SPRAWOZDANIE Z DZIAŁALNOŚCI
PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
w ROKU 2023

Sprawozdanie stanowi wykonanie art. 59 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 10 maja 2018 r. o ochronie danych osobowych[1].

[1] Sprawozdanie obejmuje działalność Prezesa Urzędu Ochrony Danych Osobowych od 1 stycznia 2023 r. do 31 grudnia 2023 r.

Zgodnie z art. 59 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 środków podjętych zgodnie z art. 58 ust. 2 RODO. 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[3]. Powołany przepis jest uzupełniony przez art. 50 ustawy z 10 maja 2018 r. o ochronie danych osobowych[4], w myśl którego Prezes Urzędu Ochrony Danych Osobowych[5] 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 informacje o liczbie i rodzaju prawomocnych orzeczeń sądowych uwzględniających skargi na decyzje lub postanowienia Prezesa UODO oraz wnioski ze stanu przestrzegania przepisów o ochronie danych osobowych (art. 50 ust. 1 ustawy o ochronie danych osobowych). Prezes UODO udostępnia sprawozdanie na swojej stronie podmiotowej Biuletynu Informacji Publicznej (art. 50 ust. 2 ustawy o ochronie danych osobowych).

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r. str. 1 ze zm.), dalej: „RODO" lub „ogólne rozporządzenie o ochronie danych".
[3] Dalej także: „EROD".
[4] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), dalej: „ustawa o ochronie danych osobowych".
[5] Dalej także: „Prezes UODO".

Spis treści

I. WPROWADZENIE ... 6

1. ŹRÓDŁA PRAWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH ... 6
2. URZĄD OCHRONY DANYCH OSOBOWYCH ... 9
2.1. Struktura organizacyjna ... 10
2.2. Pracownicy UODO ... 11
2.3. Zadania jednostek organizacyjnych UODO ... 12
2.4. Budżet UODO za 2023 r. ... 13

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI ... 14

1. WYDAWANIE DECYZJI ADMINISTRACYJNYCH I ROZPATRYWANIE SKARG ... 14
1.1. Skargi ... 15
1.1.1. Sektor publiczny ... 20
1.1.2. Sektor prywatny ... 35
1.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa ... 44
1.1.4. Sektor finansów, telekomunikacji i ubezpieczeń ... 64
1.1.5. Postępowania transgraniczne ... 74
2. KONTROLA PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH ... 78
2.1. Aplikacje mobilne ... 79
2.2. Aplikacje internetowe (webowe) ... 83
2.3. System Informacyjny Schengen, Wizowy System Informacyjny ... 83
2.4. Sprawdzenia dotyczące prewencyjnych wpisów małoletnich do SIS ... 83
2.5. Kontrole w wyniku zgłoszonego naruszenia ... 85
2.6. Kontrole w wyniku otrzymania informacji o nieprawidłowościach ... 86
2.7. Decyzje administracyjne w postępowaniach kontrolnych ... 88
2.8. Wyroki WSA w Warszawie i NSA dotyczące decyzji Prezesa UODO w sprawie kontroli ... 90
3. EGZEKUCJA ADMINISTRACYJNA – ZAPEWNIENIE WYKONANIA DECYZJI ... 91
4. ADMINISTRACYJNE KARY PIENIĘŻNE ... 96
5. OPINIOWANIE PROJEKTÓW AKTÓW PRAWNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH ... 102
5.1. Ocena skutków dla ochrony danych osobowych na etapie legislacji ... 104
5.2. Hierarchia aktów prawnych – zasada praworządności ... 109
5.3. Precyzyjne określenie ról podmiotów w procesie przetwarzania danych ... 113
5.4. Systemy teleinformatyczne. Łączenie baz danych ... 116
5.5. Korzystanie z nowych technologii przy przetwarzaniu danych osobowych ... 119
5.6. Zakres pozyskiwanych danych osobowych ... 121
5.7. Projekty aktów prawnych tworzonych na poziomie Unii Europejskiej ... 126
5.8. Podsumowanie ... 127
6. ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ... 129
6.1. Statystyka zgłaszanych naruszeń ochrony danych osobowych ... 130
6.2. Wyjaśnienia ... 134
6.3. Postępowania administracyjne ... 135
6.4. Decyzje administracyjne ... 136
6.5. Administracyjne kary pieniężne w związku z naruszeniem ... 136
7. ORZECZNICTWO SĄDÓW ADMINISTRACYJNYCH W SPRAWACH DECYZJI LUB POSTANOWIEŃ ORGANU NADZORCZEGO ... 146
8. UPRZEDNIE KONSULTACJE ... 155
9. KODEKSY POSTĘPOWANIA ... 157
10. AKREDYTACJA PODMIOTÓW MONITORUJĄCYCH KODEKSY POSTĘPOWANIA ... 159
11. CERTYFIKACJA ... 160
12. PYTANIA DOTYCZĄCE WYKŁADNI PRAWA, WNIOSKI O DOSTĘP DO INFORMACJI I WYSTĄPIENIA PREZESA UODO ... 161
12.1. Pytania dotyczące wykładni prawa ... 161
12.1.1. Pytania od administratorów i osób fizycznych ... 163
12.1.2. Pytania od inspektorów ochrony danych ... 184
12.1.3. Zapytania innych organów nadzorczych ... 201
12.2. Wnioski o dostęp do informacji publicznej ... 204
12.3. Skargi na działanie UODO ... 206
12.4. Wystąpienia ... 207

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA 211

1. DZIAŁALNOŚĆ EDUKACYJNA 211
1.1. Szkolenia zewnętrzne 212
1.2. Projekty i programy 212
1.2.1. Ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa" 212
1.2.2. Letnia Akademia Liderów RODO 217
1.3. Program wymiany pracowników 218
1.4. Porozumienia o współpracy 219
1.5. Publikacje 220
1.6. Współpraca krajowa przy Polskim Komitecie Normalizacyjnym (PKN) 221
1.7. Nagroda im. Michała Serzyckiego 221
1.8. Konferencje, seminaria, spotkania 221
2. DZIAŁALNOŚĆ INFORMACYJNA 226
2.1. Strona internetowa i media społecznościowe 227
2.2. Współpraca z mediami 231
2.3. Odpowiedzi na indywidualne pytania dziennikarzy 234
2.4. „Newsletter UODO dla IOD" / „Biuletyn UODO" 235
2.5. Infolinia UODO 236
2.6. Inne 237

IV. UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ ZAGADNIENIAMI OCHRONY DANYCH OSOBOWYCH 240

1. WSPÓŁPRACA W RAMACH EROD 240
1.1. Wytyczne i zalecenia 241
1.2. Konsultacje prawodawcze i dokumenty skierowane do instytucji UE lub organów krajowych 242
1.3. Inne wskazówki i oświadczenia 242
1.4. Opinie dotyczące spójności 242
1.5. Wiążące decyzje 244
1.6 Udział UODO w pracach EROD 249
2. WSPÓŁPRACA W RAMACH IMI 250
3. SIEĆ INSPEKTORÓW OCHRONY DANYCH 253
4. NADZÓR NAD WIELKOSKALOWYMI SYSTEMAMI 253
5. WNIOSKI PREJUDYCJALNE 255
6. PRZEKAZYWANIE DANYCH OSOBOWYCH POZA EOG 262
7. INNE SPRAWY 264
8. WIZYTA STUDYJNA 266
9. MIĘDZYNARODOWE KONFERENCJE, SEMINARIA I SPOTKANIA 266

V. CHARAKTERYSTYKA DZIAŁALNOŚCI UODO I WYZWANIA NA PRZYSZŁOŚĆ 269

ZAŁĄCZNIK NR 1 282

WYKAZ ADMINISTRACYJNYCH KAR PIENIĘŻNYCH NAŁOŻONYCH PRZEZ PREZESA UODO W 2023 R. 282

ZAŁĄCZNIK NR 2 284

WYKAZ WYDARZEŃ OBJĘTYCH PATRONATEM PREZESA UODO W 2023 R. 284

ZAŁĄCZNIK NR 3 285

WYKAZ KONFERENCJI, SEMINARIÓW, SPOTKAŃ I INNYCH WYDARZEŃ KRAJOWYCH I MIĘDZYNARODOWYCH Z UDZIAŁEM PREZESA UODO LUB JEGO PRZEDSTAWICIELI, ZORGANIZOWANYCH W 2023 R. W POLSCE PRZEZ UODO LUB INNE PODMIOTY 285

ZAŁĄCZNIK NR 4 290

WYKAZ WYDARZEŃ MIĘDZYNARODOWYCH I EUROPEJSKICH, W TYM POSIEDZEŃ PLENARNYCH EROD I PODGRUP, Z UDZIAŁEM PREZESA UODO LUB JEGO PRZEDSTAWICIELI, KTÓRE ODBYŁY SIĘ W 2023 R. 290

ZAŁĄCZNIK NR 5 300

DZIAŁALNOŚĆ URZĘDU OCHRONY DANYCH OSOBOWYCH W 2023 ROKU W LICZBACH 300

Szanowni Państwo,

wykonując obowiązek nałożony przez przepisy ustawy o ochronie danych osobowych, przedkładam Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2023. Na mocy art. 59 ogólnego rozporządzenia o ochronie danych sprawozdanie jest także udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

W sprawozdaniu przedstawione są wyniki prac organu nadzorczego w okresie, kiedy urząd ten sprawował mój poprzednik – Jan Nowak, pełniący funkcję Prezesa Urzędu Ochrony Danych Osobowych do dnia 25 stycznia 2024 r.

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 osób, których dane zostały naruszone. Ważnym zadaniem jest również działalność edukacyjno-informacyjna oraz uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

W 2023 r. minął piąty rok bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych w Polsce. Na tej podstawie można już dokonać podsumowania, jak w świetle prawa o ochronie danych podmioty różnych sektorów poradziły sobie z obsługą procesów przetwarzania danych osobowych w swoich organizacjach oraz zastanowić się nad funkcjonowaniem Urzędu Ochrony Danych Osobowych – jak jego obecna struktura organizacyjna sprawdziła się w praktyce pod kątem wymagań, jakie stawia RODO.

Zapraszam do lektury sprawozdania z działalności polskiego organu ochrony danych osobowych w roku 2023, które jest nie tylko informacją o działalności polskiego organu nadzorczego, ale również przedstawia proces analizy prawnej leżącej u podstaw podejmowania decyzji służących zwiększeniu poziomu bezpieczeństwa danych osobowych obywateli.

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

I. WPROWADZENIE

Każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo to zostało zagwarantowane w art. 51 w zw. z art. 47 Konstytucji RP, art. 8 Karty praw podstawowych Unii Europejskiej[6], a także w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej[7]. Szczegółowe normy służące realizacji tego prawa wprowadza przede wszystkim RODO, określając zasady przetwarzania danych, związane z tym obowiązki administratorów oraz prawa osób, których dane dotyczą.

1. Źródła prawa w zakresie ochrony danych osobowych

Podstawę prawną działania Prezesa UODO stanowią przede wszystkim:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- ustawa z 10 maja 2018 r. o ochronie danych osobowych oraz wydane na jej podstawie akty wykonawcze;
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 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[8];
- ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[9] oraz wydane na jej podstawie akty wykonawcze.

Na mocy art. 57 RODO Prezes UODO:

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 rozumienie 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;

[6] Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 202 z 2016 r. str. 389), dalej: „KPP”.
[7] Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 202 z 2016 r. str. 1), dalej: „TFUE”.
[8] Dz. Urz. UE L 119 z 04.05.2016, s. 89. Dalej: „dyrektywa 2016/680" lub „dyrektywa policyjna".
[9] Dz. U. z 2023 r. poz. 1206.

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;
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 RODO;
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 RODO oraz podmiotów certyfikujących na mocy art. 43 RODO;
17) akredytuje podmiot monitorujący kodeksy postępowania zgodnie z art. 41 oraz podmiot certyfikujący na mocy art. 43 RODO;
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 RODO 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 RODO):

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 bądź usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 RODO 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 RODO):

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 na podstawie art. 43 RODO;
6) udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5 RODO;
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.

Z chwilą rozpoczęcia stosowania od 25 maja 2018 r. RODO i ustawy z 10 maja 2018 r. o ochronie danych osobowych, 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 minimalizujących zidentyfikowane ryzyka. Analiza spraw, którymi Prezes UODO zajmował się w okresie analizowanego roku 2023, w tym w szczególności zgłaszanych skarg i pytań prawnych oraz naruszeń, pozwoliła na zidentyfikowanie problemów związanych ze stosowaniem RODO, które najczęściej pojawiały się zarówno po stronie podmiotów danych, jak i administratorów.

2. Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych zapewnia wykonanie zadań wynikających z kompetencji Prezesa UODO określonych w RODO i w ustawie z 10 maja 2018 r. o ochronie danych osobowych, a także w innych przepisach powszechnie obowiązującego prawa.

Na mocy art. 34 ust. 1 ustawy, Prezes UODO jest organem właściwym w sprawie ochrony danych osobowych. Zgodnie z art. 34 ust. 2 ww. ustawy, Prezes UODO jest organem nadzorczym w rozumieniu:

- RODO;
- dyrektywy 2016/680;
- rozporządzenia 2016/794[10].

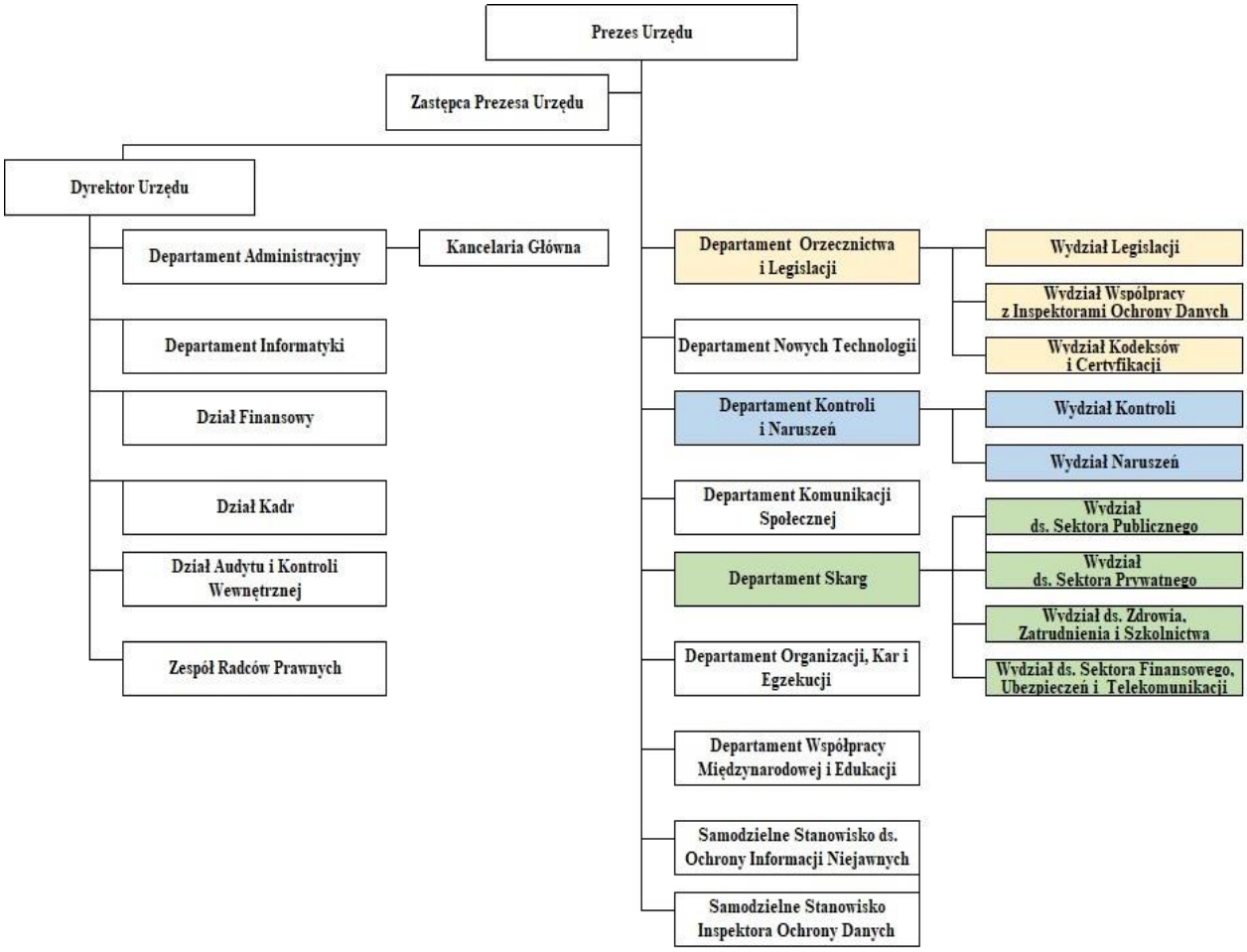
W skład UODO wchodzą następujące komórki organizacyjne: Departament Orzecznictwa i Legislacji (DOL), Departament Współpracy Międzynarodowej i Edukacji (DWME), Departament Kontroli i Naruszeń (DKN), Departament Komunikacji Społecznej (DKS), Departament Skarg (DS), Departament Organizacji, Kar i Egzekucji (DOKE), Departament Informatyki (DIF), Departament Nowych Technologii (DNT), Departament Administracyjny (DA), Dział Finansowy, Dział Audytu i Kontroli Wewnętrznej, Dział Kadr, Zespół Radców Prawnych, Samodzielne Stanowisko Inspektora Ochrony Danych oraz Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych.

W trzech departamentach wyodrębnione zostały wydziały, które zajmują się sprawami z określonych sektorów. 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 znajduje się Wydział Kontroli i Wydział Naruszeń, zaś 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.

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, zmieniony zarządzeniem nr 19/2023 Prezesa Urzędu Ochrony Danych Osobowych z 25 lipca 2023 r. w sprawie zmiany oraz wprowadzenia tekstu jednolitego statutu Urzędu Ochrony Danych Osobowych. Strukturę organizacyjną Urzędu Ochrony Danych Osobowych przedstawia poniższy rysunek.

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. Urz. UE L. z 2016 r. Nr 135, str. 53 ze zm.), dalej: „rozporządzenie 2016/794".



2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2023 r. (nie wliczając Prezesa UODO i jego Zastępcy) wynosił 262,20 etatu (tj. 267 osób)[11]. Natomiast zatrudnienie w UODO na dzień 31 grudnia 2023 r. wynosiło 265,25 etatu (tj. 271 osób). Na koniec 2023 r. na stanowiskach merytorycznych zatrudnionych było 238 osób, a na stanowiskach pomocniczych 33 osoby. Wyższe wykształcenie ogółem posiadało 240 pracowników, w tym 147 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2023 r. (bez Prezesa UODO i jego Zastępcy) przedstawiała się następująco:

1) Dyrektor Urzędu – 1 osoba;
2) Departament Orzecznictwa i Legislacji – 30 osób (30,0 etatów), w tym:
   - Wydział Legislacji – 9 osób (9,0 etatów),
   - Wydział Współpracy z Inspektorami Ochrony Danych – 4 osoby (4,0 etaty),
   - Wydział Kodeksów i Certyfikacji – 4 osoby (4,0 etaty);
3) Departament Współpracy Międzynarodowej i Edukacji – 14 osób (14,00 etatów);

[11] Dane zawarte w tym podpunkcie zostały ustalone zgodnie ze sposobem liczenia zatrudnienia w „Sprawozdaniu RB-70 o zatrudnieniu i wynagrodzeniach", Rozporządzenie Ministra Finansów z 11 stycznia 2022 r. w sprawie sprawozdawczości budżetowej (Dz. U. poz. 144 ze zm.).

4) Departament Kontroli i Naruszeń – 47 osób (47,0 etatów), w tym:
   - Wydział Kontroli – 14 osób (14,0 etatów),
   - Wydział Naruszeń – 25 osób (25,0 etatów);
5) Departament Komunikacji Społecznej – 17 osób (16,55 etatu);
6) Departament Skarg – 88 osób (86,15 etatu), w tym:
   - Wydział ds. Sektora Publicznego – 17 osób (17,0 etatów),
   - Wydział ds. Sektora Prywatnego – 20 osób (20,0 etatów),
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 16 osób (15,1 etatów),
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 20 osób (20,0 etatów);
7) Departament Organizacji, Kar i Egzekucji – 16 osób (16,0 etatów);
8) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,33 etatu);
9) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba (1,0 etat);
10) Departament Administracyjny – 26 osób (24,5 etatu);
11) Departament Informatyki – 10 osób (9,42 etatu);
12) Departament Nowych Technologii – 5 osób (5,0 etatów);
13) Dział Finansowy – 5 osób (5,0 etatów);
14) Dział Kadr – 4 osoby (4,0 etaty);
15) Dział Audytu i Kontroli Wewnętrznej – 1 osoba (0,5 etatu);
16) Zespół Radców Prawnych – 3 osoby (3,0 etaty);
17) Radca – 1 osoba (0,8 etatu).

2.3. Zadania jednostek organizacyjnych UODO

Do zadań jednostek organizacyjnych Urzędu Ochrony Danych Osobowych należy w szczególności: rozpatrywanie skarg w sprawach wykonania przepisów RODO 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 RODO przez branże różnych sektorów.

Urząd Ochrony Danych Osobowych prowadzi działania kontrolne na podstawie przygotowanych wcześniej planów kontroli. Czynności kontrolne podsumowywane są w odpowiednich protokołach oraz pismach dokumentujących poszczególne czynności kontrolne. W razie stwierdzenia uchybień prowadzone są postępowania administracyjne.

W przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych nakładane są 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 polegają m.in. na przyjmowaniu zawiadomień o wyznaczeniu inspektora ochrony danych (IOD), udzielaniu odpowiedzi na pytania od inspektorów ochrony danych, administratorów i podmiotów przetwarzających, przygotowaniu wystąpień w sprawach dotyczących statusu i zadań inspektorów ochrony danych oraz na podejmowaniu działań informacyjno-edukacyjnych budujących świadomość prawną w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych. Ważnym zadaniem jest także przyjmowanie wniosków o uprzednie konsultacje, zgłoszeń naruszeń ochrony danych osobowych oraz podejmowanie czynności wobec administratorów i podmiotów przetwarzających w celu powiadomienia o naruszeniu ochrony danych osób, których dane dotyczą.

Przepis 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.

2.4. Budżet UODO za 2023 r.

Budżet UODO ustalony w ustawie budżetowej na 2023 r. (plan po zmianach), przedstawiał się następująco:

- wynagrodzenia 28 618 tys. zł
- pochodne od wynagrodzeń 6 086 tys. zł
- wydatki majątkowe 1 460 tys. zł
- pozostałe wydatki 9 203 tys. zł

Wydatki zrealizowane przez UODO w 2023 r. objęły:

- wynagrodzenia 28 600 tys. zł
- pochodne od wynagrodzeń 5 408 tys. zł
- wydatki majątkowe 1 452 tys. zł
- pozostałe wydatki 8 997 tys. zł

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI

1. 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 K.p.a. 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.

W okresie od 1 stycznia 2023 r. do 31 grudnia 2023 r. w sprawach dotyczących skarg obywateli wydanych zostało **1796 decyzji.** W decyzjach tych Prezes UODO w **965** przypadkach, w oparciu o art. 58 RODO, zastosował środki naprawcze, w tym:

- w 630 sprawach udzielił upomnienia za naruszenie przepisów RODO, zaś
- w 335 przypadkach zastosował środek naprawczy w postaci nakazu.

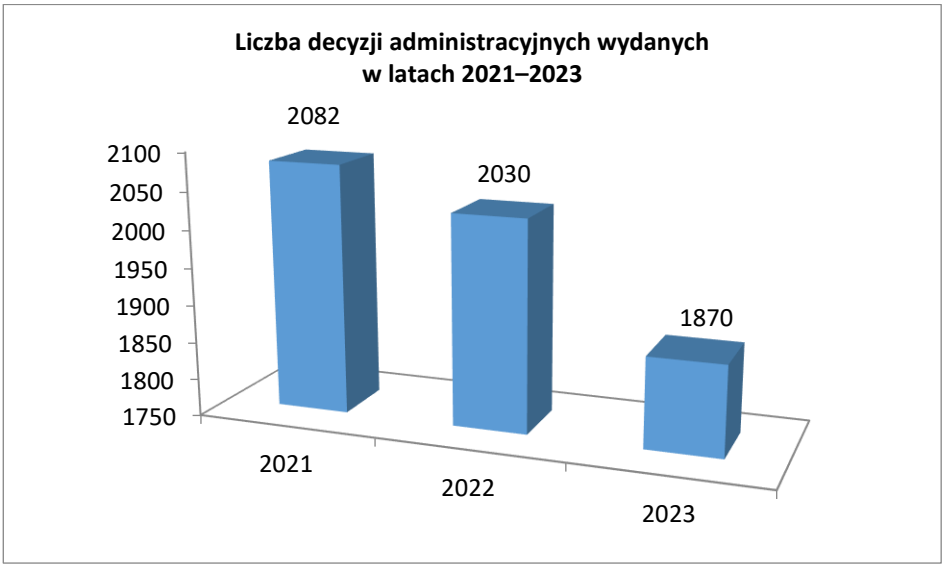
Liczba zastosowanych przez organ nadzorczy środków naprawczych w sprawach skargowych utrzymała się na zbliżonym poziomie w stosunku do roku 2022, w którym Prezes UODO zastosował środki naprawcze w 974 sprawach, w tym w 637 sprawach udzielił upomnienia, zaś w 337 przypadkach zastosował środek naprawczy w postaci nakazu.

W omawianym roku 2023 zaobserwowano natomiast wzrost liczby skarg na decyzje Prezesa UODO, składanych do sądów administracyjnych. Do Wojewódzkiego Sądu Administracyjnego w Warszawie w analizowanym roku 2023 zostały zaskarżone **223** decyzje Prezesa UODO, zaś do Naczelnego Sądu Administracyjnego wniesiono **66** skarg kasacyjnych od wyroków w sprawach dotyczących decyzji wydanych przez Prezesa UODO, podczas gdy w roku 2022 było to odpowiednio 177 i 55 skarg[12].

W roku 2023 Prezes UODO wydał ogółem **1870 decyzji administracyjnych,** na które złożyło się:

- 1796 decyzji w sprawach skargowych (1750 DS, 43 DKN, 3 DOL);
- 30 decyzji w sprawach nałożenia administracyjnych kar pieniężnych;
- 36 decyzji dotyczących naruszeń;
- 4 decyzje dotyczące kontroli;
- 3 decyzje dotyczące kodeksu postępowania;
- 1 decyzja dotycząca akredytacji podmiotu monitorującego kodeks.

[12] Zob. rozdział II pkt 7: „Orzecznictwo sądów administracyjnych w sprawach decyzji lub postanowień organu nadzorczego”.



Wykres 1: Liczba decyzji administracyjnych wydanych przez Prezesa UODO w latach 2021–2023.

1.1. Skargi

Rozpatrywanie skarg, zgodnie z art. 57 ust. 1 lit. f) ogólnego rozporządzenia o ochronie danych, jest jednym z głównych zadań Prezesa Urzędu Ochrony Danych Osobowych jako organu nadzorczego. Wpływ skargi do organu nadzorczego inicjuje postępowanie administracyjne, zmierzające do rozstrzygnięcia sprawy poprzez wydanie decyzji administracyjnej.

Każda ze skarg analizowana jest na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami ustawy z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[13]. W sytuacji gdy skarga nie spełnia warunków wymaganych przez ww. przepisy prawa, organ właściwy do spraw ochrony danych osobowych wzywa wnioskodawcę do uzupełnienia braków formalnych. W sprawach, w których nie uzupełniono braków formalnych, skargi pozostawiane są bez rozpoznania.

Podobnie jak w latach ubiegłych, w 2023 r. jednym z najczęstszych powodów kierowania do strony wezwania do uzupełnienia braków formalnych skargi było niewskazanie lub nieprecyzyjne wskazanie żądania, z jakim skarżący zwracali się do Prezesa Urzędu Ochrony Danych Osobowych lub też niewskazanie podmiotu, którego dotyczyła skarga. W przypadku wniesienia skargi spełniającej warunki formalne organ w pierwszej kolejności wzywał skarżony podmiot o złożenie wyjaśnień oraz przedłożenie dowodów na ich poparcie i odniesienie się do zarzutów podniesionych w skardze, informując jednocześnie strony o wszczęciu postępowania administracyjnego.

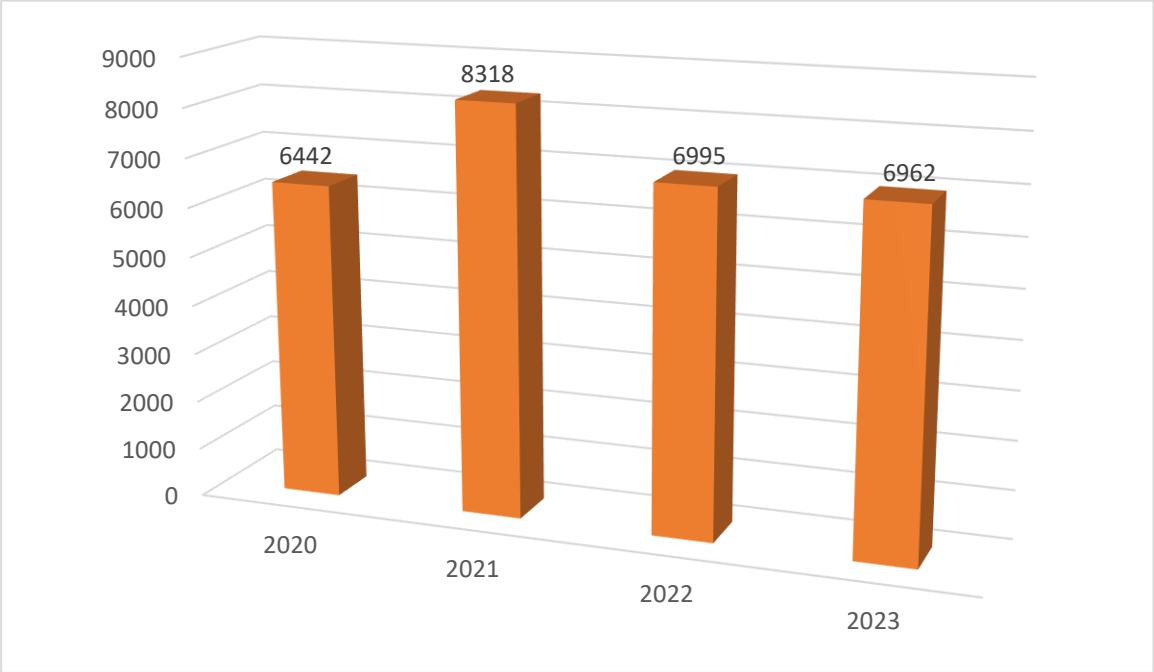
Każdej osobie, która złożyła skargę na naruszenie przepisów RODO w procesie przetwarzania jej danych osobowych, przysługuje prawo do informacji o postępach i wynikach rozpatrzenia skargi, dlatego podejmując szereg czynności koniecznych do zebrania materiału dowodowego, niezbędnego do wydania rozstrzygnięcia, organ nadzorczy informuje o postępach i wynikach rozpatrzenia skargi.

W analizowanym okresie sprawozdawczym Prezes Urzędu Ochrony Danych Osobowych prowadził postępowania administracyjne, wszczęte w wyniku skarg wniesionych w roku 2023, jak i w latach poprzednich, które toczyły się zgodnie z przepisami

[13] Dz. U. z 2024 r. poz. 572, dalej jako K.p.a.

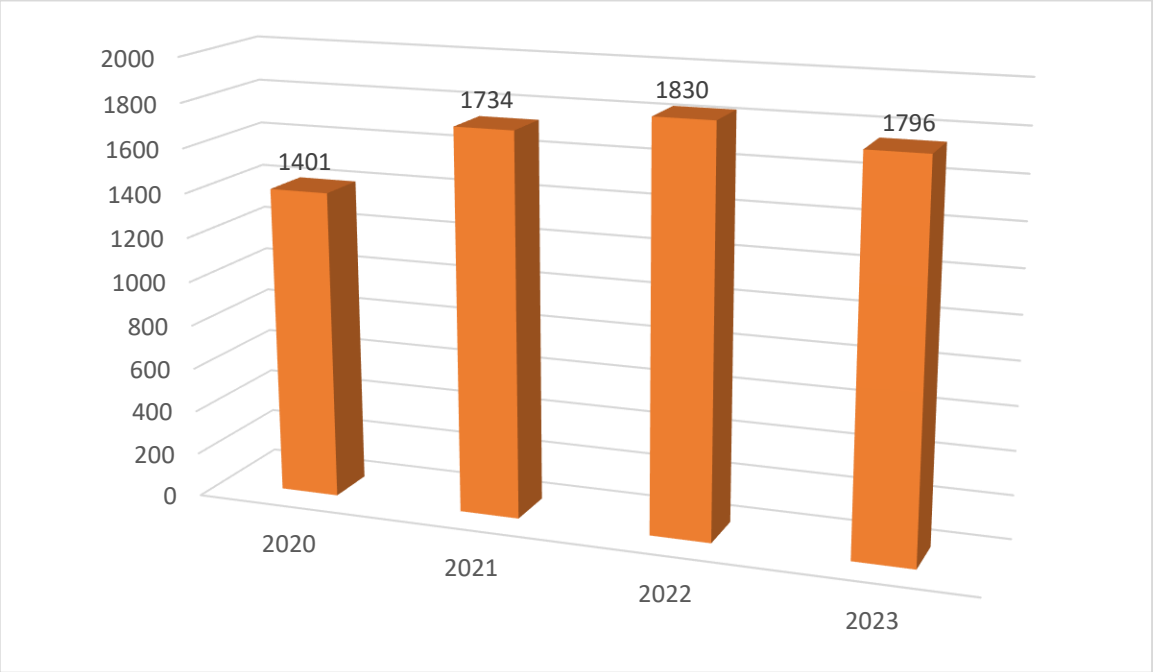
ustawy o ochronie danych osobowych oraz na podstawie przepisów K.p.a., zgodnie z art. 7 ust. 1 ww. ustawy.

W roku 2023 do Urzędu Ochrony Danych Osobowych wpłynęły **6962 skargi krajowe,** a zatem o 33 skarg mniej niż w roku poprzednim (6995 skarg). Znaczny wzrost liczby wpływających skarg w latach poprzednich i utrzymywanie się tego wysokiego wskaźnika przez kolejne lata, przełożyło się na zwiększoną liczbę spraw prowadzonych w Urzędzie w analizowanym 2023 r. Sprawy te pozostawały w toku i konieczne było podjęcie czynności niezbędnych do zebrania materiału dowodowego oraz wydania decyzji administracyjnej.



Wykres 2: Liczba skarg, które wpłynęły do UODO w latach 2020–2023.

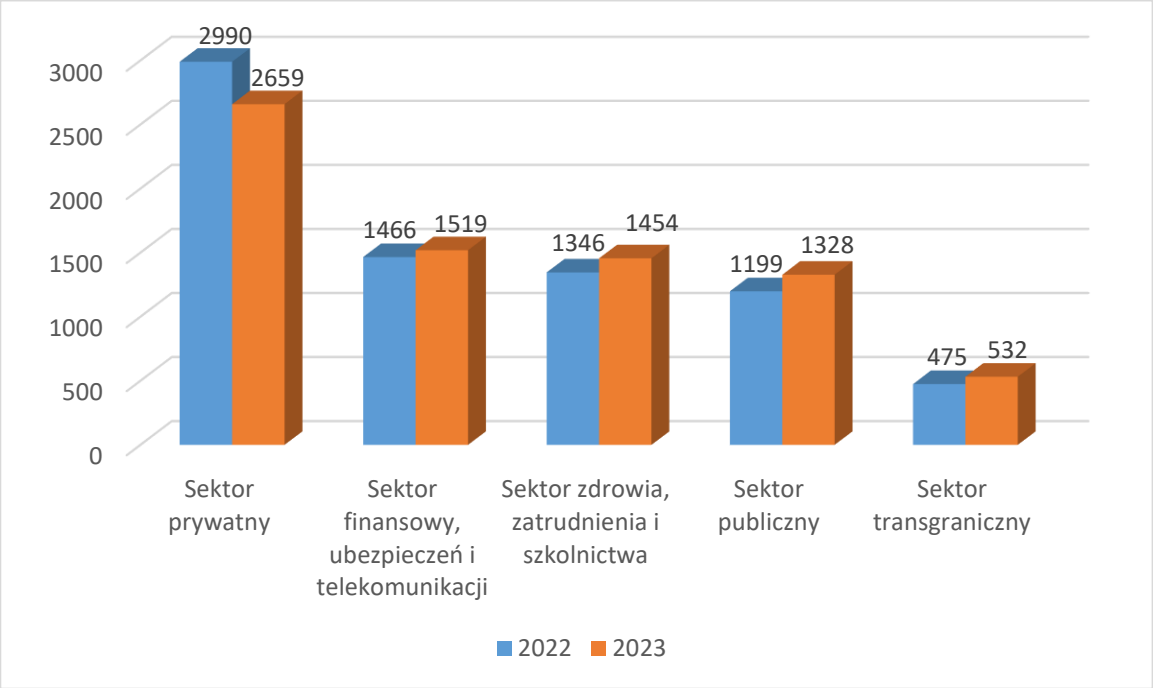
W analizowanym roku 2023 **postępowania zakończono w 5898 sprawach**, spośród których **1750** zakończyło się wydaniem decyzji administracyjnych w samym tylko Departamencie Skarg (DS). Dane porównawcze z lat poprzednich wykazują, że liczba wydawanych przez Prezesa UODO decyzji administracyjnych, w sprawach zainicjowanych skargami osób, których dane dotyczą, utrzymała się na zbliżonym poziomie w stosunku do ubiegłych lat (w roku 2022 wydanych zostało 1830 decyzji administracyjnych w sprawach skargowych, zaś w roku 2021 wydaniem decyzji administracyjnej zakończyły się 1734 sprawy zainicjowane skargą).



Wykres 3: Liczba decyzji administracyjnych wydanych w latach 2020–2023 w sprawach zainicjowanych indywidualną skargą.

Uwzględniając podział skarg na poszczególne sektory, ich liczba przedstawia się następująco:

- 2659 skarg na podmioty sektora prywatnego (2990 skarg w roku 2022);
- 1519 skarg na podmioty sektora finansowego, ubezpieczeń i telekomunikacji (1466 skarg w roku 2022);
- 1454 skargi na podmioty sektora zdrowia, zatrudnienia i szkolnictwa (1346 skarg w roku 2022);
- 1328 skarg na podmioty sektora publicznego (1199 skarg w roku 2022);
- 532 skargi na podmioty sektora transgranicznego (475 skarg w roku 2022).



Wykres 4: Liczba skarg, które wpłynęły do UODO w latach 2022–2023 z podziałem na sektory.

W omawianym 2023 r. utrzymała się – podobna do roku poprzedniego – wysoka liczba skarg wnoszonych do Urzędu Ochrony Danych Osobowych. Spadek liczby wnoszonych skarg odnotowano w sektorze prywatnym, w pozostałych sektorach, w tym w sektorze transgranicznym, liczba ta wzrosła.

Spadek liczby skarg na podmioty sektora prywatnego wiązać należy z sytuacją ekonomiczną i mniejszą skłonnością osób, których dane dotyczą, do zawierania umów z podmiotami z ww. sektora. Zauważyć należy, że skargi na podmioty z ww. sektora najczęściej związane były z zawarciem lub wykonywaniem umów i przetwarzaniem danych osobowych z tym związanych.

Wśród skarg na podmioty z sektora finansowego, niezmiennie w stosunku do lat ubiegłych, najwięcej miało związek z umowami zawieranymi z bankami i instytucjami kredytowymi.

Skargi na podmioty z sektora zdrowia często dotyczyły wystawiania recept przez lekarzy z posługujących się danymi osób, które z usług tych lekarzy nie korzystały w ogóle lub nie korzystały w dniu wystawienia recepty oraz nieuprawnionego dostępu do danych za pośrednictwem platformy PUE ZUS.

Częstym powodem złożenia skargi na pracodawcę było natomiast przetwarzanie wizerunku pracowników w związku z prowadzonym monitoringiem wizyjnym oraz niezapewnienie dostępu do danych osobowych przetwarzanych w związku z tym monitoringiem.

Ponadto w każdym spośród wskazanych wyżej sektorów, podobnie jak w latach ubiegłych, osoby, których dane dotyczyły, często skarżyły się na przetwarzanie ich danych osobowych bez podstawy prawnej, w tym na nieuprawnione udostępnienie ich danych osobowych podmiotom nieuprawnionym, czy też nieuprawnione działania marketingowe z wykorzystaniem ich danych. Duża część skarg dotyczyła także niespełnienia

obowiązków informacyjnych, wynikających z RODO, w tym nieprzekazania kopii danych, zgodnie z art. 15 ust. 3 RODO. Odnotowano również liczne skargi na nieprawidłowe wykonanie obowiązku sprostowania danych oraz nieprawidłową realizację prawa do usunięcia danych, wynikającego z art. 17 RODO i prawa sprzeciwu, o którym mowa w art. 21 RODO.

Choć analiza wnoszonych skarg wykazała zauważalny wzrost świadomości przepisów RODO przez osoby wnoszące skargi, które coraz częściej wykazują znajomość przepisów i powołują się na przysługujące im prawa, świadomie korzystając z nich w stosunku do administratorów ich danych osobowych, to Prezes UODO dostrzega potrzebę dalszego upowszechniania wśród osób, których dane dotyczą, informacji na temat zakresu kompetencji Prezesa UODO w związku z wnoszonymi przez nich skargami. Skarżący nie zawsze potrafili właściwie określić naruszenia przepisów RODO, przez co zdarzało się, że ich żądania wykraczały poza kompetencje Prezesa UODO. W roku 2023 zwracali się oni do organu m.in. w sprawach dotyczących naruszenia tajemnicy korespondencji, naruszenia dóbr osobistych, ścigania przestępstw, przyznania odszkodowania za naruszenia ochrony danych osobowych. W kierowanych do stron postępowania pismach organ wskazywał, gdzie dana osoba powinna zgłosić się z żądaniami, gdyż ich realizacja pozostawała poza jego kompetencjami. Wskazywał m.in. na odpowiednie sądy lub inne organy właściwe w zgłaszanej przez skarżącego sprawie. Skarżący zwracali się również do Prezesa UODO z żądaniami dotyczącymi kompetencji autonomicznych organu nadzorczego, np. nałożenia kary administracyjnej lub przeprowadzenia kontroli w siedzibie administratora, których to działań organ nie podejmuje na wniosek osoby, której dane dotyczą.

Prezes UODO odnotował rosnącą świadomość obowiązków spoczywających na administratorach, zwłaszcza w zakresie obowiązku przetwarzania danych w sposób rzetelny i przejrzysty dla osób, których dane dotyczą. Większa liczba administratorów zaczęła tworzyć oficjalne dokumenty opisujące politykę przetwarzania danych oraz stosować pisemne klauzule informacyjne o przetwarzaniu danych.

W zdecydowanej większości spraw administratorzy udzielali wyczerpujących wyjaśnień i odpowiedzi na pytania Prezesa UODO. Jednocześnie wciąż często popełniali błędy w zakresie wskazania prawidłowej podstawy prawnej przetwarzania danych osobowych oraz konkretnych przepisów prawa regulujących konkretne procesy przetwarzania.

Administratorzy danych wzywani do złożenia wyjaśnień mieli najczęściej trudność w podawaniu podstaw prawnych, w oparciu o które przetwarzali dane osobowe skarżących. Często byli w stanie poprawnie opisać cel przetwarzania, ich wyjaśnienia były logiczne i sensowne, ale nie zawsze byli w stanie wskazać właściwy przepis prawa uprawniający ich do przetwarzania danych w oparciu o przesłankę z art. 6 ust. 1 lit. c) RODO. Prezes UODO zaobserwował, że administratorzy często też uchybiali terminowi na spełnienie żądania osoby, której dane dotyczą.

Administratorzy w toku prowadzonych przez Prezesa UODO postępowań administracyjnych podejmowali wymagane czynności celem zminimalizowania ponownego wystąpienia naruszenia w przyszłości. Dodatkowo podmioty, względem których organ skorzystał wcześniej z uprawnień naprawczych, o których mowa w art. 58 ust. 2 RODO, podchodziły z większą ostrożnością i dbałością do realizowanych przez

siebie operacji przetwarzania danych osobowych. Niemniej jednak w 2023 r. zdarzały się również przypadki wszczęcia postępowań w zakresie nałożenia administracyjnej kary pieniężnej na administratora ze względu na brak współpracy z Prezesem UODO i część z tych postępowań zakończyła się nałożeniem ww. kary na administratora.

Poniżej przytoczone zostały przykłady wybranych skarg z każdego sektora, które w roku sprawozdawczym 2023 były przedmiotem analizy organu nadzorczego.

1.1.1. Sektor publiczny

Skargi, które wpłynęły do organu na podmioty z **sektora publicznego (1328 skarg),** podobnie jak w latach ubiegłych, najczęściej dotyczyły udostępnienia danych osobowych na stronach internetowych Biuletynu Informacji Publicznej (BIP).

Udostępnienie danych osobowych w związku z publikacją treści uchwały rady gminy w Biuletynie Informacji Publicznej

Przedmiotem jednej ze skarg było udostępnienie na stronie internetowej BIP urzędu gminy danych osobowych skarżącej w postaci imienia, nazwiska oraz informacji, że jej oferta nie spełnia wymogów formalnych na stanowisko zastępcy głównego księgowego, zawartych w uchwale rady gminy i w uzasadnieniu do tej uchwały. Jak wynikało z ustaleń postępowania, skarżąca złożyła skargę na działalność kierownika centrum usług wspólnych odnośnie do przeprowadzenia naboru na stanowisko zastępcy głównego księgowego. Rada gminy rozpatrzyła uchwałą ww. skargę i uznała ją za bezzasadną. W treści uchwały postanowiono, że podlega ona podaniu do publicznej wiadomości m.in. przez zamieszczenie jej treści na stronie internetowej BIP urzędu gminy. W treści uchwały znajdowały się dane osobowe skarżącej w zakresie jej imienia i nazwiska oraz informacji, że oferta skarżącej nie spełnia wymogów formalnych stawianych pracownikom samorządowym w ustawie o pracownikach samorządowych. Uchwała wraz z uzasadnieniem, bez anonimizacji, została udostępniona na stronie internetowej BIP. W wydanej w tej sprawie decyzji administracyjnej Prezes UODO podkreślił, że zgodnie z art. 6 ust. 1 pkt 4 lit. a) ustawy o dostępie do informacji publicznej[14], 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), przy czym zgodnie z art. 5 ust. 2 tej ustawy, prawo do informacji publicznej podlega ograniczeniu m.in. ze względu na prywatność osoby fizycznej. Prezes UODO uznał, że publikacja ww. uchwały po dokonaniu odpowiedniej anonimizacji danych osobowych skarżącej, jako wnoszącej skargę, pozwoliłaby na poznanie treści uchwały oraz czyniła zadość warunkom jej dostępności oraz powszechnej znajomości, bez naruszenia prawa do prywatności skarżącej. W ocenie Prezesa UODO prywatność skarżącej, jako dobro chronione prawem, powinno mieć pierwszeństwo przed innym dobrem prawem chronionym – dostępnością do informacji publicznej. Prezes UODO w decyzji podzielił nadto pogląd wyrażony przez Naczelny Sąd Administracyjny w wyroku z 14 marca 2013 r.[15], że zainicjowanie przez stronę postępowania skargowego stanowi realizację uprawnień obywatelskich.

[14] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).
[15] Sygn. akt I OSK 620/12.

Korzystanie zaś z praw obywatelskich nie wyklucza automatycznie ochrony prawa do prywatności. Prezes UODO uznał, że skarżone udostępnienie danych osobowych nie miało uzasadnienia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO, a ponadto naruszało zasadę „minimalizacji danych" (art. 5 ust. 1 lit. c RODO). Z materiału dowodowego zgromadzonego w sprawie wynikało, że dane osobowe skarżącej w postaci imienia i nazwiska zostały usunięte z ww. strony internetowej. Wobec tego Prezes UODO uznał, że dane osobowe skarżącej nie są obecnie przetwarzane w kwestionowany przez nią sposób. Z uwagi na powyższe, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, Prezes UODO udzielił wójtowi upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych[16].

Udostępnienie danych osobowych w BIP w związku z publikacją protokołu z sesji rady powiatu

W roku 2023 toczyło się także postępowanie administracyjne w sprawie publikacji danych osobowych skarżącej w zakresie imienia i nazwiska na stronie BIP starostwa powiatowego, w związku z publikacją protokołu z obrad sesji rady powiatu. Jak wynikało z ustaleń postępowania, skarżąca złożyła skargę do rady powiatu, która przekazała skargę do załatwienia staroście. Skarga dotyczyła działań dyrektora zespołu szkół odnośnie do odmowy wypłaty skarżącej świadczeń ze stosunku pracy, tj. odprawy emerytalnej i świadczeń socjalnych. Projekt uchwały w sprawie rozpatrzenia ww. skargi został przedstawiony przez przewodniczącego komisji rewizyjnej podczas obrad sesji rady powiatu, a z ww. obrad został sporządzony protokół. Jak wynikało z treści protokołu, zawarto w nim dane osobowe skarżącej w postaci jej imienia i nazwiska. Jako podstawę prawną udostępnienia ww. danych osobowych skarżącej starosta wskazał art. 18 ust. 1 w zw. z art. 19 ustawy o dostępie do informacji publicznej. Z ustaleń postępowania wynikało zatem, że starosta udostępnił protokół z obrad sesji rady powiatu w celu realizacji nałożonego przez ww. przepisy obowiązku udostępniania protokołów z obrad kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów. W wydanej decyzji administracyjnej Prezes UODO wskazał, że zgodnie z art. 5 ust. 2 ww. ustawy prawo do informacji publicznej podlega ograniczeniom m.in. ze względu na prywatność osoby fizycznej. Prezes UODO uznał, że starosta publikując na stronie internetowej BIP dane osobowe skarżącej w zakresie jej imienia i nazwiska zawarte w protokole z obrad sesji rady powiatu, nie legitymował się żadną z przesłanek legalizujących ten proces spośród określonych w art. 6 ust. 1 RODO, co przesądziło o naruszeniu tego przepisu. Jednakże przed wydaniem przez Prezesa UODO decyzji w sprawie ww. dane osobowe skarżącej zostały usunięte z protokołu z sesji rady powiatu dostępnego na stronie BIP starostwa powiatowego. Z tego względu Prezes UODO – uznając, że na dzień wydania decyzji starosta nie udostępnia już danych osobowych skarżącej w sposób zakwestionowany w skardze – skorzystał z instrumentu o charakterze naprawczym, przewidzianego w art. 58 ust. 2 lit. b) RODO i udzielił staroście upomnienia w związku z naruszeniem art. 6 ust. 1 RODO[17].

Udostępnienie stronom postępowania administracyjnego, w wydanej przez organ decyzji, danych osobowych osoby zgłaszającej naruszenie przepisów ustawy

[16] DS.523.5723.2021.
[17] DS.523.4794.2022.

o ochronie przyrody oraz udostępnienie na stronie internetowej BIP danych osobowych zawartych w odpowiedzi burmistrza na interpelację radnej rady miejskiej

Przedmiotem skargi było udostępnienie danych osobowych skarżącej, zawartych w decyzji burmistrza, stronom postępowania administracyjnego oraz udostępnienie na stronie internetowej BIP urzędu miejskiego danych osobowych skarżącej zawartych w odpowiedzi burmistrza na interpelację radnej rady miejskiej[18]. Skarżąca pismem poinformowała burmistrza o naruszeniu przepisów ustawy o ochronie przyrody. Na skutek pisma skarżącej burmistrz wszczął postępowanie, w którym wydał decyzję administracyjną. W decyzji tej została zamieszczona informacja, że do urzędu miejskiego wpłynął wniosek skarżącej dotyczący naruszenia przepisów ustawy o ochronie przyrody w związku z pracami w zakresie pielęgnacji drzew rosnących na działkach położonych na terenie gminy. Ponadto w decyzji został wskazany adres skarżącej, który – jak wyjaśnił burmistrz – jest także adresem siedziby stowarzyszenia, którego skarżąca jest reprezentantem. Zgodnie z wyjaśnieniami burmistrza, dane osobowe skarżącej zawarte w tej decyzji zostały udostępnione stronom postępowania. Ustalono, że skarżąca, jako osoba składająca zawiadomienie o naruszeniu przepisów ustawy, nie była stroną postępowania prowadzonego przez burmistrza.

Prezes UODO w wydanej w tej sprawie decyzji administracyjnej uznał za nieuzasadnione ujawnienie przez burmistrza stronom prowadzonego postępowania danych osobowych skarżącej jako osoby, która zawiadomiła organ o możliwych nieprawidłowościach dotyczących naruszenia przepisów ustawy o ochronie przyrody. W opinii organu działanie takie nie znajdowało podstaw w przepisach K.p.a., które wyposażają organ w instrumenty pozwalające na zbadanie sygnalizowanych przez obywateli nieprawidłowości poprzez wszczęcie postępowania z urzędu, bez konieczności ujawniania źródła pozyskanych informacji. Prezes UODO uznał, że udostępnienie w treści decyzji administracyjnej danych osobowych skarżącej, jako osoby zawiadamiającej organ o zaobserwowanych nieprawidłowościach, nie miało podstaw prawnych i naruszyło art. 6 ust. 1 RODO. Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, Prezes UODO udzielił burmistrzowi upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych.

W odniesieniu do drugiego z postawionych przez skarżącą zarzutów ustalono, że przewodnicząca rady miejskiej przekazała burmistrzowi interpelację radnej rady miejskiej w sprawie wniosków o ukaranie za niewłaściwą pielęgnację i samowolne ścięcie korony drzewa na terenie gminy celem rozpoznania i udzielenia odpowiedzi. W zamieszczonej na stronie internetowej BIP urzędu miejskiego odpowiedzi na interpelację burmistrz zawarł imię i nazwisko skarżącej jako osoby, która w imieniu stowarzyszenia podpisała wniosek o wszczęcie postępowania administracyjnego w związku z naruszeniem ustawy o ochronie przyrody oraz jako osoby, na wniosek której wszczęto postępowanie administracyjne o ukaranie podmiotu w związku ze zniszczeniem drzew. Do odpowiedzi na interpelację załączono skany dokumentów (niektóre częściowo zanonimizowane) zawierające w swej treści imię i nazwisko skarżącej. Z ustaleń postępowania wynikało, że burmistrz udostępnia obecnie na stronie internetowej BIP urzędu miejskiego dane osobowe skarżącej w postaci

[18] DS.523.664.2021.

imienia i nazwiska w związku z ustawowym obowiązkiem publikowania treści interpelacji radnych oraz treści odpowiedzi na interpelacje radnych. Zgodnie z art. 24 ust. 3 ustawy o samorządzie gminnym[19], w sprawach dotyczących gminy radni mogą kierować interpelacje i zapytania do wójta (w przedmiotowej sprawie do burmistrza), w trybie określonym w ust. 4–6. Stosownie do art. 24 ust. 7 ww. ustawy, treść interpelacji i zapytań oraz udzielonych odpowiedzi podawana jest do publicznej wiadomości poprzez niezwłoczną publikację w BIP i na stronie internetowej gminy, oraz w inny sposób zwyczajowo przyjęty, przy czym – zgodnie z art. 5 ust. 2 ustawy o dostępie do informacji publicznej, prawo do informacji publicznej podlega ograniczeniu m.in. ze względu na prywatność osoby fizycznej. Zebrany w sprawie materiał dowodowy nie dał podstaw do przyjęcia, że skarżąca zrezygnowała w stosunku do udostępnionych w odpowiedzi burmistrza na interpelację informacji z przysługującego jej prawa do prywatności. Z przywołanych przez burmistrza okoliczności nie wynikało, aby skarżąca była osobą pełniącą funkcję publiczną oraz by stowarzyszenie, którego była członkiem, było podmiotem o statusie przewidzianym w art. 4 ust. 1 pkt 5 ww. ustawy. Zdaniem Prezesa UODO udostępnienie danych skarżącej nie było niezbędne do spełnienia obowiązku publikacji treści interpelacji radnej oraz odpowiedzi na nią, który to obowiązek mógł zostać bez przeszkód spełniony przez burmistrza bez publikowania ww. danych osobowych skarżącej, po dokonaniu stosownej anonimizacji dokumentu. Prezes UODO stwierdził, że burmistrz, publikując dane osobowe skarżącej w odpowiedzi na interpelację radnej rady miejskiej na stronie internetowej BIP urzędu miejskiego, nie legitymował się żadną z przesłanek określonych w art. 6 ust. 1 RODO. Jednocześnie z materiału dowodowego zgromadzonego w sprawie wynikało, że ww. dane osobowe skarżącej są nadal udostępniane na ww. stronie internetowej. Wobec powyższego Prezes UODO skorzystał w tym zakresie z instrumentu o charakterze naprawczym, o którym mowa w art. 58 ust. 2 lit. d) RODO, i nakazał usunięcie danych osobowych skarżącej opublikowanych na stronie BIP urzędu miejskiego w odpowiedzi burmistrza na interpelację radnej rady miejskiej.

Udostępnienie w miejscach publicznie dostępnych danych osobowych zawartych w obwieszczeniu samorządowego kolegium odwoławczego

Przedmiotem innej skargi były nieprawidłowości w procesie przetwarzania danych osobowych przez wójta oraz samorządowe kolegium odwoławcze (SKO) polegające na udostępnieniu w miejscach publicznie dostępnych danych osobowych skarżącej zawartych w obwieszczeniu SKO. Ustalono, że skarżąca, posiadająca legitymację strony postępowania, złożyła do SKO odwołanie od decyzji burmistrza, w której burmistrz ustalił lokalizację inwestycji celu publicznego, jaką była budowa placu zabaw i budowa miejsc parkingowych. SKO utrzymało w mocy ww. decyzję organu I instancji i przekazało burmistrzowi (jako organowi I instancji) obwieszczenie zawierające informacje o wydaniu ww. decyzji, by organ umieścił je w miejscach oraz w terminie określonym przez ustawodawcę. Wyżej wymienione obwieszczenie zawierało informację, że SKO wydało decyzję ostateczną, która po rozpatrzeniu odwołania wniesionego przez skarżącą, utrzymała w mocy decyzję burmistrza. Obwieszczenie to zawierało imię i nazwisko skarżącej, jako osoby, która wniosła odwołanie od decyzji organu I instancji i zostało zamieszczone na tablicy ogłoszeń SKO, stronie BIP SKO, BIP urzędu gminy oraz

[19] Ustawa z 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609 ze zm.).

w miejscach ogólnodostępnych na terenie gminy. Obwieszczenie to na dzień wydania decyzji nie było udostępniane przez ww. podmioty. Zgodnie z art. 53 ust. 1 ustawy o planowaniu i zagospodarowaniu przestrzennym[20] o wszczęciu postępowania w sprawie wydania decyzji o ustaleniu lokalizacji inwestycji celu publicznego oraz postanowieniach i decyzji kończącej postępowanie, zawiadamia się strony w drodze obwieszczenia, a także w sposób zwyczajowo przyjęty w danej miejscowości. Inwestora oraz właścicieli i użytkowników wieczystych nieruchomości, na których będą lokalizowane inwestycje celu publicznego, zawiadamia się na piśmie. Natomiast zgodnie z art. 49 § 1 K.p.a., jeżeli przepis szczególny tak stanowi, zawiadomienie stron o decyzjach i innych czynnościach organu administracji publicznej może nastąpić w formie publicznego obwieszczenia, w innej formie publicznego ogłoszenia zwyczajowo przyjętej w danej miejscowości lub przez udostępnienie pisma w BIP na stronie podmiotowej właściwego organu administracji publicznej. Oceniając przedmiotowe udostępnienie, Prezes UODO wziął pod uwagę, że celem ww. przepisu jest wyeliminowanie trudności związanych z doręczaniem stronom decyzji i postanowień na piśmie – w przypadku znacznej liczby osób uczestniczących w postępowaniu administracyjnym. Uznał też, że dla poinformowania w formie obwieszczenia stron o zakończeniu postępowania odwoławczego oraz wydaniu decyzji nie było niezbędne zamieszczenie w obwieszczeniu danych osobowych osoby, na wniosek której wszczęto postępowanie odwoławcze. Co prawda, strony w toczącym się postępowaniu administracyjnym są uprawnione do zapoznawania się z informacjami zawartymi w materiale zgromadzonym w toku postępowania, w tym z danymi osobowymi identyfikującymi pozostałe strony, jednakże oznaczenie stron postępowania lub jego uczestników powinno mieć miejsce w treści rozstrzygnięcia administracyjnego (decyzji), a nie w treści publicznego obwieszczenia dostępnego także dla osób postronnych (innych niż strony lub uczestnicy postępowania administracyjnego). Jak wynika z treści obwieszczenia, strony postępowania mogły zapoznać się z pełną treścią decyzji w urzędzie.

Skarżone udostępnienie nie znajdowało oparcia w art. 53 ust. 1 ustawy o planowaniu i zagospodarowaniu przestrzennym, nie było bowiem niezbędne do poinformowania stron o wynikach postępowania administracyjnego prowadzonego przez SKO. Prezes UODO uznał, że udostępnienie danych osobowych skarżącej przez SKO oraz burmistrza w miejscach publicznie dostępnych naruszyło art. 6 ust. 1 RODO i korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, udzielił ww. podmiotom upomnień za stwierdzone naruszenia przepisów o ochronie danych osobowych[21].

Udostępnienie danych osobowych podczas sesji rad miejskich oraz w nagraniach z sesji rad miejskich

W 2023 r. Prezes UODO rozpatrywał również skargi dotyczące udostępnienia danych osobowych podczas obrad kolegialnych organów jednostek samorządu terytorialnego oraz w nagraniach z obrad.

W jednej z takich spraw radny ujawnił podczas obrad sesji rady miejskiej dane osobowe skarżącego w postaci imienia i nazwiska, zawarte w jego skardze do rady miejskiej na działanie zastępcy prezydenta miasta, odczytując treść tej skargi bez

[20] Ustawa z 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz. U. z 2024 r. poz.1130).
[21] DS.523.3953.2021.

pominięcia ww. danych. Następnie dane te zostały upublicznione na stronie internetowej w transmisji na żywo oraz w nagraniu z sesji rady miejskiej. W ocenie Prezesa UODO za nieznajdujące podstaw prawnych należało uznać upublicznienie danych osobowych skarżącego podczas przedstawiania jego skargi na sesji rady. Upublicznienie to nie było w ocenie organu niezbędne do rozpatrzenia wniesionej skargi. Obrady sesji mają często charakter dynamiczny, jednakże planując ich przebieg w zakresie dotyczącym skarg składanych przez mieszkańców, administrator posiada wiedzę na temat treści tych skarg i jest w stanie przedstawić je w sposób zapewniający odpowiedni stopień ochrony danych osobowych w nich zawartych. Wskazać należy, że skarżący wnosząc skargę na działanie zastępcy prezydenta miasta nie pełnił funkcji publicznej oraz nie zrezygnował ze swojego prawa do prywatności w tym zakresie. Wobec tego rada, jako administrator danych osobowych skarżącego zawartych w skardze, zobowiązana była do ich przetwarzania tak, by nie naruszać przepisów o ochronie danych osobowych. Prezes UODO uznał w niniejszej sprawie, że rada udostępniając dane osobowe skarżącego w postaci jego imienia i nazwiska podczas sesji rady miejskiej, nie posiadała legitymacji prawnej do ich udostępnienia w przedmiotowy sposób, co naruszyło przepis art. 6 ust. 1 RODO.

Publikacja transmisji oraz nagrania zawierającego dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna była nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych. Biorąc pod uwagę incydentalny charakter naruszenia oraz fakt, że udostępnione na stronie internetowej dane osobowe w nagraniu sesji rady miejskiej zostały usunięte, Prezes UODO wydał decyzję[22], w której udzielił upomnienia:

- radzie miejskiej za udostępnienie danych osobowych skarżącego w postaci imienia i nazwiska podczas sesji rady miejskiej bez podstawy prawnej,
- prezydentowi miasta za udostępnienie danych osobowych skarżącego w postaci imienia i nazwiska na stronie internetowej w transmisji na żywo oraz w nagraniu z sesji rady miejskiej bez podstawy prawnej.

Udostępnienie podczas sesji rady miejskiej danych osobowych zawartych w powiadomieniu o zamiarze wystąpienia z inicjatywą przeprowadzenia referendum

Przedmiotem kolejnej opisywanej skargi było udostępnienie adresu zamieszkania skarżącego podczas sesji rady miejskiej i w nagraniu na kanale gminy w serwisie YouTube. W postępowaniu ustalono, że burmistrz został powiadomiony o zamiarze wystąpienia z inicjatywą przeprowadzenia referendum w przedmiocie jego odwołania. Inicjatorami referendum była grupa mieszkańców gminy, w tym skarżący. Podczas sesji rady miejskiej burmistrz w punkcie porządku obrad „Sprawozdanie z działalności Burmistrza w okresie międzysesyjnym” odczytał tekst powiadomienia o zamiarze wystąpienia z inicjatywą przeprowadzenia referendum wraz z zawartymi w nim informacjami o imieniu i nazwisku skarżącego oraz nazwie miejscowości i numerze posesji, na której zamieszkuje. Nagranie z sesji rady miejskiej, zawierające wypowiedź burmistrza, zostało udostępnione na kanale gminy w serwisie YouTube. Jednakże przed wydaniem przez Prezesa UODO decyzji administracyjnej kończącej postępowanie fragment tego nagrania zawierający ww. dane osobowe skarżącego, został usunięty.

[22] DS.523.2.2020.

W decyzji administracyjnej Prezes UODO wskazał, że w jego ocenie na burmistrzu spoczywał obowiązek wyłączenia jawności tych informacji podczas odczytywania powiadomienia o zamiarze wystąpienia z inicjatywą przeprowadzenia referendum. W stanie faktycznym sprawy te informacje nie stanowiły bowiem informacji publicznej, a nawet gdyby taką informację stanowiły, to ich udostępnienie podlegałoby ograniczeniu ze względu na prywatność osoby fizycznej. Uzasadniając powyższe stanowisko Prezes UODO wskazał, że z materiału dowodowego zgromadzonego w sprawie wynika, że burmistrz odczytując w punkcie porządku obrad „Sprawozdanie z działalności Burmistrza w okresie międzysesyjnym" tekst powiadomienia o zamiarze wystąpienia z inicjatywą przeprowadzenia referendum, działał stosownie do dyspozycji statutu gminy. W świetle art. 18 ust. 2 pkt 2 ustawy o samorządzie gminnym[23] rada miejska była właściwa do zapoznania się ze sprawozdaniem burmistrza. Do udostępnienia danych osobowych skarżącego doszło zatem w ramach sprawowania władzy publicznej przez burmistrza i radę miejską. Zdaniem Prezesa UODO rozważyć jednak należy, czy w tym stanie faktycznym nastąpić powinno ograniczenie jawności, o którym mowa w art. 11b ust. 1 zdanie drugie ustawy o samorządzie gminnym, czyli ograniczenie wynikające z ustaw, oraz wskazał, że należy zwrócić uwagę na ograniczenia, jakie nakłada art. 5 ust. 2 ustawy o dostępie do informacji publicznej[24], który stanowi, że prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Informacje składające się na adres zamieszkania skarżącego dotyczą jego prywatnej sfery życia, a zebrany w sprawie materiał dowodowy nie daje podstaw do przyjęcia, iż skarżący zrezygnował z przysługującego mu prawa do prywatności. Ponadto odczytana przez burmistrza informacja o nazwie miejscowości i numerze posesji, w której zamieszkuje skarżący, nie odnosiła się do niego w kontekście pełnionej funkcji publicznej. Prezes UODO podkreślił również, że przepisy o referendum lokalnym[25] jednoznacznie wskazują, kto, kiedy, komu i w jaki sposób udostępnia dane osobowe inicjatorów referendum, jak również zakres tego udostępniania. Przepisy te nie ustanawiają po stronie burmistrza obowiązku lub uprawnienia do podania do publicznej wiadomości informacji składających się na adresy zamieszkania ww. osób.

Konkludując, Prezes UODO stwierdził, że burmistrz udostępniając dane osobowe skarżącego w zakresie informacji o nazwie miejscowości i numerze posesji skarżącego podczas sesji rady miejskiej, nie legitymował się żadną z przesłanek określonych w art. 6 ust. 1 RODO, która legalizowałaby ten proces. Z uwagi na tę okoliczność, uwzględniając wagę i charakter stwierdzonego naruszenia oraz jego nieodwracalność, Prezes UODO uznał za zasadne skorzystanie w tym zakresie z instrumentu o charakterze naprawczym, przewidzianego w art. 58 ust. 2 lit. b) RODO, i udzielił burmistrzowi upomnienia.

W kwestii udostępnienia danych osobowych skarżącego w nagraniu na kanale gminy w serwisie YouTube Prezes UODO wskazał, że publikacja nagrania powinna była nastąpić po odpowiednim przetworzeniu zawartych w nim danych osobowych skarżącego i uznał za niezasadne ich upublicznienie w nagraniu. Stwierdził też, że burmistrz publikując dane osobowe skarżącego na kanale gminy w serwisie YouTube nie posiadał legitymacji prawnej do ich udostępniania w przedmiotowy sposób, co naruszyło przepis art. 6 ust. 1

[23] Ustawa z 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609 ze zm.).
[24] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).
[25] Ustawa z 15 września 2000 r. o referendum lokalnym (Dz. U. z 2023 r. poz. 1317 ze zm.).

RODO. Z uwagi na tę okoliczność, uwzględniając wagę i charakter stwierdzonego naruszenia oraz fakt, że burmistrz zaprzestał udostępniania w powyższy sposób informacji o nazwie miejscowości i numerze posesji skarżącego, Prezes UODO również w tym zakresie udzielił burmistrzowi upomnienia za udostępnienie danych[26].

Udostępnienie w piśmie skierowanym do osoby trzeciej danych osobowych osoby zgłaszającej naruszenie przepisów ustawy

Przedmiotem jednej ze skarg było udostępnienie przez wójta danych osobowych skarżącej w zakresie imienia, nazwiska oraz adresu zamieszkania w piśmie wójta skierowanym do osoby trzeciej. Wójt przetwarzał dane osobowe skarżącej w związku z licznymi zawiadomieniami telefonicznymi skarżącej, w których informowała, że czuje się zagrożona z tego powodu, że sąsiad nie pilnuje swoich psów, które pozostawione są bez opieki na drodze. Wójt uznał, że doszło do naruszenia zakazu określonego w art. 10a ust. 3 ustawy o ochronie zwierząt[27], według którego zabrania się puszczania psów bez możliwości ich kontroli i bez oznakowania umożliwiającego identyfikację właściciela lub opiekuna. Skierował więc do właściciela psów pismo, w którym przypomniał o obowiązkach właścicieli zwierząt wynikających z ustawy oraz z regulaminu utrzymania czystości i porządku na terenie gminy, wprowadzonego uchwałą rady gminy. Na końcu ww. pisma zamieszczono rozdzielnik, w którym znalazła się informacja, iż pismo skierowano także do wiadomości skarżącej oraz podano jej dane osobowe, tj. imię, nazwisko oraz adres. Prezes UODO uznał, że skierowanie pouczenia do właściciela psów o jego obowiązkach nie uzasadniało w żaden sposób przytoczenia w rozdzielniku ww. pisma danych osobowych skarżącej. W ocenie Prezesa UODO zainicjowanie przez skarżącą działań ze strony wójta w kierunku realizacji obowiązków wynikających z ustawy o ochronie zwierząt, nie uzasadnia późniejszego zamieszczenia jej danych w piśmie skierowanym do właściciela zwierząt, który zdaniem gminy nie wypełnia tych obowiązków. Działania skarżącej stanowiły realizację jej uprawnień obywatelskich i nie wykluczały ochrony prawa do prywatności, ani też jej praw wynikających z przepisów o ochronie danych osobowych. Prezes UODO wskazał także, że żaden z przepisów K.p.a. nie nakazuje umieszczania w korespondencji kierowanej do adresatów pism rozdzielnika zawierającego dane osobowe wszystkich osób, do których kierowane jest pismo. Prezes UODO uznał, że ww. udostępnienie danych osobowych nie miało uzasadnienia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO oraz naruszało zasadę „minimalizacji danych" (art. 5 ust. 1 lit. c RODO). Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, Prezes UODO udzielił wójtowi upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych[28].

Udostępnienie danych osobowych zawartych w decyzji na rzecz podmiotów nieuprawnionych

Przedmiotem kolejnej skargi było udostępnienie przez wójta danych osobowych skarżącego zawartych w wydanej decyzji na rzecz wojewódzkiego inspektora ochrony środowiska, prokuratury oraz komornika. Ustalono, że wójt prowadził z urzędu postępowanie administracyjne w sprawie odpadów porzuconych na działce, której

[26] DS.523.3944.2020.
[27] Ustawa z 21 sierpnia 1997 r. o ochronie zwierząt (Dz. U. z 2023 r. poz. 1580 ze zm.).
[28] DS.523.4084.2022.

współwłaścicielem był skarżący. Postępowanie to zostało zainicjowane wnioskiem wojewódzkiego inspektora ochrony środowiska, który zwrócił się do wójta o podjęcie działań polegających na usunięciu odpadów z ww. nieruchomości oraz poinformowanie o podjętych działaniach w sprawie na podstawie art. 16 ust. 1 i 2 ustawy o Inspekcji Ochrony Środowiska[29]. Po przeprowadzeniu postępowania w ww. sprawie, wójt wydał decyzję administracyjną, którą doręczył wojewódzkiemu inspektorowi ochrony środowiska, prokuraturze oraz komornikowi. W decyzji wójta zawarte były dane osobowe skarżącego w zakresie imienia i nazwiska, informacja, że jest jedynym współwłaścicielem przedmiotowej działki, że na terenie tejże działki znajduje się nieczynna stacja paliw i nieruchomość zabudowana jest zniszczonym i nieużytkowanym budynkiem oraz ile wynosi udział skarżącego we własności ww. działki. Wójt w złożonych w sprawie wyjaśnieniach powoływał się na to, że wojewódzki inspektor ochrony środowiska, prokuratura oraz komornik byli stronami postępowania i z tego względu decyzja została im doręczona. Zebrany w sprawie materiał dowodowy nie potwierdził jednak, aby wojewódzki inspektor ochrony środowiska oraz prokuratura były stronami prowadzonego przez wójta postępowania.

Zauważyć należy, że art. 16 ust. 3 pkt 2 ustawy o Inspekcji Ochrony Środowiska stanowi, że w razie stwierdzenia nieprawidłowości w działaniach organów administracji publicznej w zakresie ochrony środowiska, organ inspekcji ochrony środowiska może m.in. uczestniczyć w tych postępowaniach – na prawach przysługujących prokuratorowi. Z analizy materiału dowodowego w niniejszej sprawie nie wynikało, aby wojewódzki inspektor ochrony środowiska zgłosił swoje przystąpienie do prowadzonego przez wójta postępowania. Z uwagi na powyższe na wójcie ciążył jedynie obowiązek poinformowania wojewódzkiego inspektora ochrony środowiska o podjętych działaniach w sprawie usunięcia odpadów, na podstawie art. 16 ust. 1 i 2 ustawy o Inspekcji Ochrony Środowiska, do czego został zobligowany pismem ww. organu.

Z analizy materiału dowodowego nie wynikało, aby prokurator zgłosił swoje przystąpienie do prowadzonego przez wójta postępowania. Wójt korespondował z prokuraturą w celu wyjaśnienia sprawy w ramach wzajemnej współpracy, zatem na wójcie ciążył jedynie obowiązek poinformowania prokuratury o podejmowanych działaniach w sprawie.

W związku z tym, że wójt naruszył przepisy o ochronie danych osobowych, tj. art. 6 ust. 1 RODO, udostępniając bez podstawy prawnej dane osobowe skarżącego zawarte w wydanej decyzji administracyjnej na rzecz wojewódzkiego inspektora ochrony środowiska oraz prokuratury, Prezes UODO – korzystając z przysługującego mu uprawnienia określonego w art. 58 ust. 2 lit. b) RODO – udzielił wójtowi upomnienia za powyższe naruszenie.

Udostępnienie wojewodzie przez burmistrza danych osobowych radnego w związku ze skierowaniem do wiadomości wojewody pisma adresowanego do rady miejskiej

Przedmiotem innej skargi było udostępnienie wojewodzie przez burmistrza danych osobowych skarżącego w postaci numeru PESEL oraz numeru dowodu osobistego, zawartych w akcie notarialnym i umowie najmu części nieruchomości, oraz w zakresie daty, od jakiej skarżący był zameldowany pod wskazanym adresem na terenie miasta,

[29] Ustawa z 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (Dz. U. z 2024 r. poz. 425).

w związku ze skierowaniem do wiadomości wojewody pisma adresowanego do rady miejskiej. Celem przetwarzania danych osobowych skarżącego, będącego radnym rady miejskiej, była konieczność weryfikacji, czy zaistniały przesłanki do wygaszenia sprawowanego przez niego mandatu radnego, którą to okoliczność stwierdza organ stanowiący gminy w drodze uchwały. Postępowanie zostało wszczęte na skutek skargi, z której wynikało między innymi, że skarżący nie spełnia warunków pełnienia funkcji radnego, tj. konieczności zamieszkiwania radnego na terenie gminy oraz zakazu prowadzenia działalności gospodarczej z wykorzystaniem mienia komunalnego. Burmistrz skierował do rady miejskiej pismo z załączonymi dokumentami zawierającymi dane osobowe skarżącego, celem zainicjowania przez radę postępowania zmierzającego do ewentualnego wygaszenia mandatu radnego sprawowanego przez skarżącego. Powyższe pismo zostało przesłane do wiadomości wojewody.

Postępowanie dotyczące wygaśnięcia mandatu radnego odbywa się na podstawie przepisów ustawy – Kodeks wyborczy[30] oraz ustawy o samorządzie gminnym[31]. Obowiązek wszczęcia przez wojewodę takiego postępowania zachodzi w przypadku wystąpienia jednej z okoliczności wskazanych w art. 383 § 1 Kodeksu wyborczego i odbywa się w trybie określonym w art. 98a ust. 1–2 ustawy o samorządzie gminnym. Zgodnie z ww. przepisem brak czynności ze strony organu stanowiącego gminy aktualizuje obowiązek po stronie wojewody do wydania zarządzenia zastępczego (art. 98a ust. 2 ustawy o samorządzie gminnym).

W wydanej w tej sprawie decyzji Prezes UODO wskazał, że przepisy prawa nie przewidują po stronie burmistrza obowiązku przesyłania do wiadomości wojewody pisma skierowanego do organu uchwałodawczego gminy, celem przeprowadzenia postępowania wyjaśniającego przed wszczęciem postępowania w trybie art. 383 ustawy Kodeks wyborczy. Powyższego nie uzasadnia także konieczność zapewnienia realizacji przez wojewodę jego kompetencji nadzorczych wynikających z art. 86 ustawy o samorządzie gminnym. Prezes UODO wskazał, że działalność samorządu terytorialnego podlega nadzorowi wyłącznie z punktu widzenia legalności. Organy nadzoru, w tym wojewoda, nie zostały wyposażone w prawo ciągłego ingerowania w działalność samorządową i mogą w nią wkraczać tylko w ściśle określonych przypadkach. Prezes UODO podkreślił, że ustawodawca jednoznacznie określił etapy postępowania związanego z wygaszaniem mandatu radnego wskazując, że wyłącznie brak działania ze strony właściwego organu gminy upoważnia wojewodę do wezwania organu gminy do podjęcia odpowiedniego aktu w terminie 30 dni (art. 98a ust. 1). Jak stwierdził Prezes UODO, brak jest przepisu, który nakładałby na burmistrza obowiązek dla realizacji którego konieczne byłoby udostępnienie wojewodzie danych osobowych zawartych w piśmie skierowanym do rady miejskiej celem ewentualnego przeprowadzenia procedury wygaśnięcia mandatu radnego. Prezes UODO wskazał ponadto, że działania burmistrza nie legalizuje okoliczność, że dane osobowe skarżącego w zakresie numeru PESEL i numeru dowodu osobistego, zawarte w akcie notarialnym i umowie najmu części nieruchomości oraz w zakresie daty, od jakiej skarżący jest zameldowany pod wskazanym adresem na terenie miasta, oraz pozostałe dane osobowe zawarte w ww. akcie notarialnym, były już znane wojewodzie. W związku z tym udostępnienie przez burmistrza danych osobowych skarżącego nie znajdowało oparcia

[30] Ustawa z 5 stycznia 2011 r. Kodeks wyborczy (Dz. U. z 2023 r. poz. 2408 ze zm.).
[31] Ustawa z 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2024 r. poz. 609 ze zm.).

w żadnej spośród przesłanek określonych w art. 6 ust. 1 RODO, stanowiących o legalności ich udostępnienia. Korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, Prezes UODO udzielił ww. podmiotowi upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych[32].

Udostępnienie danych osobowych w zakresie zadłużenia w Kasie Rolniczego Ubezpieczenia Społecznego osobie trzeciej

Nieprawidłowości w procesie przetwarzania danych osobowych przez Kasę Rolniczego Ubezpieczenia Społecznego (KRUS), polegające na udostępnieniu danych osobowych skarżącej w zakresie jej zadłużenia w KRUS na rzecz osoby trzeciej, były przedmiotem kolejnej skargi do Prezesa UODO. Ustalono, że pracownica placówki terenowej KRUS przeprowadziła wizytację w gospodarstwie rolnym należącym do skarżącej w związku z jej zadłużeniem w opłacaniu składek na ubezpieczenie. Podczas wizytacji pracownica nie zastała jednak skarżącej i rozmowę przeprowadziła z jej matką. Pracownica KRUS poinformowała matkę skarżącej o posiadanym przez córkę zadłużeniu w opłacaniu składek i poprosiła, by córka skontaktowała się w sprawie zadłużenia z placówką terenową KRUS. Ponadto poprosiła matkę skarżącej o podpisanie protokołu z przeprowadzonej wizytacji.

W złożonych wyjaśnieniach KRUS przyznał, że podczas opisanej wyżej wizytacji pracownicy placówki terenowej KRUS w gospodarstwie rolnym należącym do skarżącej doszło do udostępnienia danych osobowych skarżącej w zakresie jej zadłużenia w KRUS matce skarżącej. KRUS przeprowadził w tej sprawie postępowanie wyjaśniające, w wyniku którego potwierdzono niewłaściwe zachowanie pracownicy placówki terenowej KRUS w Piasecznie i ustalono, że doszło do naruszenia przepisów dotyczących ochrony danych osobowych oraz procedur KRUS w zakresie przedmiotowego udostępnienia danych osobowych. W niniejszej sprawie Prezes UODO uznał, że udostępnienie przez KRUS danych osobowych skarżącej jej matce nie znajdowało oparcia w żadnej spośród przesłanek określonych w art. 6 ust. 1 RODO, która stanowiłaby o legalności tego procesu i nastąpiło tym samym bez podstawy prawnej.

Mając to na uwadze, Prezes UODO udzielił KRUS upomnienia w związku z zaistniałym naruszeniem art. 6 ust. 1 RODO[33].

Udostępnienie przez Zakład Ubezpieczeń Społecznych danych osobowych w zakresie informacji o niezdolności do pracy z tytułu choroby na rzecz podmiotów trzecich – byłego i nowego pracodawcy

Przedmiotem skargi było udostępnienie przez Zakład Ubezpieczeń Społecznych (ZUS) danych osobowych skarżącego w zakresie informacji o niezdolności do pracy z tytułu choroby na rzecz podmiotów trzecich – pracodawców, którzy w okresie choroby nie zatrudniali skarżącego.

Ustalono, że skarżący podlegał obowiązkowo ubezpieczeniom emerytalnemu i rentowemu, chorobowemu oraz wypadkowemu z tytułu zatrudnienia u byłego pracodawcy. Skarżący był niezdolny do pracy z powodu choroby. Do ZUS wpłynął wniosek skarżącego o zasiłek chorobowy za okres po ustaniu zatrudnienia. ZUS wystąpił do płatnika składek – byłego pracodawcy o przedłożenie zaświadczenia na druku Z-3 w celu

[32] DS.523.1044.2022.
[33] DS.523.5350.2021.

ustalenia prawidłowej podstawy wymiaru zasiłku chorobowego oraz wyrównania skarżącemu wypłaconego już zasiłku chorobowego. Udostępnienie danych osobowych skarżącego w postaci informacji o wypłaceniu mu zasiłku chorobowego za okres po ustaniu zatrudnienia u byłego pracodawcy nastąpiło w celu wezwania byłego pracodawcy do przedłożenia zaświadczenia ZUS Z-3 w związku z obowiązkiem ustalenia prawidłowej wysokości podstawy wymiaru zasiłku chorobowego przyznanego skarżącemu oraz wyrównania zasiłku już wypłaconego, a zatem nastąpiło w ramach realizacji obowiązku prawnego ciążącego na ZUS wynikającego z art. 61a ust. 1 i ust. 2 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa[34] oraz art. 68 ust. 1 lit. b ustawy o systemie ubezpieczeń społecznych[35]. Podstawę prawną udostępnienia danych osobowych skarżącego przez ZUS na rzecz byłego pracodawcy stanowił zatem w tym zakresie art. 9 ust. 2 lit. b) RODO.

Jak ustalono w sprawie, ZUS decyzją przyznał skarżącemu prawo do świadczenia rehabilitacyjnego, ale skarżący złożył rezygnację z tego świadczenia w związku z podjęciem zatrudnienia u nowego pracodawcy. Następnie ZUS wydał decyzję odmawiającą skarżącemu prawa do wypłaty z tytułu świadczenia rehabilitacyjnego. Decyzja została przesłana do skarżącego oraz do wiadomości płatnika składek, u którego skarżący podjął zatrudnienie. Zdaniem ZUS przekazanie do nowego płatnika składek danych osobowych skarżącego w postaci informacji o przyznanym świadczeniu rehabilitacyjnym miało na celu zapobieżenie wypłacie nienależnych świadczeń. W przypadku wystąpienia niezdolności do pracy skarżącemu nie przysługiwałoby bowiem prawo do zasiłku chorobowego w ramach nowego okresu zasiłkowego, tylko do świadczenia rehabilitacyjnego w ramach „poprzedniego" okresu zasiłkowego, gdyż świadczenie rehabilitacyjne jest przedłużeniem zasiłku chorobowego zgodnie z art. 9 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.

Prezes UODO uznał jednak, że ZUS nie wykazał w trakcie postępowania, aby udostępnienie danych osobowych skarżącego na rzecz nowego płatnika składek było niezbędne do realizacji ciążących na ZUS obowiązków prawnych. Podstawy takiej nie stanowił powołany przez ZUS art. 98 ust. 1 pkt 4 ustawy o systemie ubezpieczeń społecznych ani żaden z pozostałych przepisów ustawy o systemie ubezpieczeń społecznych oraz ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, na podstawie których ZUS realizuje swoje zadania. Udostępnienie danych osobowych na rzecz nowego pracodawcy skarżącego nie znajdowało zatem oparcia w żadnej spośród przesłanek określonych w art. 6 ust. 1 RODO – co do danych zwykłych ani w art. 9 ust. 2 RODO – co do danych osobowych szczególnej kategorii (dane dotyczące zdrowia), stanowiących o legalności przetwarzania (udostępnienia) danych osobowych, i tym samym nastąpiło bez podstawy prawnej. Prezes UODO uznał za zasadne skorzystanie w tej sprawie z instrumentu o charakterze naprawczym, przewidzianego w art. 58 ust. 2 lit. b) RODO i udzielił ZUS upomnienia za powyższe naruszenie[36].

---

[34] Ustawa z 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz. U. z 2023 r. poz. 2780).
[35] Ustawa z 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2024 r. poz. 497).
[36] DS.523.5494.2022.

Przetwarzanie danych osobowych w Krajowym Systemie Informacyjnym Policji

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

Prezes UODO wskazywał, że zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności, zostały określone w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[37]. Zgodnie z przepisami ww. ustawy Komendant Główny Policji może przetwarzać dane osobowe wyłącznie w zakresie niezbędnym do zrealizowania uprawnień bądź spełnienia obowiązków wynikających z przepisów prawa. Zakres uprawnień oraz ustawowych zadań organów Policji został określony w ustawie o Policji[38]. Do zadań ustawowych Policji należy m.in: ochrona bezpieczeństwa i porządku publicznego, inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców. W granicach ustawowych zadań Policja wykonuje czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze i administracyjno-porządkowe w celu rozpoznawania, zapobiegania i wykrywania przestępstw, przestępstw skarbowych i wykroczeń.

Organy Policji zgodnie z art. 20 ust. 1 ustawy o Policji, z zachowaniem ograniczeń wynikających z art. 19, są uprawnione do przetwarzania informacji, w tym danych osobowych. Przetwarzanie oraz wymiana informacji, w tym danych osobowych, może dotyczyć także danych osobowych, o których mowa w art. 14 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (tzw. danych osobowych wrażliwych), przy czym dane dotyczące wyników analizy kwasu deoksyrybonukleinowego (DNA) obejmują informacje wyłącznie o niekodującej części DNA (art. 20 ust. 1a ustawy o Policji). Stosownie do art. 20 ust. 2b ustawy o Policji informacje przez nią przetwarzane mogą obejmować: dane wrażliwe, z tym że dane dotyczące kodu genetycznego obejmują informacje wyłącznie o niekodującej części DNA, odciski linii papilarnych, zdjęcia, szkice i opisy wizerunku, cechy i znaki szczególne, pseudonimy, a także informacje o: miejscu zamieszkania lub pobytu, wykształceniu, zawodzie, miejscu i stanowisku pracy oraz sytuacji materialnej i stanie majątku, dokumentach i przedmiotach, którymi sprawca się posługuje, sposobie działania sprawcy, jego środowisku i kontaktach, sposobie zachowania się sprawcy wobec osób pokrzywdzonych.

