrony danych osobowych z państw Europy Środkowej i Wschodniej w celu wspierania rozwoju ochrony prywatności na tym obszarze. W trakcie zorganizowanego 17 grudnia 2001 roku przez GIODO spotkania, podpisana została Deklaracja Końcowa, w której przedstawiciele organów ochrony danych osobowych z Czech, Węgier, Litwy, Słowacji, Estonii, Łotwy oraz Polski zadeklarowali chęć współpracy i wzajemnej pomocy w zakresie niezbędnym do zapewnienia odpowiedniej ochrony danych osobowych w swoich krajach[570].

Obecnie w skład grupy Państw Europy Środkowej i Wschodniej wchodzą przedstawiciele organów ochrony danych osobowych z Czech, Węgier, Litwy, Słowacji, Łotwy, Polski Bułgarii, Chorwacji, Macedonii Północnej, Rumunii, Słowenii, Albanii, Mołdawii, Serbii, Ukrainy, Bośni i Hercegowiny, Czarnogóry, Gruzji, Federacji Rosyjskiej, Kosowa i Armenii.

Celem tych spotkań jest wspieranie państw kandydujących do Unii Europejskiej oraz będących nowymi członkami, dzielenie się informacjami i doświadczeniami, podnoszenie poziomu świadomości w zakresie prawa do prywatności i ochrony danych osobowych i co najważniejsze – dalsza harmonizacja przepisów krajowych z prawem Unii Europejskiej. Spotkania CEEDPA odbywają się w formule cyklicznych konferencji i bieżącej – w zależności od aktualnych potrzeb – współpracy.

11) 54. posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108, 20–21.12.2021 r.

W dniach 20–21 grudnia 2021 r. odbyło się ostatnie w roku posiedzenie Biura, w którym wziął udział przedstawiciel UODO. Uczestnicy, połączeni online, podsumowali prace wykonane w ciągu ostatnich dwóch lat. Jednocześnie kontynuowane były prace odpowiednio nad przyszłą oceną i mechanizmem działań następczych w ramach Konwencji 108+, tożsamości cyfrowej, międzypaństwowej wymiany danych na potrzeby przeciwdziałania praniu pieniędzy/finansowaniu

[570] Więcej informacji o Grupie Państw Europy Środkowej i Wschodniej dostępnych jest na stronie Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl/pl/62.

terroryzmu i celów podatkowych, wykładni art. 11 zmodernizowanej Konwencji 108, klauzul umownych w kontekście transgranicznych przepływów danych. W ramach posiedzenia prowadzone były wymiany z konsultantami-ekspertami zajmującymi się wskazanymi tematami.

Wszystkie te tematy ujęte w Programie prac Komitetu na lata 2022–2025 będą dalej rozwijane w 2022 roku[571].

W analizowanym roku sprawozdawczym odbyły się cztery (4) **Spotkania Sieci Inspektorów Ochrony Danych (DPO Network)** – 5.02.2021, 23.04.2021, 29.09.2021, 6.12.2021. We wszystkich uczestniczył Inspektor Ochrony Danych UODO.

DPO Network to niezależna sieć inspektorów ochrony danych, której prace koordynuje EROD. W jej skład wchodzi IOD każdego z organów nadzorczych, inspektor ochrony danych EROD i inspektor ochrony danych EIOD.

Członkowie sieci podczas spotkań dzielili się wiedzą i praktyką dotyczącą m.in. przetwarzania danych w zakresie stosowania procedur współpracy i spójności. Sieć opracowywała także wewnętrzny zestaw dokumentów i narzędzi dotyczących stosowania RODO w praktyce.

V. Podsumowanie

Przechodząc do podsumowania niniejszego *Sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2021* podkreślić należy, że wyraźny wzrost liczby wpływających do Urzędu skarg osób, których dane dotyczą, z jednej strony wciąż wskazuje na problemy z przestrzeganiem prawa tych osób do ochrony danych przez administratorów, z drugiej jednak strony wskazywać może także na wzrost świadomości podmiotów danych, co do przysługujących im praw.

Spośród **8318 skarg,** które w 2021 roku wpłynęły do Urzędu, **1412** z nich dotyczyło podmiotów sektora publicznego, co stanowi ok. 17% wszystkich skarg. Dla porównania, w 2020 roku skargi na podmioty sektora publicznego stanowiły ok. 20%. Mamy więc w 2021 roku nieznaczny ich spadek.

Ogólne rozporządzenie o ochronie danych osobowych nadało osobom, których dane są przetwarzane, liczne narzędzia do kontroli przetwarzania ich danych. Wśród nich, jednym z najważniejszych, jest **prawo do uzyskania informacji na temat okoliczności przetwarzania**

[571] https://rm.coe.int/t-pd-2021-wp2022-2025-work-program-2022-2025-final/1680a3025d

danych osobowych, o którym mowa w art. 15 rozporządzenia 2016/679 (tzw. obowiązek informacyjny realizowany na wniosek). To ono, w pierwszej kolejności, pozwala administratorowi wyjaśnić i usunąć wszelkie wątpliwości klienta dotyczące podstaw prawnych przetwarzania jego danych osobowych. Z kolei osobie, której dane dotyczą, pozwala skontrolować te podstawy, wykryć ewentualne nieprawidłowości lub nieaktualność przetwarzanych danych, a w następstwie podjąć decyzję co do dalszych działań.

Niestety, zarówno po stronie podmiotów danych, jak i administratorów, zauważa się tendencję do ignorowania obowiązków informacyjnych, zwłaszcza tego, który jest realizowany na wniosek. Skarżący często pomijają tę drogę, pomimo że w większości przypadków skorzystanie z niej wyjaśniłoby wszelkie wątpliwości co do okoliczności przetwarzania. Częstym przypadkiem jest sytuacja, w której podmiot danych nie podejmował żadnej próby kontaktu z administratorem danych osobowych uciekając się wyłącznie do złożenia skargi. Powodowało to zbędne wszczynanie postępowań w przypadkach, które tego nie wymagały. Często również skargi kierowane były wobec podmiotów, które nie są administratorami, a jedynie prowadzą marketing produktów lub usług tego podmiotu, korzystając ze swoich własnych baz danych (marketing na zlecenie). Z kolei administratorzy często ignorują wezwania osób do udzielenia informacji. Jest to materia złożona, gdyż często w takiej korespondencji poruszane są roszczenia i skargi związane z realizacją samych usług (a więc roszczeniami na gruncie prawa cywilnego). Niewątpliwie kwestia ta wymaga uwagi administratorów, zwłaszcza szkoleń personelu w zakresie obsługi takich zgłoszeń.

Warto w tym miejscu zauważyć, że w styczniu 2022 roku opublikowano długo oczekiwane wytyczne Europejskiej Rady Ochrony Danych 01/2022 dotyczących praw osoby, której dane dotyczą w zakresie prawa dostępu do danych[572]. Wytyczne określają sposób realizacji tego obowiązku, zwłaszcza w kontekście dostępu do kopii danych, i wskazują wiele problemów z tym związanych.

Co roku głównym tematem skarg jest przetwarzanie danych osobowych **w celach marketingowych**. Problemy związane były głównie z nierealizowaniem obowiązków informacyjnych albo nieuwzględnianiem sprzeciwu osoby, której dane dotyczą na taki sposób przetwarzania jej danych. Obecnie marketing jest procesem zinformatyzowanym, automatycznym i masowym. Niepokojącą sytuacją jest brak pełnej kontroli administratora nad każdym aspektem takiego przetwarzania. Zauważalne jest to zwłaszcza w przypadkach zmiany systemu służącego do

[572] Obecnie wytyczne dostępne są w języku angielskim pod adresem, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_pl, Guidelines 01/2022 on data subject rights - Right of access.

prowadzenia akcji marketingowych. Systemy te okazują się nie być w pełni kompatybilne. W przypadku migracji baz danych, oznaczenie wyłączenia marketingu w stosunku do danej osoby w jednym systemie może nie zostać odczytane w drugim. Zjawisko to jest niepokojące, bo to po stronie administratora leży obowiązek zapewnienia prawidłowości przetwarzanych danych osobowych.

Organ dostrzegł również problem związany z ponownym wprowadzeniem danych do bazy danych, pomimo faktu ich wcześniejszego usunięcia. Kwestię tę na gruncie ustawy[573] z dnia 29 sierpnia 1997 r. regulował art. 32 ust. 3, który wskazywał prawo administratora do zatrzymania części danych wyłącznie w celu uniknięcia ponownego wykorzystania danych osoby, w związku z jej sprzeciwem na przetwarzanie danych w celach marketingowych. Obecnie, zgodnie z obowiązującym art. 11 ust. 1 rozporządzenia 2016/679, jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagały lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia. Niewątpliwie w wyniku ponownego wprowadzenia danych osobowych raz już usuniętych może dojść do naruszenia ochrony danych osobowych. Pożądane jest, aby administratorzy przedsięwzięli środki mające na celu uniknięcie ponownego wprowadzenia danych.

Co do **sektora zdrowia,** częstymi skargami, które w 2021 roku, jak i w latach ubiegłych, wpłynęły do Prezesa Urzędu Ochrony Danych Osobowych, były skargi na uzyskiwanie przez lekarzy dostępu do danych osobowych przetwarzanych w systemach ZUS oraz te, związane z wystawianiem recept.

Z kolei w **sektorze szkolnictwa** tematyka skarg dotyczyła głównie organizacji nauczania w placówkach oświatowych, w związku z koniecznością dostosowania ich działalności do wymogów i obostrzeń w związku z pandemią COVID-19, w szczególności w związku z publikowaniem wizerunków uczniów i nauczycieli na stronach internetowych tych placówek lub na portalach społecznościowych.

W okresie sprawozdawczym 2021 roku, w toku prowadzonych **kontroli przestrzegania przepisów rozporządzenia 206/679,** Prezes UODO zwracał szczególną uwagę na zaimplementowanie przez administratorów odpowiednich środków technicznych i organizacyjnych

[573] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2016 r. poz. 922 z późn. zm.

zapewniających bezpieczeństwo przetwarzanych danych osobowych, przeprowadzoną ocenę skutków dla ochrony danych osobowych oraz analizę ryzyka naruszenia praw lub wolności osób fizycznych, których dotyczyło naruszenie ochrony danych osobowych. Ocenie podlegały m.in. przesłanki legalności przetwarzania danych osobowych, w szczególności warunki wyrażenia zgody na przetwarzanie tych danych, w tym informacji o stanie zdrowia, umowy powierzenia przetwarzania danych osobowych, zabezpieczenia systemów informatycznych z uwzględnieniem mechanizmu tworzenia i weryfikacji kopii zapasowych, systemów antywirusowych/antyspamowych, jak również zabezpieczenia fizyczne pomieszczeń strategicznych dla bezpieczeństwa danych osobowych. Wątpliwości Prezesa UODO w kontrolowanych podmiotach wzbudziło przetwarzanie biometrycznych danych osobowych pod kątem spełniania jednego z warunków wskazanych w art. 9 ust. 2 rozporządzenia 2016/679 oraz w zakresie niezbędności i proporcjonalności identyfikacji do celów uwierzytelniania.

W analizowanym 2021 roku nastąpił znaczący wzrost liczby decyzji administracyjnych wydawanych przez Prezesa UODO nakładających na administratorów administracyjne kary pieniężne oraz decyzji, w których udzielił upomnienia administratorom w związku ze stwierdzeniem **naruszenia ochrony danych osobowych.** Zaobserwować także należy znaczący wzrost wysokości kar pieniężnych nakładanych przez organ nadzoru za naruszenia przepisów o ochronie danych osobowych.

Prezes UODO w wydanych decyzjach zwracał szczególną uwagę na:

- zawiadamianie osób, których dane dotyczą o naruszeniu ochrony ich danych osobowych, pod kątem spełniania przesłanek z art. 34 ust. 1 rozporządzenia 2016/679 lub art. 34 ust. 3 rozporządzenia 2016/679 – jako wyjątku od zasady bezpośredniego zawiadomienia – i obowiązek notyfikacji naruszeń organowi nadzorczemu;
- wdrożenie odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzania danych osobowych, poprzedzone szacowaniem poziomu ryzyka dla procesu przetwarzania danych, uwzględniając przy tym kryteria wskazane w art. 32 ust. 1 rozporządzenia 2016/679, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku;
- regularne testowanie, mierzenie i oceniania skuteczności ww. środków na każdym etapie przetwarzania.

W zgłoszonych Prezesowi UODO naruszeniach będących przedmiotem postępowania administracyjnego, istotnym problemem był brak weryfikacji doboru i poziomu skuteczności stosowanych środków technicznych, ocenianych przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu i celów przetwarzania, brak działań zmierzających do optymalnej konfiguracji wykorzystywanych systemów operacyjnych poprzez regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych, w postaci testów bezpieczeństwa w zakresie infrastruktury informatycznej oraz aplikacji, które powinny wynikać z przeprowadzonej analizy ryzyka, identyfikującej podatności odnoszące się do wykorzystywanych zasobów oraz wynikające z nich zagrożenia.

Analiza treści zgłoszonych naruszeń pozwala na stwierdzenie, że administratorzy w przeprowadzanych analizach ryzyka nie uwzględniali: podatności przyjętego przez nich systemu sporządzania kopii zapasowej na działanie oprogramowania typu *ransomware*, a tym samym nie uwzględniali ryzyka wystąpienia zdarzenia zaszyfrowania kopii zapasowych przez złośliwe oprogramowanie bądź zagrożenia w postaci niespójności baz danych odtworzonych z kopii zapasowej, a także kwestii związanych z aktualizacją systemów informatycznych wykorzystywanych do przetwarzania danych osobowych, w tym zagrożeniach związanych z używaniem nieaktualnych wersji systemów informatycznych. Zasady tworzenia kopii zapasowych, wprowadzone u administratorów, nie zapewniały realizacji obowiązków wynikających z art. 32 ust. 1 lit. b) i c) rozporządzenia 2016/679, tj. zdolności do ciągłego zapewniania dostępności systemów i usług przetwarzania oraz zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu technicznego lub fizycznego. Ponadto szacowanie ryzyka dokonywane przez administratorów przed_wystąpieniem naruszenia ochrony danych osobowych, jak i po jego wystąpieniu nie uwzględniało w sposób prawidłowy stopnia ryzyka dla osób, których dane dotyczą. W jednej z rozpatrywanych spraw z przeprowadzonej analizy ryzyka wynikało zaniżenie prawdopodobieństwa pojawienia się ryzyka w postaci ataku hakerskiego, czy ataku *ransomware*, co miało wpływ na brak prawidłowej oceny zagrożenia dla procesu przetwarzania danych i w konsekwencji brak wdrożenia dodatkowych środków technicznych i organizacyjnych.

W procesie powierzenia przetwarzania danych osobowych Prezes UODO badał spełnianie przez administratorów obowiązków wynikających z art. 28 rozporządzenia 2016/679, w szczególności poddawał analizie treść umowy powierzenia przetwarzania danych pod kątem

spełniania przesłanek określonych w art. 28 ust. 3 RODO. Istotną kwestią dla ochrony praw i wolności osób fizycznych w kontekście naruszenia ich danych osobowych było zawiadomienie zarówno tych osób, jak i organu nadzorczego, o zaistniałym incydencie bezpieczeństwa. Nie bez znaczenia dla ochrony danych osobowych pozostają także działania administratorów mające na celu zwiększanie świadomości w zakresie ochrony danych osobowych oraz szkolenie pracowników biorących udział w operacjach przetwarzania danych.

Mając powyższe na uwadze, w ocenie Prezesa UODO istotnym z punktu widzenia naruszeń ochrony danych osobowych jest wdrożenie odpowiednich procedur pozwalających na wykrycie i zgłoszenie tego incydentu, dokonanie klasyfikacji i analizy zdarzenia, jego stopnia i rodzaju oraz dokonanie oceny skutków dla praw i wolności osób fizycznych, niezbędnej do podjęcia decyzji w przedmiocie notyfikacji naruszenia organowi nadzorczemu i zawiadomienia osób, których ten incydent dotyczy, a także sprawne podjęcie działań mających na celu m.in. ograniczenie rozmiaru naruszenia i odzyskanie dostępności do baz danych.

Urząd Ochrony Danych Osobowych nieustannie podejmuje szereg **działań edukacyjnych**, które wpisują się w misję organu nadzorczego. Poprzez edukację i informację upowszechnia w społeczeństwie wiedzę o ochronie danych osobowych i ryzyku, a także o przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienia tych zjawisk – poświęcając szczególną uwagę działaniom skierowanym do dzieci. Efektem takiego podejścia jest realizowany od 12 lat ww. ogólnopolski program edukacyjny dla szkół, uczniów i ośrodków doskonalenia nauczycieli „Twoje dane – Twoja sprawa". Uczestnicy Programu podkreślają, jak ważny był dla nich praktyczny aspekt przekazywanych w jego ramach treści i informacji oraz możliwość wykorzystywania ich na co dzień. Dużym zainteresowaniem cieszą się zwłaszcza materiały opracowane przez UODO – tzw. pigułki wiedzy z cyklu „Warto wiedzieć", które pozwalają zdobyć wiedzę z zakresu ochrony danych osobowych, szczególnie w środowisku cyfrowym. Podczas realizacji Programu ważne było również wsparcie ekspertów nie tylko Urzędu Ochrony Danych Osobowych, ale także inspektorów ochrony danych osobowych. Spotkania z ekspertami, zajęcia i współpraca z licznymi instytucjami, a także zaangażowanie rodziców czy seniorów w działania edukacyjne szkół miały znaczny wpływ na skuteczność podejmowanych działań w ramach tego przedsięwzięcia.

Podobnie jak w poprzednich edycjach Programu, nauczyciele i uczniowie bardzo pozytywnie go ocenili. Nauczyciele podkreślają konieczność organizowania zajęć w tym obszarze tematycznym

w szkołach – jako niezbędny element zapewnienia bezpieczeństwa nauczania w placówkach oświatowych.

Wieloletnia realizacja przedsięwzięcia w szkołach przyczynia się do kształtowania prawidłowych podstaw i nawyków dzieci i młodzieży w zakresie bezpieczeństwa, wzrostu świadomości w zakresie ochrony prywatności, popularyzacji wiedzy na temat ochrony danych osobowych wśród uczniów i nauczycieli, a także wzrostu zainteresowania tym tematem. Program stanowi źródło aktualnej wiedzy i dobrych praktyk w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty.

Doświadczenia przy realizacji Programu pokazują, że w trakcie edukacji szkolnej można skutecznie uczyć bezpiecznych zachowań w życiu codziennym, tak aby dzieci już od najmłodszych lat rozumiały szanse i zagrożenia związane z rozwojem nowoczesnych technologii. Odpowiednia wiedza umożliwia bowiem uczniom odpowiedzialne i bezpieczne funkcjonowanie we współczesnym świecie.

Warto również podkreślić ogromną rolę podmiotów współpracujących i popierających działania edukacyjne Urzędu Ochrony Danych Osobowych m.in. Rzecznika Praw Dziecka, Ministra Edukacji Narodowej (obecnie Ministra Edukacji i Nauki), które jest dowodem na to, że temat ten jest ważny i niezbędny w edukacji dzieci i młodzieży. Coraz więcej dyrektorów szkół widzi również potrzebę podniesienia świadomości nauczycieli w organizacji procesu zdalnej edukacji oraz współpracę z inspektorem ochrony danych osobowych.