Prezes UODO zwrócił uwagę, że powyższe nie oznacza możliwości nieograniczonego w czasie przetwarzania przez organy Policji danych osobowych gromadzonych w KSIP. Na gruncie przepisów obowiązującej ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości,

[37] Ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).
[38] Ustawa z 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145 ze zm.).

przetwarzane dane osobowe podlegają okresowej weryfikacji i usunięciu w przypadku uznania za niecelowe dalsze ich przetwarzanie. Komendant Główny Policji ma obowiązek dokonywania weryfikacji danych osobowych nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji tych danych. Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. W jednym z prowadzonych postępowań Komendant Główny Policji stwierdził dalszą zasadność przetwarzania danych osobowych skarżącego w KSIP[39]. Organy Policji dokonały stosownej weryfikacji gromadzonych w KSIP danych skarżącego, zgodnie z obowiązującymi w tym zakresie przepisami. Komendant Główny Policji dokonał weryfikacji danych po otrzymaniu informacji o zakończeniu postępowań w sprawach przeciwko skarżącemu. Dodatkowych weryfikacji tych danych Komendant Główny Policji dokonał w związku z otrzymanym wnioskiem skarżącego o usunięcie jego danych osobowych z KSIP, a także w związku ze skargą skarżącego do Prezesa UODO. Weryfikacji dokonano w szczególności pod kątem przesłanek z art. 51 ust. 4 Konstytucji RP oraz pod kątem legalności i celowości przetwarzania danych osobowych. Organy Policji dokonując powyższych weryfikacji, zgodnie z przepisami rozdziału 15 zarządzenia nr 70 Komendanta Głównego Policji z 2 grudnia 2019 r., uwzględniły m.in. czas, który upłynął od momentu wprowadzenia informacji, w tym danych osobowych, do zbiorów danych KSIP do momentu dokonywania oceny, oraz aktualność przesłanek legalności i niezbędności dalszego przetwarzania informacji, w tym danych osobowych, do wykonania zadań ustawowych Policji. Ze zgromadzonego materiału dowodowego w sprawie wynikało, iż Komendant stwierdził dalszą zasadność przetwarzania danych osobowych skarżącego w KSIP i w wyjaśnieniach wskazał, że ustawowym celem przetwarzania tych danych osobowych jest zapobieżenie popełnieniu przez niego w przyszłości przestępstwa, jak również – w przypadku niemożności zapobieżenia – wykrycie go. W związku z naruszeniem norm prawnokarnych przez skarżącego oraz rodzajem norm naruszonych, Komendant Główny Policji uznał, że nie można stwierdzić, że dane osobowe skarżącego stały się zbędne dla realizacji zadań Policji, zwłaszcza wymienionych w art. 1 ust. 2 ustawy o Policji, m.in. ochrony życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra. Komendant Główny Policji podkreślił, że przetwarzanie to ma na celu po pierwsze uniemożliwienie ponownego popełnienia takiego czynu, po drugie zaś właściwe dokonywanie dalszych prognoz kryminologicznych oraz czynności analitycznych, a także pełną realizację ustawowych zadań Policji.

W ocenie Prezesa UODO w omawianej sprawie brak było podstaw do stwierdzenia, że dane osobowe skarżącego są przetwarzane przez Komendanta Głównego Policji w sposób niezgodny z ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, wobec czego Prezes UODO odmówił uwzględnienia wniosku skarżącego.

Udostępnienie przez Policję na rzecz państwowego powiatowego inspektora sanitarnego danych osobowych osoby, która nie zakryła ust i nosa maseczką

Kolejne postępowanie administracyjne toczyło się w sprawie udostępnienia przez komendanta miejskiego policji na rzecz państwowego powiatowego inspektora

[39] DS.523.4287.2022.

sanitarnego danych osobowych osoby, która nie zakryła ust i nosa maseczką. W sprawie tej ustalono, że w kwietniu 2021 r. policjanci podjęli interwencję w stosunku do skarżącego, który nie chciał założyć maseczki i sporządzili „Notatkę urzędową dot. naruszeń nakazów, zakazów lub ograniczeń związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19", zawierającą opis działań Policji z udziałem skarżącego. W treści ww. notatki wskazano również, że zachowanie skarżącego narusza przepisy prawa dotyczące nakazu zakrywania ust i nosa maseczką. Notatka została sporządzona według opracowanego przez Komendanta Głównego Policji wzoru notatki dla potrzeb związanych z COVID-19. Komendant miejski policji w złożonych w sprawie wyjaśnieniach poinformował, że ww. notatka została wysłana do państwowego powiatowego inspektora sanitarnego celem sprawdzenia, czy skarżący nie przebywa na kwarantannie lub izolacji. Prezes UODO ustalił również, że państwowy powiatowy inspektor sanitarny, w związku z notatką urzędową przesłaną przez Policję, wszczął z urzędu postępowanie administracyjne w sprawie wymierzenia skarżącemu administracyjnej kary pieniężnej z tytułu naruszenia przepisów zawartych w § 25 ust. 1 pkt 2 lit. d) rozporządzenia w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[40].

W wydanej w tej sprawie decyzji administracyjnej Prezes UODO uznał, że do oceny działania komendanta miejskiego policji należy zastosować przepisy ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[41], bowiem zebrany w sprawie materiał dowodowy wskazywał, że dane osobowe skarżącego zostały zebrane przez Policję w ramach czynności ukierunkowanych na ukaranie skarżącego za popełnienie wykroczenia. Prezes UODO uznał również, że celem udostępnienia na rzecz państwowego powiatowego inspektora sanitarnego danych osobowych skarżącego zawartych w treści notatki, było dostarczenie ww. organowi informacji potrzebnych do wszczęcia postępowania administracyjnego w sprawie wymierzenia skarżącemu administracyjnej kary pieniężnej za naruszenie nakazu zakrywania ust i nosa maseczką. Niemniej dostarczenie przedmiotowej informacji państwowemu powiatowemu inspektorowi sanitarnemu nie należy do celów wskazanych w art. 1 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, co oznacza, że dopuszczalność udostępnienia danych osobowych skarżącego należy ocenić przez pryzmat przesłanki określonej w art. 13 ust. 3 ww. ustawy, czyli zbadać, czy w dniu udostępnienia danych osobowych przepisy prawa zezwalały na takie udostępnienie. Prezes UODO uznał, że art. 14 ust. 1 i ust. 2 ustawy o Policji nie są w rozstrzyganej sprawie przepisami zezwalającymi na udostępnienie danych osobowych. Podkreślił przy tym, że obowiązek, o którym mowa w art. 14 ust. 2 ustawy o Policji, czyli obowiązek działania przez Policję na polecenie sądu, prokuratora, organów administracji państwowej i samorządu terytorialnego, musi wynikać z przepisów rangi ustawowej, a zatem nie może on być skutkiem np. wyłącznie ustaleń (porozumień, umów) pomiędzy organami lub jednostkami organizacyjnymi Policji a organami Państwowej Inspekcji Sanitarnej, oraz że w ocenie Prezesa UODO również pozostałe przepisy ustawy o Policji oraz przepisy innych aktów prawa nie zezwalały na

[40] Rozporządzenie Rady Ministrów z 19 marca 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz. U. z 2021 r. poz. 512 ze zm.).
[41] Ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

udostępnienie przez komendanta miejskiego policji danych osobowych skarżącego na rzecz państwowego powiatowego inspektora sanitarnego w okolicznościach, w jakich to nastąpiło. W oparciu o powyższe okoliczności Prezes UODO stwierdził, że udostępnienie danych osobowych skarżącego zawartych w treści notatki urzędowej naruszyło przepisy o ochronie danych osobowych. Z uwagi jednak na fakt, że udostępnienie danych osobowych skarżącego już nastąpiło i jest procesem nieodwracalnym, Prezes UODO nie mógł skorzystać ze swojego uprawnienia określonego w art. 8 ust. 2 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (nakazać przywrócenie stanu zgodnego z prawem). Wobec tego Prezes UODO odmówił uwzględnienia wniosku skarżącego[42].

1.1.2. Sektor prywatny

Udostępnienie na rzecz pozostałych członków wspólnoty mieszkaniowej danych osobowych skarżącej zawartych we wniesionym przez nią pozwie o uchylenie uchwał ww. wspólnoty

Przedmiotem innej skargi było udostępnienie danych osobowych skarżącej w postaci numeru PESEL, stałego adresu zamieszkania i numeru rachunku bankowego, zawartych we wniesionym przez nią pozwie o uchylenie uchwał wspólnoty mieszkaniowej, na rzecz pozostałych członków ww. wspólnoty. W trakcie postępowania ustalono, że skarżąca jest członkiem wspólnoty mieszkaniowej. Zarządca nieruchomości wspólnej, działając w imieniu wspólnoty mieszkaniowej, przesłał za pośrednictwem poczty elektronicznej (e-mail) do wszystkich członków tej wspólnoty informację o wniesieniu przez skarżącą przeciwko ww. wspólnocie pozwu do sądu o uchylenie uchwał wspólnoty mieszkaniowej. Do wiadomości e-mail został załączony skan pozwu wraz z załącznikami. Zarządca nieruchomości wspólnej wyjaśnił, że udostępnienie danych osobowych skarżącej zawartych w pozwie nastąpiło na podstawie przepisów ustawy o własności lokali[43] – art. 27, art. 29, art. 26 oraz 30 ust. 2 pkt 3 ww. ustawy. Zarządca nieruchomości wspólnej wyjaśnił również, że do sprawowania kontroli nad działalnością zarządu niezbędny jest dostęp do informacji o sprawach związanych z zarządzaniem nieruchomością wspólną, a członkowie wspólnoty mają prawo do otrzymywania tych informacji od zarządu (lub zarządcy).

W tej sprawie działanie zarządcy nieruchomości wspólnej oceniano m.in. przez pryzmat art. 27 ustawy o własności lokali, który gwarantuje każdemu właścicielowi lokalu prawo i obowiązek współdziałania w zarządzie nieruchomością wspólną oraz art. 29 ust. 3 ww. ustawy, zgodnie z którym prawo kontroli działalności zarządu służy każdemu właścicielowi lokalu. Prezes UODO w wydanej w sprawie decyzji administracyjnej uznał, że udostępnienie będących przedmiotem skargi danych osobowych skarżącej, zawartych we wniesionym przez nią pozwie o uchylenie uchwał wspólnoty mieszkaniowej, na rzecz pozostałych członków tej wspólnoty nie było niezbędne do realizacji celu, jakim było powiadomienie członków ww. wspólnoty o wniesieniu przeciwko niej pozwu. Zdaniem Prezesa UODO udzielenie ww. informacji członkom wspólnoty możliwe było bez udostępniania danych osobowych skarżącej, których dotyczyła skarga wniesiona przez nią

[42] DS.523.3032.2021.
[43] Ustawa z 24 czerwca 1994 r. o własności lokali (Dz. U. z 2021 r. poz. 1048).

do Prezesa UODO. Udostępnienie to nie znajdowało oparcia w żadnej z przesłanek z art. 6 ust. 1 RODO oraz naruszało zasady określone w art. 5 ust. 1 lit. a) oraz c) RODO (zasada zgodności z prawem oraz zasada minimalizacji danych). Za działania zarządcy nieruchomości wspólnej, działającego jako podmiot przetwarzający dane w imieniu administratora, odpowiedzialna jest zaś wspólnota mieszkaniowa, jako administrator danych osobowych skarżącej. To ta wspólnota zobowiązana była zapewnić, że dane osobowe skarżącej będą przetwarzane zgodnie z prawem i w zakresie ograniczonym do tego, co niezbędne dla realizacji celów przetwarzania. Prezes UODO skorzystał z instrumentu o charakterze naprawczym przewidzianego w art. 58 ust. 2 lit. b) RODO i skierował do wspólnoty mieszkaniowej, jako administratora danych skarżącej, upomnienie za udostępnienie danych osobowych skarżącej w postaci numeru PESEL, stałego adresu zamieszkania i numeru rachunku bankowego na rzecz pozostałych członków ww. wspólnoty bez podstawy prawnej[44].

Prawo dostępu do danych a monitoring wizyjny

W jednej ze spraw[45] skarżący zwrócił się do wspólnoty mieszkaniowej z wnioskiem o udostępnienie mu kopii danych osobowych obejmujących jego wizerunek zarejestrowany za pomocą monitoringu wizyjnego w obrębie nieruchomości należącej do wspólnoty. Skarżący we wniosku podał podstawę prawną żądania, a także szczegółowe informacje dotyczące wnioskowanych danych osobowych (data i godzina, rodzaj kamer, a także określenie ubioru wnioskodawcy). Wspólnota odmówiła skarżącemu udostępnienia wnioskowanych kopii danych osobowych ze względu na prawa i wolności innych osób wskazując, że zapis z monitoringu może obejmować nie tylko wizerunek skarżącego, ale również innych osób. Ponadto wskazała, że skarżący nie przedstawił uzasadnionego interesu uzyskania kopii jego danych osobowych. W tej sprawie znaczenie miało, że art. 15 ust. 3 RODO nakłada na administratora obowiązek dostarczenia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu. Administrator danych osobowych, także tych pozyskiwanych za pomocą monitoringu wizyjnego, ma zaś obowiązek zagwarantowania osobom, których dane są przetwarzane, możliwości realizowania ich uprawnień, wynikających z RODO.

Prezes UODO nie podzielił stanowiska wspólnoty mieszkaniowej dotyczącego uzależniania udostępnienia kopii danych na podstawie art. 15 ust. 3 RODO od wykazania interesu, czy celu, w jakim zainteresowany zwraca się z wnioskiem o udostępnienie kopii danych osobowych obejmujących jego wizerunek zarejestrowany za pomocą monitoringu wizyjnego. Zgodnie z przepisami RODO osoba, której dane dotyczą, ma prawo dostępu do swoich danych osobowych, a administrator danych dostęp ten powinien jej zapewnić we wnioskowanym zakresie. Art. 15 ust. 3 RODO nakłada na administratora obowiązek dostarczenia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu, przy czym przepis ten nie upoważnia administratora do żądania wykazania przez osobę, której dane dotyczą jakichkolwiek interesów lub celów uzyskania kopii danych. Ponadto w ocenie Prezesa UODO uznanie, że udostępnienie kopii danych może powodować naruszenie praw i wolności osób trzecich nie stanowi podstawy do odmowy realizacji prawa osoby, której dane dotyczą, wskazanego w art. 15 ust. 3 RODO.

[44] DS.523.505.2021.
[45] DS.523.6315.2020.

Obowiązkiem administratora jest bowiem wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających realizację tych uprawnień.

Kwestionowany przez skarżącego proces przetwarzania jego danych osobowych naruszył przepisy art. 15 ust. 3 RODO. W analizowanej sprawie Prezes UODO, wobec ustalenia, że wnioskowane dane nie są aktualnie przetwarzane przez wspólnotę mieszkaniową, udzielił jej upomnienia w związku z bezpodstawną odmową udostępnienia skarżącemu kopii jego danych.

Udostępnienie danych osobowych skarżącej innym członkom wspólnoty mieszkaniowej w wiadomości e-mail wysłanej przez zarządcę nieruchomości wspólnej

Przedmiotem innej skargi było udostępnienie danych osobowych skarżącej w wiadomości e-mail wysłanej przez zarządcę nieruchomości wspólnej członkom wspólnoty mieszkaniowej, której skarżąca była członkiem. Zarządca nieruchomości wspólnej, działając w imieniu wspólnoty mieszkaniowej, udostępnił dane osobowe skarżącej w zakresie imienia, nazwiska, numeru lokalu (adres), adresu e-mail oraz informacji dotyczących zadłużenia względem ww. wspólnoty w korespondencji elektronicznej (e-mail) skierowanej do właścicieli lokali we wspólnocie mieszkaniowej. Zarządca nieruchomości wspólnej wskazywał, że historia zadłużenia skarżącej została przedstawiona właścicielom lokali na podstawie art. 27 wspomnianej już ustawy o własności lokali w celu przedstawienia członkom wspólnoty mieszkaniowej przebiegu windykacji zadłużenia wobec tej wspólnoty. Art. 27 ww. ustawy gwarantuje każdemu właścicielowi lokalu prawo i obowiązek współdziałania w zarządzie nieruchomością wspólną. Zgodnie z art. 29 ust. 3 ustawy o własności lokali prawo kontroli działalności zarządu służy każdemu właścicielowi lokalu.

Prezes UODO uznał, że brak było podstaw prawnych do udostępnienia danych osobowych skarżącej na rzecz pozostałych członków wspólnoty mieszkaniowej w celu poinformowania ich o przebiegu windykacji zadłużenia w ww. wspólnocie. Żaden przepis prawa, w szczególności ustawy o własności lokali, nie nakładał na ww. wspólnotę obowiązku, którego realizacja wymagałaby udostępnienia danych osobowych skarżącej w zakwestionowany przez nią sposób. Wskazane przez zarządcę nieruchomości wspólnej przepisy ustawy o własności lokali: art. 27, art. 29, art. 26 oraz art. 30 ust. 2 pkt 3 ww. ustawy, nie kreują po stronie wspólnoty mieszkaniowej obowiązków prawnych, których realizacja wymagałaby udostępnienia danych osobowych skarżącej w ww. zakresie na rzecz pozostałych członków tej wspólnoty. Udostępnienie danych osobowych skarżącej nie znajdowało zatem oparcia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO stanowiących o legalności przetwarzania (udostępnienia) danych osobowych i tym samym nastąpiło bez podstawy prawnej, a ponadto naruszało zasadę określoną w art. 5 ust. 1 lit. c) RODO (zasada minimalizacji danych). Ponieważ za działania zarządcy nieruchomości wspólnej, działającego jako podmiot przetwarzający, odpowiedzialna jest wspólnota mieszkaniowa, jako administrator danych osobowych skarżącej, Prezes UODO uznał za zasadne skorzystanie z instrumentu o charakterze naprawczym, przewidzianego w art. 58 ust. 2 lit. b) RODO, i skierował do wspólnoty upomnienie[46] za zaistniałe naruszenie.

[46] DS.523.2979.2020.

Udostępnienie przez wspólnotę mieszkaniową i spółdzielnię mieszkaniową danych osobowych skarżącego osobom nieuprawnionym na tablicy ogłoszeń na klatce schodowej bloku

Prezes UODO rozpatrywał również skargę na udostępnienie przez wspólnotę mieszkaniową i spółdzielnię mieszkaniową danych osobowych skarżącego osobom nieuprawnionym na tablicy ogłoszeń na klatce schodowej bloku. Skarżący był członkiem wspólnoty mieszkaniowej. Pomiędzy wspólnotą mieszkaniową a spółdzielnią mieszkaniową została zawarta umowa o zarządzanie nieruchomością. Wspólnota mieszkaniowa wywiesiła na tablicy ogłoszeń na klatce schodowej bloku informację o podjęciu uchwały w sprawie przeznaczenia środków z konta eksploatacyjnego na wynagrodzenie adwokata w postępowaniu karnym przeciwko skarżącemu, w której udostępniono dane osobowe skarżącego w postaci imienia i nazwiska. Wspólnota mieszkaniowa wyjaśniła, że udostępniła na tablicy ogłoszeń na klatce schodowej bloku ww. dane osobowe skarżącego w celu poinformowania członków wspólnoty mieszkaniowej o treści podjętej przez tę wspólnotę uchwały, ponieważ była do tego prawnie zobligowana zgodnie z art. 23 ust. 3 ustawy o własności lokali.

Prezes UODO uznał, że udostępnienie przez wspólnotę mieszkaniową danych osobowych skarżącego w miejscu ogólnodostępnym na klatce schodowej w budynku nie znajdowało oparcia w przesłance określonej w art. 6 ust. 1 lit. c) RODO. Ponadto żadna z pozostałych przesłanek określonych w art. 6 ust. 1 RODO nie znajdowała zastosowania w tej sprawie. Udostępnienie to było również nadmiarowe w stosunku do realizowanego celu, co stanowiło naruszenie art. 6 ust. 1 w zw. z art. 5 ust. 1 lit. c) RODO. Prezes UODO skierował do wspólnoty mieszkaniowej upomnienie[47] w związku z zaistniałym naruszeniem.

Przetwarzanie danych jako następstwo zawartych umów

Częstym powodem składanych skarg było przekonanie, że dane osobowe mogą być przetwarzane wyłącznie za zgodą podmiotu danych. Tymczasem nie tylko zgoda, ale również inne przesłanki, w tym np. zawarta umowa, może stanowić legalną przesłankę przetwarzania danych osobowych. Zawarcie umowy nierozerwalnie wiąże się z ich przetwarzaniem nie tylko na etapie jej zawierania, określenia jej stron, czy podjęcia działań koniecznych przed jej zawarciem, ale również na późniejszym etapie – wykonania, a po wykonaniu dodatkowo dane mogą być przetwarzane w celach podatkowych, czy księgowych. Przetwarzanie to musi jednak pozostawać w ścisłej relacji z tą umową i być konieczne do jej realizacji. Odnosząc się do samej zgody na przetwarzanie danych osobowych zwykłych, należy zauważyć, że nie zawsze musi ona przybrać formę pisemną. Zgoda może być również wyrażona m.in. poprzez oświadczenie lub wyraźne działanie przyzwalające.

W jednej z takich spraw przedmiotem swojej skargi[48] skarżąca uczyniła brak podstaw prawnych do przetwarzania jej danych osobowych przez spółkę w dwóch sytuacjach, tj. poprzez nagranie wideo na zajęciach szkoleniowych oraz publikację zdjęcia grupowego

[47] DS.523.3042.2021.
[48] DS.523.5.2023.

z wizerunkiem skarżącej na profilu społecznościowym spółki. Skarżąca oświadczyła, że nie wyrażała zgody na tego rodzaju przetwarzanie jej danych osobowych.

Prezes UODO ustalił, że skarżąca zawarła ze spółką umowę o świadczenie usług polegającą na przeprowadzeniu szkolenia. Jednym z elementów zajęć jest praca z kamerą, o czym kursanci są wcześniej informowani. Skarżąca aktywnie uczestniczyła, w tym przygotowała rzeczone nagranie. Nagrania przygotowywane przez kursantów były następnie analizowane i oceniane pod względem merytorycznym przez prowadzącego, a następnie kasowane. Odnośnie do zdjęcia grupowego spółka wyjaśniła, że było to zdjęcie uczestników szkolenia. Miało charakter spontaniczny i na zasadzie dobrowolnego udziału. Prowadzący zapytał, czy ktoś zgłasza uwagi do wykonania i opublikowania zdjęcia na profilu spółki. Ostatecznie, w wyniku otrzymania żądania usunięcia jej danych, spółka usunęła zdjęcie.

Prezes UODO uznał, że nie można przyjąć, że nagrywanie kamerą było dokonywane w sposób nadmiarowy i nieadekwatny, nie było też dokonywane w sposób podstępny i z ukrycia. Zgodnie z praktyką spółki nagrania są kasowane po zajęciach, po spełnieniu celu dydaktycznego ćwiczenia dokonywanego w ramach szkolenia. Jak wskazała skarżąca, po odtworzeniu nagrania, które przygotowała, została upokorzona przez prowadzącego na forum całej grupy. Poczucie skarżącej co do niewłaściwej oceny lub zachowania osoby prowadzącej zajęcia nie wpływa na legalność tego przetwarzania i nie może być rozpatrywane jako naruszenie prawa do ochrony danych osobowych, lecz dóbr osobistych. Prezes UODO nie ma jednak uprawnień do wydawania decyzji administracyjnej w takim zakresie.

Odnosząc się do drugiej sytuacji, Prezes UODO zauważył, że złożenie oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych zwykłych nie wymaga żadnej szczególnej formy. Zgoda może przybrać formę oświadczenia lub wyraźnego działania potwierdzającego przyzwolenie na przetwarzanie dotyczących jej danych osobowych. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Spółka na zasadach dobrowolności praktykuje wykonywanie zdjęcia grupy uczestniczącej w szkoleniu. Prowadzący poinformował o zamiarze zamieszczenia tego zdjęcia na profilu społecznościowym spółki. Nie jest to praktyka zaskakująca dla uczestników szkoleń grupowych, warsztatowych. Zdaniem Prezesa UODO skarżąca wyraziła akceptację dla takiego przetwarzania poprzez jednoznaczne działanie przyzwalające (pozowanie do zdjęcia, w którym jej wizerunek był częścią większej grupy). Nie można było zatem zgodzić się, że zdjęcie zostało zrobione i opublikowane bez jej zgody.

Prezes UODO uznał, że przetwarzanie danych osobowych skarżącej w zakresie jej wizerunku za pomocą kamery na zajęciach szkoleniowych miało podstawę prawną w art. 6 ust. 1 lit. b) rozporządzenia 2016/679, gdyż było niezbędne do wykonania umowy, której stroną była skarżąca. Z kolei publikacja zdjęcia z wizerunkiem skarżącej na profilu społecznościowym spółki odbyła się na podstawie wynikającej z art. 6 ust. 1 lit. a) rozporządzenia 2016/679, tj. zgody skarżącej.

W innej sprawie[49] skarżąca zawarła umowę sprzedaży i podjęła działania w celu odstąpienia od niej z powodu wad rzeczy. Zarzuciła przedsiębiorcy niespełnienie wobec

[49] DS.523.1649.2021.

niej obowiązku informacyjnego wynikającego z art. 13 rozporządzenia 2016/679, w szczególności niepoinformowania jej o okresie przetwarzania danych (retencji), celach przetwarzania oraz ewentualnych skutkach braku zgody na przetwarzanie jej danych. Skarżąca podkreśliła, że nie poinformowano jej również o możliwości cofnięcia zgody na przetwarzanie danych.

W przedmiotowej sprawie Prezes UODO ustalił, że obowiązek informacyjny został dopełniony w treści umowy i załączniku do niej. Na umowie widnieje podpis skarżącej, zatem należało przyjąć, że przed podpisaniem niniejszej umowy sprzedaży skarżąca zapoznała się z jej treścią. Prawodawca nie narzuca administratorowi żadnej szczególnej formy, w której obowiązek informacyjny ma zostać spełniony wobec podmiotu danych. Dopuszczalne jest zatem udzielenie określonych w art. 13 informacji zarówno na piśmie, jak i w każdy inny sposób. Prezes UODO odmówił uwzględnienia skargi. Postępowanie wykazało, że nie doszło do naruszenia przepisów o ochronie danych osobowych.

W kolejnej opisywanej sprawie[50] skarżąca złożyła skargę na nieprawidłowości w procesie przetwarzania jej danych osobowych, polegające na przetwarzaniu ich w serwisie internetowym wideo bez podstawy prawnej i pomimo wniesionego żądania usunięcia danych osobowych. Ze względu na zawartą umowę skarżąca wskazywała, że ma utrudnioną możliwość skorzystania z prawa do usunięcia jej danych osobowych.

Skarżąca wzięła udział w konkursie. W tym celu podpisała stosowną umowę z organizatorem, który opublikował w serwisie wideo nagranie z wizerunkiem skarżącej wraz z jej imieniem, nazwiskiem, wiekiem, wzrostem i miastem zamieszkania. Skarżąca była poinformowana o celu nagrania oraz formach jego rozpowszechniania. Z umowy wynikało, że skarżąca udzieliła organizatorowi zgody na rozpowszechnianie jej wizerunku i danych w związku i w celu realizacji zawartej umowy o współpracy. Podpisując stosowną umowę, zgodziła się na jej warunki. Z tego powodu nie sposób było stwierdzić, że przetwarzanie danych osobowych skarżącej odbywa się niezgodnie z prawem, a tym bardziej, że można odstąpić od wykonania umowy, odwołując zgodę na przetwarzanie danych. Przesłanki, o których mowa w art. 6 ust. 1 rozporządzenia 2016/679, są równoważne, co oznacza, że posiadanie jednej z nich, w tym przypadku określonej w art. 6 ust. 1 lit. b), determinuje legalność przetwarzania danych. Prezes UODO odmówił uwzględnienia skargi.

Prawo dostępu do danych

Przedmiotem wielu spraw rozpoznawanych przez Prezesa UODO były nieprawidłowości w realizacji prawa dostępu do danych. Ze względu na trudności w określeniu zakresu i ram tego prawa jest to temat trudny zarówno dla administratorów danych osobowych, jak również dla samych podmiotów danych. W pracy organu spotkać można sprawy, w których administratorzy niesłusznie odmawiali prawa dostępu do danych. Rozpatrywano również takie sprawy, w których osoby, których dane dotyczą, wykraczały swoim żądaniem poza zakres swojego uprawnienia. Zgodnie z art. 15 ust. 1 rozporządzenia 2016/679 osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy w ogóle są przetwarzane jakiekolwiek dane osobowe jej dotyczące, a jeżeli tak, to powinna jej zostać udzielona stosowna informacja na temat ich

[50] DS.523.5481.2022.

przetwarzania. Prawidłowe i rzetelne wypełnienie tego obowiązku jest niezbędne do zapewnienia osobie, której dane osobowe dotyczą, kontroli prawidłowości procesu przetwarzania jej danych. Ze względu na wydane w 2023 r. orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w tej materii oraz wytyczne Europejskiej Rady Ochrony Danych (EROD) należy uznać, że prawo dostępu do danych jest niezwykle ważnym zagadnieniem.

W jednej ze spraw[51] skarżąca próbowała bezskutecznie skorzystać z prawa dostępu do danych w celu uzyskania informacji na temat okoliczności przetwarzania jej danych osobowych. Skarżąca kilkukrotnie zwracała się do spółki z żądaniem dostępu do danych w zakresie informacji dotyczących długości czasu przechowywania danych osobowych w formie nagrań rozmów telefonicznych pomiędzy nią a infolinią spółki oraz o udzielenie informacji związanych z zakresem dostępu do danych przez ekspedientów sklepów stacjonarnych spółki. Skarżąca nie uzyskała żądanych informacji.

W toku przeprowadzonego przez Prezesa UODO postępowania spółka wyjaśniła, że udzielając odpowiedzi na żądanie skarżącej napotkała na problemy z identyfikacją osoby, od której pochodzi żądanie. Trudności były związane z wielokrotnymi zmianami danych na koncie klienta, włącznie ze zmianą danych kontaktowych, a obecnie dane zostały tak zmodyfikowane, że prawdopodobnie są w większości fikcyjne. Z uwagi na bardzo wąski zakres danych, jakie spółka zbiera na temat swoich klientów, identyfikacja jest zasadniczo możliwa tylko w oparciu o adres e-mail, który stanowi jedyny unikalny identyfikator klienta na potrzeby obsługi sklepu i programu lojalnościowego. Dodatkowo spółka doszła do wniosku, że skarżąca prawdopodobnie nigdy nie posługiwała się w relacjach ze spółką prawdziwym nazwiskiem, pod którym wystąpiła ze skargą do organu.

Prezes UODO przypomniał, że złożenie wniosku o realizację prawa dostępu do danych, zależnie od jego treści, zobowiązuje administratora danych do udzielenia pełnych informacji o procesie przetwarzania danych w zakresie nie węższym niż przewiduje powołany przepis art. 15 ust. 1 rozporządzenia 2016/679. Przepis ten określa minimum informacji, jakie administrator danych zobligowany jest przekazać wnioskodawcy, co nie oznacza, że zakres podawanych informacji nie może być większy niż wskazany w tym przepisie, zwłaszcza gdy ich podanie nie koliduje z interesem administratora danych i mogą być one w prosty sposób wyselekcjonowane i przekazane.

Prezes UODO zauważył, że realizacja żądania prawa podmiotu danych musi być poprzedzona identyfikacją osoby występującej z żądaniem[52]. Określenie sposobu identyfikacji osób realizujących prawa wynikające z rozporządzenia 2016/679 należy do administratora. Spółka powinna przyjąć takie rozwiązania techniczne i organizacyjne, aby nie dopuścić do sytuacji, w której utrudniona jest weryfikacja tożsamości osoby, której dane dotyczą. Jeżeli natomiast informacje przekazane przez osobę wnioskującą byłyby niewystarczające do ustalenia jej uprawnień, spółka powinna poprosić ją o dodatkowe informacje, na podstawie których uzyskałaby pewność co do jej tożsamości. Administrator danych na uwadze winien mieć jednak wyrażoną w art. 5 ust. 1 lit. c) rozporządzenia

[51] DS.523.1179.2020.

[52] Zgodnie z art. 12 ust. 6 rozporządzenia 2016/679, zgodnie z którym, bez uszczerbku dla art. 11, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

2016/679 zasadę minimalizacji danych. Zgodnie z tą zasadą, administrator nie tylko jest zobowiązany do tego, aby ustalić zakres niezbędnych danych, ale również, aby poddać szczegółowej analizie poszczególne ich kategorie, w celu wyeliminowania danych potencjalnie nadmiarowych, czyli takich, których przetwarzanie nie jest niezbędne w danym procesie przetwarzania.

Odnośnie do żądania nakazania spółce udzielenia informacji o zakresie dostępu do danych przez ekspedientów sklepów stacjonarnych spółki, Prezes UODO odmówił uwzględnienia skargi. Prezes UODO zauważył, że żądanie w tym zakresie dotyczy ogólnych praktyk stosowanych przez spółkę w zakresie przetwarzania danych osobowych oraz stosowanych procedur bezpieczeństwa. Celem skargi jest przywrócenie stanu zgodnego z prawem z uwagi na stwierdzone naruszenie praw osoby, której dane dotyczą, w zakresie naruszenia prawa dostępu do danych. Skarga złożona w sprawie indywidualnej nie służy nakazaniu dokonania ujawnienia zabezpieczeń danych osobowych na wniosek osoby, czy też ujawniania metodyki organizacji pracy danego administratora. Ocena prawidłowości czy kontrola stosowanych przez określonego administratora ogólnych praktyk może nastąpić w ramach postępowania administracyjnego prowadzonego przez organ nadzorczy z urzędu. Osobie, której dane dotyczą przysługują zaś prawa, o których mowa w rozdziale III rozporządzenia 2016/679, w tym prawo do informowania o przetwarzaniu danych, lecz nie do wszystkich informacji z nim związanych. Prawo dostępu do danych nie jest obowiązkiem bezwzględnym i jako taki może podlegać ograniczeniu. Administrator danych jest podmiotem, który z natury prowadzonej działalności musi ową działalność organizować „wewnętrznie", tzn. w ramach pewnej autonomii organizacji, którą ma też prawo chronić przed dostępem do niej chociażby podmiotów konkurencyjnych. W tej sprawie Prezes UODO nie dostrzegł interesu skarżącej w uzyskaniu wnioskowanych informacji. Przyjęcie przeciwnego stanowiska oznaczałoby możliwość zapoznania się ze sposobem zabezpieczenia danych przez administratora danych osobowych, co może powodować zmniejszenie poziomu ochrony danych[53]. Spółka zasadnie nie udzieliła tych informacji, jednakże stosownie do art. 12 ust. 4 rozporządzenia 2016/679, spółka zobowiązana była poinformować skarżącą niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – o powodach niepodjęcia działań w odniesieniu do przedmiotowego żądania skarżącej oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem, czego spółka w niniejszej sprawie nie uczyniła. Spółka nie przedstawiła niebudzących wątpliwości dowodów zrealizowania prawa dostępu do danych. Skarżąca nie wiedziała, czy spółka zignorowała jej żądanie, co zmusiło ją do egzekwowania swoich praw poprzez złożenie skargi do organu nadzorczego.

Prezes UODO nakazał spółce wypełnienie obowiązku informacyjnego wynikającego z art. 15 ust. 1 rozporządzenia 2016/67, w zakresie żądania skarżącej o udzielenie informacji o okresie przechowywania danych pochodzących z nagranej rozmowy, odbiorcach danych i sposobach ich przetwarzania oraz udzielił upomnienia za naruszenie polegające na nieudzieleniu odpowiedzi na wniosek w ustawowym terminie, a także o powodach nieudzielenia informacji, w tym o prawie wniesienia skargi do organu

[53] Zob. m.in. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 7.01.2016 r. sygn. akt II SA/Wa 1238/15.

nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem (art. 12 ust. 4 rozporządzenia 2016/679).

Obowiązek współpracy podmiotu przetwarzającego i administratora danych

Administrator danych osobowych samodzielnie decyduje o celach i środkach przetwarzania danych osobowych. W realizacji swoich celów może on korzystać z pomocy wyspecjalizowanych podmiotów oferujących określone narzędzia lub wiedzę. Na mocy stosownej umowy powierzenia administrator powierza (zleca) podmiotowi przetwarzającemu przetwarzanie zgromadzonych przez administratora danych osobowych. Przetwarzanie to dokonywane jest w imieniu i na rzecz administratora, jest działaniem prawnie dopuszczalnym i nie stanowi nieuprawnionego udostępnienia danych.

Jak wynika z obserwowanej praktyki UODO, strony takiej umowy często nie określają szczegółowo zasad współpracy między sobą, tj. powinności w związku z realizacją praw osób, których dane dotyczą. Efektem jest np. niespełnienie obowiązku informacyjnego w wyniku braku komunikacji przekazującej żądanie do właściwego podmiotu lub spełnienie go w sposób wprowadzający w błąd co do tożsamości administratora. Szczególną uwagę powinni zwrócić uwagę przedsiębiorcy korzystający z platform internetowych pomagających im w realizacji ich działalności gospodarczej, ponieważ to ostatecznie administrator odpowiada za prawidłowe przetwarzanie danych osobowych. Jednocześnie podmioty profesjonalne niekiedy występują w podwójnej roli, podmiotu przetwarzającego, ale również jako samodzielny administrator. Popełnione błędy w komunikacji mogą powodować eskalację problemu i konieczność angażowania organu nadzorczego, pomimo że sprawy te mogłyby zostać rozwiązane na etapie pierwszego kontaktu osoby, której dane dotyczą, bądź z administratorem, bądź z podmiotem przetwarzającym.

W jednej z takich spraw[54] skarżący wskazał, że otrzymał od spółki wiadomość marketingową, na którą nie wyrażał zgody. Skarżący zwrócił się do spółki na wskazany w tym celu adres e-mail z żądaniem przesłania kopii jego danych osobowych oraz ich usunięcia. Spółka udzieliła skarżącemu odpowiedzi, że na podany przez niego adres e-mail nie ma zarejestrowanego konta w systemie spółki. Skarżący doprecyzował, że prawdopodobnie nie zakładał konta, ale został zapisany na wykonanie usługi za pomocą systemu spółki. Spółka ponownie poinformowała skarżącego, że nie posiada zarejestrowanego konta na wskazany przez skarżącego adres e-mail.

Prezes UODO ustalił, że skarżący pozostawał w błędzie co do tożsamości administratora konstatując, że administratorem jego danych osobowych jest nadawca wiadomości SMS. Faktycznym administratorem danych osobowych był przedsiębiorca, który jakiś czas temu świadczył usługę na jego rzecz. Spółka pełniła rolę podmiotu przetwarzającego na podstawie stosownej umowy powierzenia (art. 28 ust. 1 rozporządzenia 2016/679).

Wprawdzie swoje żądania skarżący błędnie skierował do podmiotu przetwarzającego, niemniej jednak, jak zauważył Prezes UODO, na administratorze oraz podmiocie przetwarzającym ciąży obowiązek współpracy w realizacji uprawnień osób, których dane dotyczą, w taki sposób, aby nie dochodziło do uszczerbku w ich realizacji (art. 28 ust. 3 lit. e rozporządzenia 2016/679). Dopiero po wszczęciu postępowania administracyjnego przez Prezesa UODO spółka ustaliła i poinformowała przedsiębiorcę

[54] DS.523.1645.2022.

o wniesionej skardze do organu nadzorczego. Spółka nie poinformowała administratora o żądaniach podmiotu danych, co jak wskazała, wynikało z jej omyłki, a sama sytuacja była incydentalna. Prezes UODO zauważył, że przepisy nie określają dokładnego terminu na powiadomienie administratora o żądaniu podmiotu danych, jednakże powinno to nastąpić niezwłocznie, pozwalając administratorowi na reakcję zgodną z terminami wynikającymi z art. 12 rozporządzenia 2016/679. Zawiadomienie administratora o żądaniu podmiotu danych powinno być wyraźne.

W toku postępowania ustalono, że spółka zrealizowała wysyłkę wiadomości tekstowej SMS o charakterze marketingowym na wyraźne polecenie administratora zlecone w systemie. Spółka nie zmieniła samodzielnie celu ani sposobu przetwarzania (art. 28 ust. 10 rozporządzenia 2016/679). Przedsiębiorca nie zaznaczył w systemie spółki posiadania zgody osób, których dane dotyczą, jednocześnie jednak zdecydował, że chce wysłać wiadomość do osób, które nie wyraziły zgody na otrzymywanie treści marketingowych – pomimo wyświetlonego ostrzeżenia w systemie. Przedsiębiorca rzeczywiście nie miał zgody skarżącego do przetwarzania danych osobowych w tym celu.

Przedsiębiorca wyjaśnił, że nie przetwarza danych osobowych skarżącego, a dane w systemie spółki zablokował. Jednocześnie do akt sprawy załączył kopie dokumentów związanych ze świadczoną usługą, potwierdzające, że dane osobowe skarżącego są jednak nadal przetwarzane. Prezes UODO zwrócił uwagę, że zablokowanie danych osobowych w systemie, czy też ich zarchiwizowanie, nie jest równoznaczne z ich usunięciem.

Prezes UODO upomniał spółkę za brak współpracy z przedsiębiorcą (administratorem), a także udzielił przedsiębiorcy upomnienia za przetwarzanie danych osobowych skarżącego w celach marketingowych bez podstawy prawnej, a następnie nakazał mu ich usunięcie ze względu na brak podstaw prawnych do dalszego ich przetwarzania.

1.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa

Przetwarzanie przez lekarza danych osobowych osoby będącej świadkiem w sprawie sądowej, pozyskanych za pośrednictwem PUE ZUS

Przedmiotem postępowania przed Prezesem UODO w jednej ze spraw były nieprawidłowości w przetwarzaniu przez lekarza danych osobowych skarżącej, zlokalizowanych na Platformie Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE ZUS). Lekarz w złożonych w sprawie wyjaśnieniach wskazał, że został zniesławiony przez dziennikarza, przez co ten złożył przeciwko niemu prywatny akt oskarżenia, w efekcie czego dziennikarz został uznany winnym zarzucanego mu przestępstwa zniesławienia.

W toku postępowania przed sądem skarżąca wystąpiła jako świadek obrony dziennikarza i zeznała, że była przed laty pacjentką lekarza. Lekarz natomiast ustalił, że skarżąca nigdy nie była w podanym okresie jego pacjentką, przez co zdecydował się złożyć zawiadomienie o składaniu przez nią fałszywych zeznań.

Z uwagi na to, że lekarz nie posiadał adresu zamieszkania skarżącej, do jego uzyskania wykorzystał posiadany dostęp do PUE ZUS. Lekarz stał na stanowisku, że uzyskując dostęp do danych osobowych skarżącej zgromadzonych na PUE ZUS, działał

na potrzeby toczącego się postępowania karnego, a więc ze względu na swój prawnie uzasadniony interes.

W ocenie Prezesa UODO skorzystanie przez lekarza z danych osobowych skarżącej zawartych na PUE ZUS mogło być uzasadnione tylko celami zawodowymi lub związanymi z wykonywaną działalnością zawodową. Lekarz, jako osoba posiadająca uprawnienia oraz mająca możliwość dostępu do PUE ZUS w związku z wykonywaną działalnością zawodową, nie mógł korzystać z posiadanych uprawnień do innego celu i w efekcie uzyskał bez podstawy prawnej dostęp do danych skarżącej. W przedmiotowej sprawie, w ocenie Prezesa UODO, nie zaistniała przesłanka z art. 6 ust. 1 lit. f) RODO, na którą powoływał się lekarz, przez co organ stwierdził, że lekarz przetwarzał dane osobowe skarżącej niezgodnie z prawem i udzielił mu upomnienia[55].

Pozyskanie z PUE ZUS informacji o współmałżonku lekarza i ich wspólnym dziecku

W jednej ze spraw skarżąca zgłosiła, że lekarz uzyskał dostęp do jej danych osobowych zawartych w PUE ZUS, a korzystanie z danych skarżącego przez lekarza nie było zakończone wystawieniem zaświadczenia lekarskiego lub jego anulowaniem.

Lekarz w toku postępowania wyjaśnił, że nie świadczył usług na rzecz skarżącej, a wykorzystał swoje uprawnienia nadane mu w systemie PUE ZUS celem uzyskania dostępu do danych widniejących na PUE ZUS skarżącej i pozyskania informacji o stanie zdrowia ich wspólnej córki, tj. ustalenia, czy skarżącej udzielono zwolnień lekarskich w celu opieki nad ich wspólnym dzieckiem. Lekarz wskazał, że skarżąca w sposób nieuprawniony ogranicza mu kontakt z dzieckiem i uniemożliwia od około 1,5 roku dostęp do informacji w najważniejszych kwestiach życia ich córki, w tym o stanie jej zdrowia. Lekarz oświadczył, że nie wykorzystał danych skarżącej pochodzących z PUE ZUS w żaden sposób, ani prywatnie, ani w zakresie prowadzonej przez niego działalności gospodarczej, i nie odniósł z tego tytułu żadnych korzyści majątkowych, a korzystał z tych danych tylko w charakterze czysto osobistym i domowym, koncentrując się na potrzebie pozyskania informacji o dziecku.

Organ, oceniając legalność przetwarzania danych osobowych przez lekarza wskazał, iż brak jest przepisów prawa, które legalizowałyby takie wykorzystywanie przez niego danych osobowych skarżącej, jakie miało miejsce w opisywanej sprawie, tj. celem uzyskania dostępu do PUE ZUS przez lekarza, nieuzasadnionego względami medycznymi, w szczególności zamiarem wystawienia, anulowania lub sprostowania zaświadczenia lekarskiego lub potwierdzenia prawdziwości zawartych w zaświadczeniu danych. Wobec tego organ, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, udzielił lekarzowi upomnienia za naruszenie art. 5 ust. 1 lit. a) oraz art. 6 ust. 1 i art. 9 ust. 1 RODO poprzez bezpodstawne przetwarzanie danych osobowych skarżącej celem uzyskania dostępu do danych zgromadzonych na PUE ZUS oraz bezpodstawne przetwarzanie (przeglądanie) danych osobowych skarżącej zawartych na jej profilu w PUE ZUS[56].

Uzyskanie przez lekarza dostępu do PUE ZUS w celu ustalenia adresu zamieszkania swojej krewnej

[55] DS.523.997.2023.
[56] DS.523.578.2023.

Skarżąca zgłosiła, że lekarka uzyskała dostęp do jej danych osobowych zawartych na PUE ZUS, a korzystanie z danych skarżącej przez lekarkę nie było zakończone wystawieniem zaświadczenia lekarskiego lub jego anulowaniem.

W toku postępowania organ ustalił, że lekarka wykorzystała dane osobowe skarżącej w zakresie numeru PESEL bez podstawy prawnej w celu uzyskania dostępu do jej danych osobowych oraz pozyskaniu jej adresu zamieszkania za pośrednictwem PUE ZUS. W wyjaśnieniach złożonych organowi lekarka wskazała, że skarżąca jest jej kuzynką i sama udostępniła swój numer PESEL w celu wydania zaświadczenia lekarskiego i wystawienia skierowania na szczepienie przeciwko COVID-19. Lekarka wyjaśniła, że w wyniku uzyskania dostępu do danych osobowych skarżącej pozyskała jej adres zamieszkania. Okoliczność ta podyktowana była zamiarem poinformowania skarżącej o śmierci członka rodziny i dacie jego pogrzebu – z uwagi na brak innej możliwości kontaktu ze skarżącą. Lekarka podkreśliła, że była to incydentalna i wyjątkowa sytuacja podyktowana względami rodzinnymi i danych tych nikomu nie udostępniła ani nie zamierza w przyszłości udostępniać.

Organ w wydanej decyzji podkreślił, że lekarka wprawdzie znała dane osobowe skarżącej, z uwagi na okoliczność pozyskania ich od samej skarżącej w celu wystawienia skierowania na szczepienie przeciwko COVID-19, nie zmienia to jednak faktu ich bezpodstawnego wykorzystania celem uzyskania dostępu do PUE ZUS skarżącej. Prezes UODO stwierdził, że lekarka wykorzystała dane osobowe skarżącej (w szczególności nr PESEL) w celach prywatnych, do czego nie była w danej sytuacji uprawniona.

Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, organ udzielił lekarce upomnienia za naruszenie art. 5 ust. 1 lit. a) oraz art. 6 ust. 1 RODO poprzez wykorzystanie danych osobowych skarżącej bez podstawy prawnej w celu uzyskania dostępu do jej danych osobowych zlokalizowanych na PUE ZUS[57].

Uzyskanie dostępu do PUE ZUS w związku z powstałym konfliktem sąsiedzkim

Polski organ nadzorczy rozstrzygał także w sprawie dotyczącej nieprawidłowości w procesie przetwarzania szczególnych kategorii danych osobowych skarżącego przez lekarza, polegających na uzyskaniu dostępu do danych osobowych skarżącego zlokalizowanych na PUE ZUS.

Powodem uzyskania dostępu do danych skarżącego przez lekarza były względy osobiste, bowiem skarżący nie był nigdy jego pacjentem. Lekarz, który uzyskał dostęp do danych skarżącego, wykorzystując swoje uprawnienia zawodowe, był sąsiadem skarżącego i między mężczyznami istniał konflikt sąsiedzki. Lekarz potwierdził, że uzyskał jednorazowo dostęp do PUE ZUS skarżącego w oparciu o dane podane mu w pozwie skarżącego, skierowanym przeciwko niemu i jego żonie przed sądem okręgowym o naruszenie dóbr osobistych. W pozwie skarżący podał swoje dane osobowe, tj. imię i nazwisko, adres oraz numer PESEL. Lekarz wyjaśnił, że po otrzymaniu pozwu chciał zweryfikować nazwisko skarżącego, bowiem lekarzowi wydawało się, że skarżący, przedstawiając się, podał inne dane. Lekarz przyznał, że jest świadomy nieuprawnionego użycia platformy PUE ZUS, i wskazał, iż jego intencją nie było naruszenie jakiegokolwiek przepisu z zakresu przetwarzania danych osobowych.

[57] DS.523.5595.2022.

Organ w decyzji zwrócił uwagę, że co do ogólnej zasady lekarz – jako podmiot zobowiązany do oceny zasadności wystawienia zaświadczenia lekarskiego – jest upoważniony do dostępu do danych zgromadzonych na PUE ZUS, ale dostęp taki nie jest bezwarunkowy. Przy ocenie procesu przetwarzania danych osobowych skarżącego w tej sprawie organ miał na względzie, że lekarz działał jako samodzielny administrator, bowiem uzyskując dostęp do danych osobowych skarżącego, zlokalizowanych w PUE ZUS, i przeglądając te dane, sam decydował o celach oraz sposobach ich przetwarzania. Wobec takich założeń organ zbadał, czy lekarz legitymował się przesłanką uprawniającą go do pozyskania danych skarżącego zawartych na PUE ZUS. W efekcie stwierdzenia braku spełnienia przesłanki organ udzielił lekarzowi upomnienia[58].

Uzyskanie przez pracownika lekarza dostępu do PUE ZUS w celu potwierdzenia adresu zamieszkania znanej pracownikowi osoby

W jednym z prowadzonych przez Prezesa UODO postępowań organ ustalił, że pracownica lekarki, wykorzystując w sposób nieuprawniony dane do logowanie do systemu PUE ZUS lekarki, uzyskała dostęp do ww. systemu i sprawdziła dane osobowe skarżącej. Pracownica lekarki złożyła oświadczenie, w którym potwierdziła, iż posiadała już wcześniej dane osoby skarżącej, takie jak imię, nazwisko, PESEL i jedynie chciała się upewnić co do jej adresu. Z tego powodu w sposób nieuprawniony zalogowała się do PUE ZUS. W ocenie administratora zachowanie pracownicy było spowodowane jej „sytuacją rodzinną". Zdaniem Prezesa UODO ww. działanie stanowiło naruszenie RODO. Dostęp do danych zgromadzonych na profilu PUE ZUS nie był związany ze świadczeniem na rzecz osoby wnoszącej skargę usług medycznych. Z kolei nie ma przepisów, które legalizowałyby pozyskiwanie przez lekarzy czy personel administratora dostępu do danych osobowych za pośrednictwem systemów medycznych – w celu innym niż wystawienie, anulowanie lub sprostowanie zaświadczenia lekarskiego[59].

Pozyskanie danych osobowych pracownika przychodni przez innego pracownika

Prezes UODO prowadził w analizowanym roku postępowanie w sprawie kwestionowanego nieuprawnionego uzyskania przez lekarkę dostępu do danych osobowych skarżącej na PUE ZUS, w którym to postępowaniu skarżąca wskazywała, że nie odbyła wizyty lekarskiej w dniu wejścia lekarki na jej PUE ZUS. Organ ustalił, że skarżąca była nie tylko pacjentką przychodni, w której pracowała lekarka, która uzyskała dostęp do PUE ZUS skarżącej, ale także była pracownikiem tej przychodni. Z zebranego materiału dowodowego wynikało ponadto, że przychodnia, w której pracowała lekarka oraz skarżąca, wyodrębniła w swoim miejscu pracy stanowiska asystentów medycznych, którzy w imieniu lekarzy byli uprawnieni do wystawiania zwolnień lekarskich. Do obowiązków asystentów medycznych należało także uzupełnianie listy obecności pracowników przychodni. Asystent medyczny uznał, że mając uprawnienia dostępowe lekarki do platformy PUE ZUS, może wykorzystywać przetwarzane informacje również do celów związanych z weryfikacją absencji chorobowej, czasu niezdolności do pracy i sprawdzić przyczynę nieobecności danej osoby w miejscu zatrudnienia. W treści decyzji organ wskazał, że płatnik składek, aby przetwarzać dane na PUE ZUS musi działać przez ustawowych lub statutowych przedstawicieli, ewentualnie udzielić pełnomocnictwa osobie

[58] DS.523.3633.2022.
[59] DS.523.1262.2022.

fizycznej, np. swojemu pracownikowi albo pracownikowi biura rachunkowego. Osoba upoważniona musi mieć wcześniej założone swoje konto na PUE ZUS. W portalu PUE ZUS tworzony jest profil klienta, na którym udostępnione są dane w rolach, w których ten klient występuje w ZUS i do których ma dostęp: ubezpieczony, płatnik składek, świadczeniobiorca, lekarz, komornik. Dostęp do profilu ma osoba fizyczna, która działa w imieniu swoim lub podmiotu, który ją upoważnił. Zatem przychodnia jako płatnik składek winna była działać przez upoważnione do tego osoby oraz występować w roli do tego przeznaczonej z odpowiedniego profilu i konta utworzonego na PUE ZUS (jako płatnik), a nie, jak to miało miejsce w omawianym przypadku, kiedy to pracownik przychodni uzyskał dostęp do PUE ZUS skarżącej, korzystając z uprawnień lekarki w celu weryfikacji przyczyny nieobecności skarżącej w miejscu pracy. Prezes UODO ocenił, że nie została spełniona w tym przypadku żadna z przesłanek określonych w art. 9 ust. 2 RODO odnośnie do kwestionowanego przez stronę skarżącą nieuprawnionego dostępu do jej danych osobowych przetwarzanych za pośrednictwem PUE ZUS, i udzielił przychodni – jako podmiotowi odpowiadającemu za działania swojego pracownika – upomnienia[60].

Wykorzystanie dostępu do danych osobowych osoby, której one dotyczą, przetwarzanych na PUE ZUS przez lekarza w celu związanym z zatrudnieniem tej osoby

Jedna z rozpatrzonych spraw dotyczyła lekarza, który posiadał dostęp do PUE ZUS zarówno z racji wykonywanego zawodu, jak i faktu bycia osobą upoważnioną przez pracodawcę skarżącej – spółkę, jako płatnika składek. Lekarz, chcąc wygenerować (jako upoważniony przez spółkę – płatnika składek) z systemu PUE ZUS zwolnienia lekarskie pracownicy (skarżącej), uzyskał kilkukrotnie nieuprawniony dostęp do jej danych osobowych zawartych na PUE ZUS, występując w roli lekarza, pomimo iż skarżąca nigdy nie była pacjentką tego lekarza i nie udzielał jej on również nigdy żadnych świadczeń medycznych.

Lekarz nie był faktycznym pracodawcą skarżącej, gdyż była nim spółka, w której skarżąca była zatrudniona. Lekarz mógł działać z upoważnienia spółki i na rzecz spółki, jednak w omawianej sprawie nie miało to miejsca, w szczególności biorąc pod uwagę fakt, że trzykrotne logowanie na PUE ZUS przeprowadzono za pośrednictwem jego profilu lekarza.

Lekarz, z uwagi na absencję upoważnionej do ww. czynności osoby, wykorzystał więc numer PESEL skarżącej i uzyskał dostęp do jej danych zgromadzonych w systemie PUE ZUS w celu nieuzasadnionym względami medycznymi, jak również w celu niezwiązanym z wykonywaniem przez niego zawodu lekarza, lecz wyłącznie w związku z chęcią wygenerowania zwolnień lekarskich pracownicy, tj. skarżącej, do czego nie był upoważniony.

W przedmiotowej sprawie, po przeprowadzeniu postępowania wyjaśniającego, Prezes UODO skorzystał ze swoich uprawnień i upomniał lekarza za naruszenie polegające na wykorzystaniu numeru PESEL skarżącej, w celu uzyskania dostępu do jej danych zgromadzonych w systemie teleinformatycznym PUE ZUS, bez podstawy prawnej oraz następnie trzykrotnym uzyskaniu za pośrednictwem PUE ZUS dostępu do danych skarżącej w zakresie jej imienia i nazwiska, daty urodzenia, adresu zamieszkania nazwy

[60] DS.523.745.2023.

skróconej i nr NIP płatnika składek (pracodawcy) oraz danych zawartych w wystawionych jej trzech zwolnieniach lekarskich, tj. informacji o okresie jej niezdolności do pracy, kodu choroby oraz wskazania lekarskiego bez podstawy prawnej[61].

Wykorzystanie dostępu do PUE ZUS przez lekarza w związku z występowaniem przez niego w roli pracodawcy

W kolejnej z rozpatrywanych spraw uzyskanie przez lekarkę dostępu do danych osobowych skarżącej, zgromadzonych na PUE ZUS, nastąpiło w następstwie otrzymania przez nią pisma z Zakładu Ubezpieczeń Społecznych, informującego ją o decyzji wydanej w kwestii przyznania skarżącej prawa do zasiłku chorobowego za okres przebywania na zwolnieniu lekarskim. W zaistniałej sytuacji lekarka, która nie posiadała wtedy żadnych znanych jej związków ze skarżącą, które uzasadniałyby wystosowanie do niej przez ZUS korespondencji o ww. treści, podjęła decyzję o zweryfikowaniu informacji dotyczących rzeczonego zwolnienia lekarskiego poprzez system PUE ZUS. Z treści otrzymanego pisma wynikało, że ZUS traktuje lekarkę jako „płatnika składek" względem skarżącej i zgodnie z takim pojmowaniem stanu faktycznego poinformował lekarkę o ww. decyzji odmownej.

Prezes UODO ustalił, że skarżąca, starając się o uzyskanie zwolnienia lekarskiego, podała jako miejsce pracy gabinet lekarski należący do lekarki. Jak ustaliła lekarka, adres zamieszkania, który wskazała skarżąca, był równocześnie adresem, pod którym żył mąż lekarki, z którym lekarka toczy sprawę rozwodową. W momencie otrzymania korespondencji od ZUS lekarka nie była świadoma ani bycia wskazaną przez skarżącą jako jej pracodawca, ani też relacji osobistej łączącej jej męża ze skarżącą. W efekcie doszło do sytuacji, w której skarżąca, związana z mężem lekarki, zgłosiła do ZUS podjęcie pracy w gabinecie lekarskim należącym do lekarki, dodatkowo sama, będąc niezdolną do pracy we wskazanym dniu podjęcia pracy – o wszystkim lekarka zaś dowiedziała się w ramach własnej analizy sprawy oraz z pisma przesłanego przez ZUS.

W omawianej sprawie charakterystyczne było po pierwsze wystąpienie przez administratora w „podwójnej" roli, tj. lekarki mającej upoważnienie do wystawiania zaświadczeń lekarskich oraz pracodawcy, w związku z przyjętym przez ZUS podejrzeniem zatrudniania skarżącej przez lekarkę, a po drugie, że zdarzenie zaistniało w następstwie przedstawienia przez skarżącą nieprawdziwych informacji ZUS w zakresie jej sytuacji zawodowej. Organ w decyzji zwrócił uwagę na to, że właściwość PUE ZUS umożliwia osobom wystawiającym zaświadczenia lekarskie dostęp do danych osobowych, w tym informacji o stanie zdrowia pacjentów. Dane dotyczące zdrowia są szczególną kategorią danych osobowych, a uzyskanie dostępu do nich przez lekarza wymaga spełnienia przesłanek legalności, określonych w art. 9 ust. 2 RODO.

Prezes UODO podkreślił, że lekarz, mając dostęp do danych zgromadzonych na PUE ZUS, nie może z tego dostępu korzystać w sposób dowolny. Aby dostęp ten nie naruszał przepisów RODO, musi zostać spełniony przynajmniej jeden warunek z art. 9 ust. 2 RODO. W opisywanej sprawie nie został spełniony żaden warunek legalizujący wykorzystanie danych w sposób, w jaki uczyniła to lekarka. Organ wyjaśnił w decyzji, że lekarka przyczynę wysłania do niej listu przez ZUS mogła ustalić opierając się na samej treści korespondencji, w której wskazane było wprost, że list informujący o odmownej decyzji

[61] DS.523.3480.2023.

otrzymuje z uwagi na bycie wpisaną jako płatnik składek wobec skarżącej, która ubiegała się o zasiłek chorobowy.

Organ podkreślił, że lekarz nie może w ramach tego samego procesu przetwarzania pełnić równocześnie funkcji lekarza świadczącego usługi medyczne oraz pracodawcy. Zabronione jest korzystanie z dostępu do PUE ZUS, który został przyznany lekarce z powodu wykonywanej profesji, w celach związanych z jej rolą jako pracodawcy. ZUS skierował zapytanie do lekarki w związku z uzasadnionym podejrzeniem zatrudniania przez nią skarżącej, tymczasem lekarka mogła we własnym zakresie (bez konieczności uzyskiwania dostępu do PUE ZUS z poziomu lekarza) ustalić, że żadnych relacji służbowych ze skarżącą nie posiadała. Lekarka była świadoma, że nie udzielała świadczeń medycznych skarżącej, więc brak było uzasadnienia dla korzystania z przysługującego jej, jako lekarzowi, dostępu do PUE ZUS w związku z pismem, które otrzymała od ZUS. W tej sprawie Prezes UODO skorzystał z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO i udzielił lekarce upomnienia za naruszenie art. 5 ust. 1 lit. a) oraz art. 9 ust. 1 RODO[62].

Recepty i skierowania na badania wystawiane skarżącym przez nieznanych lekarzy

Do Prezesa UODO wpłynęły liczne skargi dotyczące błędnego wystawienia przez lekarzy recept oraz skierowań. W przedmiotowych sprawach skarżący zarzucali, że z Internetowego Konta Pacjenta (IKP) uzyskali informację o wystawieniu przez nieznanych im lekarzy recept lub skierowań na badania, które widnieją w systemie jako zrealizowane, a oni sami ich nie wykorzystywali. Ponadto skarżący wskazywali, że błędne wpisy w IKP i wystawiane recepty zniekształcają ich historie choroby.

W toku postępowań administratorzy (placówki medyczne, lekarze) wskazywali, że do wystawienia recept/skierowań dochodziło m.in. w wyniku omyłki i błędnej weryfikacji pacjenta lub jej braku przez pracowników rejestrujących pacjenta na wizytę (rejestracja przygotowała złą kartę; skarżący był pacjentem placówki, ale nie korzystał z wizyty lekarza) lub lekarza (recepta wystawiona na skarżącą zamiast na inną osobę o tym samym imieniu i nazwisku; błędnie wpisany przez lekarza nr PESEL do systemu przy wystawianiu recepty/skierowania i wystawienie pacjentowi dokumentu z danymi osobowymi skarżącego; zamiana pacjentów w kolejce lub wejście pacjenta poza kolejnością). W niektórych przypadkach dochodziło do udostępnienia danych skarżących osobie nieuprawnionej poprzez wydanie błędnie wystawionej recepty lub skierowania na badania.

Prezes UODO uznał, że w przedmiotowych sprawach administratorzy nie dopełnili obowiązków, które spoczywają na nich w związku z przepisami o ochronie danych osobowych poprzez bezpodstawne przetwarzanie, w tym w niektórych przypadkach udostępnianie, danych osobowych skarżących (imię, nazwisko, adres zamieszkania, numer PESEL), w związku ze świadczeniem usług medycznych na rzecz innej osoby – pacjenta podmiotu, co stanowiło naruszenie art. 5 ust. 1 lit. a) oraz art. 6 ust. 1 RODO. W związku z powyższym, biorąc pod uwagę podjęte przez administratorów działania po uzyskaniu informacji o nieprawidłowościach w przetwarzaniu danych osobowych skarżących oraz nieodwracalny skutek naruszenia, Prezes UODO udzielił administratorom upomnienia[63].

[62] DS.523.4058.2022.
[63] DS.523.1110.2023; DS.523.5552.2022; DS.523.8053.2021; DS.523.3990.2023.

Przetwarzanie danych osobowych byłego pracownika (w tym jego wizerunku) przez urząd gminy na jego stronie internetowej oraz w Biuletynie Informacji Publicznej

Skarżący w treści złożonej do Prezesa UODO skargi wskazywał, że nigdy nie wyrażał zgody na przetwarzanie jego danych osobowych po wygaśnięciu stosunku pracy, podkreślając przy tym, że jego dane osobowe są bezprawnie przetwarzane na stronie internetowej urzędu gminy w związku z czym zwrócił się do Prezesa UODO o zbadanie słuszności stanowiska w tym zakresie.

Prezes UODO, w celu zbadania legalności przetwarzania danych skarżącego po ustaniu stosunku w oparciu o przepisy o ochronie danych osobowych, odwołał się również do przepisów ustawy o dostępie do informacji publicznej (u.d.i.p.) z uwagi na to, że kluczową kwestią dla oceny przedmiotowej sprawy było określenie czy skarżący, będąc zatrudnionym w urzędzie gminy był osobą wykonującą zadania publiczne. Prezes UODO stwierdził, że skarżący, jako osoba zatrudniona w urzędzie gminy na stanowiskach głównego specjalisty oraz zastępcy kierownika wydziału, wykonująca na jego rzecz zadania, był osobą wykonującą zadania publiczne oraz osobą świadczącą pracę w ramach zatrudnienia w instytucji publicznej. W omawianej sprawie nie zachodziła przesłanka ograniczająca udostępnianie informacji publicznej ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy, gdyż przydzielone skarżącemu, zatrudnionemu na stanowisku zastępcy kierownika wydziału, określone zadania w urzędzie były powiązane ze sprawowaniem przez niego funkcji publicznej, w ramach struktur władzy publicznej lub na stanowisku decyzyjnym w strukturze administracji publicznej. Skarżącemu przysługiwał co najmniej wąski zakres kompetencji decyzyjnej w ramach instytucji publicznej.

Prezes UODO uznał więc, że przetwarzanie danych osobowych skarżącego w zakresie jego imienia i nazwiska na stronie internetowej urzędu gminy, w tym w Biuletynie Informacji Publicznej, miało oparcie w przepisach RODO. W wydanym rozstrzygnięciu odniósł się również do przetwarzania wizerunku skarżącego na stronie internetowej urzędu gminy i wskazał, że uprawnienie urzędu gminy do przetwarzania danych osobowych skarżącego bez jego zgody nie obejmowało na gruncie przepisów Kodeksu pracy (K.p.) publikacji jego wizerunku na stronie internetowej urzędu gminy – zarówno w trakcie zatrudnienia, jak i po jego ustaniu. Okoliczność ta pozwoliła na stwierdzenie, że urząd gminy nie legitymował się podstawą prawną uprawniającą do przetwarzania wizerunku skarżącego i brak ten miał charakter pierwotny. Prezes UODO wskazał, iż przepisy u.d.i.p., K.p., czy też przepisy ustawy o samorządzie gminnym, nie mają zastosowania do okoliczności i zakresu przetwarzania wizerunku skarżącego, w szczególności na gruncie ochrony danych osobowych, tj. publikacji wizerunku. Organ zwrócił uwagę na to, że wizerunek jako dana osobowa, podlega szczególnej ochronie na mocy przepisów RODO. Prezes UODO podkreślił, że skarżący nie wyrażał zgody na udostępnienie jego wizerunku przez urząd gminy, jak również urząd gminy nie wykazał w tym zakresie spełnienia jakiejkolwiek z przesłanek uzasadniających przetwarzanie kwestionowanych danych osobowych skarżącego.

Podsumowując, po przeprowadzeniu omawianego postępowania, Prezes UODO nakazał urzędowi gminy usunięcie danych osobowych skarżącego w zakresie jego wizerunku ze stron internetowych urzędu gminy. Następnie, wobec ustalenia, że przetwarzanie danych osobowych skarżącego w zakresie jego imienia i nazwiska, polegające na udostępnieniu zarządzeń urzędu gminy w Biuletynie Informacji Publicznej,

zawierających ww. dane osobowe skarżącego w związku z powołaniem go do określonych zadań przez urząd gminy oraz udostępnienie artykułów na stronie internetowej urzędu gminy w ramach wykonywanych przez skarżącego w czasie zatrudnienia obowiązków, jak też w celu promocji gminy, było zgodne z obowiązującymi przepisami. Wobec tego Prezes UODO uznał skargę w tym zakresie za nieuzasadnioną i odmówił w tej części uwzględnienia wniosku skarżącego. Urząd Gminy, zgodnie z nakazem usunięcia wizerunku skarżącego, wykonał decyzję Prezesa UODO i usunął wizerunek skarżącego ze strony internetowej[64].

Przetwarzanie przez instytucję kultury danych osobowych dotyczących braku posiadania przez osobę, której dane dotyczą, certyfikatu COVID-19

Sprawa dotyczyła nieprawidłowości w procesie przetwarzania danych skarżącej przez instytucję kultury – kino, będące administratorem – polegającego na przetwarzaniu danych skarżącej w zakresie informacji dotyczącej braku posiadania certyfikatu COVID-19. Istotne w tym postępowaniu było to, że administrator pomimo faktycznego niepozyskania szczególnych kategorii danych skarżącej, która odmówiła ich podania, przypisał skarżącej te dane i je przetwarzał, chociaż nie były to prawdziwe dane skarżącej.

Organ ustalił, że skarżąca zamierzała wziąć udział w projekcji filmu, na którą miała kupione dwa bilety. W ówczesnym czasie, ze względu na sytuację pandemiczną w kraju i obowiązujące przepisy rozporządzenia Rady Ministrów z 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[65], dotyczące wprowadzenia przez ustawodawcę w okresie od 26 czerwca 2021 r. do 28 lutego 2022 r. ograniczeń dla przedsiębiorców, prowadzących działalność związaną z wszelkimi zbiorowymi formami kultury i rozrywki, istniały limity osób mogących być jednocześnie uczestnikami wydarzenia. Limity te zostały wskazane w § 9 ust.19c pkt 1 ww. rozporządzenia Rady Ministrów. Zgodnie z § 26a do tych limitów nie zaliczało się osób, które poddały się szczepieniu przeciwko COVID-19. Powyższe ograniczenia obligowały instytucje kultury do pilnowania, aby dopuszczalna liczba uczestników wydarzenia kulturalnego nie została przekroczona. Jednocześnie prawodawca nie sformułował przepisu ani wytycznych, w oparciu o które przedsiębiorca mógłby zakwalifikować daną osobę w grupie osób podlegających limitowi, czy też w grupie zwolnionych z weryfikacji z uwagi na posiadanie certyfikatu covidowego. Organ nadzorczy uznał, że przesłanką dopuszczającą przetwarzanie przez podmiot skarżony danych osobowych widza w kinie, w zakresie danych o posiadaniu (bądź nie) paszportu covidowego, byłaby jedynie wyraźna zgoda tej osoby na przetwarzanie tej kategorii danych osobowych (art. 9 ust. 2 lit. a RODO).

Jak ustalono, skarżąca nie okazała pracownikowi kina paszportu covidowego, a ponadto ani nie potwierdziła, ani nie zaprzeczyła jego posiadaniu. Skarżącej nie wpuszczono na seans i oddano jej pieniądze za bilety, natomiast w protokole zwrotu towaru (biletów) jako przyczynę jego dokonania wskazano „brak certyfikatu covid", tłumacząc, że brak certyfikatu oznaczał w tym przypadku jedynie podstawę do zwrotu należności za bilety i była to informacja wskazująca, że pracownik kina z takim certyfikatem się nie zapoznał. Podmiot skarżony uznał i wskazał w wyjaśnieniach, że mógł przetwarzać

[64] DS.523.5731.2022.
[65] Dz. U. z 2021 r. poz. 861.

ww. dane skarżącej opierając się na art. 6 ust. 1 lit. f) RODO w zw. z art. 6 ust. 1 lit. b) RODO i art. 6 ust. 1 lit. c) RODO, w celu realizacji jej prawa do uzyskania zwrotu należności za niewykorzystany bilet oraz ze względu na przepisy podatkowe dotyczące przechowywania dokumentów księgowych.

Organ nie podzielił stanowiska podmiotu skarżonego i zakwalifikował informację o braku certyfikatu COVID jako dane osobowe dotyczące zdrowia skarżącej, do których zastosowanie mają przesłanki przetwarzania danych wskazane w art. 9 ust. 2 RODO, natomiast przetwarzanie przez podmiot skarżony informacji o posiadaniu paszportu covidowego mogło odbywać się na podstawie art. 9 ust. 2 lit. a) RODO, czyli wyraźnej zgody osoby, której dane dotyczą. Organ nadzorczy ocenił, że niezasadne było posłużenie się przez podmiot skarżony podczas zwrotu należności za bilety opisem, który charakteryzował stan zdrowia skarżącej, czym naruszył przepis art. 9 ust. 2 lit. a) RODO. Dodatkowo organ nadzorczy stwierdził również po stronie podmiotu skarżonego naruszenie zasad przetwarzania danych osobowych wynikających z art. 5 ust. 1 RODO, ponieważ posłużył się nieprawdziwymi danymi skarżącej – mimo że skarżąca odmówiła okazania paszportu covidowego, administrator przypisał jej brak tego dokumentu. Podmiot skarżony miał świadomość, że informacja o odmowie okazania przez skarżącą certyfikatu covidowego nie jest tożsama z informacją o jego braku, a jednak taką informacją w odniesieniu do skarżącej się posługiwał – i tym samym nie zapewnił prawidłowego przetwarzania danych osobowych skarżącej.

Organ nadzorczy skorzystał z uprawnienia naprawczego wynikającego z art. 58 ust. 2 lit. g) RODO, nakazującego usunięcie danych osobowych skarżącej przetwarzanych niezgodnie z prawem[66].

Skutki nieprawidłowej anonimizacji danych osobowych w związku z realizacją obowiązku udostępnienia informacji publicznej

Prezes UODO rozpatrywał sprawę dotyczącą skargi na nieprawidłowości w procesie przetwarzania danych osobowych skarżącej poddanych pseudonimizacji oraz informacji, że jest matką jednej z uczennic szkoły podstawowej, a także danych osobowych samej małoletniej uczennicy, polegające na udostępnieniu ww. danych osobowych dotyczących skarżącej i jej córki w treści protokołu kontroli doraźnej.

W toku postępowania organ ustalił, że skarżąca zwróciła się do jednego z kuratoriów oświaty z pismem, w którym wskazała na szereg nieprawidłowości po stronie szkoły. Na mocy decyzji tego kuratorium w szkole została przeprowadzona kontrola doraźna w zakresie nadzoru dyrektora szkoły nad pracą nauczycieli. Z kontroli sporządzony został protokół, który następnie doręczono dyrektorowi szkoły. W dalszej kolejności dyrektor szkoły otrzymał wniosek o udostępnienie informacji publicznej poprzez zamieszczenie w BIP szkoły m.in. ww. protokołu kontroli doraźnej, który został, zgodnie z wnioskiem, udostępniony.

W omawianej sprawie Prezes UODO ocenił, czy dane udostępnione w protokole kontroli doraźnej opublikowanym na stronie internetowej szkoły w BIP, stanowiły dane osobowe w rozumieniu RODO. Zgodnie z motywem 26 RODO, zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Dane osobowe poddane pseudononimizacji, które

[66] DS.523.1226.2022.

przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. W celu stwierdzenia, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.

W wyniku wyodrębnienia z treści opublikowanego na stronie internetowej szkoły w BIP protokołu kontroli i nazwy pliku, Prezes UODO ustalił następujący zakres danych dotyczących skarżącej: imię, informacja, że skarżąca jest matką jednej z uczennic szkoły o konkretnym imieniu i uczęszczającej do konkretnej klasy oraz początkową część nazwiska skarżącej. W wyodrębnionym zbiorze danych odnoszących się do małoletniej znajdowały się jej imię, informacja dotyczące tego, że małoletnia jest uczennicą szkoły w konkretnym oddziale (klasie) oraz informacja o nieharmonijnym rozwoju u małoletniej niektórych funkcji poznawczych. Powyższe dane, zarówno w odniesieniu do skarżącej, jak i małoletniej, oceniane odrębnie od pozostałych nie stanowią danych osobowych w rozumieniu art. 4 pkt 1 RODO, ponieważ na podstawie samego imienia bądź fragmentu nazwiska lub informacji, nie można jednoznacznie zidentyfikować osoby fizycznej.

W ocenie Prezesa UODO dane i informacje dotyczące zarówno skarżącej, jak i małoletniej, udostępnione w zmodyfikowanej kopii protokołu kontroli doraźnej na stronie internetowej szkoły w BIP, można było przypisać odpowiednio ww. osobom. Dane obejmujące imię skarżącej w połączeniu z nazwą szkoły i klasy, do której uczęszcza jej córka, już samodzielnie pozwalały przypisać spseudonimizowane dane osobie fizycznej – skarżącej. Wynikało to m.in. z faktu, iż skarżąca była jedynym rodzicem noszącym dane imię wśród rodziców uczniów konkretnej klasy. Powyższy sposób mógł być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania skarżącej z uwagi na łatwość ustalenia, że skarżąca jest jedyną osobą noszącą dane imię w określonej grupie przy jednoczesnym braku ponoszenia kosztów. W ocenie organu było to również możliwe w stosunkowo niedługim czasie ze względu na niewielką liczebność oddziału – klasa składała się z 15 uczniów. W analogiczny sposób możliwe było przypisanie spseudonimizowanych danych małoletniej z uwagi na fakt, iż była ona jedyną uczennicą konkretnej klasy noszącą dane imię, będąc jednocześnie jedną z dwóch osób o tym imieniu w zbiorze ogółu uczniów szkoły.

Rozpatrując sprawę, Prezes UODO miał na względzie, że szkoła była obowiązana udostępnić w BIP informację publiczną, obejmującą m.in. dokumentację przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających, do których zalicza się protokół kontroli doraźnej przeprowadzonej przez organ sprawujący nadzór pedagogiczny nad szkołą.

W przedmiotowej sprawie szkoła podniosła, że przetwarzanie danych osobowych odbywało się na podstawie przesłanki określonej w art. 6 ust. 1 lit. c) RODO. Organ dostrzegł, że szkoła, jako podmiot wykonujący zadania publiczne, stosownie do dyspozycji

art. 4 ust. 1 pkt 5 ustawy o dostępie do informacji publicznej (u.d.i.p.), podlega obowiązkowi udostępnienia informacji publicznej. Obowiązek ten nie ma jednak charakteru bezwzględnego i podlega ograniczeniom, w tym wynikającym z art. 5 ust. 2 u.d.i.p.

Prezes UODO ocenił, że szkoła udostępniając dane w związku z publikacją protokołu kontroli doraźnej na stronie internetowej (w wersji spseudonimizowanej przez jej dyrektora), naruszyła zasadę minimalizacji danych, określoną w art. 5 ust. 1 lit. c) RODO, bowiem udostępnione dane osobowe skarżącej i małoletniej w Biuletynie Informacji Publicznej szkoły nie były adekwatne, stosowne ani ograniczone do celu, w którym były przetwarzane, tj. nie służyły celowi wypełnienia obowiązku nałożonego na dyrektora szkoły w art. 4 ust. 1 pkt 5 u.d.i.p.

W opisywanej sprawie szkoła nie dochowała również obowiązku wynikającego z art. 5 ust. 2 u.d.i.p., przez co Prezes UODO stwierdził, że szkoła naruszyła również zasadę zgodności z prawem przetwarzania danych osobowych, określoną w art. 5 ust. 1 lit. a) RODO. Szkoła nie wykazała też istnienia którejkolwiek z przesłanek legalizujących, określonych w art. 6 ust. 1 RODO, odnośnie do przetwarzania danych osobowych skarżącej i małoletniej polegającego na udostępnieniu tych danych w treści protokołu kontroli doraźnej na stronie internetowej szkoły w BIP. Tym samym szkoła naruszyła art. 6 ust. 1 i art. 9 ust. 1 RODO, udostępniając dane dotyczące zdrowia małoletniej, poprzez upublicznienie w treści spseudonimizowanego protokołu kontroli doraźnej, udostępnionego na stronie internetowej szkoły w BIP informacji o nieharmonijnym rozwoju u małoletniej niektórych funkcji poznawczych, przy jednoczesnym braku wykazania którejkolwiek z przesłanek wyłączających zakaz ustanowiony w ww. przepisie[67].

Realizacja prawa dostępu do danych przez pracodawcę

Sprawa, która częściowo może zobrazować problematykę naruszenia przez pracodawców ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą, dotyczy skargi byłego pracownika spółki na niespełnienie żądania dostępu do danych zgodnie z art. 15 RODO. Skarżący po ustaniu zatrudnienia skierował do spółki wniosek o udzielenie informacji na podstawie art. 15 RODO, w którym zawarł szczegółowe pytania dotyczące przetwarzania przez spółkę jego danych osobowych. Spółka, po upływie 11 dni udzieliła skarżącemu odpowiedzi, w której wskazała, że dane są przetwarzane zgodnie z prawem, w związku z czym nie ma powodu do zmartwień. Ze względu na brak spełnienia żądania w terminie miesiąca, zgodnie z art. 12 ust. 3 RODO, skarżący wniósł skargę do Prezesa UODO.

Prezes UODO zwrócił się do spółki o złożenie wyjaśnień w sprawie, w efekcie czego spółka udzieliła skarżącemu żądanych przez niego informacji, a następnie pismem udzieliła Prezesowi UODO wyjaśnień, w których wskazała, że mimo dołożenia należytej staranności, aby skompletować odpowiedź w najkrótszym możliwym czasie, termin na przygotowanie odpowiedzi przez spółkę z przyczyn niezależnych od jakiejkolwiek złej woli jej przedstawicieli, przekroczył termin miesięczny od otrzymania żądania. Organ zwrócił uwagę, że w pierwszej odpowiedzi przekazanej skarżącemu spółka nie wspomina o trudnościach w przygotowaniu odpowiedzi, tym samym nie spełniając warunku określonego w art. 12 ust. 3 RODO dla przedłużenia terminu na udzielenie odpowiedzi na żądanie osoby, której dane dotyczą o kolejne dwa miesiące. Istotny ponadto był fakt, że

[67] DS.523.1601.2023.

spółka udzieliła skarżącemu żądanych przez skarżącego informacji już po tym, jak dowiedział się o wszczętym postępowaniu administracyjnym.

Prezes UODO udzielił spółce upomnienia, stwierdzając naruszenie art. 12 ust. 3 i 4 w zw. z art. 15 ust. 1 i 3 RODO, polegające na nieudzieleniu odpowiedzi skarżącemu na wniosek złożony w oparciu o art. 15 ust. 1 RODO oraz nieprzekazaniu kopii danych zgodnie z art. 15 ust. 3 RODO, w związku z jego żądaniem z 27 maja 2022 r., w terminie określonym w art. 12 ust. 3 RODO, a także niepoinformowaniu o powodach nieudzielenia mu informacji stosownie do jego żądania oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem, zgodnie z art. 12 ust. 4 RODO.

Powyższa sprawa obrazuje stosunek wielu podmiotów przetwarzających dane osobowe, dla których ochrona danych oraz działanie zgodne z wymogami RODO jest zagadnieniem drugorzędnym. Dopiero świadomość konsekwencji, jakie może nieść za sobą prowadzone wobec takich podmiotów postępowanie administracyjne w sprawie naruszenia RODO stanowi czynnik motywujący do dostosowania operacji przetwarzania danych do obowiązujących przepisów prawa[68].

Pozyskanie przez byłego pracodawcę danych osobowych pracownika niezwiązanych ze stosunkiem pracy oraz przekazanie danych osobowych pracownika na rzecz skonfliktowanego współmałżonka

Prezes UODO rozpatrywał skargę na działania byłego pracodawcy, któremu skarżąca zarzuciła bezprawne pozyskanie od osoby trzeciej (jej ówczesnego męża) danych dotyczących m.in.: sprawy rozwodowej i sytuacji rodzinnej; brak spełnienia obowiązku informacyjnego z art. 14 RODO w związku z kwestionowanym pozyskaniem jej danych osobowych od osoby trzeciej; udostępnienie na rzecz jej ówczesnego męża jej danych osobowych dotyczących zatrudnienia, w tym danych o nieobecnościach w pracy z powodów zdrowotnych oraz danych dotyczących oceny jej pracy; udostępnienie na rzecz innych osób trzecich (pacjentów) danych o przyczynie nieobecności w pracy; udostępnienie i przechowywanie danych dotyczących wykształcenia i dorobku zawodowego na stronie internetowej byłego pracodawcy; brak spełnienia obowiązku informacyjnego z art. 13 ust. 1 i 2 RODO poprzez brak przekazania klauzuli informacyjnej podczas zatrudniania.

Prezes UODO ocenił, że pracodawca pozyskał nowe dane osobowe skarżącej, ale legitymował się przesłanką określoną w art. 6 ust. 1 lit. f) RODO. Informacje te nie stanowiły szczególnych kategorii danych osobowych i były niezbędne do przetwarzania oraz archiwizowania korespondencji. Z materiału dowodowego wynikało, że powstał nowy cel przetwarzania danych osobowych skarżącej polegający na obsłudze korespondencji z jej mężem i jej późniejszej archiwizacji. Mąż skarżącej był osobą korzystającą poprzednio z pomocy pracodawcy, więc pracodawca miał prawnie uzasadniony interes w przetwarzaniu danych, które podał on na spotkaniu oraz w treści korespondencji zgodnie z art. 6 ust. 1 lit. f) RODO. Prezes UODO zauważył jednocześnie, że w chwili pozyskania ww. danych osobowych skarżącej, po stronie pracodawcy jako administratora, powstał obowiązek informacyjny, którego pracodawca nie spełnił. W ocenie organu pracodawca naruszył art. 14 ust. 1 i 2 RODO poprzez brak przekazania skarżącej klauzuli informacyjnej w związku

[68] DS.523.3820.2022.

z pozyskaniem jej danych dotyczących sytuacji rodzinnej i sprawy rozwodowej od osoby trzeciej. Organ odmówił uwzględnienia wniosku skarżącej w związku z pozyskaniem jej danych osobowych od osoby trzeciej, ale zastosował upomnienie za brak spełnienia obowiązku informacyjnego w wyniku pozyskania danych.

Co do zarzutu udostępnienia danych osobowych skarżącej na rzecz jej ówczesnego męża organ wskazał, że doszło do ujawnienia informacji dotyczących zatrudnienia skarżącej na rzecz osoby trzeciej w treści przesłanej korespondencji. W treści pisma skierowanego do męża skarżącej znajdowały się jej dane osobowe, takie jak: informacje dotyczące przebywania przez skarżącą na zwolnieniach lekarskich podczas świadczenia stosunku pracy, informacje o przebiegu zatrudnienia, ocena pracy oraz dodatkowe opinie pracodawcy odnoszące się do charakteru skarżącej. Pracodawca jako administrator nie wskazał w postępowaniu żadnej podstawy prawnej tego przetwarzania. Wskazał on jedynie, że podanie mężowi skarżącej tych informacji było niezbędne do ustalenia, dochodzenia lub obrony roszczeń przez męża skarżącej, gdyż chciał on te informacje wykorzystać w postępowaniu rozwodowym.

W ocenie organu pracodawca, udostępniając dane osobowe skarżącej na rzecz jej ówczesnego męża, nie legitymował się żadną przesłanką legalności przetwarzania danych określoną w art. 6 ust. 1 RODO oraz w art. 9 ust. 2 RODO. Wskazany przez pracodawcę cel przetwarzania polegający na ustaleniu, dochodzeniu lub obronie roszczeń przez męża skarżącej, wymaga dokonania wyważenia interesów strony trzeciej (męża) z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą (skarżącej). Na administratorze ciąży obowiązek uwzględnienia zasad przetwarzania danych, m.in. zasady minimalizacji danych i ograniczonego celu. Organ ocenił, że pracodawca powinien był powstrzymać się od udostępnienia mężowi skarżącej jakichkolwiek informacji jej dotyczących. Wobec tego organ stwierdził, że pracodawca naruszył przepisy RODO poprzez bezprawne udostępnienie osobie trzeciej danych osobowych, w tym danych dotyczących przebywania na zwolnieniach lekarskich i w tym zakresie udzielił upomnienia.

W odniesieniu do zarzutu udostępnienia danych osobowych dotyczących zdrowia skarżącej na rzecz pacjentów pracodawcy organ ustalił, że pracodawca informował pacjentów o tym, iż skarżąca przebywa na zwolnieniach lekarskich. Tym samym pracodawca ujawnił swoim pacjentom, że w danym okresie skarżąca, jako zatrudniony psycholog, jest niedostępna z przyczyn zdrowotnych. Informacje te wprost dotyczyły sytuacji zdrowotnej, gdyż ujawniały kto i w jakim okresie przebywał na zwolnieniu lekarskim. Organ stwierdził, że pracodawca naruszył przepisy RODO poprzez bezprawne udostępnienie osobom trzecim – pacjentom – danych osobowych w zakresie przebywania przez skarżącą na zwolnieniach lekarskich i udzielił w tym zakresie upomnienia.