Analiza spraw prowadzonych w roku 2021 pozwala z jednej strony na wskazanie pewnych pozytywnych tendencji, a z drugiej wyzwań, z jakimi w zakresie ochrony danych osobowych trzeba będzie się zmierzyć w najbliższym czasie.

Stwierdzić można, że konsekwentne, prowadzone od chwili rozpoczęcia stosowania RODO, działania organu nadzorczego, zapewniające wielu różnym środowiskom wsparcie eksperckie na etapie tworzenia oraz stosowania prawa, przynoszą zamierzone rezultaty. Z roku na rok rośnie bowiem wiedza i świadomość zarówno administratorów i podmiotów przetwarzających, jak i osób, których dane dotyczą.

Do budowania kultury ochrony danych osobowych w istotny sposób przyczyniają się również wytyczne Europejskiej Rady Ochrony Danych (EROD), której polski organ nadzorczy jest członkiem i w której pracach aktywnie uczestniczy. Dokumenty te, służące właściwemu i jednolitemu stosowaniu RODO, budzą duże zainteresowanie administratorów i niejednokrotnie już na etapie ich

publicznych konsultacji bywają przedmiotem pogłębionych analiz skutkujących kierowaniem do UODO bardzo szczegółowych pytań. Tak było m.in. w przypadku wytycznych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO czy wytycznych 5/2021 w sprawie wzajemnych relacji pomiędzy art. 3 i rozdziałem V RODO, których celem jest pomoc w ustaleniu, czy operacja przetwarzania stanowi międzynarodowe przekazywanie danych.

Podnoszeniu świadomości i zapewnieniu wsparcia w projektowaniu rozwiązań zapewniających poszanowanie prawa do ochrony danych osobowych, a także wymianie stanowisk i opinii służyła również współpraca UODO z innymi regulatorami, w tym m.in. z Rzecznikiem Praw Pacjenta[574] czy Urzędem Komisji Nadzoru Finansowego[575]. Cel ten realizowany był także poprzez takie działania, jak szkolenie dla legislatorów sejmowych czy stała współpraca ze środowiskami pracującymi nad stworzeniem kodeksów postępowania.

Z satysfakcją należy też odnotować fakt, że część podmiotów pracujących nad **nowymi regulacjami prawnymi korzysta z eksperckiego wsparcia organu nadzorczego na bardzo wczesnym etapie**. Jako przykład takich działań wskazać można spotkania robocze dotyczące projektu ustawy o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw czy spotkania mające na celu omówienie kwestii ochrony danych osobowych w procesie składania podpisu biometrycznego zorganizowane przez Ministerstwo Sprawiedliwości. Przedstawiciele UODO uczestniczyli też z głosem doradczym w posiedzeniach Zespołu problemowego ds. rozwoju dialogu społecznego Rady Dialogu Społecznego, podczas których dyskutowano o możliwości korzystania przez związkowych oraz pozazwiązkowych przedstawicieli pracowników z możliwości komunikacji z pracownikami drogą mailową, przy jednoczesnym poszanowaniu ich prywatności. Tego typu działania sprzyjają przygotowywaniu przepisów zgodnych z zasadami określonymi w RODO, a jednocześnie klarownych, niebudzących wątpliwości w praktyce.

Warto podkreślić, że na skutek uwag wniesionych w toku prac legislacyjnych udało się wprowadzić wiele istotnych zmian. Przykładowo, podczas prac nad projektem rozporządzenia Rady

[574] Z Rzecznikiem Praw Pacjenta w sprawie o sygn. DOL.023.572.2021 konsultowano kwestie odbierania od pacjentów zgody na udostępnienie ich dokumentacji medycznej zakładom ubezpieczeń w sytuacji, gdy placówki medyczne występują w roli strony umowy obowiązkowego ubezpieczenia odpowiedzialności cywilnej w procesie dochodzenia roszczeń przez pacjentów, w związku z udzieleniem im świadczeń zdrowotnych lub niezgodnego z prawem zaniechania ich udzielenia.

[575] Współpraca z Urzędem Komisji Nadzoru Finansowego dotyczy m.in. udoskonalenia art. 70a Prawa bankowego, regulującego kwestię przekazywania przez banki osobom ubiegającym się o kredyt informacji o dokonanej ocenie ich zdolności kredytowej (DOL.071.42.2021). Przedstawiciele UODO uczestniczyli też w pracach Zespołu roboczego ds. rozwoju innowacji finansowych FinTech pod auspicjami UKNF, deklarując eksperckie wsparcie na etapie opiniowania konkretnych propozycji zmian przepisów (DOL.071.44.2021).

Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2022, uzgodniono istotne ograniczenie zakresu pozyskiwanych na te potrzeby danych osobowych[576], a w projekcie ustawy o ekonomii społecznej dodano dział „Ochrona danych osobowych".

Niemniej w opinii organu nadzorczego wciąż jest jeszcze wiele, niekiedy podstawowych kwestii, które wymagają analizy, dyskusji oraz wprowadzenia stosownych zmian. Jedną z nich jest potrzeba dokończenia przeglądu krajowych przepisów prawa pod kątem zapewnienia ich zgodności z RODO. Analiza taka, przeprowadzona w 2018 r. w związku z rozpoczęciem stosowania RODO i zakończona wprowadzeniem w porządku prawnym szeregu zmian ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, mimo że obejmowała wiele aktów prawnych, nie była pełna i wymaga kontynuacji.

Nie podjęto np. wysiłku dostosowania do RODO prawodawstwa w zakresie tak istotnej kwestii, jak dostęp do informacji publicznej. Tymczasem ustawa o dostępie do informacji publicznej zawiera unormowania, które nie tylko nie uwzględniają wymogów wynikających z RODO, ale wprost wyłączają ochronę danych osobowych. Pozbawia to osoby, których dane dotyczą, możliwości realizacji ich fundamentalnych uprawnień wynikających z RODO, co było już sygnalizowane w „Sprawozdaniu z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2020"[577].

Kolejnym istotnym zagadnieniem jest niewłaściwa implementacja tzw. dyrektywy policyjnej[578], która w praktyce powoduje wątpliwości interpretacyjne. W związku z otrzymywanymi w tej sprawie sygnałami, UODO przygotował materiał wyjaśniający niektóre wątpliwości, co do stosowania przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, które zostały przekazane do Inspektora Nadzoru Wewnętrznego w MSWiA, a za jego pośrednictwem – służbom podległym temu resortowi. Niezależnie od tego, kwestia potrzeby wprowadzenia zmian w przepisach prawa na początku 2022 r. została zasygnalizowana MSWiA stosownym wystąpieniem[579] i będzie przez organ nadzorczy monitorowana.

W opinii organu nadzorczego, konieczny jest również przegląd przepisów dotyczących wykorzystywania i upubliczniania numeru PESEL, który jest krajowym numerem identyfikacyjnym

[576] https://uodo.gov.pl/pl/138/2098
[577] Zob. s. 115–118.
[578] 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. Urz. UE L 119 z 4.5.2016, str. 89 z późn. zm.).
[579] DOL.413.4.2022.

w rozumieniu RODO. Niektóre polskie regulacje budzą wątpliwości, co do zgodności z art. 87 powołanego rozporządzenia, zgodnie z którym numeru tego można używać, ale wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, a które przewiduje wskazane rozporządzenie. Tymczasem ujawnienie numeru PESEL może rodzić szereg ryzyk, w tym ryzyko kradzieży tożsamości, gdy trafia on do osoby niepowołanej, jak również, gdy jest zestawiany z innymi danymi i wykorzystywany w innych celach niż pierwotnie wskazane. Na szczególne ryzyka są tym bardziej narażone osoby, których PESEL jest powszechnie dostępny w rejestrach publicznych i to bez spełnienia żadnych dodatkowych warunków. W tej sytuacji prowadzący taki rejestr, upowszechniając PESEL, traci automatycznie kontrolę nad tym, kto i w jakich celach oraz w jaki sposób będzie dalej dane te wykorzystywał. Z drugiej strony natomiast istnieją ryzyka związane z dalszym przetwarzaniem numerów PESEL przez kolejnych administratorów w celach innych niż pierwotny cel ich pozyskania. Problem ten jest systematycznie poruszany przez organ nadzorczy. I to zarówno w toku prac legislacyjnych nad poszczególnymi regulacjami, w których model powszechnej dostępności numeru PESEL jest przyjmowany bez uprzedniej oceny skutków dla ochrony danych (analizy ryzyk przy określaniu sposobów przetwarzania), jak i w toku realizacji innych zadań organu nadzorczego, m.in związanych z kontrolą rozwiązań prowadzących do rozpowszechnienia bez żadnych dodatkowych warunków numeru PESEL i innych danych, np. zawartych w księgach wieczystych[580], czy w innych rejestrach publicznych, takich jak np. Krajowy Rejestr Sądowy, co z kolei było przedmiotem wystąpienia Prezesa UODO do Ministra Sprawiedliwości[581].

W najbliższym czasie poważnym wyzwaniem będzie także przegląd prawa tworzonego na potrzeby realizacji zadań mających na celu ograniczenie i złagodzenie skutków pandemii COVID-19. Europejska Rada Ochrony Danych, zachęcając do rozważnego budowania rozwiązań prawnych w okresie epidemii, wskazywała na konieczność zapewnienia im charakteru epizodycznego[582]. Stąd też i organ nadzorczy wielokrotnie zwracał uwagę na ryzyko konstruowania przepisów, w których w sposób blankietowy określa się cele przetwarzania, buduje bazy z szerokim zakresem danych osobowych, czy też kształtuje ograniczenia podstawowych praw i wolności podmiotów

[580] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 24 sierpnia 2020 r. dotycząca udostępniania danych za pośrednictwem Geoportalu2, znak: DKN.5112.13.2020.
[581] Wystąpienie Prezesa UODO z dnia 26 kwietnia 2019 r. znak: ZSPU.023.53.2019.
[582] Wytyczne 04/2020 w sprawie wykorzystywania danych o lokalizacji oraz narzędzi służących ustalaniu kontaktów zakaźnych w kontekście pandemii COVID-19 przyjętych 21 kwietnia 2020 r.

danych na poziomie aktów wykonawczych, a nie ustaw i to w sposób nieograniczony czasowo[583]. Dlatego z chwilą ogłoszenia całkowitego zakończenia pandemii COVID-19[584] konieczny będzie przegląd systemu prawa dla wyeliminowania z niego rozwiązań, którym nie nadano charakteru epizodycznego, a które są zbędne/nieadekwatne z punktu widzenia podstawowych praw i wolności osób fizycznych, w tym prawa do prywatności. Będzie to jednak zadanie przede wszystkim dla projektodawców, a organ nadzorczy będzie mógł się włączyć do niego w roli eksperckiej.

Podobne działania powinny zostać również podjęte przez administratorów. Powinni oni rozważyć, czy nie przetwarzają danych nadmiarowych, zbędnych, gdyż zamierzony cel został osiągnięty, a nie ma innej podstawy legalizującej takie działanie.

Niepokojącą tendencją, która będzie przedmiotem szczególnej troski organu nadzorczego, jest tworzenie przepisów przewidujących przetwarzanie danych osobowych, często na wielką skalę lub prowadzących do łączenia różnych baz i rejestrów, bez wnikliwej analizy wszystkich aspektów przetwarzania, bez oceny wiążących się z tym ryzyk, a często regulujących kwestie związane z pozyskiwaniem danych osobowych przepisami rangi rozporządzenia, a nie ustawy. Przykładem takich budzących zastrzeżenia rozwiązań jest wskazany już projekt ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, do którego Prezes UODO zgłosił szereg uwag na różnych etapach procesu legislacyjnego[585].

Dla organu nadzorczego wyzwaniem będzie zapewnienie właściwej ochrony danych osobowych przetwarzanych przy użyciu aplikacji, portali, wspólnych systemów czy innych rozwiązań informatycznych. Są one coraz powszechniej stosowane, lecz tworzone z pominięciem określonych w RODO zasad. Tymczasem jego przepisy wskazują, że każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony danych (i prywatności)

[583] Pismo z dnia 5 stycznia 2022 r. (znak: DOL.401.627.2021.WL.EKR) dot. projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz niektórych innych ustaw, czy też pismo z dnia 16 grudnia 2021 r. (znak: DOL.401.601.2021.WL.PM) dot. poselskiego projektu ustawy o szczególnych rozwiązaniach zapewniających możliwość prowadzenia działalności gospodarczej w czasie epidemii COVID-19 (druk nr 1846).

[584] Rozporządzeniem Rady Ministrów z dnia 13 maja 2022 r. zmieniającym rozporządzenie w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz. U. z 2022 r. poz. 1025), z dniem 16 maja 2022 r. zniesiono w Polsce stan epidemii zastępując go stanem „zagrożenia epidemicznego".

[585] Uwagi organu nadzorczego były zgłaszane do projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, która nowelizowała przepisy ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, wprowadzając ZPA, zarówno na rządowym etapie prac legislacyjnych, jak i po przekazaniu projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego do Sejmu Rzeczypospolitej Polskiej i Senatu Rzeczypospolitej Polskiej [pisma: z 12 maja 2021 r., z 14 czerwca 2021 r., z 15 czerwca 2021 r., z 13 lipca 2021 r. i z 2 sierpnia 2021 r. (sygn. DOL.401.398.2020)]. Organ nadzorczy zgłaszał też liczne uwagi do – przesłanego przez Ministra Cyfryzacji – dokumentu Opis założeń projektu informatycznego „Zintegrowana Platforma Analityczna" (pismo z 28 sierpnia 2018 r. i kolejna korespondencja w sprawie, znak: ZSPU.023.78.2018), wskazując na swoje wątpliwości, co do sposobu i zakresu przetwarzania danych osobowych.

zarówno w fazie projektowania (*privacy by design*), jak i w czasie samego przetwarzania. Oznacza to, że jeśli przewiduje się przetwarzanie danych osobowych przy wykorzystaniu określonych rozwiązań informatycznych, to od samego początku, na każdym etapie projektowania ich wykorzystywania, pod uwagę należy brać wpływ, jaki ich stosowanie wywrze na sferę prywatności. Uwzględniać przy tym trzeba stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych, a jednocześnie tak projektować cyfrowe rozwiązania, by były odpowiednie dla konkretnego przypadku. Dodatkowo wzięte pod uwagę powinno być wynikające z przetwarzania ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Oprócz uwzględniania ochrony danych w fazie projektowania (art. 25 ust. 1 RODO) równie istotne jest też wdrożenie mechanizmów zapewniających stosowanie zasady domyślnej ochrony danych (art. 25 ust. 2 RODO). Zasadę tę należy rozumieć jako postulat uwzględnienia jak najdalej posuniętych gwarancji, środków ochrony praw i wolności, w tym zabezpieczeń prywatności w ustawieniach początkowych każdego systemu. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego mają być zbierane (minimalizacja danych). Pożądane jest, aby ten aspekt brać pod uwagę już na etapie projektowania rozwiązań prawnych. To one powinny być skonstruowane tak, by z jednej strony umożliwiały spełnianie wskazanych w RODO funkcjonalności i zasad, a z drugiej strony pozwalały na zachowanie gwarantowanej w RODO neutralności technologicznej. Jeśli zaś w przetwarzaniu danych z wykorzystaniem nowoczesnych rozwiązań informatycznych uczestniczyć będą różne podmioty, ważne jest precyzyjne określenie ich ról oraz praw i obowiązków, tak, by w sposób niebudzący wątpliwości wiadomo było, kto, na jakich etapach jest odpowiedzialny za to przetwarzanie (w tym m.in. pozyskiwanie czy udostępnianie danych). Nie bez znaczenia w kontekście art. 25 RODO jest też uwzględnianie ochrony danych w czasie samego przetwarzania określonego przepisami prawa, stąd uwagi organu do projektowanych przepisów przyjmują również charakter *de lege ferenda* w uzasadnionych przypadkach. Przykładem takich działań są np. uwagi zgłoszone w czasie prac nad projektem rozporządzenia Ministra Sprawiedliwości w sprawie sposobu zamieszczania danych w Krajowym Rejestrze Zadłużonych, sposobu przetwarzania i ujawniania danych zawartych w Rejestrze, a także trybu i sposobu przetwarzania oraz przekazywania danych zgromadzonych w Rejestrze do badań naukowych oraz do celów statystycznych[586], w toku których

[586] DOL.401.55.2021.

podnieśliśmy kwestię upublicznienia numeru PESEL w Krajowym Rejestrze Zadłużonych na podstawie obowiązującej ustawy z dnia 6 grudnia 2018 r. o Krajowym Rejestrze Zadłużonych.

Urząd Ochrony Danych Osobowych niezmiennie prowadzi intensywną współpracę z wyspecjalizowanymi podmiotami, jakimi są **inspektorzy ochrony danych**. Potrafią oni w wielu obszarach objaśniać osobom odpowiedzialnym za przetwarzanie danych osobowych sposób stosowania przepisów o ochronie danych, a w przypadkach najtrudniejszych, często wymagających działań systemowych (w tym o charakterze legislacyjnym), sygnalizują je UODO. Organ wyjaśniał wątpliwości inspektorów nie tylko w udzielonych indywidualnie odpowiedziach, ale również m.in. w przygotowanych na ich podstawie materiałach zamieszczonych na stronie internetowej Urzędu[587]. Można również dostrzec, że dla inspektorów przedstawione w poprzednich latach wyjaśnienia i wskazówki organu ds. ochrony danych osobowych, wyznaczające kierunek i zasady interpretacji przepisów, posłużyły również jako podpowiedź dla rozstrzygania nowych pojawiających się wątpliwości.

Dlatego tak wielką wagę organ nadzorczy przywiązuje do współpracy z inspektorami ochrony danych. Bo to oni – dysponując odpowiednią wiedzą i umiejętnościami, a także mając odpowiednią pozycję w organizacji, w której funkcjonują – stanowią fundament **skutecznego systemu ochrony danych osobowych**. Dla administratora realizują bowiem istotne funkcje: weryfikacyjną i doradczą. Jednocześnie pełnią inną ważną rolę – punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą, oraz między administratorem lub podmiotem przetwarzającym a organem nadzorczym. Stąd tak ważne jest ich wspieranie we właściwym wypełnianiu tych funkcji, w tym weryfikowanie przestrzegania przez podmioty powołujące IOD przepisów dotyczących ich funkcjonowania, czy udzielanie konsultacji we wszelkich sprawach, którymi się zajmują.

Jest to szczególnie ważne, gdy weźmie się pod uwagę wciąż rosnące zainteresowanie obywateli problematyką ochrony danych osobowych i działalnością organu nadzorczego.

[587] Głównie w zakładce Inspektor Ochrony Danych (https://uodo.gov.pl/p/najwazniejsze-tematy/inspektor-ochrony-danych) czy w newsletterze UODO dla IOD.

ZAŁĄCZNIKI

Załącznik nr 1

Wykaz administracyjnych kar pieniężnych wymierzonych przez Prezesa UODO w 2021 r.