W przedmiocie zarzutu udostępnienia danych na stronie internetowej pracodawcy organ ocenił, że opublikowanie informacji mieści się w granicach prawnie uzasadnionego interesu pracodawcy, który informuje użytkowników Internetu o swoich statutowych działaniach. Tym samym pracodawca, udostępniając dane skarżącej w zakresie jej działalności na rzecz fundacji, nie naruszył przepisów o ochronie danych osobowych. Organ zauważył jednak, że administrator zobowiązany jest do ciągłego monitorowania i oceny procesów oraz zasad przetwarzania danych. Skarżąca zakończyła stosunek pracy w 2019 r., zatem w chwili wydania decyzji, zdaniem organu, nie istniał już cel przetwarzania danych skarżącej polegający na uhonorowania udziału skarżącej w realizowanym przez

pracodawcę projekcie. Organ – ze względu na znaczny upływ czasu pomiędzy ustaniem stosunku pracy a dalszym publikowaniem danych w Internecie uznał, że dalsze przetwarzanie danych skarżącej na ww. stronie internetowej narusza zasadę ograniczenia przechowywania danych określoną w art. 5 ust. lit. e) RODO i nakazał usunięcie tych danych.

W zakresie zarzutu braku spełnienia obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO, organ uznał, że pracodawca przedłożył skarżącej klauzulę informacyjną i tym samym spełnił ww. obowiązek. Wobec tego organ odmówił uwzględnienia wniosku w tym zakresie[69].

Niezbędne, do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, przetwarzanie przez niego danych osobowych osoby, której dane te dotyczą

Przedmiotowa decyzja dotyczyła skargi na przetwarzanie i udostępnienie na rzecz podmiotów trzecich danych osobowych skarżącego przez młodzieżowy ośrodek wychowawczy (dalej ośrodek) w celu innym niż do kontaktu, tj. w celu dochodzenia należności z tytułu wyżywienia byłego małoletniego wychowanka ośrodka, którego skarżący nie był prawnym opiekunem, a także niedopełnienia przez ośrodek wobec skarżącego obowiązków wynikających z art. 15, art. 17 i art. 21 RODO.

Ośrodek pozyskał dane skarżącego, gdy ten odwiózł skierowanego przez sąd małoletniego do ośrodka. Małoletni nie był dzieckiem skarżącego, jak również skarżący nie był jego prawnym opiekunem. Ośrodek pozyskane dane skarżącego wykorzystał w celu dochodzenia należności z tytułu wyżywienia małoletniego jako byłego wychowanka ośrodka.

W zakresie udostępnienia danych osobowych skarżącego, Prezes UODO umorzył postępowanie z uwagi na to, iż kwestionowane udostępnienie miało miejsce w czasie obowiązywania ustawy z 29 sierpnia 1997 r., która określała zasady przetwarzania danych osobowych do 24 maja 2018 r. Zatem proces przetwarzania danych osobowych przez skarżony podmiot rozpoczął się i zakończył przed 25 maja 2018 r.

Prezes UODO wskazał na art. 99 ust. 1 RODO, że rozporządzenie to ma zastosowanie od 25 maja 2018 r. W związku z tym, przepisy RODO mają zastosowanie wyłącznie w sprawach, w których skargę wniesiono od 25 maja 2018 r. i w tej dacie kwestionowany proces przetwarzania danych osobowych trwał.

Prezes UODO stwierdził, że z uwagi na fakt, iż kwestionowane w skardze zdarzenie miało miejsce i zakończyło się w czasie, gdy obowiązywały przepisy ustawy z 29 sierpnia 1997 r., a postępowanie administracyjne przed organem nadzorczym zostało zainicjowane w czasie, gdy zaczęły obowiązywać przepisy ustawy z 10 maja 2018 r., do rozstrzygnięcia przedmiotowej sprawy nie jest możliwe również zastosowanie przepisów ustawy z 29 sierpnia 1997 r. Zwrócił także uwagę, że art. 160 ust. 1 i 2 ustawy z 10 maja 2018 r. stanowi, że jedynie postępowania wszczęte i niezakończone przed dniem wejścia w życie ustawy z 10 maja 2018 r. są prowadzone przez Prezesa UODO na podstawie ustawy z 29 sierpnia 1997 r. Tym samym Prezes UODO nie ma możliwości prowadzenia postępowania administracyjnego w oparciu o przepisy ustawy z 29 sierpnia 1997 r., gdyż postępowanie w przedmiotowej sprawie zostało wszczęte po dniu wejścia w życie ustawy z 10 maja 2018

[69] DS.523.4880.2021.

r., brak było również podstawy do korzystania przez Prezesa UODO z uprawnień przewidzianych w uchylonej ustawie z 29 sierpnia 1997 r., w tym do oceny zgodności zachowania administratora z ww. przepisami, w przypadku gdy skarżony proces przetwarzania nie był kontynuowany po 25 maja 2018 r. Organ podkreślił również, że nie może dokonać oceny zgodności z RODO kwestionowanych w skardze działań administratora, ponieważ zdarzenie będące przedmiotem skargi miało charakter zakończony i nie było kontynuowane po 25 maja 2018 r. Ponadto brak jest obecnie przepisów kompetencyjnych uprawniających organ do prowadzenia postępowania w przedmiocie oceny zgodności działania administratora z przepisami ustawy z 29 sierpnia 1997 r.

Natomiast w zakresie legalności przetwarzania i udostępnienia na rzecz podmiotów trzecich przez ośrodek danych osobowych skarżącego w celu dochodzenia należności z tytułu wyżywienia byłego wychowanka, Prezes UODO nie stwierdził nieprawidłowości.

Ośrodek przetwarzał i udostępnił dane osobowe skarżącego w celu dochodzenia należności z tytułu wyżywienia byłego wychowanka w postępowaniu sądowym i windykacyjnym. Na podstawie dokumentacji osobowej byłego wychowanka pozyskanej ze starostwa ośrodek przyjął, że skarżący był osobą zobowiązaną do ponoszenia należności za pobyt małoletniego w ośrodku, co potwierdził w postępowaniu sądowym sąd rejonowy wydając nakaz zapłaty. Prezes UODO w decyzji wskazał, że sąd podejmując czynności zmierzające do wykonania tytułu wykonawczego bada, czy istnieje stosunek zobowiązaniowy między podmiotami wymienionymi w tytule wykonawczym. Zatem sąd rejonowy dokonał zapewne oceny, czy skarżący jest osobą zobowiązaną, wobec której prowadzona będzie egzekucja. Prezes UODO podkreślił, że jego rolą nie jest ocena zasadności dochodzenia przez ośrodek należności. Ocena ta leżała w gestii sądu i sąd tej oceny dokonał, uznając skarżącego za osobę zobowiązaną do ponoszenia kosztów związanych z pobytem byłego wychowanka w ośrodku.

Prezes UODO podkreślił również, że nie ma kompetencji do oceny ustaleń dokonanych w postępowaniu sądowym. Zaznaczył również, że skarżący mógł skorzystać z przysługujących mu uprawnień i złożyć sprzeciw wobec wydanego przez sąd rejonowy nakazu zapłaty.

Mając na uwadze fakt, iż sąd uznał za zasadne dochodzenie przez ośrodek należności od skarżącego, Prezes UODO nie dostrzegł nieprawidłowości w procesie przetwarzania danych osobowych skarżącego, podkreślając jednocześnie, że niezależnie od zgody osoby, której dane dotyczą – art. 6 ust. 1 lit. a) RODO – przetwarzanie danych osobowych jest dopuszczalne między innymi wtedy, gdy jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora – art. 6 ust. 1 lit. f) RODO. Natomiast wyegzekwowanie należności z tytułu wyżywienia byłego wychowanka ośrodka stanowi, w ocenie Prezesa UODO, prawnie usprawiedliwiony cel ośrodka. W zakresie niedopełnienia przez ośrodek obowiązków wynikających z art. 15, art. 17 i art. 21 RODO Prezes UODO udzielił ośrodkowi upomnienia. Ośrodek bowiem uchybił dyspozycji określonej w art. 12 ust. 3 RODO. Wobec tego, że ośrodek ani nie dochował terminu wskazanego w art. 12 ust. 3 RODO na realizację praw skarżącego wynikających z art. 15 ust. 1, ani nie poinformował skarżącego o przyczynie opóźnienia realizacji jego wniosku, Prezes UODO upomniał ośrodek w tym zakresie. Natomiast w zakresie skierowanych do ośrodka wniosków o realizacje uprawnień z art.17 ust. 1 lit. b)

i lit. c) oraz art. 21 ust. 1 RODO ośrodek nie dochował ciążącego na nim obowiązku ustosunkowania się do żądań skarżącego, przez co naruszył jego prawa wynikające z ww. przepisów, jak również uchybił terminom wynikającym z art. 12 ust. 3 i 4 RODO, co skutkowało udzieleniem przez Prezesa UODO upomnienia[70].

Nieuprawnione wykorzystanie danych osobowych kandydata na pracownika pozyskanych w procesie rekrutacji

Przedmiotem oceny Prezesa UODO w jednej ze spraw zakończonych w analizowanym roku sprawozdawczym były nieprawidłowości w przetwarzaniu danych osobowych skarżącego pozyskanych w procesie rekrutacji. Skarżący, uczestnicząc w procesie rekrutacji, przekazał potencjalnemu pracodawcy m.in. kopię dyplomu ukończenia studiów geodezyjnych w celu potwierdzenia swoich kwalifikacji zawodowych. Finalnie pomiędzy skarżącym a pracodawcą nie doszło jednak do nawiązania stosunku pracy.

Pracodawca był zleceniobiorcą regionalnego oddziału Agencji Restrukturyzacji i Modernizacji Rolnictwa (dalej: ARiMR) w zakresie kontroli działek rolnych metodą FOTO (geodezyjna kontrola przeprowadzana na podstawie ortofotomapy). Pracodawca, w celu uzyskania upoważnienia do kontroli metodą FOTO upraw rolników dla wskazanego pracownika, wykorzystał dane osobowe skarżącego i przekazał do ARiMR dokumenty zwierające jego dane osobowe, w tym kopię dyplomu ukończenia studiów oraz oświadczenie zawierające rzekomo podpis skarżącego. Skarżący o nieuprawnionym procederze dowiedział się po kontakcie z ARiMR. Pracodawca w toku prowadzonego przez organ postępowania administracyjnego wyjaśnił, iż do nieuprawnionego wykorzystania danych osobowych skarżącego pozyskanych w toku rekrutacji doszło wskutek błędu w wewnętrznej bazie danych oraz omyłki pracownika.

Prezes UODO nie stwierdził, by pracodawca legitymował się którąkolwiek z przesłanek wskazanych w art. 6 ust. 1 RODO w kwestionowanym procesie przetwarzania. Wobec tego Prezes UODO korzystając z przysługujących mu na mocy przepisów RODO uprawnień naprawczych, upomniał pracodawcę za niezgodne z prawem udostępnienie danych osobowych skarżącego[71].

Upublicznienie danych osobowych pracownika pełniącego funkcje publiczne na oficjalnym profilu Facebook prezydenta miasta

Prezes UODO rozpatrywał skargę na działanie urzędującego prezydenta miasta, który na swoim oficjalnym profilu Facebook upublicznił informacje o wysokości nagrody pracowniczej przyznanej przez ustępującego prezydenta miasta na rzecz pracownika urzędu miejskiego pełniącego funkcję zastępcy prezydenta.

Prezydent zasadność swojego działania argumentował tym, że upublicznienie informacji o wysokości przyznanej nagrody pracowniczej jest możliwe na gruncie przepisów ustawy o dostępie do informacji publicznej (u.d.i.p.), bowiem odnosi się do osoby pełniącej funkcje publiczne w zakresie dotyczącym wykonywania tych funkcji. Prezydent wskazał, że skarżący był funkcjonariuszem publicznym, a udostępnione dane pozostawały w związku z pełnioną przez niego funkcją. Prezydent podkreślił, iż udostępnienie danych osobowych skarżącego było konieczne, gdyż obrazowało przyczyny

[70] DS.523.3644.2020.
[71] DS.523.4536.2022.

problemów finansowych miasta i konieczność wprowadzenia w mieście planu oszczędnościowego.

W sprawie tej Prezes UODO podkreślił, iż nie kwestionuje uprawnień prezydenta do udostępnienia informacji o organizacji urzędu miejskiego, organach i osobach sprawujących w nich funkcje oraz ich kompetencjach, co wynika z art. 6 ust. 1 pkt 2 ustawy o dostępie do informacji publicznej. Organ zauważył jednak, iż zgodnie z art. 7 ust. 1 pkt 1 u.d.i.p. udostępnianie informacji publicznych następuje w drodze ogłaszania informacji publicznych, w tym dokumentów urzędowych, w Biuletynie Informacji Publicznej, o którym mowa w art. 8. Organ ustalił, że informacja publiczna figuruje nie na ogólnodostępnej stronie internetowej Biuletynu Informacji Publicznej urzędu miejskiego, a na portalu Facebook, konkretnie na profilu prezydenta miasta, który nie jest przestrzenią służącą do wypełniania przez prezydenta obowiązku zamieszczania informacji publicznej. Właściwym miejscem na udostępnienie informacji publicznej przez organ publiczny, którym jest niewątpliwie prezydent, z uwagi na konieczność zapewnienia transparentności jego działań, jest Biuletyn Informacji Publicznej. Udostępnienie danych osobowych pracownika urzędu miejskiego poza publikatorem urzędowym pozbawia prezydenta kontroli nad kwestionowanym procesem przetwarzania danych osobowych, a ponadto niesie za sobą wiele potencjalnych ryzyk naruszenia praw lub wolności osoby, której dane dotyczą. Udostępnienie ww. informacji poza wskazanym trybem dowodziło, że w sprawie nie dokonano właściwej analizy wskazanego ryzyka, a także nie zachowano zasad przetwarzania danych wynikających z przepisów o ochronie danych osobowych (art. 5 ust. 1 i 2 oraz art. 6 ust. 1 RODO).

Wobec stwierdzenia naruszenia ochrony danych osobowych skarżącego Prezes UODO nakazał prezydentowi miasta usunięcie z jego profilu Facebook upublicznionych danych osobowych skarżącego[72].

Posłużenie się umową o pracę na okres próbny zawierającą dane osobowe skarżącego, jako wzorem umowy udostępnianym osobom trzecim

W prowadzonej przez Prezesa UODO sprawie skarżący wskazywał na nieprawidłowości w przetwarzaniu jego danych osobowych polegające na udostępnianiu przez byłego pracodawcę jego danych osobowych (imienia, nazwiska, adresu, informacji o wysokości wynagrodzenia oraz zajmowanym stanowisku pracy, numeru konta bankowego) znajdujących się na umowie o pracę na okres próbny zawartej ze skarżącym na rzecz osób nieuprawnionych.

Przeprowadzając postępowanie wyjaśniające organ ustalił, że skarżący zawarł ze spółką umowę o pracę na okres próbny podając dane osobowe w zakresie imienia, nazwiska, adresu zamieszkania, wysokości wynagrodzenia, stanowiska pracy oraz numeru konta bankowego. Dane te następnie posłużyły spółce jako wzór umowy wysłanej wiadomością e-mail do osoby trzeciej.

W wydanej decyzji administracyjnej, mocą której organ upomniał spółkę za udostępnienie danych osobowych skarżącego pozyskanych przez spółkę w związku z jego zatrudnieniem, Prezes UODO wskazał, że przepisy RODO zobowiązują administratora do przetwarzania danych osobowych zgodnie z prawem w sposób rzetelny i przejrzysty (art. 5 ust. 1 lit. a RODO). Co więcej, oceniając zgłoszone przez skarżącego naruszenie organ

[72] DS.523.101.2021.

zauważył, że administrator jest zobligowany do uaktualniania danych oraz podejmowania także niezwłocznie takich działań, które prowadzą do sprostowania lub usunięcia danych, których przetwarzanie jest zbędne – art. 5 ust.1 lit. d) RODO. Działania spółki opisane w przeprowadzonym postępowaniu nie wykazały, by udostępniając wzór umowy o pracę osobie trzeciej dochowała ona należytej staranności w ocenie, czy na wzorze tym nie znajdują się dane osoby faktycznie przez nią zatrudnianej. Wobec braku zachowania ostrożności skutkującego udostępnieniem danych osobowych skarżącego, zawartych w treści umowy o pracę na rzecz osób nieuprawnionych doszło do udostępnienia danych osobowych skarżącego w zakresie: imienia, nazwiska, adresu, wysokości wynagrodzenia, stanowiska pracy, numeru rachunku bankowego, co stanowiło naruszenie przez spółkę przepisów o ochronie danych osobowych, w szczególności art. 5 ust. 1 lit. a) oraz art. 6 ust. 1 RODO[73].

Udostępnienie danych pracownika przez pracodawcę w zakresie informacji o przyczynie rozwiązania stosunku pracy na rzecz pozostałych współpracowników

Przedmiotem oceny Prezesa UODO była skarga byłego pracownika na nieprawidłowości w procesie przetwarzania jego danych osobowych przez pracodawcę. Polegały one na tym, że pracodawca – w korespondencji mailowej skierowanej do współpracowników – poinformował, że zakończył współpracę ze skarżącą, a powodem tego było niezrealizowanie przez nią planu narzuconego wcześniej przez pracodawcę. Prezes UODO, po przeprowadzeniu postępowania administracyjnego wydał decyzję, mocą której udzielił administratorowi upomnienia za naruszenie art. 5 ust. 2 RODO oraz art. 6 ust. 1 RODO. Prezes UODO wskazał, że pracodawca wykonując swoje obowiązki związane z rozwiązywaniem umowy o pracę, a także nieprzedłużaniem tej umowy, jest związany przepisami prawa, a zwłaszcza przepisami prawa pracy uregulowanymi w szczególności w przepisach K.p. oraz innych ustawach i aktach wykonawczych dotyczących stosunku pracy. Przepisy K.p. określają sposób postępowania pracodawców przy wypowiadaniu pracownikowi umowy o pracę. Nie przewidują one natomiast uprawnienia pracodawcy do przekazywania informacji innym pracownikom na temat przyczyny zakończenia stosunku pracy danego pracownika. Organ zwrócił uwagę, że pracodawca posiada status administratora wobec danych osobowych swoich pracowników. Z tego względu jest on zobowiązany przestrzegać reguł wynikających z unormowań przepisów RODO. Informacje dotyczące pracowników, w tym odnoszące się do określonych zdarzeń, tj. wypowiedzenie umowy o pracę, nieprzedłużenie tej umowy, mogą być dostępne jedynie dla ograniczonego kręgu osób u danego pracodawcy. Wśród nich wymienić można np. osoby zarządzające zakładem pracy w imieniu pracodawcy, radców prawnych świadczących dla pracodawcy usługi prawne czy też osoby zajmujące się sprawami kadrowymi. Wskazane powyżej osoby, w ramach wykonywanych obowiązków, są najczęściej upoważnione do przetwarzania danych osobowych innych pracowników w danym zakładzie pracy[74].

Monitoring pracownika z wykorzystaniem systemu GPS

[73] DS.523.4329.2022.
[74] DS.523.1924.2023.

Prezes UODO otrzymał również skargę dotyczącą instalacji systemu GPS w samochodzie służbowym i prowadzenia przez pracodawcę monitoringu pracownika w tym zakresie. Pomimo iż zasady przetwarzania danych osobowych w związku ze stosowaniem monitoringu, w tym monitoringu GPS, zostały wprowadzone znowelizowanymi przepisami Kodeksu pracy (K.p.) w 2018 r. nadal wiele podmiotów nie uregulowało na piśmie celów, zakresu oraz sposobów zastosowania tego monitoringu w organizacji.

Skarżący przyznał, że został poinformowany przez zarząd spółki ustnie o fakcie wyposażenia pojazdów służbowych w monitoring GPS. Spółka jednak nie dopełniła ciążących na niej obowiązków wynikających z ww. przepisów, m.in. nie ustaliła celów, zakresu oraz sposobu zastosowania monitoringu w regulaminie pracy, ani nie poinformowała o powyższym skarżącego na piśmie przed dopuszczeniem go do pracy, czym w ocenie Prezesa UODO naruszyła art. 13 ust. 1 i 2 RODO w zw. z art. 22³ § 4 K.p.[75]

Udostępnienie danych osobowych małoletniego na grupie internetowej osobom nieuprawnionym

Przedmiotem postępowania przed Prezesem UODO były nieprawidłowości w przetwarzaniu danych osobowych małoletniego na grupie internetowej w mediach społecznościowych przedszkola z oddziałami integracyjnymi, polegające na udostępnieniu listy dzieci przyjętych do grupy przedszkolnej z imieniem i nazwiskiem małoletniego z dopiskiem litery „o". Skarżąca, będąca opiekunem prawnym małoletniego, podniosła w treści skargi, iż jej zdaniem dopisek „o" stanowił ujawnienie danych osobowych szczególnej kategorii i miał on oznaczać orzeczenie o niepełnosprawności i potrzebie kształcenia specjalnego. Przedszkole wskazało, że nauczyciel bez wiedzy oraz zgody przedszkola umieścił na zamkniętej grupie internetowej roboczą listę grupy dzieci przyjętych na nowy rok szkolny do przedszkola, a do listy nie była załączona legenda znaku „o" i z listy nie wynikało jego znaczenie, na przykład, że dziecko podlega obserwacji, ma opinię, orzeczenie lub wymaga dodatkowego odpoczynku.

W ocenie Prezesa UODO przedszkole uznawało grupę internetową jako jeden z kanałów komunikacji z rodzicami. Nie było możliwe przyjęcie, że nauczyciel, który ujawnił na grupie internetowej listę dzieci zawierającą dane małoletniego, działał jako samodzielny i niezależny administrator. Nauczyciel ujawnił listę stworzoną przez przedszkole wobec rodziców dzieci do niego przyjętych. Nie wykonywał on więc czynności o czysto prywatnym charakterze, lecz podejmował działania bezpośrednio związane ze swoją pracą na rzecz przedszkola – administratora znajdujących się na ujawnionej liście. Wobec tego to przedszkole ponosiło odpowiedzialność za ujawnienie osobom nieuprawnionym danych osobowych małoletniego znajdujących się na liście.

Pomimo wskazania przez przedszkole sposobu, w jaki dokonywano weryfikacji osób mających dostęp do zamkniętej grupy internetowej, przedszkole nie wykazało żadnej podstawy prawnej ujawnienia w takiej formie danych osobowych dzieci przyjętych do przedszkola. Art. 158 ustawy prawo oświatowe, która w dniu udostępnienia listy, tj. 5 lipca 2022 r. obowiązywała w wersji od 4 czerwca do 12 sierpnia 2022 r.[76] przewidywał, że wyniki postępowania rekrutacyjnego podaje się do publicznej wiadomości w formie listy

[75] DS.523.3182.2023.
[76] Ustawa z 14 grudnia 2016 r. - Prawo oświatowe (Dz. U. z 2024 r. poz. 737 ze zm.).

kandydatów poprzez umieszczenie jej w widocznym miejscu w siedzibie danego podmiotu. Listy te zawierają imiona i nazwiska kandydatów uszeregowane w kolejności alfabetycznej oraz najniższą liczbę punktów, która uprawnia do przyjęcia. Przedszkole zaś nie powołało się w swoich wyjaśnieniach na żadne konkretne przepisy pozwalające na odstępstwo od rozwiązań przyjętych w art. 158 ustawy prawo oświatowe i publikację danych w innej formie – w tym przypadku publikację danych na zamkniętej grupie internetowej.

W ocenie Prezesa UODO umieszczenie na ujawnionej liście dopisku „o" przy nazwisku małoletniego, nawet w kontekście uczęszczania przez niego do przedszkola z oddziałami integracyjnymi, nie pozwalało na wysnucie jednoznacznego wniosku, że dopisek ten odnosił się do stanu zdrowia małoletniego w postaci niepełnosprawności oraz potrzeby kształcenia specjalnego. Prezes UODO nie uznał, że dopisek „o" przy nazwisku małoletniego pozwalał na jednoznaczne i bezsporne stwierdzenie, że małoletni jest osobą niepełnosprawną z potrzebą kształcenia specjalnego, jak podnosiła skarżąca, a tym samym Prezes UODO nie uznał, że doszło do ujawnienia szczególnej kategorii danych osobowych. Prezes UODO stwierdził, że doszło do ujawnienia danych osobowych małoletniego jedynie w postaci jego imienia i nazwiska poprzez umieszczenie listy dzieci przyjętych do przedszkola na zamkniętej grupie internetowej, mimo że prawo oświatowe nie przewiduje takiej formy i nie zostały wykazane żadne podstawy dla odstępstwa od właściwych przepisów prawa oświatowego. Ze względu na fakt, że lista dzieci przyjętych do przedszkola została usunięta tego samego dnia, w którym ją opublikowano, Prezes UODO zadecydował, że wystarczające będzie zastosowanie wobec przedszkola upomnienia[77].

1.1.4. Sektor finansów, telekomunikacji i ubezpieczeń

W omawianym roku 2023 działalność Prezesa Urzędu Ochrony Danych Osobowych w obszarze sektora finansowego, ubezpieczeń i telekomunikacji skupiała się, podobnie jak w latach poprzednich, na rozpatrywaniu skarg osób kwestionujących proces przetwarzania ich danych związanych z zawieraniem różnego rodzaju umów, przede wszystkim umów skutkujących powstaniem zobowiązań finansowych po stronie osób skarżących, co wiązało się następnie także z dochodzeniem roszczeń majątkowych przez firmy windykacyjne, którym wierzyciele zlecali dochodzenie wierzytelności, ale także przez fundusze inwestycyjne, które w drodze cesji wierzytelności nabyły wierzytelności od wierzycieli pierwotnych, oraz przez podmioty zarządzające portfelem wierzytelności funduszy inwestycyjnych. Organ często podkreślał w rozstrzygnięciach wydanych w ww. sprawach, że rozwiązywanie sporów dotyczących istnienia roszczeń, czy też skuteczności zawierania umów, w tym umów będących źródłem tychże roszczeń, pozostaje poza zakresem kompetencji przysługujących Prezesowi UODO. Organ władny był wyłącznie do oceny procesu przetwarzania danych związanego z powyższymi zagadnieniami.

Znaczna część skarg wpływających do organu nadzorczego dotyczyła działalności podmiotów sektora finansowego, takich jak: banki, instytucje pożyczkowe, spółdzielcze kasy oszczędnościowo-kredytowe, instytucje utworzone na podstawie art. 105 ust. 4

[77] DS.523.1084.2023.

Prawa bankowego[78], związanej z przetwarzaniem danych osobowych w związku z dokonywaniem oceny zdolności kredytowej i analizy ryzyka kredytowego.

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

Wiele skarg, które wpłynęły do Prezesa Urzędu Ochrony Danych Osobowych w 2023 r., podobnie jak w latach poprzednich, dotyczyła procesów przetwarzania danych osobowych klientów banków w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Osoby wnoszące skargi dotyczące ww. procesu przetwarzania danych osobowych kierowały się z reguły zamiarem poprawy swojej zdolności kredytowej i wyeliminowania takiego nielegalnego – w ich ocenie – procesu przetwarzania ich danych osobowych, który może im w przyszłości utrudnić lub nawet uniemożliwić uzyskanie kredytu lub pożyczki.

Banki, jako instytucje uprawnione do udzielania kredytów, mają obowiązek przeprowadzania oceny zdolności kredytowej osób ubiegających się o udzielenie kredytu, a także analizy ryzyka kredytowego. Powyższy obowiązek wynika z art. 70 Prawa bankowego, zgodnie z którym 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. Regulacje dotyczące uprawnienia do przetwarzania informacji stanowiących tajemnicę bankową zawarto w art. 105a Prawa bankowego, w ramach którego ustawodawca przewidział różne sytuacje mogące stanowić podstawę przetwarzania danych osobowych. W ust. 1 ww. przepis reguluje ww. uprawnienie przed oraz w trakcie istnienia zobowiązania, natomiast ust. 2, 3 – po wygaśnięciu zobowiązania.

Przetwarzanie danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego po wygaśnięciu zobowiązania, wynikającego z zawartej umowy

Prezes UODO oceniał m.in. przetwarzanie danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego w oparciu o art. 105a ust. 3 Prawa bankowego. Powyższy przepis reguluje kwestie uprawnienia do przetwarzania danych osobowych kredytobiorców w celu oceny zdolności kredytowej i analizy ryzyka kredytowego po wygaśnięciu zobowiązania (np. w wyniku jego spłaty) bez zgody podmiotu danych. Dopuszczalność kwestii ww. przetwarzania danych osobowych stanowi często oś sporu podmiotów danych z administratorami danych będącymi bankami.

Należy zauważyć, że zgodnie z brzmieniem ww. przepisu banki, instytucje oraz podmioty, o których mowa w art. 105a ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową i informacje udostępnione przez instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z 12 maja 2011 r. o kredycie konsumenckim, dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z: bankiem, inną instytucją ustawowo upoważnioną do udzielania kredytów, instytucją pożyczkową lub podmiotem, o którym mowa w art. 59d ustawy z 12 maja 2011 r. o kredycie konsumenckim, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem, inną instytucją ustawowo upoważnioną do udzielania kredytów, instytucją pożyczkową lub podmiotem, o którym mowa w art.

[78] Ustawa z 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2023 r. poz. 2488 ze zm.).

59d ustawy z 12 maja 2011 r. o kredycie konsumenckim, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez: bank, inną instytucję ustawowo upoważnioną do udzielania kredytów, instytucję pożyczkową albo podmiot, o którym mowa w art. 59d ustawy z 12 maja 2011 r. o kredycie konsumenckim, o zamiarze przetwarzania dotyczących jej tych informacji, bez jej zgody. Powyższy przepis formułuje zatem kilka wymogów, które banki muszą spełnić, aby móc przetwarzać informacje o zobowiązaniu oraz których spełnienie bank powinien być w stanie wykazać. Wykazanie przez banki spełnienia ww. wymogów warunkuje zaś w takim przypadku możliwość przetwarzania danych w sposób legalny, co jest o tyle istotne, że związany z tym proces przetwarzania danych osobowych rzutować może na zdolność kredytową osoby, której dane dotyczą.

Powyższy przepis nie uzależnia uprawnienia do ww. przetwarzania danych od zgody podmiotu danych, lecz od spełnienia przez administratora danych wymogów w zakresie zwłoki oraz poinformowania podmiotu danych o zamiarze przetwarzania danych osobowych w ww. celu. W wydanych w 2023 r. decyzjach Prezes UODO wskazał, że chociaż sam przepis nie ustanawia żadnych konkretnych wymogów odnośnie do sposobu poinformowania podmiotu danych, nie oznacza to jednak pełnej dobrowolności w tym zakresie[79] – administrator musi wykazać, że upłynęło 30 dni od dnia poinformowania podmiotu danych o zamiarze przetwarzania jego danych osobowych w oparciu o art. 105a ust. 3 Prawa bankowego. Oznacza to, że sposób poinformowania powinien być wykonany w taki sposób, aby możliwe było jednoznaczne ustalenie początku biegu ww. terminu[80]. Ustaleń w powyższym zakresie nie można opierać na domniemaniach[81]. W świetle powyższego Prezes UODO przyjmował w swoich decyzjach, że przedłożenie dowodów na sporządzenie i wysłanie pisma zawierającego informację, o której mowa w art. 105a ust. 3 Prawa bankowego, nie stanowi dowodu na to, że doszło do poinformowania podmiotu danych o zamiarze przetwarzania jego danych stanowiących tajemnicę bankową, bez jego zgody, na podstawie art. 105a ust. 3 Prawa bankowego[82]. Sam fakt, iż dłużnik nie wykonał zobowiązania lub spóźnił się z jego wykonaniem co najmniej 60 dni, nie upoważnia banku do przetwarzania jego danych na warunkach określonych w art. 105a ust. 3 Prawa bankowego[83].

W analizowanym roku 2023 Prezes UODO rozpoznawał także skargi na proces przetwarzania danych osobowych, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, dokonywany przez instytucje pożyczkowe. W wydanych decyzjach stwierdzał, że instytucje pożyczkowe nie przedstawiły dowodów na spełnienie wobec osób, których dane dotyczą, obowiązku określonego w art. 105a ust. 3 Prawa bankowego, tj. nie wykazały, iż doszło do skutecznego poinformowania o zamiarze przetwarzania dotyczących ich informacji, stanowiących tajemnicę bankową, bez zgody po wygaśnięciu

[79] Zob. również: wyrok Naczelnego Sądu Administracyjnego z 7 sierpnia 2018 r., sygn. akt I OSK 2123/16.
[80] DS.523.7702.2021, zob. również: wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 18 stycznia 2022 r. sygn. akt II SA/Wa 3584/21.
[81] DS.523.4869.2021, tak również: wyrok Naczelnego Sądu Administracyjnego z 27 sierpnia 2019 r. sygn. akt I OSK 2514/17.
[82] DS.523.5517.2020, DS.523.110.2022.
[83] DS.523.44.2022.

zobowiązań, wynikających z umów[84]. Podobne decyzje zapadły również w odniesieniu do spółdzielczych kas oszczędnościowo-kredytowych[85].

Wydano również decyzje, w których uznano, że powyższe instytucje wykazały spełnienie wobec skarżących ww. obowiązku – w takich sytuacjach organ legalizował procesy przetwarzania danych osobowych skarżących na podstawie przesłanki z art. 6 ust. 1 lit. f) RODO[86].

Niezależnie od regulacji zawartych w art. 105a ust. 3 Prawa bankowego banki oraz inne instytucje wymienione w art. 105a ust. 1 Prawa bankowego mogą przetwarzać dane osobowe po wygaśnięciu zobowiązania również na podstawie zgody, opierając się na w oparciu o art. 105a ust. 2 Prawa bankowego. W przypadku ustalenia, że osoba, której dane dotyczą, wyraziła zgodę, o której mowa w ww. przepisie, Prezes UODO stwierdzał legalność przetwarzania danych osobowych, po wygaśnięciu zobowiązania, wynikającego z zawartej z bankiem lub ww. instytucją umowy[87].

Przetwarzanie danych osobowych przez bank w związku z istniejącym zobowiązaniem, wynikającym z zawartej umowy

Art. 105a ust. 3 Prawa bankowego dotyczy przetwarzania danych osobowych po wygaśnięciu zobowiązania. Natomiast w przypadku, gdy zobowiązanie nadal istnieje (np. nie zostało spłacone lub rachunek bankowy nadal jest otwarty), proces przetwarzania danych osobowych prowadzony może być zgodnie z art. 105a ust. 1 Prawa bankowego, który ma zastosowanie w przypadku oceny zdolności kredytowej i analizy ryzyka kredytowego przed powstaniem zobowiązania oraz w trakcie jego istnienia[88]. Chociaż w części postępowań podmioty danych kwestionowały proces przetwarzania danych osobowych wskazując, że odbywa się on nielegalnie, w oparciu o art. 105a ust. 3 Prawa bankowego, po przeprowadzeniu postępowania administracyjnego okazywało się, że proces ten nie dotyczy istniejącego zobowiązania wobec banku, nie zaś tego, które wygasło. Wówczas Prezes UODO w swoich rozstrzygnięciach stwierdzał, że w związku z istniejącym zobowiązaniem kwestionowany proces przetwarzania danych jest legalnie kontynuowany na podstawie art. 105a ust. 1 Prawa bankowego. W jednej z decyzji, w kontekście przetwarzania dokonywanego w oparciu o art. 105a ust. 1 Prawa bankowego, Prezes UODO uznał, że bank na ww. podstawie prawnej – w celu oceny zdolności kredytowej i analizy ryzyka kredytowego – może przetwarzać również dane poręczycieli[89].

Przetwarzanie danych osobowych w związku ze złożeniem zapytania kredytowego

Do licznie wnoszonych skarg zaliczyć także należy te dotyczące przetwarzania danych osobowych przez banki oraz instytucje utworzone na podstawie art. 105 ust. 4 Prawa bankowego, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego w związku z obsługą zapytań kredytowych, które nie zakończyły się zawarciem umowy kredytu. Prezes Urzędu Ochrony Danych Osobowych w wydawanych decyzjach odnosił się m.in. do powoływanych przez podmioty skarżone jako podstawy prawne przetwarzania danych osobowych wynikających z niezakończonych zawarciem umowy zapytań

[84] DS.523.7621.2021.
[85] DS.523.4219.2021.
[86] DS.523.6650.2020, DS.523.2093.2022, DS.523.1417.2022.
[87] DS.523.910.2021.
[88] ZSPR.440.591.2019.
[89] DS.440.400.2019.

kredytowych, m.in. art. 105a ust. 1 w zw. z art. 70 ust. 1 Prawa bankowego, konsekwentnie wskazując, że w przypadku odmowy udzielenia kredytu cel przetwarzania w postaci oceny zdolności kredytowej i analizy ryzyka kredytowego został zrealizowany i brak jest podstaw prawnych do kontynuowania tego procesu po dokonaniu przedmiotowej oceny[90]. W konsekwencji Prezes UODO uznawał, że takie przetwarzanie danych osobowych w zakresie wynikającym z zapytań kredytowych po dokonaniu oceny zdolności kredytowej jest niedopuszczalne, bowiem nie znajduje uzasadnienia w którejkolwiek z przesłanek uregulowanych w art. 6 ust. 1 RODO. Analogiczna sytuacja miała miejsce również w przypadku powołania się na art. 9 ust. 1 ustawy o kosztach komorniczych[91].

Przetwarzanie przez bank danych osobowych utrwalonych w skanach dowodów osobistych

Prezes UODO w analizowanym roku 2023 oceniał również legalność przetwarzania przez bank danych osobowych pozyskanych w wyniku wykonania skanu dowodu osobistego osoby, która zgłosiła się do banku wyłącznie w celu otrzymania potwierdzenia spłaty kredytu. Zgodnie z art. 112b Prawa bankowego banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych. Powyższe jest jednak legalne wyłącznie wtedy, kiedy taki obowiązek nakłada na bank przepis rangi ustawy. Co istotne, powyższy przepis nie przewiduje obowiązku pozyskiwania kopii dowodów tożsamości, a jedynie w sposób ogólny reguluje uprawnienie do przetwarzania informacji w nich zawartych. Dodatkowo art. 33 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[92] nakłada na określony katalog „instytucji obowiązanych" obowiązek m.in. stosowania wobec swoich klientów środków bezpieczeństwa finansowego (art. 33 ust. 1 ustawy AML). Zgodnie z art. 34 ust. 1 ustawy AML środki bezpieczeństwa obejmują m.in. identyfikację klienta oraz weryfikację jego tożsamości, natomiast zgodnie z art. 34 ust. 4 ustawy AML 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.

Należy jednak podkreślić, że nie każda wizyta osoby, której dane dotyczą, w oddziale banku wiązać się będzie z obowiązkiem zastosowania środków bezpieczeństwa finansowego. Ustawa AML wyraźnie wskazuje sytuacje, kiedy bank jako instytucja obowiązana ma obowiązek zastosowania środków bezpieczeństwa finansowego, przesłanki ich stosowania określone zostały bowiem w art. 35 ustawy AML. Prezes UODO wyraził przekonanie, że w każdym przypadku decyzja o pozyskaniu danych osobowych, poprzez wykonanie skanu dokumentu tożsamości, powinna być poprzedzona analizą i zweryfikowaniem, czy rzeczywiście taka czynność jest niezbędna, zgodnie z zasadami zgodności z prawem, celowości i minimalizacji, do których przestrzegania administratorzy danych, w tym banki, zobowiązane są na podstawie art. 5 ust. 1 lit. a), b) i c) RODO.

W omawianej sprawie ustalono, że osoba, której dane dotyczą spłaciła kredyt, a następnie udała się do oddziału banku, by uzyskać potwierdzenie jego spłacenia. Tymczasem bank uzależnił udzielenie tej osobie ww. potwierdzenia od wykonania skanu

[90] DS.523.932.2020.
[91] DS.523.8376.2021.
[92] Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124 ze zm.), zwana dalej „ustawą AML".

jej dowodu osobistego. W ocenie Prezesa UODO bank powinien w pierwszej kolejności rozważyć, czy do realizacji celu, jakim w tym przypadku było udzielenie osobie, której dane dotyczą, informacji o spłaconym kredycie, niezbędne było pozyskanie skanu jej dowodu osobistego z utrwalonymi w nim jej danymi osobowymi. W ocenie organu, w świetle ww. przepisów, taka niezbędność nie zachodziła, co przyznał także bank uznając, że wykonanie przez pracownika banku skanu dowodu osobistego było w tym przypadku działaniem nadmiarowym, w wyniku którego doszło do nieuprawnionego przetwarzania danych osobowych. Ostatecznie skan ten został usunięty.

W przedmiotowej sprawie Prezes UODO uznał, że w powyższej sytuacji kwestionowany proces przetwarzania polegający na pozyskaniu danych zawartych w skanie dowodu tożsamości po zakończeniu obowiązywania umowy z bankiem, nie znajdował oparcia w żadnej z przesłanek wynikających z art. 6 ust. 1 RODO[93].

Przetwarzanie danych osobowych przez firmy windykacyjne w celu dochodzenia wierzytelności nabytych w wyniku cesji wierzytelności

Znaczna część postępowań, zakończonych w analizowanym okresie sprawozdawczym, dotyczyła przetwarzania danych w związku z dochodzeniem roszczeń[94]. W tego rodzaju postępowaniach poruszana była często kwestia udostępniania danych przez wierzyciela pierwotnego na rzecz innego podmiotu, opierając się na zawieranych na podstawie art. 509 K.c. umowach cesji wierzytelności, które wiążą się z uprawnieniem do przekazania nabywcy danych osobowych dłużnika, umożliwiających podjęcie względem niego stosownych działań – zmierzających do odzyskania należności. Organ nadzorczy dostrzegł, że dopuszczalność przelewu wierzytelności nie podlega ograniczeniom umownym ani ustawowym. Nie była również wymagana zgoda osoby, której dane dotyczą, na przelew wierzytelności. Prezes UODO w postępowaniach tych stwierdzał najczęściej, że udostępnienie danych osobowych przez wierzycieli w oparciu o umowy cesji wierzytelności nie może być oceniane jako naruszające prawa i wolności osoby, której dane dotyczą, będącej dłużnikiem. Prezes UODO wskazywał, że osoba ta, jako dłużnik, musi liczyć się z tym, że popadając w zwłokę w spełnieniu zobowiązania, jej prawo do prywatności może zostać ograniczone ze względu na dochodzenie przez wierzyciela należnych mu wierzytelności. W przeciwnym przypadku mogłoby dojść do sytuacji, w której dłużnik, powołując się na prawo do ochrony danych osobowych (prawo do prywatności), skutecznie uchyliłby się od spoczywającego na nim obowiązku spełnienia świadczenia i w konsekwencji ograniczone zostałoby prawo wierzyciela do uzyskania należnej mu zapłaty. Wobec powyższego udostępnienie przez zbywcę wierzytelności danych osobowych na podstawie zawartych umów cesji wierzytelności jest dokonywane w zakresie niezbędnym do osiągnięcia celu, jakim jest sprzedaż wierzytelności przysługującej zbywcy wobec osoby, której dane dotyczą, i stanowi prawnie uzasadniony cel administratora, o którym mowa w art. 6 ust. 1 lit. f) RODO. W przypadku gdy udostępnienie to dokonane zostało w zakresie niezbędnym do osiągnięcia tego celu, to jako takie nie narusza praw i wolności dłużnika.

Udostępnianie danych dłużników na giełdach wierzytelności

[93] DS.523.1175.2020.

[94] DS.440.125.2019, DS.523.1921.2022, DS.523.6473.2021, DS.523.1776.2022, DS.523.2545.2021, DS.523.701.2021.

Prezes UODO dokonywał oceny legalności procesu udostępniania danych osobowych dłużników na giełdach wierzytelności. W ocenie organu nadzorczego publikacja danych dłużnika na giełdzie wierzytelności nie może być postrzegana jako naruszenie jego praw i wolności. Powyższe stanowi dopuszczalne ograniczenie tych praw, a tym samy proces przetwarzania danych związany z publikacją danych na giełdzie wierzytelności znajduje uzasadnienie w przesłance z art. 6 ust. 1 lit. f) RODO. Organ uznał również, że administrator, który oferuje na stronie internetowej giełdy wierzytelności i jej podstronach do sprzedaży wierzytelność, ujawnia dane osobowe w zakresie: imienia, nazwiska, adresu w postaci nazwy miejscowości oraz nazwy ulicy, lecz bez numeru nieruchomości oraz wysokości zadłużenia, działa zgodnie z określoną w art. 5 ust. 1 lit. c) RODO zasadą minimalizacji, zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych")[95].

Udostępnienie danych osobowych w związku z wydaniem osobie trzeciej duplikatu karty SIM

Przedmiotem jednej ze spraw było zdarzenie polegające na wydaniu osobie trzeciej przez operatora telekomunikacyjnego duplikatu karty SIM przypisanej do skarżącego. Na duplikacie karty SIM znajdowały się dane w zakresie numeru SIM, kodu PUK i PIN. Karta SIM umożliwia dostęp do usług telekomunikacyjnych świadczonych przez danego operatora telekomunikacyjnego. Znajduje się na niej numer SIM, który jest unikalnym numerem identyfikującym abonenta. Ponadto na tzw. „ramce", do której przymocowana jest ww. karta, znajduje się kod PIN i PUK, które umożliwiają korzystanie i odblokowanie karty SIM. Organ powołał wyrok Trybunału Sprawiedliwości UE, który w wyroku *Digital Rights Ireland* z 8 kwietnia 2014 r. podkreślił znaczenie danych telekomunikacyjnych, wskazując, że mogą one dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane[96]. Prezes UODO uznał, że informacje, które wiążą się z określoną osobą – choćby pośrednio – niosą o niej pewien komunikat. Dlatego też informacją dotyczącą osoby jest zarówno ta odnosząca się do niej wprost, jak i ta, która dotyczy bezpośrednio przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio stanowi informację także o niej samej. Organ uznał, że doszło do udostępnienia nieuprawnionej osobie trzeciej danych osobowych skarżącego w zakresie: numeru telefonu i SIM, kodu PUK oraz PIN, bowiem osoba trzecia mogła, dysponując tymi danymi, dokonać jednoznacznej identyfikacji skarżącego.

Dynamiczny adres IP jako dane osobowe

W roku 2023 organ nadzorczy wydał również wobec podmiotów sektora telekomunikacyjnego szereg decyzji upominających za nieprawidłową realizację żądania, wniesionego w trybie art. 15 ust. 3 RODO udostępnienia kopii dynamicznego adresu IP. W przedmiotowych sprawach organ zajął stanowisko, zgodnie z którym dynamiczny numer IP stanowi dane osobowe w myśl art. 4 pkt 1 RODO, a w związku z tym osoba, której dane

[95] DS.523.701.2020, ZWOS.440.5452.2019, ZSPR.440.1177.2019.
[96] Wyrok TS z 8.4.2014 r. w sprawach połączonych C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.*, EU:C:2014:238.

dotyczą, jest uprawniona do otrzymania kopii danych w tym zakresie w trybie art. 15 ust. 3 RODO. W uzasadnieniu prawnym sentencji przedmiotowych decyzji organ powołał się m.in. na stanowisko Grupy Roboczej art. 29[97]. W przedmiotowych sprawach Prezes Urzędu Ochrony Danych Osobowych stanął na stanowisku, że operator telekomunikacyjny zobowiązany jest do przetwarzania tego rodzaju danych na podstawie przepisów prawa telekomunikacyjnego przez okres 12 miesięcy, stosownie do treści art. 180a ust. 1 pkt 1 ustawy PT. Niektórzy z administratorów spełnili żądania dopiero na skutek złożenia przez osoby, których dane dotyczą, skarg do Prezesa UODO, tym samym udzielili oni odpowiedzi z naruszeniem terminu wskazanego w art. 12 ust. 3 RODO. W pozostałych natomiast przypadkach doszło upływu okresu retencji danych, który – stosownie do treści art. 180a ust. 1 pkt 1 ustawy PT – wynosi 12 miesięcy, licząc od dnia połączenia, a zatem nie było możliwe wydania decyzji nakazującej spełnienie żądania w powyższym zakresie. W związku z tym Prezes UODO udzielił upomnień operatorom telekomunikacyjnym za naruszenie art. 15 ust. 3 w zw. z art. 12 ust. 3 RODO, polegające odpowiednio na spełnieniu żądania z naruszeniem terminu wskazanego w art. 12 ust. 3 RODO lub niezasadnej odmowie spełnienia żądania w tym terminie[98].

Umieszczenie na karcie SIM kontaktów SDN, zawierających informacje o usługach, jako przetwarzanie danych w celach marketingowych

Przedmiotem oceny Prezesa UODO była również kwestia przetwarzania danych osobowych w celach marketingowych w związku z umieszczeniem na karcie SIM osoby, której dane dotyczą, kontaktów SDN zawierających ofertę usług. Organ nadzorczy zauważył, że karta SIM jest urządzeniem, o którym mowa w art. 2 pkt 43 Prawa telekomunikacyjnego, zgodnie z którym telekomunikacyjne urządzenie końcowe jest to urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci. Wskazuje się, że urządzeniem końcowym *sensu stricto* jest ta część urządzenia, która jest przeznaczona do współpracy z siecią. Urządzeniem końcowym może być zatem nie całe urządzenie techniczne, lecz znaczący element (podzespół) urządzenia. Z kolei za marketing należy uznać informację o produktach, które stanowią podkreślenie ich atrakcyjności i nakłonienie do działania polegającego na skorzystaniu z prezentowanej oferty. Ponadto działania marketingowe mają nie tyle informować, co przekonywać do podjęcia określonych działań poprzez oddziaływanie na emocje odbiorcy. W ocenie Prezesa UODO w przedmiotowej sprawie nazwy kontaktów SDN prezentowane na karcie SIM skarżącego miały na celu zachęcenie go do skorzystania z dodatkowych usług oferowanych przez administratora. Kontakty te, oprócz numeru kontaktowego, zawierały także informację na temat ceny danej usługi wraz z wyrazem „włącz", zachęcającym do ich aktywacji. W ocenie Prezesa UODO zamieszczenie tego rodzaju treści w nazwach kontaktów SDN stanowi marketing bezpośredni i tym samym świadczy o przetwarzaniu danych osobowych skarżącego w celach marketingowych. Wskazane kontakty SDN zostały umieszczone na karcie SIM, którą należy uznać za urządzenie końcowe *sensu stricto.* Organ wskazał, że wynikający z art. 172 Prawa

[97] Grupa Robocza ds. Ochrony Danych Osobowych powołana na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 95.281.31 ze zm.).
[98] DS.523.5413.2020, DS.523.5418.2020, DS.523.5426.2020, DS.523.5427.2020, DS.523.5415.2020, DS.523.5625.2020, DS.523.6228.2020.

telekomunikacyjnego zakaz wykorzystania telekomunikacyjnych urządzeń końcowych bez zgody abonenta lub użytkownika końcowego dotyczy wykorzystania tych urządzeń po stronie nadawcy komunikatów marketingowych, czyli w przedmiotowej sprawie – po stronie administratora jako podmiotu, który przekazał skarżącemu kartę SIM ze znajdującymi się na niej kontaktami SDN. Administrator, zamieszczając treści marketingowe na wskazanej karcie SIM, powinien uzyskać na to uprzednią ww. zgodę skarżącego. Organ podkreślił, że nie jest to zgoda na podstawie art. 6 ust. 1 lit. a) RODO, niemniej jednak jej wyrażenie jest niezbędne, aby uznać za legalny proces przetwarzania danych osobowych w celu związanym z prowadzeniem marketingu bezpośredniego z użyciem telefonicznego kanału kontaktu. Zgoda ta bowiem była niezbędna dla uznania procesu przetwarzania danych osobowych w celach marketingowych za znajdujący uzasadnienie w przesłance z art. 6 ust. 1 lit. f) RODO. Organ podkreślił, że zgodnie z motywem 47 RODO podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem, nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. 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 natomiast w każdym przypadku przeprowadzić dokładną ocenę, w tym 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. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych – w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania[99].

Przetwarzanie danych osobowych przez zakład ubezpieczeń w związku z zawarciem umowy ubezpieczenia cywilnego

W jednej ze spraw organ oceniał proces przetwarzania danych przez zakład ubezpieczeń związany z zawarciem przez skarżącego umowy ubezpieczenia odpowiedzialności cywilnej (OC). Skarżący w trakcie ubezpieczenia zbył ubezpieczony pojazd, nie informując zakładu ubezpieczeń o sprzedaży. Obowiązek poinformowania zakładu ubezpieczeń o zbyciu pojazdu wynika z art. 32 ust. 1 ustawy o ubezpieczeniach obowiązkowych[100]. Skarżony podmiot wyjaśnił, że wysłał skarżącemu informację o warunkach umowy w kolejnym roku, w związku z obowiązkiem wynikającym z art. 28 ustawy o ubezpieczeniach obowiązkowych, a następnie kierował do niego wezwania do zapłaty składki umowy ubezpieczenia OC. Skarżący przekazał informację o sprzedaży pojazdu dopiero rok później, jednak nie wskazał danych nabywcy. W związku z brakiem możliwości poprawnej rejestracji danych aktualnego posiadacza pojazdu i kontaktu z nim

[99] ZSPR.440.1103.2019.

[100] Ustawa z 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. z 2023 r. poz. 2500).

umowa ubezpieczenia OC została rozwiązana w dniu upływu ważności ubezpieczenia. Prezes UODO nie dopatrzył się nieprawidłowości w procesie przetwarzania danych osobowych przez zakład ubezpieczeniowy. Dane osobowe osoby, która złożyła skargę, były przetwarzane w związku z wykonywaniem umowy ubezpieczenia, co znajdowało oparcie w przesłance z art. 6 ust. 1 lit. b) RODO, zaś korespondencja, którą skarżący otrzymał od zakładu ubezpieczeń w trakcie trwania ubezpieczenia została do niego skierowana w związku z obowiązkiem wynikającym z art. 28 ustawy o ubezpieczeniach obowiązkowych. Proces przetwarzania z tym związany znajdował tym samym oparcie w przesłankach z art. 6 ust. 1 lit. c) RODO. Na gruncie ww. sprawy zakład ubezpieczeń wskazał również, że po rozwiązaniu umowy przetwarza dane osobowe skarżącego w celu realizacji obowiązków prawnych ciążących na nim, jako administratorze, na mocy art. 29 ust. 10 UDUiR[101], przez okres przedawnienia roszczeń na podstawie art. 819 w zw. z art. 442^1 § K.c. Prezes UODO uznał powyższy proces przetwarzania za legalny i mający oparcie w art. 6 ust. 1 lit. c) RODO[102].

Przetwarzanie danych osobowych zawartych w dokumentacji medycznej przez ubezpieczyciela w postępowaniu likwidacyjnym

W roku 2023 Prezes UODO prowadził także postępowanie dotyczące procesu przetwarzania danych zawartych w dokumentacji medycznej wykorzystanej w postępowaniu likwidacyjnym przez ubezpieczyciela. W postępowaniu tym organ nadzorczy oceniał, czy w ww. procesie przetwarzania spełnione zostały przesłanki przetwarzania szczególnych kategorii danych osobowych, uregulowane w art. 9 ust. 2 RODO. Zgodnie z art. 26 ust. 3 pkt 7 ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[103] podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną zakładom ubezpieczeń, za zgodą pacjenta. W związku ze zgłoszoną przez skarżącą szkodą konieczne było uzyskanie opinii lekarskiej celem ustalenia, czy w sprawie doszło do popełnienia błędu medycznego. Zakład ubezpieczeń wystąpił o sporządzenie opinii lekarskiej do spółki, z którą zawarł umowę o współpracy w zakresie opiniowania lekarskiego w szkodach osobowych z ubezpieczeń odpowiedzialności cywilnej oraz umowę powierzenia przetwarzania danych osobowych. Z przedłożonej do akt dokumentacji wynikało, że skarżąca złożyła w formie pisemnej oświadczenie w sprawie szkodowej, w którym upoważniła kierownictwo wszystkich placówek służby zdrowia i lekarzy do udzielania zakładowi ubezpieczeń informacji o stanie jej zdrowia, w tym dotyczących: przyczyn hospitalizacji i leczenia ambulatoryjnego, wyników badań diagnostycznych (z wyłączeniem badań genetycznych), przeprowadzonych konsultacji, wyników leczenia, a także do przekazania zakładowi ubezpieczeń kopii jej dokumentacji medycznej. Oświadczenie to zawierało również informację, że upoważnienie to jest konieczne, aby ustalić odpowiedzialność zakładu ubezpieczeń z tytułu zdarzeń objętych ubezpieczeniem i wysokość świadczenia. W ocenie Prezesa UODO w sprawie tej zgoda została przez udzielona skutecznie, z zachowaniem wymagań z art. 7 RODO oraz zgodnie z motywem 42 RODO, i upoważniała zakład

[101] Ustawa z 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2024 r. poz. 838).
[102] DS.523.5913.2022.
[103] Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2024 r. poz. 581).

ubezpieczeń do pozyskiwania wszelkiej dokumentacji medycznej skarżącej, niezbędnej do określenia odpowiedzialności odszkodowawczej zakładu ubezpieczeń, z wyłączeniem dokumentacji w zakresie wyników badań genetycznych. Prezes UODO uznał powyższy proces przetwarzania danych osobowych, dotyczących dokumentacji medycznej, za legalny i znajdujący uzasadnienie w przesłance wynikającej z art. 6 ust. 1 lit. a) RODO oraz art. 9 ust. 2 lit. a) RODO[104].

Agent ubezpieczeniowy jako podmiot przetwarzający dane w imieniu zakładów ubezpieczeń

W jednej z prowadzonych przez Prezesa UODO spraw zarzucono podmiotowi skarżonemu, że udostępnił dane osobowe skarżącego zakładowi ubezpieczeń bez podstawy prawnej. Istotne w powyższej sprawie było to, że skarżony podmiot – przedsiębiorca przetwarzał dane osobowe skarżącego na podstawie zawartej z zakładem ubezpieczeń umowy agencyjnej oraz zawartych w umowie zasad powierzenia przetwarzania danych osobowych klientów. Dla rozstrzygnięcia zasadnicze znaczenie miał fakt, że skarżony podmiot był agentem ubezpieczeniowym współpracującym z różnymi zakładami ubezpieczeń, tzw. multiagentem.

Ustalono, że skarżony podmiot pozyskał dane osobowe od skarżącego w celu przedstawienia skarżącemu ofert ubezpieczenia nieruchomości od różnych zakładów ubezpieczeń, a następnie, po zaakceptowaniu oferty zakładu ubezpieczeń i wniosku skarżącego o przygotowanie polisy, w celu przygotowania konkretnej wybranej przez skarżącego polisy ubezpieczenia nieruchomości. Przedsiębiorca oraz zakład ubezpieczeń przedłożyły wraz z wyjaśnieniami w sprawie dokumentację potwierdzającą wyrażoną przez skarżącego chęć zapoznania się z propozycją ubezpieczenia, które oferowała spółka. Multiagent, w ramach prowadzonej działalności agencyjnej, wykonywał czynności w zakresie dystrybucji ubezpieczeń, działając w imieniu zakładu ubezpieczeń, zgodnie z art. 4 ust. 3 ustawy o dystrybucji ubezpieczeń (u.d.u.)[105]. Administratorem danych osobowych skarżącego, pozyskanych przez multiagenta w celu przygotowania i przedstawienia oferty ubezpieczeniowej zakładu ubezpieczeń, a następnie w celu zawarcia z skarżącym umowy ubezpieczenia, był zakład ubezpieczeń. Natomiast multiagent działał w ww. zakresie na zlecenie zakładu ubezpieczeń, który powierzył mu przetwarzanie danych osobowych w granicach niezbędnych do wykonania umowy agencyjnej. Powyższe odbywało się w oparciu o zawartą przez multiagenta z zakładem ubezpieczeń umową agencyjną, obejmującą powierzenie przetwarzania danych osobowych przez zakład ubezpieczeń na rzecz multiagenta, było zatem zgodne z art. 28 ust. 3 RODO i nie wymagało zgody skarżącego. Natomiast przesłanką legalizującą proces przetwarzania danych osobowych przez zakład ubezpieczeń był art. 6 ust. 1 lit. b) RODO, gdyż było to niezbędne do podjęcia działań zmierzających do zawarcia umowy na żądanie osoby, której dane dotyczą[106].

1.1.5. Postępowania transgraniczne

Prezes Urzędu Ochrony Danych Osobowych, jako jeden z organów nadzorczych ochrony danych, uczestniczy w ramach wzajemnej współpracy w egzekwowaniu

[104] DS.523.4719.2022.
[105] Dz. U. z 2023 r. poz. 1111.
[106] DS.523.542.2022.

przestrzegania i stosowania przepisów wynikających z RODO w EOG. Organy nadzorcze współdziałają poprzez System Wymiany Informacji na Rynku Wewnętrznym Komisji Europejskiej (IMI), z wykorzystaniem którego prowadzone są postępowania o charakterze transgranicznym. Postępowania te nie są prowadzone zawsze w ten sam sposób z uwagi na odmienne proceduralne przepisy krajowe państw członkowskich UE. Europejska Rada Ochrony Danych (EROD) wraz z wszystkimi organami nadzorczymi prowadzą prace nad wspólnymi wytycznymi dotyczącymi ujednolicania przepisów, w szczególności kluczowych, jak np. sposób i forma przyjmowania skarg dla wszystkich organów nadzorczych, które często są od siebie odmiennie.

Istnieje wiele wytycznych przyjętych przez EROD odnośnie do współpracy pomiędzy organami nadzorczymi oraz prowadzenia postępowań transgranicznych, jednak nie w każdym przypadku (zgodnie z przepisami krajowymi danego organu) jest możliwość zastosowania się do nich w pełni przez każdy z organów nadzorczych. Skomplikowany charakter spraw transgranicznych, w tym sposób ich prowadzenia i komunikacji, a także ich znaczna liczba, wpływają na dłuższy czas ich rozpatrzenia.

W 2023 r. skarżący, kierując żądania podjęcia działań przez Prezesa UODO, często nie wskazywali, jakich czynności się domagali. Zwracali się też do Prezesa UODO z żądaniami dotyczącymi kompetencji autonomicznych organu nadzorczego, np. nałożenia kary administracyjnej lub przeprowadzenia kontroli w siedzibie administratora.

W 2023 r. skargi dotyczyły najczęściej realizacji praw skarżących wobec administratorów oferujących dostęp do portali społecznościowych, takich jak Facebook oraz Instagram, zwłaszcza w zakresie prawa dostępu do danych oraz prawa usunięcia danych, jak również braku przejrzystej komunikacji z administratorem czy braku udzielenia terminowej odpowiedzi na żądania z rozdziału III RODO. W ramach skarg, które wpłynęły w 2023 r. administratorzy zazwyczaj udzielali wyczerpujących odpowiedzi na zadane pytania oraz nie ukrywali ewentualnych naruszeń ochrony danych, tłumacząc je często błędem ludzkim.

Odnosząc się do komunikacji z administratorem w ramach rozpatrywania skarg, których przedmiotem jest transgraniczne przetwarzanie danych, należy zaznaczyć, że zależy ona w dużej mierze od współpracy z organem wiodącego organu nadzorczego, tj. organu właściwego do rozpatrzenia sprawy ze względu na siedzibę administratora. Należy zauważyć, że zwłaszcza współpraca z niemieckimi organami nadzorczymi, jak i z francuskim oraz irlandzkim organem nadzorczym przebiega sprawnie, natomiast kontakt z włoskim, luksemburskim oraz holenderskim organem nadzorczym bywa utrudniony, m.in. z uwagi na występujące różnice w zakresie stosowanych procedur występujących w prowadzonych postępowaniach.

Poprzez szeroką współpracę i współdziałanie wszystkich organów nadzorczych w zakresie ochrony danych osobowych rozpatrywanie skarg transgranicznych ma, zdaniem Prezesa UODO, znaczny wpływ na większą świadomość korzystania ze swoich praw przez skarżących. Sprawy dotyczące takich administratorów, jak Meta czy Twitter, w tym nakładanych kar administracyjnych przez Irlandię jako organ wiodący za naruszenia, powoduje zawsze większy rozdźwięk społeczny, który wpływa na świadomość ludzi. W szczególności, jeżeli sprawy dotyczą znanych serwisów społecznościowych.

Konta użytkowników na dużych platformach mediów społecznościowych[107]

Do Prezesa UODO w 2023 r. wpłynęło wiele skarg na duże platformy mediów społecznościowych. Dotyczyły one w przeważającej mierze: braku możliwości uzyskania dostępu do danych osobowych lub ich usunięcia, braku przejrzystej komunikacji z administratorem, a także żądania przekazania nadmiernej ilości danych w celu weryfikacji tożsamości użytkowników tych platform, na przykład skanów dokumentów tożsamości. Problemem zidentyfikowanym przez Prezesa UODO w tym kontekście był brak wnoszenia, zarówno do administratorów, jak i do Prezesa UODO, odpowiednich żądań odnoszących się do danych osobowych. Skarżący bowiem wielokrotnie zwracali się z żądaniami dotyczącymi kont w mediach społecznościowych, a nie znajdujących się na nich danych osobowych. Prezes UODO nie ma zaś kompetencji do nakazania przywrócenia pełnej funkcjonalności, dostępu lub usunięcia kont użytkowników stron internetowych i aplikacji. Zadaniem Prezesa UODO jest ocena procesu przetwarzania danych osobowych, a nie kwestii związanych z obsługą kont użytkowników stron internetowych i aplikacji.

Prezes UODO informował o tym rozróżnieniu i zakresie swoich kompetencji. W rezultacie skarżący wnosili już prawidłowe żądania do administratorów, odnoszące się do ich danych osobowych. Z uwagi na to, że wielu administratorów dużych platform mediów społecznościowych ma swoje główne siedziby w innych państwach Unii Europejskiej, Prezes UODO ściśle współpracował z innymi organami nadzorczymi w ramach postępowań o charakterze transgranicznym, w celu zapewnienia ochrony praw osób, których dane dotyczą.

Prezes UODO aktywnie uczestniczył w postępowaniach o charakterze transgranicznym, zarówno w charakterze wiodącego organu nadzorczego, jak i organu, którego sprawa dotyczy, co przyczyniło się do zacieśnienia współpracy między organami nadzorczymi UE i zwiększenia harmonizacji stosowania RODO w państwach członkowskich UE.

Tworzenie i wykorzystywanie narzędzi służących usprawnieniu współpracy między organami w ramach rozpoznawania spraw o charakterze transgranicznym[108]

Do Prezesa UODO wpłynęła skarga dotycząca utracenia przez skarżącego dostępu do konta na portalu społecznościowym Instagram. Skarżący wskazał, że administrator portalu bezpodstawnie odebrał mu dostęp do konta, które było połączone z działalnością zarobkową skarżącego, przez co stracił on kontakt z kontrahentami i zaufanie budowane latami. Prezes UODO zidentyfikował skargę jako mającą charakter transgraniczny ze względu na siedzibę administratora w Irlandii, dokonał tłumaczenia skargi oraz przekazał ją irlandzkiemu organowi nadzorczemu (Data Protection Commission – DPC).

W odpowiedzi DPC stwierdził, że po przeanalizowaniu skargi zamyka postępowanie w sprawie z powodu braku elementów konstytutywnych dla skargi dotyczącej ochrony danych osobowych, bowiem w treści skargi nie ma żądania ochrony danych ani informacji. Utracenie dostępu do swojego konta na Instagramie nie stanowi problemu ochrony danych oraz nie jest objęte zakresem stosowania RODO. Jest to kwestia obsługi klienta, w której DPC nie jest w stanie pomóc. W załączeniu DPC przekazał dokument, w ramach którego

[107] DS.523.2250.2022, DS.523.4669.2021.
[108] DS.523.3694.2023.

zawarł „listę kontrolną” elementów, które w jego opinii powinna zawierać skarga o charakterze transgranicznym, dotycząca spełnienia prawa osoby, której dane dotyczą. Irlandzki organ nadzorczy zwrócił się do Prezesa UODO z prośbą o weryfikację każdej skargi na podmiot mający siedzibę na terenie Irlandii pod kątem ww. listy kontrolnej.

W załączonym dokumencie, który został przygotowany w sposób ogólny oraz ma zastosowanie do wszystkich organów nadzorczych w rozumieniu art. 4 pkt 21 RODO, DPC zwraca się z prośbą o załączenie wymienionej poniżej dokumentacji przy składaniu transgranicznych akt skarg za pośrednictwem systemu IMI. Na listę kontrolną wymaganą przez irlandzki organ nadzorczy składały się następujące elementy:

1. Kopia żądania spełnienia prawa osoby, której dane dotyczą, do administratora, w tym data złożenia żądania.
2. Kopia odpowiedzi (jeśli dotyczy) od administratora, w tym data udzielenia odpowiedzi.
3. Dowód, czy administrator skorzystał z przedłużenia o dwa miesiące terminu na realizację żądania, na podstawie art. 12 ust. 3 RODO, a jeżeli tak, to wskazanie daty poinformowania przez administratora osoby, której dane dotyczą, o przedłużeniu terminu.
4. Szczegóły wszelkich dodatkowych informacji wymaganych przez administratora w celu weryfikacji tożsamości osoby, której dane dotyczą, zgodnie z art. 12 ust. 6 RODO.
5. Kopia wszelkiej innej korespondencji między osobą, której dane dotyczą, a administratorem – w związku z żądaniem spełnienia prawa osoby, której dane dotyczą.
6. Kopia wszelkiej stosownej korespondencji między zainteresowanym organem nadzorczym a: (i) osobą, której dane dotyczą, oraz (ii) administratorem, w stosownych przypadkach, w związku z żądaniem spełnienia prawa osoby, której dane dotyczą.
7. Kopia skargi osoby, której dane dotyczą, złożona do zainteresowanego organu nadzorczego, przedstawiająca datę złożenia skargi.
8. Przetłumaczone dokumenty dla każdego z powyższych, jeśli jest to wymagane.

Data Protection Commission wskazał, że lista kontrolna ma odgrywać rolę przewodnika dla innych organów ochrony danych, dotyczącego informacji i/lub dokumentów, których potrzebuje DPC w celu oceny i postępów potencjalnych skarg transgranicznych w zakresie żądania dotyczącego praw osób, których dane dotyczą, złożonych zgodnie z art. 15–22 RODO.

Celem przedstawionych wytycznych jest ograniczenie opóźnień w ocenie ewentualnych skarg transgranicznych otrzymanych od organów ochrony danych. Można to osiągnąć poprzez zapewnienie, że przy składaniu transgranicznych akt skarg za pośrednictwem systemu IMI cała odpowiednia wymagana dokumentacja zostanie dołączona do skargi, a w następstwie zmniejszy to liczbę potrzebnych wymian zarówno z organami wysyłającymi, jak i z osobą, której dane dotyczą, a to z kolei przyspieszy rozpatrywanie skarg i zmniejszy obciążenie pracą tak organów wysyłających, jak i DPC. Celem dokumentu jest również ograniczenie ilości potrzebnej korespondencji z osobą, której dane dotyczą, oraz zapewnienie jej skuteczniejszej i wydajniejszej usługi.

Powyższa sprawa to przykład bardzo sprawnej współpracy wiodącego organu nadzorczego oraz organu, którego sprawa dotyczy. Warto zaznaczyć, że ze względu na siedzibę wielu spółek świadczących usługi platform społecznościowych na terenie Irlandii do DPC wpływa bardzo duża liczba skarg, dotyczących między innymi utraty dostępu do

konta na tego typu platformach. W związku z powyższym przygotowany przez DPC dokument z listą kontrolną, który odciąża na początkowym etapie DPC w dokonywaniu oceny skargi pod kątem jej dopuszczalności, należy przyjąć z aprobatą, jako środek mogący przyczynić się do usprawnienia pracy DPC oraz zmniejszenia liczby prowadzonych przez niego czynności wstępnych wobec wpływających skarg.

Współpraca między organami nadzorczymi w ramach rozpoznawania sprawy o charakterze lokalnym[109]

Sprawa dotyczyła niespełnienia przez administratora posiadającego swój oddział w Rumunii żądania skarżącego usunięcia jego danych osobowych. Po dokonaniu ustaleń z rumuńskim organem nadzorczym uznano, że sprawa ta dotyczy tylko oddziału w Rumunii i ma wpływ wyłącznie na osoby, których dane dotyczą w Rumunii, wobec czego sprawa została poprowadzona na szczeblu lokalnym przez rumuński organ nadzorczy na podstawie art. 56 ust. 2 RODO. Skarżący podpisał umowy jedynie z oddziałem banku w Rumunii, a sprawa miała charakter indywidualny i dotyczyła nieprawidłowości w przetwarzaniu danych skarżącego.

Polski organ wskazał przy tym rumuńskiemu organowi nadzorczemu główną zasadę, która wynika z pkt 3 Wewnętrznego dokumentu EROD 1/2019, dotyczącego rozpatrywania skarg mających jedynie skutki lokalne na mocy art. 56 ust. 2 RODO (wersja 2.0)[110], że ww. przepis obejmuje przypadki będące odstępstwem od zasady ogólnej. Przypadki te obejmują przetwarzanie transgraniczne, ale mające jedynie lokalne skutki w państwie członkowskim organu nadzorczego, w którym po raz pierwszy złożono skargę lub który po raz pierwszy wykrył możliwe naruszenie, a w pkt 4 czytamy, że w przypadku takich spraw o skutkach wyłącznie lokalnych art. 56 ust. 2 i 3 RODO stanowi, że organ nadzorczy, który otrzymał skargę lub został poinformowany o możliwym naruszeniu, jest właściwy, jeżeli wiodący organ nadzorczy (w tym przypadku polski organ nadzorczy) postanowi nie zajmować się sprawą.

Rumuński organ nadzorczy poprowadził więc przedmiotową sprawę lokalnie, na podstawie art. 56 ust. 2 RODO, zgodnie z sugestią Prezesa UODO. Następnie przekazał polskiemu organowi nadzorczemu pismo potwierdzające, że postępowanie w przedmiotowej sprawie zostało zakończone. Rumuński organ nadzorczy decyzją zarządził wobec banku w Polsce, za pośrednictwem jego oddziału w Rumunii, nałożenie grzywny za stwierdzone naruszenia na podstawie sprawozdania z ustaleń opartego na art. 83 ust. 5 lit. a) RODO, tj. za naruszenie przepisów art. 5 ust. 1 lit. a) i lit. b) oraz art. 6 RODO, a także zastosowanie środka naprawczego przewidzianego w art. 58 ust. 2 lit. d) RODO.

2. Kontrola przestrzegania przepisów o ochronie danych osobowych

Celem czynności kontrolnych jest ustalenie, czy jednostka kontrolowana przetwarza dane zgodnie z przepisami o ochronie danych osobowych. Uprawnienia kontrolerów UODO zostały uregulowane odrębnie w rozdziale 9 ustawy z 10 maja 2018 r. o ochronie danych osobowych. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa UODO

[109] DS.523.1740.2022.

[110] Internal EDPB Document 1/2019 on handling cases with only local impacts under Article 56.2 GDPR (Version 2.0).

planem kontroli lub na podstawie uzyskanych przez niego informacji, a także w ramach monitorowania przestrzegania stosowania przepisów RODO.

W okresie od 1 stycznia do 31 grudnia 2023 r. Prezes UODO przeprowadzał czynności kontrolne w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych **w trzydziestu trzech (33) podmiotach.** Wymienione działania były realizowane w wykonaniu uprawnień przysługujących organowi nadzorczemu na podstawie art. 58 ogólnego rozporządzenia o ochronie danych. Dziesięć (10) kontroli przeprowadzono na podstawie przyjętego na 2023 rok planu kontroli sektorowych. Trzy (3) kontrole przeprowadzone zostały w związku ze zgłoszonymi Prezesowi UODO przez administratorów naruszeniami ochrony danych osobowych. Osiemnaście (18) kontroli podjęto w rezultacie powzięcia przez Prezesa UODO informacji o występujących nieprawidłowościach w związku z przetwarzaniem danych osobowych. Przeprowadzono również jedną (1) kontrolę w ramach monitorowania przestrzegania stosowania RODO oraz jedną (1) na podstawie art. 34 ustawy z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym.

Prezes UODO ponadto przeprowadził trzynaście (13) sprawdzeń stosowania art. 11 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Zgodnie z planem kontroli sektorowych UODO na 2023 r. czynnościami kontrolnymi zostały objęte:

1) podmioty przetwarzające dane osobowe przy użyciu aplikacji mobilnych (3 kontrole);
2) podmioty przetwarzające dane osobowe przy użyciu aplikacji internetowych (5 kontroli);
3) organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym (2 kontrole).

2.1. Aplikacje mobilne

W zakresie kontroli procesu przetwarzania danych osobowych przy użyciu aplikacji mobilnych czynnościami kontrolnymi objęto piętnaście podmiotów (w 2022 r. – 13, w 2023 r. – 2). Kontrole te zostały przeprowadzone zgodnie z przyjętymi planami kontroli sektorowych na poszczególne lata. Zakres kontroli obejmował głównie badanie wdrożenia odpowiednich środków technicznych i organizacyjnych, stosowanych w celu przetwarzania danych osobowych, tak aby odbywało się ono 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 ocenę, czy środki te były poddawane regularnym przeglądom i uaktualnieniom (art. 32 i art. 24 rozporządzenia 2016/679). Podmioty, w których Prezes UODO przeprowadził kontrole, reprezentowały różne branże: medyczną, bankową, handlową, gastronomiczną, turystyczną, transportową, a także administrację publiczną.

Kontroli poddano w szczególności: 1) elementy bezpieczeństwa wykorzystywane w celu ochrony danych osobowych przetwarzanych w aplikacjach mobilnych i w powiązanych z tymi aplikacjami systemach informatycznych; 2) mechanizmy tworzenia i weryfikacji kopii zapasowych; 3) zasady stosowania systemów antywirusowych, antyspamowych i innych systemów wspomagających ochronę aplikacji mobilnych oraz systemów informatycznych; 4) metody logowania oraz kontrolowania zdarzeń w systemach informatycznych; 5) sposób realizowania dostępu do przetwarzanych danych

osobowych (ze szczególnym uwzględnieniem mechanizmów zapewniających: poufność, integralność, dostępność danych); 6) kontrolę metod i zakresu informowania użytkowników aplikacji mobilnych o charakterze dostępu tych aplikacji do funkcjonalności wbudowanych w urządzenia mobilne.

W ramach kontroli procesu przetwarzania danych osobowych przy użyciu aplikacji mobilnych, przeprowadzonej w **podmiocie medycznym,** ustalono, że w polityce prywatności brak było informacji o prawie wniesienia skargi do organu nadzorczego, zaś w regulaminie aplikacji mobilnej – wyraźnego wskazania odbiorców danych lub kategorii odbiorców, którym udostępniane były dane osobowe. W obu tych dokumentach zabrakło też informacji o tym, czy podanie danych osobowych jest wymogiem ustawowym, umownym, czy też warunkiem zawarcia umowy, oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych. Odnotowano również konieczność stworzenia w rejestrze czynności szczegółowego opisu niektórych czynności odnoszących się do przetwarzania danych przy użyciu aplikacji mobilnej. Dotychczasowy opis był zbyt ogólnikowy, nie wskazywał, że aplikacja posiada określone funkcjonalności, które są powiązane z konkretnymi procesami przetwarzania danych.

Skutkiem przeprowadzenia kontroli w **jednym z banków** było wszczęcie postępowania administracyjnego ze względu na naruszenie przepisów RODO. Polegało ono na tym, że klauzula zgody, udzielanej przez klienta na przekazanie jego danych osobowych spółkom z grupy kapitałowej banku oraz towarzystwom ubezpieczeniowym dla celów marketingu, nie spełniała kryteriów definicji zawartej w art. 4 pkt 11 RODO. Co więcej, ocena skutków dla ochrony danych osobowych nie została przeprowadzona w sposób prawidłowy. Bank jako administrator nie prowadził rejestru czynności przetwarzania danych osobowych w sposób odpowiadający wymogom art. 30 ust. 1 ogólnego rozporządzenia o ochronie danych. Zgodnie z treścią art. 5 ust. 2 RODO administrator jest odpowiedzialny za przestrzeganie przepisów art. 5 ust. 1 tego aktu i musi być w stanie wykazać ich respektowanie. Oznacza to, że ma obowiązek realizacji działań związanych z zapewnieniem przestrzegania przepisów dotyczących danych osobowych w taki sposób, żeby móc wykazać ich wykonanie przed organem nadzorczym, np. w przypadku kontroli. Niemożność wykazania przestrzegania przepisów art. 5 ust. 1 RODO obciąża administratora i działa na jego niekorzyść w tym sensie, że organ nadzorczy, rozpatrując materiał dowodowy w prowadzonym postępowaniu, musi przyjąć, iż administrator nie podjął określonych działań niezbędnych do spełnienia wymogów, a więc i do przestrzegania przepisów art. 5 ust. 1 rozporządzenia 2016/679.

W przypadku pozostałych trzech instytucji finansowych, które przetwarzały dane przy użyciu aplikacji mobilnych, kontrole nie wykazały naruszenia przepisów o ochronie danych osobowych, które stanowiłyby podstawę do wszczęcia postępowania administracyjnego.

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przy użyciu aplikacji mobilnej przeprowadzono również w **spółce zajmującej się wynajmem i dzierżawą pojazdów samochodowych.** Analiza dokumentacji spółki wykazała, że regulamin prowadzonej przez nią usługi zawierał postanowienia niezgodne ze stanem faktycznym. Z regulaminu wynikało bowiem, że umowa wypożyczenia pojazdu zawierana jest pomiędzy klientem a partnerem lub

kontrolowaną spółką. Tymczasem w toku kontroli ustalono, że umowy zawierane były wyłącznie pomiędzy klientem a tą spółką. Ponadto stwierdzono, że z niektórymi franczyzobiorcami działającymi na terenie kraju spółka zawarła umowy powierzenia, gdyż podmioty te we własnym zakresie miały prowadzić marketing oferowanych usług, windykację oraz przetwarzać dane osobowe w przypadku zaginięcia wypożyczonego pojazdu. Natomiast z wyjaśnień złożonych w toku kontroli wynikało, że podmioty, o których mowa powyżej, czynności tych nie prowadziły i w związku z tym nie przetwarzały danych osobowych użytkowników aplikacji mobilnej w ww. celach.

Kontrola przeprowadzona **w placówce medycznej** wykazała**,** że użytkownik w celu uruchomienia aplikacji mobilnej wprowadzał swój numer PESEL jako login. Zastosowana metoda wzbudza obawy w zakresie zachowania właściwej ochrony praw i wolności osób, których dane dotyczą. Podmiot tworzący system informatyczny ponosi odpowiedzialność za takie ukształtowanie zasad dostępu do niego, by minimalizować ryzyko dla przetwarzanych w nim danych osobowych. Z ustaleń kontroli wynikało, że utworzonych zostało około kilkunastu tysięcy kont w portalu pacjenta. Zatem proces logowania się do aplikacji w omawianym przypadku można byłoby uznać za przetwarzanie danych osobowych na dużą skalę. Istotne było przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 ust. 3 lit. b) RODO, który wprost wskazuje, iż ocena ta jest wymagana w szczególności w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO. Prawidłowo przeprowadzona ocena skutków dla ochrony danych niezwłocznie wskazywałaby ryzyka wiążące się z ustanowieniem numeru PESEL jako loginu. Zgodnie z art. 25 ust. 1 RODO administrator, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby chronić prawa osób, których dane dotyczą. Tymczasem sposób zabezpieczania profilu pacjenta poprzez logowanie się do aplikacji za pomocą numeru ewidencyjnego PESEL, biorąc pod uwagę aktualny stan wiedzy technicznej, może w określonych sytuacjach determinować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Kolejny skontrolowany **podmiot leczniczy** wykorzystywał aplikację mobilną do obsługi pacjentów w zakresie ich rejestracji, jednocześnie umożliwiając pacjentom wgląd w wyniki ich badań. Zalogowany użytkownik konta otrzymywał dostęp do historii zarezerwowanych wizyt oraz historii wyników badań laboratoryjnych. W zakresie objętym kontrolą nie stwierdzono naruszenia przepisów o ochronie danych osobowych.

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono również **w spółce zajmującej się obsługą platformy do zamawiania jedzenia online** i korzystającej w ramach świadczonych usług z aplikacji mobilnej w celu uzyskania kontaktu z klientami. Skutkiem kontroli było wszczęcie postępowania administracyjnego, w zakresie naruszenia art. 5 ust. 1 lit. c) oraz art. 5 ust. 2 RODO poprzez nadmiarowe i nieadekwatne do założonych celów przetwarzanie danych osobowych użytkowników aplikacji mobilnej, gdyż pozyskiwano zdjęcia/skany dowodów osobistych lub paszportów klientów. Spółka nie wykazała przestrzegania zasady minimalizacji danych.

Kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przeprowadzono także w **spółce zajmującej się wypożyczaniem**

i dzierżawą sprzętu rekreacyjnego oraz sportowego, która oferowała swoim klientom mobilną platformę komunikacji z klientem, umożliwiającą wypożyczanie sprzętu. Stwierdzono, że adres e-mail podawany klientom do kontaktu z inspektorem ochrony danych był nieaktualny. Ustalono także, że w spółce prowadzony był rejestr kategorii czynności przetwarzania, chociaż spółka działała wyłącznie jako administrator, a nie podmiot przetwarzający, który – zgodnie z art. 30 ust. 2 RODO – jest zobowiązany do prowadzenia takiego rejestru. Konieczność prowadzenia rejestru kategorii przetwarzania miałaby miejsce wtedy, gdyby spółka była podmiotem przetwarzającym dane. Zgromadzony w toku kontroli materiał tego nie potwierdził.

Generalnie należy stwierdzić, że kontrolowane podmioty, stosujące aplikacje mobilne do przetwarzania danych, w większości przypadków wdrożyły wymagane 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; wdrożenie środków kryptograficznych; ciągłe monitorowanie bezpieczeństwa systemów, w których przetwarzane były dane osobowe; stosowanie systemów antyspamowych i antywirusowych; przeprowadzanie okresowych testów bezpieczeństwa; szyfrowanie plików i nośników; monitorowanie przepływu danych z nośników 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. Większość podmiotów kontrolowanych, jako administratorzy danych, w sposób prawidłowy wywiązywało się także z innych obowiązków, tj. prowadzenia dokumentacji opisującej sposób przetwarzania danych, wdrożenia polityki ochrony danych, wyznaczenia i zgłoszenia inspektorów ochrony danych. Kontrolowane podmioty podjęły też działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora, która ma dostęp do danych osobowych, przetwarzała je na polecenie administratora, ponadto dokumentowano naruszenia ochrony danych osobowych oraz prowadzono rejestry czynności przetwarzania danych.

Należy podkreślić, że ochrona danych osobowych przetwarzanych w aplikacjach mobilnych jest obecnie bardzo istotna. Według dostępnych źródeł na początku 2022 r. istniało ponad 6 mln aplikacji mobilnych, a prawie każda z nich gromadziła określone informacje o swoich użytkownikach. W związku z tym wskazane jest, aby twórcy aplikacji mobilnych zapewnili zgodność produktu z ochroną danych osobowych i aby sprostali wymogom wynikającym wprost z przepisów prawa o ochronie danych osobowych oraz tym, które nakładają na nich platformy dystrybuujące aplikacje mobilne. Wiele aplikacji mobilnych gromadzi dane, które umożliwiają identyfikację konkretnego użytkownika – są to na ogół te aplikacje, które wymagają założenia konta i podania danych osobowych niezbędnych do korzystania z ich funkcjonalności. Niektóre aplikacje mobilne zbierają dane, które pozornie mogą wydawać się anonimowe, ale z prawnego punktu widzenia (i w powiązaniu z innymi przetwarzanymi danymi) mogą „stać się” danymi osobowymi. Takie dane również podlegają ochronie. Etap tworzenia aplikacji mobilnych to najlepszy

moment, aby zapewnić zgodność tego produktu z zasadami ochrony danych osobowych. Również każdy deweloper powinien zapewnić bezpieczeństwo danych osobowych użytkowników aplikacji mobilnych, a którzy powinni mieć po pierwsze kontrolę nad swoimi danymi poprzez możliwość decydowania o tym, jakie informacje zamierzają ujawnić, komu i w jakich celach, a po drugie zapewnione prawo do korekty swoich danych przetwarzanych w aplikacjach mobilnych oraz prawo ich usunięcia. Istotne wydaje się również, aby przed wdrożeniem aplikacji mobilnych do użytkowania określony został czas retencji danych osobowych przetwarzanych za ich pomocą lub danych pozyskanych w aplikacjach mobilnych, które są przetwarzane w powiązanych systemach informatycznych. Przestrzeganie powyższych zasad pozwoli na uniknięcie problemów związanych z potencjalnym naruszeniem przepisów o ochronie danych osobowych.

2.2. Aplikacje internetowe (webowe)

Zgodnie z przyjętym planem kontroli sektorowych na 2023 r., który zakładał kontrolę przetwarzania danych osobowych w związku z użytkowaniem aplikacji internetowych (webowych), czynnościami kontrolnymi objęto pięć (5) podmiotów reprezentujących branże: ubezpieczeniową, handlową, bukmacherską i hostingową. Kontrole dotyczące w szczególności sposobu zabezpieczenia i udostępniania danych osobowych przetwarzanych przy użyciu aplikacji internetowych nadal trwają i będą kontynuowane w następnym roku.

2.3. System Informacyjny Schengen, Wizowy System Informacyjny

Sektorowymi kontrolami przetwarzania danych osobowych objęto w 2023 r. dwa (2) konsulaty RP w związku z dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych VIS oraz wglądu do danych VIS i danych SIS. Konsulom przysługuje dostęp do Wizowego Systemu Informacyjnego w celu dokonania wglądu do danych VIS w związku z rozpatrywaniem złożonych przez cudzoziemców wniosków wizowych i wydawaniem decyzji dotyczących tych wniosków.