L.p.	Data decyzji	Departament prowadzący postępowanie	Sygnatura	Administrator	Wysokość kary w zł
1.	5.01.2021	Departament Kontroli i Naruszeń	DKN.5131.6.2020	Śląski Uniwersytet Medyczny	25 000,00
2.	5.01.2021	Departament Kar i Egzekucji	DKE.561.16.2020	ANWARA Sp. z o.o.	21 397,00
3.	5.01.2021	Departament Kar i Egzekucji	DKE.561.11.2020	Osoba fizyczna prowadząca działalność z zakresu ochrony zdrowia	85 588,00
4.	11.02.2021	Departament Kontroli i Naruszeń	DKN.5131.7.2020	ENEA S.A.	136 437,00
5.	11.02.2021	Departament Kontroli i Naruszeń	DKN.5130.2024.2020	Krajowa Szkoła Sądownictwa i Prokuratury	100 000,00
6.	19.03.2021	Departament Kar i Egzekucji	DKE.561.25.2020	Funeda Sp. z o.o.	22 739,00
7.	22.04.2021	Departament Kontroli i Naruszeń	DKN.5130.3114.2020	Cyfrowy Polsat S.A.	1136 975,00
8.	27.04.2021	Departament Kar i Egzekucji	DKE.561.23.2020	PNP S.A.	22 739,00
9.	8.06.2021	Departament Kontroli i Naruszeń	DKN.5131.10.2020	P4 Sp. z o.o.	10 000,00
10.	21.06.2021	Departament Kontroli i Naruszeń	DKN.5131.3.2021	Sopockie Tow. Ubez. ERGO Hestia S.A.	159 176,00
11.	30.06.2021	Departament Kontroli i Naruszeń	DKN.5131.11.2020	Fundacja Promocji Mediacji i Edukacji Prawnej Lex Nostra	13 644,00
12.	13.07.2021	Departament Kontroli i Naruszeń	DKN.5131.22.2021	Prezes Sądu Rejonowego w Zgierzu	10 000,00

13.	14.10.2021	Departament Kontroli i Naruszeń	DKN.5131.16.2021	Bank Millennium S.A.	363 832,00
14.	1.12.2021	Departament Kar i Egzekucji	DKE.561.16.2021	Pactum Poland Sp. z o.o.	18 192,00
15.	9.12.2021	Departament Kontroli i Naruszeń	DKN.5130.2559.2020	Politechnika Warszawska	45 000,00
16.	22.12.2021	Departament Kar i Egzekucji	DKE.561.13.2021	Osoba fizyczna prowadząca działalność w zakresie doradztwa i pośrednictwa podatkowego	4 548,00
17.	23.12.2021	Departament Kar i Egzekucji	DKE.561.19.2021	Osoba fizyczna prowadząca działalność w zakresie świadczenia usług finansowych	4 548,00
18.	31.12.2021	Departament Kar i Egzekucji	DKE.561.1.2021	Solid Workers24 Sp. z o.o.	18 192,00

Załącznik nr 2

Wykaz wydarzeń objętych patronatem Prezesa UODO w 2021 r.

1. Konferencja pt. „IOD wobec nowych wyzwań w ochronie danych osobowych". Organizator: SABI – Stowarzyszenie Inspektorów Ochrony Danych. 26.01.2021 r.
2. Konferencja „Ochrona Danych Osobowych – wyzwania 2021". Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp.k., 27.01.2021 r.
3. VII Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej, 3.02.2021 r.
4. Konferencja Naukowa pt. „Zatrudnienie pracowników tymczasowych a RODO". Organizatorzy: Katedra Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego oraz portal GDPR.pl, 18.03.2021 r.
5. Konferencja online pt. „Przemysł żywnościowy a ochrona danych osobowych – szanse i zagrożenia w dobie gospodarki opartej o dane". Organizator: Polska Federacja Producentów Żywności Związek Pracodawców, 14.04.2021 r.
6. Konferencja online pt. „RODO w sektorze medycznym – gdzie jesteśmy, dokąd zmierzamy? – edycja III". Organizator: Polska Federacja Szpitali, 25.05.2021 r.
7. Konferencja pt. „AI w Zdrowiu". Organizatorzy: Polska Federacja Szpitali, Ambasada Brytyjska i Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu. 8.06.2021 r.
8. „Ochrona danych osobowych w dobie pandemii" oraz „Zagrożenie dla bezpieczeństwa i ochrony danych zdaniem Polaków – raport z badań". Inicjatorzy: Krajowy Rejestr Długów i serwis ChronPESEL.pl.
9. X Konwent Ochrony Danych Osobowych i Informacji pt. „RODO – naruszenia, decyzje, kary". Organizatorzy: FORSAFE Sp. z o.o. oraz Lubasz i Wspólnicy – Kancelaria Radców Prawnych Sp.k., 6–7.10.2021 r.
10. Konferencja pt. „RODO w zakładzie pracy. Przetwarzanie danych osobowych pracowników dotyczących zdrowia a BHP". Organizator: Katedra Prawa Pracy i Polityki Społecznej WPiA Uniwersytetu Jagiellońskiego. Kraków, 10.12.2021 r.
11. Badanie pt. „Ochrona danych osobowych w 2022 r.". Inicjatorzy: Krajowy Rejestr Długów i serwis ChronPESEL.pl.

Załącznik nr 3

Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2021 r. w Polsce przez UODO lub inne podmioty.

L. p.	Data	Wydarzenie	Miejsce
1.	14.01.2021	Spotkanie sieci współpracy placówek doskonalenia zawodowego nauczycieli w ramach XI ed. programu TDTS.	online
2.	15.01.2021	Spotkanie informacyjne przedstawicieli resortów i urzędów centralnych poświęcone IGF 2021 – Szczyt Cyfrowy ONZ. Organizator: Departament Polityki Cyfrowej KPRM.	Warszawa online
3.	21.01.2021	Konferencja pt. „Tożsamość cyfrowa – kim jesteśmy w Internecie". Organizator: Dolnośląski Ośrodek Doskonalenia Nauczycieli we Wrocławiu.	Wrocław online
4.	26.01.2021	Dzień IOD – Konferencja „IOD wobec nowych wyzwań w ochronie danych osobowych". Organizator: SABI – Stowarzyszenie Inspektorów Ochrony Danych Osobowych.	Warszawa online
5.	27.01.2021	Ceremonia wręczenia Nagrody im. Michała Serzyckiego, GIODO III kadencji, laureatom III edycji.	Warszawa online
6.	27.01.2021	Konferencja „Ochrona Danych Osobowych – Wyzwania 2021". Organizator: Lubasz i Wspólnicy Kancelaria Radców Prawnych.	Łódź online
7.	28.01.2021	XV Dzień Ochrony Danych Osobowych – Konferencja „Realna ochrona danych osobowych w zdalnej rzeczywistości". Organizator: Urząd Ochrony Danych Osobowych.	Warszawa online
8.	3.02.2021	VII Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej.	online
9.	15.02.2021	Webinarium dot. wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Organizator: UODO.	online
10.	17.02.2021	Debata medialna pt. „Praca zdalna w urzędzie i rozwój e-administracji. Szanse i zagrożenia". Organizator: Polska Agencja Prasowa.	online
11.	18.02.2021	Webinarium nt. bezpieczeństwa ochrony danych w Internecie. Organizatorzy: UODO i OEZiK.	online
12.	22.02.2021	Spotkanie UODO z KSP dot. wspólnych działań edukacyjnych.	online
13.	23–25.02.2021	Konferencja „Polskie prawo o ochronie danych: trendy, ryzyka i szanse". Organizator: Privacy Laws & Business.	online
14.	25.02.2021	Udział w spotkaniu przedstawicieli ALK w Warszawie z przedstawicielami Polskiej Komisji Akredytacyjnej. Organizator: Kolegium Prawa Akademii Leona Koźmińskiego w Warszawie.	online
15.	5.03.2021	Webinarium w ramach programu Reaguj i wspieraj. Organizator: UODO i Mazowieckie Kuratorium Oświaty.	online
16.	11.03.2021	Webinarium pt. „Bezpieczeństwo danych osobowych na odległość". Organizatorzy: UODO i Mazowieckie Kuratorium Oświaty w Warszawie.	online
17.	18.03.2021	Konferencja Naukowa pt. „Zatrudnienie pracowników tymczasowych a RODO". Organizatorzy: Katedra Prawa Pracy i Polityki Społecznej oraz portal GDPR.	online
18.	27.03.2021	Wykład pt. „Podstawy prawne (międzynarodowe, europejskie, krajowe) ochrony danych osobowych" inaugurujący 21. ed. studiów podyplomowych „Ochrona danych osobowych" w ALK w Warszawie.	online
19.	31.03.2021	Spotkanie wykładowców UODO z przedstawicielami KSAP w związku z inauguracją 5. ed. Studium dla IOD.	online