Dodatkowo konsulom przysługuje:

- uprawnienie dostępu do Wizowego Systemu Informacyjnego w celu dokonywania wpisów danych VIS;
- wgląd do danych SIS dotyczących cudzoziemców, których dane zostały wpisane do Systemu Informacyjnego Schengen dla celów odmowy wjazdu;
- wgląd do danych SIS dotyczących blankietów dokumentów urzędowych, które zostały skradzione, przywłaszczone lub utracone, oraz wydanych dokumentów tożsamości, takich jak: paszporty, dowody tożsamości, prawa jazdy, dokumenty pobytowe i dokumenty podróży, które zostały skradzione, przywłaszczone, utracone lub unieważnione.

W zakresie objętym kontrolami nie stwierdzono naruszenia przepisów o ochronie danych osobowych, które stanowiłyby podstawę do wszczęcia postępowania administracyjnego.

2.4. Sprawdzenia dotyczące prewencyjnych wpisów małoletnich do SIS

Realizując zadania nadzorcze nad przetwarzaniem danych osobowych za pośrednictwem wielkoskalowych systemów informatycznych, w związku z rozpoczęciem eksploatacji zmodernizowanego SIS (tzw. SIS Recast), które nastąpiło 7 marca 2023 r.,

Prezes Urzędu Ochrony Danych Osobowych, działając na podstawie art. 11 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, wystąpił do inspektorów ochrony danych wytypowanych siedmiu (7) jednostek Policji oraz sześciu (6) oddziałów Straży Granicznej o dokonanie sprawdzenia operacji zgodności przetwarzania danych dotyczących prewencyjnych wpisów na temat dzieci w Systemie Informatycznym Schengen, dokonywanych na podstawie art. 32 ust. 1 lit. c) i lit. d) rozporządzenia 2018/1862[111] i art. 3 ust. 1 pkt 7, 8, 9 i art. 4 ust. 1 pkt 7, 8, 9 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[112] oraz właściwych aktów wykonawczych.

Należy podkreślić, iż System Informacyjny Schengen (SIS) to najskuteczniejsze narzędzie zapewniające efektywną współpracę między organami imigracyjnymi, policją, organami celnymi i organami sądowymi w UE oraz państwach stowarzyszonych w ramach Schengen. Właściwe organy w państwach członkowskich, takie jak: policja, straż graniczna i funkcjonariusze celni, powinny mieć dostęp do wysokiej jakości informacji na temat sprawdzanych przez siebie osób lub przedmiotów, a także do wyraźnych instrukcji dotyczących działań, które należy podjąć w każdym przypadku. Ten wielkoskalowy system informacyjny jest najważniejszym elementem współpracy Schengen i ma kluczowe znaczenie dla ułatwienia swobodnego przepływu osób w strefie Schengen. Umożliwia on właściwym organom wprowadzanie i przeglądanie danych dotyczących: osób poszukiwanych, osób, które mogą nie mieć prawa do wjazdu lub pobytu na terytorium UE, osób zaginionych – w szczególności dzieci – oraz przedmiotów, które mogły zostać skradzione, sprzeniewierzone lub zgubione. Oprócz informacji na temat konkretnej osoby lub konkretnego przedmiotu SIS zawiera także wyraźne instrukcje określające sposób postępowania właściwych organów po odnalezieniu danej osoby lub konkretnego przedmiotu.

Zmodernizowany SIS przewiduje możliwość wprowadzania tzw. „wpisów prewencyjnych". Nowe przepisy mają rozwiązać kwestię potencjalnej luki w przepisach, na podstawie których wpisy dotyczące dzieci można było wprowadzać dopiero po ich zaginięciu. Dzięki zmianie w przepisach władze w państwach członkowskich mogą wskazywać dzieci, w przypadku których ryzyko uprowadzenia jest szczególnie wysokie. Oznacza to, że funkcjonariusze straży granicznej i służby wymiaru sprawiedliwości zostaną powiadomieni w przypadku występowania dużego ryzyka rychłego uprowadzenia dziecka przez jednego z rodziców i będą w stanie dokładniej zbadać okoliczności podróży takiego dziecka, w razie potrzeby stosując wobec niego pieczę ochronną. Informacje uzupełniające, w tym decyzja właściwego organu sądowego, który zwrócił się o wprowadzenie wpisu, będą udzielane przez biura SIRENE. Tego rodzaju wpis wymaga odpowiedniej decyzji organów sądowych udzielających pieczy tylko jednemu rodzicowi. Kolejnym warunkiem jest występowanie bezpośredniego ryzyka uprowadzenia. Status

[111] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z 28.11.2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz. Urz. L 312 z 7.12.2018, str. 56).

[112] Ustawa z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. z 2023 r. poz. 1355).

wpisów dotyczących zaginionego dziecka powinien być w stosownych przypadkach automatycznie aktualizowany w momencie osiągnięcia przez dziecko pełnoletności.

Zgodnie z uzasadnieniem do ustawy o zmianie ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym oraz niektórych innych ustaw (druk sejmowy nr 2662 IX kadencji Sejmu RP) – dodanie art. 3 ust. 1 pkt 7–10 miało na celu uwzględnienie nowych zakresów wpisów przetwarzanych w SIS, dotyczących w szczególności małoletnich zagrożonych uprowadzeniem przez rodzica, członka rodziny lub opiekuna oraz małoletnich, którym należy uniemożliwić podróżowanie ze względu na realne zagrożenie, że staną się ofiarami przestępstw o charakterze terrorystycznym lub wezmą udział w popełnianiu takich przestępstw bądź zostaną zwerbowani lub zaciągnięci do ugrupowań zbrojnych czy zmuszeni do aktywnego udziału w działaniach wojennych oraz osób pełnoletnich i małoletnich narażonych na niebezpieczeństwo, którym należy uniemożliwić podróżowanie dla ich własnej ochrony (np. gdy podróż może się wiązać z ryzykiem handlu ludźmi, przymusowego małżeństwa lub przemocą warunkowaną płcią).

W toku sprawdzeń Prezes Urzędu nie wniósł zastrzeżeń do przedstawionych sprawozdań właściwych inspektorów ochrony danych.

2.5. Kontrole w wyniku zgłoszonego naruszenia

W 2023 r. Prezes UODO przeprowadził **trzy (3) postępowania kontrolne w związku ze zgłoszonym przez administratora naruszeniem ochrony danych.** Kontrole te obejmowały w szczególności sprawdzenie, czy wykonana ocena ryzyka i ocena skutków dla ochrony danych miały odzwierciedlenie we wdrożonych przez administratorów środkach 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 oraz wolności osób fizycznych, a także czy środki te były w razie potrzeby poddawane przeglądom i uaktualniane.

W jednym z podmiotów została przeprowadzona kontrola, w toku której ustalono, że naruszenie polegało na przekazaniu osobom nieuprawnionym bazy danych **pośredników ubezpieczeniowych** (osób fizycznych wykonujących czynności agencyjne). W bazie tej przetwarzane były takie dane, jak: imię i nazwisko, adres, numer PESEL, adres e-mail oraz numer telefonu. Ustalono też, że początkowo spółka w bazie danych pośredników ubezpieczeniowych nie przetwarzała numerów PESEL, lecz na wniosek jednego z wiodących agentów ubezpieczeniowych, w celu poprawnej identyfikacji danego pośrednika ubezpieczeniowego, rozszerzono zakres danych agentów o numer PESEL. Jak wskazywały dowody, utworzenie oraz wdrożenie bazy pośredników ubezpieczeniowych było konsultowane z inspektorem ochrony danych, natomiast spółka nie przedłożyła dowodów, które potwierdzałyby, że modyfikacja zakresu przetwarzania danych agentów ubezpieczeniowych poprzez dodanie numeru PESEL była z nim omawiana. Po wykryciu naruszenia zarząd spółki, chcąc mieć pewność, że nieuprawnieni adresaci e-maila usunęli go ze swoich zasobów, podjął decyzję o konieczności pozyskania pisemnych potwierdzeń od wszystkich osób, do których e-mail został wysłany. Od każdego z adresatów e-maila spółka w korespondencji zwrotnej otrzymała wypełnione oświadczenie. Z jego treści wynikało, że dany podmiot usunął z poczty elektronicznej

otrzymany plik z danymi osobowymi oraz że podmiot ten w żaden inny sposób nie przetwarzał otrzymanych danych.

W skontrolowanej spółce, w ramach działań naprawczych, zastosowano m.in. mechanizm blokowania wysyłki wiadomości e-mail i generowania alertów bezpieczeństwa w przypadku, gdy w treści e-mail lub w treści załączników do wiadomości e-mail znajdowały się dane dotyczące numeru PESEL lub numeru dowodu osobistego. Jednocześnie wdrożono system informatyczny służący do identyfikowania typowych luk w zabezpieczeniach oraz umożliwiający automatyczne mapowanie elementów kontroli bezpieczeństwa – w celu ułatwienia eliminowania tych luk z systemów informatycznych. Ustalenia z kontroli zostały uwzględnione przy wydawaniu decyzji administracyjnej w sprawie zgłoszenia naruszenia ochrony danych.

W odpowiedzi na liczne zapytania pacjentów oraz wzmożone zainteresowanie medialne wyciekiem dużej ilości danych osobowych, w tym dotyczących zdrowia wielu osób ze **spółki świadczącej usługi medyczne,** Prezes UODO postanowił przeprowadzić kontrolę dotyczącą zgłoszonego przez tę spółkę naruszenia ochrony danych osobowych. Dotyczyło ono wycieku dużej ilości danych osobowych w wyniku ataku hakerskiego i przełamania zabezpieczeń. Celem ataku było wyłudzenie od administratora danych określonych korzyści finansowych. Na skutek naruszenia przełamane zostały zabezpieczenia techniczne, a nie organizacyjne. Kontrolę przeprowadzono w celu weryfikacji, czy administrator wdrożył odpowiednie środki techniczne i organizacyjne dotyczące funkcjonowania systemu informatycznego objętego naruszeniem.

Ustalenia dokonane w ramach przeprowadzonych czynności kontrolnych w przedmiotowym zakresie oraz zgromadzony materiał dowodowy zostały poddane szczegółowej analizie – w celu weryfikacji przestrzegania oraz realizacji przez administratora obowiązków nałożonych przepisami ogólnego rozporządzenia o ochronie danych. W sprawie wyżej opisanego naruszenia ochrony danych osobowych Prezes UODO wszczął postępowanie administracyjne.

2.6. Kontrole w wyniku otrzymania informacji o nieprawidłowościach

W 2023 r. Prezes UODO przeprowadził **osiemnaście (18) kontroli w rezultacie otrzymania informacji o nieprawidłowościach w związku z przetwarzaniem danych.**

Zakresem jednej z kontroli przeprowadzonej **w placówkach medycznych** objęto przetwarzanie danych osobowych za pomocą środków technicznych umożliwiających rejestrację obrazu lub dźwięku. W wyniku tej kontroli zostało wszczęte postępowanie administracyjne w sprawie naruszenia przez przedsiębiorcę art. 30 ust. 1 lit. b) i lit. f)[113] RODO. Przedsiębiorca, jako administrator danych, w prowadzonym rejestrze czynności przetwarzania danych nie wskazał czynności wykonywanej na danych osobowych w związku z prowadzonym monitoringiem, nie określił też celu przetwarzania danych w zakresie wizerunku osób oraz nie sprecyzował planowanego terminu usunięcia danych osób monitorowanych. W odpowiedzi przedsiębiorca wyjaśnił, że w związku z awarią systemu monitoringu dane osobowe przez pewien okres czasu nie były przetwarzane (obraz z kamer nie był rejestrowany) i w związku z tym w prowadzonym rejestrze czynności

[113] Stosownie do art. 30 ust. 1 lit. b) i lit. f) RODO każdy administrator prowadzi rejestr czynności przetwarzania danych, w którym zamieszczone są informacje dotyczące celu przetwarzania oraz – jeżeli jest to możliwe – planowane terminy usunięcia poszczególnych kategorii danych.

przetwarzania danych nie było informacji o czynnościach wykonywanych na danych osobowych w związku ze stosowaniem monitoringu. Po usunięciu awarii przedsiębiorca dokonał aktualizacji rejestru czynności przetwarzania danych osobowych. Na potwierdzenie tego faktu do Urzędu Ochrony Danych Osobowych został przesłany dowód w postaci wydruku zmodyfikowanego rejestru. Obecnie sprawa jest analizowana w celu wydania decyzji.

Kolejna kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych przeprowadzona została w jednym z podmiotów reprezentujących **sektor bankowy.** Dokonano czynności kontrolnych w zakresie dokumentowania przez administratora naruszeń ochrony danych osobowych, o którym jest mowa w art. 33 ust. 5 ogólnego rozporządzenia o ochronie danych.

W ramach tej kontroli dokonano weryfikacji sposobu dokumentowania naruszeń, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. Sprawdzono, czy zostały opracowane i wdrożone procedury dotyczące sposobu postępowania w sytuacji wystąpienia naruszenia ochrony danych osobowych oraz ustalono, czy w przypadku wystąpienia przesłanek, o których mowa w art. 34 RODO, administrator zawiadomił osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych.

Ustalenia dokonane w ramach przeprowadzonych czynności kontrolnych w przedmiotowym zakresie oraz zgromadzony materiał dowodowy stanowiły przedmiot analizy weryfikacji przestrzegania i realizacji przez administratora obowiązków nałożonych na niego przepisami ogólnego rozporządzenia o ochronie danych.

Kolejną kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych pracownicy UODO przeprowadzili **w spółce, której przedmiotem działalności było doręczanie przesyłek kurierskich.** Kontrolą objęto przetwarzanie przez spółkę danych osobowych w związku ze świadczeniem usługi w zakresie doręczania przesyłek kurierskich w rozumieniu art. 3 pkt 19 ustawy z 23 listopada 2012 r. Prawo pocztowe[114], w szczególności ich odpowiedniego zabezpieczania przed utratą i zniszczeniem.

Z materiału dowodowego wynikało, że spółka nie przedsięwzięła odpowiednich działań celem zapewnienia przetwarzania danych osobowych przez jej pracowników na polecenie spółki jako administratora. Zarząd spółki nie upoważnił żadnego pracownika do udzielania upoważnień do przetwarzania danych – pomimo zawarcia w polityce ochrony danych spółki stosownego postanowienia odnoszącego się do tej kwestii. Stanowiło to przejaw częściowego niewdrożenia postanowień polityki ochrony danych, do którego każdy administrator jest zobowiązany w świetle treści art. 24 ust. 2 RODO, a więc i naruszenia rzeczonego przepisu.

Kontrola wykazała, że w spółce nie były prawidłowo udzielane upoważnienia do przetwarzania danych w rozumieniu ww. przepisów ogólnego rozporządzenia. Ponadto przyjęto błędne założenie, że funkcję upoważnień do przetwarzania danych będą pełnić treści zawarte w plikach elektronicznych, przesyłanych w zautomatyzowany sposób do komputerów poszczególnych pracowników, nieopatrzonych podpisem w formie pisemnej czy elektronicznej, ani innymi cechami, które wyraźnie i bez wątpliwości łączyłyby

[114] Dz. U. z 2023 r. poz. 1640 ze zm.

każdorazowo treść upoważnień ze świadomym działaniem uprawnionej do ich udzielenia osoby. Przesyłanie oświadczenia o upoważnieniu, bez związku z określonym zachowaniem się uprawnionej osoby, a więc, przykładowo, złożeniem przez nią podpisu, logowaniem w systemie zarządzania dokumentacją itd., stanowiło naruszenie art. 29 oraz art. 32 ust. 4 w zw. z art. 5 ust. 2 RODO, z uwagi na nieudzielanie prawidłowo upoważnień do przetwarzania danych.

Ponadto spółka nie uwzględniła w katalogu stosowanych przez nią środków organizacyjnych, służących zapewnieniu odpowiedniego bezpieczeństwa danych, upoważnień do ich przetwarzania (art. 24 ust. 1 i ust. 2 oraz art. 32 ust. 1 RODO). Z kolei w umowach zawartych przez nią z podmiotami wykonującymi usługi przewozowe nie uwzględniono postanowień dotyczących powierzenia przetwarzania danych w związku z transportem przesyłek, mimo że powierzenie takie miało faktycznie miejsce, z uwagi na sposób i zakres świadczenia usług przez przewoźników.

Należy zauważyć, że zgodnie z treścią ww. umów podmioty świadczące przewozy czynią to, co do zasady, za pomocą środków transportu, do których posiadania mają tytuł prawny. Nie ma go natomiast spółka, poza wyjątkami wskazanymi w umowach, gdy udostępnia ona do transportu przewoźnikom własne naczepy. Powyższe oznacza, że w czasie realizacji transportów podmioty świadczące przewozy mają fizyczne i zarazem wyłączne władztwo (kontrolę) nad powierzonymi im przez spółkę przesyłkami oraz danymi osobowymi zawartymi na etykietach adresowych oraz wewnątrz przesyłek.

Z postanowień umów o świadczenie transportu wynikało ponadto, że przewoźnicy obowiązani byli do pomocy przy załadunku (wyładunku) przesyłek i tym samym mieli, albo mogli mieć, bezpośredni dostęp do przesyłek oraz znajdujących się na ich etykietach adresowych danych osobowych. Powyższe przeczy wyjaśnieniom złożonym w toku kontroli przez pracowników spółki, że przewoźnicy nie mieli w ogóle kontaktu z przesyłkami.

W wyniku kontroli stwierdzono, że przewoźnicy pełnili funkcje podmiotów przetwarzających, o których mowa w art. 4 pkt 8 rozporządzenia 2016/679. Przetwarzali dane osobowe w imieniu administratora, jednak bez formalnego umocowania, wymaganego w treści art. 28 ust. 3 rozporządzenia 2016/679, tj. bez zawarcia stosownych umów dotyczących kwestii powierzenia danych, co stanowi jego naruszenie. Prezes UODO wszczął z urzędu postępowanie administracyjne w sprawie przetwarzania przez spółkę danych osobowych w związku ze świadczeniem usługi w zakresie doręczania przesyłek kurierskich. Przedmiotem postępowania było naruszenie przepisów o ochronie danych osobowych, które zostało stwierdzone w trakcie opisanej kontroli.

2.7. Decyzje administracyjne w postępowaniach kontrolnych

W wyniku nieprawidłowości stwierdzonych w trakcie przeprowadzonych kontroli w 2023 r. Prezes UODO wszczął z urzędu **trzynaście (13) postępowań administracyjnych** dotyczących przetwarzania danych osobowych. Po ich zakończeniu wydał cztery (4) decyzje, w tym w jednym przypadku udzielił upomnienia i nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679. W dwóch decyzjach Prezes UODO udzielił upomnienia, a w jednej – umorzył postępowanie.

Poniżej przytoczona została decyzja Prezesa UODO[115], w której udzielił upomnienia oraz nakazał dostosowanie operacji przetwarzania do przepisów RODO, po przeprowadzeniu postępowania kontrolnego w jednym z **banków.** Zakresem tej kontroli objęto przetwarzanie przez bank danych osobowych przy użyciu aplikacji mobilnej.

Prezes UODO w wydanej decyzji przytoczył treść naruszonego przepisu art. 4 pkt 11 rozporządzenia 2016/679, w myśl którego zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli tej osoby, w formie oświadczenia lub wyraźnego działania potwierdzającego, w którym przyzwala na przetwarzanie dotyczących jej danych osobowych. Natomiast treść klauzuli udzielenia zgody przez klienta na przekazanie jego danych osobowych przez bank spółkom grupy kapitałowej banku oraz towarzystwom ubezpieczeniowym dla celów marketingu, znajdującej się w formularzu umowy rachunków płatniczych, kanałów zdalnych oraz karty debetowej, nie spełniała kryteriów definicji zawartej w ww. przepisie. Przede wszystkim nie spełniała wymogu konkretności z uwagi na niewymienienie wszystkich administratorów, którym dane mają być udostępnione. Zamiast wymienienia nazw (firm) poszczególnych administratorów (spółek, towarzystw ubezpieczeniowych) klauzula zawarta w formularzu, dotycząca udostępniania danych klienta podmiotom trzecim, zawierała jedynie ogólnikowe określenia „spółki grupy kapitałowej banku" oraz „towarzystwa ubezpieczeniowe, z którymi bank ma zawarte umowy ubezpieczenia grupowego klientów banku".

W treści ww. decyzji Prezes UODO powołał się również na art. 35 ust. 7 RODO, zgodnie z którym ocena skutków dla ochrony danych osobowych zawiera co najmniej: a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą oraz d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia, oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia 2016/679, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, oraz innych osób, których sprawa dotyczy. W wyniku przeprowadzonych czynności kontrolnych stwierdzono, że bank nie dokonał w sposób prawidłowy oceny skutków dla ochrony danych w związku z funkcjonowaniem aplikacji mobilnej. Przedłożony przez bank w toku kontroli dokument nie stanowił realizacji obowiązku, o którym mowa w powołanym wyżej przepisie art. 35 ust. 7 RODO, gdyż nie zawierał wszystkich wskazanych w nim wymaganych elementów.

Z treści ww. dokumentu nie wynikało również, że jest w nim zawarty systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym prawnie uzasadnionych interesów realizowanych przez administratora, które w przypadku banku również powinny być uwzględnione z uwagi na fakt, że powołuje się on niejednokrotnie na art. 6 ust. 1 lit. f) RODO, jako podstawę prawną przetwarzania danych. Wspomniany opis, zawarty w ocenie skutków, był ogólnikowy, odnosił się jedynie „hasłowo" do operacji i celów przetwarzania. Opis ten nie zawierał również dokładnego wskazania istoty i przebiegu planowanych operacji przetwarzania związanych z funkcjonowaniem aplikacji mobilnej. Innymi słowy, operacje przetwarzania danych nie były przejrzyście wyodrębnione ani

[115] DKN.5112.9.2022.

opisane w systematyczny sposób, z uwzględnieniem: ich istotnych elementów technicznych, specyfiki, etapów oraz przyporządkowanych do nich środków i zasobów służących przetwarzaniu danych.

Prezes UODO wskazał także w decyzji na przepis art. 30 ust. 1 RODO, zgodnie z którym każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje: a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych; b) cele przetwarzania; c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych; e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Prezes UODO stwierdził, że bank, jako administrator, nie prowadził rejestru czynności przetwarzania danych osobowych w sposób odpowiadający wymogom art. 30 ust. 1 RODO. Dokument przedstawiony przez bank w toku kontroli jako rejestr czynności przetwarzania nie spełniał wymogów ww. przepisu. Nie zawierał bowiem wszystkich elementów treści wskazanych w ww. przepisie, tj.: imienia i nazwiska lub nazwy oraz danych kontaktowych administratora oraz inspektora ochrony danych, a także kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione. Ponadto brak w nim było opisu technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO. Z kolei pozostałe elementy rejestru czynności przetwarzania wskazane w art. 30 ust. 1 rozporządzenia 2016/679 zostały ujęte w niewystarczający sposób, tj. niewyczerpująco i ogólnikowo.

W wydanej decyzji Prezes UODO udzielił bankowi upomnienia za naruszenie ww. przepisów oraz nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679, tj. art. 4 pkt 11.

2.8. Wyroki WSA w Warszawie i NSA dotyczące decyzji Prezesa UODO w sprawie kontroli

W roku 2023 Wojewódzki Sąd Administracyjny w Warszawie utrzymał w mocy dwie (2) decyzje[116] Prezesa UODO nakładające administracyjną karę pieniężną, które wydane były w poprzednich latach po przeprowadzeniu postępowań kontrolnych w przedmiocie przetwarzania danych osobowych. W przypadku jednej z ww. decyzji złożona została skarga kasacyjna do Naczelnego Sądu Administracyjnego. Jedna decyzja Prezesa UODO

[116] DKN.5110.12.2021 utrzymana w mocy wyrokiem WSA z 26 kwietnia 2023 r. o sygn. akt II SA/Wa/1272/22 oraz DKN.5112.1.2020 utrzymana w mocy wyrokiem WSA z 21 czerwca 2023 r. o sygn. akt II SA/Wa/150/23.

wydana po przeprowadzeniu postępowania kontrolnego została uchylona przez Naczelny Sąd Administracyjny[117].

3. 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[118], 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.

Egzekucji administracyjnej podlegają wszystkie niewykonane przez zobowiązanych decyzje administracyjne Prezesa UODO, to jest:

a) **ostateczne decyzje** nakładające na administratora lub podmiot przetwarzający (zobowiązanego) **obowiązek z zakresu ochrony danych osobowych mający charakter niepieniężny** (decyzje zawierające tzw. nakaz). Decyzje te co do zasady stają się wykonalne z dniem ich doręczenia stronie (niezależnie od ich ewentualnego zaskarżenia do sądu administracyjnego)[119]. Jeżeli decyzja administracyjna zawiera postanowienia dodatkowe – określające termin jej wykonania, to obowiązek z niej wynikający podlega wykonaniu i w razie potrzeby egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek niepieniężny nakładany na 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) **prawomocne decyzje nakładające administracyjne kary pieniężne** – zaskarżenie do sądu administracyjnego takiej decyzji wstrzymuje jej wykonanie i tym samym możliwość wszczęcia egzekucji administracyjnej[120].

Zadania związane z zapewnieniem wykonywania przez zobowiązanych obowiązków wynikających z decyzji administracyjnych Prezesa UODO, zarówno niepieniężnych

[117] ZSPR.421.2.2019 uchylona wyrokiem NSA z 9 lutego 2023 r. o sygn. akt III OSK 3945/21.
[118] Ustawa z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2023 r. poz. 2505 ze zm.).
[119] Art. 61 § 1 ustawy z 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2024 r. poz. 935 ze zm.).
[120] Art. 74 ustawy o ochronie danych osobowych.

(nakazy decyzji), jak i pieniężnych (nałożone kary) są realizowane w Urzędzie Ochrony Danych Osobowych przez Departament Organizacji, Kar i Egzekucji.

Postępowanie prowadzone w urzędzie, którego ostatecznym efektem ma być stwierdzenie wykonania decyzji Prezesa UODO lub – w razie potrzeby – wyegzekwowanie jej wykonania od zobowiązanego podmiotu, jest kilkuetapowe i odmienne w zależności od tego, czy egzekwowany obowiązek ma charakter pieniężny (administracyjna kara pieniężna, grzywna w celu przymuszenia itp.) czy niepieniężny (nakaz).

Pierwszym etapem postępowania prowadzonego w UODO, wspólnym dla postępowań dotyczących decyzji nakładających oba rodzaje obowiązków, jest postępowanie sprawdzające wykonanie przez zobowiązanego decyzji (i dające też możliwość zobowiązanemu dobrowolnego jej wykonania na tym jeszcze etapie sprawy). W przypadku gdy postępowanie to nie wykaże, że decyzja została wykonana, do zobowiązanego kierowane jest upomnienie[121] zawierające wezwanie do wykonania obowiązku z zagrożeniem skierowania sprawy na drogę postępowania egzekucyjnego.

Jeżeli zobowiązany, mimo otrzymania upomnienia, nadal nie wykonuje nakazu decyzji Prezesa UODO (obowiązku o charakterze niepieniężnym), sporządzone zostają: tytuł wykonawczy (dokument urzędowy stwierdzający istnienie oraz wymagalność obciążającego zobowiązanego obowiązku) oraz postanowienie o nałożeniu na zobowiązanego grzywny w celu przymuszenia – środka egzekucyjnego przewidzianego przepisami ustawy o postępowaniu egzekucyjnym w administracji. Doręczenie zobowiązanemu obu tych dokumentów wszczyna wobec niego **egzekucję obowiązku o charakterze niepieniężnym.** Jak wskazano wyżej, w postępowaniu tym Prezes UODO występuje jednocześnie w roli wierzyciela i organu egzekucyjnego.

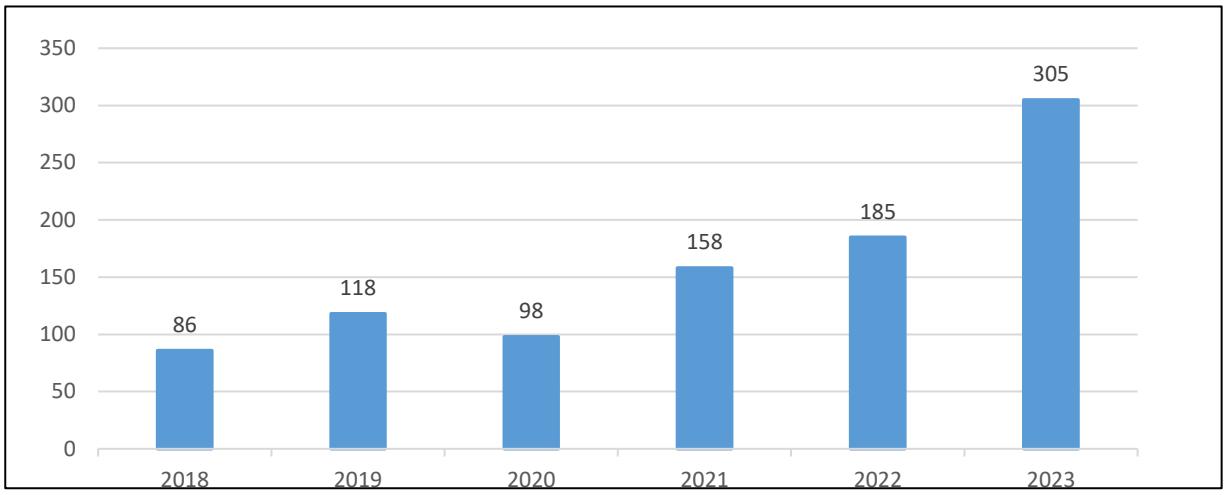
Brak zapłaty przez zobowiązanego orzeczonej na poprzednim etapie postępowania grzywny w celu przymuszenia powoduje konieczność wszczęcia wobec niego **egzekucji należności pieniężnych.** Takie też postępowanie wszczynane jest w przypadku stwierdzenia w postępowaniu sprawdzającym braku dobrowolnej zapłaty należności pieniężnych innych niż grzywna w celu przymuszenia – w szczególności administracyjnych kar pieniężnych. Egzekucja należności pieniężnych rozpoczyna się od wystawienia przez Prezesa UODO tytułu wykonawczego oraz przesłania go organowi egzekucyjnemu – właściwemu dla zobowiązanego naczelnikowi urzędu skarbowego. Dalsze czynności prowadzi organ egzekucyjny dysponujący odpowiednimi: uprawnieniami, środkami egzekucyjnymi, informacjami i narzędziami, pozwalającymi na skuteczne działanie przy użyciu środków przymusu państwowego.

Postępowania w zakresie egzekucji decyzji Prezesa UODO

W 2023 r. wszczętych zostało **305 postępowań sprawdzających wykonanie decyzji Prezesa UODO** (7 postępowań dotyczyło sprawdzenia wykonania decyzji nakładających administracyjne kary pieniężne, pozostałe 298 decyzji podlegających sprawdzeniu były decyzjami zawierającymi nakaz – obowiązek o charakterze niepieniężnym). Oznacza to **wzrost liczby takich postępowań o 65% w stosunku do roku 2022** (w którym wszczęto 185 tego typu postępowań) i o 255% w odniesieniu do roku, w którym zaczęto stosować przepisy RODO (86 postępowań).

[121] Art. 6 § 1 i art. 15 ustawy o postępowaniu egzekucyjnym w administracji.

Trend wzrostowy liczby tego rodzaju postępowań obrazuje poniższy wykres.



Wykres 5: Zestawienie decyzji Prezesa UODO przekazanych w latach 2018–2023 do sprawdzenia wykonania i ewentualnej egzekucji administracyjnej

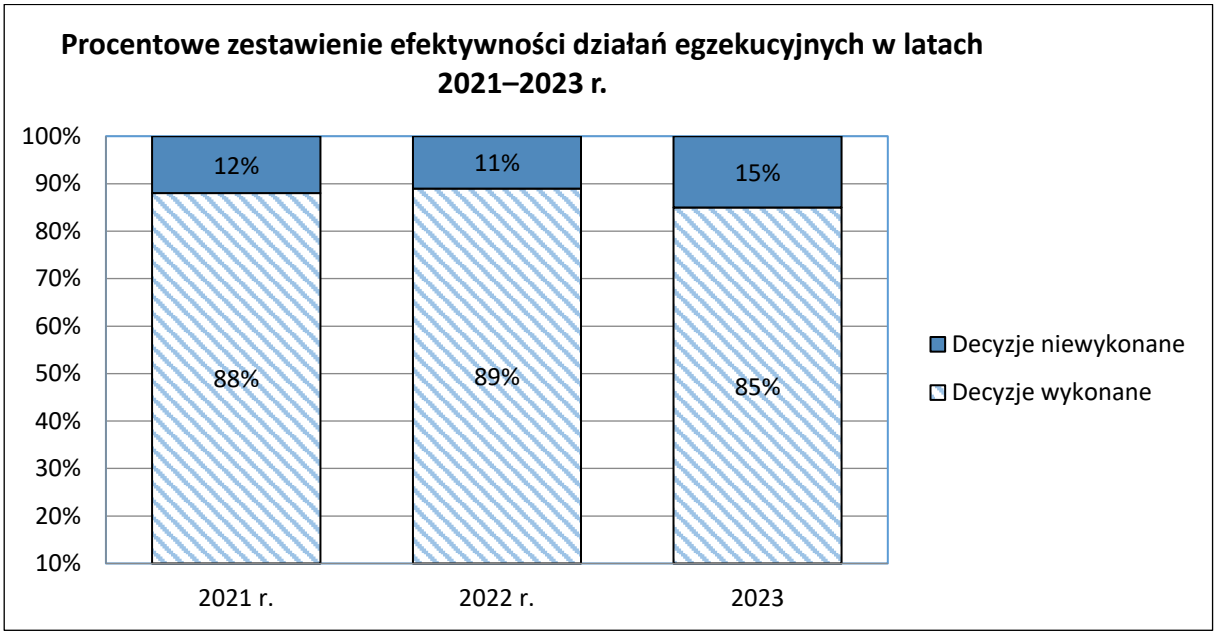
Efektywność prowadzonych przez UODO działań, mających na celu sprawdzenie i spowodowanie wykonania przez zobowiązanych obowiązków nałożonych na nich decyzjami administracyjnymi, przedstawia się następująco:

- spośród 305 decyzji, w odniesieniu do których wszczęte zostały postępowania w 2023 r., **wykonanych zostało przez zobowiązanych 260 decyzji,** natomiast
- co do 45 decyzji Prezes UODO nie uzyskał dowodów na ich wykonanie. Decyzje te w dalszym ciągu objęte są działaniami UODO.

W 11 przypadkach wszczęta została egzekucja obowiązku o charakterze niepieniężnym, w ramach których na zobowiązanych nałożone zostały grzywny w celu przymuszenia. W stosunku do 2 zobowiązanych Prezes UODO orzekł administracyjną karę pieniężną za nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy[122]. W odniesieniu do pozostałych 32 decyzji prowadzone są w dalszym ciągu działania mające na celu sprawdzenie ich wykonania lub spowodowanie ich dobrowolnego wykonania przez zobowiązanych.

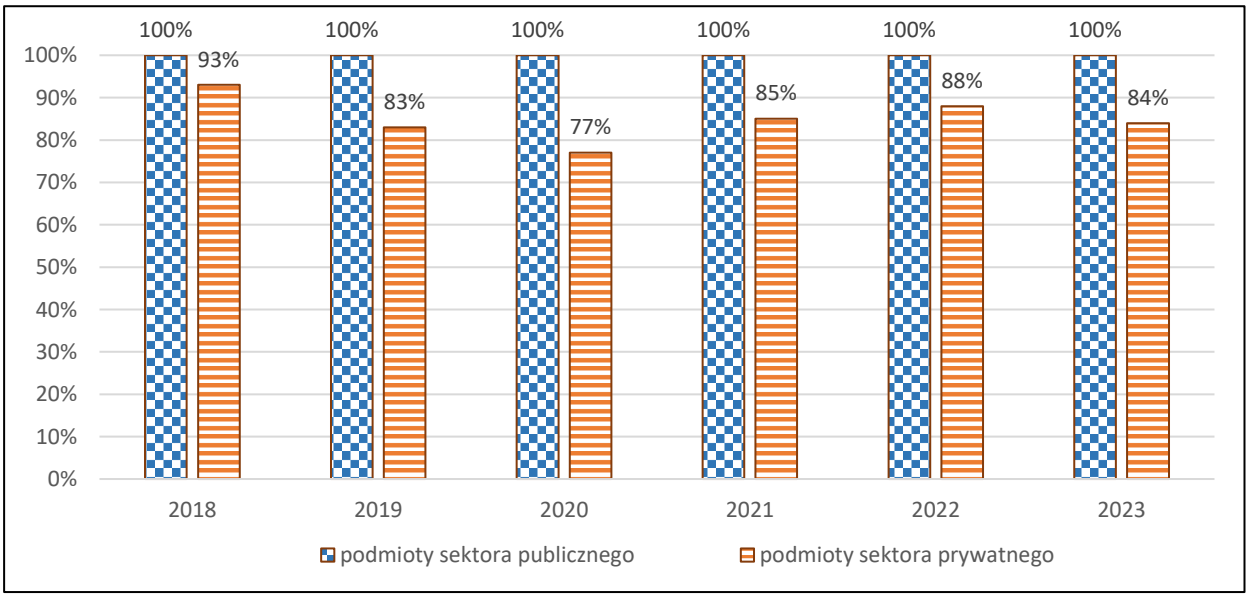
Procentowy wskaźnik efektywności działań w odniesieniu do wszystkich decyzji administracyjnych wszczętych w 2023 r. wyniósł **85%.** Porównanie wskaźników efektywności w latach 2021–2023 ilustruje wykres 6.

[122] Art. 83. ust. 6 RODO.



Wykres 6: Procentowe zestawienie efektywności działań egzekucyjnych UODO w latach 2021–2023

W 2023 r. działania Prezesa UODO w zakresie sprawdzenia wykonania i egzekucji decyzji administracyjnych dotyczyły w 7 % przypadków podmiotów z sektora publicznego (22 postępowania), a w pozostałych 93 % przypadków – podmiotów prywatnych (283 postępowania). Podobnie jak w 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, odnotować należy stale utrzymujący się w latach 2018–2023 wskaźnik stuprocentowej wykonalności nakazów orzeczonych przez Prezesa UODO wobec podmiotów należących do sektora publicznego.



Wykres 7: Zestawienie efektywności prowadzonych działań egzekucyjnych w odniesieniu do podmiotów z sektora publicznego i sektora prywatnego w latach 2018–2023

Egzekucja obowiązków o charakterze niepieniężnym

Wobec stwierdzenia niewykonania przez zobowiązanych nakazów decyzji Prezesa UODO w 2023 r. wszczętych zostało **13 egzekucji obowiązków o charakterze niepieniężnym.** Wystawione w tym okresie tytuły wykonawcze objęły nakazy orzeczone 17 decyzjami administracyjnymi, a łączna kwota grzywien w celu przymuszenia zastosowanych wobec zobowiązanych przez Prezesa UODO w tych postępowaniach wyniosła **99 000 zł.** Spośród 13 wszczętych w 2023 r. egzekucji obowiązków o charakterze niepieniężnym:

1) jedna egzekucja okazała się skuteczna – zobowiązany wykonał nakaz decyzji Prezesa UODO, a nałożona na niego grzywna w celu przymuszenia w wysokości 3 000 zł została umorzona;
2) 9 egzekucji okazało się bezskutecznymi na tym etapie sprawy, w związku z czym wobec zobowiązanych wszczęto egzekucje należności pieniężnych mających na celu wyegzekwowanie grzywien w celu przymuszenia nałożonych na nich w łącznej kwocie 75 000 zł;
3) w trakcie postępowania były 3 egzekucje, w których nałożono grzywny w celu przymuszenia w łącznej kwocie 21 000 zł.

Egzekucja należności pieniężnych

W 2023 r. Prezes UODO doprowadził do wszczęcia **16 egzekucji należności pieniężnych**, których łączna wysokość wynosiła 261 242 zł. Porównując liczbę tego rodzaju spraw z poprzednimi latami wskazać należy, że po wzroście na poziomie 400% w poprzednim roku sprawozdawczym, ich liczba w roku 2023 osiągnęła poziom podobny do roku 2022, w którym wszczęto 15 postępowań. W omawianym okresie sprawozdawczym egzekucje należności pieniężnych dotyczyły dwóch rodzajów należności: (1) nałożonych przez Prezesa UODO administracyjnych kar pieniężnych oraz (2) grzywien w celu przymuszenia orzeczonych przez Prezesa UODO, jako środków egzekucyjnych w egzekucjach obowiązków o charakterze niepieniężnym.

W ujęciu liczbowym postępowania te oraz ich efekty przedstawiają się następująco:

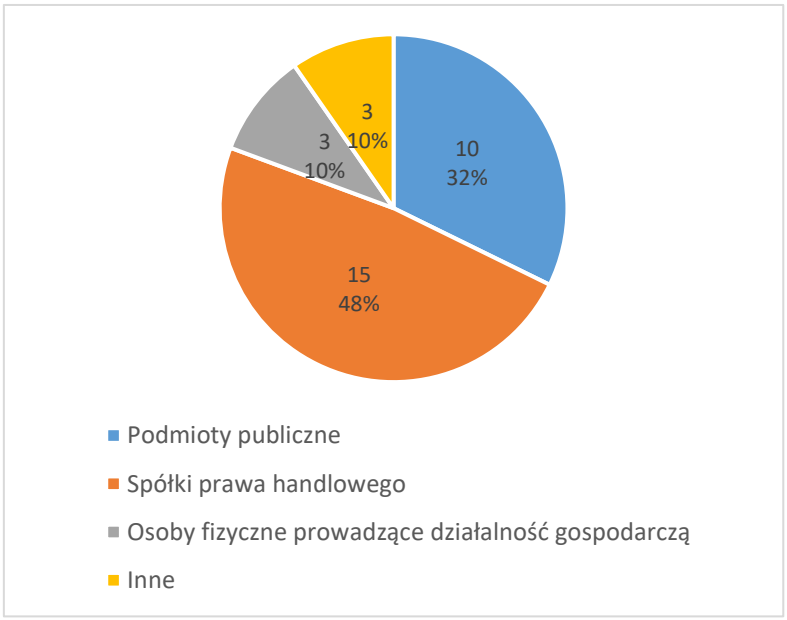
1) Prezes UODO w bieżącym okresie sprawozdawczym doprowadził do wszczęcia **9 egzekucji,** których przedmiotem były **administracyjne kary pieniężne** w łącznej wysokości 211 242 zł. Wszystkie egzekwowane w tych postępowaniach kary pieniężne nałożone zostały na podmioty prywatne – spółki prawa handlowego. W przypadku 4 spośród tych egzekucji (w których egzekwowane były kary w łącznej wysokości 97 865 zł), organy egzekucyjne (właściwi miejscowo naczelnicy urzędów skarbowych) odmówiły przystąpienia do egzekucji ze względu na brak majątku lub źródła dochodu, z których możliwa byłaby egzekucja, lub – z tego samego powodu – umorzyły wszczęte już postępowania egzekucyjne. W pozostałych przypadkach (5 kar w łącznej kwocie 113 377 zł) właściwe organy egzekucyjne prowadzą w dalszym ciągu działania egzekucyjne.
2) Przedmiotem **7** wszczętych przez Prezesa UODO egzekucji należności pieniężnych były **grzywny w celu przymuszenia,** w łącznej kwocie 50 000 zł. Wszystkie tego rodzaju środki egzekucyjne orzeczone zostały wobec podmiotów prywatnych – sześciu spółek prawa handlowego i jednej osoby fizycznej prowadzącej indywidualną

działalność gospodarczą. W przypadku dwóch tytułów wykonawczych wystawionych przez Prezesa UODO na kwotę 15 000 zł właściwi naczelnicy urzędów skarbowych odmówili przystąpienia do egzekucji ze względu na brak majątku lub źródła dochodu, z których możliwa byłaby egzekucja, lub – z tego samego powodu – umorzyli wszczęte już postępowanie egzekucyjne. Pozostałe egzekucje – pięć tytułów wykonawczych na łączną kwotę 35 000 zł – nadal były prowadzone przez właściwe organy egzekucyjne.

4. Administracyjne kary pieniężne

Stosownie do art. 58 ust. 2 lit. i) RODO Prezesowi UODO przysługuje uprawnienie do zastosowania administracyjnej kary pieniężnej, oprócz lub zamiast innych środków naprawczych, zależnie od okoliczności konkretnej sprawy. W oparciu o art. 210a Prawa telekomunikacyjnego[123] Prezes UODO uprawniony jest do nakładania administracyjnych kar pieniężnych za naruszenie niektórych obowiązków przewidzianych przepisami tego aktu prawnego[124].

W 2023 r. Prezes UODO skorzystał z uprawnienia do zastosowania administracyjnej kary pieniężnej w 30 sprawach, nakładając na **31 podmiotów** administracyjne kary pieniężne w łącznej kwocie **1 230 331,28 zł.** W porównaniu z rokiem poprzednim oznacza to **wzrost ilościowy nałożonych kar o 55% i spadek ich łącznej wysokości o 85%.** Dla porównania, w 2022 r. orzeczonych zostało 20 administracyjnych kar pieniężnych na łączną kwotę 7 850 861 zł.



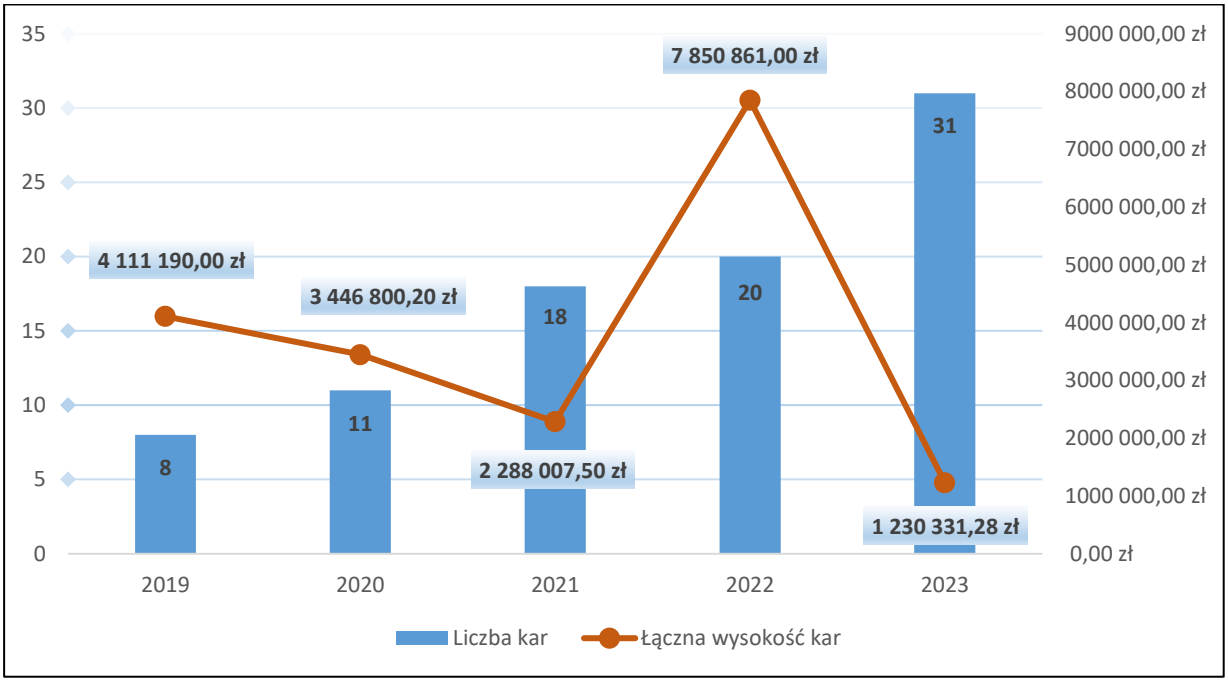
Spośród 31 ukaranych podmiotów 10 z nich należało do sektora finansów publicznych, natomiast wśród pozostałych 21 podmiotów prywatnych – 15 to spółki prawa handlowego, 3 to osoby fizyczne prowadzące działalność gospodarczą, a pozostałe 3 to wspólnota mieszkaniowa, spółdzielnia mieszkaniowa oraz organ samorządu zawodowego.

Wykres 8: Zestawienie podmiotów podlegających ukaraniu administracyjną karą pieniężną, z podziałem na ich status i formę prawną

Wykres 9 przedstawia liczbę i łączną wysokość administracyjnych kar pieniężnych orzeczonych przez Prezesa UODO w omawianym okresie sprawozdawczym w porównaniu do lat poprzednich – począwszy od dnia rozpoczęcia stosowania przepisów RODO, które przyznały mu prawo do stosowania administracyjnych kar pieniężnych, i od

[123] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34).
[124] W omawianym okresie sprawozdawczym 2023 r. Prezes UODO w żadnym przypadku nie skorzystał z tego uprawnienia.

roku, w którym Prezes UODO zaczął korzystać z tego rodzaju uprawnienia naprawczego, to jest od roku 2019.



Wykres 9: Zestawienie liczby i łącznej wysokości administracyjnych kar pieniężnych orzeczonych przez Prezesa UODO w latach 2019–2023

Przedstawiając w ujęciu statystycznym, z jednej strony działania podmiotów ukaranych, a z drugiej – działania Prezesa UODO w odniesieniu do orzeczonych w omawianym okresie sprawozdawczym administracyjnych kar pieniężnych, wskazać należy, że było:

1) **9 prawomocnych** na dzień 31 grudnia 2023 r. decyzji (niezaskarżonych do sądu administracyjnego) nakładających administracyjne kary pieniężne na **10 podmiotów** w łącznej kwocie **208 293,28 zł**. Spośród tych kar:
   a) 5 kar zapłaconych zostało dobrowolnie przez ukarane podmioty[125];
   b) wobec 4 ukaranych podmiotów wszczęta została egzekucja należności pieniężnych[126];
   c) w odniesieniu do jednej kary działania mające na celu jej wyegzekwowanie wstrzymane zostały w związku ze złożonym przez ukaranego, i rozpatrywanym przez Prezesa UODO, wnioskiem o uchylenie decyzji orzekającej karę[127].

2) **13 decyzji nieprawomocnych** na dzień 31 grudnia 2023 r. i **zaskarżonych** do Wojewódzkiego Sądu Administracyjnego w Warszawie, nakładających administracyjne kary pieniężne w łącznej wysokości **856 660 zł**, z czego:

[125] DKN.5131.31.2021, DKN.5131.50.2021 (dwie kary orzeczone jedną decyzją), DKN.5131.56.2022, DOKE.561.1.2023.
[126] DKE.561.35.2022, DKE.561.37.2022, DKN.5131.8.2021, DKE.561.38.2022.
[127] DKN.5131.43.2022.

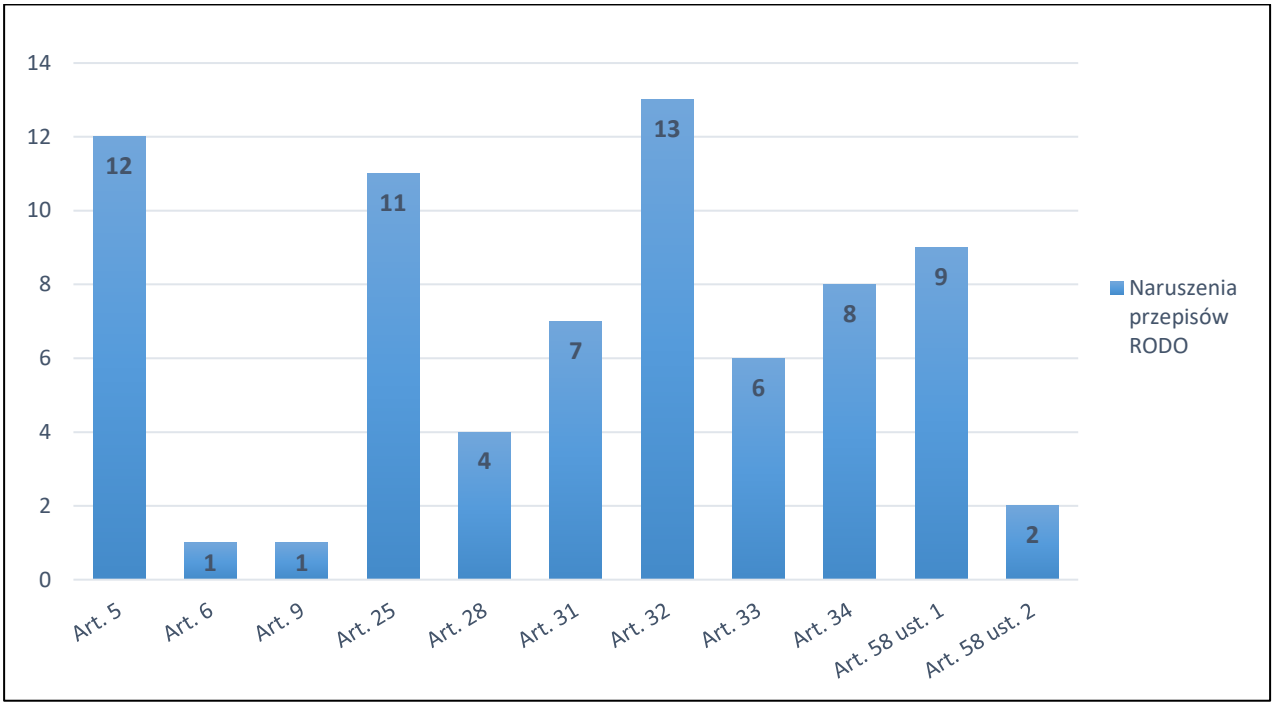
a) w 2 przypadkach skargi zostały oddalone przez Wojewódzki Sąd Administracyjny w Warszawie[128];
b) jedna kara została uchylona przez Wojewódzki Sąd Administracyjny w Warszawie; skargę kasacyjną do Naczelnego Sądu Administracyjnego na wyrok złożył Prezes UODO[129];
c) w odniesieniu do 10 administracyjnych kar pieniężnych trwa postępowanie sądowo-administracyjne[130].

3) **7 decyzji nieprawomocnych** na dzień 31 grudnia 2023 r., i **niezaskarżonych** do Wojewódzkiego Sądu Administracyjnego w Warszawie, nakładających administracyjne kary pieniężne w łącznej wysokości **142 530 zł**, z czego:
   a) 3 kary zapłacone zostały dobrowolnie przez ukarane podmioty między upływem okresu sprawozdawczego a dniem sporządzenia niniejszego sprawozdania[131];
   b) 4 kary oczekują na uprawomocnienie się lub wszczęcie egzekucji[132].
4) W odniesieniu do **jednej kary** (w wysokości **22 848 zł**) Prezes UODO wznowił postępowanie na podstawie art. 145 § 1 pkt 5 K.p.a., a po jego ponownym przeprowadzeniu uchylił własną decyzję orzekającą administracyjną karę pieniężną i w jej miejsce udzielił administratorowi upomnienia[133].

Na wykresie 10 przedstawiono informację o rodzajach naruszeń podlegających ukaraniu administracyjnymi karami pieniężnymi oraz o przepisach RODO, których naruszenie stwierdzone zostało przez Prezesa UODO w decyzjach nakładających na administratorów lub podmioty przetwarzające administracyjne kary pieniężne.

W związku z tym, że jedna administracyjna kara pieniężna może być wymierzona za naruszenie kilku przepisów RODO, przedstawiona poniżej liczba naruszeń poszczególnych przepisów RODO nie odpowiada liczbie nałożonych przez Prezesa UODO w omawianym okresie sprawozdawczym kar pieniężnych.

[128] DKN.5131.12.2020, DKN.5131.45.2022.
[129] DKN.5131.49.2021.
[130] DKN.5131.31.2022, DKN.5131.44.2022, DKN.5131.47.2022, DOKE.561.8.2023, DKN.5131.55.2022, DKN.5131.6.2023, DKN.5131.26.2023, DKN.5131.13.2022, DKN.5131.42.2022, DKN.5131.32.2023.
[131] DOKE.561.2.2023, DKN.5131.34.2022, DKN.5131.35.2022.
[132] DOKE.561.7.2023, DOKE.561.5.2023, DOKE.561.18.2023, DOKE.561.14.2023.
[133] DKE.561.24.2022.



Wykres 10: Zestawienie naruszeń poszczególnych przepisów RODO podlegających ukaraniu administracyjnymi karami pieniężnymi w roku 2023

W ramach kompetencji Prezesa Urzędu Ochrony Danych Osobowych do orzekania o sankcjach finansowych, przysługuje mu uprawnienie do nakładania **administracyjnych kar pieniężnych o szczególnym dyscyplinującym charakterze.** Kary te mają na celu zdyscyplinowanie administratorów i podmioty przetwarzające, po pierwsze – **do prawidłowej współpracy z Prezesem UODO** przejawiającej się w szczególności w zapewnieniu dostępu do wszelkich danych i informacji niezbędnych w prowadzonych przez niego postępowaniach, a po drugie – **do wykonywania obowiązków nałożonych na te podmioty decyzjami Prezesa UODO.** Funkcja drugiego rodzaju z tych kar jest alternatywną lub uzupełniającą wobec narzędzi, którymi dysponuje Prezes UODO – w celu wyegzekwowania orzeczonych przez siebie obowiązków niepieniężnych – w oparciu o przepisy ustawy o postępowaniu egzekucyjnym w administracji.

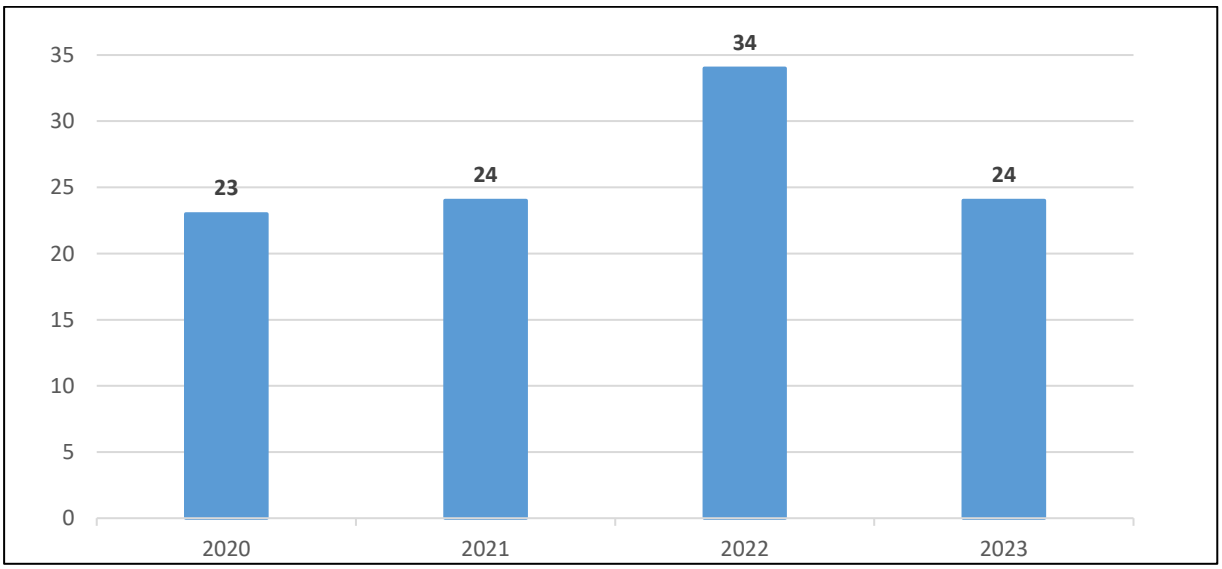
Administracyjne kary pieniężne za brak współpracy z organem nadzorczym i za niezapewnienie dostępu do informacji niezbędnych do realizacji jego zadań.

Obowiązkiem Prezesa UODO jest realizowanie zadań związanych z ochroną danych osobowych, w tym egzekwowanie 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 (art. 31 RODO) oraz obowiązek zapewnienia organowi nadzorczemu dostępu do informacji niezbędnych do realizacji jego zadań – art. 58 ust. 1 lit. a) i e) RODO.

W omawianym roku sprawozdawczym, tak jak w poprzednich latach, Prezes UODO dostrzegał problem braku współpracy stron w prowadzonych przez siebie postępowaniach i braku dostępu do informacji niezbędnych do realizacji jego zadań. Do tego rodzaju naruszeń ze strony uczestników postępowań dochodziło zarówno w postępowaniach zainicjowanych skargami osób fizycznych, jak i w postępowaniach prowadzonych z urzędu, w szczególności w związku z naruszeniami ochrony danych osobowych. Naruszenia te polegały głównie na niepodejmowaniu korespondencji kierowanej do uczestników postępowań, na ignorowaniu wezwań Prezesa UODO bądź na udzielaniu informacji niepełnych, sprzecznych ze sobą czy wręcz lekceważących – innymi słowy: takich, które nie pozwalają na rozstrzygnięcie sprawy lub wydłużają w sposób nieuzasadniony czas trwania postępowań.

W związku z powyższym, w celu zdyscyplinowania stron postępowań do prawidłowego wypełniania obowiązków procesowych, Prezes UODO wszczął w 2023 r. z urzędu **24 postępowania** w przedmiocie nałożenia administracyjnej kary pieniężnej za tego rodzaju naruszenia. Oznacza to spadek liczby tego rodzaju postępowań o 29% w stosunku do poprzedniego okresu sprawozdawczego, w którym wszczęto 34 tego rodzaju postępowania.

Porównanie liczby wszczętych w 2023 r. postępowań, w przedmiocie nałożenia kary za brak współpracy z Prezesem UODO i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań, z liczbą tego rodzaju postępowań zainicjowanych w poprzednich okresach sprawozdawczych przedstawia wykres 11.



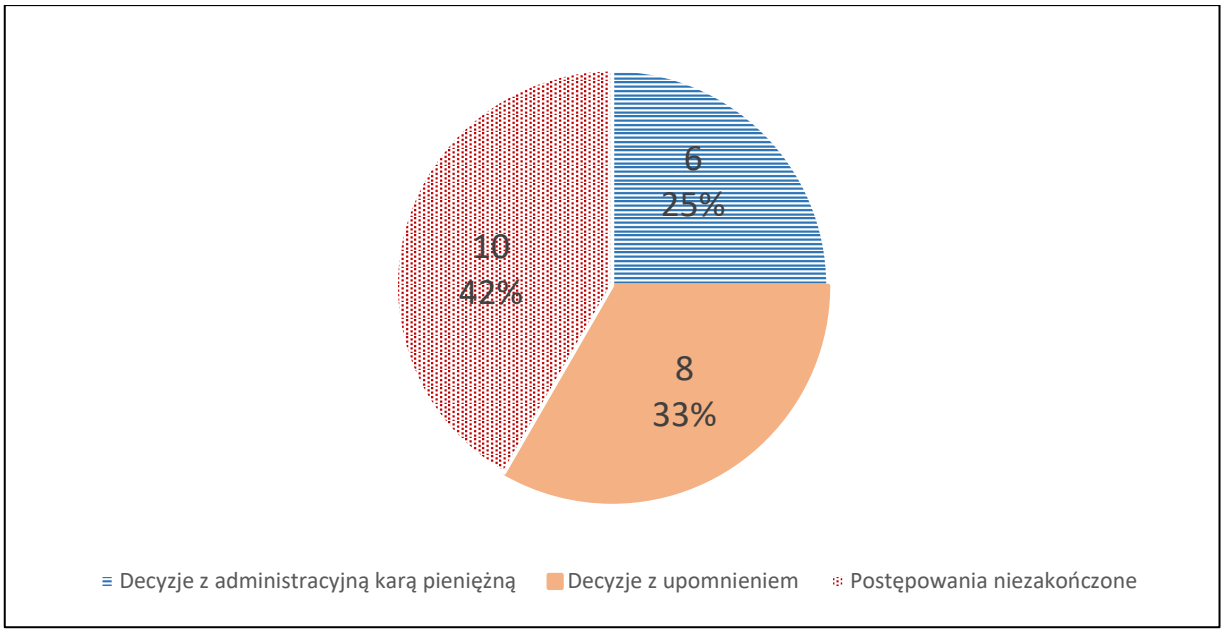
Wykres 11: Zestawienie liczby wszczętych w latach 2020–2023 postępowań w przedmiocie nałożenia kary za brak współpracy z organem i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań

W 8 przypadkach samo wszczęcie postępowania w przedmiocie nałożenia kary okazało się skuteczne i strony zaczęły współpracować z Prezesem UODO – udzieliły żądanych przez niego informacji niezbędnych do rozstrzygnięcia sprawy oraz usprawiedliwiły swoje zaniedbania w postępowaniu, co spowodowało podjęcie przez

Prezesa UODO decyzji o odstąpieniu od nałożenia kary i poprzestaniu na udzieleniu stronom **upomnień.**

Decyzjami nakładającymi administracyjne kary pieniężne zakończyło się 6 postępowań, zaś wysokość nałożonych tymi decyzjami kar wyniosła łącznie 148 554 zł. Do dnia sporządzenia niniejszego sprawozdania dwie z tych kar (w łącznej wysokości 47 160 zł) zostały dobrowolnie zapłacone przez ukaranych[134], jedna (w kwocie 56 592 zł) zaskarżona została przez stronę do Wojewódzkiego Sądu Administracyjnego w Warszawie[135], pozostałe 3 oczekują na uprawomocnienie się lub na wszczęcie egzekucji[136].

Pozostałych **10 postępowań** w przedmiocie nałożenia kary za brak współpracy z organem i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań, wszczętych w 2023 r., **nie zostało zakończonych** do dnia sporządzenia niniejszego sprawozdania.



Wykres 12: Zestawienie stanu oraz sposobu rozstrzygnięcia wszczętych w 2023 r. postępowań w przedmiocie nałożenia kary za brak współpracy z organem i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań

Poza sześcioma wskazanymi wyżej sprawami, wszczętymi w 2023 r. i zakończonymi w tym samym roku nałożeniem administracyjnych kar pieniężnych, w omawianym okresie sprawozdawczym orzeczone zostały dodatkowo **3 kary pieniężne** za tego samego rodzaju naruszenia w postępowaniach wszczętych jeszcze w 2022 r.[137] Łączna kwota tych kar wyniosła **51 291 zł.**

[134] DOKE.561.1.2023, DOKE.561.2.2023.
[135] DOKE.561.8.2023.
[136] DOKE.561.5.2023, DOKE.561.7.2023, DOKE.561.14.2023.
[137] DKE.561.35.2022, DKE.561.37.2022, DKE.561.38.2022.

Administracyjne kary pieniężne jako środek naprawczy przymuszający do wykonania nakazu decyzji

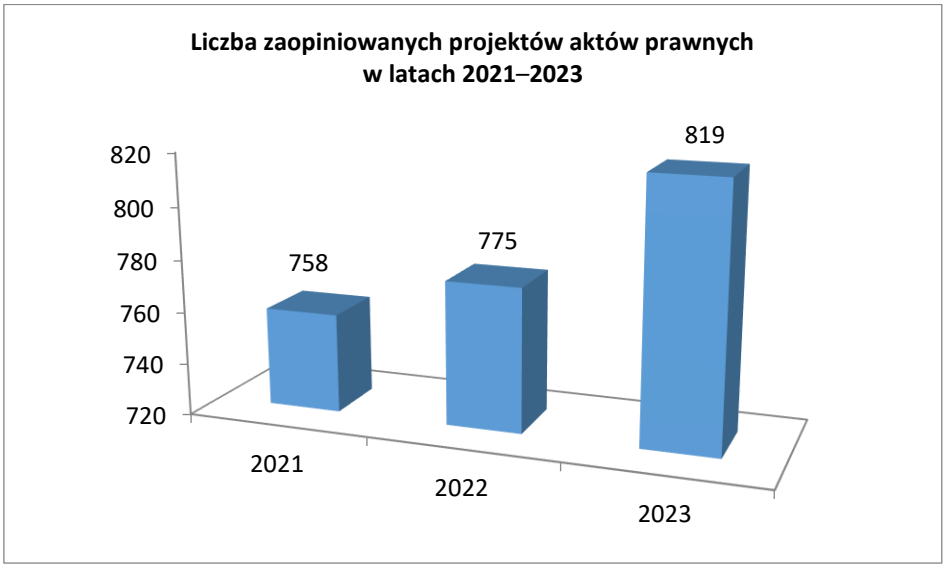
Nakazy zawarte w decyzjach Prezesa UODO to środki naprawcze, które służą przywróceniu stanu zgodnego z prawem i są elementem systemu ochrony danych osobowych. Należy podkreślić, że są one odpowiedzią na stan naruszenia jednego z podstawowych praw osoby fizycznej, jakim jest prawo do ochrony jej danych osobowych. Zadaniem Prezesa UODO jest monitorowanie przestrzegania przepisów o ochronie danych osobowych, w tym także 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 nakazów decyzji jest uprawnienie organu nadzorczego do nakładania kar za ich nieprzestrzeganie – zgodnie z art. 83 ust. 6 RODO.

W roku 2023 Prezes UODO wszczął **jedno postępowanie** w przedmiocie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie orzeczonego przez siebie w decyzji administracyjnej nakazu. W postępowaniu tym nałożona została na administratora (spółkę prawa handlowego) administracyjna kara pieniężna w wysokości **23 580 zł**[138]**.** Dodatkowo w 2023 r. **jedno postępowanie**, wszczęte jeszcze w 2022 r., zakończone zostało nałożeniem na zobowiązanego (spółkę prawa handlowego) administracyjnej kary pieniężnej w kwocie **22 848 zł** za nieprzestrzeganie nakazu orzeczonego przez Prezesa UODO[139]. W odniesieniu do decyzji nakładającej tę karę Prezes UODO wznowił jednak w omawianym okresie sprawozdawczym postępowanie na podstawie art. 145 § 1 pkt 5 K.p.a., a po jego ponownym przeprowadzeniu uchylił własną decyzję orzekającą administracyjną karę pieniężną i w jej miejsce udzielił administratorowi upomnienia.

5. Opiniowanie projektów aktów prawnych dotyczących ochrony danych osobowych

Ważnym zadaniem organu nadzorczego jest opiniowanie projektów aktów prawnych. Jego realizacja w toku procesu legislacyjnego następuje poprzez analizę projektowanych lub nowelizowanych przepisów pod kątem zapewnienia zgodności treści projektowanych regulacji z przepisami RODO. W 2023 r. organ nadzorczy zaopiniował ***819 projektów aktów prawnych*** *(zarówno na poziomie regulacji krajowych, jak i międzynarodowych). Dla porównania w 2022 r. zaopiniowanych zostało 775 projektów aktów prawnych, a w 2021 r. 758 projektów – co przedstawia poniższy wykres.*

[138] DOKE.561.18.2023.
[139] DKE.561.24.2022.



Wykres 13: Liczba zaopiniowanych projektów aktów prawnych, które wpłynęły do Urzędu Ochrony Danych Osobowych w latach 2021–2023

Zgodnie z art. 51 ustawy o ochronie danych osobowych założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych. Natomiast na mocy art. 57 ust.1 lit. c) RODO rolą organu nadzorczego w procesie legislacyjnym jest doradzanie zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem. Do tej roli organu nadzorczego odnosi się także art. 36 RODO, regulujący konstrukcję instrumentu prawnego – uprzednich konsultacji z organem nadzorczym. Wspomniany art. 36 w ust. 4 nakłada na państwo członkowskie obowiązek prowadzenia w toku prac legislacyjnych konsultacji z organem nadzorczym w przypadku gdy projekty aktów normatywnych dotyczą przetwarzania danych. Warto również zwrócić uwagę, że § 38 ust. 1 pkt 3 uchwały Nr 190 Rady Ministrów z 29 października 2013 r. Regulamin pracy Rady Ministrów zobowiązuje do skierowania projektu dokumentu rządowego do zaopiniowania przez instytucję, jaką jest organ nadzorczy, wskazany w przepisach regulujących zakres jego kompetencji, jeżeli projektowany dokument dotyczy zakresu działania organu. Nierzadko poszczególni ministrowie słusznie wskazują tę regulację jako podstawę prawną kierowania projektu aktu prawnego do zaopiniowania przez organ nadzorczy.

Niemniej zauważyć należy, że niektóre organy publiczne – poprzez pominięcie procesu uzgodnień i opiniowania – nie przekazują istotnych projektów aktów normatywnych, dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie, do oceny organu nadzorczego. Jest to nie tylko działanie wbrew obowiązującym przepisom i obowiązkom, ale także utrata okazji do eksperckiego wsparcia projektodawcy przez organ nadzorczy na jak najwcześniejszym etapie procesu legislacyjnego. W dużej części przypadków projekty niekonsultowane z Prezesem UODO na wcześniejszym etapie procesu legislacyjnego są do niego później kierowane z prośbą o opinię/stanowisko przez Rządowe Centrum Legislacji, a w przypadku ustaw – przez Sejm i Senat.

Organ nadzorczy, stojąc na straży praw osób, których dane dotyczą (podmiotów danych), wykonawców norm (administratorów, podmiotów przetwarzających), wspiera prawodawcę i doradza w sprawie aktów prawnych, celem zapewnienia stosowania w przepisach krajowych – przepisów RODO. W swoich opiniach legislacyjnych wskazuje aspekty wymagające uwzględnienia dla zgodności z przepisami ogólnego rozporządzenia o ochronie danych. Zaangażowanie organu nadzorczego w proces legislacyjny wymaga przeprowadzenia wielowątkowej analizy i oceny, zwłaszcza tego, czy *ratio legis* projektowanej regulacji wymaga przetwarzania danych osobowych oraz tego, w jaki sposób uwzględnia stosowanie norm ogólnego rozporządzenia o ochronie danych. **Efektem eksperckiego udziału organu nadzorczego w pracach legislacyjnych było sformułowanie w 2023 r. opinii legislacyjnych do wspomnianych już 819 projektów aktów prawnych.**

W 2023 r. większość uwag i zastrzeżeń organu przedstawionych po analizie projektowanych regulacji, dotyczyła głównie: właściwej konstrukcji podstaw prawnych, celów i sposobów przetwarzania danych, przyjęcia właściwych zakresów danych podlegających przetwarzaniu, prawidłowego określenia ról podmiotów w procesach przetwarzania danych osobowych, przetwarzania danych przy użyciu różnego rodzaju rozwiązań informatycznych (systemy teleinformatyczne, rejestry lub bazy danych), hierarchii aktów prawnych stanowiących o prawach i obowiązkach w zakresie przetwarzania danych osobowych – niedopuszczalności stanowienia podstaw prawnych dla praw i obowiązków związanych z przetwarzaniem danych w aktach wewnętrznych lub o charakterze cywilno-prawnym (np. zarządzeniach, wytycznych, porozumieniach).

W kontekście procesów legislacyjnych przedmiotem zainteresowania organu nadzorczego były następujące zagadnienia:

1) ocena skutków dla ochrony danych, w tym przeprowadzenie testu prywatności w procesie tworzenia prawa – tj. projektowanie ochrony danych osobowych przy określaniu sposobów przetwarzania;
2) hierarchia aktów prawnych – zasada praworządności, przyjęcie właściwej konstrukcji podstawy prawnej przetwarzania danych osobowych;
3) kwestie związane z określeniem ról poszczególnych podmiotów biorących udział w procesie przetwarzania danych osobowych;
4) systemy teleinformatyczne, łączenie baz danych;
5) wykorzystywanie nowych technologii w procesach przetwarzania danych, automatyczna weryfikacja, automatyczne podejmowanie decyzji przez systemy;
6) zakres pozyskiwanych danych osobowych;
7) potrzeba uregulowania i szczegółowego określenia zadań, kompetencji, praw i obowiązków krajowego organu nadzorczego w projektach aktów prawnych tworzonych na szczeblu Unii Europejskiej.

5.1. Ocena skutków dla ochrony danych osobowych na etapie legislacji

Istotnym aspektem przyjmowania określonej podstawy prawnej przetwarzania danych jest przeprowadzenie oceny skutków dla ochrony danych (zwanej testem prywatności) w rozumieniu art. 35 ust. 1 oraz art. 25 ust. 1 RODO. W sytuacji gdy projektowane rozwiązania mogą powodować wysokie ryzyko naruszenia praw i wolności,

ze względu na charakter, zakres, kontekst i cele przetwarzania, to planowane ich wprowadzenie powinno być poprzedzone testem prywatności – oceną skutków dla ochrony danych osobowych, zwłaszcza gdy projektowane przepisy prawa przewidują stosowanie nowych technologii w przetwarzaniu danych na dużą skalę, także tych w systemach i rejestrach państwowych. Tym samym przeprowadzenie przez projektodawcę analizy projektowanych rozwiązań, dotyczących przetwarzania danych, a w rezultacie identyfikacja i eliminacja ryzyk, związanych z proponowanym w przepisach przetwarzaniem danych osobowych w kontekście istoty i celów przyjmowanych rozwiązań oraz stosowanych technik przetwarzania danych, przyczynia się do stanowienia przepisów zgodnych z normami ogólnego rozporządzenia o ochronie danych. Ponadto należy zwrócić uwagę, że art. 25 ust. 1 RODO, odnoszący się do uwzględnienia ochrony danych w fazie projektowania, stanowi, aby także projektodawcy, przyjmując warunki przetwarzania danych, w treści projektowanych norm wdrażali odpowiednie rozwiązania (w zakresie środków technicznych i organizacyjnych) niezbędne dla ochrony prywatności.

Poprawnie przeprowadzona ocena skutków powinna wskazywać związek między wykonywanymi na danych osobowych operacjami a konkretnym celem ich przetwarzania. Art. 6 ust. 3 RODO wymaga, aby cel przetwarzania był określony w podstawie prawnej, gdy są nią przepisy prawa powszechnie obowiązującego (podstawa prawna przetwarzania wynikająca z prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator). Podstawa prawna może zawierać również przepisy szczegółowe, które dostosowują projektowane regulacje do przepisów RODO, 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. Organ nadzorczy w opiniach legislacyjnych postuluje uwzględnienie wymogów z art. 6 ust. 3 RODO i ich ważenie z *ratio legis* i zakresem projektowanej regulacji.

Niestety, część projektodawców nie dostrzega potrzeby dokonywania oceny skutków dla ochrony danych, jak również powołuje argument braku istnienia takiego obowiązku, nawet gdy akt prawny w zasadniczej swej części dotyczy przetwarzania danych osobowych, i to z użyciem nowych technologii. Mimo iż obowiązek przeprowadzenia oceny skutków dla ochrony danych nie jest wprost nałożony na twórcę przepisów prawa (projektodawcę) przepisami ogólnego rozporządzenia o ochronie danych, to wywodzić go należy z art. 35 ust. 10 RODO. Stanowi on bowiem, że procesy przetwarzania mające podstawę prawną w prawie Unii Europejskiej lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej, to wykonywanie wstępnej oceny skutków przez administratora nie jest już wymagane. Do podobnych wniosków prowadzi także analiza art. 25 ust. 1 RODO, odnoszącego się do uwzględniania ochrony danych w fazie projektowania, co organ nadzorczy wskazuje w swoich opiniach legislacyjnych. W efekcie konsekwentnego podnoszenia tego istotnego aspektu przez organ nadzorczy w eksperckich ocenach projektów aktów prawnych, niektóre resorty dokonują oceny skutków projektowanych regulacji dla ochrony danych. Dostrzegają jej

wagę, choć nadal są 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, z inicjatywy projektodawcy. Zdarza się również, i należy to ocenić pozytywnie, że resorty nie opracowują odrębnej oceny skutków dla ochrony danych, ale przedstawiają szczegółowo analizę proponowanych zmian w ramach OSR (oceny skutków regulacji), wyraźnie odnosząc się do aspektów przetwarzania danych osobowych, która również stanowi cenne źródło informacji m.in. dla organu nadzorczego.

Jako przykład aktu, w którym projektodawca nie wyważył wpływu planowanego przetwarzania danych osobowych na prywatność osób, których dane dotyczą, wskazać można **projekt ustawy o zmianie ustawy o wymianie informacji podatkowych z innymi państwami oraz niektórych innych ustaw** (ustawa DAC7)[140]. Organ nadzorczy zwrócił uwagę, że przepisy projektowanej ustawy powinny być poprzedzone oceną skutków, ponieważ mają na celu wdrożenie do krajowego porządku prawnego przepisów dyrektywy Rady (UE) 2021/514 z 22 marca 2021 r. zmieniającej dyrektywę 2011/16/UE w sprawie współpracy administracyjnej w dziedzinie opodatkowania (tzw. dyrektywa DAC7). Status i rola w procesach przetwarzania danych poszczególnych podmiotów/organów (m.in. raportującej instytucji finansowej, raportującego operatora platformy), które będą brać udział w wymianie informacji, wymagają pogłębionej analizy oraz wyeliminowania propozycji niezgodnych z zasadami przetwarzania danych osobowych, które mogą negatywnie wpłynąć na standard przetwarzania danych. Organ wskazał, że użyte w projektowanych przepisach sformułowania wskazują, iż czynności związane z wymianą informacji podatkowych odbywać się mają w sposób zautomatyzowany. Konstrukcja taka jest związana szeregiem ryzyk, na które projektodawca powinien zwrócić uwagę i stworzyć w przepisach tej ustawy mechanizmy je niwelujące. Organ podkreślił, że stosowne normy powinny gwarantować właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą (warunki z art. 22 RODO).

Opiniując projekt **rozporządzenia Ministra Cyfryzacji w sprawie szczegółowych warunków uwierzytelnienia z wykorzystaniem profilu mObywatel[141],** organ podkreślił, iż w jego ocenie – biorąc pod uwagę fakt, że na mocy projektowanego rozporządzenia dopuszcza się uwierzytelnianie użytkownika aplikacji mObywatel przy użyciu danych biometrycznych, stanowiących szczególną kategorię danych osobowych w rozumieniu art. 9 ust. 1 oraz zdefiniowanych w art. 4 pkt 14 RODO – przeprowadzenie testu prywatności, w tym oceny skutków dla ochrony danych, przed skierowaniem projektowanego aktu do uzgodnień jest niezbędne. Niemniej z projektowanego rozporządzenia ani dokumentów do niego dołączonych nie wynikało, aby projektodawca dokonał takiej oceny. Prezes UODO wskazał, że dane biometryczne są danymi szczególnej kategorii i aby zobowiązywać do ich podawania i dalej móc je przetwarzać, muszą istnieć szczególne rozwiązania gwarancyjne, o których stanowi art. 9 ust. 2, 3 i 4 RODO. Organ podkreślił, że ochrona danych jest wprawdzie neutralna technologicznie, ale wykorzystywanie danych biometrycznych jest przedmiotem szczególnego zainteresowania organów UE oraz Europejskiej Rady Ochrony Danych (EROD), która wskazywała na niedopuszczalność gromadzenia danych biometrycznych w odrębnych bazach. Także orzecznictwo TSUE

[140] DOL.401.63.2023.
[141] DOL.401.262.2023.

wskazuje na liczne warunki, jakie muszą być spełnione przy pozyskiwaniu i dalszym przetwarzaniu danych tej kategorii. Nie można też pominąć faktu, że dane biometryczne będą pobierane przy pomocy prywatnych urządzeń użytkowników aplikacji mObywatel, tj. technologii niezweryfikowanej pod względem zgodności z ogólnym rozporządzeniem o ochronie danych, co stanowi istotne ryzyko dla przetwarzania tych danych przez podmiot publiczny – Ministra Cyfryzacji – jako administratora danych.

Analiza przepisów **projektu ustawy o zmianie ustawy – Prawo restrukturyzacyjne oraz niektórych innych ustaw**[142] wykazała, że projektowane rozwiązania, wdrażające przepisy unijne[143], powodują wysokie ryzyko naruszenia praw lub wolności osób i wymagają przeprowadzenia oceny skutków operacji przetwarzania dla ochrony danych osobowych. Wątpliwości organu nadzorczego wzbudziło zobowiązanie Ministra Sprawiedliwości do gromadzenia, przechowywania oraz udostępniania Komisji Europejskiej danych, na zasadach określonych w art. 29 wdrażanej dyrektywy. Organ nadzorczy w przedstawionej opinii legislacyjnej podkreślił, że przepisy krajowe powinny szczegółowo regulować kwestie związane z przetwarzaniem danych, a nie w sposób ogólny czynić odwołanie do zasad przetwarzania określonych informacji, w tym także do danych osobowych. Organ podkreślił, że jest to tym bardziej istotne, że ma dotyczyć przetwarzania danych osobowych przez organ publiczny, w wykonaniu przypisanego mu projektowanymi przepisami obowiązku prawnego (czy dla zadania realizowanego w interesie publicznym), które to działania mogą być podejmowane jedynie zgodnie z konstytucyjną zasadą praworządności oraz zasadą zgodności z prawem, rzetelności i przejrzystości, tj. w granicach i na podstawie przepisów prawa statuujących określone obowiązki i kompetencje (zadania). Organ wskazał, że projektowane przepisy wymagają uzupełnienia i wskazania, w jakim celu/celach, na jakich zasadach oraz jakie podmioty będą odpowiedzialne za prowadzenie/uzupełnianie rejestru/systemu oraz przetwarzanie danych; czy rejestr będzie nowym rejestrem, czy też dane będą gromadzone w ramach już istniejącego rozwiązania. W opinii organu konieczne jest określenie, czy powstały w ten sposób zasób informacyjny będzie spełniał warunki rejestru publicznego, a zatem, czy istnieje wymóg kształtowania wszystkich jego elementów stosownie do przepisów ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Uzasadnienie do projektu ustawy nie zawierało stosownych wyjaśnień ani oceny skutków w wyżej przedstawionym zakresie.

Podobne zastrzeżenia dotyczyły także **projektu rozporządzenia Ministra Finansów w sprawie egzaminu potwierdzającego wiedzę i niezbędne umiejętności do świadczenia doradztwa w zakresie ogólnoeuropejskiego indywidualnego produktu emerytalnego**[144]**.** Organ nadzorczy zwrócił uwagę na przewidziane w nim wykorzystanie systemu teleinformatycznego do przetwarzania danych osobowych, którego wdrożenie uzasadnia przeprowadzenie przez projektodawcę testu prywatności

[142] DOL.401.179.2023.

[143] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1023 z 20 czerwca 2019 r. w sprawie ram restrukturyzacji zapobiegawczej, umorzenia długów i zakazów prowadzenia działalności oraz w sprawie środków zwiększających skuteczność postępowań dotyczących restrukturyzacji, niewypłacalności i umorzenia długów, a także zmieniająca dyrektywę (UE) 2017/1132 (dyrektywa o restrukturyzacji i upadłości) (Dz. Urz. UE L 172 z 26.06.2019, str. 18).

[144] DOL.401.472.2023.

i uwzględnienie ochrony danych w fazie projektowania przy określaniu sposobów przetwarzania.

Opiniując **projekt rozporządzenia Ministra Finansów w sprawie korzystania z e-Urzędu Skarbowego[145],** organ zwrócił uwagę na brak w nim rozwiązań zapewniających poszanowanie zasad przetwarzania danych osobowych (w szczególności w zakresie podstawy prawnej, rzetelności oraz przejrzystości regulacji dotyczących przetwarzanych danych osobowych). Wskazał, że przepisy dotyczące funkcjonowania systemu e-Urzędu Skarbowego, ze względu na zakładaną przez projektodawcę skalę, zakres i sposoby przetwarzania danych osobowych, wymagają dogłębnej analizy pod kątem gwarancji z zakresu ochrony danych osobowych i prawa do prywatności. W nawiązaniu do tej uwagi organu projektodawca zadeklarował przeprowadzenie oceny skutków dla ochrony danych osobowych.

Na brak analizy i oceny skutków dla ochrony danych organ nadzorczy zwrócił również uwagę, opiniując **projekt rozporządzenia Ministra Infrastruktury w sprawie egzaminowania osób ubiegających się o uprawnienia do kierowania pojazdami, szkolenia, egzaminowania i uzyskiwania uprawnień przez egzaminatorów oraz wzorów dokumentów stosowanych w tych sprawach[146],** na mocy którego miałby powstać ogólnopolski państwowy rejestr danych (określany w projekcie jako system teleinformatyczny). Ani z jego przepisów, ani z dołączonych do niego dokumentów nie wynikało, czy funkcjonowanie takiego jednolitego systemu nie doprowadziłoby do gromadzenia danych osobowych w zbiorze mającym cechy rejestru publicznego, co ma znaczenie z punktu widzenia zasad towarzyszących prowadzeniu takiego rejestru. Wyjaśnienie tej okoliczności i uregulowanie zasad przetwarzania danych za pomocą tego systemu ma kluczowe znaczenie dla poszanowania przepisów o ochronie danych osobowych, zwłaszcza w kwestii odpowiedzialności za bezpieczeństwo gromadzonych danych, nadawania upoważnień dostępowych i zgłaszania naruszeń.

W odniesieniu do **projektu rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie świadectw, dyplomów państwowych i innych druków[147]** organ nadzorczy zwrócił uwagę, że wprowadzanie do porządku prawnego nowej usługi/rozwiązania technologicznego – jakim jest dokument elektroniczny odpowiadający usłudze związanej z mLegitymacją szkolną – powinno być poprzedzone testem prywatności oraz oceną skutków dla ochrony danych. Zdaniem organu pozwoliłoby to na zredagowanie przejrzystych przepisów definiujących status zarówno legitymacji szkolnej jako takiej, jak również w konsekwencji mLegitymacji szkolnej oraz na odpowiednie do celów przetwarzania ukształtowanie adekwatnych katalogów danych osobowych.

Z kolei w wyniku przeprowadzonej analizy **projektu ustawy o ochronie ludności oraz o stanie klęski żywiołowej (UD432)[148]** organ nadzorczy wskazał, że wprowadzane przepisy – jako dotyczące przetwarzania danych osobowych w systemie teleinformatycznym oraz rejestrze centralnym – determinują zasadność przeprowadzenia

[145] DOL.401.247.2023.
[146] DOL.401.443.2023.
[147] DOL.401.495.2023.
[148] DOL.401.236.2023.

testu prywatności (projektowania ochrony danych osobowych w procesie tworzenia prawa, w tym przeprowadzenia oceny skutków dla ochrony danych). Taka ocena powinna być dokonywana ze względu na rodzaj przetwarzania, zwłaszcza następujący przy użyciu nowych technologii (w tym przypadku poprzez utworzenie Krajowego Systemu Informacji o Zasobach Ochrony Ludności „SI OMNIBUS", rejestru członków formacji obrony cywilnej oraz osób przewidzianych do realizacji zadań obrony cywilnej), ponieważ charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób. Przeprowadzenie takiej analizy powinno wykazać niezbędność przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i w zakresie w projektowanych rozwiązaniach.

5.2. Hierarchia aktów prawnych – zasada praworządności

Organ nadzorczy w toku prac legislacyjnych zwracał uwagę, że projektodawca w przepisach rangi ustawy (a nie rozporządzenia wykonawczego bądź aktu wewnętrznego lub aktu o charakterze cywilno-prawnym, np. zarządzenia, porozumienia, wytyczne) powinien: 1) zawrzeć odpowiednio (wyczerpująco) skonstruowaną podstawę prawną dla określania obowiązku przetwarzania danych osobowych; 2) określić cel i zakres niezbędnych – dla osiągnięcia tego celu – danych, ich kategorie (tzw. dane zwykłe i/lub dane szczególnej kategorii); 3) określić sposoby przetwarzania danych adekwatnie do celów przetwarzania i przyporządkować wykonywanie operacji na danych osobowych ściśle określonym organom i/lub podmiotom, zgodnie z ich kompetencjami wynikającymi z powszechnie obowiązujących przepisów prawa; 4) określić okresy przetwarzania danych i ich retencję; 5) wskazać inne elementy niezbędne dla kompleksowego uregulowania przetwarzania danych dla osiągnięcia celów prawodawcy.

O przyjęcie właściwej konstrukcji podstawy prawnej przetwarzania danych osobowych organ nadzorczy postulował, opiniując **projekt rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia**[149]. Zwrócił uwagę projektodawcy na tworzone w drodze projektowanego rozporządzenia nowe w krajowym porządku prawnym rozwiązanie, przewidujące gromadzenie danych osobowych uczniów związanych z ich talentami sportowymi w systemie teleinformatycznym „Sportowe Talenty". Wskazał, że zdawkowa, a przez to blankietowa w swej treści, a ponadto wskazana w załączniku do aktu wykonawczego, regulacja co do tego, że: „Wyniki przeprowadzonych testów i wiek ucznia nauczyciel wychowania fizycznego wpisuje do systemu teleinformatycznego »Sportowe Talenty«, prowadzonego przez ministra właściwego do spraw kultury fizycznej", nie może być uznana za wystarczającą dla uregulowania powstania i funkcjonowania systemu teleinformatycznego oraz dla przetwarzania danych osobowych uczniów. Organ przypomniał, że rozwiązania – nakładające prawa i obowiązki, w tym nierozerwalnie związane z przetwarzaniem danych osobowych, na wykonawców (adresatów) norm – powinny wynikać z przepisów rangi ustawy, a nie rozporządzenia wykonawczego. Wskazał ponadto, że rozporządzenie może jedynie doprecyzowywać warunki techniczne funkcjonowania systemu teleinformatycznego, natomiast nakładanie na adresatów norm

[149] DOL.401.90.2023.

praw i obowiązków poprzez tej rangi akt prawa nie odpowiada konstytucyjnym zasadom praworządności i autonomii informacyjnej jednostki.

Kolejnym przykładem opiniowanego projektu rozporządzenia, którego materia powinna być uregulowana w ustawie, był **projekt rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie świadczeń gwarantowanych z zakresu leczenia szpitalnego[150].** Wątpliwości organu nadzorczego budziła treść zmian w załączniku 4 do projektu rozporządzenia, w którym projektodawca wśród „pozostałych wymagań" wskazał, że: „Świadczeniodawca przekazuje dane do rejestru zabiegów z zastosowaniem systemu robotowego prowadzonego przez Prezesa Narodowego Funduszu Zdrowia dostępnego za pomocą aplikacji internetowej". Organ nadzorczy zwrócił uwagę, że to w przepisach rangi ustawy należy określić, za pomocą jakiej aplikacji internetowej (projektodawca nie wskazał, czy chodzi o aplikację, o której mowa w art. 188ba ustawy z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych) oraz na jakich zasadach dane będą przekazywane do wymienionego wyżej rejestru.

Innym przykładem dokumentu podlegającego opiniowaniu był **projekt rozporządzenia Ministra Zdrowia w sprawie wymagań, jakim powinno odpowiadać medyczne laboratorium diagnostyczne oraz kwalifikacji personelu[151].** Organ nadzorczy zwrócił uwagę na nowe rozwiązanie wymagane dla laboratoriów, tj. „laboratoryjny system informatyczny", który zawiera m.in. takie funkcje, jak: „rejestracja zleceń, w tym przesłanych drogą elektroniczną", kontrola jakości, autoryzacja i odprawianie wyników badań czy generowanie wyników badań laboratoryjnych. Uzasadnione jest zatem założenie, że w treści materiałów przetwarzanych w laboratorium, w tym przez ww. system informatyczny, znajdują się zarówno dane pacjentów, w tym dane o stanie ich zdrowia, jak i dane osób obsługujących system. Organ wskazał, że prawidłowym rozwiązaniem byłoby uregulowanie podstaw prawnych oraz zasad działania systemu i sposobów przetwarzania danych osobowych w przepisach ustawy delegującej wydanie przedmiotowego rozporządzenia, bądź też odesłanie do przepisów rangi ustawy, które regulują tę problematykę, a przez to uczynienie zadość zasadzie zgodności z prawem – art. 5 ust. 1 lit. a) RODO. Zwrócił również uwagę na to, że zgodnie z konstytucyjną zasadą praworządności (art. 7 Konstytucji RP), zasadą ochrony wolności (art. 31 Konstytucji RP) oraz prawem do ochrony danych osobowych (art. 51 Konstytucji RP) nakładanie praw i obowiązków, w tym dotyczących przetwarzania danych osobowych, również z użyciem systemu informatycznego – wymaga regulacji ustawowej.

W opinii dotyczącej **projektu rozporządzenia Ministra Finansów w sprawie sprawozdań spółdzielczych kas oszczędnościowo-kredytowych oraz Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej[152]** organ wskazał projektodawcy na brak określenia w przepisach rangi ustawowej zasad funkcjonowania systemu informatycznego, za pomocą którego zgodnie z projektowanym rozporządzeniem

[150] DOL.401.350.2023.
[151] DOL.401.529.2023.
[152] DOL.401.494.2023.

przekazywane mają być dane sprawozdawcze (zawierające również dane osobowe) do Komisji Nadzoru Finansowego (KNF).

Organ nadzorczy zgłosił też wątpliwości w zakresie rejestru postępowań dyscyplinarnych, przewidzianego w **projektowanym rozporządzeniu Ministra Sprawiedliwości w sprawie obiegu dokumentów związanych z postępowaniem dyscyplinarnym funkcjonariuszy Służby Więziennej[153],** wskazując, że podstawy jego funkcjonowania powinny być uregulowane w akcie rangi ustawowej, a nie w rozporządzeniu wykonawczym.

Podobną uwagę organ zgłosił, oceniając **projekt ustawy o czasie pracy maszynistów[154].** Postulował, by z art. 25y ust. 6 pkt 1 ustawy z 28 marca 2003 r. o transporcie kolejowym usunięta została delegacja do wydania rozporządzenia regulującego kwestie wprowadzania, zmiany, udostępniania usuwania danych zgromadzonych w krajowym rejestrze maszynistów i prowadzących pojazdy kolejowe, a przepisy w tym zakresie zostały włączone do ustawy o transporcie kolejowym. Zwrócił uwagę, że tak istotne regulacje odnoszące się do tworzenia i funkcjonowania nowej bazy danych powinny być zawarte w ustawie, a nie akcie wykonawczym.

Z kolei w opinii do przedstawionego przez **Prezydenta Rzeczypospolitej Polskiej projektu ustawy o szczególnej opiece geriatrycznej[155]** organ nadzorczy zwrócił uwagę na kwestie dotyczące zawierania regulacji związanych z przetwarzaniem danych osobowych w aktach pozaustawowych (porozumieniach). W analizowanym projekcie przewidywano bowiem, że: „Do zadań powiatu z zakresu szczególnej opieki geriatrycznej należy zawieranie porozumień" oraz że jeden powiat może zawrzeć z powiatem sąsiednim, położonym na terenie tego samego województwa, porozumienie o przekazaniu powiatowi sąsiedniemu realizacji zadania utworzenia centrum. Z proponowanych przepisów nie wynikało, czy porozumienie będzie dotyczyło także przetwarzania danych osobowych. Organ wskazał, że jeśli takie są plany prawodawcy, to wyjaśnić trzeba, że nie jest to rozwiązanie prawidłowe i pożądane, gdyż przetwarzanie danych powinno być uregulowane w akcie prawa rangi ustawy. Dodatkowo podniósł, że wszelkie kluczowe rozwiązania dotyczące przetwarzania danych osobowych dla realizacji zadań publicznych powinny być określone w przepisach prawa, a nie w aktach pozaustawowych, np. porozumieniach nieposiadających mocy konstytucyjnego źródła prawa.

Organ nadzorczy zgłosił też uwagi do **projektu rozporządzenia Ministra Zdrowia w sprawie nadania statutu Krajowej Radzie Onkologicznej[156].** Dotyczyły one trybu zdalnego obradowania Krajowej Rady Onkologicznej za pośrednictwem systemów teleinformatycznych. W ocenie organu projektowana regulacja nie odpowiada wymogom art. 6 ust. 3 i art. 5 RODO w zakresie przetwarzania danych osobowych w „systemie teleinformatycznym", a projektowane przepisy nie wskazują w sposób jednoznaczny i przejrzysty, czym są te systemy teleinformatyczne, przez co w konsekwencji nie wiadomo, jakim procesom przetwarzania poddane będą dane osobowe. Organ zaznaczył, że zakres danych przetwarzanych dla wykonywania projektowanej regulacji powinien

[153] DOL.401.49.2023.
[154] DOL.401.93.2023.
[155] DOL.401.319.2023.
[156] DOL.401.195.2023.

zostać określony w przepisach rangi ustawy, tak by zapewnione zostało stosowanie zasad określonych wskazanych w RODO, w szczególności zasady zgodności z prawem, rzetelności i przejrzystości oraz zasady integralności i poufności, a przede wszystkim rozliczalności.

W opinii legislacyjnej do **projektu rozporządzenia Ministra Infrastruktury w sprawie egzaminowania osób ubiegających się o uprawnienia do kierowania pojazdami, szkolenia, egzaminowania i uzyskiwania uprawnień przez egzaminatorów oraz wzorów dokumentów stosowanych w tych sprawach**[157] organ nadzorczy wskazał, że przeniesienie do aktu o randze rozporządzenia materii, która powinna być regulowana wyłącznie w drodze ustawy, narusza prawidłową konstrukcję podstawy prawnej przetwarzania danych osobowych. Projektowany nowy, ogólnopolski rejestr publiczny (w projekcie nazywany „systemem teleinformatycznym") nie miał żadnego umocowania w przepisach ustawowych, z których to powinny wynikać rozwiązania nakładające prawa i obowiązki na wykonawców (adresatów) norm.

W stanowisku odnoszącym się do **projektu rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie świadectw, dyplomów państwowych i innych druków**[158] organ nadzorczy podkreślił, iż zarówno zakres pozyskiwanych danych, jak i korzystanie z rejestrów powiązanych z aplikacją mObywatel nie mogą być regulowane aktem rangi rozporządzenia wykonawczego przy braku stosownej regulacji ustawowej. Prawodawca powinien określić na poziomie ustawy status dokumentu legitymacji szkolnej, jak również dokumentu elektronicznego, odpowiadający usłudze związanej z mLegitymacją szkolną. Rozwiązanie takie stanowiłoby właściwą podstawę prawną dla przetwarzania danych osobowych w treści legitymacji szkolnej, niezależnie od jej rodzaju czy formy.

Opiniując **projekt ustawy o ochronie ludności oraz o stanie klęski żywiołowej (UD432)**[159]**,** organ nadzorczy zwrócił uwagę na to, że rodzaje niezbędnych ograniczeń wolności i praw człowieka i obywatela wymagają uregulowania w akcie prawa powszechnie obowiązującego rangi ustawy, a nie – jak to przewiduje projektowana ustawa – w rozporządzeniu wykonawczym. Ustawa zasadnicza, tj. Konstytucja RP, w szczególności w odniesieniu do stanów nadzwyczajnych, kształtuje zakres podmiotowy i przedmiotowy ewentualnych ograniczeń praw i wolności. Stan klęski żywiołowej został uregulowany w przepisach poświęconych stanom nadzwyczajnym, w tym w art. 228 Konstytucji RP – tym regułom odpowiadać powinien zakres projektowanej ustawy, co zostało podkreślone w opinii organu.

Zasadnicze wątpliwości organu nadzorczego wzbudziły zmiany przepisów dotyczących informatyzacji sądów powszechnych, proponowane w **projekcie ustawy o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw**[160]**.** Zważywszy na to, iż w systemach teleinformatycznych wspierających działalność sądów powszechnych znajdują się dane osobowe szczególnych kategorii lub

[157] DOL.401.443.2023.
[158] DOL.401.495.2023.
[159] DOL.401.236.2023.
[160] DOL.401.150.2023.

o szczególnym charakterze (art. 9 ust. 1 i art. 10 RODO), to zagadnienie (ewentualnej) współpracy Ministra Sprawiedliwości z innymi, pozasądowymi podmiotami w procesie informatyzacji sądów powszechnych powinno, jako nakładające prawa i obowiązki, być uregulowane w przepisach ustawy, nie zaś w porozumieniach zawieranych przez tego ministra. Z przepisów ustawy, a nie porozumienia (umowy), ma jednoznacznie wynikać rola poszczególnych podmiotów w procesie przetwarzania danych osobowych w związku z informatyzacją sądów powszechnych.

Również w opinii do **projektu rozporządzenia Rady Ministrów w sprawie zakresu danych i wykazu rejestrów publicznych oraz systemów teleinformatycznych podmiotów publicznych, z których użytkownik aplikacji mObywatel może pobrać dane[161],** zwrócono uwagę, że zarówno zakres danych, jak i wykaz rejestrów powiązanych z aplikacją mObywatel nie mogą być ustalane aktem wykonawczym, dodatkowo fakultatywnie wydanym przez Radę Ministrów. Jako postulat *de lege ferenda* organ nadzorczy wskazał na konieczność przeniesienia materii regulowanej rozporządzeniem do ustawy.

5.3. Precyzyjne określenie ról podmiotów w procesie przetwarzania danych

Kolejnym istotnym wyzwaniem, pojawiającym się przy opiniowaniu projektów aktów prawnych, było prawidłowe określenie ról podmiotów w procesach przetwarzania danych, zwłaszcza w sytuacjach, gdy procesy przetwarzania były złożone, uczestniczyło w nich wiele podmiotów wyposażonych w różne uprawnienia, realizujących odmienne cele przetwarzania danych i w różny sposób przetwarzających dane. Analiza projektów aktów prawnych wskazuje, że projektodawcy nie określali ról podmiotów/organów biorących udział w procesach przetwarzania danych. Organ nadzorczy niejednokrotnie zwracał uwagę na konieczność kształtowania przepisów odpowiadających rzeczywistym potrzebom i celom tworzonych regulacji prawnych, odwołując się wprost do interpretacji przyjętej 7 lipca 2021 r. przez Europejską Radę Ochrony Danych w Wytycznych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego. Wskazywał zwłaszcza, że na gruncie ogólnego rozporządzenia o ochronie danych pojęcie administratora (rozumianego jako podmiot, który samodzielnie bądź z innymi decyduje o celach i sposobach przetwarzania, czy też powierza przetwarzanie) 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. Skomplikowane procesy przetwarzania danych mogą też wymagać tworzenia regulacji dotyczących działań na danych osobowych prowadzonych przez więcej niż jeden podmiot, podmiotów realizujących różne cele przetwarzania na tych samych danych, jak np. zabezpieczenie procesów przetwarzania danych nierozerwalnie związane z zasilaniem zasobów danymi oraz udostępnianiem danych. Takie sytuacje wymagają, aby przepisy prawa odpowiednio regulowały rolę odrębnych administratorów czy administratorów współadministrujących danymi.

[161] DOL.401.263.2023.

Opiniując **projekt rozporządzenia Ministra Infrastruktury w sprawie egzaminowania osób ubiegających się o uprawnienia do kierowania pojazdami, szkolenia, egzaminowania i uzyskiwania uprawnień przez egzaminatorów oraz wzorów dokumentów stosowanych w tych sprawach[162],** organ zakwestionował definicję administratora niezgodną z definicją administratora zawartą w art. 4 pkt 7 RODO. Za administratora uznano bowiem: „osobę zatrudnioną w ośrodku egzaminowania, która prowadzi obsługę systemu teleinformatycznego ośrodka egzaminowania". Tymczasem, w rozumieniu przepisów RODO, rolę tę pełni na gruncie obowiązujących przepisów wojewódzki ośrodek ruchu drogowego reprezentowany przez dyrektora, jako podmiot, który ustala cele i sposoby przetwarzania danych osobowych. Projektodawca nie doprecyzował, o jakiego administratora chodzi, a tym samym, jaki będzie jego status z punktu widzenia odpowiedzialności za realizację przepisów o ochronie danych osobowych. Organ wskazał zatem na konieczność określenia – w akcie rangi ustawy – ról i obowiązków odpowiednio do celów przetwarzania podmiotów przetwarzających, w tym pozyskujących dane osobowe z wykorzystywanego dla realizacji przedmiotowych przepisów systemu teleinformatycznego oraz wprowadzających dane osobowe do systemu, a także podmiotu odpowiedzialnego za prowadzenie tego systemu.

Wątpliwości organu wzbudził też **rządowy projekt ustawy o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw[163],** zgodnie z którym Szef Służby Cywilnej jest administratorem systemu teleinformatycznego i zapewnia jego funkcjonowanie, w tym dostępność systemu teleinformatycznego dla podmiotów przetwarzających dane w tym systemie. Projektowany akt przewidywał, że określone czynności w tym systemie, np. zamieszczanie ogłoszeń o naborach w służbie cywilnej, będą wykonywać jego użytkownicy (w imieniu podmiotów publicznych zatrudniających członków korpusu służby cywilnej) uwierzytelnieni w tym systemie. W związku z tym powstało pytanie, czy dodatkowo inne podmioty będą uczestniczyły w procesach przetwarzania danych w tym systemie, mając np. możliwość uwierzytelniania w nim użytkowników, a co za tym idzie, jaki będzie status tych podmiotów i granice ich odpowiedzialności za przetwarzanie danych (np. za ich: aktualizację, usuwanie, retencję, realizację praw podmiotów danych itd.), na co wskazał organ w przedstawionym stanowisku.

Także opiniując **projekt rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie programu pilotażowego „Profilaktyka 40 PLUS"[164],** organ nadzorczy zwrócił uwagę na wątpliwość dotyczącą identyfikacji podmiotu, który będzie pełnił rolę administratora danych przetwarzanych w centralnej rejestracji danych osobowych – jako „funkcjonalności Systemu P1". Funkcjonalność ta umożliwia dokonanie przez świadczeniobiorcę centralnego zgłoszenia i przydzielenie mu terminu udzielenia świadczenia u wybranego realizatora programu pilotażowego, zmiany lub rezygnacji w zakresie dokonanego centralnego zgłoszenia lub terminu udzielenia świadczenia i przypisania mu praw i obowiązków co do wykonywania operacji na danych osobowych.

[162] DOL.401.443.2023.
[163] DOL.401.134.2023.
[164] DOL.401.227.2023.

Z kolei nowelizacją **ustawy z 14 kwietnia 2023 r. o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw**[165] projektodawca zamierzał m.in. wprowadzić system teleinformatyczny umożliwiający: zamieszczanie ogłoszeń o naborze oraz o wyniku naboru, składanie wymaganych dokumentów, po zastosowaniu zapewnionych w systemie teleinformatycznym sposobów potwierdzenia pochodzenia, dokumentowanie przebiegu naboru, w tym oceny kandydatów oraz założenie profilu użytkownika systemu teleinformatycznego. W opinii organu brak zdefiniowania w projekcie pojęcia „użytkownika sytemu" powoduje, że nie wiadomo, na jakie inne osoby – oprócz Szefa Służby Cywilnej (jako administratora zapewniającego funkcjonowanie systemu) i użytkowników dokonujących określonych czynności (w imieniu podmiotów publicznych zatrudniających członków korpusu służby cywilnej) uwierzytelnionych w tym systemie – nakładane będą obowiązki związane z przetwarzaniem danych osobowych. Powstaje więc pytanie, czy dodatkowo inne podmioty będą uczestniczyły w procesach przetwarzania danych w tym systemie, mając np. możliwość uwierzytelniania w nim użytkowników, a co za tym idzie, jaki będzie status tych podmiotów i granice ich odpowiedzialności za przetwarzanie danych (np. za aktualizację, usuwanie, retencję danych oraz za realizację praw podmiotów danych itd.).

Wątpliwości organu co do **projektu rozporządzenia Ministra Zdrowia w sprawie programu pilotażowego w zakresie kompleksowej opieki nad pacjentem z wczesnym zapaleniem stawów**[166] dotyczyły regulacji związanych z podmiotem, który pełnić miał rolę administratora w odniesieniu do danych przetwarzanych w Bazie Zapalnych Chorób Reumatycznych i przypisania mu w tworzonych przepisach praw i obowiązków odnoszących się do wykonywania operacji na danych osobowych. W opinii organu nazwanie podmiotu „administratorem" nie zawsze jest konieczne. Najistotniejsze jest bowiem rzeczywiste, a nie deklarowane wykonywanie operacji przetwarzania danych i wykonywanie ról (m.in. administratora) w tych procesach. Ten aspekt wskazano jako niejednokrotnie powoływany przez Europejską Radę Ochrony Danych (EROD) w wytycznych dotyczących szeregu różnych procesów przetwarzania danych. W Wytycznych 07/2020 dotyczących pojęć administratora i podmiotu przetwarzającego, zawartych w RODO, przyjętych 7 lipca 2021 r. EROD wskazała, że: „Pojęcia administratora, współadministratora i podmiotu przetwarzającego są pojęciami funkcjonalnymi w tym sensie, że ich celem jest podział obowiązków zgodnie z rzeczywistymi rolami stron oraz pojęciami autonomicznymi w tym sensie, że powinno się je interpretować głównie zgodnie z prawem Unii o ochronie danych".

Natomiast przy opiniowaniu **projektu ustawy o krwiodawstwie i krwiolecznictwie**[167] wątpliwości organu budziły regulacje wskazujące, że zarówno minister właściwy do spraw zdrowia, jak i podmioty, o których mowa w art. 4 pkt 1–3 projektu ustawy (tj. jednostki organizacyjne publicznej służby krwi, Instytut Hematologii i Transfuzjologii, Narodowe Centrum Krwi), są współadministratorami danych osobowych przetwarzanych w Systemie e-krew, a wzajemne prawa i obowiązki współadministratorów określa porozumienie. Powstała wówczas wątpliwość dotycząca podziału praw

[165] DOL.401.134.2023.
[166] DOL.401.102.2023.
[167] DOL.401.108.2023.

i obowiązków pomiędzy ww. podmiotami w zakresie wykonywania operacji na danych osobowych. Biorąc pod uwagę to, że projektowane przepisy będą zawarte w akcie prawnym rangi ustawy, organ zaznaczył, że w celu zapewnienia bezpieczeństwa przetwarzanych danych pożądane byłoby doprecyzowanie powyższej kwestii w ustawie, a nie w porozumieniu, zarówno ze względu na zasadę praworządności, jak i w celu zminimalizowania wątpliwości interpretacyjnych, które mogą wystąpić przy pozostawieniu proponowanej treści przepisu. Wskazał również, że projektodawca powinien uregulować podział obowiązków między współadministratorami tak w sferze wewnętrznej – pomiędzy nimi, jak i w kontekście zewnętrznym – w relacji do osoby, której dane dotyczą. Współadministrowanie wymaga ustalenia określonych zasad realizacji praw osób, których dane dotyczą, a także odpowiedniego podziału obowiązków i odpowiedzialności między współadministratorami.

5.4. Systemy teleinformatyczne. Łączenie baz danych

Łączenie baz danych, a konkretnie łączenie danych zawartych w zbiorach czy rejestrach, to od wielu lat istotne zagadnienie będące przedmiotem szczególnego zainteresowania UODO. Organ nadzorczy w swoich opiniach legislacyjnych wielokrotnie podkreślał, że w tym kontekście istotne jest poszanowanie motywu 31 RODO i nieprzyjmowanie w treści przepisów prawa podstaw prawnych dla łączenia zbiorów danych. Zgodnie z powołanym motywem organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takim jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), 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, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

Istotnym przykładem odnoszącym się do powyższej materii był **projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji[168],** zakładający zmianę kilkudziesięciu ustaw w deklarowanym przez projektodawcę celu – wprowadzenia podstaw prawnych dla funkcjonowania rozwiązań usprawniających oraz rozwijających funkcjonowanie e-administracji. W istocie jednak projekt wprowadzał szereg rozwiązań związanych m.in. z tworzeniem oraz łączeniem rejestrów publicznych generujących istotne ryzyka i znaczną ingerencję w rozwiązania przeznaczone ochronie danych osobowych. Projektowane i zakwestionowane przez organ zmiany odnosiły się do rozwiązań dotyczących: Zintegrowanej Platformy Analitycznej (ZPA) w nowelizacji **ustawy z 20 lipca 2018 r. o Polskim Instytucie Ekonomicznym,** regulacji w zakresie funkcjonowania i udostępniania danych z systemu „EZD RP" oraz uprawnień ministra właściwego do spraw informatyzacji do udostępniania usług online oraz zbiorczych usług online przy wykorzystaniu systemów teleinformatycznych ministra oraz publicznej aplikacji mobilnej,

[168] DOL.401.169.2022.

w celu wykonywania zadań publicznych zarówno przez ministra, jak i przez inne podmioty publiczne, w nowelizowanej **ustawie z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne**. Zastrzeżenia organu wzbudziła również próba przekształcenia systemu teleinformatycznego udostępnionego przez Centrum e-Zdrowia, zwanego dotychczas „Ewidencją Wjazdów do Polski (EWP)", z posiadającego status systemu epizodycznego w system utrzymywany w sposób ciągły mocą nowelizacji **ustawy z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.** Również rozwiązanie mające na celu zapewnienie podmiotom publicznym oraz podmiotom realizującym zadania publiczne możliwości dostępu do informacji z Krajowego Rejestru Sądowego za pośrednictwem usług sieciowych, w szczególności poprzez interfejsy API, na podstawie decyzji Ministra Sprawiedliwości – przewidywane w nowelizacji **ustawy z 20 sierpnia 1997 r. – o Krajowym Rejestrze Sądowym** – wzbudziło wątpliwości organu. Projektowane zmiany w nowelizacji **ustawy z 29 sierpnia 1997 r. – Ordynacja podatkowa** przyznawały ministrowi właściwemu do spraw informatyzacji – w zakresie niezbędnym do udostępniania przez tego ministra usług online oraz zbiorczych usług online zgodnie z art. 19aa ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne – dostęp do danych z Centralnego Rejestru Danych Podatkowych. Z kolei projektowane przepisy w nowelizowanej **ustawie z 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym** nakładały na firmy audytorskie obowiązek przekazywania akt z prowadzonych postępowań celem ich gromadzenia oraz utrwalania przez Polską Agencję Nadzoru Audytowego.

Przykładowo wymienione próby nowelizacji poszczególnych ustaw, w ramach **projektu ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji,** pokazują skalę tworzenia, zmian zakresu, funkcjonalności oraz łączenia rejestrów publicznych i systemów teleinformatycznych. Opisywany projekt nie wszedł w życie, co należy ocenić pozytywnie – ze względu na jego istotne zagrożenia dla prywatności osób fizycznych.

W opinii dotyczącej **projektu ustawy o krwiodawstwie i krwiolecznictwie**[169] organ nadzorczy zalecił doprecyzowanie projektowanych przepisów, przewidujących wymianę danych między Systemem e-krew a systemami teleinformatycznymi podmiotów leczniczych oraz rejestrem przypadków zakażeń i zachorowań na chorobę zakaźną drogą elektroniczną, biorąc pod uwagę kwestie bezpieczeństwa zarówno danych, jak i samych systemów.

Prezentowane zagadnienie było również przedmiotem opinii w związku z **projektem ustawy o zmianie ustawy o odnawialnych źródłach energii oraz niektórych innych ustaw**[170]**,** w której organ zakwestionował brak regulacji dotyczących funkcjonowania „systemu teleinformatycznego udostępnianego przez Dyrektora Generalnego KOWR" oraz zapewnienia bezpieczeństwa przetwarzanych w nim danych osobowych (zawartych w składanych wnioskach o wpis do rejestru wytwórców biogazu rolniczego).

Kwestia korzystania z rejestrów publicznych były przedmiotem uwag organu nadzorczego w opinii dotyczącej **projektu ustawy o kolejnym dodatkowym rocznym**

[169] DOL.401.108.2023.
[170] DOL.401.119.2023.

świadczeniu pieniężnym dla emerytów i rencistów[171]. Projektowane rozwiązania nie precyzowały, jaki konkretnie system będzie wykorzystywany – czy będzie to wyłącznie system teleinformatyczny czy rejestr publiczny w rozumieniu przepisów ustawy z 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne, co uniemożliwiłoby organowi nadzorczemu ocenę tego istotnego aspektu związanego z przetwarzaniem danych osobowych na potrzeby kolejnego dodatkowego rocznego świadczenia pieniężnego.

Analizując z kolei **projekt ustawy o ochronie ludności oraz o stanie klęski żywiołowej (UD432)**[172]**,** organ nadzorczy zwrócił uwagę na braki regulacji w postaci niedookreślenia, czy system „SI OMNIBUS" – jako „narzędzie stanowiące jednolity system teleinformatyczny, pozwalające na sprawne zarządzanie, a także bieżące weryfikowanie dostępnego personelu, stanu sił i środków posiadanych na wszystkich poziomach administracji od centralnych organów ochrony ludności począwszy, a na gminach skończywszy" – będzie rejestrem centralnym i czy w systemie będą przetwarzane dane osobowe, co wymagałoby rozbudowania projektowanej regulacji o rozwiązania gwarantujące prawidłowość, integralność i poufność przetwarzanych w systemie danych osobowych.

Opiniując projekt **rozporządzenia Ministra Finansów w sprawie informacji dotyczącej wypłaty transferowej z subkonta OIPE**[173]**,** organ nadzorczy zwrócił uwagę na brak odniesienia do systemu teleinformatycznego w ustawie z 7 lipca 2023 r. o ogólnoeuropejskim indywidualnym produkcie emerytalnym, a także na brak definicji tego pojęcia w samym projekcie rozporządzenia. Organ wskazał, że zaproponowane przez projektodawcę rozwiązanie należy ocenić jako blankietowe i budzące wątpliwości co do sposobu przetwarzania danych w przedmiotowym systemie teleinformatycznym, w kontekście praw i obowiązków osób fizycznych, których dane osobowe mają być przetwarzane. Przepisy nie precyzowały, jaki konkretnie system będzie wykorzystywany – czy będzie to wyłącznie system teleinformatyczny administratora, czy system teleinformatyczny w rozumieniu przepisów ustawy z 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne, jako obowiązujący wszystkich administratorów, stworzony przez właściwego ministra. Projektowane rozporządzenie nie wskazywało, przez kogo i na jakich zasadach będą przetwarzane dane osobowe z użyciem ww. systemu.

Na niedoprecyzowanie przepisów dotyczących pozyskiwania przez Prezesa Głównego Urzędu Statystycznego danych osobowych z systemów teleinformatycznych prowadzonych przez inne podmioty, organ nadzorczy wskazał w opinii do **projektu ustawy o zmianie ustawy o statystyce publicznej**[174]**.** W pierwszej kolejności projekt ten przewiduje korzystanie przez Prezesa Głównego Urzędu Statystycznego z danych zawartych w rejestrze PESEL i nie precyzuje, na czym to „korzystanie" ma polegać, jak i z wykorzystaniem jakich środków oraz metod ma się ono odbywać, co budzi

[171] DOL.401.226.2023.
[172] DOL.401.236.2023.
[173] DOL.401.447.2023.
[174] DOL.401.7.2023.

wątpliwości w świetle regulacji ustawy z 24 września 2010 r. o ewidencji ludności[175] normujących udostępnianie danych z tego rejestru. Oprócz niejednoznaczności samego sformułowania „korzystanie” (z danych zawartych w rejestrze PESEL) projekt pozostawia niejasnym również cel, dla realizacji którego Prezes Głównego Urzędu Statystycznego miałby pozyskiwać dane osobowe z rejestru PESEL. Podobnie nieprecyzyjny przepis projektu dotyczy „informowania” Prezesa Głównego Urzędu Statystycznego przez organ prowadzący ewidencję lub rejestr urzędowy – o stwierdzonych niezgodnościach w zakresie danych i informacji zawartych w rejestrze REGON z danymi oraz informacjami wynikającymi z jego ewidencji lub rejestru, nie określając jednocześnie, w jaki sposób i z wykorzystaniem jakich metod oraz środków przedmiotowe „informowanie” ma się odbywać. W projekcie brak było jasnych przepisów dotyczących udostępniania komornikom sądowym danych z rejestru REGON za pomocą, niesprecyzowanych w projekcie, usług sieciowych, jak również „w inny uzgodniony sposób”, i to w sytuacji, gdy zagadnienie zapewnienia odpowiedniego poziomu ochrony danych osobowych w procesie ich udostępniania komornikom sądowym było przedmiotem zainteresowania sądów administracyjnych[176].

5.5. Korzystanie z nowych technologii przy przetwarzaniu danych osobowych

Potrzeba stanowienia przepisów prawa regulujących wykorzystywanie nowych technologii w procesie przetwarzania danych, istotnie zaangażowała organ nadzorczy w procesy legislacyjne – zarówno na poziomie regulacji krajowych, jak i unijnych. Organ w kierowanych opiniach legislacyjnych odnosił się do licznych kwestii związanych z bezpieczeństwem przetwarzania danych za pomocą nowoczesnych technologii w rozbudowanych technicznie i organizacyjnie systemach.

Opiniując **projekt ustawy o zmianie ustawy – Prawo o notariacie oraz niektórych innych ustaw[177],** organ odniósł się do przepisów dotyczących automatycznej weryfikacji notariuszy, zastępców notarialnych, a także notariuszy emerytowanych, jeżeli zostali wyznaczeni do zastępstwa notariuszy za pośrednictwem systemu teleinformatycznego prowadzonego przez Krajową Radę Notarialną. Organ zwrócił uwagę, że projektowane przepisy, zakładające przetwarzanie danych osobowych przez sądy prowadzące księgi wieczyste oraz przez Szefa Krajowej Administracji Skarbowej na potrzeby „automatycznej weryfikacji” notariuszy, wymagają uszczegółowienia, tak aby kompleksowo regulowały planowany mechanizm oraz prawa i obowiązki związane z przetwarzaniem danych osobowych.

Dokonując oceny **projektu ustawy o zmianie ustawy o wymianie informacji podatkowych z innymi państwami oraz niektórych innych ustaw (Ustawa DAC7)[178],** organ zwrócił uwagę na zawarte w nim sformułowania wskazujące, że czynności związane z wymianą informacji podatkowych będą odbywać się w sposób zautomatyzowany.

[175] Dz. U. z 2022 r., poz. 1191 ze zm.
[176] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 19 lipca 2018 r. o sygn. akt II SAB/Wa 2168/17 i wyrok Naczelnego Sądu Administracyjnego z 3 grudnia 2021 r. o sygn. akt III OSK 590/21 oddalający skargę kasacyjną.
[177] DOL.401.20.2023.
[178] DOL.401.63.2023.

Tymczasem konstrukcja taka jest związana szeregiem ryzyk, na które projektodawca powinien zwrócić uwagę i stworzyć w przepisach mechanizmy je niwelujące.

Z kolei przedstawiając stanowisko do **projektu ustawy o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli[179],** organ pozytywnie ocenił deklarację projektodawcy stosowania w systemie teleinformatycznym zapewniającym obsługę bonu na zakup laptopa przez nauczycieli, którego prowadzenie zostało przypisane ministrowi właściwemu do spraw informatyzacji, określonych w art. 32 RODO środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych. Zauważył jednak, że to administrator, a nie system, zapewnia bezpieczeństwo przetwarzanych danych osobowych, w tym stosowanie środków określonych w art. 32 RODO. Zgodnie z przepisami RODO prawa i obowiązki związane z przetwarzaniem danych osobowych muszą być przypisane podmiotowi, a nie narzędziu służącemu do przetwarzania danych. W konsekwencji odpowiedzialność za przetwarzanie danych osobowych także musi być przypisana podmiotowi, w wykonaniu zasad legalizmu i przejrzystości – art. 5 ust. 1 lit. a) RODO. Wskazał więc, że w związku z tym projektowane przepisy wymagają zmiany.

Oceniając **projekt rozporządzenia Ministra Cyfryzacji w sprawie spisu wyborców[180],** organ nadzorczy zwrócił uwagę na konieczność rozbudowy przepisów w zakresie sposobu i trybu sporządzania spisu wyborców oraz jego aktualizacji tak, aby dodatkowo ograniczyć dostęp do zawartych w nim danych osobowych osobom nieuprawnionym.

W związku z opiniowaniem **ustawy z 13 lipca 2023 r. o zmianie ustawy o ochronie zabytków i opiece nad zabytkami[181]** organ nadzorczy wskazał, że projektodawca zdecydował się na aplikację mobilną jako jedyną formę zgłoszenia poszukiwań (ukrytych lub porzuconych zabytków ruchomych przy użyciu urządzeń elektronicznych i technicznych), wykluczając papierową formę zgłoszenia oraz dopuszczając użycie w tym celu elektronicznej platformy usług administracji publicznej ePUAP jedynie jako rozwiązania tymczasowego. Podkreślił, że wprowadzanie nowych obowiązków dotyczących obywateli i przetwarzania ich danych osobowych w oparciu o narzędzia informatyczne, których funkcjonalność, nawet na poziomie ogólnym, jest nieuregulowana, nie odpowiada zasadom określonym w ogólnym rozporządzeniu o ochronie danych. O ile można przyjąć, że w imię elektronizacji procesu zgłaszania poszukiwań projektodawca nie wprowadza papierowej formy zgłaszania wniosku, o tyle niezrozumiałe jest, zdaniem organu, niedopuszczenie zgłoszeń za pomocą elektronicznej platformy usług administracji publicznej ePUAP, mającej wyraźne umocowanie w ustawie z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i nie wymaga korzystania z urządzeń mobilnych typu smartfon, mogących generować szereg zagrożeń dla prywatności użytkowników.

W omawianym kontekście należy wskazać także na budzący wątpliwości organu **projekt rozporządzenia Ministra Finansów w sprawie egzaminu potwierdzającego**

[179] DOL.401.229.2023.
[180] DOL.401.300.2023.
[181] DOL.401.308.2023.

wiedzę i niezbędne umiejętności do świadczenia doradztwa w zakresie ogólnoeuropejskiego indywidualnego produktu emerytalnego[182], zgodnie z którym system teleinformatyczny umożliwia „automatyczne wygenerowanie wyniku egzaminu ze wskazaniem liczby prawidłowych i nieprawidłowych odpowiedzi oraz braku odpowiedzi". Wskazane rozwiązanie sugeruje, że może dochodzić do zautomatyzowanego przetwarzania wyników egzaminu, a więc danych osobowych osoby zdającej egzamin oraz oceny wyniku egzaminu (pozytywnego lub negatywnego) decyzją systemu. Tymczasem osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływa. Projektowane rozwiązanie wymaga wyjaśnienia i ewentualnego dostosowania do wymogów stawianych zautomatyzowanemu przetwarzaniu, wyrażonych w art. 22 RODO, w szczególności w zakresie właściwych, czyli dostosowanych do *ratio legis* przeprowadzania egzaminu, środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby egzaminowanej (podmiotu danych).

Natomiast, dokonując analizy **projektu ustawy o ochronie ludności oraz o stanie klęski żywiołowej (UD432)[183],** organ wskazał na brak jasności co do tego, czy realizacja projektowanych rozwiązań wiązać się będzie z automatycznym przetwarzaniem danych osobowych w systemie/rejestrze, w tym z profilowaniem – w ramach „zautomatyzowanego systemu wymiany informacji" dotyczącego Krajowego Systemu Informatycznego o Zasobach Ochrony Ludności „SI OMNIBUS".

Z kolei w opinii do **projektowanego rozporządzenia Ministra Finansów zmieniającego rozporządzenie w sprawie Rejestru Należności Publicznoprawnych[184],** regulującego zautomatyzowany tryb pozyskiwania danych z Rejestru Należności Publicznoprawnych (RNP) przez podmioty uprawnione, organ nadzorczy wskazał potrzebę wyjaśnienia i wskazania w przepisach, jakie środki będą przyjęte przez projektodawcę dla realizacji zasady rozliczalności (art. 5 ust. 2 RODO). W jego ocenie projektowane rozporządzenie powinno precyzować, w jaki sposób administrator RNP będzie odnotowywał pobranie informacji o zobowiązanym przez poszczególne uprawnione podmioty i czy będzie ono wiązało się podejmowaniem zautomatyzowanych decyzji o osobie. Jest to istotne ze względu na przepis art. 22 oraz motywu 71 RODO, z których wynika prawo osoby, której dane dotyczą, do niepodlegania decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Z tego uprawnienia pośrednio wynika zakaz podejmowania decyzji wyłącznie na podstawie zautomatyzowanego przetwarzania i profilowania.

5.6. Zakres pozyskiwanych danych osobowych

Artykuł 5 RODO określa zasady dotyczące przetwarzania danych osobowych, których przestrzeganie w kontekście tworzonych lub nowelizowanych regulacji organ nadzorczy rekomenduje w formułowanych opiniach legislacyjnych. Prawidłowy zakres

[182] DOL.401.472.2023.
[183] DOL.401.236.2023.
[184] DOL.401.278.2023.

pozyskiwanych danych osobowych wyznaczają zasady: ograniczenia celu – art. 5 ust. 1 lit. b) RODO oraz minimalizacji danych – art. 5 ust. 1 lit. c) RODO.

Organ nadzorczy, opiniując **projekt rozporządzenia Ministra Cyfryzacji w sprawie katalogu danych gromadzonych w centralnej ewidencji pojazdów[185],** zwrócił uwagę, że sposób sformułowania zakresu danych gromadzonych w ewidencji pojazdów (tj. m.in. „dane osoby wskazanej w dokumencie jako właściciel, posiadacz lub użytkownik") w projektowanym rozporządzeniu stwarza ryzyko przekroczenia zakresu danych wyznaczonego mocą ustawy delegującej jego wydanie. Zdaniem organu uzasadnione jest precyzyjne określenie zakresu/katalogu danych gromadzonych w ewidencji. Zapewni to również wyznaczenie podstaw i granic prawa dla wykonawców norm w toku stosowania prawa, eliminując ryzyko powstania istotnych wątpliwości interpretacyjnych.

Na nadmiarowy zakres danych osobowych organ nadzorczy zwrócił uwagę, opiniując **projekt rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia[186].** Organ podkreślił, że informacje w postaci wyników testów i wieku ucznia, które mają być gromadzone w systemie teleinformatycznym „Sportowe Talenty", stanowią dane osobowe i przywołał interpretację zawartą w wyroku TSUE z 20.12.2017 r., C-434/16, w sprawie *Peter Nowak v. Data Protection Commissioner*[187]. Trybunał uznał w nim, że: „art. 2 lit. a) dyrektywy 95/46 należy interpretować w ten sposób, że w okolicznościach, takich jak te rozpatrywane w postępowaniu głównym, pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi, stanowią dane osobowe w rozumieniu tego przepisu". Za wyrokiem TSUE, polski organ nadzorczy podkreślił, że: „(…) ochrona podstawowego prawa do poszanowania życia prywatnego wiąże się między innymi z tym, aby każda osoba fizyczna mogła upewnić się, iż dotyczące jej dane osobowe są prawidłowe i przetwarzane zgodnie z prawem. Jak wynika z motywu 41 dyrektywy 95/46, aby móc dokonać koniecznych weryfikacji, osobie, której dane dotyczą, przysługuje zgodnie z art. 12 lit. a) tej dyrektywy prawo dostępu do dotyczących jej danych, które są poddane przetwarzaniu. To prawo dostępu jest niezbędne między innymi po to, aby umożliwić osobie, której dotyczą dane, uzyskanie w razie potrzeby od administratora danych ich sprostowania, usunięcia lub zablokowania, a tym samym – wykonanie prawa określonego w art. 12 lit. b) tej dyrektywy".

Na kwestię zakresu gromadzonych danych organ nadzorczy zwrócił również uwagę, opiniując **projekt ustawy o certyfikacji wykonawców zamówień publicznych oraz o zmianie niektórych innych ustaw[188].** Jego wątpliwości wzbudziło sformułowanie „w szczególności" użyte w odniesieniu do podawania innych danych umożliwiających jednoznaczną identyfikację. Zwrot ten jednoznacznie wskazuje na otwarty katalog danych osobowych. W tym przypadku prawodawca musi pamiętać, aby zbierane dane nie

[185] DOL.401.360.2023.
[186] DOL.401.90.2023.
[187] Wyrok TSUE z 20.12.2017 r. w sprawie C-434/16 *Peter Nowak v. Data Protection Commissioner,* EU:C:2017:994.
[188] DOL.401.379.2023.

wykraczały poza potrzeby wynikające z celu ich zbierania. Rozwiązaniem tej kwestii byłoby stworzenie zamkniętego katalogu danych.

Podobne zastrzeżenia organ wskazał również w odniesieniu do **projektu ustawy o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw[189].** Zauważył, że w (nowelizowanych przez ten projekt) przepisach ustawy z 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji projektodawca, wskazując elementy, które powinien zawierać wniosek organizacji o ogólnokrajowym zasięgu działania prowadzącej działalność statutową w obszarze danej branży lub danego sektora o włączenie kwalifikacji sektorowej do Zintegrowanego Systemu Kwalifikacji, posłużył się enigmatycznym sformułowaniem: „wskazanie osób uprawnionych do reprezentowania w przypadku podmiotu będącego osobą prawną lub jednostką organizacyjną niebędącą osobą prawną, której odrębna ustawa przyznaje zdolność prawną". Takie zaprojektowanie kształtu ww. wniosku czyniło omawianą regulację nieczytelną dla odbiorców, jak również skutkowało niebezpieczeństwem przetwarzania (przekazywania w ramach wniosku ministrowi właściwemu) dowolnych danych „osób uprawnionych do reprezentowania". Mogłoby to prowadzić do zamieszczania we wnioskach danych nieadekwatnych i nadmiarowych do celów przetwarzania. Dlatego organ postulował zmianę (nowelizowanego w projekcie) przepisu ustawy z 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji, polegającą na wprowadzeniu w nim zamkniętego katalogu danych osobowych „osób uprawnionych do reprezentowania". Analizując unormowania ustawy z 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji, organ zauważył, że podobne wady regulacji dotyczyły wniosków nienowelizowanych w projekcie ustawy o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw. W opinii do tego projektu zawarł więc wniosek o poprawienie także tych przepisów ustawy z 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji.

Powyższe uwagi organu nadzorczego zyskały akceptację projektodawcy, który w toku procesu legislacyjnego dotyczącego projektu ustawy o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw zdecydował się znowelizować – w oczekiwanym przez organ kierunku – wszystkie zakwestionowane przepisy ustawy z 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji[190].

Kwestie związane z katalogiem danych były przedmiotem opinii dotyczącej **projektu rozporządzenia Ministra Finansów w sprawie korzystania z e-Urzędu Skarbowego[191],** w której organ wskazał na niezbędność wyznaczenia zamkniętego katalogu danych osobowych służących do obsługi konta przez urząd i korzystania z niego przez użytkowników.

Podczas prac nad **projektem ustawy o osłonach socjalnych dla pracowników sektora elektroenergetycznego i branży górnictwa węgla brunatnego[192]** organ nadzorczy zwrócił uwagę na konieczność doprecyzowania unormowań związanych z rejestrem pracowników sektora elektroenergetycznego i branży górnictwa węgla

[189] DOL.401.132.2023.
[190] Ustawa z 30 sierpnia 2023 r. o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw (Dz. U. poz. 2005).
[191] DOL.401.247.2023.
[192] DOL.401.103.2023.

brunatnego, którzy skorzystali ze świadczenia socjalnego oraz jednorazowej odprawy pieniężnej. Projektodawca uwzględnił ten wniosek, doprecyzował zakres danych gromadzonych w powołanym rejestrze.

W toku opiniowania **ustawy o pomocy państwa w oszczędzaniu na cele mieszkaniowe**[193] wątpliwości organu budziły regulacje przewidujące, że: „Konto i lokata są prowadzone na podstawie umowy zawieranej z oszczędzającym. Umowa określa w szczególności strony umowy, w tym imię i nazwisko oraz numer PESEL oszczędzającego, a w przypadku oszczędzającego nieposiadającego numeru PESEL – numer dokumentu potwierdzającego jego tożsamość wraz z nazwą państwa, które wydało ten dokument”. Takie brzmienie przepisu, poprzez użycie określeń „w szczególności” oraz „w tym”, pozostawia możliwość przetwarzania danych osobowych oszczędzającego nie tylko wskazanych w treści normy, ale również innych. Organ podkreślił, że katalog danych przetwarzanych na podstawie przepisów prawa bankowego jest o wiele szerszy niż przedstawiony w opiniowanym projekcie ustawy. Dlatego uzasadnione byłoby precyzyjne wskazanie zakresu danych niezbędnego dla realizacji celów projektowanej ustawy, co powinno zostać poprzedzone oceną skutków dla ochrony danych. Pozostawienie przepisu w obecnym kształcie dawałoby możliwość nieograniczonego, a więc potencjalnie nadmiarowego i dowolnego, przetwarzania danych dotyczących oszczędzającego.

Uwaga organu dotycząca zakresu danych kandydatów uczestniczących w naborze, a przetwarzanych w systemie teleinformatycznym tworzonym mocą nowelizowanej **ustawy z 14 kwietnia 2023 r. o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw**[194] wskazywała, że projektowany zakres przetwarzanych danych wykracza poza katalog danych wymaganych od osoby ubiegającej się o zatrudnienie na podstawie zarówno ustawy z 21 listopada 2008 r. o służbie cywilnej, jak i ustawy z 26 czerwca 1974 r. Kodeks pracy (np. adres poczty elektronicznej, numer telefonu, płeć czy wizerunek zamieszczony w CV). W ocenie organu nadzorczego zakres danych użytkowników/kandydatów powinien zostać ograniczony i skorelowany z wymogami Kodeksu pracy. Nie można wymagać, aby pracodawcy z pominięciem przepisów prawa pracy byli obligowani do pozyskiwania od pracowników ich danych dla innego administratora (Szefa Służby Cywilnej) celem prowadzenia przez niego rejestru. W przypadku zaś innych użytkowników sytemu, takich jak pracownicy działu kadr, zaprojektowany katalog danych użytkownika jest rażąco nieadekwatny i powinien być ograniczony wyłącznie do danych, takich jak: imię, nazwisko, stanowisko służbowe czy służbowy adres poczty elektronicznej, gdyż reprezentują oni swoich pracodawców, a nie działają we własnym interesie.

Z problematyką nadmiarowego przetwarzania (pozyskiwania) danych organ zetknął się także przy opiniowaniu projektów na podstawie przepisów innych niż RODO.

W przypadku **projektu rozporządzenia Ministra Sprawiedliwości w sprawie zasad organizacji i warunków przeprowadzania badań psychologicznych i psychiatrycznych w ośrodkach diagnostycznych**[195] organ, w kontekście zasady

[193] DOL.401.53.2023.
[194] DOL.401.134.2023.
[195] DOL.401.147.2023.

minimalizacji danych z art. 13 ust. 1 ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[196] w zw. z art. 4 ust. 1 lit. c dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW[197], wyraził wątpliwości co do zasadności identyfikowania skazanego dla celów związanych z jego badaniami psychologicznymi lub psychiatrycznymi z wykorzystaniem imienia ojca. Zdaniem organu wobec – przewidzianego w projekcie – kierowania skazanego na badania za pomocą Centralnej Bazy Danych Osób Pozbawionych Wolności, imię ojca nie jest daną osobową niezbędną dla zweryfikowania tożsamości skazanego, gdyż w bazie tej zamieszczonych jest wiele danych pozwalających na jednoznaczne zidentyfikowanie skazanego badanego w ośrodku diagnostycznym.

Podobnie, wzgląd na dyspozycję art. 66 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1862 z 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE[198] w związku z – przywoływanymi już – zasadami dotyczącymi przetwarzania danych osobowych określonymi w RODO, przesądził o zgłoszeniu przez organ nadzorczy uwag odnośnie do unormowań **projektu rozporządzenia Ministra Sprawiedliwości zmieniającego rozporządzenie – Regulamin urzędowania sądów powszechnych[199]** dotyczących zakresu danych osobowych zamieszczanych w postanowieniu sądu opiekuńczego o zakazie opuszczania kraju przez małoletniego wydawanym z przyczyn, o których mowa w art. 32 ust. 1 lit. c i d ww. rozporządzenia UE oraz art. 3 ust. 1 pkt 7–9 ustawy z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[200]. W opinii organu zaproponowane w projekcie odesłanie w tej kwestii do katalogu danych osobowych z art. 4 ust. 8 pkt 1 lit. a–k ustawy z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym jest wystarczające do jednoznacznej identyfikacji małoletniego, którego dotyczy postanowienie sądu opiekuńczego. Zatem (mając na uwadze zasadę minimalizacji danych) zbędne są – także zamieszczone w projekcie – sfomułowania „co najmniej” i „oraz inne dostępne dla sądu dane”.

[196] Dz. U. z 2023 r,. poz. 1206.
[197] Dz. Urz. UE L 119 z 4.5.2016, str. 89 ze zm.
[198] Dz. Urz. UE L 312 z 7.12.2018, str. 56 ze zm.
[199] DOL.401.19.2023.
[200] Dz. U. z 2023 r. poz. 1355.

5.7. Projekty aktów prawnych tworzonych na poziomie Unii Europejskiej

W 2023 r. bardzo istotnym zagadnieniem z punktu widzenia zadań organu nadzorczego było dążenie do wyraźnego określenia jego kompetencji, jeśli takie miałyby być przewidziane mocą tworzonych unijnych rozporządzeń lub dyrektyw. Przypisanie: zadań, kompetencji, praw i obowiązków, które miałyby spoczywać mocą przepisów projektowanych aktów na organie nadzorczym w rozumieniu przepisów RODO, zwłaszcza w zakresie: konsultacji, współpracy, wymiany informacji, nakładania sankcji, powinno wynikać wprost z precyzyjnych regulacji i być szczegółowo określone. Część przedstawianych organowi do zaopiniowania unijnych projektów tworzonych przepisów – poprzez zastosowanie sformułowań, takich jak: „odpowiednie organy publiczne", „inne właściwe organy" – nie wskazuje wprost, czy i w jakim zakresie organowi nadzorczemu przypisane zostaną kompetencje odnoszące się do regulowanej materii. Z reguły ogólne sformułowanie, zobowiązujące organ nadzorczy do nadzoru nad przetwarzaniem danych osobowych w kontekście projektowanego aktu, wiąże się ze znacznym rozszerzeniem zadań polskiego organu nadzorczego, a obowiązek w postaci „współpracy" organu nadzoru z właściwymi organami może prowadzić do sporów kompetencyjnych z innymi organami właściwymi w rozumieniu projektowanych regulacji.

Powyższe postulaty organu zawierały opinie legislacyjne w odniesieniu do: **założeń projektu ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw wdrażającej rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Akt o usługach cyfrowych)**[201]; **projektu rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ram dostępu do danych finansowych i zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2022/2554 (Regulation on a framework for Financial Data Access – FIDA)**[202]**; projektu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) DGA**[203]**; projektu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) DSA**[204]**; projektu rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679**[205].

Wartym zaznaczenia aspektem prac legislacyjnych organu nadzorczego w 2023 r. było opiniowanie projektów aktów prawa UE. Co do zasady projekty unijnych aktów prawnych, tj. rozporządzeń i dyrektyw, są przekazywane do UODO przez odpowiednie ministerstwa na potrzeby opracowywania stanowiska Rady Ministrów do projektowanych dokumentów oraz dalszych prac nad nimi na poziomie Rady UE. Udział organu

[201] DOL.401.18.2023.
[202] DOL.401.329.2023.
[203] DOL.401.361.2023.
[204] DOL.401.21.2023.
[205] DOL.401.346.2023.

nadzorczego w tego typu procesie legislacyjnym uzależniony jest od potrzeb oraz praktyki danego ministerstwa i może wiązać się z wielokrotnym wydawaniem opinii na potrzeby prac grup roboczych Rady UE. W swoich stanowiskach organ wielokrotnie podkreślał konieczność zachowania ich spójności ze stanowiskami prezentowanymi przez Europejską Radę Ochrony Danych.

Wkład organu nadzorczego w prace na poziomie unijnym dotyczył: **projektu rozporządzenia Parlamentu Europejskiego w sprawie sztucznej inteligencji (AI Act)[206]; projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych i zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2022/2554 (FIDA)[207]; projektów rozporządzeń w ramach pakietu cyfrowego euro (tj. rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia cyfrowego euro[208], rozporządzenia Parlamentu Europejskiego i Rady w sprawie świadczenia usług cyfrowego euro przez dostawców usług płatniczych z państw członkowskich spoza strefy euro[209], rozporządzenia Parlamentu Europejskiego i Rady w sprawie statusu prawnego środka płatniczego banknotów i monet w walucie euro[210]); projektu rozporządzenia PSR – w sprawie usług płatniczych w ramach rynku wewnętrznego i zmieniające rozporządzenie (UE) nr 1093/2010[211]; projektu dyrektywy PSD3 – w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym w ramach rynku wewnętrznego, zmieniająca dyrektywę 98/26/WE i uchylająca dyrektywy (UE) 2015/2366 i 2009/110/WE[212]; dyrektywy Parlamentu Europejskiego i Rady ustanawiającej europejską kartę osoby z niepełnosprawnością i europejską kartę parkingową dla osób z niepełnosprawnościami COM(2023) 512[213]; projektu rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenia (UE) nr 1092/2010, (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2021/523 w odniesieniu do niektórych wymogów sprawozdawczych w dziedzinach usług finansowych i wsparcia inwestycyjnego[214]; projektu dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywę 2012/29/UE ustanawiającą minimalne normy w zakresie praw, wsparcia oraz ochrony ofiar przestępstw oraz zastępującej decyzję ramową Rady 2001/220/WSiSW[215].**

5.8. Podsumowanie

Tworzenie przepisów powszechnie obowiązujących wymaga pogodzenia treści regulowanej materii – zarówno kierunkowo, jak i w odniesieniu do brzmienia poszczególnych jednostek redakcyjnych aktu prawa – z wymogami z zakresu ochrony danych osobowych. Istotne jest, aby zgodnie z gwarancjami dla ochrony danych

[206] DOL.401.337.2023.
[207] DOL.401.329.2023.
[208] DOL.401.330.2023.
[209] DOL.401.334.2023.
[210] DOL.401.333.2023.
[211] DOL.401.331.2023.
[212] DOL.401.335.2023.
[213] DOL.401.473.2023.
[214] DOL.401.546.2023.
[215] DOL.401.608.2023.

osobowych, wyrażonymi w Konstytucji RP oraz prawie unijnym i krajowym, przy uwzględnieniu orzecznictwa TSUE i sądów krajowych, wytycznych Europejskiej Rady Ochrony Danych (EROD) i stanowisk Prezesa UODO, wprowadzać do porządku prawnego regulacje przejrzyste, zupełne i mające efektywne zastosowanie.

Wyżej przedstawiony udział organu nadzorczego w tym procesie nie wyczerpuje całego katalogu zagadnień legislacyjnych, którymi w 2023 r. zajmował się Urząd Ochrony Danych Osobowych, a przedstawione projekty aktów normatywnych prowadzą jedynie do kierunkowego wskazania istotnych, z punktu widzenia ochrony danych, zjawisk w procesie stanowienia prawa.

Analiza spraw prowadzonych w 2023 r. pozwala na przyjęcie wniosku, że od chwili rozpoczęcia stosowania RODO konsekwentne działania organu nadzorczego zapewniają wielu różnym sektorom gospodarki wsparcie eksperckie na etapie tworzenia prawa oraz w większości przypadków przynoszą zamierzone rezultaty. W analizowanym roku sprawozdawczym prace organu w tym zakresie pozwalają na sformułowanie następujących wniosków:

1) Twórcy przepisów coraz częściej biorą pod uwagę standardy ochrony danych wyznaczone ogólnym rozporządzeniem o ochronie danych i wskazywane w opiniach legislacyjnych organu. Tym samym wzrasta ich świadomość i odpowiedzialność za jakość stanowionego prawa, niegodzącego w prawa osób i nienarażającego wykonawców norm na sankcje. Podejmując decyzję co do ostatecznego kształtu przyjmowanych przepisów, coraz częściej uznają (choć czasem wybiórczo) eksperckie wskazówki organu nadzorczego.
2) Projektodawcy częściej przekonują się do niezbędności przeprowadzenia testu prywatności, oceny wpływu planowanych rozwiązań na ochronę danych, choć czynią to dopiero po zapoznaniu się z opiniami legislacyjnymi organu, podnoszącymi ten istotny aspekt. Konsekwentnie jednak projektodawcy rezygnują z uprzednich konsultacji na potrzeby tworzenia przepisów prawa.
3) Pozytywnie ocenianym zjawiskiem jest coraz częstsze poświęcanie odrębnych części lub rozdziałów projektowanych regulacji zagadnieniu przetwarzania danych osobowych. Wskazuje to na świadomość istoty tych regulacji oraz troskę o ich kompleksowość. Na przyjęcie takiego rozwiązania (bądź zastosowania standardowych klauzul umownych jako instrumentu transferu danych osobowych) nierzadko decydowali się także projektodawcy redagujący treść umów międzynarodowych, których przedmiotem było m.in. przekazywanie danych osobowych poza Europejski Obszar Gospodarczy.
4) Twórcy przepisów coraz częściej, uwzględniając zasadę minimalizmu, proponowali przetwarzanie danych jedynie w zakresie niezbędnym do celów regulacji, jak też biorąc pod uwagę zasadę ograniczenia celu, wykazywali wyczerpująco cele przetwarzania danych.
5) Duża część opinii legislacyjnych wiązała się z kwestionowaniem projektowanych rozwiązań dotyczących tworzenia, zmiany zakresu, funkcjonalności rejestrów publicznych i systemów teleinformatycznych oraz łączenia baz danych, dla których projektodawca wielokrotnie nie przeprowadzał testów prywatności, mimo iż proponowane rozwiązania budziły wątpliwości w sferze ochrony danych osobowych.

Przepisy ogólnego rozporządzenia wymagają, by każde przetwarzanie danych osobowych było planowane z uwzględnieniem koncepcji ochrony danych (i prywatności) w fazie projektowania (*privacy by design*), jak i w czasie samego przetwarzania. W sytuacji gdy twórca przepisów przewiduje, że przetwarzanie danych osobowych będzie prowadzone z wykorzystaniem określonych rozwiązań informatycznych, to od samego początku, na każdym etapie projektowania ich wykorzystywania, pod uwagę powinien brać wpływ, jaki ich stosowanie będzie wywierało na prywatność osób, których dane dotyczą. Uwzględniać przy tym powinien także stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych, a jednocześnie tak powinien projektować planowane cyfrowe rozwiązania, by były odpowiednie dla konkretnego przypadku, a jednocześnie pozbawione były na jak najwyższym poziomie ryzyk naruszeń praw i wolności podmiotów danych. Pożądane jest, by aspekt ważenia ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze brać pod uwagę już na etapie projektowania rozwiązań prawnych. 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). Należy ją 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). Rozwiązania prawne powinny być skonstruowane tak, by z jednej strony wypełnianie celów prawodawcy następowało ze spełnieniem wskazanych w RODO funkcjonalności i zasad, a z drugiej strony pozwalało 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, w związku z jakimi etapami operacji na danych osobowych jest odpowiedzialny za to przetwarzanie (w tym m.in. pozyskiwanie czy udostępnianie danych).

6. Zgłaszanie naruszeń ochrony danych osobowych

Zadaniem Urzędu Ochrony Danych Osobowych realizowanym od 25 maja 2018 r. jest przyjmowanie od administratorów zgłoszeń naruszeń o ochronie danych osobowych, które stwarzają ryzyko naruszenia praw lub wolności osób fizycznych. 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 o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem

przestępczości 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 UODO o naruszeniu danych osobowych w terminie nie późniejszym niż 24 godziny od wykrycia naruszenia danych osobowych, zgodnie z art. 174a ust. 1 ustawy z 6 lipca 2024 r. Prawo telekomunikacyjne w zw. z art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013 z 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.

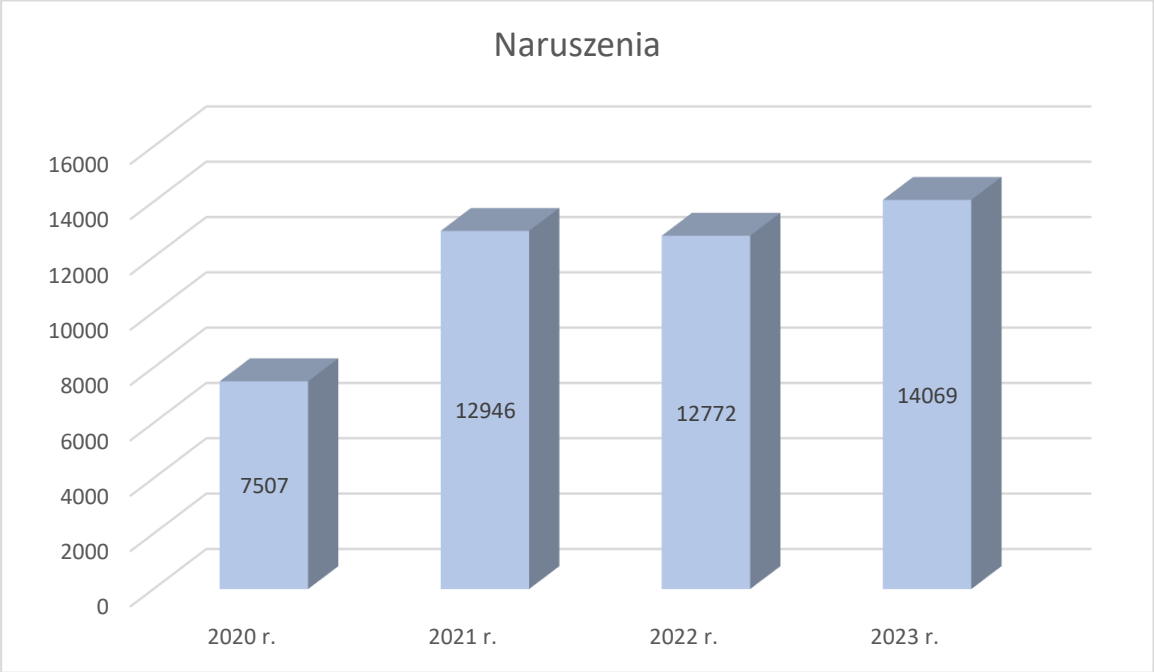
W celu zapewnienia należytego wywiązania się z tego obowiązku przez administratorów UODO przygotował formularz zgłoszeniowy, który umożliwia każdemu administratorowi nie tylko przekazanie wszystkich niezbędnych informacji określonych w RODO, ale także podanie dodatkowych danych umożliwiających organowi nadzorczemu dokonanie analizy naruszenia pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Dotychczasowa praktyka wskazuje, że w przypadku administratorów zgłaszających naruszenia na zaproponowanym formularzu ryzyko przekazania niewystarczających informacji jest mniejsze, niż w przypadku naruszeń przesyłanych przez administratora 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) RODO. Prezes UODO dokonuje weryfikacji oceny dokonanej przez administratora i może – jeżeli administrator nie zawiadomił osoby, której dane dotyczą – 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 jego potencjalnymi skutkami. 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 – na ocenę modyfikacji i usprawnień służących zapobieżeniu nieprawidłowościom analogicznym do objętych zgłoszeniem.

6.1. Statystyka zgłaszanych naruszeń ochrony danych osobowych

W 2023 r. do Urzędu Ochrony Danych Osobowych wpłynęło **14 069 zgłoszeń naruszeń.**



Wykres 14: Liczba naruszeń ochrony danych osobowych, które wpłynęły do UODO w latach 2020–2023

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

a) nieprawidłowe zaadresowanie korespondencji – zarówno w formie tradycyjnej, jak i elektronicznej

Konsekwencją tych naruszeń było udostępnienie danych osobowych osobom nieuprawnionym. Powodem ww. naruszeń najczęściej był błąd pracownika administratora danych, a naruszenia miały z reguły charakter jednorazowego incydentu. Zdarzały się jednak naruszenia będące konsekwencją błędów już na etapie gromadzenia danych adresowych, polegających na wskazaniu administratorom nieprawidłowych danych adresowych przez niedoszłych adresatów korespondencji. Wciąż bardzo często zgłaszanym naruszeniem było udostępnienie danych osobowych niewłaściwym adresatom z powodu przesyłania masowej korespondencji elektronicznej bez ukrycia adresów e-mail innych osób (UDW). W celu zminimalizowania ryzyka ponownego wystąpienia podobnych naruszeń w przyszłości administratorzy: przeprowadzali dodatkowe szkolenia pracowników, dokonywali aktualizacji baz danych, zobowiązywali osoby nieuprawnione, które weszły w posiadanie danych osobowych, do trwałego i bezpowrotnego usunięcia danych i potwierdzenia braku ich nieuprawnionego wykorzystania. Wdrażali też środki bezpieczeństwa w postaci np. szyfrowania przesyłanej wiadomości czy wymuszenia dwukrotnego podania adresu do korespondencji w formularzu.

b) udostępnienie danych niewłaściwej osobie

Tego rodzaju naruszenia miały miejsce najczęściej z powodu wydania dokumentów, np. zaświadczeń czy deklaracji podatkowych, osobom nieposiadającym uprawnień do ich otrzymania. W celu ograniczenia częstotliwości występowania tego typu naruszeń w przyszłości administratorzy danych 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.

c) nieprawidłowa anonimizacja danych lub niezamierzona ich publikacja

Do tego typu naruszeń dochodziło poprzez publikację danych osobowych na stronie internetowej administratora oraz przez udostępnienie ich w trybie dostępu do informacji publicznej, w tym również w Biuletynie Informacji Publicznej i dziennikach urzędowych. Takie naruszenia spowodowane były najczęściej nieprawidłową anonimizacją danych oraz błędami pracowników udostępniających dokumenty i materiały do zamieszczenia w Internecie. Aby zminimalizować negatywne skutki takich naruszeń oraz zapobiec powtórzeniu się analogicznych nieprawidłowości, administratorzy z reguły usuwali opublikowane informacje z witryn internetowych oraz wprowadzali dodatkowe środki bezpieczeństwa np. w postaci dodatkowej weryfikacji anonimizacji dokumentów.

d) zagubienie korespondencji przez operatora pocztowego lub otwarcie korespondencji przed zwróceniem jej do nadawcy

Tego rodzaju naruszenia najczęściej były efektem działań operatora pocztowego. Administratorzy, w ramach działań zapobiegających wystąpieniu podobnych incydentów w przyszłości, po stwierdzeniu naruszenia ochrony danych składali reklamację do operatora pocztowego, dokonywali aktualizacji instrukcji kancelaryjnej oraz zmieniali postanowienia umów zawartych z operatorem pocztowym.

e) nieuprawniony dostęp do baz danych

Tego typu naruszenia były spowodowane najczęściej błędami oprogramowania ujawniającymi się po przeprowadzeniu aktualizacji programu, brakiem regularnych, wewnętrznych testów bezpieczeństwa w kierunku wykrycia podatności systemu, a także nieprawidłowościami na etapie nadawania uprawnień w systemach informatycznych, co skutkowało ujawnieniem danych osobom nieuprawnionym. W ramach działań naprawczych administratorzy zlecali zewnętrznym podmiotom świadczącym usługi informatyczne wykonanie audytów, przeprowadzali testy systemów w środowisku budowy kodów aplikacji – tzw. środowisku deweloperskim, a także przeprowadzali analizę nadawanych uprawnień, ograniczając je do takich, które są niezbędne pracownikom do wykonywania obowiązków służbowych.

f) zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej

Tego rodzaju naruszenia ochrony danych miały charakter jednorazowych incydentów i były konsekwencją niefrasobliwości pracowników. W celu zmniejszenia prawdopodobieństwa wystąpienia takich naruszeń w przyszłości administratorzy danych podejmowali działania, które koncentrowały się na podnoszeniu świadomości pracowników w zakresie zapewnienia bezpieczeństwa powierzonych dokumentów, a także upominali osoby odpowiedzialne za naruszenia. Dodatkowo dokonywali weryfikacji obowiązujących procedur dotyczących przetwarzania danych osobowych utrwalonych w dokumentacji papierowej, poza siedzibą administratora. W przypadku kradzieży dokumentów administratorzy zawiadamiali organy ścigania.

g) zagubienie lub kradzież nośnika danych

Tego rodzaju naruszenia ochrony danych osobowych miały miejsce na skutek utraty nośników danych, takich jak laptop lub niezaszyfrowany pendrive. W celu zminimalizowania prawdopodobieństwa wystąpienia tego typu naruszeń w przyszłości administratorzy: decydowali się na zastosowanie środków bezpieczeństwa w postaci szyfrowania urządzeń wykorzystywanych do przetwarzania danych osobowych, dokonywali weryfikacji w zakresie stosowania się przez pracowników do zasady ograniczonego czasu przechowywania danych osobowych, wprowadzali rozwiązania umożliwiające zdalne usuwanie danych osobowych z urządzeń znajdujących się poza siedzibą administratora oraz zwiększali wykorzystywanie rozwiązań chmurowych. Dodatkowo podejmowane były działania mające na celu podnoszenie świadomości pracowników w zakresie zapewnienia bezpieczeństwa danych przetwarzanych za pomocą powierzonych im urządzeń. Kradzieże nośników danych zgłaszano organom ścigania.

h) wykorzystanie złośliwego oprogramowania ingerującego w poufność, integralność lub dostępność danych osobowych

Powodem tych incydentów bezpieczeństwa było wykorzystanie przez osoby specjalizujące się w tego typu działaniach podatności systemów informatycznych na atak. Do przełamania zabezpieczeń często przyczyniali się sami administratorzy danych, którzy korzystali z nieaktualnego oprogramowania. Aby zaradzić tego rodzaju naruszeniom ochrony danych, z reguły odzyskiwano dane osobowe z kopii zapasowych, które jednak nie zawsze były przez administratorów regularnie sporządzane. W przypadku braku kopii zapasowych administratorzy zwracali się o pomoc w odszyfrowaniu danych do wyspecjalizowanych w tej dziedzinie podmiotów. W celu eliminowania w przyszłości tego typu naruszeń administratorzy: przeprowadzali dodatkowe testy bezpieczeństwa, aktualizowali programy antywirusowe, podnosili wymogi regularnego testowania, mierzenia i oceniania skuteczności stosowanych środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania. Ponadto zgłaszali naruszenia organom ścigania oraz Zespołowi CERT Polska.

i) naruszenia spowodowane błędami w aplikacjach

Kolejnym z rodzajów naruszeń ochrony danych osobowych były te występujące na skutek istniejących w aplikacjach błędów umożliwiających nieautoryzowany dostęp do zasobów, poprzez dostęp do identyfikatora wskazanego zasobu (podatności IDOR). Podatność IDOR w połączeniu z numerycznymi identyfikatorami sprawiała, że ryzyko nieuprawnionego dostępu do danych istotnie rosła. Jednym z najprostszych do wychwycenia IDOR-ów jest możliwość manipulacji adresem URL. W przypadku podatności IDOR błędy w aplikacji umożliwiały modyfikację identyfikatora lub innego dowolnego parametru w adresie strony, przez co dochodziło do uzyskania dostępu do danych innego konta zawierającego dane osobowe. Zapobieganie atakom typu IDOR opiera się na projektowaniu i tworzeniu profesjonalnych aplikacji biznesowych w taki sposób, aby odwołania do obiektów, jak klucze SSH, hasła czy nazwy plików w katalogu nie były nigdy widoczne po stronie frontendu. Szczególnie ważne jest to w aplikacjach, które służą do przetwarzania wrażliwych danych po stronie klienta.

Wskazać należy, że rośnie świadomość wśród administratorów, którzy nie po raz pierwszy zgłaszają organowi nadzorczemu naruszenie ochrony danych osobowych. Składając kolejny raz formularze naruszeń, administratorzy potrafili trafnie ocenić, czy

wystąpiło wysokie ryzyko naruszenia dla praw lub wolności osób fizycznych oraz stwierdzić wskutek dokonanej analizy, czy należy powiadomić osoby o naruszeniu ich danych osobowych w myśl art. 34 ust. 1 i 2 rozporządzenia 2016/679, bez interwencji organu nadzorczego. Jednocześnie inspektorzy ochrony danych coraz częściej byli w stanie określić środki bezpieczeństwa, jakie powinni zastosować w celu uniknięcia podobnych zdarzeń w przyszłości (szkolenia personelu czy środki mitygacji ryzyka w systemach teleinformatycznych).

6.2. Wyjaśnienia

Zasadniczym uprawnieniem organu nadzorczego, niezbędnym do prawidłowego prowadzenia czynności w następstwie dokonanego zgłoszenia naruszenia ochrony danych osobowych, jest uprawnienie do nakazania dostarczenia informacji przez zgłaszającego. Prawodawca nadaje te uprawnienia Prezesowi UODO w art. 58 ust. 1 lit. a) i e) RODO. 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 UODO wystosował do administratorów danych osobowych dokonujących zgłoszeń naruszeń **759 pisemnych wezwań do złożenia wyjaśnień i udzielił 4 pisemnych informacji w związku z przypadkami naruszeń ochrony danych osobowych.**

Na podstawie art. 52 ust. 1 ustawy o ochronie danych osobowych Prezesowi UODO przysługuje uprawnienie skierowania do podmiotów wymienionych w tym przepisie wystąpień zmierzających do zapewnienia skutecznej ochrony danych osobowych. W analizowanym 2023 r. Prezes UODO skierował **684 wystąpienia** do administratorów, którzy złożyli w UODO zgłoszenie naruszenia ochrony danych osobowych, ale mimo istnienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych nie powiadomili osób, których dotyczyło naruszenie, lub zawiadomienie to nie zawierało informacji wymaganych zgodnie z art. 34 ust. 2 rozporządzenia 2016/679.

Wystąpienia dotyczyły podjęcia stosownych działań mających na celu niezwłoczne ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych i przekazania tej osobie szczegółowych informacji na temat charakteru naruszenia.

W większości przypadków wezwań wątpliwości Prezesa UODO budziły:

- zastosowane lub proponowane przez administratorów środki bezpieczeństwa w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia;
- środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą;
- nieprawidłowe oszacowania poziomu ryzyka naruszenia praw lub wolności osób fizycznych;
- nieprawidłowe wskazania terminu dokonanego zgłoszenia oraz wyjaśnienia przyczyn opóźnienia powiadomienia organu nadzorczego o naruszeniu;
- dochowanie obowiązku zawiadomienia osób, których dane dotyczą;
- wskazanie przez administratorów kategorii i liczby osób oraz danych objętych naruszeniem.

Adresaci wezwań w zdecydowanej 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 naruszeń ochrony danych osobowych wynika, że realizacja kompetencji Prezesa UODO w trybie art. 58 ust. 1 lit. a) i e) RODO pozytywnie wpływała na ochronę danych osobowych. Znacznie bowiem skracała proces przywracania stanu zgodnego z prawem, pozwalając organowi nadzorczemu na natychmiastowe działanie bez konieczności prowadzenia sformalizowanego postępowania administracyjnego. 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 szybką reakcję na zgłoszenia naruszenia, tak aby w jak najkrótszym 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.

6.3. Postępowania administracyjne

W 2023 r. Prezes UODO **wszczął z urzędu 24 postępowania administracyjne** w sprawie naruszenia przepisów o ochronie danych osobowych. W niektórych przypadkach podjęta została decyzja o przeprowadzeniu u administratora danych kontroli przestrzegania przepisów o ochronie danych. Zastrzeżenia Prezesa UODO w związku ze zgłoszonymi 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: 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 d) RODO;
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 RODO, w szczególności dotyczące spełniania obowiązku przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, podejmowania wszelkich środków wymaganych na mocy art. 32 RODO oraz – po zakończeniu świadczenia

usług związanych z przetwarzaniem danych osobowych – usuwania lub zwracania administratorowi wszelkich danych osobowych i usuwania wszelkich ich istniejących kopii[216];

e) treści zawiadomienia osób, których dane dotyczą, o naruszeniu ich danych osobowych pod kątem spełniania wymogów określonych w art. 34 ust. 2 RODO.

6.4. Decyzje administracyjne

W wyniku prowadzonych przez Prezesa UODO postępowań administracyjnych, które zostały zakończone w 2023 r., wydano **36 decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych.** W 17 decyzjach Prezes UODO udzielił upomnienia administratorowi danych, w tym w 1 decyzji udzielił upomnienia i nakazał dostosowanie operacji przetwarzania do przepisów RODO.

W przypadku **19 naruszeń** Prezes Urzędu Ochrony Danych Osobowych, po przeprowadzeniu postępowań administracyjnych, w wydanych decyzjach administracyjnych zdecydował się nałożyć na administratorów danych administracyjne kary pieniężne, w tym w **8 przypadkach** dodatkowo nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 lub zawiadomienie o naruszeniu osoby, których dane dotyczyły, w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 RODO.

W analizowanym roku sprawozdawczym **7 decyzji Prezesa UODO, wydanych po przeprowadzeniu postępowań administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych, zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie.**

Wojewódzki Sąd Administracyjny w Warszawie utrzymał w mocy **4 i uchylił 2 decyzje Prezesa UODO,** wydane w okresie sprawozdawczym oraz w poprzednich latach po przeprowadzeniu postępowań administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych.

Wybrane przykłady decyzji Prezesa UODO nakładające administracyjną karę pieniężną administratorowi w związku ze stwierdzeniem naruszenia przepisów RODO, zostały przedstawione w rozdziale 4 niniejszego sprawozdania.

6.5. Administracyjne kary pieniężne w związku z naruszeniem

Po przeprowadzeniu postępowania administracyjnego wobec dwóch podmiotów – administratora oraz podmiotu przetwarzającego – Prezes UODO wydał decyzję[217], którą nałożono na nich administracyjną karę pieniężną. Ponadto decyzja ta obejmowała nakaz dostosowania operacji przetwarzania danych osobowych poprzez zaprzestanie powierzania przetwarzania danych osobowych podmiotowi przetwarzającemu w oparciu o umowę powierzenia przetwarzania danych osobowych, która nie zawiera elementów wskazanych w art. 28 ust. 3 lit. c), e) i f) rozporządzenia 2016/679.

W przypadku administratora Prezes Urzędu Ochrony Danych Osobowych stwierdził naruszenie przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 28 ust. 1 i 3 oraz art. 32 ust. 1 i 2 RODO. Naruszenie to polegało na niewdrożeniu odpowiednich

[216] Art. 28 ust. 3 lit. a), c) i g) RODO.
[217] DKN.5131.50.2021.

środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych, co skutkowało naruszeniem ich poufności i rozliczalności, oraz na braku weryfikacji podmiotu przetwarzającego, czy zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą**.** Natomiast w przypadku podmiotu przetwarzającego stwierdzono naruszenie art. 32 ust. 1 i 2 oraz art. 32 ust. 1 i 2 w zw. z art. 28 ust. 3 lit. c) i f) RODO, polegające na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych, w tym ich poufności.

Powyższa decyzja została wydana w związku z naruszeniem ochrony danych osobowych polegającym na niezamierzonej publikacji danych osobowych klientów administratora, który działał jako **broker ubezpieczeniowy.** Administrator, chcąc umożliwić swoim pracownikom pracę zdalną, zlecił podmiotowi przetwarzającemu (wykonującemu na jego rzecz usługi informatyczne) wdrożenie takiego rozwiązania. W wyniku zmian wprowadzonych w systemie informatycznym doszło do niezamierzonej publikacji danych osobowych obejmującej szeroki zakres danych.

Decyzja wydana w tej sprawie przez Prezesa UODO pokazuje wagę funkcji brokera ubezpieczeniowego w zapewnieniu ochrony danych osobowych jego klientów, rolę administratora i podmiotu przetwarzającego w procesie przetwarzania danych osobowych i wzajemnych relacji tych dwóch podmiotów.

Kolejna decyzja Prezesa UODO[218] dotyczyła **spółdzielni mieszkaniowej.** Jedna z członkiń spółdzielni weszła w konflikt z władzami spółdzielni, która zadecydowała o złożeniu zawiadomienia o podejrzeniu popełnienia przestępstwa przez tę osobę. Kopia tego zawiadomienia, zawierająca dane osobowe członkini spółdzielni w zakresie jej: imienia, nazwiska, adresu zamieszkania oraz numeru ewidencyjnego PESEL, została udostępniona dziennikarzom. Doszło również do sytuacji, że dane te otrzymała osoba związana z mediami informacyjnymi, która o ich udostepnienie w ogóle nie wnioskowała. Spółdzielnia nie zgłosiła jednak zaistniałego naruszenia Prezesowi Urzędu Ochrony Danych Osobowych, nie zawiadomiła o zaistniałym naruszeniu osoby, której dane znalazły się w ww. dokumencie.

W decyzji[219] Prezes UODO stwierdził naruszenie przez administratora – spółdzielnię mieszkaniową – przepisów art. 33 ust. 1 i art. 34 ust. 1 RODO. Organ nadzorczy zadecydował o nałożeniu na spółdzielnię administracyjnej kary pieniężnej oraz o nakazaniu jej zawiadomienia – w terminie 3 dni od dnia doręczenia decyzji – osoby, której dane zostały ujawnione w wyniku przedmiotowego udostępnienia, o naruszeniu ochrony jej danych osobowych, zgodnie z wymogami art. 34 ust. 2.

Kolejna sprawa dotyczyła bezpieczeństwa przetwarzania danych osobowych w **systemach informatycznych.** Przetwarzane w stosunkowo szerokim zakresie przez administratora dane pracowników zostały zaszyfrowane w wyniku ataku ransomware. Administrator nie miał możliwości szybkiego przywrócenia dostępności tych danych przetwarzanych w formie elektronicznej (odstąpiono od ich odszyfrowywania). Co więcej, administrator nie zgłosił Prezesowi Urzędu Ochrony Danych Osobowych zaistniałego

[218] DKN.5131.49.2021.
[219] DKN.5131.49.2021.

naruszenia ochrony danych osobowych oraz zaniechał zawiadomienia o nim osób, których dane te dotyczyły.

W wydanej decyzji[220] Prezes UODO stwierdził naruszenie przez administratora przepisów: art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1 oraz art. 32 ust. 1 i 2, art. 33 ust. 1 i art. 34 ust. 1 i 2 RODO, i nałożył administracyjną karę pieniężną. Naruszenie polegało na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą, a także odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności tych środków, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia. Skutkuje to bowiem naruszeniem zasady integralności – art. 5 ust. 1 lit. f) RODO i rozliczalności – art. 5 ust. 2 RODO. W uzasadnieniu decyzji Prezes UODO dużo miejsca poświęcił na rozważania dotyczące konieczności wdrażania przez administratora odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą.

Kolejna decyzja[221] Prezesa UODO – o nałożeniu na administratora administracyjnej kary pieniężnej oraz nakazu wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zminimalizowania ryzyka wiążącego się z przetwarzaniem danych osobowych za pomocą zewnętrznych nośników danych – dotyczyła zagubienia niezaszyfrowanego nośnika danych typu pendrive na skutek uszkodzenia przesyłki, w której znajdował się nośnik obrońcy w postępowaniu dyscyplinarnym. Na nośniku tym znajdowało się nagranie rozprawy rozwodowej z danymi osobowymi ośmiu osób, w zakresie: imienia, nazwiska, szczegółów dotyczących życia rodzinnego, relacji stron oraz podejrzeń o niewierność małżeńską. Obecnie skarga administratora na decyzję Prezesa UODO oczekuje na rozpatrzenie przez Wojewódzki Sąd Administracyjny (WSA) w Warszawie.

Po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego Prezes UODO wydał kolejną decyzję[222], która nałożyła na jedną z **publicznych uczelni akademickich** administracyjną karę pieniężną za naruszenie przepisów rozporządzenia 2016/679. Naruszenie polegało na nieodpowiednim zabezpieczeniu aplikacji wykorzystywanej w procesie rejestracji kandydatów na wyjazdy organizowane w ramach studenckiej wymiany międzynarodowej oraz braku regularnego testowania, mierzenia i oceniania skuteczności środków mających zapewnić bezpieczeństwo przetwarzanych za jej pośrednictwem danych osobowych.

Postępowanie w sprawie zostało wszczęte w konsekwencji zgłoszenia przez administratora naruszenia ochrony danych osobowych, na skutek którego doszło do przypadkowego ujawnienia w sieci Internet informacji zgromadzonych w zasobach ww. systemu. Do incydentu doszło w następstwie błędu popełnionego w ramach prac programistycznych mających na celu przeniesienie aplikacji na nowy serwer produkcyjny,

[220] DKN.5131.8.2021.
[221] DKN.5131.31.2022.
[222] DKN.5131.26.2023.

podczas których kontrola dostępu do przetwarzanych w systemie danych została wyłączona. Incydent doprowadził do zaindeksowania niezabezpieczonych danych przez jedną z wyszukiwarek internetowych, stwarzając możliwość niezgodnego z prawem przetwarzania ich przez osoby trzecie. W związku z zaistniałym zdarzeniem na uczelni przeprowadzona została kontrola, której zakresem objęto m.in. operacje przetwarzania objęte naruszeniem.