20.	9.04.2021	Webinarium w ramach TDTS pt. „Bezpieczeństwo cyfrowe dzieci i młodzieży a odpowiedzialność". Organizator UODO oraz KSP.	online
21.	13.04.2021	Wideokonferencja przedstawicieli UODO ze Związkiem Pracodawców Innowacyjnych Firm Farmaceutycznych INFARMA, nt. przystąpienia do prac nad kodeksem postępowania. Organizator: UODO.	online
22.	13–14.04.2021	Ogólnopolska Konferencja Naukowa 7. Forum Prawa Mediów Elektronicznych. Organizatorzy: Okręgowa Izba Radców Prawnych we Wrocławiu, Uniwersytet Wrocławski, Uniwersytet Opolski, Uniwersytet Szczeciński, Ośrodek Naukowo-Szkoleniowy przy Krajowej Radzie Komorniczej.	online
23.	14.04.2021	Konferencja pt. „Przemysł żywnościowy a ochrona danych osobowych – szanse i zagrożenia w dobie gospodarki opartej o dane". Organizator: Polska Federacja Producentów Żywności Związek Pracodawców.	online
24.	20.04.2021	VII Ogólnopolska Konferencja Compliance & AML. Organizator: Stowarzyszenie Compliance Polska.	online
25.	23.04.2021	Spotkanie przedstawicieli UODO z przedstawicielami Ministerstwa Funduszy i Polityki Regionalnej dot. opublikowanej przez KE fiszki twiningowej KG 20 DCI OT 01 21 Support to Digitalisation Agenda in Kyrgyzstan.	online
26.	26.04.2021	Seminarium Naukowe pt. „Sztuczna inteligencja – w kontekście ochrony danych osobowych". Organizator: UODO	online
27.	28.04.2021	Webinarium „RODO w szkolnej ławce. Przetwarzanie danych biometrycznych", w ramach Programu TDTS. Organizator UODO.	online
28.	11.05.2021	Inauguracja 5. ed. Studium dla IOD organizowanej w Krajowej Szkole Administracji Publicznej im. Prezydenta RP Lecha Kaczyńskiego we współpracy z Urzędem Ochrony Danych Osobowych oraz wykłady przedstawicieli UODO w ramach tego Studium.	online
29.	24.05.2021	Wykład dla słuchaczy Studium dla IOD w Krajowej Szkole Administracji Publicznej im. Prezydenta RP Lecha Kaczyńskiego (KSAP). Organizatorzy: UODO, KSAP.	online
30.	25.05.2021	Konferencja pt. „RODO w sektorze medycznym – gdzie jesteśmy, dokąd zmierzamy – Edycja III". Organizator: Polska Federacja Szpitali.	online
31.	26.05.2021	Wykład dla słuchaczy Studium dla IOD w Krajowej Szkole Administracji Publicznej im. Prezydenta RP Lecha Kaczyńskiego (KSAP). Organizatorzy: UODO, KSAP.	online
32.	26.05.2021	Konferencja pracownicza PZU Zdrowie pt. „IODowisko". Organizator: PZU Zdrowie.	online
33.	27.05.2021	Spotkanie w ramach sieci współpracy placówek doskonalenia nauczycieli w XI edycji programu „Twoje dane – Twoja sprawa".	online
34.	28.05.2021	Webinarium „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków". Organizatorzy: UODO, Krajowy Rejestr Długów, ChronPESEL.pl.	online
35.	31.05.2021	Warsztaty dla Dyrektorów Generalnych Służby Cywilnej. Organizatorzy: Urząd Ochrony Danych Osobowych, Krajowa Szkoła Administracji Publicznej im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego, Służba Cywilna.	online
36.	8.06.2021	Konferencja „AI w zdrowiu". Polska Federacja Szpitali, Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu oraz Ambasada Brytyjska w Warszawie.	online
37.	8.06.2021	Uroczystość wręczenia nagród dla Szkoły Podstawowej Nr 9 im. Władysława Jagiełły w Kutnie, w ramach programu TDTS.	Kutno

		Organizatorzy: UODO, SP Nr 9 im. Władysława Jagiełły w Kutnie.	
38.	8–9.06.2021	Wykłady dla słuchaczy Studium dla IOD w Krajowej Szkole Administracji Publicznej im. Prezydenta RP Lecha Kaczyńskiego (KSAP). Organizatorzy: UODO, KSAP.	online
39.	8–9.06.2021	VIII Ogólnopolska Konferencja Samorządu i Oświaty EDUKACJA PRZYSZŁOŚCI. Organizatorzy: Redaktor Naczelny Pisma Samorządu Terytorialnego WSPÓLNOTA oraz Municipium S.A.	Lublin
40.	9.06.2021	Webinarium „Zgłoszenie naruszenia ochrony danych osobowych w praktyce". Organizator: UODO.	online
41.	10–11.06.2021	XIII Konferencja z cyklu „Bezpieczeństwo w Internecie", pt. „Globalne Gry. Global Games. Własność intelektualna, edukacja, bezpieczeństwo. Organizatorzy: UKSW, UODO, Urząd Patentowy, PTI, PIIiT, Naukowe Centrum Prawno-Informatyczne, Rada Sektorowa ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo.	online
42.	11.06.2021	Wręczenie wyróżnienia w Konkursie dla placówek oświatowych w ramach programu TDTS dla Szkoły Podstawowej Nr 360 w Warszawie.	Warszawa
43.	21.06.2021	Wykłady dla słuchaczy Studium dla IOD w Krajowej Szkole Administracji Publicznej im. Prezydenta RP Lecha Kaczyńskiego (KSAP). Organizatorzy: UODO, KSAP.	online
44.	21.06.2021	Warsztaty ONZ nt. wpływu pandemii na prawo do prywatności i ochrony danych.	online
45.	21.06.2021	Wręczenie nagrody za zajęcie I miejsca w Konkursie dla placówek oświatowych w ramach programu TDTS.	Lublin
46.	22.06.2021	Wręczenie III nagrody w Konkursie dla uczniów w ramach programu TDTS.	Warszawa
47.	23.06.2021	Wręczenie wyróżnienia w Konkursie dla placówek oświatowych dla SP nr 17 z Rzeszowa, w ramach programu TDTS.	Warszawa
48.	28.06.2021	Spotkanie przedstawicieli UODO z przedstawicielami Ministerstwa Funduszy i Polityki Regionalnej w sprawie oferty dot. projektu Support to Digitalisation Agenda in Kyrgyzstan.	online
49.	8.07.2021	Ceremonia wręczenia nagród w XI edycji Konkursu na esej dla studentów prawa i administracji.	Warszawa
50.	20.07.2021	Konferencja nt. sztucznej inteligencji „Regulation of the Artificial Intelligence – Ethical And Fundamental Rights Aspects". Organizator: Ministerstwo Sprawiedliwości Republiki Słowenii.	online
51.	21.07.2021	Spotkanie z przedstawicielami MFiPR oraz KPRM dot. projektu Support Digitalisation Agenda in Kyrgyzstan oraz Konferencji organizowanej przez Ministerstwo Sprawiedliwości Republiki Słowenii.	online
52.	30.07.2021	Spotkanie wewnętrzne „Wytyczne EROD 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO". Organizator: UODO.	online
53.	26.08.2021	Webinarium nt. internetowej platformy Konferencji w sprawie przyszłości Europy.	online
54.	7–9.09.2021	XXX Forum Ekonomiczne „Europa w poszukiwaniu przywództwa". Organizator: Fundacja Instytut Studiów Wschodnich.	Karpacz
55.	9.09.2021	Spotkanie przedstawicieli UODO z przedstawicielami Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie (OEIiZK) dot. współpracy w ramach programu TDTS.	online

56.	16.09.2021	Konferencja LegalFinTech2021 pt. „Wyzwania prawne w sektorze technologii finansowych". Organizatorzy: C.H.Beck oraz Stowarzyszenie Prawa Nowych Technologii – SPNT.	Warszawa
57.	20.09.2021	Seminarium naukowe pt. „Sztuczna inteligencja a prawa podstawowe". Organizator: Urząd Ochrony Danych Osobowych.	online
58.	20–24.09.2021	Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w Internecie". Organizatorzy: Polskie Centrum Programu Safer Internet (PCPSI) oraz ITU (Międzynarodowy Związek Telekomunikacyjny).	online
59.	30.09.2021	Uroczysta inauguracja roku akademickiego 2021/2022 na UKSW w Warszawie.	Warszawa
60.	4.10.2021	Inauguracja roku akademickiego 2021/2021 w Akademii Leona Koźmińskiego w Warszawie.	Warszawa
61.	5.10.2021	Szkolenie warsztatowe dla przedstawicieli pionów właściwych do ochrony danych osobowych z Komend Głównych: Policji, Straży Granicznej, Państwowej Straży Pożarnej oraz Służby Ochrony Państwa.	Warszawa
62.	6.10.2021	X Konwent Ochrony Danych i Informacji „RODO – naruszenia, decyzje, kary". Organizatorzy: FORSAFE Sp. z o.o. oraz Lubasz i Wspólnicy – Kancelaria Radców Prawnych Sp.k.	online
63.	7–9.10.2021	Szkolenie „Ochrona danych osobowych w podmiotach kościelnych: kontrola, kancelaria, odpowiedzi". Organizator: Konferencja Episkopatu Polski.	Zakopane
64.	9.10.2021	Inauguracja XII edycji Podyplomowego studium ochrony danych osobowych w ALK w Warszawie.	online
65.	12.10.2021	#RODO w edukacji. Konferencja inaugurująca XII edycję ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa". Organizator: UODO i Szkoła Podstawowa nr 9 im. Władysława Jagiełły w Kutnie.	Kutno
66.	12.10.2021	Konferencja Cyber24 Day. Organizator: Grupa Defence24.	Warszawa
67.	18.10.2021	Konferencja pt. „Jak sprostać wymaganiom współczesnej edukacji?". Organizator: Mazowiecki Kurator Oświaty w Warszawie.	online
68.	20.10.2021	Warsztaty online z IAB Polska – konsultacje dot. NOYB. Organizator: UODO.	online
69.	26.10.2021	VIII edycja Dnia Otwartego dla Służby Cywilnej.	Warszawa
70.	20.10.2021	Warsztaty z IAB dot. ochrony danych osobowych zawartych w banerach cookies. Organizator: UODO.	online
71.	21–22.10.2021	Szkolenie z zakresu ochrony danych osobowych dla Kancelarii Sejmu RP. Organizator: Kancelaria Sejmu RP.	online
72.	22.10.2021	Spotkanie w sprawie uregulowania skutków prawnych podpisu biometrycznego. Organizator: Polski Komitet Normalizacyjny.	online
73.	22.10.2021	I Spotkanie w Ministerstwie Sprawiedliwości dot. zmian w Kodeksie cywilnym w sprawie podpisów elektronicznych.	online
74.	26.10.2021	VIII ed. Dnia Otwartego dla Służby Cywilnej.	
75.	26.10.2021	Konferencja promująca „Kodeks branżowy Data Driven Marketing". Organizatorzy: Stowarzyszenie Marketingu Bezpośredniego oraz Wydział Zarządzania UW.	online
76.	27–28.10.2021	Szkolenie z zakresu ochrony danych osobowych dla uczestników XII edycji programu TDTS.	online
77.	3.11.2021	Konferencja „Tożsamość cyfrowa – bezpieczne finanse w Internecie" organizowana w ramach programy TDTS. Organizator: Dolnośląski Ośrodek Doskonalenia nauczycieli we Wrocławiu.	online
78.	4–5.11.2021	Szkolenie z zakresu ochrony danych osobowych dla Kancelarii Sejmu RP. Organizator: Kancelaria Sejmu RP.	online