Prezes UODO w uzasadnieniu decyzji podkreślił, że administrator nie był zdolny wykazać w toku postępowania, iż wdrożone przez niego środki bezpieczeństwa danych były adekwatne wobec potencjalnych zagrożeń. Administrator nie przedstawił też dowodów wskazujących na przeprowadzanie przez niego analizy ryzyka w okresie poprzedzającym naruszenie. W świetle dokonanych ustaleń organ nadzorczy wskazał, że uczelnia nie testowała regularnie skuteczności zabezpieczeń stosowanych w tym obszarze. Nieprzeprowadzenie analizy ryzyka, skutkujące doborem nieodpowiednich środków bezpieczeństwa oraz brak regularnego testowania, mierzenia i oceniania przez administratora skuteczności wdrożonych rozwiązań, mających zapewnić bezpieczeństwo przetwarzania, w ocenie Prezesa UODO nie tylko doprowadziło do naruszenia ochrony danych osobowych, ale przesądziło też o niedopełnieniu przez uczelnię obowiązków spoczywających na niej jako administratorze danych.

Przedmiotowa decyzja została zaskarżona przez uczelnię do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Następna decyzja[223] Prezesa UODO dotyczyła jednej ze **wspólnot mieszkaniowych,** a naruszenie ochrony danych osobowych było wynikiem kradzieży dokumentów, w tym kopii aktu notarialnego, znajdujących się u zarządcy wspólnoty. Działania wspólnoty – administratora – stały się przedmiotem oceny organu nadzorczego w rozumieniu przepisów postępowania administracyjnego. W jego toku stwierdzono kilka uchybień ze strony administratora, tj.: brak zgłoszenia naruszenia ochrony danych osobowych (organ powziął informację o jego wystąpieniu na podstawie anonimowego zgłoszenia); brak zawiadomienia osób, których dane utrwalone były w utraconym akcie notarialnym; przetwarzanie danych członków tej wspólnoty powierzono bez pisemnej umowy oraz bez przeprowadzenia weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia 2016/679 i chroniło prawa osób, których dane dotyczą. Wszystkie te uchybienia stanowiły łącznie o naruszeniu przez administratora przepisów:! art. 5 ust. 1 lit. a), art. 28 ust. 1, 3 i 9, art. 33 ust. 1 oraz art. 34 ust. 1 i 2 RODO.

W konsekwencji powyższego Prezes UODO nałożył na wspólnotę administracyjną karę pieniężną, a także nakazał zawiadomienie, w terminie 3 dni od dnia doręczenia niniejszej decyzji, osób, których dane przetwarzane były na skradzionej kopii aktu notarialnego, o naruszeniu ochrony ich danych osobowych, w celu przekazania tym osobom wymaganych informacji i środków – zgodnie z art. 34 ust. 2 rozporządzenia 2016/679.

W uzasadnieniu przedmiotowej decyzji organ nadzorczy dokonał wykładni przepisów rozporządzenia 2016/679 objętych zakresem postępowania administracyjnego, a motywy,

[223] DKN.5131.31.2021.

którymi kierował się, wymierzając karę, stanowić mogą istotne wskazówki interpretacyjne dla innych administratorów. Gdy prawa lub wolności osób fizycznych są zagrożone na skutek naruszenia, trzeba je zgłosić do UODO. W omawianym przypadku jednym z zaniechań administratora było niezawiadomienie organu nadzorczego o wystąpieniu naruszenia ochrony danych. Z kolei fakt wystąpienia naruszenia ochrony danych osobowych obliguje administratora do dokonania odpowiednich czynności notyfikacyjnych. Nie ma wątpliwości, że w sytuacji wystąpienia incydentu bezpieczeństwa, zidentyfikowanego jako naruszenie ochrony danych osobowych, administrator ma obowiązek zgłosić go organowi nadzorczemu nie później niż w terminie 72 godzin od jego stwierdzenia. Co istotne, obowiązek ten jednak nie ma charakteru bezwzględnego. Administrator, na podstawie przeprowadzonej analizy ewentualnego wpływu naruszenia na prawa lub wolności osób fizycznych, może się od tego obowiązku zwolnić, jeżeli zgodnie z zasadą rozliczalności wykaże, że ryzyko dla praw lub wolności osób fizycznych nie jest wyższe niż znikome. Wówczas ważne jest, aby – zgodnie z zasadą rozliczalności – wykazać dokonanie bilansu możliwych szkód materialnych i niematerialnych, jakie mogą wiązać się z powstaniem naruszenia dla osób, których dane dotyczą. W przedmiotowej sprawie ryzyko wystąpienia negatywnych konsekwencji dla członków wspólnoty było wyższe niż znikome, dlatego też administrator miał obowiązek dokonania zgłoszenia naruszenia organowi nadzorczemu.

Drugim powodem nałożenia administracyjnej kary pieniężnej na wspólnotę było niezawiadomienie o naruszeniu osób, których dane dotyczyły. W tym przypadku wspólnota nie tylko nie zgłosiła do UODO faktu naruszenia ochrony danych osobowych wszystkich swoich członków, ale także odstąpiła od zawiadomienia dwóch osób, których dane przetwarzane były na skradzionej kserokopii aktu notarialnego, dotyczącego ich nieruchomości. Tym samym w praktyce pozbawiła te osoby możliwości przeciwdziałania potencjalnym szkodom, które mogą się względem nich zmaterializować. W ocenie organu wystąpiło wysokie ryzyko naruszenia praw lub wolności tych osób, co wiąże się z koniecznością zawiadomienia ich o naruszeniu. Należy zaznaczyć, że zarządca ustnie poinformował o zdarzeniu tylko jedną z osób, których dane przetwarzane były w skradzionej dokumentacji. Lokator ten sam podjął decyzję o zgłoszeniu sprawy do organów ścigania i wystąpił o wydanie nowego dowodu osobistego. Fakt podjęcia takiego działania przez osobę objętą naruszeniem w żaden sposób nie zwalnia wspólnoty od wystosowania do tej osoby zindywidualizowanego komunikatu w formie pisemnej oraz skierowania również do drugiej z osób zindywidualizowanego zawiadomienia. Należy zauważyć, że wysokie ryzyko naruszenia praw lub wolności nie musi się w istocie zmaterializować, a więc zgodnie z podejściem opartym na ryzyku istotne jest samo prawdopodobieństwo wystąpienia strat o charakterze materialnym lub niematerialnym w dobrach osoby, której dane dotyczą. Sprawa ta dotyczyła naruszenia, które rodziło wysokie ryzyko, zatem organ nadzorczy oprócz nałożenia kary pieniężnej dodatkowo nakazał administratorowi, aby ten zawiadomił o naruszeniu osoby, których dane dotyczą, w terminie 3 dni od dnia doręczenia decyzji.

Prezes UODO dopatrzył się również uchybień ze strony wspólnoty w postaci powierzenia przetwarzania danych osobowych jej członków bez zawarcia pisemnej umowy powierzenia przetwarzania tych danych oraz bez przeprowadzenia weryfikacji podmiotu przetwarzającego. Wspólnota i zarządca współpracowali w oparciu o zawartą umowę

cywilnoprawną opisującą wzajemne prawa i obowiązki wyłącznie w odniesieniu do zarządu nieruchomością wspólną. Umowa ta nie odnosiła się do wartości prawnie chronionych, do jakich bez wątpienia należy sfera prywatności osób fizycznych. Nie spełniała ona także wymogów określonych w przepisach RODO. Zatem uznano, że pomiędzy administratorem danych osobowych a podmiotem przetwarzającym dane nie została zawarta umowa powierzenia przetwarzania danych osobowych. Administrator, korzystając z usług podmiotów przetwarzających, powinien mieć pewność, że zapewnią one wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, dzięki czemu przetwarzanie danych osobowych będzie zgodne z RODO oraz będzie zapewniało bezpieczeństwo przetwarzania danych osobowych, jako jednego z praw podstawowych. Na administratorze spoczywa ocena, czy gwarancje te są wystarczające. Dopiero wnikliwe zbadanie kompetencji wybranego podmiotu przetwarzającego może dla administratora stanowić punkt wyjścia do zawarcia stosownej umowy powierzenia przetwarzania danych osobowych. Z przeprowadzonego postępowania wynikało, że zarządca, który przetwarzał dane osobowe członków wspólnoty, dokonywał tego w sposób dowolny, tj. działając bez udokumentowanego polecenia ze strony wspólnoty. Administrator z kolei nie sprawował żadnej kontroli nad realizowanymi w jego imieniu i na jego rzecz procesami przetwarzania danych osobowych, dokonywanymi w miejscu zamieszkania zarządcy, bez wdrożenia odpowiednich środków technicznych i organizacyjnych.

Kolejna z wydanych w 2023 r. decyzji[224] dotyczyła naruszenia ochrony danych osobowych przez Ministra Zdrowia. Opublikował on w serwisie społecznościowym X (dawniej Twitter) wpis zawierający informację na temat lekarza, który wystawił receptę *pro auctore* na lek z grupy psychotropowych i przeciwbólowych, którego dotyczy rozporządzenie Ministra Zdrowia z 12 lipca 2023 r. zmieniające rozporządzenie w sprawie środków odurzających, substancji psychotropowych, prekursorów kategorii 1 i preparatów zawierających te środki lub substancje[225]. Wpis zawierał dane osobowe lekarza w postaci imienia, nazwiska, miejsca pracy oraz informacji o kategorii leku, na który została wystawiona recepta. W związku ze zgłoszeniem przez Ministra Zdrowia naruszenia ochrony danych osobowych Prezesowi UODO podjęte zostały czynności wyjaśniające, które doprowadziły następnie do nałożenia administracyjnej kary pieniężnej oraz nakazał wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zminimalizowania ryzyka wiążącego się z przetwarzaniem danych osobowych przy wykorzystaniu Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych (dalej: Platforma, system P1), z której pochodziły ujawnione dane, 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, po uprzednim przeprowadzeniu analizy ryzyka, uwzględniającej stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, jak również nakazał zawiadomienie osoby, której dane dotyczą, w celu przekazania jej

[224] DKN.5131.32.2023.
[225] Dz. U. z 2023 r., poz. 1368.

brakujących informacji, które nie zostały zawarte w zawiadomieniu do tej osoby pomimo skierowania wystąpienia Prezesa UODO.

Prowadzone przez Prezesa UODO postępowanie administracyjne w niniejszej sprawie wykazało szereg nieprawidłowości w funkcjonowaniu systemu ochrony danych osobowych u Administratora. Naruszenie ochrony danych osobowych, skutkujące wydaniem decyzji nakładającej administracyjną karę pieniężną, dotyczyło bowiem nie tylko nieprawidłowości w dostępie do systemu P1, ale także braku adekwatnego stopnia zabezpieczenia przekazywanych danych osobowych. Dostęp Ministra Zdrowia do danych osobowych odbył się poza przyjętymi w obowiązującym prawie kompetencjami wynikającymi z przydzielonej mu funkcji, z nadużyciem stanowiska, na które został mianowany. Ponadto wątpliwości Prezesa UODO wzbudził sposób przekazania Ministrowi Zdrowia danych osobowych (za pomocą komunikatora WhatsApp), co w ocenie Prezesa UODO stanowi naruszenie zasad bezpieczeństwa i mogło prowadzić do daleko idących konsekwencji dla podmiotu danych – w związku z utratą przez niego kontroli nad własnymi danymi.

W treści decyzji Prezes UODO zdecydowanie przeciwstawia się wykorzystaniu nadanych Ministrowi Zdrowia uprawnień w celu innym niż wynikające z przepisów prawa. Co więcej, wskazuje na naganność lekceważenia obowiązków administratorów związanych z zaistnieniem naruszenia ochrony danych osobowych, jak również na odpowiedzialność organów władzy państwowej za bezprawne działania podejmowane przez nie z wykorzystaniem swojej władzy oraz możliwości, które ta władza daje.

W analizowanym 2023 r. Prezes UODO nałożył administracyjną karę pieniężną na Sąd Rejonowy Szczecin-Centrum za naruszenie: art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1 i 2 oraz art. 32 ust. 1 i 2 RODO[226]. Sprawa dotyczyła zagubienia przez osobę X trzech nośników danych typu pendrive (jednego służbowego – szyfrowanego oraz dwóch prywatnych – nieszyfrowanych), zawierających dane osobowe nieustalonej liczby osób. W kolejnych dniach wpłynęło do UODO zgłoszenie uzupełniające. Jak wskazał administrator, na zagubionych nośnikach znajdowały się: dane osobowe w zakresie imion i nazwisk, adresów zamieszkania lub pobytu, dane dotyczące zakładu pracy oraz dane o stanie zdrowia, zawarte w projektach orzeczeń i uzasadnień sporządzanych przez osobę w okresie obejmującym kilkanaście lat.

Naruszenie ww. przepisów polegało na niewdrożeniu przez sąd odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu przenośnych pamięci, które to środki zapobiegłyby utrwaleniu przez osobę X danych osobowych na dwóch prywatnych niezabezpieczonych nośnikach danych i w konsekwencji pozwoliłyby uniknąć naruszenia ochrony danych osobowych w związku z zagubieniem tych nośników.

Z analizy ryzyka przeprowadzonej przez sąd przed powstaniem naruszenia wynika, że administrator danych przewidział zagrożenie utraty poufności poprzez: „dostęp do danych przez osoby nieupoważnione ze względu na przechowywanie na niezabezpieczonych nośnikach wymiennych, przechowywanie danych/zdjęć na prywatnych urządzeniach”. Pierwotne ryzyko zostało ocenione na poziomie średnim, o wartości „6”. Jako wniosek z dokonanej analizy ryzyka zostało wskazane, że pomimo

[226] DKN.5131.12.2020.

ustalenia poziomu ryzyka na poziomie średnim – z uwagi na zastosowane zabezpieczenia przez administratora – spadło ono do poziomu akceptowalnego. Podkreślono jednak, że: „w celu jego zminimalizowania można wprowadzić blokadę używania nośników zewnętrznych lub obowiązek stosowania tylko szyfrowanych nośników danych". Prezes UODO jednakże wskazał, że administrator w przeprowadzonej analizie ryzyka nie przewidział zagrożenia utraty poufności danych, ze względu na ich przechowywanie na niezabezpieczonych lub prywatnych nośnikach pamięci, którego źródłem byłby sam pracownik sądu (w tym X). W tym przypadku nie można bowiem uznać, iż X był osobą nieupoważnioną do przetwarzania danych, którymi dysponował na zagubionych nośnikach danych. Wnioskiem z przeprowadzonej analizy była sugestia wprowadzenia blokady użytkowania prywatnych nośników pamięci lub obowiązek stosowania szyfrowanych nośników danych. Niezależnie od źródła osobowego takiego zagrożenia administrator, jak się okazuje w związku z wystąpieniem naruszenia ochrony danych osobowych, nie wdrożył blokady portów USB celem całkowitego uniemożliwienia korzystania z prywatnych nośników danych, ani nie zablokował możliwości użytkowania niezaewidencjonowanych przez dział IT sądu nośników pamięci. Poprzestał jedynie na wprowadzeniu formalnego zakazu użytkowania „prywatnych nośników". Taki zakaz wynikał z regulaminu.

Administrator dysponował programem umożliwiającym blokowanie portów USB, co dawało działowi IT możliwość kontrolowania nośników zewnętrznych oraz blokowania stacji roboczych przed podłączeniem nieautoryzowanego sprzętu. Taka blokada została wprowadzona w sądzie, jednak dopiero w późniejszym czasie, po około 11 miesiącach od momentu zakupu ww. programu i przeprowadzenia analizy ryzyka (a dwa miesiące po zmaterializowaniu się zagrożenia). Podkreślenia również wymaga, iż po każdym z przeprowadzonych w sądzie audytów osoby je przeprowadzające identyfikowały ww. podatność i artykułowały zalecenia zablokowania portów USB dla zwiększenia bezpieczeństwa danych i uniemożliwienia korzystania w sądzie z prywatnych nośników danych. W tym przypadku administrator zastosował zatem wyłącznie środki organizacyjne, ale już nie techniczne. Takim działaniem administrator nie zadbał w sposób skuteczny o bezpieczeństwo danych przetwarzanych przez sąd – nie wdrożył środków technicznych poprzez zablokowanie portów USB, choć takie wnioski były zawarte w raportach z przeprowadzonych audytów oraz wynikały z przeprowadzonej przez sąd analizy ryzyka.

Decyzja została zaskarżona do WSA w Warszawie. Sąd ten w wyroku z 15 listopada 2023 r. utrzymał w mocy ww. decyzję[227].

Kolejna decyzja[228], na mocy której Prezes UODO stwierdził naruszenie przepisów art. 33 ust. 1 i 3 RODO i nałożył administracyjną karę pieniężną, wydana została dla **Sądu Okręgowego w Krakowie.** W decyzji tej Prezes UODO nakazał Sądowi Okręgowemu w Krakowie zawiadomienie, w terminie 3 dni od dnia otrzymania niniejszej decyzji, czterech osób, których dane były zawarte na dokumentach znajdujących się w uszkodzonej przesyłce pocztowej (tj. powódki, 2 pozwanego oraz dwójki ich dzieci), o naruszeniu ochrony ich danych osobowych – w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 RODO.

[227] Sygn. akt II SA/WA552/23.
[228] DKN.5131.42.2022.

Zgłoszenie naruszenia ochrony danych osobowych złożone zostało przez Ministra Spraw Zagranicznych (dalej: MSZ). Polegało ono na dostarczeniu adresatowi przez brytyjskiego operatora pocztowego uszkodzonej i niekompletnej korespondencji zawierającej dane osobowe, wysłanej przez Konsulat Generalny RP na wniosek sądu. Jak ustalono, Konsulat Generalny RP pisemnie poinformował sąd o doręczeniu adresatowi uszkodzonej i niekompletnej przesyłki. Prezes UODO wszczął postępowanie z urzędu w przedmiocie możliwości naruszenia przez Sąd Okręgowy w Krakowie, jako administratora danych, obowiązków wynikających z art. 33 ust. 1 i 3 oraz art. 34 ust. 1 i 2 RODO.

W przedmiotowej sprawie doszło do naruszenia ochrony danych osobowych siedmiu osób, przy czym wobec czterech z nich powstało wysokie ryzyko naruszenia ich praw lub wolności z uwagi na zakres dotyczących ich danych osobowych. W przypadku powódki naruszenie obejmowało m.in. jej numer PESEL oraz dane o stanie zdrowia zawarte w dokumentacji medycznej, w przypadku pozwanego – jego numer PESEL, a w przypadku dwojga dzieci – informacje o ich stanie zdrowia, zawarte w opinii psychologicznej. Wszystkie ww. dane znajdowały się w dokumentacji przesłanej stronie postępowania rozwodowego.

Prezes UODO w uzasadnieniu decyzji stwierdził, że dostarczenie korespondencji nie stanowiło sprawowania przez sąd wymiaru sprawiedliwości ani ochrony prawnej, lecz techniczną, administracyjną czynność. Prezes UODO podkreślił, że do kompetencji sądowych organów nadzorczych, o których mowa w art. 175 dd § 1 ustawy Prawo o ustroju sądów powszechnych, nie należy przyjmowanie zgłoszeń naruszeń ochrony danych osobowych, czy też ich merytoryczna ocena. Zakres kompetencji tych organów bowiem został enumeratywnie wymieniony w art. 175 dd § 2 i 3 ustawy Prawo o ustroju sądów powszechnych i należy traktować go jako katalog zamknięty.

W ocenie Prezesa UODO doszło do naruszenia poufności danych (uszkodzona koperta, do zawartości której mogły mieć dostęp osoby nieuprawnione) i ich dostępności (brak niektórych dokumentów). Nie miało przy tym znaczenia, iż zawinił operator pocztowy, uszkadzając przesyłkę, bowiem przedmiotem postępowania był brak zgłoszenia naruszenia ochrony danych oraz brak zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. Prezes UODO stwierdził, że w sprawie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób objętych przedmiotowym naruszeniem, co z kolei skutkowało powstaniem po stronie sądu obowiązku jego zgłoszenia organowi nadzorczemu, zgodnie z art. 33 ust. 1 RODO.

W uzasadnieniu decyzji Prezes UODO wskazał, że inspektor ochrony danych sądu błędnie ocenił poziom ryzyka naruszenia praw lub wolności osób fizycznych w związku z przedmiotowym naruszeniem ochrony danych osobowych. Wskazał bowiem, że z uwagi na to, że dokumenty zostały sporządzone w języku polskim, a wysłane do Wielkiej Brytanii, nie powoduje to powstania wysokiego ryzyka w tym zakresie. W ocenie Prezesa UODO fakt, że dokumenty zawierające dane osobowe były sporządzone w języku polskim i wysłane do kraju, gdzie językiem podstawowym jest język angielski, nie obniża jednak poziomu tego ryzyka. W dobie instrumentów pozwalających na szybkie tłumaczenie dokumentów, jak również z uwagi na fakt, iż w Wielkiej Brytanii spora część mieszkańców posługuje się językiem polskim, nie można przyjmować, że okoliczność ta pozwala na obniżenie poziomu ryzyka.

Decyzja została zaskarżona do WSA w Warszawie (jest nieprawomocna).

Następną decyzję[229] Prezes UODO wydał wobec **prokuratury rejonowej,** nakładając na nią administracyjną karę pieniężną za naruszenie art. 33 ust. 1 oraz art. 34 ust. 1 rozporządzenia 2016/679. Sprawa dotyczyła przekazania przez prokuraturę rejonową lokalnemu dziennikarzowi – w ramach odpowiedzi na jego wniosek złożony w trybie ustawy z 6 września 2001 r. o dostępie do informacji publicznej – niezanonimizowanej dokumentacji z zakończonego postępowania przygotowawczego. Jak wskazał sam administrator, lokalnemu dziennikarzowi: „przekazano (…) skany niektórych dokumentów z akt, z tym iż istotnie nie dokonano ich anonimizacji". Naruszenie objęło swoim zakresem dane osobowe trzech osób, w tym dziecka. Udostępnione dane obejmowały w szczególności: imię i nazwisko, numer PESEL, datę urodzenia oraz stopień pokrewieństwa, a w przypadku dziecka także dane podlegające szczególnej ochronie na gruncie art. 9 ust. 1 RODO, tj. dane o stanie zdrowia.

Prezes UODO, po przeprowadzeniu postępowania wyjaśniającego, wszczął z urzędu postępowanie administracyjne w przedmiocie możliwości naruszenia przez prokuraturę rejonową, jako administratora danych, ochrony danych osobowych – w związku z brakiem zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO oraz braku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dotyczyło naruszenie.

Prezes UODO uznał, że sprawę należy rozpatrzyć na podstawie przepisów RODO, a nie ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, ze względu na to, iż przekazanie, w ramach odpowiedzi na wniosek o udostępnienie informacji publicznej, dokumentacji z zakończonego postępowania przygotowawczego nie należy do zadań prokuratury, o których mowa w art. 3 ustawy z 28 stycznia 2016 r. Prawo o prokuraturze[230].

Prezes UODO w decyzji nie zakwestionował samego udostępnienia dokumentacji w trybie dostępu do informacji publicznej. Przy jej udostępnieniu muszą być jednak zachowane zasady z zakresu ochrony danych osobowych. Podkreślić należy, że rezultatem udostępnienia niezanonimizowanej dokumentacji było ujawnienie danych osobowych zawartych w jej treści osobie nieuprawnionej do ich otrzymania, czego konsekwencją było powstanie naruszenia ochrony danych osobowych.

Co ważne, w związku z odmową wszczęcia śledztwa w tym zakresie przez Prokuraturę Rejonową w Z. (…) administrator uznał, że nie doszło do naruszenia ochrony danych osobowych. Administrator nie przedstawił jednak żadnej analizy w tym zakresie. Nie udokumentował, że przeprowadził analizę ryzyka naruszenia praw lub wolności osób fizycznych objętych przedmiotowym naruszeniem ochrony danych osobowych, której wynik uprawniałyby go do stwierdzenia, że w prokuraturze rozważano, czy doszło do naruszenia ochrony danych osobowych, skutkującego koniecznością zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych oraz osób, których incydent dotyczył. Administrator uznał, że konieczność taka nie zachodziła.

Organ w decyzji podkreślił, że odmowa wszczęcia postępowania nie może stanowić podstawy do przyjęcia, że w związku z ww. zdarzeniem nie doszło do naruszenia ochrony

[229] DKN.5131.45.2022.
[230] Dz. U. z 2024 r. poz. 390.

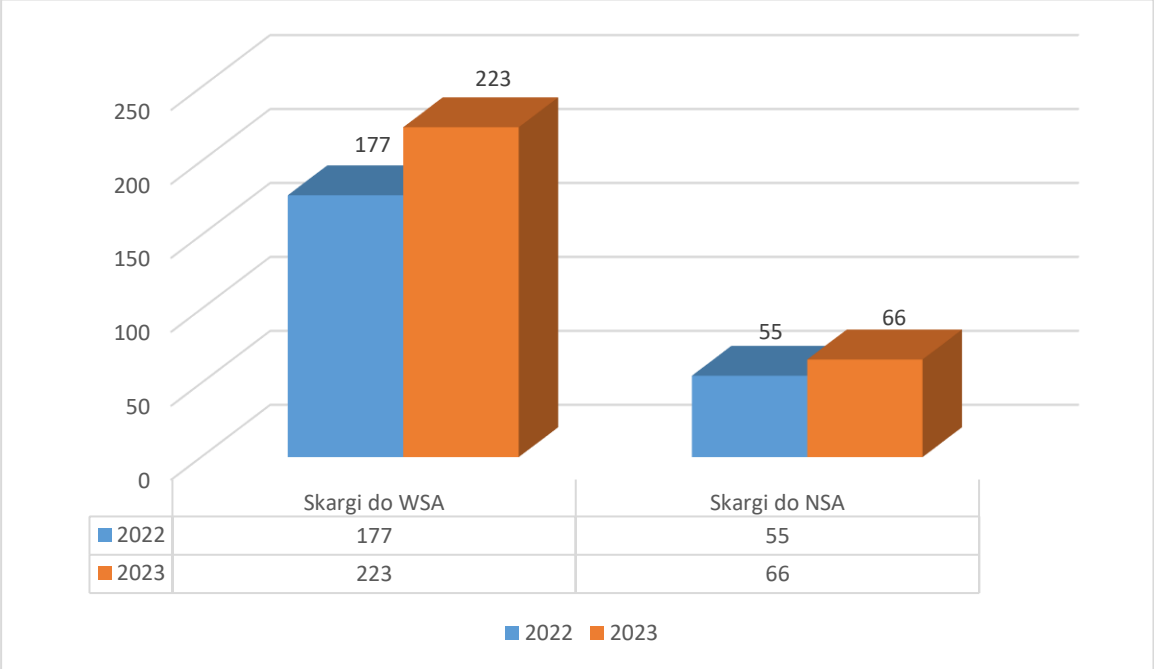
danych osobowych i nie może zastąpić rzetelnie przeprowadzonej analizy ryzyka naruszenia praw lub wolności osób fizycznych. Ocena dokonana przez Prokuraturę Rejonową w Z. została bowiem oparta na przepisach prawa karnego, tymczasem ocena czy wystąpiło naruszenie ochrony danych osobowych i czy związane jest ono z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, musi być przeprowadzona na gruncie przepisów RODO.

W przedmiotowej sprawie Prezes UODO stwierdził, że administrator nie przeprowadził oceny ryzyka naruszenia praw lub wolności osób fizycznych w związku z zaistniałym naruszeniem ochrony danych osobowych opartej o obiektywne kryteria, a także nie wykazał zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 6 listopada 2023 r.[231] utrzymał ww. decyzję w mocy.

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

W roku 2023 odnotowano wzrost liczby skarg wniesionych na decyzje organu do Wojewódzkiego Sądu Administracyjnego w Warszawie. W analizowanym roku skarga taka została wniesiona w 223 przypadkach, a zatem nastąpił wzrost w porównaniu z rokiem 2022, kiedy to odnotowano 177 takich skarg. Wzrosła także zaskarżalność wyroków wydanych przez Wojewódzki Sąd Administracyjny w Warszawie w sprawach decyzji Prezesa Urzędu Ochrony Danych Osobowych wydanych w sprawach skargowych. Takich skarg do Naczelnego Sądu Administracyjnego w roku 2023 wniesiono 66, a w roku 2022 – 55.



[231] Sygn. akt II SA/Wa 996/23.

Wykres 15: Decyzje wydane w postępowaniach skargowych, zaskarżone do WSA i skargi do NSA w sprawach wyroków WSA dotyczących decyzji wydanych przez Prezesa UODO w latach 2022–2023

Wyroki dotyczące przetwarzania danych osobowych klientów banków, po wygaśnięciu zobowiązania wobec banku

W roku 2023 Wojewódzki Sąd Administracyjny w Warszawie (WSA) rozstrzygał w sprawie skarg na decyzje Prezesa UODO, które dotyczyły przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego.

WSA w **wyroku z 14 kwietnia 2023 r.**[232] podzielił stanowisko organu nadzorczego, przyjęte w przedmiocie oceny przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego. Sąd uznał, że interpretowanie obowiązku poinformowania podmiotu danych, wynikającego z ww. przepisu, wyłącznie w oparciu o przepisy K.c. stanowi nieprawidłową wykładnię ww. przepisu. Zdaniem sądu prawidłowa wykładnia zawartego w art. 105a ust. 3 Prawa bankowego zwrotu „poinformowania tej osoby" winna uwzględnić nie tylko treść normy zawartej w art. 61 § 1 K.c., ale także tę część normy zawartej w art. 105a ust. 3 ustawy – Prawo bankowe, która ustanawia dodatkowy trzydziestodniowy termin na wykonanie zobowiązania. Jak wyjaśnił w dalszej części uzasadnienia wyroku sąd, konstrukcja przyjęta w art. 61 § 1 zdanie pierwsze K.c. odpowiada tzw. kwalifikowanej teorii doręczenia, która zadowala się dojściem oświadczenia woli do adresata w taki sposób, że miał on możliwość zapoznania się z jego treścią. Rozwiązanie to wiąże się z pewnym zagrożeniem dla osoby, której oświadczenie woli jest składane, zakłada bowiem możliwość zaistnienia sytuacji, w których oświadczenie to zostanie uznane za złożone, z czym częstokroć będą związane istotne skutki prawne, choć jego adresat nie wiedział o tym oświadczeniu albo nie znał jego treści. Sąd wskazał, że nadanie powiadomienia, o którym mowa w art. 105a ust. 3 ustawy – Prawo bankowe, listem poleconym nie pozwala – w okolicznościach badanej sprawy – na ustalenie początku biegu wskazanego terminu poinformowania. Skoro to bank wywodzi skutki prawne z powiadomienia uczestnika o zamiarze przetwarzania jego danych osobowych, stanowiących tajemnicę bankową, bez jego zgody, to musi wykazać, że bezskutecznie upłynęło 30 dni od daty poinformowania go o tym zamiarze. Wykazanie tej okoliczności wymaga jednak – co oczywiste – wykazania początku biegu owego trzydziestodniowego terminu.

Wyrokiem z 16 maja 2023 r.[233] WSA oddalił skargę na decyzję Prezesa UODO, uznając, że przetwarzanie danych osobowych przez uczestnika postępowania nie znajdowało oparcia w art. 105a ust. 3 *in fine* Prawa bankowego, z którego wynika, że warunkiem dopuszczalności przetwarzania informacji o kliencie, będącym osobą fizyczną, po wygaśnięciu zobowiązania jest upływ co najmniej 30 dni od poinformowania tej osoby przez bank o zamiarze przetwarzania tych informacji. Niewystarczające zdaniem sądu było przedstawienie skanu oświadczenia, zawierającego ww. informację o zamiarze przetwarzania oraz fragmentu elektronicznej książki nadawczej w przypadku przesyłki

[232] Sygn. akt II SA/Wa 2198/22.
[233] Sygn. akt II SA/Wa 1696/22.

nierejestrowanej. W ocenie sądu dokument ten nie pozwala stwierdzić, że bank poinformował (umożliwił zapoznanie się z informacją w zwykłym biegu zdarzeń) dłużnika o zamiarze przetwarzania jego danych osobowych, oraz ustalić, kiedy rozpoczął bieg termin trzydziestu dni, w którym uczestnik postępowania mógł uchylić się od negatywnych konsekwencji. Opisany wyrok jest prawomocny.

Wyrok w sprawie decyzji dotyczącej udostępnienia numeru tablicy rejestracyjnej pojazdu podczas obrad sesji rady miasta

W 2023 r. **wyrokiem z 6 października 2023 r.**[234] WSA w Warszawie oddalił skargę na pkt 1 decyzji Prezesa UODO, w którym organ udzielił upomnienia prezydentowi za udostępnienie numeru tablicy rejestracyjnej pojazdu skarżącego (osoby pełniącej funkcję publiczną) podczas obrad sesji rady miasta. Sąd podzielił stanowisko organu nadzorczego, że numer tablicy rejestracyjnej skarżącego stanowi w niniejszym postępowaniu jego dane osobowe stwierdzając, że co do zasady nie jest możliwe w sposób prosty i łatwy powiązać numer rejestracyjny pojazdu z konkretną osobą – właściciela (lub posiadacza) pojazdu, jednak w omawianej sprawie ujawnienie numeru rejestracyjnego samochodu skarżącego nastąpiło w sytuacji, gdy ujawnione zostały także jego dane w postaci imienia i nazwiska oraz wizerunku. Możliwa zatem była identyfikacja właściciela samochodu (posiadacza) bez użycia nadzwyczajnych środków, dostępów do baz czy rejestrów. W przypadku zarejestrowanym w tej sprawie numer rejestracyjny samochodu w połączeniu z innymi danymi osobowymi (imieniem i nazwiskiem skarżącego i jego wizerunkiem) pozwalał na identyfikację osoby właściciela/posiadacza. Wyżej wymieniony wyrok jest prawomocny.

Wyrok w sprawie decyzji dotyczącej udostępnienia danych osobowych przez komornika w skierowanym do byłego pracodawcy (dłużnika wierzytelności) zawiadomieniu o zajęciu wierzytelności

Prawomocnym **wyrokiem z 24 października 2022 r.**[235] WSA w Warszawie oddalił skargę na decyzję Prezesa UODO, odmawiającą uwzględnienia wniosku skarżącego w sprawie skargi na udostępnienie przez komornika danych osobowych skarżącego byłemu pracodawcy w skierowanym do byłego pracodawcy zawiadomieniu o zajęciu wierzytelności. Sąd podzielił stanowisko organu nadzorczego, uznając, że komornik przetwarzał dane osobowe skarżącego zgodnie z art. 6 ust. 1 lit. c) RODO, tj. dla potrzeb prowadzonej egzekucji – w celu wypełnienia ciążącego na nim obowiązku prawnego. Dane osobowe przekazane zostały byłemu pracodawcy wobec ustalenia przez komornika, że jest on dłużnikiem wierzytelności i w celu przeprowadzenia jej zajęcia. Sąd (podobnie jak organ nadzorczy) wskazał, że okoliczność, iż na dzień dokonania zajęcia skierowanego do dłużnika wierzytelności (byłego pracodawcy skarżącego) – skarżący nie był jego pracownikiem, nie może przesądzać o naruszeniu przez komornika przepisów o ochronie danych osobowych. Sąd wskazał, że żaden przepis prawa nie zobowiązuje komornika do działania polegającego na obowiązku zweryfikowania, czy dana osoba lub podmiot są dłużnikami wierzytelności. Doręczenie byłemu pracodawcy zawiadomienia o zajęciu wierzytelności skarżącego w momencie, gdy skarżący nie był już jego pracownikiem, odniosło jedynie ten skutek, że nie doszło do zajęcia jakiejkolwiek wierzytelności.

[234] Sygn. akt II SA/Wa 446/23.
[235] Sygn. akt II SA/Wa 355/22.

Wyrok w sprawie decyzji dotyczącej przetwarzania danych osobowych za pomocą systemu monitoringu wizyjnego zainstalowanego w altanach śmietnikowych

Wyrokiem z 23 stycznia 2023 r.[236] WSA w Warszawie oddalił skargę na decyzję Prezesa UODO, w której organ nakazał wspólnocie mieszkaniowej usunięcie danych osobowych skarżącego w zakresie jego wizerunku z nagrań zarejestrowanych przez system monitoringu wizyjnego zainstalowany w altanach śmietnikowych oraz zaprzestanie pozyskiwania danych osobowych skarżącego za pomocą systemu monitoringu wizyjnego zainstalowanego w altanach śmietnikowych będących w zasobach wspólnoty. Sąd podzielił stanowisko organu nadzorczego, uznając, że wspólnota nie wykazała, aby wystąpiły przesłanki pozwalające na przetwarzanie danych osobowych poprzez rejestrowanie wizerunku skarżącego za pomocą monitoringu wizyjnego zainstalowanego w altanach śmietnikowych zgodnie z art. 6 ust. 1 lit. f) RODO, tj. aby przetwarzanie danych osobowych w ww. sposób było niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, wskazując jedynie na trudności w wyegzekwowaniu prawidłowej segregacji odpadów. Sąd podkreślił, że wspólnota mieszkaniowa, jako administrator, winna była uwzględnić, w jakim stopniu monitoring wpływa na interesy, podstawowe prawa i wolności osób fizycznych i czy powoduje on naruszenia lub wywołuje negatywne skutki dla praw osób, których dane dotyczą. Wyważanie interesów ma charakter obowiązkowy. Z jednej strony należy ocenić i z rozwagą wyważyć podstawowe prawa i wolności, a z drugiej strony prawnie uzasadnione interesy administratora. Sąd, podobnie jak Prezes UODO, nie zgodził się ze wspólnotą mieszkaniową, aby potrzeba wyegzekwowania poprawnej segregacji odpadów, w tym w szczególności względy finansowe, które stały się główną przyczyną montażu monitoringu wizyjnego w altanach śmietnikowych znajdujących się w zasobach wspólnoty mieszkaniowej, miała charakter nadrzędny wobec podstawowych praw i wolności osób, których dane dotyczą, jakimi niewątpliwie są prawo do prywatności i ochrona wizerunku. Omówiony w tym miejscu wyrok jest prawomocny.

Wyrok w sprawie decyzji dotyczącej udostępnienia danych osobowych na nagraniu z sesji rady miejskiej

W 2023 r. do UODO wpłynął **prawomocny wyrok WSA w Warszawie z 18 października 2021 r.**[237]**,** w którym WSA w Warszawie oddalił skargę na decyzję Prezesa UODO, nakazującą burmistrzowi usunięcie z nagrania z sesji rady miejskiej, zamieszczonego na stronie internetowej, danych osobowych skarżącego w zakresie nazwiska[238]. W toku przeprowadzonego postępowania Prezes UODO ustalił, że w porządku obrad sesji rady miejskiej uwzględniony został punkt dotyczący złożenia przez burmistrza sprawozdania z działalności między sesjami. Burmistrz w swoim sprawozdaniu wielokrotnie odniósł się do kwestii mających wpływ na wydatkowanie środków gminnych. Burmistrz zapoznał też członków rady miejskiej z wynikiem postępowań sądowych, których gmina oraz skarżący byli stronami, a w których to postępowaniach gmina została pozwana przez skarżącego o odszkodowanie i zadośćuczynienie. Podczas wystąpienia burmistrz

[236] Sygn. akt II SA/Wa 763/22.
[237] II SA/Wa 1944/21.
[238] ZWOS.440.5319.2019.

udostępnił dane osobowe skarżącego w zakresie nazwiska oraz treści rozstrzygnięć zapadłych w ww. postępowaniach sądowych. Nagranie z sesji rady miejskiej zostało udostępnione na stronie internetowej. Sąd podzielił stanowisko organu nadzorczego, uznając, że Prezes UODO prawidłowo stwierdził, iż w niniejszej sprawie wyłączenia z ustawy o dostępie do informacji publicznej nie występują, albowiem dane osobowe ujawnione w nagraniu nie dotyczą osoby pełniącej funkcję publiczną, jak również skarżący nie zrezygnował z przysługującego mu prawa do prywatności. Ponadto ww. sąd podniósł, zgadzając się z Prezesem UODO, iż wniosku takiego nie można wysnuć z samego charakteru działalności zawodowej, ani z aktywności skarżącego w stosunku do organów gminy. Sąd zauważył, że sprawa poruszana przez burmistrza w jego wystąpieniu na sesji rady miejskiej ma charakter cywilny (powództwo o zapłatę odszkodowania) niezwiązany z działalnością zawodową skarżącego, ani z jego wnioskami o dostęp do informacji publicznej. W ocenie sądu fakt, że ww. jest osobą powszechnie znaną w środowisku lokalnym nie oznacza, że owo środowisko jest uprawnione do zidentyfikowania skarżącego jako powoda w sprawie cywilnej przeciwko gminie i powzięcia wiedzy o wysokości żądanych czy zasądzonych kwot. Jednocześnie sąd wyjaśnił, że definicja osoby publicznej, która funkcjonuje w orzecznictwie nie pozwala uznać za osobę pełniącą tę funkcję dziennikarza prowadzącego portal internetowy, czy też osobę prowadzącą działalność gospodarczą, niezwiązaną z wydatkowaniem środków publicznych. Zdaniem sądu fakt, że skarżący informował opinię publiczną o kierowanych przez niego do burmistrza wnioskach w trybie dostępu do informacji publicznej, a także wnosił o odczytywanie jego wniosków na sesji rady miejskiej wraz z podaniem imienia i nazwiska, nie może być interpretowany rozszerzająco, poprzez przyjęcie, iż skarżący wyraził zgodę na udzielanie informacji o prowadzonych z jego udziałem postępowaniach sądowych o odszkodowanie, kwotach sporu oraz wynikach tych postępowań, które mają charakter cywilny. Wyrok ten został zaskarżony do NSA przez burmistrza.

Wyrokiem z 13 lipca 2023 r.[239] NSA oddalił skargę kasacyjną. W uzasadnieniu wyroku NSA wskazał, że użytego w art. 5 ust. 2 ustawy o dostępie do informacji publicznej[240] pojęcia osoby pełniącej funkcję publiczną należy poszukiwać na gruncie obowiązującego systemu prawa oraz że do kategorii tej zaliczyć należy osoby pozostające formalnie w strukturach aparatu państwa, wykonujące jego zadania i decydujące w określonym formalnie zakresie o życiu publicznym. Powyższe oznacza, że przepis art. 5 ust. 2 ustawy o dostępie do informacji publicznej wyklucza uznanie za osoby pełniące funkcje publiczne takie osoby, które są znane publicznie (w skali całego kraju lub określonej wspólnoty regionalnej lub lokalnej), lecz pozostają poza strukturami aparatu państwa. Są to w rozumieniu ustawy o dostępie do informacji publicznej osoby prywatne. Naczelny Sąd Administracyjny podkreślił, że jeśli określona osoba nie pełni funkcji publicznej, to informacje publiczne odnoszące się do niej i zawierające jej dane osobowe podlegają ochronie ze względu na konieczność ochrony jej prawa do prywatności, chyba że osoba zrezygnuje z przysługującego jej prawa. Zgodnie ze stanowiskiem NSA, wykładnia językowa art. 5 ust. 2 ustawy o dostępie do informacji publicznej, jak również wykładnia systemowa, w tym zasady stosowane do wyrażenia zgody na przetwarzanie danych osobowych wynikające z art. 6 ust. 1 lit. a) oraz art. 4 pkt 11 RODO, wskazują, że

[239] Sygn. akt III OSK 595/22.
[240] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).

rezygnacja z prawa do prywatności musi mieć charakter: dobrowolny, konkretny, świadomy i przyjmujący postać jednoznacznego okazania woli przez osobę, która rezygnuje z prawa do prywatności, w formie oświadczenia lub wyraźnego działania potwierdzającego rezygnację z prawa do prywatności. Wynika z tego, iż rezygnacji z prawa do prywatności nie można ani domniemywać, ani ustalać na podstawie całokształtu działań i oświadczeń danej osoby fizycznej, niepozostających w związku z kwestią udostępnienia jej danych osobowych w trybie dostępu do informacji publicznej. Za rezygnację z prawa do prywatności można uznać zatem jednoznaczne oświadczenie woli danej osoby w tym zakresie lub inne wyraźne działanie potwierdzające rezygnację z prawa do prywatności, lecz pozostające w niewątpliwym związku z zamiarem organu upublicznienia danych osobowych konkretnej osoby – w trybie przepisów ustawy o dostępie do informacji publicznej.

Wyrok w sprawie decyzji dotyczącej przechowywania w aktach osobowych pracownika danych osobowych zawartych w zbędnych dokumentach

W dniu 10 sierpnia 2023 r. WSA w Warszawie wydał wyrok[241], w którym oddalił skargę na decyzję Prezesa UODO, uznając, że organ prawidłowo ustalił okoliczności faktyczne i zebrał materiał dowodowy w sprawie dotyczącej administratora, który naruszył zasadę minimalizacji danych poprzez gromadzenie w aktach osobowych skarżącego dokumentów, które w istocie są zbędne do osiągnięcia celu przetwarzania. Prezes UODO zasadnie zatem przyjął, że administrator naruszył art. 6 ust. 1 w zw. z art. 5 ust. 1 lit. a) RODO poprzez bezprawne przechowywanie w aktach osobowych dokumentów zawierających dane skarżącego, które dotyczyły wniosku o zwiększenie wynagrodzenia, i udzielił w tym zakresie upomnienia. Organ, w ramach zarzutu ujawnienia danych skarżącego znajdujących się na kopercie przesyłki pocztowej zaadresowanej na adres domowy skarżącego nadanej przez administratora za pośrednictwem Poczty Polskiej, zawierającej imię, nazwisko, adres oraz informacje o stanowisku służbowym i miejscu pracy, prawidłowo stwierdził, że naruszało to zasadę minimalizacji danych, określoną w art. 6 ust. 1 w zw. z art. 5 ust. 1 lit. c) RODO, i nie było niezbędne do prawidłowego doręczenia przesyłki skarżącemu. W efekcie poczynionych ustaleń organ udzielił w tym zakresie upomnienia.

Jak podkreślił sąd, organ udzielając upomnienia za wykazane uchybienia, nie naruszył prawa, a zastosowany instrument prawny jest adekwatny do wagi stwierdzonych naruszeń. Organ należycie wykazał także, dlaczego poza zakresem rozpatrywanej sprawy pozostały inne zarzuty – podnoszone przez skarżącego w jego skardze wobec administratora – dotyczące: sposobu postępowania z materiałami włączanymi i wyłączanymi z akt osobowych, w tym notatkami służbowymi, dokumentami obsługi kadrowej jego akt osobowych, braku informowania go o danych czynnościach dokonywanych w jego aktach osobowych oraz dostępu do tych akt.

Organ prawidłowo ponadto przyjął, że nie jest organem kompetentnym do badania i oceny tych kwestii, ponieważ nie wynika to z przepisów RODO oraz ustawy o ochronie danych osobowych.

[241] Sygn. akt II SA/Wa 287/23.

Wyrok w sprawie decyzji dotyczącej udostępnienia szczególnych kategorii danych pracownika innym osobom

W zapadłym w dniu **28 grudnia 2023 r.**[242] **wyroku** WSA w Warszawie oddalił skargę na decyzję Prezesa UODO, mocą której organ w pkt 1 udzielił jednej ze spółek upomnienia za naruszenie art. 9 ust. 1 oraz art. 5 ust. 1 lit. a) RODO, polegające na udostępnieniu szczególnych kategorii danych osobowych skarżącej – w zakresie informacji o wystawionym zwolnieniu lekarskim z powodu ciąży przez kierownika sklepu na rzecz kierownika sprzedaży produktów świeżych i innych pracowników.

Głównym zarzutem spółki wobec organu nadzorczego było błędne (w ocenie spółki) uznanie przez Prezesa UODO, iż osoba, której bezpośredni przełożony skarżącej (kierownik sklepu) udostępnił dane skarżącej (kierownikowi sprzedaży produktów świeżych), nie była uprawniona do ich przetwarzania, podczas gdy w ocenie spółki, zarówno na gruncie obowiązków tej osoby jako reprezentanta spółki oraz ze względu na pozycję w strukturze organizacyjnej wraz z powierzonym przez spółkę kierownikowi sprzedaży produktów świeżych zakresem obowiązków, jak i z treści upoważnienia, wynikało, że zostały spełnione wszelkie przesłanki prawidłowego upoważnienia do przetwarzania danych osobowych skarżącej. Zarzut spółki dotyczył przede wszystkim naruszenia art. 9 ust. 1 RODO w zw. z art. 9 ust. 2 lit. b) oraz art. 5 ust. 1 lit. a) RODO.

Sąd natomiast podzielił stanowisko organu nadzorczego, zgodnie z którym spółka nie miała podstaw prawnych do przetwarzania, polegającego na udostępnieniu szczególnych kategorii danych skarżącej w sposób, w jaki to nastąpiło, tj. na rzecz kierownika sprzedaży produktów świeżych. Sąd uznał, zgodnie ze stanowiskiem organu, że nie można przyjąć, aby niezbędne było informowanie przez przełożonego skarżącej, tj. kierownika sklepu, zarówno pracownika zastępującego skarżącą o przyczynach jej zwolnienia lekarskiego, czy też innych pracowników niebędących bezpośrednimi przełożonymi skarżącej. Sąd uznał, że organ prawidłowo ustalił, na podstawie nadesłanego przez spółkę zakresu obowiązków kierownika sprzedaży produktów świeżych, że nie była ona przełożoną skarżącej ani kierownika sklepu, ani też że do jej zadań i kompetencji nie należały sprawy kadrowe związane z nadzorem nad pracą pracowników sklepu. Niezasadne okazały się zatem zarzuty spółki naruszenia przepisów prawa materialnego. Sąd uznał, że pracodawca może przetwarzać szczególne kategorie danych osobowych swoich pracowników, jednak dane w zakresie zdrowia podlegają rygorom z art. 9 ust. 2 RODO. Sąd nie uwzględnił żadnych podniesionych w skardze zarzutów naruszenia art. 7, art. 77 § 1, art. 80 K.p.a., natomiast postępowanie administracyjne, zdaniem sądu, było prowadzone rzetelnie, a strona miała możliwość złożenia obszernych wyjaśnień. Sąd uznał, że uzasadnienie decyzji z kolei zawierało wszelkie wymagane prawem elementy, a w szczególności wyjaśniono w sposób obszerny podstawę prawną rozstrzygnięcia, przytoczono kluczowe dla sprawy przepisy, przedstawiono stan faktyczny sprawy oraz dokonano subsumcji tego stanu faktycznego pod określone normy prawne. W ocenie sądu rozstrzygnięcie zawarte w zaskarżonej decyzji było zrozumiałe, jasne i odpowiadało wymaganiom prawa, wbrew zarzutom skargi.

Wyrok w sprawie monitoringu prowadzonego przez osoby prywatne i związanego z tym obowiązku informacyjnego, o którym mowa w art. 13 RODO

[242] Sygn. akt II SA/Wa 714/23.

W orzeczeniu WSA w Warszawie z 15 marca 2023 r.[243] poruszono kwestię monitoringu prowadzonego przez osoby prywatne i związanego z tym obowiązku informacyjnego, o którym mowa w art. 13 RODO.

W trakcie przeprowadzonego postępowania administracyjnego Prezes UODO ustalił, że zasięg monitoringu wizyjnego należącego do skarżonych sąsiadów wykracza poza ich nieruchomość, gdyż monitoring wizyjny obejmuje swym zasięgiem przestrzeń wspólną (współwłasność). Wskazana przez sąsiadów potrzeba zapewnienia bezpieczeństwa swojego oraz dzieci jest uzasadnieniem dla wykonywania monitoringu wizyjnego ograniczonego swoim zasięgiem wyłącznie do terenu nieruchomości będącej ich wyłączną własnością. Zasięgiem monitoringu objęta była natomiast również część wspólna, na której mogą przebywać wszyscy współwłaściciele. Prezes UODO nakazał zaprzestania przetwarzania danych zebranych za pomocą monitoringu prowadzonego na obszarze obejmującym swym zasięgiem część nieruchomości wspólnej. W zakresie monitoringu niewykraczającego poza obręb wyłącznej własności skarżonych organ odmówił uwzględnienia skargi. Jednocześnie organ udzielił upomnienia za niespełnienie obowiązku informacyjnego. Skarżeni sąsiedzi zaskarżyli decyzję organu.

Sąd uznał za prawidłową argumentację organu, że dane osobowe pozyskane za pomocą zainstalowanego przez skarżonych monitoringu, obejmującego swym zasięgiem nieruchomość wspólną, nie są przetwarzane w celach wyłącznie czysto osobistych[244]. Ponadto sąd zgodził się z organem, że samo poinformowanie o zainstalowaniu monitoringu i jego zasięgu nie stanowi spełnienia obowiązku informacyjnego, o którym mowa w art. 13 RODO, jeżeli nie zostaną zawarte pozostałe informacje wymienione w treści tego przepisu. Na obowiązek poinformowania o przetwarzaniu nie wpływa fakt ograniczenia czasowego gromadzenia danych pozyskanych przez monitoring. Jak podkreślił sąd, przechowywanie danych jest również ich przetwarzaniem. Tym samym należy zauważyć, że monitoring przydomowy, jako taki, stanowi formę przetwarzania danych osobowych (wizerunku), a co za tym idzie – powinien być zgodny z przepisami o ochronie danych osobowych. Decyzja o jego stosowaniu nie powinna ograniczać się wyłącznie do wyboru sprzętu czy oprogramowania, ale również uwzględniać analizę podstawy prawnej i celu jego prowadzenia, a przede wszystkim refleksję o prawie drugiego człowieka do prywatności. Współwłasność nad nieruchomością nie oznacza, że przetwarzanie danych osobowych za pomocą monitoringu jest dozwolone bez ograniczeń i bez poszanowania praw innych współwłaścicieli.

Wyrok w sprawie uznania numeru telefonu za dane osobowe

W dniu **9 maja 2023 r.**[245] **zapadł wyrok WSA w Warszawie,** w którym sąd podzielił stanowisko Prezesa UODO w zakresie dotyczącym uznania numeru telefonu za dane osobowe – niezależnie od tego, czy podmiot posiada dodatkowe dane lub informacje identyfikujące. Jest to kolejne orzeczenie potwierdzające to stanowisko, uprzednio sąd wypowiadał się także w tej materii w wyroku wydanym w 2022 r.[246]

[243] Sygn. akt II SA/Wa 1340/22.
[244] Zgodnie z art. 2 ust. 2 lit. c) RODO rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze.
[245] II SA/Wa 2256/22.
[246] Wyrok WSA z 22.12.2022 r. sygn. akt II SA/Wa 981/22.

W niniejszej sprawie numer telefonu był wykorzystywany przez spółkę do kontaktu z posiadaczem tego numeru w celu zaoferowania mu usług lub produktów. Organ uznał, że skarżący nie mógł spodziewać się pozyskania ani przetwarzania jego danych osobowych do celów marketingowych, nie zachodziło bowiem o żadne powiązanie pomiędzy nim a spółką. Ze względu na usunięcie danych osobowych skarżącego Prezes UODO upomniał spółkę za stwierdzone naruszenie. Spółka zaskarżyła ww. decyzję, twierdząc, że numer telefonu nie stanowi danych osobowych, a zatem do przetwarzania tych informacji nie stosuje się przepisów RODO.

Sąd podzielił stanowisko[247], zgodnie z którym w przypadkach, gdy celem przetwarzania jest identyfikacja osób, można przypuszczać, że administratorzy lub inne zainteresowane osoby dysponują sposobami, jakimi można się posłużyć w celu zidentyfikowania osoby, której dane dotyczą, także wtedy, gdy przetwarzają jedynie niekompletne informacje bez jakiejkolwiek wzmianki o nazwisku lub innym bezpośrednim czynniku identyfikującym. Sąd wskazał, że zidentyfikowanie osoby fizycznej nie musi polegać na określeniu jej imienia i nazwiska, a wystarczające jest oznaczenie danej osoby w sposób umożliwiający wywieranie na nią określonego wpływu. Taką możliwość daje numer telefonu osoby fizycznej, nawet gdy podmiot, który jest w jego posiadaniu, nie dysponuje innymi danymi identyfikującymi tę osobę lub rozsądnie prawdopodobnym do wykorzystania sposobem uzyskania takich danych. Numer telefonu osoby fizycznej stanowi niepowtarzalną kombinację cyfr, która jest do tej osoby przypisana, i odróżnia go od innych. Sąd zauważył, że na gruncie Prawa telekomunikacyjnego[248] numer telefonu jest silnie związany z osobą fizyczną (abonentem). Podzielił on stanowisko organu, że wykonywanie połączeń telefonicznych w celu zaproszenia do skorzystania z usług oferowanych przez kontrahentów spółki jest marketingiem bezpośrednim, ponieważ jest przekazaniem informacji w celu reakcji ze strony konsumenta w postaci skorzystania z tych usług i w szczególności ma na celu ich promocję, a następnie zakup. Nie ma przy tym znaczenia, że usługa, do skorzystania z której zachęcała spółka, nie była oferowana przez nią, lecz przez jej kontrahenta.

Sąd podzielił zdanie Prezesa UODO, że spółka przetwarzała dane osobowe skarżącego bez podstawy prawnej. Skoro używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego dopuszczalne jest pod warunkiem uprzedniego wyrażenia zgody na użycie takiej formy komunikacji przez abonenta lub użytkownika końcowego, to brak takiej zgody ze strony uczestnika postępowania powoduje, że nie mógł on spodziewać się, że może nastąpić przetwarzanie jego danej osobowej w postaci numeru telefonu do tych celów[249]. Tym samym spółka nie była uprawniona do przetwarzania danych osobowych skarżącego w zakresie jego numeru telefonu art. 6 ust. 1 lit. f) RODO. W tym przypadku nadrzędny charakter nad prawnie uzasadnionym interesem spółki ma prawo do prywatności.

[247] Opinia nr 4/2007 Grupy Roboczej ds. ochrony danych, powołanej na mocy art. 29 dyrektywy 95/46/WE. w sprawie pojęcia danych osobowych.
[248] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34).
[249] Patrz: art. 172 ust. 1 w zw. z art. 174 Prawa telekomunikacyjnego.

Potwierdzone przez orzecznictwo sądów administracyjnych stanowisko Prezesa UODO niewątpliwie wzmocni prawo do ochrony danych osobowych obywateli przed przetwarzaniem ich danych w celach marketingowych bez podstawy prawnej.

8. Uprzednie konsultacje

Do zadań organu nadzorczego realizowanych przez Wydział Współpracy z Inspektorami Ochrony Danych należy udzielanie administratorom zaleceń w ramach procedury uprzednich konsultacji, która uregulowana jest w art. 36 RODO, art. 57 ustawy o ochronie danych osobowych, a także w art. 38 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[250]*. Jak wyjaśniono w motywie 94 RODO, z organem nadzorczym należy się skonsultować w ramach ww. procedury, jeżeli ocena skutków dla ochrony danych wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia. Wobec tego celem uprzednich konsultacji jest udzielenie administratorowi pomocy w znalezieniu środków umożliwiających zmniejszenie, do dopuszczalnego poziomu, ryzyka zdiagnozowanego podczas oceny skutków dla ochrony danych jako wysokie*.

W omawianym okresie sprawozdawczym do UODO wpłynęły **3 wnioski o przeprowadzenie uprzednich konsultacji.** W poprzednim roku wpłynęło ich 7, w 2021 i 2020 r. – po 3, w 2019 r. – 5, a w 2018 r. – 2. Wynika z tego, że administratorzy w niewielkim zakresie korzystają z tego uprawnienia. Powodem może być m.in. to, iż złożenie takiego wniosku poprzedzone musi być dokonaniem przez administratora wnikliwej analizy całego planowanego procesu przetwarzania. Zanim bowiem administrator przystąpi do oceny ryzyka, będącego elementem oceny skutków dla ochrony danych, powinien w pierwszej kolejności prawidłowo ustalić i ocenić zagadnienia o podstawowym znaczeniu dla zgodności z prawem przetwarzania danych osobowych, a w szczególności status wnioskodawcy w procesie przetwarzania, kwalifikację informacji jako danych osobowych oraz istnienie podstawy prawnej do prowadzenia określonych operacji przetwarzania danych osobowych.

Wymienione zagadnienia mają pierwszoplanowe znaczenie i wymagają uprzedniej prawidłowej oceny. Innymi słowy, ocena skutków dla ochrony danych jest dalszym etapem, do którego można przejść dopiero wtedy, gdy określono, jaki podmiot w konkretnej sytuacji ustala cele i sposoby przetwarzania danych osobowych, a tym samym ponosi odpowiedzialność za planowane przetwarzanie, oraz czy przetwarzanie danych osobowych przez ten podmiot jest dopuszczalne w świetle przesłanek legalności przetwarzania danych osobowych.

Wniesione w 2023 r. wnioski o uprzednie konsultacje nie zostały poprzedzone przez administratorów analizami w zakresie powyższych zagadnień, co spowodowało, że nie mogły zainicjować postępowania i udzielenia zaleceń. Podkreślenia wymaga zatem, że jeżeli np. brak jest podstawy prawnej do przetwarzania, to planowane przetwarzanie nie

[250] Dz. U. z 2023 r. poz. 1206.

może się odbyć i ani ocena skutków dla ochrony danych, ani procedura uprzednich konsultacji nie będą rozwiązaniem pozwalającym na wyeliminowanie tej przeszkody.

Jako przykład takiej sytuacji można wskazać **wniosek o udzielenie uprzednich konsultacji dotyczący wątpliwości w zakresie istnienia podstaw prawnych do udostępnienia danych osobowych.** W odpowiedzi organ nadzorczy wskazał, że tego rodzaju wątpliwości należy rozstrzygać na podstawie analizy właściwych przepisów prawa, określających kompetencje i uprawnienia danego podmiotu do pozyskania określonych danych, nie zaś w trybie uruchamianym na podstawie art. 36 RODO. Ponadto organ poinformował, że jeżeli wniosek o udostępnienie danych osobowych zawiera braki lub budzi wątpliwości, celowe jest zwrócenie się do wnioskodawcy o uzupełnienie lub wyjaśnienie tych braków, lub przedstawienie dodatkowych informacji pozwalających na pełną ocenę dopuszczalności udostępnienia danych w konkretnej sytuacji. Gdy o udostępnienie danych osobowych występuje podmiot realizujący zadania publiczne, powinien on w pierwszej kolejności wyraźnie wskazać przepisy uprawniające go do pozyskania danych. W przypadku zaś stwierdzenia braku podstawy prawnej do udostępnienia danych osobowych administrator nie powinien takich danych udostępnić.

Kolejny przykład dotyczy **wniosku o uprzednie konsultacje, którego złożenie nie zostało poprzedzone dokonaniem przez administratora oceny w zakresie istnienia podstawy prawnej do przetwarzania danych osobowych w celach i zakresie wskazanych w tym wniosku.** Wnioskodawca wskazał, że zamierza wprowadzić monitoring miejski. Jako cel zamierzonego przetwarzania podał bezpieczeństwo osób i mienia. Jednocześnie poinformował, że budowa systemu miejskiego monitoringu wizyjnego nastąpić ma w celu: prewencji, podniesienia stanu bezpieczeństwa mieszkańców i osób przebywających na terenie miasta, ograniczenia napadów, wybryków chuligańskich, kradzieży, niszczenia mienia, poprawy przestrzegania zasad ruchu drogowego, identyfikacji i możliwości wyciągnięcia konsekwencji wobec sprawców powyższych czynów. We wniosku wskazano, że monitoring będzie prowadzony na podstawie art. 9a ust. 1 ustawy z 8 marca 1990 r. o samorządzie gminnym. Zgodnie z brzmieniem tego przepisu gmina – w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej – może stosować środki techniczne umożliwiające rejestrację obrazu (monitoring) w obszarze przestrzeni publicznej, za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru, lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy lub jednostek organizacyjnych gminy, a także na terenie wokół takich nieruchomości i obiektów budowlanych, jeżeli jest to konieczne do zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej. Tymczasem z zawartego we wniosku opisu planowanego przetwarzania wynikało, że w ramach monitoringu nie będzie dochodziło jedynie do rejestracji obrazu, ale również do zastosowania innych funkcjonalności obejmujących analizę i selekcję danych oraz identyfikację, np. śledzenie pojazdów. Zauważyć należy, że działania te wykraczają poza uprawnienie gminy wskazane w powołanej przez administratora podstawie prawnej, tj. w art. 9a ust. 1 ustawy o samorządzie gminnym.

Z opisanych powyżej powodów **wniesione w 2023 r. wnioski nie mogły być procedowane w trybie uprzednich konsultacji.** Wobec tego organ nadzorczy – podobnie jak w latach poprzednich – informował wnioskodawców o nieudzieleniu konsultacji oraz przedstawiał obszerne wyjaśnienia dotyczące powodów ich nieudzielenia.

Złożenie wniosku o uprzednie konsultacje powinno poprzedzać przeprowadzenie przez administratora oceny skutków dla ochrony danych. Przy czym pogłębiona ocena ryzyka, jaką jest ocena skutków dla ochrony danych, nie powinna być przeprowadzona, jeśli administrator nie ma podstawy prawnej do przetwarzania danych osobowych w określonym celu. Czym innym jest bowiem ocena ryzyka związanego z przetwarzaniem danych, a czym innym formalna ocena zgodności przetwarzania z prawem.

Przedmiotem uprzednich konsultacji powinno być udzielenie administratorowi pomocy w znalezieniu środków służących zmniejszeniu, do dopuszczalnego poziomu, wysokiego ryzyka zdiagnozowanego podczas oceny skutków dla ochrony danych, nie zaś np. poszukiwanie podstawy prawnej dla określonego przetwarzania, czy też udzielanie odpowiedzi na pytania prawne.

Zauważyć zatem należy, że – pomimo podejmowanych działań informacyjnych UODO dotyczących korzystania przez administratorów z uprzednich konsultacji (np. przeznaczona uprzednim konsultacjom zakładka na stronie internetowej urzędu) – niewiele podmiotów decyduje się na korzystanie z tej formy wsparcia, a te, które decydują się na złożenie takiego wniosku, nieprawidłowo rozumieją cel tego narzędzia.

9. 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 podejmowania 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 zatwierdza kodeks postępowania w formie decyzji administracyjnej, o ile uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO.

Wraz z rozpoczęciem stosowania RODO wiele organizacji zainicjowało prace nad stworzeniem branżowych kodeksów postępowania. Złożone do organu nadzorczego wnioski o zatwierdzenie projektów kodeksów, ale też sygnały od inicjatyw, które rozpoczynają prace związane z opracowaniem tego mechanizmu rozliczalności, wskazują, że zarówno podmioty publiczne, jak i prywatne dostrzegają potrzebę oraz zalety korzystania z tego typu narzędzia, które pozwoli im wykazać rozliczalność, o której mowa w art. 5 ust. 2 RODO.

Kodeksy postępowania zatwierdzone przez organ nadzorczy

Organ nadzorczy 11 grudnia 2023 r. zatwierdził Kodeks postępowania dla sektora ochrony zdrowia przygotowany przez Polską Federację Szpitali[251]. Tego samego dnia odbyło się uroczyste wręczenie decyzji przedstawicielom wnioskodawcy – Polskiej Federacji Szpitali. Kodeks został opublikowany na stronie internetowej Urzędu Ochrony Danych Osobowych.

Nowe wnioski o zaopiniowanie kodeksów postępowania

W grudniu 2023 r. do organu nadzorczego wpłynął wniosek o zatwierdzenie Kodeksu postępowania i dobrych praktyk w zakresie ochrony danych osobowych w branży hotelarskiej (IGHP)[252]. Wnioskodawcą w tej sprawie była Izba Gospodarcza Hotelarstwa Polskiego. Obecnie trwa ocena wymogów formalnych tego kodeksu.

W analizowanym roku sprawozdawczym prowadzona była **współpraca organu nadzorczego z inicjatywami przygotowującymi projekty kodeksów postępowania**, **które nie złożyły jeszcze wniosków o ich zatwierdzenie.** W 2023 r. do Urzędu Ochrony Danych Osobowych zwróciło się środowisko organizacji sportowych z inicjatywą podjęcia prac nad Kodeksem ochrony danych dla branży sportowej[253]. W siedzibie UODO odbyło się spotkanie w sprawie tej inicjatywy[254].

Postępowania prowadzone w sprawie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone w latach wcześniejszych

W 2023 r. kontynuowano prace związane z:

1) zatwierdzeniem projektu Kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencje badawcze[255]. Wnioskodawca, tj. Organizacja Firm Badania Opinii i Rynku (OFBOR), przedstawił poprawioną wersję projektu kodeksu;
2) Kodeksem dla centrów handlowych Polskiej Rady Centrów Handlowych[256];
3) Kodeksem dla doradców podatkowych przygotowanym przez Krajową Izbę Doradców Podatkowych[257];
4) Kodeksem postępowania w sprawie przetwarzania danych osobowych dla celów badań naukowych przez biobanki w Polsce[258];
5) kolejną wersją projektu Kodeksu dla spółdzielni mieszkaniowych złożonego przez Związek Rewizyjny Spółdzielni Mieszkaniowych RP (postępowanie zostało umorzone ze względu na wycofanie wniosku[259]);

[251] ZAS.070.4.2018.
[252] DOL.4421.1.2023.
[253] DOL.023.213.2023.
[254] Informacja na ten temat została zamieszczona w „Biuletynie UODO” nr 4/06/23.
[255] DOL.4421.2.2020.
[256] DOL.4421.3.2020.
[257] DOL.4421.12.2020.
[258] DOL.4421.1.2021.
[259] ZAS.070.5.2019.

6) zatwierdzeniem Kodeksu postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego (postępowanie zostało umorzone ze względu na wycofanie wniosku[260]).

W 2023 r. rozpoczęto także prace nad projektem transgranicznego kodeksu ochrony danych osobowych dotyczącego badań klinicznych (*Code for Conduct Service Providers in Clinical Research[261]*). Tworzenie kodeksu koordynowane było przez francuski organ nadzorczy, zaś UODO aktywnie uczestniczył w kolejnych etapach projektu.

Kodeks, który jest właściwie przygotowany (co oznacza, że nie jest jedynie powtórzeniem przepisów RODO, tylko doprecyzowuje problemowe kwestie z uwzględnieniem specyfiki danej branży), przynosi wiele korzyści[262]. Administratorom i podmiotom przetwarzającym będącym członkami kodeksu ułatwia stosowanie przepisów i wypełnianie wielu obowiązków, wskazując właściwe rozwiązania w razie zaistnienia dylematów natury prawnej. Pomaga też odpowiednio organizować system ochrony danych osobowych w danej branży, podnosząc jego poziom. Jego wdrożenie jest korzystne nie tylko dla administratorów i podmiotów przetwarzających, ale również dla osób, których dane są przetwarzane, gdyż dodatkowo będą one mogły liczyć na zbliżony standard ochrony danych oraz obsługę w zakresie realizacji ich praw przez daną branżę.

10. 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.

Zaletą odpowiednio przygotowanego kodeksu jest nie tylko gwarancja pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy. Administratorzy mogą także liczyć na nadzór nad procesami przetwarzania danych osobowych przez niezależny podmiot monitorujący kodeks. Podmioty monitorujące w celu uzyskania akredytacji organu nadzorczego muszą wykazać swoją niezależność w stosunku do twórcy kodeksu oraz posiadanie odpowiednich: zasobów finansowych, personalnych, środków organizacyjnych i materialnych (technicznych). Szczegółowe wymagania w tym zakresie zostały opisane w Wymogach akredytacji podmiotów monitorujących kodeksy postępowania – przygotowanych przez Prezesa UODO. Natomiast kodeksy obejmujące podmioty sektora publicznego, choć nie podlegają obowiązkowi wskazania podmiotu monitorującego, to muszą zawierać skuteczny

[260] DOL.4421.1.2022.
[261] DOL.614.14.2023.
[262] W ocenie EROD kodeksy postępowania to dobrowolne narzędzia w zakresie rozliczalności, zawierające szczegółowe przepisy o ochronie danych w odniesieniu do kategorii administratorów i podmiotów przetwarzających. Mogą one stanowić użyteczne i skuteczne narzędzie w zakresie rozliczalności, zawierające szczegółowy opis najodpowiedniejszych, zgodnych z prawem i etycznych zbiorów zachowań w danym sektorze. Z punktu widzenia ochrony danych osobowych kodeksy mogą zatem funkcjonować jako zbiór instrukcji dla administratorów danych i podmiotów przetwarzających, którzy projektują oraz wdrażają zgodne z RODO czynności przetwarzania danych, nadających znaczenie operacyjne zasadom ochrony danych określonym w prawie europejskim i krajowym (pkt 7 Wytycznych EROD 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, wersja 2.0, 4 czerwca 2019 r.).

mechanizm monitorowania, o którym mowa w pkt 40 Wytycznych EROD 1/2019. Cel taki można osiągnąć poprzez dostosowanie obowiązujących mechanizmów audytów i kontroli w administracji publicznej, tak aby obejmowały one monitorowanie kodeksu.

W 2020 r. organ nadzorczy przygotował projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Po przekazaniu dokumentu do Europejskiej Rady Ochrony Danych (EROD) i po otrzymaniu opinii EROD w tej sprawie **Wymogi akredytacji podmiotów monitorujących kodeksy postępowania** zostały przyjęte i opublikowane w 2021 r. na stronie internetowej UODO.

Akredytacje udzielone w 2023 r. przez organ nadzorczy

W 2023 r. Polska Federacja Szpitali, będąca twórcą Kodeksu postępowania dla sektora ochrony zdrowia, przedłożyła organowi nadzorczemu odpowiednie propozycje monitorowania przestrzegania kodeksu przez podmioty publiczne. W związku z ich pozytywną oceną 11 grudnia 2023 r. Prezes UODO zatwierdził ww. kodeks i udzielił akredytacji **KPMG Advisory sp. z o.o. sp.k.** do monitorowania przestrzegania jego postanowień. Tego samego dnia nastąpiło uroczyste wręczenie decyzji w przedmiocie zatwierdzenia kodeksu dla Polskiej Federacji Szpitali i certyfikatu akredytacyjnego dla KPMG Advisory sp. z o.o. sp.k. Odbyło się również webinarium, podczas którego przedstawiciele obu ww. podmiotów omówili przebieg prac związanych z opracowywaniem treści kodeksu i procedur, na podstawie których będzie działał podmiot go monitorujący.

11. 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 10 maja 2018 r. o ochronie danych osobowych w Polsce certyfikacja będzie dokonywana przez podmioty certyfikujące, które będą 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 organ nadzorczy. 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 lutym 2023 r. polski organ nadzorczy przedłożył EROD projekt dodatkowych wymogów akredytacji podmiotów certyfikujących[263], zmieniony zgodnie z zaleceniami Europejskiej Rady Ochrony Danych, wynikającymi z Opinii 11/2022 w sprawie projektu

[263] DOL.602.1.2022.

decyzji właściwego organu nadzorczego w Polsce w sprawie zatwierdzenia wymogów akredytacji podmiotów certyfikujących zgodnie z art. 43 ust. 3 (RODO). Ze względu na wielość realizowanych zadań EROD nie była gotowa wydać opinii uzupełniającej (następczej) do ww. projektu wymogów do końca 2023 r. Dlatego polski organ nadzorczy zatwierdził 8 grudnia 2023 r. **Dodatkowe wymogi akredytacji podmiotów certyfikujących,** których treść została opublikowana na stronie internetowej UODO i przesłana do EROD. Publikacja ww. wymogów została połączona z działaniami edukacyjnymi, których celem jest zachęcanie rynku do tworzenia mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych w rozumieniu art. 42 RODO.

Tematowi certyfikacji poświęcone zostało pierwsze webinarium z serii „Certyfikacja w ochronie danych", które z inicjatywy organu nadzorczego odbyło się 12 grudnia 2023 r. za pośrednictwem strony internetowej UODO, na której zostało również udostępnione nagranie z tego wydarzenia.

Wznowiony został kontakt roboczy Urzędu Ochrony Danych Osobowych z Polskim Centrum Akredytacji, które będzie akredytować podmioty certyfikujące. Celem jest ustalenie kierunków współpracy w promowaniu certyfikacji jako narzędzia wykazywania zgodności z RODO[264].

12. Pytania dotyczące wykładni prawa, wnioski o dostęp do informacji 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. 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.

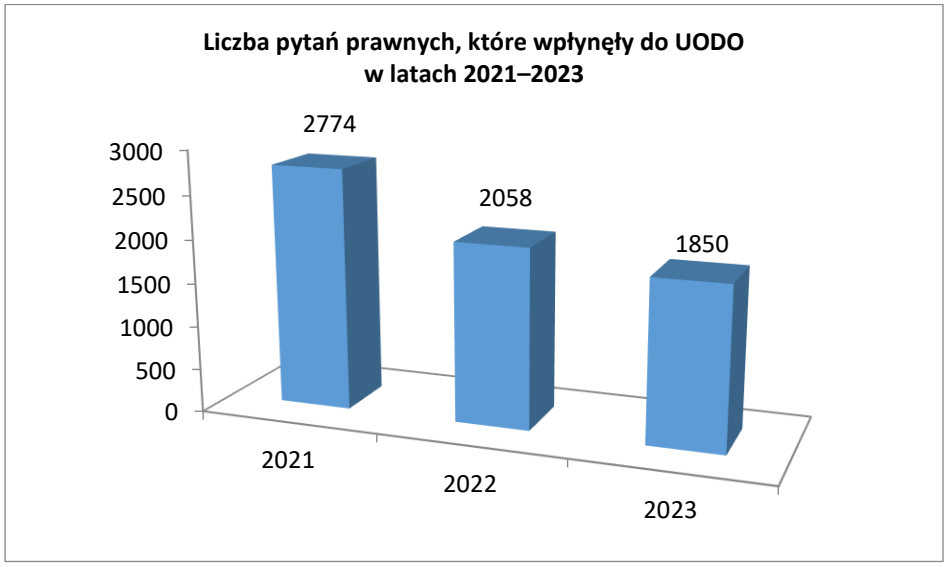
12.1. Pytania dotyczące wykładni prawa

W związku z wpływającymi do UODO pytaniami organ nadzorczy informuje osoby, których dane dotyczą, o prawach przysługujących im na mocy RODO, zaś administratorom i podmiotom przetwarzającym udziela kierunkowych wskazówek co do ich obowiązków w zakresie ochrony danych osobowych. W wyjaśnieniach udzielanych administratorom dodatkowo podkreśla, że swoje wątpliwości co do przetwarzania danych osobowych w pierwszej kolejności powinni konsultować z inspektorami ochrony danych, którzy posiadają fachową wiedzę na temat prawa i praktyk w tej dziedzinie.

[264] DOL.421.1.2022.

Problemy sygnalizowane w pismach zawierających pytania są często wspólne dla różnych grup podmiotów i mogą stanowić ważny impuls do podjęcia określonych działań z urzędu (takich jak np. komunikaty, poradniki, wystąpienia).

W roku 2023 **administratorzy oraz osoby fizyczne** skierowali do Urzędu Ochrony Danych Osobowych **1597** pism z **pytaniami prawnymi,** zaś **253** pisma wpłynęły od **inspektorów ochrony danych.** Zatem **w sumie** w 2023 r. do UODO wpłynęło **1850 pytań prawnych.** To mniej niż w latach ubiegłych, kiedy wpłynęło ich odpowiednio 2058 w roku 2022 i 2774 w roku 2021.



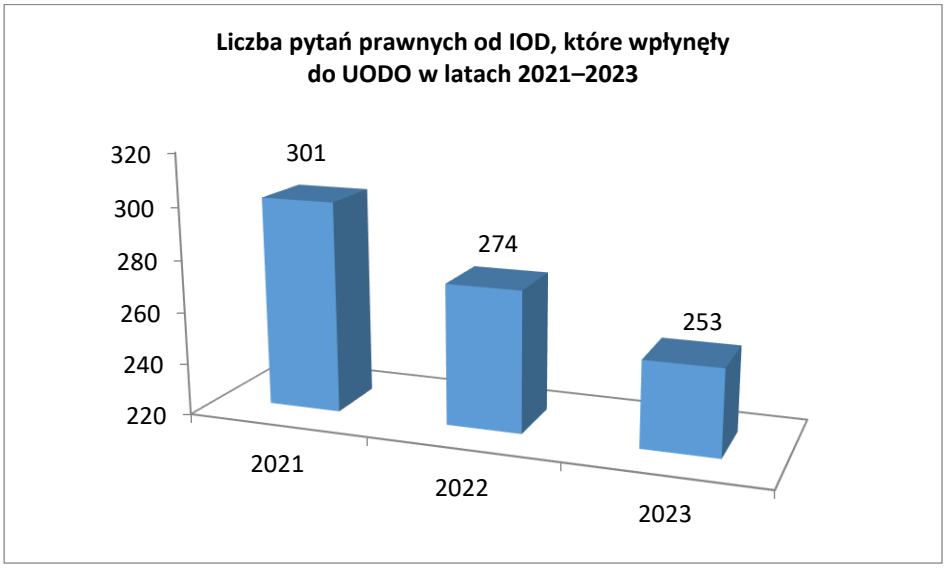
Wykres 16: Liczba pytań dotyczących przepisów prawnych, które wpłynęły do UODO w latach 2021–2023

W ogólnej liczbie 1850 pytań uwzględniono 27 zapytań organów nadzorczych z innych państw, które zostały skierowane do polskiego organu nadzorczego w 2023 r.

Spadek liczby wpływających pytań może być spowodowany tym, że wiele kwestii zostało już przez organ nadzorczy wyjaśnionych, np. w komunikatach zamieszczonych na stronie internetowej urzędu czy w „Newsletterze UODO dla IOD" (obecnie „Biuletyn UODO").

W roku 2023 rozpatrzonych zostało 1846 pism z pytaniami od administratorów oraz osób fizycznych.

Osobną grupę spraw stanowiły pytania od inspektorów ochrony danych (IOD), do których organ nadzorczy – biorąc pod uwagę niezwykle ważną rolę, jaką osoby wykonujące tę funkcję mają pełnić w systemie ochrony danych osobowych – podchodzi ze szczególną uwagą. W 2023 r. do UODO wpłynęły 253 pytania od IOD – odpowiedzi udzielono na 246 pytań. W poprzednich latach takich pytań wpłynęło: w 2022 r. – 274, a w 2021 r. – 301.



Wykres 17: Liczba pytań prawnych od inspektorów ochrony danych, które wpłynęły do UODO w latach 2021–2023

12.1.1. Pytania od administratorów i osób fizycznych

Zakres tematyczny zagadnień poruszanych w pytaniach prawnych od administratorów i osób fizycznych dotyczył różnych aspektów przetwarzania danych osobowych oraz stosowania nie tylko RODO, ale także innych, szczególnych przepisów prawa. Zarówno podmioty z sektora publicznego, jak i prywatnego oraz osoby fizyczne zgłaszały wątpliwości dotyczące takich kwestii, jak:

1) stosowanie monitoringu wizyjnego,
2) przetwarzanie danych osobowych w związku z zatrudnieniem,
3) udostępnianie danych w toku prowadzonych kontroli,
4) przetwarzanie danych w służbie zdrowia,
5) przetwarzanie danych w związku z wyborami parlamentarnymi,
6) ujawnianie danych osobowych w Internecie,
7) przetwarzanie danych z wykorzystaniem nowych technologii,
8) przetwarzanie danych osobowych w ramach dostępu do informacji publicznej.

Ad 1. Stosowanie monitoringu wizyjnego

1) Monitoring wizyjny

W 2023 r., podobnie jak w latach ubiegłych, wiele pytań dotyczyło podstaw prawnych instalowania monitoringu, np.: na prywatnej posesji[265], przy nieruchomości wspólnej[266], na ulicy[267] itp. W takich sprawach organ nadzorczy wyjaśniał, kiedy przetwarzanie można uznać za czynność o charakterze osobistym lub domowym, do której RODO nie będzie miało zastosowania, a w jakich sytuacjach przetwarzanie danych w ramach monitoringu podlegać będzie przepisom o ochronie danych osobowych. Istotny w tej materii był

[265] DOL.023.651.2023, DOL.023.251.2023, DOL.023.320.2023, DOL.023.248.2023.
[266] Np. DOL.023.427.2023, DOL.023.375.2023.
[267] DOL.023.561.2023.

przywoływany wielokrotnie wyrok TSUE z 11 grudnia 2014 r. w sprawie C-212/13[268] oraz Wytyczne 3/2019 Europejskiej Rady Ochrony Danych w sprawie przetwarzania danych osobowych przez urządzenia wideo. Zwracano przy tym uwagę na konieczność poszanowania zasady przejrzystości, tak aby wprowadzone rozwiązania z użyciem kamer wideo nie prowadziły do bezprawnej inwigilacji osób monitorowanych.

Do UODO wpływały też pytania odnoszące się do stosowania monitoringu w obszarach należących do administratorów z sektora medycznego.

2) Monitoring w gabinecie lekarskim

Organ nadzorczy otrzymał pytanie od komendy powiatowej policji prowadzącej postępowanie czy istnieją procedury i wytyczne dotyczące montażu kamer w takich miejscach[269]. W odpowiedzi UODO wyjaśnił, że legalność stosowania dozoru wizyjnego w pomieszczeniach, w których udzielane są świadczenia zdrowotne, uzależniona jest od istnienia przepisów prawa dopuszczających jego stosowanie. Przepisy ustawy z 15 kwietnia 2011 r. o działalności leczniczej wprost wskazują, w jakich pomieszczeniach i w jakim celu taki monitoring może zostać zainstalowany. Zgodnie z art. 23a ust. 1 powołanej ustawy kierownik podmiotu wykonującego działalność leczniczą może określić w regulaminie organizacyjnym sposób obserwacji: 1) pomieszczeń ogólnodostępnych, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pacjentów lub pracowników; 2) pomieszczeń, w których są udzielane świadczenia zdrowotne oraz pobyt pacjentów, w szczególności pokoi łóżkowych, pomieszczeń higieniczno-sanitarnych, przebieralni, szatni, jeżeli wynika to z przepisów odrębnych – za pomocą urządzeń umożliwiających rejestrację obrazu (monitoring). W przypadku pomieszczeń ogólnodostępnych, aby przetwarzanie danych osobowych z użyciem monitoringu można było uznać za legalne, musi być ono związane z koniecznością zapewnienia bezpieczeństwa pracownikom pomieszczeń lub pacjentom. Kwestię monitoringu regulują także szczegółowo przepisy rozporządzenia Ministra Zdrowia z 26 marca 2019 r. w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą oraz ustawy z 19 sierpnia 1994 r. o ochronie zdrowia psychicznego. Przepisy te dokładnie określają, kiedy i w jakich pomieszczeniach stosowanie dozoru wizyjnego jest dopuszczalne, na jakich zasadach odbywa się dostęp do nagrań oraz jak długo takie nagrania są przechowywane i w jaki sposób usuwane.

Ad 2. Przetwarzanie danych osobowych w związku z zatrudnieniem

W 2023 r. – podobnie jak w latach ubiegłych – do UODO wpłynęło wiele pytań od pracodawców, pracowników czy związków zawodowych dotyczących przetwarzania danych osobowych w związku z zatrudnieniem. Dotyczyły one głównie legalności przetwarzania danych osobowych pracowników, np. wizerunku, danych biometrycznych, a także przechowywania danych w aktach osobowych. Pytano również o stosowanie

[268] Wyrok TSUE z 11 grudnia 2014 r. w sprawie C-212/13 *František Ryneš vs. Úřad pro ochranu osobních údajů*, przesądzający, że art. 3 ust. 2 tiret drugie dyrektywy 95/46 należy interpretować w ten sposób, że wykorzystywanie systemu kamer przechowującego zapis obrazu osób na sprzęcie nagrywającym w sposób ciągły, takim jak dysk twardy, zainstalowanego przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, który to system monitoruje również przestrzeń publiczną, nie stanowi przetwarzania danych w trakcie czynności o czysto osobistym lub domowym charakterze w rozumieniu tego przepisu.

[269] DOL.023.136.2023.

monitoringu w miejscu pracy. Pojawiły się też nowe kwestie, jak stosowanie kamer nasobnych czy monitoringu fonicznego, a także podstawy prawnej do przetwarzania danych osobowych chorego dziecka pracownika w ramach zbiórki charytatywnej prowadzonej na terenie zakładu pracy.

1) Wizerunek pracownika

Jedno z pytań od pracownika dotyczyło legalności przetwarzania wizerunku pracownika za pośrednictwem kamery internetowej oraz poprzez umieszczenie fotografii w poczcie służbowej[270]. Wizerunek osoby fizycznej utrwalony na fotografii, umożliwiający bezpośrednią lub pośrednią identyfikację tej osoby fizycznej, co do zasady jest daną osobową w rozumieniu art. 4 pkt 1 RODO. Podkreślenia wymaga, że to przepisy Kodeksu pracy regulują, jaki zakres danych osobowych może przetwarzać (w tym pozyskiwać i dalej wykorzystywać) pracodawca. Określają także zasady tego przetwarzania (art. 22^1, art. 22^{1a} Kodeksu pracy). Przepisy te wyraźnie wskazują, że w przypadku, gdy pracodawca ma zamiar przetwarzać szerszy zakres danych o pracowniku niż wynika to z przepisów Kodeksu pracy i przepisów szczególnych (np. jego wizerunek), to przesłanką legalności powinna być co do zasady zgoda pracownika. Brak takiej 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. O ile jednak miałaby mieć zastosowanie inna przesłanka (spośród wskazanych w art. 6 ust. 1 RODO), wówczas administrator musiałby wykazać przede wszystkim, że takie dane może pozyskiwać bez naruszenia zasad określonych w Kodeksie pracy, a jednocześnie z poszanowaniem zasad ochrony danych osobowych. Przy zastosowaniu przesłanki z art. 6 ust. 1 lit. f) RODO istniałaby konieczność przeprowadzenia testu równowagi w kontekście analizy konkretnych, istotnych powodów ingerencji w interesy i podstawowe prawa i wolności podmiotu danych. Organ nadzorczy podkreślał też, że umieszczanie zdjęć pracownika w poczcie służbowej lub obowiązek korzystania przez pracownika z kamery internetowej w czasie spotkań są przypadkami szczególnymi ze względu na to, iż dostęp do wizerunku pracownika ma ściśle określony krąg osób, tj. pracownicy, którzy znają się nawzajem, oraz ze względu na cel, jaki przyświeca tego typu działaniom pracodawcy, jakim jest usprawnienie procesu zarządzania i wewnętrznej komunikacji w firmie. Jeśli pracodawca jest podmiotem z sektora prywatnego, można się zastanowić, czy takie działanie będzie się mieściło w granicach jego usprawiedliwionego celu, zgodnie z art. 6 ust. 1 lit. f) RODO. Organ zwracał uwagę, że w niektórych sytuacjach może wystąpić nawet konieczność umożliwienia wizualnej identyfikacji pracownika, wynikająca np. z zakresu jego obowiązków, charakteru wykonywanej pracy czy potrzeb pracodawcy związanych z konkretnym stanowiskiem pracy. O ile więc umieszczenie zdjęć bądź ujawnienie wizerunku służy polepszeniu i usprawnieniu zarządzania przedsiębiorstwem, a dostępu do nich nie mają osoby z zewnątrz, to można przyjąć to za dopuszczalne przy zachowaniu warunków wynikających z przepisów o ochronie danych osobowych. Wskazywano ponadto na możliwość skorzystania przez podmiot danych z prawa przysługującego mu

[270] DOL.023.293.2023.

na podstawie art. 21 ust. 1 RODO, tj. prawa do sprzeciwu z przyczyn związanych ze szczególną sytuacją takiej osoby.

Odpowiadając zaś na pytanie, czy zdjęcie pracownika wraz z jego imieniem i nazwiskiem, nazwą stanowiska, numerem telefonu kontaktowego, można udostępnić osobom z zewnątrz, np. kontrahentom[271], organ wskazał, że pracodawca powinien w pierwszej kolejności ocenić, dla jakiego celu pozyskanie i dalsze udostępnienie danych w postaci wizerunku ma być dokonywane i czy dla jego realizacji jest to niezbędne, tj. czy zakładany cel może być osiągnięty bez wskazanych danych. Zwrócił dodatkowo uwagę także na aktualny pogląd wyrażony przez Grupę Roboczą Art. 29 w dokumencie z 13 września 2001 r. pt. „Opinia Grupy Roboczej w sprawie przetwarzania danych osobowych w kontekście zatrudnienia". Grupa Robocza wskazała w nim, iż udzielona przez pracownika zgoda na przetwarzanie jego danych osobowych jest „misleading" (zwodnicza, myląca). Grupa Robocza argumentuje, że: „pracodawca musi przetwarzać dane osobowe pracowników – jest to nieunikniona i konieczna konsekwencja stosunku pracy – jednak legitymizacja procesu przetwarzania danych przez pracodawcę na podstawie zgody wyrażonej przez pracownika jest zwodnicza. Uzależnienie od zgody pracownika winno zostać ograniczone do przypadków, w których pracownik ma całkowitą swobodę jej udzielenia i jest w stanie odmówić wyrażenia zgody bez narażania się na szkodę".

Ciekawym zagadnieniem była także kwestia dopuszczalności pozyskiwania danych biometrycznych przez pracodawcę w postaci wizerunku (zdjęcia paszportowego) w celu ich użycia w elektronicznych legitymacjach służbowych pracowników Najwyższej Izby Kontroli (NIK)[272]. Odnosząc się do definicji danych biometrycznych, wskazanej w art. 4 pkt 14 RODO, organ nadzorczy wyjaśnił, że nie każdy wizerunek będzie daną biometryczną, gdyż do tego potrzebny jest jeszcze element „specjalnego przetwarzania technicznego". W motywie 51 RODO unijny prawodawca precyzuje, że: „przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją »danych biometrycznych« tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości". Kluczowa jest więc ocena, czy fotografie, które mają być wykorzystane w legitymacjach, w istocie spełniają definicję danych biometrycznych. Rozważając zaś zastosowanie przesłanki legalizującej przetwarzanie danych biometrycznych w legitymacjach służbowych pracowników NIK, Prezes UDOO wskazał, że musi być spełniona przesłanka z art. 9 ust. 2 RODO. Zgodnie z nią przetwarzanie tego rodzaju danych musi być niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez pracownika lub pracodawcę. Podstawą przetwarzania może być zatem jedynie przepis prawa regulujący jednoznacznie możliwość przetwarzania danych sensytywnych w określonych celach oraz przewidujący odpowiednie zabezpieczenia praw i interesów osoby, której dane dotyczą. Takie rozwiązanie powinno więc wprost wynikać z przepisów ustawy o NIK[273]. Jednak zarówno art. 22^{1b} ust. 1 § 2 Kodeksu pracy, jak i art. 30 ustawy

[271] DOL.023.575.2023.
[272] DOL.023.446.2023.
[273] Ustawa z 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623), dalej jako: ustawa o NIK.

o NIK (dający podstawę do używania przez kontrolerów NIK legitymacji) nie stanowią podstawy prawnej do zamieszczenia danych biometrycznych kontrolerów NIK w legitymacjach służbowych, a także przetwarzania tych danych w innych celach (np. przetwarzania cechy biometrycznej z użyciem legitymacji). Z art. 30 ust. 5 ustawy o NIK stanowiącego, że: „kontrolę spraw lub dokumentów zawierających informacje niejawne oznaczone jako ściśle tajne przeprowadza się na podstawie legitymacji służbowej i odrębnego upoważnienia wydanego przez Prezesa Najwyższej Izby Kontroli", można wnioskować, że w niektórych sytuacjach legitymacja kontrolera NIK może służyć do dostępu do szczególnie ważnych informacji lub do dostępu do pomieszczeń wymagających szczególnej ochrony. Jednak brak tu kluczowego aspektu „niezbędności" takiego rozwiązania, aby czynić to w każdym przypadku. Organ ochrony danych jednoznacznie wskazał zatem, że w obecnym stanie prawnym przetwarzanie danych biometrycznych pracowników Najwyżej Izby Kontroli w celu wykonania przez pracodawcę legitymacji służbowych nie będzie zgodne z RODO, zwłaszcza w świetle określonych w nim zasad: legalizmu – art. 5 ust. 1 lit. a), ograniczenia celu – art. 5 ust. 1 lit. b) oraz minimalizacji danych – art. 5 ust. 1 lit. c).

2) Wykorzystywanie przez pracodawcę czytnika danych biometrycznych lub linii papilarnych do ewidencjonowania czasu pracy

Podobnie jak w roku poprzednim, wpływały też pytania o możliwość wykorzystywania przez pracodawcę czytnika danych biometrycznych lub linii papilarnych do ewidencjonowania czasu pracy[274]. Odpowiadając na nie, organ właściwy do spraw ochrony danych osobowych wskazywał, że zgodnie z art. 22^{1b} § 1 Kodeksu pracy dane szczególnej kategorii (w tym dane biometryczne) mogą być przetwarzane za zgodą osoby ubiegającej się o zatrudnienie lub pracownika, jeśli są przekazane z inicjatywy tych osób. Stosownie do art. 22^{1b} § 2 Kodeksu pracy przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony. Zatem przepisy polskiego prawa pracy nie przewidują możliwości przetwarzania przez pracodawcę danych biometrycznych pracowników w celu rejestracji czasu pracy. Jednocześnie organ podkreślał, że wykorzystywanie przez pracodawcę danych biometrycznych pracownika wyłącznie w celu rejestracji czasu pracy naruszałoby określone w RODO zasady, zwłaszcza legalności – art. 5 ust. 1 lit. a), ograniczenia celu – art. 5 ust. 1 lit. b) oraz minimalizacji danych – art. 5 ust.1 lit. c). Warto dodać, że stanowisko na ten temat jest od lat konsekwentnie prezentowane przez pełniących funkcję polskiego organu ochrony danych. W stanowisku tym podkreśla się, że pracodawca może rejestrować czas pracy za pomocą innych narzędzi, których stosowanie nie wiąże się z przetwarzaniem danych biometrycznych pracowników. Cel ten może osiągnąć, wykorzystując np. listy obecności, indywidualne identyfikatory lub karty dostępu.

3) Praca zdalna

[274] Np. DOL.023.214.2023.

W 2023 r. w Kodeksie pracy uregulowane zostały kwestie dotyczące zasad świadczenia pracy zdalnej[275]. W związku z tym pojawiły się też pytania dotyczące przetwarzania danych osobowych w kontekście wprowadzenia nowych przepisów. W jednym z pism pojawiło się pytanie o legalność żądania przez pracodawcę opinii o potrzebie wczesnego wspomagania i rozwoju dziecka oraz orzeczenia o potrzebie kształcenia specjalnego w celu udzielenia zgody na pracę zdalną[276]. Dokumenty te zawierały dane o stanie zdrowia dziecka. Wyjaśniając wątpliwości pytającego, organ właściwy do spraw ochrony danych osobowych odniósł się do przepisów Kodeksu pracy dotyczących tego, kiedy i na jakich zasadach pracodawca może zezwolić na pracę zdalną. Zgodnie z art. 67^{19} Kodeksu pracy pracodawca jest obowiązany uwzględnić wniosek pracownika, o którym mowa w art. 142^{1} § 1 pkt 2 i 3, pracownicy w ciąży, pracownika wychowującego dziecko do ukończenia przez nie 4. roku życia, a także pracownika sprawującego opiekę nad innym członkiem najbliższej rodziny lub inną osobą pozostającą we wspólnym gospodarstwie domowym, posiadającymi orzeczenie o niepełnosprawności albo orzeczenie o znacznym stopniu niepełnosprawności, o wykonywanie pracy zdalnej, chyba że nie jest to możliwe ze względu na organizację pracy lub rodzaj pracy wykonywanej przez pracownika. Ponadto w art. 142^{1} § 1 pkt 3 Kodeksu pracy przesądzono, że pracodawca jest obowiązany uwzględnić wniosek pracownika – rodzica: a) dziecka legitymującego się orzeczeniem o niepełnosprawności albo orzeczeniem o umiarkowanym lub znacznym stopniu niepełnosprawności określonym w przepisach o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz b) dziecka posiadającego odpowiednio opinię o potrzebie wczesnego wspomagania rozwoju dziecka, orzeczenie o potrzebie kształcenia specjalnego lub orzeczenie o potrzebie zajęć rewalidacyjno-wychowawczych, o których mowa w przepisach ustawy z 14 grudnia 2016 r. – Prawo oświatowe[277] – o wykonywanie pracy w systemie czasu pracy, o którym mowa w art. 139, lub rozkładzie czasu pracy, o którym mowa w art. 140^{1} albo w art. 142. Organ właściwy do spraw ochrony danych osobowych zwrócił uwagę, że z powołanych przepisów prawa nie wynika jednoznacznie obowiązek przedstawiania pracodawcy dokumentów, o których mowa w art. 142^{1} Kodeksu pracy. Rozporządzenie w sprawie dokumentacji pracowniczej[278] w § 3 wskazuje zaś jedynie, że akta osobowe pracownika składają się z 5 części i obejmują: w części B oświadczenia lub dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia pracownika, w tym: pkt 2 lit. w) dokumenty dotyczące wykonywania pracy zdalnej oraz pkt 2 lit. z) dokumenty dotyczące stosowania elastycznej organizacji pracy (art. 188^{1} Kodeksu pracy). Katalog danych osobowych przez zastosowanie w analizowanym przepisie sformułowania „w tym" pozostaje otwarty, co oznacza, że mogą znaleźć się tam inne dane niż enumeratywnie wymienione. Za elastyczną organizację pracy (art. 188^{1} Kodeksu pracy) uważa się pracę zdalną – na pisemny wniosek pracownika pracodawca może ustalić indywidualny rozkład jego czasu pracy. Natomiast ustawa o rehabilitacji zawodowej i społecznej oraz

[275] Ustawa z 1 grudnia 2022 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw (Dz. U. z 2023 r. poz. 240) wprowadziła do Kodeksu pracy pracę zdalną, jednocześnie uchylając przepisy dotyczące telepracy. Nowe przepisy regulujące pracę zdalną weszły w życie 7 kwietnia 2023 r.
[276] DOL.023.637.2023.
[277] Dz. U. z 2023 r. poz. 900.
[278] Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej (Dz. U. poz. 2369 ze zm.).

zatrudnianiu osób niepełnosprawnych[279] w art. 2b ust. 1 pkt 1 lit. a) stanowi, że pracodawca przetwarza dane osobowe, w tym dane o stanie zdrowia osób będących członkami rodzin pracowników i niepracujących byłych pracowników dla celów określonych w ustawie. Przedstawienie pracodawcy dokumentów zawierających dane osobowe o stanie zdrowia jest dobrowolne (art. 2b ust. 2). Organ nadzorczy uznał zatem, że w świetle ww. przepisów wnioskowanie o pracę zdalną na podstawie art. 67^{19} w zw. z art. 142^{1} Kodeksu pracy jest uprawnieniem pracownika, nie zaś obowiązkiem, a przedstawienie odpowiedniej dokumentacji o stanie zdrowia jest dobrowolne i może stanowić podstawę realizacji uprawnień przysługujących pracownikowi. Pracodawca natomiast, kierując się zasadą ograniczenia celu z art. 5 ust. 1 lit. b) RODO oraz zasadą minimalizacji danych z art. 5 ust. 1 lit. c) RODO, może z przedłożonego dokumentu np. sporządzić odpowiednią notatkę i umieścić ją w części B akt osobowych pracownika.

4) Monitorowanie pracowników

W 2023 r. do UODO kierowane były także pytania dotyczące zagadnień związanych z monitorowaniem pracowników, np. w kwestii legalności monitoringu komputerów służbowych[280] czy możliwości pozyskiwania i udostępniania danych pochodzących z monitoringu wizyjnego w zakładzie pracy i poza nim[281]. W takich sprawach organ nadzorczy odwoływał się przede wszystkim do uregulowań ustawy Kodeks pracy, które określają: cele przetwarzania danych, sposób i obszar nadzoru, okres przechowywania nagrań, sposób wprowadzenia monitoringu oraz obowiązek informacyjny osób objętych monitoringiem. Przypominał także, że monitoring w miejscu pracy nie może naruszać życia prywatnego pracownika, w szczególności tajemnicy korespondencji, na co zwracał uwagę Europejski Trybunał Praw Człowieka w wielu wyrokach, w tym w wyroku z 5 września 2017 r.[282] Nie należy również zapominać, że jeśli pracodawca będzie chciał wprowadzić w zakładzie pracy różne formy monitoringu, to powinien przeprowadzić ocenę skutków dla ochrony danych, o której mowa w art. 35 RODO[283]. Ponieważ wiele informacji na temat monitoringu w miejscu pracy zamieszczanych było na stronie internetowej Urzędu Ochrony Danych Osobowych, organ odwoływał się także do tych informacji.

5) Monitoring foniczny

Nowym zagadnieniem, jakie wpłynęło do organu w 2023 r. było zapytanie od jednej ze spółek zarządzającej komunikacją miejską, dotyczące możliwości wprowadzenia w pojazdach komunikacji miejskiej szczególnego nadzoru w kabinie pracownika spółki – kierowcy/motorniczego – w postaci środków technicznych umożliwiających rejestrację dźwięku (monitoring foniczny)[284]. Spółka uzasadniała, że prowadzenie monitoringu fonicznego jest niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi

[279] Ustawa z 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2023 r. poz. 100 ze zm.).
[280] DOL.023.269.2023.
[281] DOL.023.218.2023.
[282] *Bărbulescu przeciwko Rumunii* – wyrok ETPC z 5 września 2017 r., Wielka Izba, skarga nr 61496/08.
[283] Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
[284] DOL.023.24.2023.

narzędzi pracy (pojazdu). Możliwość skontrolowania nagrania z monitoringu fonicznego byłaby także przydatna w przypadkach sporów z podróżnymi i dawałaby szansę na podważenie nieuzasadnionych oskarżeń wobec kierowcy autobusu/tramwaju, chroniąc go przed poniesieniem konsekwencji służbowych. Spółka postulowała wprowadzenie monitoringu fonicznego poprzez zmiany w regulaminie pracy.

Organ nadzorczy podkreślił, że proces przetwarzania danych w ramach zatrudnienia podlega szczególnym zasadom ze względu na nierówność stron stosunku pracy. Dlatego prawodawca unijny (w art. 88 RODO) upoważnił państwa członkowskie do przyjęcia bardziej szczegółowych przepisów mających zapewnić ochronę praw i wolności pracownika w związku z przetwarzaniem jego danych osobowych dla celów dotyczących zatrudnienia. Wyrazem dostosowania prawa polskiego do art. 88 RODO są regulacje wprowadzone do ustawy z 26 czerwca 1974 r. – Kodeks pracy ustawą z 10 maja 2018 r. o ochronie danych osobowych (dotyczące zakresu danych gromadzonych od pracownika, monitoringu wizyjnego w zakładzie pracy i monitoringu poczty elektronicznej pracownika), a następnie ustawą z 21 lutego 2019 r. zmieniającej Kodeks pracy z dniem 4 maja 2019 r. Przepisy Kodeksu pracy wskazują, kiedy i na jakich zasadach pracodawca może stosować monitoring swoich pracowników w celu zapewnienia ich bezpieczeństwa lub ochrony mienia, ale odnosi się to tylko do rejestracji obrazu, a nie dźwięku (art. 22^2). Nie można także wywodzić podstawy do przetwarzania danych w ww. celach za pomocą monitoringu fonicznego z art. 22^3 § 4 Kodeksu pracy, jako innej formy monitoringu. Możliwość zastosowania tej formy monitoringu musi jasno wynikać z przepisu prawa, tj. ustawy. Stanowisko takie zostało także poparte orzecznictwem sądów administracyjnych, m.in. wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie z 28 października 2022 r.[285], w którym sąd potwierdził stanowisko Prezesa Urzędu Ochrony Danych Osobowych, że nagrywanie i utrwalanie dźwięku (głosu) w zainstalowanym w ośrodku dla osób nietrzeźwych systemie monitoringu naruszało przepisy RODO, gdyż nie istniała do tego wyraźna podstawa prawna. Organ nadzorczy zwrócił także uwagę, że Europejska Rada Ochrony Danych w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo wskazała, że zapis audiowizualny stanowi niewątpliwie większą formę ingerencji w prywatność niż sam obraz. W pkt 9.3 ppkt 129 Wytycznych 3/2019 podkreślono, że wybrane przez administratora rozwiązania techniczne, odnoszące się do prowadzonego monitoringu, nie powinny zawierać funkcji, które nie są niezbędne, np.: nieograniczone śledzenie ruchów kamery, możliwość przybliżenia, transmisja radiowa, analiza i nagrania dźwiękowe. Zgodnie z przytoczonymi Wytycznymi 3/2019 funkcje, które nie są niezbędne, powinny zostać dezaktywowane.

Podobne argumenty organ przytoczył w innej sprawie dotyczącej legalności rejestrowania dźwięku (monitoring foniczny) w pojazdach komunikacji kolejowej poprzez zapis głosu przez system CCTV podczas korzystania przez pasażera z interkomu oraz zapisu audio z kabiny maszynisty[286].

6) Kamery nasobne

Ciekawym zagadnieniem rozpatrywanym w 2023 r. przez organ nadzorczy była kwestia wprowadzenia kamer nasobnych dla pracowników ochrony. Jedna z firm

[285] Sygn. akt II SA/Wa 1341/22.
[286] DOL.023.378.2023.

zajmujących się ochroną osób i mienia[287], a następnie organizacja zrzeszająca przedsiębiorców, będących pracodawcami i prowadzących działalność gospodarczą w zakresie ochrony osób i mienia, zapytały o legalność rejestrowania zadań wykonywanych przez pracowników ochrony poprzez tzw. kamery nasobne, tj. kamery rejestrujące obraz i/lub dźwięk umieszczone np. na mundurze pracownika ochrony. W ten sposób przetwarzane byłyby dane osobowe, takie jak m.in. wygląd oraz głos osób przebywających na terenie obiektu chronionego[288]. W ocenie pytającego takie rozwiązanie jest oczekiwane ze strony klientów firm ochroniarskich. Zarówno firma ochroniarska, jak i związek wyrazili stanowisko, że brak jest podstawy prawnej do używania kamer nasobnych rejestrujących obraz i dźwięk przez pracowników ochrony podczas wykonywania czynności służbowych, zarówno z punktu widzenia przepisów ustawy o ochronie osób i mienia, jak i ustawy o ochronie danych osobowych.

Organ ochrony danych osobowych zwrócił uwagę, że zakres uprawnień pracowników ochrony przy realizacji zadań w zakresie ochrony fizycznej osób i mienia został określony w art. 36 ust. 1 ustawy z 22 sierpnia 1997 r. o ochronie osób i mienia. Katalog uprawnień pracowników ochrony zawarty w powołanym artykule nie zawiera prawa do korzystania z urządzeń technicznych rejestrujących obraz lub dźwięk przy wykonywaniu zadań ochrony osób i mienia. Tym samym wyłącza on możliwość powołania się na art. 6 ust. 1 lit. c) RODO jako przesłankę legalizującą przetwarzanie w ten sposób danych osobowych.

Nie można również uznać, że używanie kamer nasobnych rejestrujących obraz i dźwięk w związku z wykonywaniem zadań służbowych przez pracownika ochrony może być stosowane na podstawie art. 6 ust. 1 lit. f) RODO – jako realizacja prawnie uzasadnionego interesu administratora lub osoby trzeciej. Stanowiłoby to próbę poszerzenia katalogu uprawnień pracownika ochrony, prowadząc tym samym do obejścia art. 36 ustawy o ochronie osób i mienia.

Organ zwrócił także uwagę, że system monitoringu stanowi istotną ingerencję w prawa i wolności nie tylko osób poddawanych takiemu monitoringowi (wśród których znajdować się mogą także osoby trzecie), ale mógłby także prowadzić do nadmiernej ingerencji w prawa i wolności osób zatrudnionych przy realizacji zadań ochrony osób i mienia. Taka ingerencja w sferę autonomii jednostki wymagałaby z pewnością wprowadzenia zmian w obowiązujących przepisach prawa i ustanowienia podstawy prawnej dla takiego rodzaju przetwarzania danych osobowych, poprzedzonego przeprowadzeniem oceny skutków dla ochrony danych w związku z art. 35 ust. 1 RODO. Wprowadzenie bowiem ograniczeń w zakresie korzystania z konstytucyjnych wolności i praw, którymi będzie rejestracja obrazu i dźwięku osób znajdujących się w polu działania kamery nasobnej, obarczone będzie koniecznością dokonania oceny skutków zawierającej co najmniej elementy wymienione w art. 35 ust. 7 RODO, tj.: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, ocenę czy operacje są niezbędne w stosunku do celów; ocenę ryzyka naruszenia praw lub wolności podmiotów danych; środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa, które mają zapewnić ochronę danych osobowych.

[287] DOL.023.261.2023.
[288] DOL.023.623.2023.

Organ nadzorczy odwołał się również do orzecznictwa, w którym podkreśla się, że pracownicy ochrony (także przedsiębiorcy prowadzący działalność z zakresu ochrony osób i mienia) powinni dawać rękojmię prawidłowego wykonywania obowiązków, choćby z tej racji, że obejmują one działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej innych osób, jak też działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, przy użyciu środków ochrony fizycznej osób i mienia, w tym wykorzystania środków przymusu bezpośredniego, a nawet broni palnej[289]. Z tego powodu w ustawie o ochronie osób i mienia wyczerpująco wymienione są środki prawne, którymi w celu ochrony osób i mienia taki pracownik może się posługiwać[290].

7) Przetwarzanie danych osobowych dziecka pracownika w ramach zbiórki charytatywnej organizowanej na terenie zakładu pracy

W 2023 r. z pytaniem do organu nadzorczego zwrócił się pracodawca, który organizował na terenie zakładu pracy zbiórkę charytatywną dla chorego dziecka pracownika. W związku z tym zapytał, czy powinien pozyskać zgodę od tego pracownika na przetwarzanie danych osobowych jego dziecka oraz danych kontaktowych rodziców[291]. W tej sytuacji organ nadzorczy nie miał wątpliwości, że taka zgoda będzie konieczna. Biorąc bowiem pod uwagę, że w przypadku organizacji zbiórki dochodzić będzie do przetwarzania danych o stanie zdrowia dziecka, a więc danych osobowych szczególnych kategorii, to na takie działanie niezbędna jest wyraźna zgoda rodzica[292]. Zgodę taką powinien pozyskać pracodawca, który – zamierzając zaangażować się w zbiórkę charytatywną – będzie przetwarzał te dane osobowe i stanie się w ten sposób ich administratorem w rozumieniu art. 4 pkt 7 RODO[293].

8) Wycofanie zgody pracownika na przetwarzanie danych w dokumencie znajdującym się w aktach osobowych

W jednym z pytań pojawiła się kwestia oceny legalności zachowania pracownika, który chcąc odzyskać kopię dokumentów przechowywanych w jego aktach osobowych, cofnął swoją zgodę na ich przetwarzanie. Chodziło o dokument potwierdzający ukończenie kursu pedagogicznego oraz o świadectwo maturalne[294]. Powstało pytanie, czy wycofanie zgody na przetwarzanie tych dokumentów nie będzie miało wpływu na dotychczasowe zatrudnienie. W tej sytuacji organ nadzorczy wskazał, że przetwarzanie danych osobowych pracownika określają przepisy ustawy – Kodeks pracy (m.in. art. 22^1 § 1 i 3, art. 22^{1a}) oraz przepisy szczególne. Zwrócił ponadto uwagę, że zgoda, o której mowa

[289] Zob. wyrok Naczelnego Sądu Administracyjnego z 19 stycznia 2022 r. sygn. akt II GSK 2447/21.
[290] Zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Warszawie z 28 października 2022 r. (sygn. akt II SA/Wa 1341/22) podmiot decydujący o stosowaniu instalacji monitoringu, która umożliwia nagrywanie i utrwalanie dźwięku powinien wpierw ocenić, czy są do tego podstawy prawne.
[291] DOL.023.172.2023.
[292] W przypadku przetwarzania danych osoby małoletniej zgodę wyraża jego rodzic lub opiekun prawny. Ponadto zgoda musi spełniać warunki określone w art. 7 RODO. Motyw 32 RODO wyjaśnia, że zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia.
[293] Więcej informacji na temat zasad wyrażania zgody można przeczytać w Wytycznych EROD 05/2020 dotyczących zgody na mocy rozporządzenia 2016/679.
[294] DOL.023.580.2023.

w art. 22^{1a} Kodeksu pracy i możliwość jej późniejszego wycofania, nie dotyczy danych wskazanych w art. 22^{1} Kodeksu pracy[295], w szczególności dokumentujących wykształcenie.

9) Wykorzystywanie adresów e-mail i numerów PESEL pracownika do przesyłania pasków płacowych

Jeden z pracodawców skierował do Prezesa UODO pytanie, czy w związku z wprowadzeniem w firmie elektronicznego wysyłania pasków płacowych pracownikom należy, ze względów bezpieczeństwa, służbowy adres mailowy zastąpić adresem prywatnym oraz czy numer PESEL może być zastosowany jako hasło do otworzenia pliku z odcinkiem płacowym[296]. Organ nadzorczy wyjaśnił, że art. 85 § 5 ustawy – Kodeks pracy nakłada na pracodawcę obowiązek udostępnienia pracownikowi na jego żądanie dokumentów, na podstawie których zostało obliczone jego wynagrodzenie. Doręczanie pracownikowi tzw. pasków wynagrodzeń drogą elektroniczną nie jest wymagane przez przepisy Kodeksu pracy i należy do autonomicznej decyzji pracodawcy. Wskazał także, że dane osobowe, zgodnie z przepisem art. 5 ust. 1 lit. f) RODO, muszą być 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"). Zgodnie z art. 24 ust. 1 RODO administrator zobowiązany jest wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami rozporządzenia i aby móc to wykazać. Przepis art. 32 RODO konkretyzuje wymogi zabezpieczenia przetwarzania danych osobowych i wskazuje na aspekty, jakie administrator i podmiot przetwarzający dane powinni wziąć pod uwagę, określając stopień ryzyka i wdrożone zabezpieczenia. Wskazane zostały także przykładowe sposoby ograniczające ryzyko naruszenia praw i wolności osób fizycznych. W szczególności administrator może stosować w konkretnym przypadku przetwarzania danych osobowych m.in. pseudonimizację i szyfrowanie danych osobowych. Z powyższych przepisów wywieść należy, iż na administratorze danych spoczywa obowiązek dokonania samodzielnej oceny w przedmiocie wdrożenia odpowiednich środków technicznych i organizacyjnych w świetle stwierdzonego ryzyka, jakie wiąże się z przetwarzaniem określonego rodzaju danych osobowych. Przepisy rozporządzenia nie wskazują jednak na konkretne środki techniczne, jakie administrator powinien zastosować w danym przypadku. Odnosząc się zaś do wykorzystywania numeru PESEL pracownika jako hasła do otworzenia pliku zawierającego pasek wynagrodzenia, Prezes UODO wskazał, iż ocena szyfrowania w tej formie powinna zostać dokonana w świetle przesłanek wskazanych w przepisach art. 24 i art. 32 RODO. Numer PESEL może być uznany w poszczególnych przypadkach przetwarzania danych osobowych za wystarczający sposób zabezpieczenia przed ryzykiem naruszenia danych, jednak ocena tego ryzyka należy do administratora i podmiotu przetwarzającego. Numer PESEL to krajowy numer identyfikujący osoby fizyczne, o którym mowa w art. 87 RODO. Podlega on szczególnej ochronie, bowiem prawodawca unijny, wprowadzając powyższą regulację,

[295] Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę innych danych osobowych niż wymienione w art. 22^{1} § 1 i 3, z wyjątkiem danych osobowych, o których mowa w art. 10 RODO.
[296] DOL.023.8.2023.

uznał, że wykorzystywanie uniwersalnych identyfikatorów osobowych może stwarzać różnego rodzaju zagrożenia w sferze ochrony danych osobowych. Nie ulega przy tym wątpliwości, iż numer PESEL osoby fizycznej był przetwarzany przez pracodawcę w związku z wykonywaniem przez pracownika umowy o pracę i – choćby w świetle tej okoliczności – administrator powinien dokonać oceny, czy stopień bezpieczeństwa danych osobowych był odpowiedni i czy właściwszym rozwiązaniem nie byłoby zastosowanie hasła dostępu o charakterze abstrakcyjnym.

Ad 3. Udostępnianie danych w toku prowadzonych kontroli

W 2023 r. do organu ochrony danych wpływały pytania dotyczące udostępniania danych w toku prowadzonych kontroli. Jedno z nich, dotyczące podstaw prawnych i zasadności udostępniania przez pracowników starostwa powiatowego dokumentów dotyczących wynagrodzeń pracowników – celem weryfikacji prawidłowości dysponowania przyznanymi środkami budżetowymi[297], zadał powiatowy urząd pracy (PUP).

W odpowiedzi organ nadzorczy ocenił, że przedmiotowa kontrola zarządcza odbywała się na podstawie przepisów ustawy o finansach publicznych[298]. Zgodnie z art. 68 ust. 1 tej ustawy kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Cele tej kontroli zostały wskazane w art. 68 ust. 2. Przepisy powołanej ustawy nie określają jednak zakresu ani kategorii danych niezbędnych do jej przeprowadzenia. Niemniej organ nadzorczy wskazał, że realizacja czynności kontrolnych nie może być dokonywana poprzez dostęp do wszelkich danych posiadanych przez kontrolowanego administratora, gdyż cały czas musi on sprawować kontrolę, jakie dane będą udostępniane. Dostęp starostwa do nieograniczonego zasobu danych osobowych PUP nie wynika także z obowiązujących przepisów prawa, gdyż to nie starostwo, a PUP jest administratorem decydującym o udostępnieniu danych. W tej sytuacji zakres udostępnianych danych powinien być określony zgodnie z zasadami minimalizacji oraz celowości (art. 5 RODO). Żądanie szczegółowego zestawienia wynagrodzeń oraz wszelkich dodatków nie jest niezbędne do osiągnięcia celu przetwarzania, jakim jest kontrola realizacji wydatków finansowych. Dodatkowo wskazano, że ewentualne badanie zgodności sposobu naliczania wynagrodzeń nie powinno być przedmiotem kontroli zarządczej. Uprawnienia dotyczące powyższych kwestii posiadają inne organy, np. Zakład Ubezpieczeń Społecznych (ZUS) czy Państwowa Inspekcja Pracy (PIP), które realizują swoje zadania na podstawie przepisów szczególnych. Organ nadzorczy zwrócił także uwagę, że to PUP jest pracodawcą i – biorąc pod uwagę przepisy prawa pracy – nie ma on podstaw prawnych do ujawnienia tak szerokiego zakresu danych związanych ze stosunkiem pracy.

Ad 4. Przetwarzanie danych w służbie zdrowia

Wiele pytań zadanych organowi nadzorczemu, pochodzących ze służby zdrowia, związanych było z przekazywaniem danych zawartych w dokumentacji medycznej. Jedno z nich dotyczyło prośby o opinię w zakresie możliwości przekazania całej dokumentacji

[297] DOL.023.250.2023.
[298] Ustawa z 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270 ze zm.).

medycznej wszystkich leczonych pacjentów – zarówno w formie papierowej, jak i elektronicznej – przez lekarza, który prowadził swoją działalność w ramach spółki cywilnej i planował wyjście z tej spółki i przejście do innego podmiotu leczniczego.

W odpowiedzi organ nadzorczy, odwołując się do definicji administratora określonej w art. 4 pkt 7 RODO, wskazał, że spółka cywilna nie jest osobą prawną, jak również nie jest realnie podmiotem. Nie jest ona też osobą fizyczną lub organem publicznym, co oznacza, że spółka cywilna w żadnym przypadku nie jest administratorem. Natomiast jest nim każdy podmiot (np. lekarz), który – prowadząc indywidualną praktykę – zawarł umowę z innymi podmiotami, tworząc tym samym spółkę cywilną. Istotne jest w takim przypadku, czy między wspólnikami zachodzi relacja współadministrowania na gruncie art. 26 RODO, co mogłoby wynikać z faktu, że wspólnie ustalają cel przetwarzania, jakim jest wspólne prowadzenie działalności gospodarczej w ramach spółki cywilnej. Organ nadzorczy zwrócił także uwagę na przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[299], które regulują sposób prowadzenia dokumentacji medycznej oraz przetwarzania danych w niej zawartych. Zgodnie z art. 26 ust. 3 pkt 1 ww. ustawy podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną również podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych. Zatem ustawodawca przewidział możliwość udostępnienia dokumentacji medycznej, jednak warunkiem jest konieczność zapewnienia ciągłości świadczeń zdrowotnych. Organ wskazał, że nie można dysponować dokumentacją medyczną w oderwaniu od przepisów regulujących jej udostępnianie (art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta) oraz praw pacjentów, które wynikają z powyższych regulacji.

Organ nadzorczy odniósł się także do pytania, które dotyczyło wniosków pacjentów o udostępnienie nagrań zarejestrowanych na stanowiskach dyspozytora medycznego i wojewódzkiego koordynatora ratownictwa medycznego, funkcjonujących w strukturze urzędu wojewódzkiego, w związku z udostępnianiem dokumentacji medycznej[300]. W odpowiedzi UODO wskazał na treść ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, która w sposób zupełny reguluje zasady prowadzenia i udostępniania dokumentacji medycznej, a do których to zasad ustawodawca odwołuje się ustawodawca w art. 24f ustawy o Państwowym Ratownictwie Medycznym, stanowiącym, że: „1. W ramach SWD PRM[301] zapewnia się rejestrowanie nagrań rozmów prowadzonych na stanowisku dyspozytora medycznego oraz wojewódzkiego koordynatora ratownictwa medycznego, z wykorzystaniem dostępnych form łączności, i ich przechowywanie przez okres co najmniej 3 lat, licząc od dnia dokonania nagrania. 2. Do nagrań, o których mowa w ust. 1, stosuje się art. 24 oraz art. 26 ust. 1, 2 i 3 pkt 2, 2a i 3 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta”. W odpowiedzi podkreślono, że przepisy tej ustawy określają również, jakie podmioty (osoby) mają dostęp do danych o stanie zdrowia pacjenta i do dokumentacji medycznej, w której są one utrwalane. Prawo pacjenta do dokumentacji medycznej, jak i forma, w której może być mu ona udostępniona (ewentualnie osobom przez niego upoważnionym lub podmiotom uprawnionym na podstawie odrębnych przepisów prawa), także jasno określają ww. przepisy. Również w ustawie o systemie

[299] Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2024 r. poz. 581).
[300] DOL.023.679.2023.
[301] System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego.

powiadamiania ratunkowego jest określony zamknięty krąg podmiotów uprawnionych do nagrań takich rozmów. Organ nadzorczy zwrócił ponadto uwagę, że wynikające z art. 23 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta prawo dostępu do dokumentacji medycznej jest jednym z praw pacjenta zapewniającym mu dostęp do informacji o jego stanie zdrowia, natomiast uprawnienie przewidziane w art. 15 ust. 3 RODO, dotyczące możliwości pozyskania kopii danych, ma – jako jedno z najważniejszych praw podmiotu danych – charakter gwarancyjny i kontrolny, pozwalający np. na zweryfikowanie zgodności przetwarzania danych z prawem. W odpowiedzi organ wskazał, że realizacja tych uprawnień nie jest tożsama – pacjent, wnioskując o dostęp do dokumentacji medycznej, ma możliwość pozyskania wielu różnych informacji, których co do zasady nie jest uprawniony żądać na podstawie RODO.

Ciekawym zagadnieniem było także pytanie dotyczące obowiązku przekazywania danych na temat „zdarzeń medycznych” w ramach rządowego projektu „Elektroniczna platforma gromadzenia, analizy i udostępniania zasobów cyfrowych o zdarzeniach medycznych" (P1) przez fizjoterapeutów[302]. W odpowiedzi organ przypomniał, że dane o stanie zdrowia, zgodnie z art. 9 ust. 1 RODO, należą do szczególnej kategorii danych osobowych, których przetwarzanie – stosownie do art. 9 ust. 2 – jest dopuszczalne tylko warunkowo. Dla podmiotów udzielających świadczeń medycznych taką przesłanką jest art. 9 ust. 2 lit. h) RODO. Uprawnia ona do przetwarzania niezbędnego m.in. do celów profilaktyki zdrowotnej lub medycyny pracy oraz zapewnienia opieki zdrowotnej. Przepis ten nie stanowi jednak samodzielnej podstawy prawnej i funkcjonuje jedynie w połączeniu z odpowiednim przepisem szczególnym, który w przypadku sektora usług medycznych może być zawarty w wielu różnych ustawach, np.: ustawie o działalności leczniczej, ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawie o zawodach lekarza i lekarza dentysty[303], ustawie o zawodach pielęgniarki i położnej[304] itp. Organ nadzorczy wskazał, że od 1 lipca 2021 r., na podstawie art. 56 ustawy z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[305], na usługodawców został nałożony obowiązek raportowania danych dotyczących zdarzeń medycznych do systemu e-zdrowie, zapewnienia przez usługodawców możliwości dokonywania wymiany danych zawartych w elektronicznej dokumentacji medycznej. Usługodawcą, zgodnie z art. 2 pkt 15 ustawy o systemie informacji w ochronie zdrowia, jest świadczeniodawca, o którym mowa w art. 5 pkt 41 ustawy z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, oraz apteka. Z kolei ta ustawa określa, że świadczeniodawcą jest m.in. podmiot udzielający świadczeń zdrowotnych. Wskazany przepis nie różnicuje w żaden sposób usługodawców na podmioty publiczne albo prywatne. Zdaniem organu w tej sytuacji należy przyjąć, że obowiązek raportowania zdarzeń medycznych (a więc np. wizyty lekarskiej, pobytu w szpitalu, badań laboratoryjnych) dotyczy obu tych grup podmiotów.

Ad 5. Przetwarzanie danych osobowych w związku z wyborami parlamentarnymi

[302] DOL.023.274.2023.
[303] Ustawa z 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty (Dz. U. z 2023 r. poz. 1516 ze zm.).
[304] Ustawa z 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2024 r. poz. 814 ze zm.).
[305] Ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465 ze zm.).

Ze względu na odbywające się w 2023 r. wybory parlamentarne do UODO wpłynęło wiele pytań związanych z tą tematyką. W celu przybliżenia kwestii zgodnego z prawem przetwarzania danych osobowych na potrzeby kampanii wyborczej UODO zaktualizował i udostępnił na swojej stronie internetowej specjalny poradnik – „Ochrona danych osobowych w kampanii wyborczej". Przedstawiono w nim m.in. akty prawne regulujące przebieg wyborów, a także omówiono zasady dotyczące przetwarzania danych osobowych w procesie wyborczym, obwiązki administratora, administracji wyborczej i komitetów wyborczych, prawa wyborców i innych osób, których dane są przetwarzane.

Ponadto organ nadzorczy udzielał indywidualnych odpowiedzi na pytania. Przykładowo, w związku ze zmianami wprowadzonymi w Kodeksie wyborczym[306] w zakresie uprawnień mężów zaufania[307], pojawiły się pytania o możliwość nagrywania i fotografowania prac obwodowych komisji wyborczych przez mężów zaufania podczas całego głosowania, z zapewnieniem właściwej ochrony danych osobowych[308]. Odpowiadając na nie, organ nadzorczy wskazywał, że uprawnienia mężów zaufania określone są w art. 103b oraz w art. 42 ww. ustawy, który daje im prawo do rejestrowania czynności komisji wyborczych. Czynności obwodowej komisji wyborczej na obszarze kraju mogą być rejestrowane przez mężów zaufania z wykorzystaniem własnych urządzeń rejestrujących. Przepisy te wyraźnie określają cel takich działań. Zgodnie bowiem z art. 42 § 6 c) mąż zaufania przetwarza materiał zawierający zarejestrowany przebieg czynności, o których mowa w § 5, wyłącznie w celu, o którym mowa w § 6 lub 6 a), tj. zakwalifikowania go jako dokumenty z wyborów oraz w celu przekazania do ministra właściwego do spraw informatyzacji i usuwa go niezwłocznie, po przekazaniu zgodnie z § 6 a), z urządzenia rejestrującego oraz wszelkich, zarówno fizycznych, jak i wirtualnych, nośników pamięci, na których został zapisany, a których mąż zaufania pozostaje posiadaczem. Urząd Ochrony Danych Osobowych zauważył, że z przepisów Kodeksu wyborczego, dotyczących uprawnień mężów zaufania, wynika ich samodzielna pozycja względem organów wyborczych, a zatem posiadają oni status administratora w rozumieniu art. 4 pkt 7 RODO. W świetle przepisów RODO to administrator ponosi odpowiedzialność za prawidłowe przetwarzanie danych osobowych. W takiej sytuacji mężowie zaufania, jak każdy administrator, są zobowiązani do przestrzegania zasad dotyczących przetwarzania danych osobowych, wynikających z art. 5 RODO, m.in. zasady legalności, minimalizacji danych czy ograniczenia celu. Odpowiadają także za bezpieczeństwo przetwarzanych danych osobowych poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych, tak aby dane te nie były udostępniane osobom nieupoważnionym oraz aby były chronione przed zniszczeniem albo utratą (np. poprzez: szyfrowanie danych, pseudonimizację, zapewnienie integralności i poufności danych). Jednocześnie organ nadzorczy zwrócił uwagę, że ocena sposobu wykonywania ustawowych uprawnień mężów zaufania, wynikających z przepisów Prawa wyborczego należy do Państwowej Komisji

[306] Ustawa z 5 stycznia 2011 r. – Kodeks wyborczy (Dz. U. z 2023 r. poz. 2408 ze zm.).
[307] Art. 42 § 6a – art. 42 § 6d ustawy – Kodeks wyborczy zostały dodane przez art. 1 pkt 42 lit. c) ustawy z 26 stycznia 2023 r. o zmianie ustawy – Kodeks wyborczy oraz niektórych innych ustaw (Dz. U. z 2023 r. poz. 497) zmieniającej niniejszą ustawę z dniem 29 sierpnia 2023 r.
[308] Np. DOL.023.579.2023.

Wyborczej (PKW), jako organu powołanego do sprawowania nadzoru nad przestrzeganiem prawa wyborczego (zgodnie z art. 160 Kodeksu wyborczego)[309].

W tym czasie do UODO wpłynęło wiele spraw m.in. od okręgowych komisji wyborczych i delegatur Krajowego Biura Wyborczego dotyczących możliwości naruszenia ochrony danych osobowych przez różne komitety wyborcze w ramach tworzenia list kandydatów w okręgach wyborczych[310]. Zawiadomienia dotyczyły m.in. wątpliwości co do autentyczności arkuszy wykazu podpisów oraz co do prawdziwości danych zawartych w wykazach podpisów i wiarygodności podpisów osób udzielających poparcia konkretnym kandydatom[311]. W takich sprawach UODO wyjaśniał, że bezprawne przetwarzanie danych osobowych w rozumieniu art. 107 ustawy z 10 maja 2018 r. o ochronie danych osobowych stanowi przestępstwo ścigane z urzędu. Z kolei art. 304 ust. 1 Kodeksu postępowania karnego z 6 czerwca 1997 r. wskazuje, iż każdy, kto dowiedział się o popełnieniu przestępstwa ściąganego z urzędu, zobowiązany jest do powiadomienia prokuratora lub Policji. W ocenie organu nadzorczego zawiadomienie właściwej prokuratury o popełnieniu przestępstwa czyni zadość powyższemu obowiązkowi i pozwoli temu organowi na kompleksową ocenę prawnokarną czynu, również z punktu widzenia ewentualnego naruszenia zasad ochrony danych osobowych. Ze względu na znaczną liczbę zawiadomień w takich sprawach powyższe stanowisko organu ochrony danych osobowych zostało przedstawione także Przewodniczącemu Państwowej Komisji Wyborczej. Informacja wyjaśniająca „Kogo należy informować o możliwości popełnienia przestępstwa w związku ze zgłaszaniem kandydatów na posłów i senatorów?" została zamieszczona także w „Biuletynie UODO" 10/10/23. Wskazano w niej wprost, że: „O podejrzeniu popełnienia przestępstwa z zakresu ochrony danych osobowych w związku ze zgłaszaniem kandydatów na posłów i senatorów należy zawiadamiać organy ścigania. Informacje dotyczące czynów zabronionych nie powinny być kierowane do Prezesa UODO z oczekiwaniem przeprowadzenia postępowania pod kątem ustalenia naruszenia przepisów karnych z zakresu ochrony danych osobowych".

Ad 6. Ujawnianie danych osobowych w Internecie

Do organu nadzorczego wpływało wiele pytań związanych z ujawnianiem na stronach internetowych, w tym na portalach społecznościowych, danych osobowych, m.in. wizerunku dziecka[312] czy wizerunku kontrolerów biletów, zamieszczanych przez osoby fizyczne[313]. Organ nadzorczy przypominał wówczas, że do przetwarzania danych osobowych na portalu społecznościowym, poprzez udostępnienie tych danych w miejscu,

[309] PKW opublikowała na swojej stronie internetowej „Wyjaśnienia w sprawie uprawnień mężów zaufania i obserwatorów społecznych", zob. https://pkw.gov.pl/uploaded_files/1693566248_wyjasnienia-pkw-dotyczace-uprawnien-mezow-zaufania-i-obserwatorow-spolecznych-zpow71362023.pdf.

[310] DOL.023.763.2023, DOL.023.610.2023, DOL.023.614.2023, DOL.023.628.2023, DOL.023.640.2023, DOL.023.655.2023, DOL.023.659.2023, DOL.023.743.2023.

[311] Nieprawidłowości polegały m.in. na tym, że poparcia na liście kandydatów udzieliły osoby zmarłe Np. DOL.023.628.2023.

[312] DOL.023.704.2023.

[313] DOL.023.181.2023.

do którego dostęp ma szerokie grono osób, stosuje się przepisy RODO[314]. Osoba, która przetwarza dane osobowe we wskazany sposób, staje się wówczas administratorem w rozumieniu RODO i powinna spełnić obowiązki w nim określone, przede wszystkim legitymować się podstawą uprawniającą do przetwarzania danych. Przetwarzanie danych osobowych tzw. zwykłych będzie zgodne z prawem, jeśli spełniona zostanie któraś z uprawniających do tego przesłanek wymienionych w art. 6 ust. 1 RODO. Zgodnie z lit. a) tego przepisu przetwarzanie może opierać się na zgodzie osoby, której dane dotyczą. Inną podstawą przetwarzania może być prawnie uzasadniony interes administratora, który jednak nie powinien mieć charakteru nadrzędnego wobec praw i wolności osoby, której dane dotyczą, w szczególności, gdy osoba ta jest dzieckiem – lit. f). Ponadto zgodnie z art. 17 ust. 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć te dane, jeżeli m.in. były one przetwarzane niezgodnie z prawem. Organ podkreślił, że przetwarzanie danych osobowych w postaci wizerunku nie jest tożsame z rozpowszechnianiem wizerunku w rozumieniu ustawy o prawie autorskim i prawach pokrewnych[315], co skutkuje tym, iż wyrażenie zgody na przetwarzanie danych osobowych nie stanowi jednocześnie zgody na rozpowszechnianie wizerunku i odwrotnie. Urząd Ochrony Danych Osobowych przypomniał też, że przetwarzanie danych osobowych przez administratora fanpage'a uznawane jest za przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany, przez co do takiego przetwarzania danych ma zastosowanie ogólne rozporządzenie o ochronie danych. Zgodnie z jego art. 2 ust. 1 przepisy rozporządzenia stosuje się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Powyższe potwierdza wciąż aktualny pogląd wyrażony przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w wyroku z 6 listopada 2003 r. w sprawie C-101/01 (*Bodil Lindqvist*), zgodnie z którym operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków (…), stanowi przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany w rozumieniu art. 3 ust. 1 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

W 2023 r. Prezes UODO odniósł się także do kwestii umieszczania w Internecie przez instytucje naukowe skanów recenzji zawierających odręczny podpis w procedurze nadawania stopnia doktora, doktora habilitowanego lub tytułu profesora[316]. Wskazał, że dla oceny takich praktyk konieczne jest ustalenie, jakie konkretnie przepisy prawa powszechnie obowiązującego wymagają zamieszczenia pełnego skanu recenzji, nie zaś

[314] Odwołał się także do swojej decyzji z 10 stycznia 2022 r., znak DS.523.3629.2020, wskazującej, że jeżeli wizerunek osoby fizycznej jest publikowany na portalu internetowym bez zgody i jest on dostępny i adresowany do nieokreślonej grupy odbiorców, którzy nie tylko mogli, ale również w dalszym ciągu mogą zapoznać się z wizerunkiem tej osoby, nie można uznać, że takie udostępnienie wizerunku ma charakter prywatny i nie stanowi naruszenia prawa osoby fizycznej do ochrony jej danych osobowych.
[315] Stanowi o tym art. 81 ustawy z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509).
[316] DOL.023.691.2023.

samej jej treści, na stronie internetowej instytucji naukowej. Zgodnie z art. 188 ust. 1 lit. b) ustawy – Prawo o szkolnictwie wyższym i nauce[317]: „podmiot doktoryzujący udostępnia w BIP na swojej stronie podmiotowej, nie później niż w terminie (…) recenzje". Przepis ten nie wskazuje na obowiązek zamieszczania pełnego skanu recenzji zawierającej podpis, więc jeśli praktyka ta wynika wyłączenie z wewnętrznych procedur danej instytucji naukowej, to instytucja ta jako administrator powinna ocenić, czy ujawnianie skanu podpisu jest niezbędne z punktu widzenia zasady zgodności z prawem, rzetelności i przejrzystości, zasady ograniczenia celu oraz zasady minimalizacji danych, wyrażonych w art. 5 ust. 1 RODO. Jeżeli administrator nie będzie w stanie wykazać podstawy prawnej przetwarzania danych, w tym skanu podpisu, to zgodnie z art. 17 RODO osobie, której dane dotyczą, przysługuje prawo do usunięcia danych. Organ nadzorczy podkreślał, że w większości przypadków podpis odręczny, jeżeli będzie umożliwiał jednoznaczną identyfikację osoby fizycznej, może zostać uznany za dane osobowe w rozumieniu art. 4 pkt 1 RODO. Sytuacja taka zachodzi w przypadku tzw. podpisów biometrycznych. Nie zmienia to jednak faktu, że administrator, umieszczając skan podpisu odręcznego w przestrzeni publicznej, powinien dokonać analizy ryzyka, zważywszy na fakt, że w określonych przypadkach ujawnienie odręcznego podpisu osoby może, w powiązaniu z dodatkowymi informacjami o tej osobie, zwiększać ryzyko takich negatywnych zjawisk, jak fałszowanie dokumentów, podszywanie się pod osobę czy kradzież tożsamości. Taka analiza ryzyka powinna być elementem projektowania ochrony danych i tzw. domyślnej ochrony danych – art. 25 ust. 1 i 2 RODO. Wykorzystanie ww. instrumentów RODO powinno przyczynić się do ograniczenia ryzyk dla osób, których dane osobowe będą umieszczane w przestrzeni powszechnie dostępnej, jaką jest Internet.

Ad 7. Przetwarzanie danych osobowych z wykorzystaniem nowych technologii

W okresie objętym niniejszym sprawozdaniem podmioty publiczne występowały do organu właściwego do spraw ochrony danych osobowych z prośbą o zajęcie stanowiska w kwestii podstaw prawnych dotyczących przetwarzania danych osobowych z wykorzystaniem różnego rodzaju aplikacji, które usprawniałyby ich funkcjonowanie. Przykładem może być sprawa dotycząca propozycji opracowania i wdrożenia aplikacji, w ramach której Krajowa Rada Kuratorów gromadziłaby dane osobowe uczestników zdarzeń niebezpiecznych z udziałem kuratorów sądowych[318]. Jak argumentowano w piśmie do organu nadzorczego, wdrożenie owego narzędzia, polegające na składaniu indywidualnych zgłoszeń oraz generowaniu raportów zdarzeń, zgodnie z przyjętymi założeniami, miałoby na celu ułatwienie procesu zgłaszania i dokumentowania tego rodzaju sytuacji. Aby aplikacja ta była w pełni funkcjonalna, a uzyskiwane raporty rzetelne i miarodajne, konieczne było gromadzenie i przetwarzanie danych osobowych, w tym m.in. imienia i nazwiska osób uczestniczących w zdarzeniu o charakterze niebezpiecznym, nazwy pracodawcy i zespołu kuratorskiego, numeru telefonu, adresu e-mail oraz opisu zdarzenia. Organ nadzorczy, przedstawiając swoje stanowisko, zauważył, że kompetencje Krajowej Rady Kuratorów – określone w art. 46 ustawy o kuratorach sądowych[319] – nie zawierają podstawy prawnej do gromadzenia i przetwarzania danych osobowych

[317] Ustawa z 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742 ze zm.).
[318] DOL.023.581.2023.
[319] Ustawa z 27 lipca 2001 r. o kuratorach sądowych (Dz. U. z 2023 r. poz. 1095).

w aplikacji. Z przepisu tego wynika, że rolą Krajowej Rady Kuratorów jest m.in.: podejmowanie działań umożliwiających kuratorom zawodowym podnoszenie kwalifikacji zawodowych i poziomu wykonywanej przez nich pracy (art. 46 ust. 1 pkt 2); występowanie do Ministra Sprawiedliwości lub innych organów państwowych z wnioskami dotyczącymi warunków pracy i płacy grupy zawodowej kuratorów sądowych (art. 46 ust. 1 pkt 4); dokonywanie okresowej oceny sądowej kadry kuratorskiej oraz liczby wykonywanych nadzorów i dozorów oraz przedstawianie wniosków w tym zakresie Ministrowi Sprawiedliwości (art. 46 ust. 1 pkt 6). Tak określone kompetencje nie dają podstawy do prowadzenia przez organ samorządu kuratorskiego aplikacji z danymi osobowymi o charakterze sensytywnym. Przepis art. 9b. ww. ustawy wskazuje, że administratorem danych przetwarzanych w celu wykonania zadań lub obowiązków przez kuratora sądowego jest prezes sądu, w którym kurator sądowy pełni obowiązki służbowe. Prezes UODO podkreślił, że brak w przepisach ustawy o kuratorach sądowych odrębnej podstawy prawnej do przetwarzania danych osobowych przez Krajową Radę Kuratorów w aplikacji powoduje, że w celu umożliwienia funkcjonowania takiego narzędzia informatycznego konieczne są zmiany w ustawie o kuratorach sądowych. To z przepisów prawa powinny bowiem wynikać kluczowe procesy związane z odpowiedzialnością za przetwarzane dane w tego typu aplikacji. Zwrócił także uwagę, że działanie aplikacji, w której mają być przetwarzane dane osobowe osób uczestniczących w zdarzeniu o charakterze niebezpiecznym, potencjalnie może wiązać się z przetwarzaniem tych danych na dużą skalę, z użyciem nowych technologii. Biorąc pod uwagę specyfikę zdarzeń o charakterze niebezpiecznym, do których dochodzi w ramach pracy kuratorów sądowych, nie może też umknąć uwadze, że w planowanej aplikacji oprócz danych zwykłych mogą być przetwarzane szczególne kategorie danych osobowych, jak np. dane o: stanie zdrowia, niepełnosprawności, seksualności, orientacji seksualnej, których przetwarzanie jest co do zasady zakazane, a dopuszczalne wyjątkowo, po spełnieniu warunków określonych w art. 9 ust. 2 ogólnego rozporządzenia o ochronie danych. Również wykonywanie operacji na danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, które to dane potencjalnie także mogą być przetwarzane w planowanej aplikacji, jest możliwe pod szczególnymi warunkami – wskazanymi w art. 10 RODO. Dlatego tworzenie takiej aplikacji, a także przepisów dających podstawę prawną do jej działania, powinno być poprzedzone szczególnie wnikliwymi analizami, uwzględniającymi wszelkie ryzyka wynikające z przyjęcia takich rozwiązań. Dodatkowo regulacje w tym zakresie powinny przewidywać odpowiednie zabezpieczenia praw i wolności osób, których dane będą przetwarzane. Prezes UODO przypomniał również, że opracowywanie i wdrażanie aplikacji, a także projektowanie rozwiązań legislacyjnych statuujących przetwarzanie w aplikacji danych osobowych, powinno być również poprzedzone testem prywatności – uwzględnieniem ochrony danych w fazie projektowania (art. 25 ust. 1 RODO) oraz oceną skutków dla ochrony danych (art. 35 ust. 1 i ust. 10 RODO).

Przedmiotem analiz organu nadzorczego była też kwestia danych pomiarowych. Do UODO wpłynęło bowiem pytanie, czy szczegółowe dane dotyczące zużycia energii (profil zużycia energii dotyczący konkretnego punktu pomiarowego, a także dane ukazujące na mapach graficzne wizualizacje udziałów poszczególnych nośników energii wraz ze wskaźnikami zużycia energii) są danymi osobowymi i czy gmina może je pozyskać od

przedsiębiorstw energetycznych[320]. Organ nadzorczy wskazał, że dane pomiarowe, które choćby pośrednio pozwalają na odtworzenie profilu zużycia energii indywidualnego odbiorcy, mogą stanowić dane osobowe w rozumieniu art. 4 pkt 1 RODO. Odniósł się przy tym do zachowującej wciąż ważność Opinii 12/2011 Grupy Roboczej Art. 29 na temat inteligentnego pomiaru zużycia (smart metering) wskazującej, że inteligentne liczniki instalowane u odbiorców energii posiadają zdolność dwustronnej komunikacji. Informują konsumentów o ilości zużywanej energii, przy czym informacja ta potencjalnie może być również przekazywana dostawcom energii i innym wyznaczonym podmiotom. Kluczową cechą inteligentnych liczników jest możliwość zdalnej komunikacji pomiędzy licznikiem i upoważnionymi podmiotami, takimi jak: dostawcy, operatorzy sieci, upoważnione osoby trzecie lub przedsiębiorstwa usług energetycznych. Jednocześnie organ nadzorczy wskazał, że pozyskiwanie danych pomiarowych, a także obowiązki z tym związane regulują przepisy ustawy – Prawo energetyczne[321]. Zasady pozyskiwania informacji przez gminę w celu opracowania projektu założeń do planu zaopatrzenia w ciepło, energię elektryczną i paliwa gazowe, zwanego dalej „projektem założeń", określa art. 19 ust. 4 Prawa energetycznego, zgodnie z którym przedsiębiorstwa energetyczne udostępniają nieodpłatnie wójtowi (burmistrzowi, prezydentowi miasta) plany, o których mowa w art. 16 ust. 1 Prawa energetycznego, w zakresie dotyczącym terenu tej gminy, oraz propozycje niezbędne do opracowania projektu założeń. Organ podkreślił, że udostępniając gminom informacje dla opracowania projektu założeń, przedsiębiorstwa energetyczne muszą w pierwszej kolejności dokonać analizy, jakie informacje są niezbędne dla realizacji tego zadania i mogą być przekazywane, z uwzględnieniem zasad ochrony danych osobowych określonych w art. 5 RODO, zwłaszcza ograniczenia celu – art. 5 ust. 1 lit. b) RODO oraz minimalizacji danych – art. 5 ust. 1 lit. c) RODO. Przedsiębiorstwa energetyczne, dokonując oceny, jakie informacje mogą być przekazywane, muszą również uwzględniać przepisy rozporządzenia Ministra Klimatu i Środowiska z 10 stycznia 2022 r. w sprawie procesów rynku energii[322], które określa m.in. wymagania dotyczące zapewnienia poprawności i kompletności informacji rynku energii oraz ich weryfikacji, a także zawiera wzory szablonu oceny skutków w zakresie ochrony danych pomiarowych. W przypadku gdy wnioskowane przez gminę informacje mogące stanowić dane osobowe (np. profil zużycia energii dotyczący poszczególnego punktu pomiarowego) nie są niezbędne dla realizacji wskazanego w przepisach celu, to przedsiębiorstwa energetyczne nie powinny przekazywać tych danych jako nadmiarowych.

Ad 8. Przetwarzanie danych osobowych w ramach dostępu do informacji publicznej

W ostatnich latach organ nadzorczy otrzymywał wiele pytań związanych z wyważaniem dwóch praw – prawa do ochrony danych osobowych i prawa do informacji publicznej/jawności życia publicznego. Przykładem mogą być sprawy związane z żądaniem udostępnienia informacji o wynagrodzeniu pracowników gminy pełniących funkcje publiczne[323], wynagrodzeniu pracowników powiatowej stacji

[320] DOL.023.272.2023.
[321] Ustawa z 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2023 r. poz. 1681 ze zm.).
[322] Dz. U. poz. 234.
[323] Np. DOL.023.617.2023.

sanitarno-epidemiologicznej[324] czy informacji o nauczycielach[325]. Prezes UODO wskazywał, że takie wnioski powinny być rozpatrywane w trybie ustawy o dostępie do informacji publicznej[326] z uwzględnieniem zwłaszcza jej art. 5 ust. 2, zgodnie z którym prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej. Ogólne rozporządzenie o ochronie danych w art. 86 wskazuje, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny, lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlega ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia. Oznacza to, że ogólne rozporządzenie o ochronie danych nie wyłącza prawa dostępu do informacji publicznej. Niemniej podmiot udostępniający informację publiczną musi czynić zadość zasadom wynikającym z art. 5 RODO, przede wszystkim zasadom ograniczenia celu oraz minimalizacji danych, oraz w każdym przypadku rozważyć, czy informacje, które udostępnia, nie będą naruszały prywatności osoby, której dane dotyczą. W sytuacji kiedy udostępnienie dokumentów, w tym danych osobowych, będzie naruszało prywatność osoby, której dane dotyczą – wówczas podmiot będący dysponentem informacji publicznej będzie zobowiązany do zanonimizowania tych danych osobowych, których przetwarzanie będzie naruszało prawo do ochrony danych osobowych. W każdym przypadku o udostępnieniu informacji publicznej w pierwszej kolejności rozstrzyga podmiot, w którego dyspozycji informacje te się znajdują. To w jego gestii pozostaje ocena, czy określone informacje mieszczą się w zakresie pojęcia informacji publicznej czy informacji sektora publicznego oraz czy ich udostępnienie na gruncie przepisów wyżej powołanej ustawy jest prawnie dopuszczalne. Podmiot ten decyduje również o zakresie udostępnianych informacji.

W 2023 r. do UODO wpłynęło także pytanie dotyczące legalności nagrywania przebiegu posiedzenia Głównej Komisji Orzekającej Ministerstwa Finansów w sprawach o naruszenia dyscypliny finansów publicznych przez uczestnika rozprawy[327]. W odpowiedzi Prezes UODO wskazał na przepisy dotyczące funkcjonowania Głównej Komisji Orzekającej, które zawarte są w ustawie z 17 grudnia 2014 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych[328]. Zgodnie z jej art. 119 rozprawa przed komisją orzekającą jest jawna (ust. 1), a wyłączenie jawności rozprawy lub jej części może nastąpić wyłącznie ze względu na bezpieczeństwo państwa lub ochronę informacji niejawnych bądź z uwagi na zagrożenie spokoju i porządku publicznego (ust. 2). Ogłoszenie orzeczenia w sprawie o naruszenie dyscypliny finansów publicznych jest jawne (ust. 3). Ponadto z przebiegu rozprawy protokolant, pod kierunkiem przewodniczącego składu orzekającego, sporządza protokół (art. 123 ust. 1). Przewodniczący składu orzekającego może zarządzić utrwalenie przebiegu rozprawy za pomocą urządzenia rejestrującego dźwięk niezależnie od sporządzania protokołu, o czym uprzedza

[324] DOL.023.344.2023.
[325] DOL.023.289.2023.
[326] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).
[327] DOL.023.341.2023.
[328] Dz. U. z 2024 r. poz. 104.

uczestników rozprawy. Zapis dźwięku przełożony na pismo może być dołączony do protokołu. Zarejestrowany dźwięk nie stanowi dowodu w postępowaniu (art. 123 ust. 3).

Organ uznał, że jawność rozprawy nie jest równoznaczna z możliwością jej nagrywania na innych zasadach niż przewidują to powołane powyżej przepisy. W sytuacji gdy przepisy przewidują określoną procedurę, to odstępstwa od niej musiałyby być w nich również przewidziane. Dlatego, jeżeli osoba biorąca udział w posiedzeniu chciałaby nagrywać jego przebieg, musi mieć na uwadze powyższe regulacje, które wprost wskazują, w jaki sposób następuje utrwalanie przebiegu postępowania. Zaznaczono również, że w każdej sytuacji, w której dana osoba chciałaby dokonać nagrania określonych osób, należy zwrócić uwagę, dla realizacji jakiego celu takie nagranie miałoby być dokonane. Jeżeli takie nagranie godziłoby – w ocenie nagrywanych osób – w ich dobra osobiste, to na gruncie procesu cywilnego będą mogły one dochodzić swoich roszczeń. Istotne jest także to, czy nagrywany będzie jedynie dźwięk, czy też obraz. Wizerunek jest bowiem dobrem osobistym, o którym mowa w art. 23 Kodeksu cywilnego, a jego ochrona uregulowana została w art. 24 Kodeksu cywilnego. Zgodnie z obowiązującymi przepisami, w celu dochodzenia swoich praw, osoba, w której odczuciu jej dobra osobiste zostały naruszone, może wystąpić na drogę sądowego postępowania cywilnego.

12.1.2. Pytania od inspektorów ochrony danych

Organ nadzorczy niezmiennie podkreśla, iż rola inspektorów ochrony danych ma fundamentalne znaczenie dla budowy skutecznego systemu ochrony danych osobowych. Przejawia się ona głównie we wspieraniu administratorów w realizacji obowiązków dotyczących ochrony danych osobowych, a także w pełnieniu funkcji punktu kontaktowego dla osób, których dane dotyczą, oraz dla organu nadzorczego. Jednocześnie IOD ma prawo zwrócić się do organu nadzorczego o udzielenie mu konsultacji w kwestiach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem swojej funkcji, co ma istotne znaczenie dla doskonalenia systemu ochrony danych osobowych. Z powyższych względów współpraca z inspektorami ochrony danych jest dla UODO niezmiernie istotna. Działania organu w tym zakresie polegają przede wszystkim na udzielaniu inspektorom konsultacji i porad. Jednocześnie pytania przesyłane przez inspektorów są dla organu nadzorczego ważnym źródłem wiedzy na temat problemów, z jakimi mierzą się oni w związku z pełnieniem swojej funkcji. W wielu przypadkach inspektorzy trafnie identyfikują problemy prawne wynikające np. z luk w przepisach prawa lub nieodpowiedniej interpretacji przepisów. W takich sytuacjach IOD oczekują od UODO wskazówek lub podjęcia stosownych działań, np. skierowania wystąpienia legislacyjnego. Zdarza się, że inspektorzy wcześniej sami przedstawiają bezpośrednio resortowi zaobserwowane problemy, a jeśli sygnały te nie doprowadzają do ich rozwiązania, wówczas zwracają się o pomoc do UODO.

W 2023 r. do Urzędu Ochrony Danych wpłynęły **253 pytania od inspektorów ochrony danych.** Udzielono zaś **246 odpowiedzi na pytania od IOD.** Nieznaczny spadek liczby wpływających pytań (w 2022 r. wpłynęły 274 pytania, w 2021 r. – 301) wynikać może z tego, że wiele kwestii związanych z właściwym stosowaniem przepisów dotyczących ochrony danych osobowych, w tym pełnienia funkcji IOD, zostało wyjaśnionych w poprzednich latach, zarówno w ramach indywidualnej korespondencji z inspektorami,

jak i w specjalnej zakładce adresowanej do inspektorów ochrony danych – „Newsletterze dla IOD” (obecnie „Biuletynie UODO”). Zamieszczane tam wskazówki nie tylko pozwalały ocenić, jak postąpić w podobnej sprawie, ale również poprzez wskazanie kryteriów i etapów działań podpowiadały na przykład, w jaki sposób dokonać analizy w zakresie określania ról podmiotów, podstaw prawnych czy oceny wniosków o udostępnienie danych. W materiałach tych organ nadzorczy prezentował również kierunek i zasady interpretacji przepisów, pomocne przy rozstrzyganiu wątpliwości z zakresu ochrony danych osobowych.

Pytania przesyłane przez inspektorów w 2023 r. dotyczyły bardzo różnych zagadnień. Zasadniczo można je podzielić na dwie większe grupy, w których wyodrębnić można kilka tematów. Pierwsza grupa pytań obejmuje zagadnienia, które niezmiennie od kilku lat pojawiają się w pytaniach IOD, mianowicie: występowanie konfliktu interesów w związku z pełnieniem funkcji IOD, określenie statusu podmiotów biorących udział w procesie przetwarzania danych osobowych, udostępnianie danych osobowych czy problemy ze stosowaniem w praktyce zarówno przepisów prawa dotyczących ochrony danych osobowych, jak i przepisów sektorowych.

Natomiast druga szeroka grupa pytań od IOD dotyczyła w 2023 r. wydarzeń i problemów bieżących, takich jak kwestie statusu podmiotów przetwarzających dane osobowe na potrzeby organizacji wyborów do parlamentu, które odbyły się w roku sprawozdawczym, czy zagadnienia związane z przetwarzaniem danych osobowych w związku ze stosowaniem przepisów ustawy o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli, która weszła w życie w 2023 r.

Przekazywane przez IOD informacje o pojawiających się problemach w stosowaniu przepisów o ochronie danych osobowych pozwoliły organowi na bieżąco podejmować działania zmierzające do podnoszenia poziomu ochrony danych osobowych, w tym m.in. poprzez:

1) udzielanie odpowiedzi na pytania IOD i przygotowywanie wyjaśnień publikowanych na stronie internetowej UODO lub w „Newsletterze UODO dla IOD” / „Biuletynie UODO”;
2) sygnalizowanie właściwym podmiotom zaobserwowanych nieprawidłowości lub potrzeby zmian legislacyjnych.

Udzielanie odpowiedzi na pytania IOD

W omawianym okresie sprawozdawczym do najczęściej poruszanych lub szczególnie ważnych zagadnień, których dotyczyły pytania i sygnały od inspektorów ochrony danych, zaliczyć można:

1) wyznaczanie, status i zadania inspektora ochrony danych i jego zastępcy,
2) określenie statusu podmiotów w procesie przetwarzania danych osobowych,
3) udostępnianie danych osobowych,
4) stosowanie różnych form monitoringu,
5) status podmiotów realizujących zadania związane z wyposażaniem uczniów i nauczycieli w laptopy,
6) nowe technologie,
7) nagrywanie rozmów z interesantami przez podmioty publiczne.

Ad 1. Wyznaczanie, status i zadania inspektora ochrony danych oraz jego zastępcy

Wiele z pytań kierowanych do UODO w 2023 r. nadal dotyczyło wątpliwości w zakresie wyznaczania, statusu i zadań IOD oraz jego zastępcy, w tym konfliktu interesów oraz prawidłowego rozdzielenia ról administratora i IOD. Mimo że Prezes UODO udzielał wielu wskazówek w tym zakresie, to jednak pewne szczegółowe i praktyczne kwestie nadal budzą wątpliwości i wymagają udzielenia dodatkowych wyjaśnień odnoszących się do konkretnych sytuacji.

Często zgłaszane w pytaniach od IOD wątpliwości dotyczyły oceny, czy nałożenie na inspektora określonego dodatkowego zadania nie spowoduje wystąpienia konfliktu interesów, o czym mowa w art. 38 ust. 6 RODO. Zgodnie z tym przepisem IOD może wykonywać inne zadania i obowiązki, o ile administrator lub podmiot przetwarzający zapewni, aby te zadania i obowiązki nie powodowały konfliktu interesów. Ze względu na charakter zadań IOD, skupiających się na doradzaniu oraz monitorowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, oraz wymóg sprawowania tej funkcji w sposób niezależny administrator nie powinien nakładać na IOD zadań, które zgodnie z przepisami RODO należą do administratora. Przyjęcie odmiennego rozwiązania, w którym IOD byłby odpowiedzialny za wykonanie określonego zadania administratora, np. zgłaszanie naruszeń, a jednocześnie miałby monitorować zgodność wykonywania tego zadania z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b) RODO, doprowadziłoby w efekcie do sytuacji, w której IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów.

Taka sytuacja może mieć miejsce np. w przypadku udzielania inspektorowi pełnomocnictwa do reprezentowania administratora w sprawach dotyczących ochrony danych osobowych. Wątpliwości w tym zakresie zgłaszane były przez inspektorów w bieżącym okresie sprawozdawczym[329]. W odpowiedziach na pytania dotyczące tego zagadnienia organ wskazywał, że IOD nie powinien być pełnomocnikiem administratora − w zakresie, w jakim mogłoby to powodować konflikt interesów, o którym mowa w art. 38 ust. 6 RODO − w tym nie powinien podpisywać zawiadomień o wyznaczeniu, odwołaniu czy zmianie danych IOD/administratora, formularzy zgłoszenia naruszenia czy pism, w których w imieniu administratora miałby zobowiązywać się do realizacji pewnych działań, w tym doskonalących np. wdrożenie nowych rozwiązań informatycznych związanych z podniesieniem bezpieczeństwa danych. Zadaniem IOD jest bowiem informowanie administratora o obowiązkach spoczywających na nim na mocy RODO oraz monitorowanie wykonania tych obowiązków – art. 39 ust. 1 lit. a) i b) RODO. Występowanie w roli pełnomocnika administratora w zakresie obowiązków nałożonych na administratora może istotnie utrudniać lub uniemożliwiać inspektorowi niezależną ocenę, czy obowiązki administratora są wykonywane prawidłowo.

Dodatkowo, odnosząc się do pytań, czy IOD może być pełnomocnikiem administratora w sprawach naruszeń, organ nadzorczy wskazywał, że zgodnie z art. 33 ust. 1 RODO obowiązkiem administratora jest zgłaszanie naruszenia ochrony danych. Natomiast stosownie do ust. 3 lit. b) powołanego przepisu zgłoszenie takie musi zawierać

[329] Np. DOL.502.141.2023, DOL.502.134.2023.

m.in. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji. Obowiązki inspektora ograniczone zostały zatem do pełnienia punktu kontaktowego dla organu nadzorczego w zakresie udzielania dodatkowych informacji na temat naruszenia. Oznacza to, że jeśli organ nadzorczy zwróciłby się do inspektora o przedstawienie dodatkowych wyjaśnień dotyczących naruszenia (jako do punktu kontaktowego w zakresie naruszeń, zgodnie z art. 33 RODO), wówczas IOD przesyłałby te wyjaśnienia we własnym imieniu (w wykonaniu własnych zadań) i opatrywał własnym podpisem. W art. 33 RODO wyraźnie rozróżniono, jakie zadania związane ze zgłoszeniem naruszenia przypisane są administratorowi, a jakie inspektorowi ochrony danych.

Warto nadmienić, że zgodnie z art. 83 ust. 4 lit. a) RODO za naruszenie art. 38 ust. 6 RODO, tj. nałożenie na IOD zadania powodującego konflikt interesów, organ nadzorczy może nałożyć na administratora administracyjną karę pieniężną. Karą administracyjną obwarowano zatem obowiązki administratorów dotyczące nie tylko wyznaczania inspektora ochrony danych, posiadania przez niego właściwych kwalifikacji i gwarancji niezależności, ale też zapewnienia, aby wyznaczony inspektor mógł prawidłowo realizować swoje zadania.

Z drugiej strony inspektor ochrony danych, ze względu na odgrywaną rolę fachowego doradcy i podmiotu monitorującego w sposób niezależny przestrzeganie przepisów o ochronie danych osobowych, powinien ze swej strony odpowiednio wcześnie identyfikować oraz sygnalizować administratorowi ryzyko wystąpienia takiego konfliktu, by możliwe było odpowiednio wczesne zapobieganie mu. W niektórych przypadkach konieczne może być powstrzymanie się przez inspektora od dokonywania czynności w imieniu administratora lub wypowiedzenie udzielonego mu pełnomocnictwa.

Analogicznie do konfliktu interesów może dochodzić w przypadku umocowania IOD do reprezentowania administratora i prowadzenia w jego imieniu korespondencji w sprawach dotyczących postępowań skargowych. Przy czym w takiej sytuacji dodatkowo, biorąc pod uwagę fakt pełnienia przez inspektora roli punktu kontaktowego dla osób, których dane dotyczą (zgodnie z art. 38 ust. 4 RODO), osoby te, mogłyby mieć uzasadnione obawy co do bezstronności IOD i – w związku z tym -– ograniczone możliwości korzystania z pomocy inspektora w wyjaśnieniu swoich wątpliwości dotyczących przetwarzania ich danych przez administratora. Dotyczy to zarówno etapu przed złożeniem skargi, jak i po jej złożeniu. Do podobnej sytuacji odniósł się włoski organ ochrony danych, który w jednej ze swoich decyzji uznał, że administrator naruszył art. 38 ust. 6 RODO, wyznaczając swojego IOD do obrony w postępowaniu sądowym. Jako argument za przyjęciem tego stanowiska wskazano w szczególności, że „w oczach zainteresowanego, który chce zwrócić się do inspektora ochrony danych, fakt, że jest to jednocześnie obrońca prawny instytucji (administratora), podważa jego niezależność”.

Dodatkowo należy zwrócić uwagę na jeszcze jeden aspekt związany z występowaniem IOD w imieniu administratora (na podstawie pełnomocnictwa) przed organem nadzorczym. Zadaniem pełnomocnika jest ochrona interesów mocodawcy, działanie według instrukcji i sugestii mocodawcy, co stoi w sprzeczności z niezależnością inspektora ochrony danych, zagwarantowaną w art. 38 ust. 3 RODO (nakaz nieotrzymywania instrukcji). Podstawowym zadaniem IOD jest monitorowanie

przestrzegania przepisów o ochronie danych osobowych przez administratora i doradzanie w tym zakresie. Zatem głównym celem IOD nie jest działanie wyłącznie w interesie administratora (wskazują na to wprost przepisy determinujące status IOD, takie jak art. 38 ust. 3, ust. 4 oraz ust. 6 RODO). Tymczasem IOD, działający przed organem nadzorczym na podstawie pełnomocnictwa wydanego przez administratora, mógłby być np. zobowiązany do składania w imieniu mocodawcy wyjaśnień dotyczących przetwarzania danych osobowych przez administratora zgodnie z wolą i interesem mocodawcy, a więc mógłby być np. zmuszony do pomijania własnych spostrzeżeń i rekomendacji, które wypracował jako IOD.

Z powyższych powodów należy uznać, że co do zasady występowanie IOD roli pełnomocnika administratora przed organem nadzorczym – w sprawach z zakresu ochrony danych osobowych – stoi w kolizji z nakazem nienakładania na IOD zadań powodujących konflikt interesów oraz z nakazem zapewnienia, aby IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań.

Kolejne pytanie dotyczyło roli, jaką powinien pełnić inspektor ochrony danych w związku z kwalifikowaniem zaistniałego naruszenia[330]. Organ nadzorczy wskazał, że rola inspektora ochrony danych powinna ograniczać się w szczególności do doradzania administratorowi, zaś ostateczna decyzja co do kwalifikacji naruszenia powinna należeć do administratora (art. 33 ust. 1 RODO). Nie można bowiem nakładać na inspektora dodatkowych obowiązków, które mogłyby powodować konflikt interesów, w szczególności obowiązków przypisanych w przepisach RODO administratorowi. Jak wskazano w Wytycznych EROD 9/2022 w sprawie powiadamiania o naruszeniu ochrony danych osobowych zgodnie z RODO, obowiązkowe zadania inspektora ochrony danych, które mają szczególne znaczenie dla powiadamiania o naruszeniu, obejmują m.in. udzielanie porad i informacji w zakresie ochrony danych administratorowi lub podmiotowi przetwarzającemu, monitorowanie zgodności z RODO oraz udzielanie porad w odniesieniu do ocen skutków dla ochrony danych. Inspektor ochrony danych musi również współpracować z organem nadzorczym i działać jako punkt kontaktowy dla organu nadzorczego i dla osób, których dane dotyczą. W związku z powyższymi zadaniami inspektora ochrony danych EROD zaleca, aby inspektor był niezwłocznie informowany o zaistnieniu naruszenia i był zaangażowany w cały proces zarządzania naruszeniami oraz powiadamiania.

Inna kwestia związana z nakładaniem na IOD zadań administratora dotyczyła tego, czy IOD jest osobą właściwą do podpisania informacji przygotowanej na podstawie art. 15 RODO. Zarówno art. 15, jak i art. 12 RODO wskazują na administratora jako podmiot, który w określony sposób i w określonym terminie ma realizować prawa osób, których dane dotyczą, a dodatkowo przewidzieć procedury mające na celu realizację tych praw i ułatwienie ich realizowania. Zatem udzielenie informacji na podstawie art. 15 RODO należy do zadań administratora. Rola IOD jako punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO), jest mocno powiązana z tymi obowiązkami administratora i ma przyczyniać się do skuteczniejszego ich wykonywania. Rolą IOD jest bowiem budowanie świadomości administratora w zakresie praw tych osób, a następnie monitorowanie skuteczności przyjętych w tym zakresie procedur i rozwiązań, a gdy to

[330] DOL.502.184.2023.

konieczne – proponowanie ich modyfikacji. Ponadto osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Jednak pełnienie ww. funkcji punktu kontaktowego dla osób, których dane dotyczą, nie powinno prowadzić do wyręczania administratora przez IOD w jego obowiązkach, ponieważ nie mógłby przez to realizować własnych, tj. w sposób niezależny monitorować i doradzać administratorowi w zakresie tych obowiązków. Nieprzestrzeganie rozróżnienia tych dwóch ról mogłoby doprowadzić do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do IOD art. 38 ust. 6 RODO. Dlatego w ocenie organu nadzorczego rolę punktu kontaktowego należy rozumieć raczej jako wsparcie dla osób, których dane dotyczą, w sytuacjach, gdy osoby zgłosiłyby zastrzeżenia, trudności czy wątpliwości co do wykonywania praw przysługujących im na mocy RODO.

Odnosząc się z kolei do dodatkowego pytania tego samego inspektora, czy w przypadku braku możliwości podpisania informacji przygotowanej na podstawie art. 15 RODO przez IOD może on podpisać taką informację jako pełnomocnik administratora, organ nadzorczy – podobnie jak w wyżej przedstawionych sprawach – wskazał, że IOD nie powinien być pełnomocnikiem administratora. Odgrywanie przez IOD roli pełnomocnika w sprawach z zakresu ochrony danych osobowych u administratora, u którego IOD pełni swoją funkcję, stoi w kolizji z nakazem nienakładania na IOD zadań powodujących konflikt interesów (art. 38 ust. 6 RODO) oraz z niezależnością inspektora ochrony danych zagwarantowaną w RODO, w tym w art. 38 ust. 3.

W odpowiedzi na pytanie, czy inspektor ochrony danych pełniący swą funkcję u pracodawcy może jednocześnie pełnić funkcję przewodniczącego/zastępcy przewodniczącego/członka zarządu w związku zawodowym działającym u tego samego pracodawcy[331], organ nadzorczy wskazał, że administrator zobowiązany jest zapewnić inspektorowi ochrony danych możliwość niezależnego i prawidłowego wykonywania jego zadań. W tym celu zobowiązany jest dokonać starannej oceny, czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów. Oceniając przedstawioną sytuację, trzeba mieć ponadto na uwadze, że związki zawodowe nie mogą mieć dostępu do danych osobowych pracowników poza przypadkami i zakresem wskazanymi przepisami prawa (ustawy o związkach zawodowych). Tymczasem w sytuacji, gdyby np. członek władz związku pełnił równocześnie funkcję IOD u pracodawcy, miałby wówczas dostęp do danych pracowników w dużo szerszym zakresie, w związku z wykonywaniem swoich zadań wskazanych w art. 39 RODO. To mogłoby prowadzić do naruszenia przepisów prawa, w tym m.in. zasad zgodności z prawem i poufności, wskazanych w art. 5 ust. 1 lit. a) i f) RODO.

Przedmiotem analizy organu nadzorczego była również możliwość pełnienia funkcji IOD przez komplementariusza spółki komandytowej[332]. Komplementariusz, gdy jest jednocześnie wspólnikiem spółki komandytowej i osobą reprezentującą tę spółkę zgodnie z umową spółki komandytowej, czyli prowadzi sprawy spółki i decyduje o celach i sposobach przetwarzania danych osobowych, nie może równolegle zajmować stanowiska inspektora ochrony danych. Prowadziłoby to bowiem do sytuacji, w której IOD

[331] DOL.502.164.2023.
[332] Materiał w tej sprawie opublikowany został w „Biuletynie UODO” nr 3/05/2023.

oceniałby i monitorowałby samego siebie. Organ nadzorczy wielokrotnie wskazywał, że z tego właśnie powodu niedopuszczalne jest powołanie na IOD osoby będącej kierownikiem (zarządzającym) podmiotem posiadającym status administratora lub podmiotu przetwarzającego, np.: członka zarządu stowarzyszenia, dyrektora szkoły, wójta, członka zarządu spółki. Zgodnie z art. 38 ust. 3 RODO IOD ma podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego, nie zaś być członkiem organu zarządzającego tym podmiotem.

W 2023 r. organ nadzorczy odnosił się też do pytania, czy IOD powołany u pracodawcy ma obowiązek świadczyć pomoc Kasie Zapomogowo-Pożyczkowej (dalej jako KZP). W odpowiedzi wskazał on, że IOD pełni swoją funkcję tylko u administratora, przez którego został wyznaczony i nie jest zobowiązany do wykonywania zadań określonych w art. 39 RODO na rzecz innych administratorów. W związku z tym, jeśli na KZP ciąży obowiązek wyznaczenia IOD, albo zdecyduje się ona na to mimo braku takiego obowiązku, wówczas powinna samodzielnie wyznaczyć taką osobę do pełnienia tej funkcji i wykonać obowiązek zgłoszenia IOD do Prezesa UODO.

W okresie objętym niniejszym sprawozdaniem organ nadzorczy odpowiadał również na pytania dotyczące wątpliwości co do funkcjonowania osoby zastępującej (zastępcy) inspektora ochrony danych[333]. Wskazywał, że administrator musi zapewnić IOD właściwe warunki funkcjonowania (w tym m.in. niezbędne zasoby), które umożliwią mu skuteczne i prawidłowe wykonywanie jego zadań. W zależności od wielkości i struktury organizacji administrator może przyjąć różne rozwiązania w zakresie kadrowego wsparcia IOD. Jednym z nich może być wyznaczenie osoby zastępującej inspektora w czasie jego nieobecności – zastępcy IOD[334]. Odnosząc się do wątpliwości w zakresie funkcjonowania osoby zastępującej IOD, organ nadzorczy wskazywał, że wyznaczenie zastępcy IOD ma służyć zapewnieniu ciągłości wykonywania zadań IOD, zatem może on pełnić swą funkcję zarówno podczas długotrwałej, jak i krótkotrwałej nieobecności IOD (np. urlop, choroba). Zgodnie z art. 11a ust. 2 ustawy o ochronie danych osobowych w związku z wykonywaniem obowiązków inspektora w czasie jego nieobecności do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora, a zatem również przepis art. 38 ust. 3 RODO. Zatem zastępca IOD, wykonując obowiązki IOD w czasie, gdy IOD jest nieobecny, powinien podlegać najwyższemu kierownictwu administratora.

Ponadto administrator zobowiązany jest stosować wobec zastępcy IOD również wymóg zapewnienia, aby nie wykonywał on innych zadań i obowiązków, jeśli powodowałyby one konflikt interesów (art. 38 ust. 6 RODO). Wobec powyższego, biorąc pod uwagę specyfikę tego obowiązku, administrator powinien przewidzieć wobec osoby wyznaczonej do zastępowania IOD takie rozwiązania, które zapewnią, aby nie wykonywała ona zadań powodujących konflikt interesów zarówno w czasie, gdy zastępuje IOD, jak również wtedy, kiedy nie zastępuje IOD. Przyjęcie odmiennego stanowiska mogłoby prowadzić np. do sytuacji, w których osoba zastępująca IOD podczas jego nieobecności oceniałaby i monitorowałaby samą siebie w związku z wykonywaniem innych zadań. Zatem administrator przed wyborem na zastępcę IOD osoby wykonującej inne zadania

[333] DOL.502.274.2022, DOL.502.82.2023.
[334] Możliwość taką polski ustawodawca przewidział w art. 11a ust. 1 ustawy z 10 maja 2018 r. o ochronie danych osobowych.

powinien dokonać analizy, czy będzie ona w stanie wykonywać prawidłowo swoje obowiązki.