79.	8.11.2021	2. Spotkanie w Ministerstwie Sprawiedliwości dot. zmian w Kodeksie cywilnym w sprawie podpisów elektronicznych.	online
80.	17.11.2021	VIII Krajowe Forum Ochrony Infrastruktury Krytycznej. Organizator: Rządowe Centrum Bezpieczeństwa (RCB).	online
81.	19.11.2021	Konferencja pt. „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online". Organizator: Safer Internet.	online
82.	23.11.2021	Webinarium dla uczniów w ramach programu TDTS „Klikam z głową – jak chronić swoje dane osobowe?". Organizatorzy: UODO i UKE.	online
83.	29.11.2021	Konferencja Naukowa „Nowe Technologie w przetwarzaniu danych medycznych". Organizator: UODO.	online
84.	6–10.12.2021	Szczyt Cyfrowy ONZ – IGF 2021.	Katowice
85.	7.12.2021	IV Krajowa Naukowo-Szkoleniowa Konferencja Biobanków Polskich. Organizatorzy: Krajowy Ośrodek Wiodący ds. Biobankowania oraz Konsorcjum BBMRI.pl.	online
86.	10.12.2021	Konferencja Pełnomocnika Rządu ds. Równego Traktowania dot. ochrony praw człowieka w sferze cyfrowej.	online
87.	10.12.2021	III Konferencja z cyklu „RODO w zakładzie pracy" pt. „Przetwarzanie danych osobowych pracowników dotyczących zdrowia a BHP". Organizator: Katedra Prawa Pracy i Polityki Społecznej WPiA Uniwersytetu Jagiellońskiego.	online/Kraków
88.	14.12.2021	Spotkanie z przedstawicielami Microsoft Corporation w sprawie projektu „EU Boundary" dot. ograniczenia przetwarzania w chmurze.	online
89.	15.12.2021	Wykład dla studentów Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego.	online
90.	15.12.2021	Wykład Prof. Davida Forte z Uniwersytetu w Cleveland, USA, nt. praw obywatelskich w USA.	Warszawa
91.	17.12.2021	3. Spotkanie w Ministerstwie Sprawiedliwości dot. zmian w Kodeksie cywilnym w sprawie podpisów elektronicznych.	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 2021 r.

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	6.01.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
2.	7.01.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
3.	7.01.2021	Posiedzenie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
4.	8.01.2021	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101) Europejskiej Rady Ochrony Danych.	online
5.	11.01.2021	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup FMES) Europejskiej Rady Ochrony Danych.	online
6.	12–13.01.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
7.	14.01.2021	44. Posiedzenie Plenarne Europejskiej Rady Ochrony Danych.	online
8.	15.01.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych	online
9.	18.01.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
10.	18–19.01.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
11.	19.01.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
12.	19.01.2021	Posiedzenie Grupy Zadaniowej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
13.	20.01.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
14.	20.01.2021	Posiedzenie Grupy Zadaniowej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
15.	20.01.2021	Konferencja „Human Rights in the Era of AI – Europe as International Standard Setter for Artificial Intelligence”.	online
16.	21.01.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE).	online
17.	26.01.2021	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
18.	26.01.2021	Wideokonferencja pt. „Kto jest suwerenny w naszym cyfrowym świecie?”, która otwierała Computers, Privacy and Data Protection – CPDP 2021. Organizatorzy: Brussels Privacy Hub, VUB-IES, UNU-CRIES i Microsoft.	online

19.	26.01.2021	Posiedzenie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
20.	27.01.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
21.	28.01.2021	Konferencja pt. „Transborder transfers. Challenges of international data transfer from the perspective of the Data Protection Convention 108+ and GDPR".	online
22.	29.01.2021	Posiedzenie Grupy Zadaniowej w sprawie badania prawnego Europejskiej Rady Ochrony Danych „Egzekwowanie obowiązków wynikających z RODO wobec podmiotów mających siedzibę poza EOG, podlegających art. 3 ust. 2 RODO".	online
23.	29.01.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. – Warsztaty dot. Wiążących Reguł Korporacyjnych	online
24.	29.01.2021	Spotkanie grupy projektowej wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
25.	2.02.2021	45. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
26.	2.02.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
27.	1–5.02.2021	Konferencja OECD „OECD International Conferences on AI in Work, Innovation, Productivity and Skills".	online
28.	3.02.2021	Spotkanie grupy projektowej wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
29.	4.02.2021	Spotkanie grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB w kontekście wyroku TSUE Schrems II (Taskforce 101).	online
30.	5.02.2021	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network) Europejskiej Rady Ochrony Danych.	online
31.	8.02.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
32.	9–10.02.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
33.	11.02.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych wraz z Koordynatorami Podgrup Ekspertów.	online
34.	12.02.2021	Spotkanie sprawozdawców wytycznych dot. administratora i podmiotu przetwarzającego Europejskiej Rady Ochrony Danych.	online
35.	15.02.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
36.	15.02.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
37.	16.02.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
38.	16–17.02.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online

39.	17.02.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement - ENF) Europejskiej Rady Ochrony Danych.	online
40.	18.02.2021	Wspólne Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
41.	19.02.2021	Spotkanie grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB w kontekście wyroku TSUE Schrems II (Taskforce 101).	online
42.	22.02.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
43.	23.02.2021	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM) Europejskiej Rady Ochrony Danych.	online
44.	23–25.02.2021	Konferencja Privacy Laws & Business „Poland's Data Protection Law: Trends, Risks & Opportunities".	online
45.	24.02.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
46.	24.02.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
47.	24.02.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. Warsztat dot. Wiążących Reguł Korporacyjnych.	online
48.	26.02.2021	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
49.	26.02.2021	Konferencja „The GDPR and International Organisations: Issues of EU Law and Public International Law".	online
50.	3.02.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
51.	2.03.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu.	online
52.	2.03.2021	Posiedzenie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
53.	2.03.2021	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
54.	3.03.2021	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory – SAESG) Europejskiej Rady Ochrony Danych – Revievof the Recommendations on Supplementary Measures.	online
55.	3.03.2021	Spotkanie sprawozdawców wytycznych dot. administratorów i podmiotu przetwarzającego.	online
56.	4.03.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
57.	4.03.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
58.	4–5.03.2021	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
59.	9.03.2021	46. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online

60.	10.03.2021	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
61.	11.03.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
62.	15–16.03.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
63.	18.03.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
64.	18.03.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
65.	19.03.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych – dot. Wiążących Reguł Korporacyjnych.	online
66.	22.03.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
67.	23.03.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
68.	23.03.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
69.	24.03.2021	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
70.	24.03.2021	Wspólne Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) i Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE).	online
71.	24–25.03.2021	52. Posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108 RE (Biura T-PD).	online
72.	24–26.03.2021	Konferencja ERA „Responding to Personal Data Breaches in the Post-GDPR era”.	online
73.	29.03.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. dot. Wiążących Reguł Korporacyjnych.	online
74.	30–31.03.2021	47. Posiedzenie plenarne ad hoc Europejskiej Rady Ochrony Danych.	online
75.	5–7.04.2021	Konferencja Privacy Symposium. 2021.	online
76.	7–8.04.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
77.	8.04.2021	Posiedzenie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
78.	8.04.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. dot. Wiążących Reguł Korporacyjnych.	online
79.	12.04.2021	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
80.	13.04.2021	48. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online

81.	14.04.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
82.	15.04.2021	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
83.	16.04.2021	Spotkanie sprawozdawców wytycznych dot. administratorów i podmiotu przetwarzającego Europejskiej Rady Ochrony Danych.	online
84.	19.04.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
85.	20.04.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
86.	21.04.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
87.	22.04.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych..	online
88.	23.04.2021	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network) Europejskiej Rady Ochrony Danych.	online
89.	23.04.2021	Spotkanie dot. Support to Digitalisation Agenda in Kyrgyzstan.	online
90.	26.04.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
91.	27–28.04.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
92.	28.04.2021	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB (Taskforce 101).	online
93.	29.04.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
94.	3.05.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE).	online
95.	4.05.2021	Posiedzenie grupy roboczej ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
96.	4.05.2021	Posiedzenie Podgrupy Ekspertów IT Users Europejskiej Rady Ochrony Danych.	online
97.	5.05.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
98.	5.05.2021	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
99.	6.05.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
100.	6.05.2021	Spotkanie grupy ds. audytów aplikacji mobilnych Europejskiej Rady Ochrony Danych.	online
101.	10.05.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
102.	11.05.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
103.	12.05.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online

104.	12.05.2021	Spotkanie sprawozdawców wytycznych dot. pojęć administratora i podmiotu przetwarzającego Europejskiej Rady Ochrony Danych.	online
105.	12.05.2021	Spotkanie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
106.	17.05.2021	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
107.	18.05.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
108.	18.05.2021	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101) Europejskiej Rady Ochrony Danych.	online
109.	19.05.2021	49. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
110.	20.05.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
111.	20.05.2021	Posiedzenie grupy roboczej Europejskiej Rady Ochrony Danych ds. środków uzupełniających (Taskforce Supplementary Measures – TFSuppM).	online
112.	21.05.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH; ESG certification session meeting) Europejskiej Rady Ochrony Danych.	online
113.	25.05.2021	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
114.	26.05.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. dot. Wiążących Reguł Korporacyjnych.	online
115.	28.05.2021	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB (Taskforce 101).	online
116.	28.05.2021	Spotkanie sprawozdawców wytycznych dot. pojęć administratora i podmiotu przetwarzającego Europejskiej Rady Ochrony Danych.	online
117.	31.05.2021	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee) Europejskiej Rady Ochrony Danych.	online
118.	31.05.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
119.	1.06.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
120.	1–2.06.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
121.	2.06.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
122.	2.06.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
123.	4.06.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
124.	7.06.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu do danych Europejskiej Rady Ochrony Danych.	online
125.	7.06.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online

126.	8.06.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
127.	8.06.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
128.	9.06.2021	Spotkanie ekspertów ds. audytu aplikacji mobilnych (Mobile App Audit Exchange Group) Europejskiej Rady Ochrony Danych.	online
129.	9.06.2021	Spotkanie Sieci Komunikacyjnej (Communications network) Europejskiej Rady Ochrony Danych	online
130.	9.06.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. Warsztat dot. Wiążących Reguł Korporacyjnych.	online
131.	10.06.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
132.	15.06.2021	Posiedzenie Rady Współpracy Europolu.	online
133.	16.06.2021	Posiedzenie GPA.	online
134.	16–17.06.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
135.	17.06.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
136.	17.06.2021	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB (Taskforce 101).	online
137.	17.06.2021	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac.	online
138.	17.06.2021	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym.	
139.	18.06.2021	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen II.	online
140.	18.06.2021	50. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
141.	21.06.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
142.	21.06.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. dot. Wiążących Reguł Korporacyjnych.	online
143.	21.06.2021	Wspólne posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup – IT Users) i Podgrupy ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
144.	21.06.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
145.	21–22.06.2021	OECD-GPA Online Workshop „One Year Later: Addressing the Data Governance and Privacy Implications of the COVID-19 pandemic and the Road to Recovery”.	online
146.	22.06.2021	Wspólne posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) oraz posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
147.	22.06.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online

148.	22.06.2021	Wspólne posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup – IT Users) i Podgrupy ekspertów ds. Współpracy (Cooperation Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
149.	23.06.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
150.	24.06.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
151.	24.06.2021	Wspólne posiedzenie Podgrupy Ekspertów BTLE i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS).	online
152.	25.06.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
153.	26.06.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
154.	28.06.2021	Spotkanie z konsorcjantami projektu twinningowego Support to Digitalisation Agenda in Kyrgyzstan.	online
155.	28–30.06.2021	41. posiedzenie plenarne Komitetu Konsultacyjnego Konwencji nr 108 RE.	online
156.	29–30.06.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
157.	30.06.2021	Spotkanie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
158.	30.06.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) i Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady ochrony Danych.	online
159.	1.07.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory – SAESG) Europejskiej Rady Ochrony Danych.	online
160.	1–2. 07.2021	Połączone spotkanie Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory – SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
161.	5.07.2021	Wspólne posiedzenie Grupy zadaniowej ds. 101 skarg złożonych przez NOYB oraz podgrupy ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
162.	5.07.2021	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg złożonych przez NOYB (Taskforce 101).	online
163.	5–6.07.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
164.	5–6.07.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
165.	6.07.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
166.	6.07.2021	Spotkanie w sprawie projektu Memerandum of Understanding pomiędzy Rządem RP a Rządem Stanów Zjednoczonych Ameryki.	online
167.	7.07.2021	51. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
168.	8.07.2021	Wspólne posiedzenie podgrup: Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert	online

		Subgroup SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych dot. Art. 66.	
169.	9.07.2021	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
170.	9.07.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
171.	9.07.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych	online
172.	9.07.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. dot. Wiążących Reguł Korporacyjnych.	online
173.	12.07.2021	52. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
174.	13.07.2021	Wspólne posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych dot. Wiążących Reguł Korporacyjnych.	online
175.	13.07.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
176.	14.07.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
177.	15.07.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
178.	15.07.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
179.	19.07.2021	Spotkanie Grupy zadaniowej ds. 101 skarg złożonych przez NOYB (Taskforce 101) Europejskiej Rady Ochrony Danych.	online
180.	20.07.2021	Konferencja „Regulation of the Artificial Intelligence – Ethical and Fundamental Rights Aspects". Organizator: Stałe Przedstawicielstwo Słowacji w związku z prezydencją w UE.	online
181.	20.07.2021	Wspólne posiedzenie Grupy zadaniowej ds. 101 skarg złożonych przez NOYB (Taskforce 101) i Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
182.	20.07.2021	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert SUbgroup – FMES) Europejskiej Rady Ochrony Danych.	online
183.	28.07.2021	53. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
184.	29.07.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory – SAESG) Europejskiej Rady Ochrony Danych	online
185.	23.08.2021	Sesja dialogowa UN GCNPxDZP: Obowiązek ochrony danych osobowych.	online
186.	1.09.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online

187.	2.09.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
188.	2–3.09.2021	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup –TECH) Europejskiej Rady Ochrony Danych.	online
189.	7–8.09.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
190.	8.09.2021	Posiedzenie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
191.	8.09.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. Warsztat dot. Wiążących Reguł Korporacyjnych.	online
192.	9.09.2021	Konferencja „Child's Rights, Age Verification and Parental Consent: Finding the balance".	online
193.	14.09.2021	54. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
194.	16.09.2021	Posiedzenie Podgrupy ds. Finansowych (Financial Matters – FMES) Europejskiej Rady Ochrony Danych.	online
195.	17.09.2021	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
196.	20.09.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych. Warsztat dot. Wiążących Reguł Korporacyjnych.	online
197.	21.09.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
198.	22.09.2021	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
199.	22.09.2021	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subroup) Europejskiej Rady Ochrony Danych.	online
200.	23.09.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
201.	23.09.2021	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych.ds. 101 skarg NOYB (Taskforce 101).	online
202.	24.09.2021	55. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
203.	27–28.09.2021	Konferencja Bitkom's Privacy 2021	online
204.	28.09.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
205.	28.09.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
206.	28.09.2021	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
207.	28–30.09.2021	53. Posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy.	online
208.	29.09.2021	Spotkanie Sieć Inspektorów Ochrony Danych (DPO Network) Europejskiej Rady Ochrony Danych.	online
209.	30.09.2021	Spotkanie punktów kontaktowych EROD w sprawie udostępniania dokumentów.	online
210.	30.09–1.10.2021	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online

211.	4.10.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu do danych osobowych Europejskiej Rady Ochrony Danych.	online
212.	5.10.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych i Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
213.	5–6.10.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
214.	6.10.2021	Spotkanie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
215.	6.10.2021	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
216.	12.10.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
217.	13.10.2021	56. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
218.	14.10.2021	Spotkanie sprawozdawców wytycznych dotyczących prawa dostępu Europejskiej Rady Ochrony Danych.	online
219.	14.10.2021	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych.ds. 101 skarg NOYB (Taskforce 101).	online
220.	18–19.10.2021	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
221.	18–21.10.2021	43. Międzynarodowa Konferencja Global Privacy Assembly (GPA).	online
222.	20.10.2021	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
223.	8.11.2021	Spotkanie organów nadzorczych w sprawie Vinted.	online
224.	10.11.2021	Spotkanie Sieci Komunikacyjnej (Communications Network) Europejskiej Rady Ochrony Danych.	online
225.	11–12.11.2021	Spotkanie sprawozdawców wytycznych dotyczących prawa dostępu Europejskiej Rady Ochrony Danych.	online
226.	16.11.2021	Konferencja „Personal Data – Future Perspective!”. Organizator: łotewski organ nadzorczy.	online
227.	16–17.11.2021	Europejskie Warsztaty Rozpatrywania Skarg. Organizator: organ nadzorczy Gibraltaru.	online
228.	17–19.11.2021	42. Posiedzenie plenarne Komitetu Konsultacyjnego Konwencji nr 108 RE (T-PD).	online
229.	18.11.2021	57. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	Bruksela
230.	19.11.2021	Spotkanie ekspertów ds. audytu aplikacji mobilnych (Mobile App Audit Exchange Group) Europejskiej Rady Ochrony Danych.	online
231.	29.11.2021	Posiedzenie Grupy Zadaniowej ds. Banerów Cookie (Cookie Banner Taskforce – BannerTF).	online
232.	29.11.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
233.	30.12.2021	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
234.	30.11.2021	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
235.	1.12.2021	Posiedzenie Rady Współpracy Europolu.	online

236.	1.12.2021	Posiedzenie Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee – CSC).	online
237.	1.12.2021	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
238.	2.12.2021	Grupa zadaniowa ds. obliczania kar administracyjnych (Taskforce on the Calculation of Administrative Fines – FINES)	online
239.	6.12.2021	Spotkanie sieci Inspektorów Ochrony Danych (DPO Network).	online
240.	6–8.12.2021	16th Annual Meeting of the Internet Governance Forum (IGF) – GF2021.	online
241.	13.12.2021	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
242.	14.12.2021	58. Posiedzenie plenarne Europejskiej Rady Ochrony Danych.	online
243.	15.12.2021	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
244.	16–17.12.2021	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
245.	16–17.12.2021	Spotkanie Grupy Państw Europy Środkowej i Wschodniej z okazji 20-lecia CEEDPA.	online
246.	17.12.2021	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
247.	17.12.2021	Spotkanie organów nadzorczych dot. Vinted.	online
248.	17.12.2021	Posiedzenie Podgrupy ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
249.	20–21.12.2021	Posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy (Biura T-PD).	online
250.	21.12.2021	Spotkanie sprawozdawców wytycznych dot. prawa dostępu Europejskiej Rady Ochrony Danych.	online
251.	21.12.2021	Posiedzenie Zespołu ds. postępowań przed Europejskim Trybunałem Praw Człowieka.	online

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
www.uodo.gov.pl