Ponadto organ nadzorczy wskazywał, że zastępca IOD może być członkiem zespołu wspierającego IOD. Przy takim rozwiązaniu „osoba zastępująca" mogłaby na bieżąco współpracować z inspektorem ochrony danych, dzięki czemu znałaby specyfikę aktualnych działań administratora i inspektora. Jednocześnie organ nadzorczy przypomniał, że Grupa Robocza Art. 29 w Wytycznych dotyczących inspektora ochrony danych wskazała, iż w przypadku powołania zespołu inspektora ochrony danych jego struktura, podział i zakres obowiązków powinny zostać jasno ustalone.

W temacie dotyczącym zastępowania IOD organ nadzorczy wskazywał również, że ważne jest przejrzyste określenie sposobu postępowania w przypadku nieobecności IOD (np. w wewnętrznym zarządzeniu), ponieważ sprzyja to dobrej organizacji pracy IOD i uniknięciu sytuacji, w której nie byłoby osoby wykonującej zadania IOD podczas jego nieobecności. Dla wszystkich, zarówno wewnątrz podmiotu będącego administratorem, jak i w relacjach zewnętrznych musi być bowiem jasne, kto w danym momencie jest odpowiedzialny za monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa.

Ad 2. Określenie statusu podmiotów w procesie przetwarzania danych osobowych

Podobnie jak w latach poprzednich wiele z pytań inspektorów ochrony danych dotyczyło określenia ról podmiotów uczestniczących w procesie przetwarzania danych osobowych. Mimo prezentowanych zarówno przez EROD, jak i przez UODO wskazówek w zakresie określania statusu administratora oraz podmiotu przetwarzającego zagadnienie to w dalszym ciągu było często tematem pytań IOD. Powodem tego może być sposób ujęcia terminu „administrator" w przepisach o ochronie danych osobowych. Choć odwołanie się w definicji administratora do kryterium decydowania o celach i sposobach przetwarzania danych osobowych uznać należy za racjonalne i uzasadnione, to jednak zastosowanie tego kryterium w praktyce wywoływało wiele wątpliwości, powodując konieczność dokonywania szczegółowej analizy konkretnych sytuacji.

Ustalenie, czy mamy do czynienia z administratorem, współadministratorem czy z podmiotem przetwarzającym ma fundamentalne znaczenia dla określenia zakresu obowiązków i odpowiedzialności określonego podmiotu, wynikającej z przepisów o ochronie danych osobowych. W szczególności każdy z ww. podmiotów ma w różny sposób ukształtowaną w przepisach RODO odpowiedzialność za właściwe przetwarzanie danych osobowych. Przykładowo zgodnie z wyrażoną w art. 5 ust. 2 RODO zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie przepisów prawa i musi być w stanie to wykazać. Zasada ta ma zastosowanie zarówno do przetwarzania realizowanego samodzielnie przez administratora, jak i w przypadku przetwarzania dokonywanego w jego imieniu przez podmiot przetwarzający. Ponadto w RODO określono obowiązki mające bezpośrednie zastosowanie do podmiotów przetwarzających, które również mogą zostać pociągnięte do odpowiedzialności lub ukarane w przypadku niedopełnienia swoich obowiązków, lub w przypadku działania poza zgodnymi z prawem instrukcjami administratora, lub wbrew nim. W przypadku zaś relacji współadministrowania, uregulowanej w art. 26 RODO, współadministratorzy zakresy

swojej odpowiedzialności, dotyczącej wypełniania obowiązków wynikających z RODO, powinni określić w drodze wspólnych uzgodnień.

W odpowiedziach udzielanych inspektorom UODO wskazywał kryteria pomocne w ocenie statusu podmiotów biorących udział w przetwarzaniu danych. W wielu przypadkach odwoływał się do wskazówek zawartych w Wytycznych Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. W dokumencie tym podkreśla się, że podstawowym celem przypisania roli administratora jest zapewnienie rozliczalności oraz skutecznej i pełnej ochrony danych osobowych. Dlatego pojęcie „administratora" powinno się interpretować w sposób odpowiednio szeroki, zapewniając w jak największym stopniu skuteczną i pełną ochronę osób, których dane dotyczą, pełną skuteczność unijnych przepisów o ochronie danych oraz nie dopuszczając do powstania luk i ewentualnego obchodzenia przepisów.

W celu zapewnienia skutecznej ochrony danych osobowych bardzo ważne jest prawidłowe określenie odpowiedzialności za przetwarzanie danych. Jeżeli wymagania wobec poszczególnych podmiotów nie są dostatecznie jasne (np. nikt nie ponosi odpowiedzialności lub jest wielu ewentualnych administratorów danych), istnieje ryzyko, że przepisy dotyczące ochrony danych pozostaną nieskuteczne. Innymi słowy: nie jest dopuszczalne takie formułowanie wymagań wobec poszczególnych podmiotów uczestniczących w operacjach przetwarzania, które powodować będzie uchybienie odpowiedzialności za przetwarzanie danych i uchylanie się od wykonywania przepisów RODO.

Przykładem może być pytanie dotyczące **statusu banku tkanek i komórek[335].** Na podstawie odpowiedzi udzielonej na to pytanie inspektora przygotowany został materiał zamieszczony w „Biuletynie UODO" nr 3/05/2023. Wskazano w nim, że choć banki tkanek i komórek (BTiK) działają w strukturach uczelni wyższych, to same ustalają cele i sposoby przetwarzania danych osobowych związane z gromadzeniem, przetwarzaniem czy przechowywaniem tkanek i komórek, dlatego też pełnią funkcję administratorów w rozumieniu RODO. Za uznaniem BTiK jako odrębnego administratora przemawia już sam sposób utworzenia tego podmiotu na podstawie ustawy z 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (dalej zwanej ustawą transplantacyjną), gdzie wprost przewidziano, że stroną postępowania o udzielenie pozwolenia na prowadzenie takiej działalności może być BTiK pozostający w strukturze innego podmiotu. Z przepisów ustawy transplantacyjnej można wywnioskować, że BTiK cechuje określona autonomia w podejmowaniu decyzji związanych z ustalaniem celów i sposobów przetwarzania danych osobowych. Przepisy te określają bowiem dokładne zasady, które musi spełnić jednostka organizacyjna, aby mogła wykonywać czynności związane z gromadzeniem, przetwarzaniem czy przechowywaniem tkanek i komórek, a także wskazują nadzór właściwego ministra do spraw zdrowia nad tą działalnością. Ponadto na BTiK nałożono obowiązek opracowania i wdrożenia systemu zapewniającego jakość, który ma określać w szczególności sposób monitorowania stanu tkanek i komórek w drodze między dawcą a biorcą oraz wszelkich wyrobów medycznych i materiałów mających bezpośrednio kontakt z tymi tkankami i komórkami. Wobec tego to nie uczelnia wyższa, w której strukturach funkcjonuje BTiK, ustala cele i sposoby przetwarzania danych

[335] DOL.502.12.2023.

osobowych związane z gromadzeniem, przetwarzaniem czy przechowywaniem tkanek i komórek, lecz robią to właśnie BTiK. Na tej podstawie można zatem uznać, że to BTiK są administratorami w rozumieniu RODO.

Innym przykładem spraw dotyczących wątpliwości co do statusu podmiotu jest przypadek opisany w tekście **„Status komisji konkursowej na dyrektora szkoły”,** zamieszczonym w „Biuletynie UODO” nr 7-8/07-08/2023, przygotowany na kanwie odpowiedzi na pytanie od inspektora ochrony danych. W odpowiedzi UODO wskazał, że to organ prowadzący szkołę lub placówkę, który na podstawie art. 63 ust. 14 ustawy z 14 grudnia 2016 r. Prawo oświatowe powołuje komisję konkursową, jest administratorem danych osobowych kandydatów na stanowisko dyrektora szkoły lub placówki, przetwarzanych przez tę komisję. Zatem to na organie prowadzącym ciąży obowiązek zastosowania środków zapewniających bezpieczeństwo przetwarzania tych danych, w tym np. nadawanie upoważnień do przetwarzania danych członkom komisji konkursowej.

Kolejnym podmiotem, którego status w procesie przetwarzania danych osobowych budził wątpliwości inspektorów, była **obwodowa komisja wyborcza**[336]**.** W odpowiedzi na pytanie w tej sprawie organ wskazał, że zarówno gmina, jak i obwodowa komisja wyborcza mają, określone w ustawie z 5 stycznia 2011 r. Kodeks wyborczy, zadania związane z organizacją i przeprowadzeniem wyborów. Do zadań gminy należy w szczególności sporządzenie i aktualizowanie spisów wyborczych, a także przekazanie w przeddzień wyborów jednego egzemplarza spisu wyborców przewodniczącemu właściwej obwodowej komisji wyborczej. Natomiast do zadań obwodowej komisji wyborczej, będącej organem wyborczym, należy w szczególności: przeprowadzenie głosowania w obwodzie; czuwanie w dniu wyborów nad przestrzeganiem prawa wyborczego w miejscu i czasie głosowania; ustalenie wyników głosowania w obwodzie i podanie ich do publicznej wiadomości; przesłanie wyników głosowania do właściwej komisji wyborczej. Analizując przepisy ww. ustawy stwierdzono, że obwodowa komisja wyborcza przetwarza dane osobowe zawarte w przekazanym jej przez gminę spisie wyborców w celu realizacji swoich własnych zadań. Zatem w sytuacji, gdy gmina przekazuje spis wyborców przewodniczącemu właściwej obwodowej komisji wyborczej, mamy do czynienia z udostępnieniem danych osobowych odrębnemu administratorowi (obwodowej komisji wyborczej) w celu realizacji przez ten podmiot jego własnych, wynikających z przepisów prawa, zadań, a nie w celu realizacji zadań udostępniającego (gminy). Wobec powyższego w takiej sytuacji nie mamy do czynienia z powierzeniem przetwarzania danych osobowych.

Ad 3. Udostępnianie danych osobowych

W wielu pytaniach od inspektorów pojawiały się kwestie dotyczące udostępniania danych osobowych. Zgodnie z przepisami RODO podmiot może przetwarzać, w tym udostępniać, dane osobowe wyłącznie wtedy, gdy istnieje podstawa prawna uprawniająca wnioskującego do pozyskania danych. W odpowiedziach na takie pytania organ nadzorczy podkreśla zazwyczaj, że każdy wniosek o udostępnienie danych wymaga indywidualnej analizy oraz że rozpatrujący go administrator musi wziąć pod uwagę konkretne okoliczności faktyczne i prawne, w tym: obowiązujące przepisy prawa, rodzaj danych osobowych, cel oraz uzasadnienie potrzeby posiadania danych przez podmiot, który

[336] DOL.502.167.2023.

występuje o ich udostępnienie. Administrator ponosi odpowiedzialność za wykazanie właściwej staranności w zapewnieniu, aby dane nie były udostępniane nieuprawnionym odbiorcom, a jeśli podejmie decyzje o ich udostępnieniu, wówczas powinien zadbać, aby zakres udostępnianych danych był odpowiedni (bez nadmiaru) do celu udostępniania – zasada minimalizacji, o której mowa w art. 5 ust. 1 lit. c) RODO.

Przykładem było pytanie przesłane przez inspektora ochrony danych w zakładzie poprawczym, **czy osoba pełnoletnia umieszczona w zakładzie poprawczym może zażądać od zakładu poprawczego zaprzestania przekazywania jakichkolwiek informacji na swój temat, w tym danych osobowych, np. rodzicom.** W odpowiedzi na to pytanie organ nadzorczy wskazał, że władza rodzicielska ustaje wraz z uzyskaniem przez dziecko pełnoletności (art. 92 ustawy z 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy), a w związku z tym osoba pełnoletnia ma prawo wskazać, że nie życzy sobie, aby informacje jej dotyczące były przekazywane np. jej rodzicom. Niemniej należy mieć na uwadze, że swoboda decydowania osoby pełnoletniej o sobie może być ograniczona np. orzeczeniem sądowym albo np. osoba pełnoletnia może zostać ubezwłasnowolniona całkowicie. Kwestie uprawnień i obowiązków opiekuna osoby pełnoletniej, która została ubezwłasnowolniona całkowicie, oraz kontaktów rodziców z pełnoletnim dzieckiem ubezwłasnowolnionym były przedmiotem rozstrzygnięć sądów. Wobec powyższego w opinii organu nadzorczego wskazana przez IOD kwestia udostępnienia danych osobowych osoby pełnoletniej np. jej rodzicom wymaga ustalenia, na jakiej podstawie rodzice domagają się informacji o swoim pełnoletnim dziecku i czy sytuacji prawnej tej osoby pełnoletniej nie modyfikuje np. wyrok sądu o ubezwłasnowolnieniu całkowitym.

Inne z pytań IOD dotyczące kwestii udostępniania danych osobowych brzmiało, **czy szkoła ma podstawę prawną do przekazania organowi prowadzącemu danych osobowych uczniów zawartych w kopii opinii z poradni psychologiczno-pedagogicznych** (w tym również szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO), **w celu zatwierdzenia arkusza organizacji szkoły.** Odnosząc się do wskazanych przez IOD wątpliwości, organ przypomniał, że ze względu na określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa organ publiczny nie może domniemywać swoich kompetencji, jeśli nie wynikają one wprost z przepisu prawa. Wobec tego, gdy o udostępnienie danych osobowych występuje podmiot realizujący zadania publiczne, powinien w pierwszej kolejności wyraźnie wskazać przepisy uprawniające go do pozyskania tych danych w celu realizacji konkretnego zadania. Działania podejmowane przez podmioty publiczne powinny mieć oparcie w obowiązujących przepisach prawa, regulujących ich działalność. Wobec tego, co do zasady, podstawa prawna do przetwarzania (w tym udostępniania) danych osobowych przez takie podmioty również powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami, natomiast wszelkie porozumienia czy umowy między podmiotami publicznymi nie mogą zastępować takich norm ani tworzyć niewynikających z nich nowych kompetencji. W przedstawionym przez inspektora przypadku analizy wymagają przede wszystkim przepisy ustawy z 14 grudnia 2016 r. – Prawo oświatowe oraz aktów wykonawczych, gdzie został przewidziany obowiązek opracowywania arkusza organizacji pracy szkoły, a także zakres informacji, jakie w szczególności powinny być zawarte w arkuszu organizacji

szkoły. Zatem, aby szkoła mogła przekazać organowi prowadzącemu w celu zatwierdzenia arkusza organizacji dane osobowe uczniów zawarte w kopiach orzeczeń o niepełnosprawności (stanowiące dane szczególnej kategorii), musiałby istnieć przepis prawa, który wprost uprawniałby organ prowadzący do pozyskiwania kopii takich dokumentów dla celów zatwierdzenia arkusza.

Ad 4. Stosowanie różnych form monitoringu

W pytaniach od inspektorów, które wpływały do UODO w 2023 r., często pojawiały się kwestie dotyczące stosowania monitoringu. Zagadnienie to, ze względu na bardzo inwazyjny charakter przetwarzania danych osobowych, było przedmiotem szczególnego zainteresowania organu nadzorczego. Wątpliwości zgłaszane przez inspektorów dotyczyły m.in. możliwości instalowania atrap kamer czy stosowania kamer w wozie strażackim.

Odnosząc się do kwestii **atrap kamer**[337] organ nadzorczy wskazał, że w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo EROD zajął następujące stanowisko: „RODO nie ma jednak zastosowania do przetwarzania danych, które nie odnoszą się do konkretnej osoby, np. jeżeli bezpośrednio lub pośrednio nie można zidentyfikować osoby". Jako przykład podano, że: „RODO nie ma zastosowania do atrap kamer, które nie funkcjonują jako kamery i w związku z tym nie przetwarzają żadnych danych osobowych". EROD zaznaczył jednak, że: „w niektórych państwach członkowskich kwestia ta może jednak podlegać innym przepisom". EROD wskazuje zatem, że warunki korzystania z atrap kamer państwa członkowskie mogą regulować indywidualnie, poprzez inne przepisy niż RODO.

W odpowiedzi przypomniano, że również UODO wyraził opinię w sprawie instalowania atrap kamer monitoringu. Znajduje się ona we Wskazówkach Prezesa Urzędu Ochrony Danych Osobowych dotyczących wykorzystywania monitoringu wizyjnego z czerwca 2018 r. W materiale tym wskazano, że: „stosowanie atrap powinno być zakazane. Atrapy kamer z jednej strony wprowadzają u potencjalnie monitorowanych poczucie ingerencji w sferę prywatności, a z drugiej mylne poczucie zwiększonego bezpieczeństwa. Niepożądane skutki związane z wykorzystaniem monitoringu, także z atrapami kamer, czy to w otwartej przestrzeni, jak np. boiska szkolne, czy też w zamkniętej, jak np. szatnie czy korytarze, mogą przeważać nad ewentualnymi korzyściami wynikającymi z ich stosowania i tym samym podawać w wątpliwość skuteczność i adekwatność tego narzędzia w realizacji zamierzonego celu w danych okolicznościach".

Analiza powołanych powyżej stanowisk organu nadzorczego wskazuje, iż w istocie dotyczą one innych kwestii i nie pozostają w kolizji. Wytyczne EROD wskazują, że RODO ma zastosowanie do sytuacji, gdy dochodzi do przetwarzania danych, a UODO we Wskazówkach Prezesa Urzędu Ochrony Danych Osobowych traktuje ten problem szerzej, uwzględniając różne prawa i wolności jednostki w kontekście poczucia bezpieczeństwa, a także zalecając ważenie korzyści i niepożądanych skutków podczas używania atrap kamer. Organ nadzorczy zwrócił również uwagę, że podmioty działające na podstawie prawa nie są upoważnione do instalowania urządzeń imitujących kamery monitorujące przestrzeń publiczną. Przepisy uprawniające do stosowania monitoringu wizyjnego nie

[337] DOL.502.102.2023.

obejmują bowiem uprawnienia do wprowadzenia osób monitorowanych w błąd co do zakresu stosowanego monitoringu poprzez instalowanie atrap kamer.

W opinii organu nadzorczego takie działanie może wzbudzać w obywatelach poczucie niepewności i braku zaufania co do rzeczywistego celu zastosowanego monitoringu. Stosowanie atrap kamer ma głównie odstraszać, ale ich prawdziwa funkcja jest znacznie szersza. Istnieje oczekiwanie, że monitoring zapewnia bezpieczne środowisko, a osoby, które tam przebywają, są chronione przez kamery. W sytuacji dojścia do przestępstwa w miejscu, w którym została zamontowana atrapa kamery, Policja nie ma możliwości zabezpieczenia nagrania, ponieważ obraz nie był rejestrowany. Ponadto samo kierowanie kamery w przestrzeń publiczną, niezależnie czy prawdziwej, czy atrapy, a także niezależnie, czy atrapy stosuje podmiot publiczny czy prywatny, może powodować naruszenie dóbr osobistych (prawa do wizerunku, prawa do prywatności, prawa do niezaburzonego spokoju psychicznego i emocjonalnego w miejscu zamieszkania).

Podsumowując, RODO nie ma zastosowania do atrap kamer, ponieważ nie dochodzi do przetwarzania danych osobowych, ale kwestia ta może podlegać innym przepisom. Możliwość naruszenia dóbr osobistych przez zamontowanie takich atrap i ewentualną późniejszą odpowiedzialność montującego są powodem, dla którego stosowanie atrap kamer powinno być zakazane. Przepisy prawa nie upoważniają do instalowania urządzeń imitujących kamery monitorujące i wprowadzania osób obserwowanych w błąd co do zakresu stosowanego monitoringu. Wobec powyższego organ nadzorczy zasugerował rozważenie użycia innych środków bezpieczeństwa, takich jak np. światło włączane poprzez ruch lub dodatkowe zabezpieczenia fizyczne.

Inne zagadnienie z zakresu monitoringu zgłoszone przez IOD dotyczyło podstawy prawnej do przetwarzania danych osobowych w przypadku **nagrywania obrazu przez kamerę zamontowaną w wozie strażackim[338].** W odpowiedzi na to pytanie organ nadzorczy wskazał, że ustalenie właściwej podstawy takiego przetwarzania danych zależy od celu, jaki miałoby realizować takie przetwarzanie. Jeżeli celem tym ma być uzyskanie dowodu dla ubezpieczyciela w razie kolizji drogowej, można rozważyć, czy przetwarzanie danych można oprzeć na przesłance z art. 6 ust. 1 lit. f) RODO (tj. uzasadniony interes administratora). Organ nadzorczy podkreślił jednak, że możliwość powoływania się na tę podstawę prawną jest ograniczona przez interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych. Uzasadniony interes administratora nie może być podstawą przetwarzania danych, jeśli wspomniane interesy lub prawa osoby, której dane dotyczą, mają charakter nadrzędny. Konieczne jest tutaj przeprowadzenie tzw. testu równowagi, którego istotą jest ustalenie: czy interes administratora 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.

Odnosząc się natomiast do rozważanej przez IOD możliwości wskazania jako podstawy takiego przetwarzania art. 5a ustawy z 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym, organ nadzorczy wskazał, że przepis ten odnosi się do monitoringu na terenie nieruchomości i w obiektach budowlanych stanowiących mienie

[338] DOL.502.194.2023.

państwowe, a także na terenie wokół takich nieruchomości i obiektów, jeżeli jest to konieczne do zapewnienia bezpieczeństwa zarządzanym mieniem państwowym. Przepis ten stanowi też o ogólnym obowiązku zapewnienia bezpieczeństwa mienia państwowego, dopuszczając zabezpieczenia techniczne, w szczególności w postaci ww. monitoringu. W ocenie organu nadzorczego rozciąganie tego przepisu na nagrywanie obrazu przez kamery samochodowe nie wydaje się uzasadnione, po pierwsze ze względu na wyraźne wskazanie na nieruchomości i obiekty budowlane, a po drugie trudno byłoby uznać, że korzystanie z kamer samochodowych jest konieczne i niezbędne do zapewnienia bezpieczeństwa mienia (w tym przypadku – wozu Straży Pożarnej).

Inne z pytań od IOD dotyczyło z kolei kwestii dopuszczalności praktyki polegającej na **stosowaniu kamer nasobnych przez inkasentów** pobierających opłaty targowe[339]. W odpowiedzi organ nadzorczy wskazał, że w każdym przypadku wdrażania rozwiązań związanych z przetwarzaniem danych osobowych administrator zobowiązany jest zapewnić, aby były one zgodne z RODO oraz aby istniała podstawa prawna do takiego przetwarzania. W przypadku podmiotów publicznych, co do zasady, podstawa prawna do przetwarzania przez nie danych osobowych powinna wynikać z przepisów prawa. Regulacje dotyczące poboru podatku przez inkasentów znajdują się przede wszystkim w przepisach ustawy z 29 sierpnia 1997 r. – Ordynacja podatkowa. Wynika z nich, że inkasentem jest osoba fizyczna, osoba prawna lub jednostka organizacyjna niemająca osobowości prawnej, obowiązana do pobrania od podatnika podatku i wpłacenia go we właściwym terminie organowi podatkowemu (art. 9). Regulacje wskazanej ustawy określają również zakres odpowiedzialności inkasenta (art. 30). Zgodnie z art. 2 § 1 pkt 3 Ordynacji podatkowej jej przepisy mają zastosowanie do opłat, o których mowa w przepisach o podatkach i opłatach lokalnych (a więc także do opłat targowych). Odnosząc się zatem do pytania o dopuszczalność stosowania przez ww. inkasentów kamer nasobnych organ nadzorczy wskazał, że z analizy zarówno przepisów Ordynacji podatkowej, jak i przepisów ustawy z 12 stycznia 1991 r. o podatkach i opłatach lokalnych, które mają zastosowanie do pobierania opłat targowych przez inkasentów (art. 1, art. 15, art. 19), wynika, iż nie przewidują one, aby pobieranie podatku mogło odbywać się przy użyciu kamer. W odpowiedzi podkreślono ponadto, że monitoring jest jedną z najbardziej inwazyjnych form przetwarzania danych osobowych i powinien być stosowany jedynie w sytuacji, gdy nie istnieją inne, mniej ingerujące w prywatność środki umożliwiające zapewnienie bezpieczeństwa. Organ nadzorczy zaznaczył również, że w opisanej przez IOD sprawie należy także wziąć pod uwagę, iż kamery mogą również obejmować osoby trzecie, a także, że przy prowadzeniu takiej formy przetwarzania należy uwzględnić przepisy dotyczące monitoringu pracownika zawarte w ustawie z 26 czerwca 1974 r. – Kodeks pracy.

Ad 5. Status podmiotów realizujących zadania związane z laptopami dla uczniów i dla nauczycieli

Przykładem sygnalizowanych przez IOD zagadnień, związanych z wątpliwościami co do sposobu realizacji nowych obowiązków nałożonych na administratorów, były kwestie wynikające z wejścia w życie ustawy z 7 lipca 2023 r. o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli. Pytania inspektorów dotyczyły m.in. tego, kto – w związku

[339] DOL.502.79.2023.

z realizacją programu „Laptop dla ucznia”, w tym zawieraniem umowy użyczenia komputera przenośnego typu laptop rodzicowi ucznia klasy objętej wsparciem – jest administratorem danych i tym samym ma obowiązek spełnienia obowiązku informacyjnego wynikającego z RODO[340]. W odpowiedzi organ nadzorczy podkreślił, że przy realizacji tego programu status administratora przysługuje organowi prowadzącemu szkołę, a nie szkole. Wskazuje na to przede wszystkim treść przepisów regulujących to zadanie. Zgodnie bowiem z art. 7 ust. 3 ww. ustawy przekazanie laptopa uczniowi klasy objętej wsparciem następuje na podstawie umowy zawartej przez organ prowadzący szkołę z rodzicem ucznia. Ponadto stosownie do art. 7 ust. 5 tej ustawy, organ prowadzący szkołę sporządza protokół z przekazania laptopa. Dodatkowo z wzoru umowy użyczenia komputera przenośnego typu laptop (określonego w załączniku do rozporządzenia Ministra Cyfryzacji z 8 września 2023 r. w sprawie określenia wzoru umowy użyczenia komputera przenośnego typu laptop rodzicowi ucznia klasy objętej wsparciem) wynika, że to organ prowadzący szkołę jest stroną umowy oraz odpowiada za obowiązki związane z ochroną danych osobowych dziecka i rodzica, w tym za wypełnianie wobec biorącego w użyczenie obowiązku informacyjnego przewidzianego w art. 13 RODO. W związku z powyższym to organowi prowadzącemu szkołę, a nie szkole, należy przyznać status administratora w rozumieniu art. 4 pkt 7 RODO. Materiał dotyczący tego zagadnienia opublikowany został w „Biuletynie UODO” nr 10/10/2023.

Inne pytanie dotyczące powyższego zagadnienia odnosiło się do kwestii statusu administratora wobec przetwarzania danych nauczycieli w celu przekazania im jednorazowych świadczeń w formie bonów na zakup laptopów[341]. W odpowiedzi organ nadzorczy wskazał m.in., że w przypadku przetwarzania danych osobowych w celu realizacji zadań publicznych zasadą jest, że dla ustalenia administratora konieczna jest analiza przepisów określających te zadania oraz podmioty, które zadania te mają realizować. Zgodnie z art. 20 ust. 3 ustawy z 7 lipca 2023 r. o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli: „administratorem danych osobowych w systemie teleinformatycznym do obsługi bonu jest minister właściwy do spraw informatyzacji”. Kompetencje organów prowadzących szkołę zostały natomiast wskazane m.in. w art. 15 powołanej ustawy. Organ prowadzący jest odpowiedzialny przede wszystkim za złożenie wniosku dla wszystkich nauczycieli uprawnionych do otrzymania wsparcia w systemie teleinformatycznym, o którym mowa w art. 20 ust. 1 ustawy oraz zobowiązanie nauczyciela do złożenia wyjaśnień w zakresie weryfikacji warunków, o których mowa w art. 15 ust. 4 ustawy, jeżeli okaże się to niezbędne. Biorąc zatem pod uwagę przywołane wyżej kompetencje obu podmiotów, organ nadzorczy wskazał, że są podstawy do uznania, że zarówno Minister Cyfryzacji, jak i organ prowadzący szkołę pełnią w tym przypadku rolę administratora, każdy w zakresie realizacji zadań wskazanych w powołanych przepisach.

Ad 6. Nowe technologie

W analizowanym okresie sprawozdawczym organ nadzorczy udzielał również odpowiedzi na pytania inspektorów dotyczące wątpliwości związanych ze stosowaniem nowych technologii. Przykładem może być pytanie odnoszące się do zastosowania

[340] DOL.502.183.2023.
[341] DOL.502.207.2023.

technologii blockchain do obsługi procesu zawierania umów z klientami[342]. Wątpliwości IOD budziła zwłaszcza kwestia zrealizowania przez administratora praw podmiotów danych w rozumieniu art. 15–22 RODO, w tym prawa do sprostowania, czy też prawa do usunięcia danych. W odpowiedzi organ nadzorczy wskazał, że na administratorze spoczywa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych w celu skutecznej realizacji zasad ochrony danych osobowych (art. 24 ust. 1 RODO). Wobec tego ewentualne ograniczenia wynikające ze stosowania technologii blockchain (np. brak możliwości usuwania/aktualizowania danych) nie zwalniają administratora z przestrzegania obowiązków wynikających z RODO. Dodatkowo administrator jest zobligowany do wykazania, że jego działania są zgodne z obowiązującym prawem (zasada rozliczalności, o której mowa w art. 5 ust. 2 RODO). Organ nadzorczy odwołał się też do Wytycznych EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z artykułu 25, gdzie wskazano, że jednym z kluczowych elementów uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych w stosunku do zasady ograniczenia przechowywania – art. 5 ust. 1 lit. c) RODO – jest zapewnienie przez administratora skuteczności usuwania danych. Wobec tego rozważane przez inspektora rozwiązanie w postaci „mocnego szyfrowania" nie wydaje się być wystarczające w zakresie zapewnienia prawa do usunięcia danych osobowych. Dane zaszyfrowane to nadal dane, a to oznacza, iż nie można zrównać szyfrowania danych z ich usunięciem. Zgodnie bowiem z motywem 83 RODO szyfrowanie może służyć jako forma zabezpieczenia danych, a nie ich usuwania czy sprostowania. Dodatkowo organ nadzorczy poinformował inspektora, że w strategii EROD na lata 2021–2023 wskazano, że ocena technologii blockchain ma być przedmiotem prac europejskich organów nadzorczych w zakresie wypracowania spójnego podejścia stosowania RODO oraz że w tym zakresie warto śledzić stronę internetową EROD.

Innym przykładem zagadnienia związanego ze stosowaniem nowych technologii, które pojawiło się w pytaniach od IOD, jest korzystanie z aplikacji mObywatel, o której mowa w ustawie z 26 maja 2023 r. o aplikacji mObywatel[343]. W tej sprawie inspektor zwrócił się do UODO o wyrażenie stanowiska w zakresie prawidłowości rozwiązania odnoszącego się do weryfikowania mDowodów obywateli przez pracowników urzędów z wykorzystaniem ich prywatnych smartfonów**.** Odnosząc się do tego pytania, organ nadzorczy wskazał, że przepisy ustawy o aplikacji mObywatel nie dają podstawy do żądania od pracowników organów administracji publicznej posługiwania się prywatnymi urządzeniami (smartfonami) w celu dokonywania weryfikacji dokumentów obsługiwanych w aplikacji mObywatel. Organ podzielił też zastrzeżenia inspektora co do wykorzystywania sprzętu prywatnego do celów służbowych. W opinii organu takie działania mogłyby bowiem powodować zagrożenie dla przetwarzania danych osobowych obywateli przekazujących dokumenty do weryfikacji, co godzi w zasadę integralności i poufności – art. 5 ust. 1 lit. f) RODO. Dlatego prawidłowym rozwiązaniem powinno być zapewnianie przez pracodawców służbowych urządzeń (tabletów, smartfonów), za pomocą których pracownicy będą mogli dokonywać weryfikacji, o której mowa w ustawie o aplikacji mObywatel.

[342] DOL.502.222.2022.
[343] DOL.502.132.2023.

Ad 7. Nagrywanie rozmów z interesantami przez podmioty publiczne

Kolejnym ważnym tematem podnoszonym przez inspektorów ochrony danych w przesyłanych do UODO pytaniach było nagrywanie rozmów z interesantami przez podmioty publiczne, np. urzędy gminy. Na podstawie odpowiedzi na pytania IOD przygotowany został materiał do „Biuletynu UODO" nr 11/11/2023. Wskazano w nim, że dla zajęcia przez UODO wiążącego stanowiska niezbędna jest dokładna znajomość wszystkich okoliczności faktycznych danego przypadku, w którym prowadzone jest nagrywanie, w tym rodzaju przetwarzanych danych, warunków i celów ich przetwarzania. Niemniej przeprowadzona analiza przepisów RODO i krajowych przepisów szczególnych, a także stanowisk innych unijnych organów nadzorczych, prowadziła do wniosku, że co do zasady praktyka ta jest bezpodstawna.

W przypadku nagrywania rozmów pracowników z interesantami telefonującymi do urzędu dochodzić będzie do przetwarzania danych osobowych zarówno dzwoniących, jak i pracowników urzędu. Odnosząc się do przetwarzania przez urząd danych osobowych interesantów, w pierwszej kolejności należy ocenić, jakie są faktyczne cele pozyskiwania i dalszego przetwarzania tych danych, co jest kluczowe dla podjęcia decyzji o potrzebie aż tak głębokiej ingerencji w prywatność osób, jaką jest ich nagrywanie. Trzeba mieć na uwadze, że osoby, których dane dotyczą, w większości przypadków telefonują do urzędu w celu uzyskania informacji odnoszących się do zadań realizowanych przez urząd i dane pozyskiwane poprzez nagrywanie tych rozmów będą dotyczyły tych zadań i spraw z nimi związanych. W przypadku nagrywania rozmów pozyskiwane mogą być dane osobowe zwykłe, których przetwarzanie jest legalne tylko wtedy, gdy odbywa się na podstawie jednej z przesłanek określonych w art. 6 RODO. Nie można też wykluczyć, że pozyskiwane będą dane szczególnych kategorii, których przetwarzanie – zgodnie z art. 9 ust. 1 RODO – jest co do zasady zabronione, a także dane, o których mowa w art. 10 RODO, których przetwarzanie jest dopuszczalne jedynie na zasadach określonych w tym przepisie.

W ocenie organu nadzorczego obecnie nie ma , który uprawniałby organy gminy do rejestrowania rozmów telefonicznych dla realizacji ich zadań, czy też w ramach sprawowania władzy publicznej. Wprawdzie przepisy procedury administracyjnej przewidują, że sprawy administracyjne mogą być załatwiane ustnie, telefonicznie, za pomocą środków komunikacji elektronicznej lub innych środków łączności, ale nie można tu jednak stosować automatyzmu. Telefoniczne załatwienie sprawy – zgodnie z art. 14 § 2 Kodeksu postępowania administracyjnego – możliwe jest jedynie wtedy, gdy przemawia za tym interes strony, a przepis prawny nie stoi temu na przeszkodzie, a ponadto treść oraz istotne motywy takiego załatwienia sprawy powinny być utrwalone w aktach w formie protokołu lub podpisanej przez stronę adnotacji, nie zaś nagrywania rozmów.

Urząd Ochrony Danych Osobowych zwrócił też uwagę, że organy administracji publicznej co do zasady nie powinny powoływać się na zgodę osób, które dzwonią do urzędu gminy w sprawach odnoszących się do zadań gminy, zwłaszcza ze względu na wyraźny brak równowagi w stosunkach między administratorem, będącym władzą publiczną, a osobą, której dane dotyczą. Co zaś do stosowania przez organy publiczne przesłanki określonej w art. 6 ust. 1 lit. f) RODO – UODO wskazał, że w przepisie tym znajduje się zastrzeżenie, iż podstawa prawna wskazana w lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Jednocześnie UODO zwrócił uwagę, że należy również dokonać analizy legalności nagrywania rozmów pracowników z interesantami na gruncie przepisów prawa pracy. W ocenie organu nadzorczego ani przepisy ustawy – Kodeks pracy, dotyczące innych form monitoringu pracownika (art. 22^3 § 4), ani zgoda pracownika nie mogą stanowić podstawy uprawniającej urząd do nagrywania rozmów z interesantami. Organ nadzorczy wskazał również, że analiza dopuszczalności nagrywania rozmów powinna uwzględniać przepisy ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (art. 159).

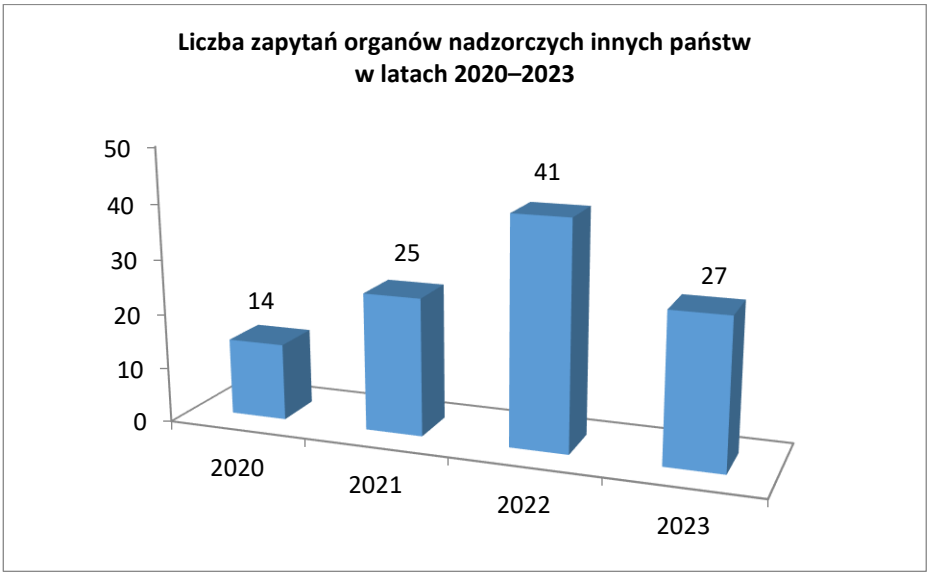
Reasumując, w większości przypadków nie ma podstaw, by urzędy nagrywały rozmowy telefoniczne z interesantami – i dlatego powinny jak najszybciej przeprowadzić kompleksową analizę swoich praktyk.

Przejawem współpracy UODO z inspektorami ochrony danych jest sygnalizowanie organowi nadzorczemu problemów, z którymi spotykają się w pracy, pełniąc swoją funkcję. Inspektorzy są bowiem najlepiej zorientowani, jak określone przepisy prawa funkcjonują w praktyce lub jak są interpretowane przez resorty w wydawanych przez nie wskazówkach lub stanowiskach. Jeśli stosowanie określonych regulacji budzi ich wątpliwości w zakresie zasad ochrony danych osobowych, wówczas przedstawiali problem organowi nadzorczemu i zwracają się o wydanie opinii oraz o podjęcie interwencji w tej sprawie. Dzięki takiej współpracy możliwe było wspólne szukanie rozwiązań zidentyfikowanych problemów. W takich przypadkach Prezes UODO mógł też skorzystać ze swoich uprawnień dotyczących sygnalizowania właściwym resortom konieczności dokonania stosownych zmian legislacyjnych, tak aby regulacje uwzględniały zasady ochrony danych osobowych.

12.1.3. Zapytania 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 na podstawie mechanizmów spójności i współpracy uregulowanych 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 zadane pytania.

W 2023 r. do Prezesa UODO wpłynęło **27 zapytań organów nadzorczych z innych państw,** w tym m.in. z: Francji, Holandii, Włoch, Lichtensteinu, Finlandii, Norwegii, Irlandii, Malty, Niemiec, Danii, Cypru, Słowenii i Słowacji. Dla porównania, w 2022 r. takich pytań wpłynęło 41, w 2021 r. – 25, zaś w 2020 r. – 14.



Wykres 18: Liczba pytań od organów nadzorczych innych państw skierowanych do Prezesa UODO w latach 2021–2023

Organy nadzorcze zwracały się do Prezesa UODO z różnymi zagadnieniami. Pytania dotyczyły m.in. opinii polskiego organu nadzorczego w takich sprawach, jak:

- Zawiadomienie organu nadzorczego o danych kontaktowych inspektora ochrony danych w okolicznościach, w których administrator/podmiot przetwarzający podlega RODO na mocy art. 3 ust. 2 RODO.
- Przypadki, w których przetwarzanie danych dotyczących beneficjenta rzeczywistego[344] można uznać za informacje dotyczące osoby prawnej, a nie osoby fizycznej będącej beneficjentem rzeczywistym. Ponadto poproszono o informacje dotyczące innych przypadków, w których informacje dotyczące osoby fizycznej uznaje się za powiązane z podmiotem prawnym.
- Które z organów nadzorczych lub rządów krajowych, lub inne organizacje krajowe działające w sferze edukacji analizują zagrożenia dla ochrony danych podczas korzystania z produktów Google w edukacji, na przykład poprzez postępowania lub spotkania z sektorem edukacji. Pytanie uwzględniało również kwestię negocjacji z Google w sprawie ograniczenia tych zagrożeń.
- Przygotowanie stanowiska w odpowiedzi na pytania dotyczące przetwarzania danych biometrycznych w celu weryfikacji/uwierzytelnienia.
- Uregulowanie w polskim ustawodawstwie kwestii samochodowych wideorejestratorów.
- Traktowanie jako naruszenie ochrony danych zdarzeń, takich jak kradzież lub utrata karty płatniczej bądź otrzymywanie danych karty płatniczej lub danych do logowania na internetowe konto bankowe.
- Zgoda na użycie przez osobę wysyłającą newsletter pikseli śledzących/monitorujących (tracking pixels).

[344] Definicja „beneficjenta rzeczywistego" została określona w polskim porządku prawnym w przepisach ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124), wdrażającej do polskiego porządku prawnego dyrektywę AML.

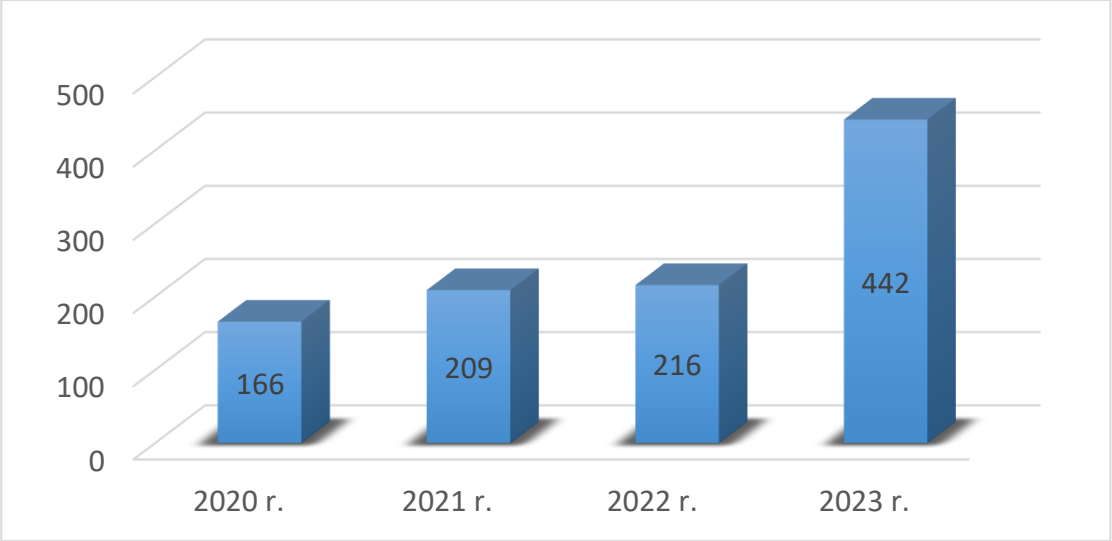
- Szyfrowanie danych.
- Monitoring wizyjny w miejscach publicznych.
- Obejmowanie przez prawo dostępu informacji dotyczących odbiorcy, któremu dane osobowe zostały przez pomyłkę ujawnione w wyniku naruszenia ochrony danych osobowych.
- Wyznaczenie właściwego organu nadzorczego dla aktu o zarządzaniu danymi (DGA).
- Informacja dotycząca: wewnętrznych procedur związanych z cyberprzemocą, rejestrów zaległości płatniczych, stref mobilności niskoemisyjnej (ZFE-m).
- Interpretacja przepisu art. 17 ust. 3 RODO.
- Duże modele językowe.
- Szacowanie wieku osób na podstawie analizy twarzy.
- Odpowiedzialność ponownych użytkowników publicznie licencjonowanych baz danych dostępnych w Internecie.
- Krajowa procedura transpozycji dyrektywy NIS2.
- Stosowanie RODO w odniesieniu do transmisji streamingu sportów młodzieżowych.
- Kwestia administratorów lub współadministratorów danych osobowych zbieranych za pośrednictwem urządzeń wideo zainstalowanych we wspólnych pomieszczeniach budynku mieszkalnego.
- Wynikający z art. 23 ust. 3 i 4 dyrektywy 2009/103 obowiązek umożliwiający poszkodowanym w wypadkach z udziałem pojazdów uzyskanie pewnych informacji (w tym danych osobowych) związanych z ubezpieczeniem od odpowiedzialności cywilnej za szkody powstałe w związku z wypadkiem.
- Przetwarzanie danych na potrzeby celów dziennikarskich, usług informacji rzecznej (RIS) na śródlądowych drogach wodnych.
- Dane dotyczące bezpieczeństwa drogowego i informacji drogowych związanych z bezpieczeństwem.
- Zarządzanie ogólnodostępnymi miejscami parkingowymi przez gminę.
- Procedura udzielania zezwolenia na przetwarzanie danych osobowych dotyczących wyroków skazujących i przestępstw lub związanych z nimi środków bezpieczeństwa na mocy prawa krajowego.

Polski organ ochrony danych osobowych dokonał analizy przedłożonych pytań, a następnie przygotował stosowne odpowiedzi w języku angielskim i przekazał je do właściwych organów nadzorczych.

Udzielanie szczegółowych odpowiedzi umacnia współpracę z krajowymi organami nadzorczymi. Dzięki informacjom pozyskanym od innych organów nadzorczych wzrasta zrozumienie sposobu, w jaki RODO jest interpretowane w państwach członkowskich. Ponadto otrzymywane pytania pozwalają rozeznać się w bieżących zagadnieniach, będących przedmiotem dyskusji innych organów nadzorczych. Sprzyja to również wypracowaniu zharmonizowanych, wspólnych stanowisk przy uwzględnieniu ustawodawstwa krajowego.

12.2. Wnioski o dostęp do informacji publicznej

W analizowanym 2023 r. do Urzędu Ochrony Danych Osobowych wpłynęły **442 wnioski o dostęp do informacji publicznej**.



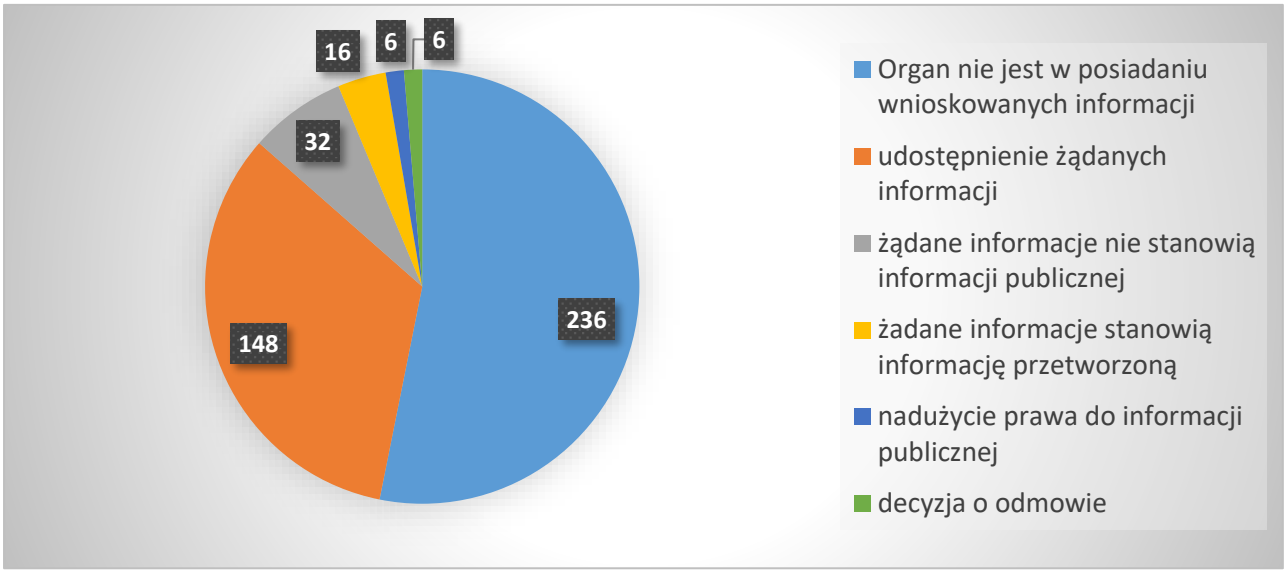
Wykres 19: Liczba wniosków o dostęp do informacji publicznej, które wpłynęły do UODO w latach 2020–2023

Wykres 19 obrazuje znaczny przyrost liczby wniosków złożonych w 2023 r. w trybie ustawy o dostępie do informacji publicznej w stosunku do poprzednich lat. W dużej mierze przyczyniły się do tego wnioski dotyczące uzasadnienia obowiązku szczepienia dzieci w Polsce. Choć Prezes UODO nie był w posiadaniu wnioskowanych informacji, to każdorazowo zobowiązany był udzielić odpowiedzi wnioskodawcy, wskazując, że nimi nie dysponuje. Dlatego też na przestrzeni jednego miesiąca – września 2023 r. – organ rozpoznał w sumie 236 wniosków o tożsamej treści. Wiele innych pytań dotyczyło realizacji ustawowych kompetencji Prezesa UODO oraz działalności urzędu w sferze organizacyjnej, finansowej i kadrowej. Wnioskodawcy wnosili o dane statystyczne uwzględniające liczbę postępowań, zgłoszonych skarg i naruszeń ochrony danych osobowych, zawiadomień z sądów powszechnych o wniesionych pozwach[345], wydanych decyzji, przeprowadzonych kontroli, a ponadto dotyczące: wysokości nałożonych kar pieniężnych, rodzaju i liczby zastosowanych uprawnień naprawczych, złożonych wniosków o uprzednie konsultacje itd. Wiele pytań odnosiło się do liczby i treści decyzji administracyjnych, liczby zgłoszonych Inspektorów Ochrony Danych, planu kontroli sektorowych, kontroli podmiotów przetwarzających dane osobowe przy użyciu aplikacji mobilnych oraz informacji o podmiotach, w których Prezes UODO przeprowadził kontrolę. Zdarzały się również wnioski o udostępnienie treści umów zawieranych przez urząd z podmiotami zewnętrznymi, statystyk dotyczących spraw kadrowych oraz ekspertyz prawnych. Często pytania dotyczyły spraw, które rozpatrywane były przez Prezesa UODO w latach ubiegłych, czy tych rozpatrywanych przez kilka komórek organizacyjnych urzędu. Nierzadko jeden wniosek zawierał kilka pytań, często ze sobą niezwiązanych tematycznie.

[345] Art. 94 ustawy o ochronie danych osobowych.

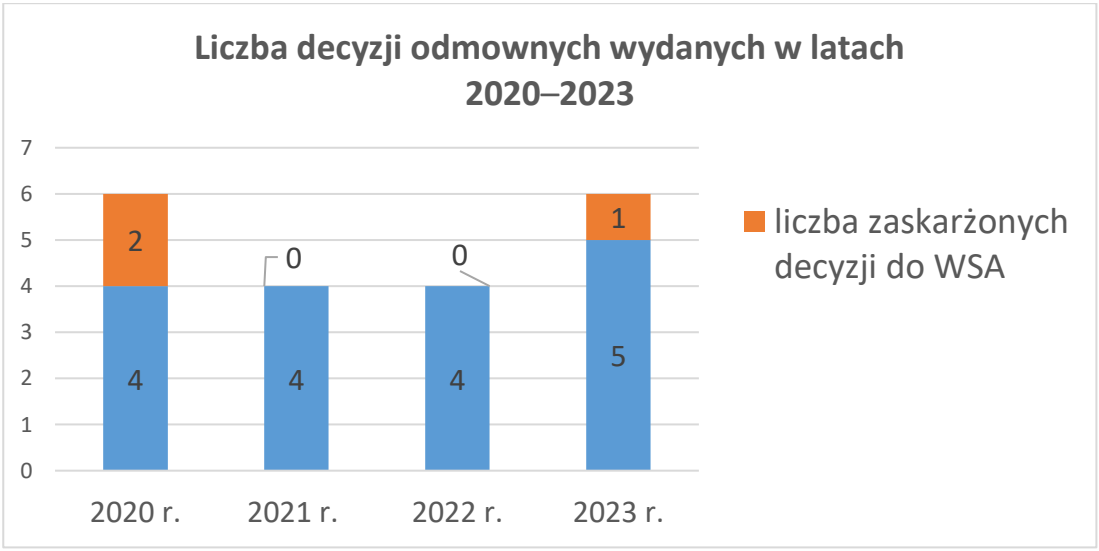
W kilku przypadkach zachodziła konieczność zwrócenia się do wnioskodawcy o uzasadnienie interesu publicznego, a potem analiza jego argumentów, uzupełnienie braków formalnych wniosku w związku z koniecznością wydania decyzji administracyjnej.

Poniższy załącznik graficzny przedstawia sposoby rozpatrywania wniosków złożonych do Urzędu Ochrony Danych Osobowych w trybie dostępu do informacji publicznej.



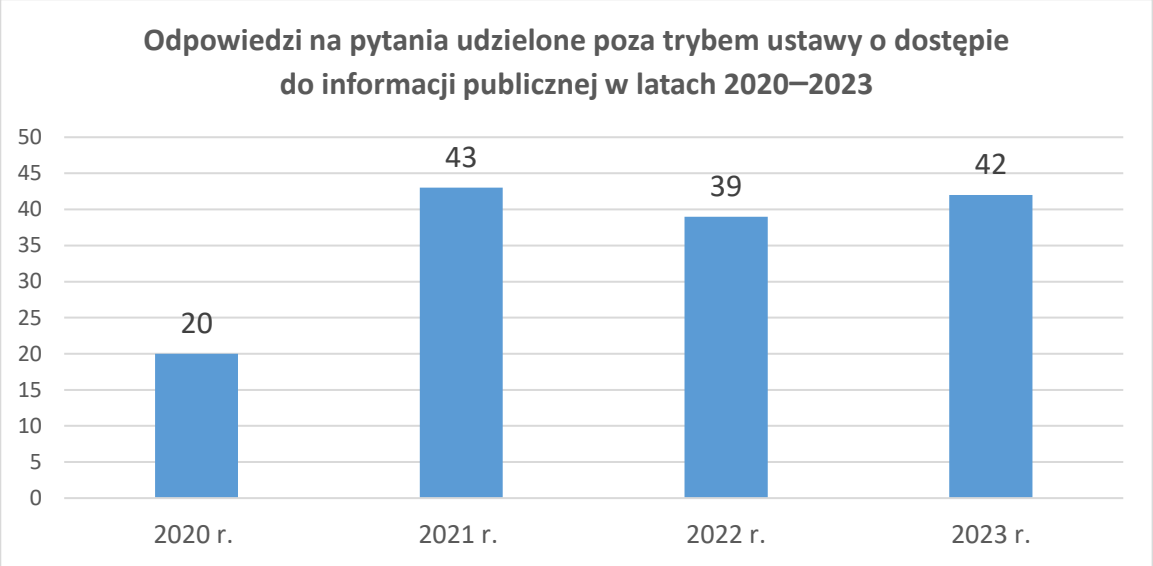
Wykres 20: Liczba wniosków o dostęp do informacji publicznej, które wpłynęły do UODO w latach 2020–2023

O transparentności działania organu świadczy także fakt, że **Prezes Urzędu Ochrony Danych Osobowych wydał tylko 6 decyzji o odmowie udostępnienia informacji publicznej,** z czego 2 decyzje dotyczyły wniosków, które wpłynęły pod koniec 2022 r. Należy podkreślić, że tylko jedna z powyższych decyzji została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie – nie została ona jednak rozpatrzona przez ten sąd w 2023 r.



Wykres 21: Liczba decyzji odmownych w sprawach wniosków o dostęp do informacji publicznej, które wpłynęły do UODO w latach 2020–2023

Poza trybem udostępniania informacji publicznej w 42 przypadkach UODO udzielił informacji i odpowiedzi na pytania z zakresu swojej działalności. Tematyka tych pytań dotyczyła takich zagadnień, jak: współpraca z organami ścigania; były już obowiązek rejestracji zbiorów danych osobowych; przedstawienie Związkowi Banków Polskich kwestii, które mogą być istotne dla działalności sektora bankowego i jego klientów w obszarze przetwarzania danych osobowych; pomoc w zakresie profilu zaufanego w serwisie e-PUAP; instrukcja złożenia skargi do Prezesa UODO; przygotowanie corocznej informacji do Ministerstwa Rodziny, Pracy i Polityki Społecznej na temat działań UODO podjętych w celu urzeczywistnienia uchwały Sejmu RP z 1 sierpnia 1997 r. Karta Praw Osób Niepełnosprawnych i in.

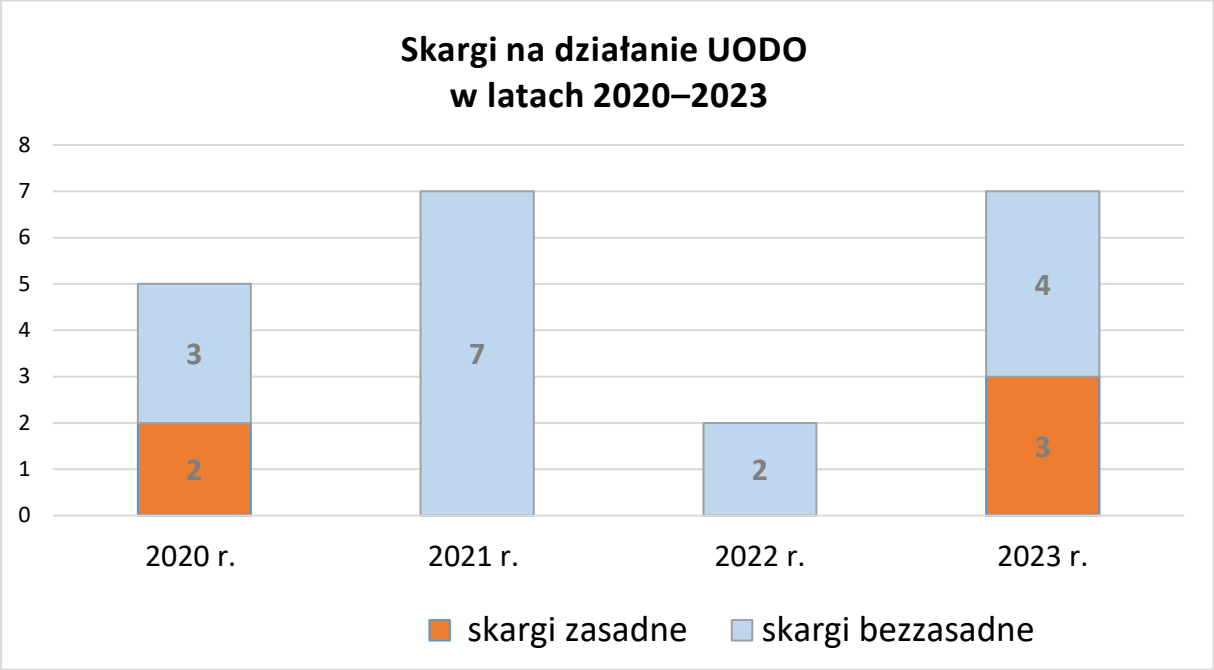


Wykres 22: Porównanie liczby odpowiedzi na pytania skierowane do UODO poza trybem ustawy o dostępie do informacji publicznej w latach 2020–2023

12.3. Skargi na działanie UODO

W 2023 r. do Urzędu Ochrony Danych Osobowych wpłynęło 7 skarg na działanie urzędu. Zdaniem skarżących UODO dopuścił się zaniedbania lub nienależytego wykonywania zadań przez jego pracowników oraz naruszył interesy skarżących wskutek przewlekłego lub biurokratycznego załatwiania spraw. W konsekwencji wywołało to niezadowolenie z rozstrzygnięć prowadzonych postępowań w UODO.

Wszystkie skargi z działu VIII Kodeksu postępowania administracyjnego dotyczące działania UODO zostały rozpatrzone w terminie przewidzianym w ustawie.



Wykres 23*:* Liczba skarg na działanie UODO złożonych w latach 2020–2023

12.4. Wystąpienia

Jak stanowi art. 52 ust. 1 ustawy 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 Ochrony Danych Osobowych 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 jego 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 2023 r. Prezes UODO wystosował **5 wystąpień** z określonymi wnioskami do różnych podmiotów administracji publicznej. Trzy z nich były reakcją na sygnały otrzymane od inspektorów ochrony danych. Dla porównania, w roku sprawozdawczym 2022 skierowano 16 wystąpień.

Poniżej przedstawione zostały wybrane przykłady wystąpień.

Istotnym postulatem organu nadzorczego z punktu widzenia przyjęcia właściwej konstrukcji podstawy prawnej przetwarzania danych osobowych w procesie stanowienia

prawa (oprócz przedstawionych powyżej opinii do poszczególnych projektów aktów) było skierowanie **wystąpienia do Ministra Zdrowia**[346] z wnioskiem o podjęcie odpowiednich działań zmierzających do zmiany i ujednolicenia zasad przyjmowania prawidłowej konstrukcji prawnej zarówno tworzonych, jak i obowiązujących przepisów dotyczących przetwarzania danych osobowych, na potrzeby realizacji programów pilotażowych w rozumieniu art. 48e ustawy z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Organ podkreślił w nim, iż przetwarzanie do celów realizacji programów pilotażowych danych osobowych dotyczących zdrowia, należących do szczególnej kategorii danych osobowych, wymaga szczególnej ochrony. Mając na względzie wagę zadania, jakim jest przygotowanie, przeprowadzenie i ewaluacja programów pilotażowych, jak również konieczność realizacji tego zadania dla budowania jak najlepszych i jak najbardziej efektywnych rozwiązań przeznaczonych ochronie zdrowia, pamiętać należy, że związane z tym przetwarzanie danych szczególnych kategorii także podlegać będzie szczególnym regułom prawnym i gwarancjom, o których mowa w unijnych przepisach o ochronie danych osobowych. Tymczasem dotychczas przedstawione do zaopiniowania przez organ projekty rozporządzeń, dotyczące funkcjonowania poszczególnych programów pilotażowych regulowanym zakresem, przekraczają umocowanie ustawowe, stanowiąc również o określonych procesach przetwarzania danych osobowych – i to danych szczególnych kategorii, nakładając skonkretyzowane obowiązki związane z przetwarzaniem danych osobowych na określone podmioty, np. podmioty medyczne, jako administratorów. Mocą tych rozporządzeń określane były także prawa administratorów czy wręcz kształtowane odrębne przesłanki dla przetwarzania danych, np. zgody osób, których dane dotyczyły, tj. pacjentów albo potencjalnych pacjentów. Prezes UODO podkreślił, że to w przepisach rangi ustawy, a nie rozporządzenia wykonawczego, należy wprowadzić odpowiednio (wyczerpująco) skonstruowaną podstawę prawną dla przetwarzania szczególnych kategorii danych osobowych, a także ściśle określić cele takiego przetwarzania, wskazać: jakie dane będą gromadzone podczas trwania programu pilotażowego, jak będą przetwarzane na potrzeby leczenia pacjentów i programu pilotażowego zarówno w czasie jego trwania, jak i po jego zakończeniu, jak długo będą przechowywane, na jakich zasadach oraz komu i w jaki sposób będą udostępniane. Kluczowe procesy przetwarzania danych szczególnych kategorii nie powinny wynikać jedynie z aktów wykonawczych, które często w sposób fragmentaryczny i niepoprzedzony oceną skutków dla ochrony danych określają prawa i obowiązki związane z przetwarzaniem danych osobowych. Resort zdrowia, odpowiadając na to wystąpienie, podzielił pogląd organu w kwestii dotyczącej konieczności dokonania analizy obowiązujących przepisów i ewentualnego wyeliminowania regulacji, które budzą lub mogą budzić wątpliwości pod kątem zapewnienia spójności polskich norm z przepisami ogólnego rozporządzenia o ochronie danych.

Przykładem działania organu nadzorczego, inspirowanego sygnałami otrzymanymi od inspektorów ochrony danych było **wystąpienie do Ministra Rodziny i Polityki Społecznej** (MRiPS)[347] o rewizję „Stanowiska w sprawie kwalifikowania do uczestnictwa

[346] DOL.413.7.2023 (w zakresie możliwości występowania do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych na podstawie art. 52 ust. 2 ustawy o ochronie danych osobowych).
[347] DOL.413.9.2023.

w klubach samopomocy (uczestnictwo w Klubie Senior+)", opublikowanego na stronie internetowej senior.gov.pl. W stanowisku tym Ministerstwo wskazuje na obowiązek przeprowadzania rodzinnego wywiadu środowiskowego wobec osób zainteresowanych uczestnictwem w zajęciach Klubu „Senior+". Resort stwierdza w nim wprost, że w przypadku udzielania świadczeń z pomocy społecznej, jak również: „w przypadku udzielenia świadczenia w postaci uczestnictwa w zajęciach klubu samopomocy, należy przeprowadzić rodzinny wywiad środowiskowy". Tymczasem z sygnałów otrzymywanych przez UODO od inspektorów ochrony danych wynikało, że obowiązek przeprowadzania rodzinnego wywiadu środowiskowego w celu kwalifikacji do uczestnictwa w Klubie Senior+ nie wynika z żadnego przepisu prawa. Zgłaszane przez IOD wątpliwości dotyczyły też tego, czy przeprowadzenie ww. wywiadu środowiskowego, biorąc pod uwagę ilość danych osobowych pozyskiwanych za pośrednictwem takiego wywiadu, nie naruszałoby określonych w RODO zasad minimalizacji danych i ograniczenia celu.

Organ nadzorczy uznał wątpliwości zgłaszane przez IOD za zasadne. W ocenie Prezesa UODO wskazywanie przez MRiPS na obowiązek przeprowadzania rodzinnego wywiadu środowiskowego we wszystkich przypadkach kwalifikowania osób do uczestnictwa w Klubie „Senior+" – nie znajduje uzasadnienia w świetle zasad ochrony danych osobowych określonych w art. 5 RODO, w tym zasady legalizmu, proporcjonalności czy celowości.

W ocenie organu obowiązujące przepisy kształtują obowiązek przeprowadzenia wywiadu środowiskowego w ściśle określonych warunkach prawnych, a mianowicie jedynie w sytuacji wydawania decyzji administracyjnej. Przeprowadzenie wywiadu środowiskowego jest bowiem ze swej istoty czynnością znacznie ingerującą w prywatność człowieka i nie ma podstaw domniemywania obowiązku realizacji takiej czynności w innych warunkach niż przewidziane w obowiązujących przepisach prawa. Jeżeli zatem udzielenie świadczenia w postaci skierowania do uczestnictwa w zajęciach klubu samopomocy nie następuje w drodze decyzji administracyjnej, nie ma podstaw do wymagania przeprowadzenia wywiadu środowiskowego.

W niektórych sytuacjach przeprowadzenie rodzinnego wywiadu środowiskowego będzie konieczne. Natomiast ww. rekomendacja MRiPS wskazuje, iż przeprowadzenie takiego wywiadu jest konieczne w każdym przypadku udzielenia świadczenia w postaci uczestnictwa w zajęciach Klubu „Senior+". Wskazywanie na obligatoryjność stosowania tego środka dowodowego wprowadza w błąd i prowadzi do nieuzasadnionego pozyskiwania zbyt szerokiego zakresu informacji, w tym danych osobowych. Jeśli jedynymi kryteriami uczestnictwa w Klubie „Senior +" są określony wiek oraz brak aktywności zawodowej, trudno byłoby uznać, że aby zweryfikować spełnianie tych kryteriów, niezbędne są wszystkie dane pozyskiwane w wywiadzie, a tym samym, aby pozyskiwanie tych danych było zgodne z zasadą minimalizacji. W analizowanej sytuacji administrator powinien zatem przyjmować rozwiązania, które nie będą powodowały pozyskiwania nadmiarowych danych osobowych. Wobec tego rodzinny wywiad środowiskowy powinien być przeprowadzany wyłącznie wówczas, gdy jest to niezbędne i uzasadnione w procedurze przyznawania określonego świadczenia.

Wobec powyższego organ nadzorczy uznał za zasadne zwrócenie się do MRiPS o zmianę przedmiotowego stanowiska resortu. Informacje szczegółowe dotyczące

powyższego wystąpienia UODO przedstawione zostały w „Biuletynie UODO" nr 10/10/2023.

W odpowiedzi na przedstawione wystąpienie Ministerstwo Rodziny i Polityki Społecznej[348] zadeklarowało, że mając na uwadze postulat Prezesa UODO, przy okazji przyszłych prac nad nowelizacją ustawy o pomocy społecznej, zostanie dokonana pogłębiona analiza konieczności przeprowadzania rodzinnego wywiadu środowiskowego w przypadku udzielenia świadczenia w postaci uczestnictwa w zajęciach klubu samopomocy.

Kolejnym przykładem działań podjętych w rezultacie przedstawienia konkretnego problemu przez IOD było **wystąpienie UODO do Prezesa Zarządu Krajowej Rady Izb Rolniczych[349].** W wystąpieniu tym organ nadzorczy zwrócił się o podjęcie działań mających na celu ograniczenie zakresu danych ujawnianych w spisie członków izby rolniczej uprawnionych do głosowania w wyborach do walnych zgromadzeń izb rolniczych (spis uprawnionych do głosowania zawiera takie dane, jak: imię i nazwisko, numer PESEL, data urodzenia oraz miejsce zamieszkania), który udostępniony jest do wglądu w siedzibie gminy, tak by możliwe było zapewnienie poszanowania zasady minimalizacji danych. Urząd Ochrony Danych Osobowych wystąpił o spowodowanie podjęcia przez organy ujawniające spisy uprawnionych do głosowania stosownych środków techniczno-organizacyjnych, zmierzających do zabezpieczenia danych ujętych w spisie przed dostępem innych osób, również tych, których dane będą się tam znajdować.

Jeszcze innym przykładem podejmowania działań przez UODO w ramach współpracy z IOD było **wystąpienie do Ministra Edukacji i Nauki[350].** Inspektorzy ochrony danych, pełniący swoją funkcję w szkołach, zasygnalizowali organowi nadzorczemu potrzebę dostosowania art. 90l ustawy z 7 września 1991 r. o systemie oświaty do zasad ochrony danych osobowych określonych w art. 5 RODO. Zgodnie z powołanym przepisem osoby fizyczne i osoby prawne inne niż jednostki samorządu terytorialnego, przyznające ze środków własnych uczniom stypendia za wyniki w nauce lub za osiągnięcia sportowe, na warunkach i w trybie określonych w ustalonym przez siebie regulaminie, mogą ubiegać się o zatwierdzenie tego regulaminu przez ministra właściwego do spraw oświaty i wychowania. W stosowaniu tego przepisu wątpliwości budzi przede wszystkim to, czy i w jakim zakresie w przetwarzaniu danych osobowych uczniów – w związku z przyznawaniem im takich stypendiów – uczestniczą szkoły i na jakiej podstawie prawnej mogą one przetwarzać ich dane osobowe, w tym udostępniać je administratorom z sektora prywatnego.

Art. 90l ustawy o systemie oświaty ma charakter blankietowy i z jego brzmienia nie wynika, jak ma wyglądać proces przyznawania stypendiów, jakie obowiązki spoczywają na fundatorze, a jakie na stypendyście, a także czy, a jeżeli tak, to jaką rolę w tym procesie mają odgrywać inne podmioty, np. szkoły. W ocenie organu nadzorczego przepis ten powinien szczegółowo regulować nie tylko minimalną zawartość regulaminu przyznawania stypendiów, ale przede wszystkim określać wszelkie istotne aspekty procesów przetwarzania danych, zwłaszcza w sytuacji, gdy będą to dane szczególnych kategorii.

[348] DPS-I.0211.122.2023.AM.
[349] DOL.413.8.2023.
[350] DOL.413.4.2023.

Organ nadzorczy zwrócił też uwagę, że RODO stawia administratorom przetwarzającym dane osobowe dzieci szczególne wymagania, zwłaszcza co do warunków ich pozyskania. Biorąc pod uwagę powyższe, Prezes UODO zwrócił się do Ministra Edukacji i Nauki o zmianę art. 90l ustawy o systemie oświaty w sposób zapewniający poszanowanie zasad ochrony danych osobowych. Wskazał, że szczególnie istotne jest precyzyjne uregulowanie, kto, w jakim celu i jakie dane osobowe (również te szczególnych kategorii) ma prawo przetwarzać, w tym, kto, komu, na jakich zasadach i w jakim trybie może je udostępniać. W ocenie organu nadzorczego równie ważne jest też wskazanie okresów retencji danych.

Prezes UODO nie otrzymał od Prezesa Zarządu Krajowej Rady Izb Rolniczych oraz Ministerstwa Edukacji i Nauki informacji w zakresie podjęcia przez te podmioty działań, o które organ nadzorczy występował w opisanych powyżej sprawach.

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA

Zgodnie z 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[351];*
- *upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO[352];*
- *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[353].*

Organ właściwy w sprawie ochrony danych osobowych podejmuje szereg działań edukacyjno-informacyjnych, których celem jest zwiększenie 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, w analizowanym 2023 r. UODO zorganizował szereg inicjatyw 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. Urząd Ochrony Danych Osobowych współpracuje ze szkołami wyższymi, a jego eksperci wspierają swoją wiedzą wiele wydarzeń krajowych i międzynarodowych.

[351] Art. 57.1.b RODO.
[352] Art. 57.1.d RODO.
[353] Art. 57.1.e RODO.

1.1. Szkolenia zewnętrzne

Cyklicznymi szkoleniami organizowanymi od 14 lat przez UODO są szkolenia realizowane w ramach ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Uczestnikami dwudniowych szkoleń, które każdego roku odbywają się w październiku, są koordynatorzy bieżącej edycji tego Programu. Następnie koordynatorzy ci przekazują zdobytą podczas szkolenia wiedzę innym nauczycielom, a także uczniom podczas prowadzonych z nimi lekcji. Działania te mają na celu upowszechnienie wiedzy na temat bezpiecznego posługiwania się danymi osobowymi w szkole i poza nią. Szkolenie to jest jednym z najważniejszych etapów Programu, dzięki któremu kadra pedagogiczna szkół i placówek doskonalenia nauczycieli jest wyposażona w 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 tematycznych zajęć z uczniami.

Szkolenie pracowników KPRM, 12.06.2023 r.

Uczestnikami szkolenia przeprowadzonego 12 czerwca 2023 r. przez ekspertów UODO byli pracownicy Kancelarii Prezesa Rady Ministrów (KPRM). Tematem spotkania była prezentacja zasad ochrony danych osobowych w organizacji pracy KPRM, projektowanie ochrony danych osobowych w przepisach prawa oraz najczęściej pojawiające się wyzwania dla ochrony prywatności. Przedstawione zostały zagadnienia dotyczące naruszeń ochrony danych osobowych odnoszące się do praktycznych aspektów związanych z realizacją zasady poufności w działalności KPRM, jak też analiza przyczyn naruszeń na wybranych przykładach i ich konsekwencje. Ważnym punktem szkolenia była prezentacja wyzwań w zakresie ochrony danych osobowych w związku z nakładanymi przez UODO karami.

1.2. Projekty i programy

1.2.1. Ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa"

XIII edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa" w roku szkolnym 2022/2023 oraz rozpoczęcie XIV edycji w roku szkolnym 2023/2024.

Program jest największym systemowym projektem edukacyjnym Prezesa Urzędu Ochrony Danych Osobowych realizowanym na skalę ogólnopolską, w którym uczestnikami są szkoły podstawowe, ponadpodstawowe oraz placówki doskonalenia nauczycieli.

Program jest szansą dla uczniów i nauczycieli na zdobywanie oraz rozwijanie praktycznych umiejętności w obszarze ochrony danych osobowych i prawa do prywatności oraz kompetencji cyfrowych, niezbędnych we współczesnym świecie. Stanowi źródło wiedzy i dobrych praktyk dla nauczycieli w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty. Rezultatem podejmowanych działań edukacyjnych jest odpowiednia wiedza i umiejętności

uczniów i nauczycieli w zakresie ochrony prywatności i danych osobowych oraz świadomość swoich praw i obowiązków wynikających z przepisów prawa.

Program „Twoje dane – Twoja sprawa” od wielu lat cieszy się popularnością i na trwałe wpisał się w kalendarz szkolnych wydarzeń, ze szczególnym uwzględnieniem obchodów Dnia Ochrony Danych Osobowych – 28 stycznia.

W ramach Programu odbywają się szkolenia, konferencje, webinaria, zajęcia lekcyjne, pozalekcyjne i wydarzenia tematyczne skierowane do uczniów, nauczycieli i dyrektorów szkół. Każdą edycję programu rozpoczyna październikowe szkolenie, a podsumowuje – spotkanie organizowane w czerwcu.

W ramach Programu uczestnicy otrzymują dostęp do platformy z materiałami edukacyjnymi, a także biorą udział w organizowanych przez UODO wydarzeniach. Praktyczne zajęcia służą budowaniu świadomości i rozumieniu pewnych zjawisk związanych z ochroną prywatności i i danych osobowych oraz umiejętnemu stosowaniu nabytej wiedzy w życiu.

Średnio co roku w ramach programu „Twoje dane – Twoja sprawa” odbywa się około 5 000 lekcji i różnorodnych wydarzeń skierowanych do: uczniów, nauczycieli, rodziców, seniorów i środowiska lokalnego. W każdej jego edycji bierze udział około 50 000 uczniów, a ponad 5 000 nauczycieli zostaje zaangażowanych w działania związane z Programem.

W roku 2023 Urząd Ochrony Danych Osobowych realizował XIII edycję Programu i rozpoczął jego XIV edycję. Każda z nich organizowana jest zgodnie z kalendarzem roku szkolnego.

XIII edycja programu „Twoje dane – Twoja sprawa” – rok szkolny 2022/2023

XIII edycja programu edukacyjnego „Twoje dane – Twoja sprawa” koncentrowała się na edukacji dzieci i młodzieży w zakresie poszanowania prawa do prywatności oraz potrzeby ochrony danych osobowych w cyfrowym świecie.

W roku szkolnym 2022/2023, w XIII edycji Programu, udział wzięło 276 placówek oświatowych, w tym 170 szkół podstawowych, 96 szkół ponadpodstawowych oraz 10 placówek doskonalenia nauczycieli. Rekrutacja uczestników rozpoczęła się 1 września 2023 r.

Najwięcej zgłoszeń wpłynęło z województwa mazowieckiego – 55 oraz śląskiego – 34.

- liczba placówek, które przystąpiły do programu po raz pierwszy – 86,
- liczba uczestników kontynuujących współpracę kolejny rok – 190,
- liczba inicjatyw edukacyjnych – 4 080, w tym 2 993 lekcji poświęconych ochronie danych osobowych i prywatności,
- liczba uczniów biorących udział w zajęciach – 47 004,
- liczba przeszkolonych nauczycieli – 2 637,
- liczba nauczycieli zaangażowanych w działania – 587.

#ODOlekcje – cykl zajęć dla uczniów

W cyklu zajęć zrealizowanych pod hasłem #ODOlekcje odbyło się 6 ogólnopolskich lekcji dla uczniów szkół podstawowych i ponadpodstawowych, w których udział wzięło

prawie 500 klas, czyli około 10 000 uczniów. Atutami zajęć była formuła online, regularność zajęć, różnorodność tematów podkreślających rolę ochrony prywatności i danych osobowych w życiu, a także dostosowanie tematyki i sposobu realizacji lekcji do potrzeb uczniów z niepełnosprawnościami.

- „Pozwólcie, że się przedstawię – moja nowa koleżanka Prywatność. Co warto i dlaczego zachować dla siebie?" z udziałem 104 klas (21.11.2022 r.);
- „Prawo do prywatności – czyli sposób na anonimizację zdjęć i usuwanie metadanych?" (9.12.2022 r.). W zajęciach udział wzięły 133 klasy, w tym uczniowie ze szkół specjalnych;
- „DODO Agencja – mitologiczna interwencja" z udziałem 73 klas (26.01.2023 r.);
- „Ile warte są Twoje dane? Kilka słów o wyzwaniach związanych z monetyzacją danych osobowych". W zajęciach udział wzięło 96 klas (7.02.2023 r.);
- „Dane biometryczne – bezpieczeństwo czy ryzyko?" z udziałem 43 klas (23.03.2023 r.);
- „Fake news – czy wiemy, jak sobie z tym radzić? Dane osobowe w świecie manipulacji informacją". W zajęciach udział wzięły 42 klasy (28.04.2023 r.).

Dodatkowe inicjatywy edukacyjne UODO w ramach XIII edycji programu „Twoje dane – Twoja sprawa"

Szkolenia, materiały edukacyjne, webinaria oraz wsparcie ekspertów UODO przyczyniają się do wzrostu wiedzy oraz podniesienia kompetencji nauczycieli i pedagogów uczestniczących w Programie. W ramach jego XIII edycji zostało zorganizowane dla dyrektorów szkół, nauczycieli oraz szkolnych inspektorów ochrony danych webinarium z cyklu „RODO w szkolnej ławce", pt. „Przetwarzanie danych osobowych przez poradnie psychologiczno-pedagogiczne i rady rodziców" z udziałem 67 uczestników (8.12.2022 r.). Podczas wykładu ekspertka UODO wyjaśniła, kto jest administratorem danych przetwarzanych przez poradnie psychologiczno-pedagogiczne w ramach kompetencji własnych oraz przez szkolnych psychologów i pedagogów. Wiele uwagi poświęciła na omówienie obowiązków administratorów wynikających z RODO, zasad, jakimi pedagodzy i psycholodzy szkolni powinni się kierować podczas udzielania odpowiedzi na wnioski o udostępnienie informacji o charakterze osobowym, oraz wyjaśnieniu roli rady rodziców w procesie przetwarzania danych osobowych w szkole.

Urząd Ochrony Danych Osobowych i Urząd Komunikacji Elektronicznej zorganizowali webinarium dla uczniów szkół podstawowych i ponadpodstawowych pt. „Na jaką przynętę dasz się złapać?". Tematem przewodnim spotkania było uwrażliwienie dzieci i młodzieży na phishing w związku ze znacznym wzrostem wyłudzeń danych osobowych w Internecie (13.04.2023 r.). W lekcji wzięło udział 386 klas.

Kolejne webinarium pt. „Z Rodusiem chronimy dane osobowe" (1.06.2023 r.) zostało zorganizowane dla uczniów edukacji wczesnoszkolnej. Spotkanie z maskotką robota Rodusia wykonanego przez dzieci było szczególną okazją do świętowania Dnia Dziecka oraz utrwalenia zasad ochrony danych osobowych w kontekście bezpiecznego korzystania z Internetu. W zajęciach wzięło udział 100 klas.

Konkursy organizowane w ramach XIII edycji programu „Twoje dane – Twoja sprawa"

Konkursy organizowane przez Prezesa UODO zachęcają uczniów do głębszego zainteresowania się tematyką ochrony danych osobowych, a szkoły do dzielenia się wiedzą i opracowywania autorskich materiałów edukacyjnych.

Konkursy zostały ogłoszone 1 marca 2023 r. Natomiast uroczystość wręczenia nagród i prezentacja prac konkursowych odbyły się 14 czerwca 2023 r. w Zespole Szkół nr 1 im. Władysława Grabskiego w Lublinie w ramach podsumowania XIII edycji programu.

Na zwycięskie prace w konkursie dla uczniów złożyły się filmy, rysunki i komiksy pt. „Ochrona danych osobowych w cyfrowej dżungli". Komisja konkursowa uhonorowała sześciu zwycięzców w dwóch kategoriach – szkoła podstawowa oraz szkoła ponadpodstawowa.

Z kolei w konkursie na inicjatywę roku 2023/2024 wybrano i nagrodzono trzy inicjatywy edukacyjne zrealizowane w oparciu o autorskie scenariusze zajęć.

Szczególnym wyróżnieniem Prezesa UODO – statuetką „Złotego pióra" – został uhonorowany Zespół Szkół nr 1 im. Władysława Grabskiego w Lublinie za zajęcie I miejsca w ww. konkursie.

XIV edycja programu „Twoje dane – Twoja sprawa", rok szkolny 2023/2024

Jak co roku, również XIV edycja programu „Twoje dane – Twoja sprawa" przyciągnęła uwagę wielu szkół i placówek oświatowych z całego kraju. 1 września 2023 r. rozpoczęła się rekrutacja uczestników tej edycji w roku szkolnym 2023/2024. Na koniec 2023 r. do udziału w XIV edycji programu przystąpiły 303 placówki oświatowe (197 szkół podstawowych, 99 szkół ponadpodstawowych oraz 7 placówek doskonalenia nauczycieli). Najliczniej reprezentowane były placówki oświatowe z województw mazowieckiego i śląskiego.

Szkolenie online, które odbyło się 25–26 października 2023 r., zainaugurowało XIV edycję Programu. Miało na celu przygotowanie szkolnych koordynatorów programu do

jego realizacji. Podczas pierwszego dnia szkolenia eksperci UODO przekazali niezbędną wiedzę w zakresie przetwarzania danych osobowych w placówkach oświatowych oraz omówili szczegóły realizacji programu. Drugi dzień szkolenia stanowił blok wymiany doświadczeń i dobrych praktykach, a także innowacyjnych pomysłów nauczycieli na realizację przedsięwzięć edukacyjnych.

W 2023 r., w ramach XIV edycji programu „Twoje dane – Twoja sporawa", Urząd Ochrony Danych Osobowych kontynuował cykl zajęć ogólnopolskich dla uczniów szkół podstawowych i ponadpodstawowych pod hasłem „#ODOlekcje". W ramach tego cyklu odbyły się następujące lekcje online:

- „To nie są ślady na piasku – cyfrowa tożsamość i cyfrowa reputacja" (20.11.2023 r.);
- „Prawo do ochrony danych osobowych jako prawo człowieka" (8.12.2023 r.).

Ponadto urząd zorganizował również webinarium dla koordynatorów programu pt. „Jak dobrze zaplanować działania w ramach Programu? Narzędzia coachingu do pracy z celami" (18.12.2023 r.).

Szczegóły XIV edycji programu „Twoje dane – Twoja sprawa" zostaną opisane w następnym roku sprawozdawczym.

Podsumowanie i wnioski

Od wielu lat program „Twoje dane – Twoja sprawa" jest szansą dla uczniów na zdobywanie wiedzy i rozwijanie praktycznych umiejętności niezbędnych we współczesnym świecie, które obejmują ochronę prywatności i danych osobowych oraz bezpieczne i odpowiedzialne korzystanie z technologii cyfrowych i wykorzystywanie ich do uczenia się, pracy i udziału w życiu społecznym. Dzieląc się z młodzieżą sprawdzonymi narzędziami oraz doświadczeniem, wspólnie tworzymy bardziej świadome społeczeństwo. Bardzo ważne jest, aby dzieci od najmłodszych lat były świadome swoich praw, znały mechanizmy ich ochrony, a nade wszystko potrafiły realizować je w życiu codziennym. To daje gwarancję przygotowania do aktywnego, bezpiecznego uczestnictwa w życiu społecznym i przestrzeni cyfrowej.

Wykorzystywane przez uczestników programu sprawdzone metody aktywizujące mają na celu nie tylko przekazanie wiedzy, ale przede wszystkim rozwijanie umiejętności krytycznego myślenia, dbania o swoje bezpieczeństwo oraz umiejętne korzystanie z nowych rozwiązań technologicznych.

Podobnie jak w latach ubiegłych, w XIII edycji programu odbyły się liczne wydarzenia skierowane do uczniów i nauczycieli. Powstało ponad 4 000 cennych społecznie przedsięwzięć na rzecz ochrony danych osobowych dzieci, z których najciekawsze zostały wyróżnione i nagrodzone w ramach organizowanych przez Prezesa UODO konkursów. Zakres omawianych tematów stanowił rozwinięcie treści i zagadnień zawartych w podstawie programowej, a także na stałe wpisał się kalendarz działań profilaktyczno-wychowawczych szkół. Spotkania z ekspertami i współpraca ze środowiskiem lokalnym, a także zaangażowanie dzieci w dialog międzypokoleniowy na temat ochrony danych osobowych poprzez różnorodne inicjatywy, poszerzyły zasięg realizowanych projektów poza mury szkoły. Dzieci i młodzież są coraz bardziej świadomi swoich praw obowiązków wynikających z przepisów prawa.

Przygotowano ofertę dostosowaną do potrzeb uczniów w różnym wieku. Wzięto pod uwagę różne potrzeby, w tym zadbano, aby treści były dostosowane do uczniów ze

szczególnymi potrzebami. Stopień spełnienia oczekiwań uczestników programu jest bardzo wysoki, o czym świadczą wysokie oceny Programu przez jego beneficjentów – uczniów i nauczycieli. Nauczyciele podkreślają konieczność kontynuowania zajęć w tym obszarze tematycznym – jako niezbędny element szkolnej i pozaszkolnej edukacji. Większość uczestników dostrzega zasadność realizacji programu w kolejnych latach i podejmowania działań edukacyjnych, aby dzieci rozumiały zagadnienia związane z ochroną danych osobowych adekwatnie do złożoności tych zagadnień i wieku dziecka. Nauczyciele wskazywali na uniwersalny zakres merytoryczny zajęć oraz duże zainteresowanie uczniów i nauczycieli jego realizacją. Uczniom najbardziej podobał się praktyczny aspekt przekazywanych informacji oraz możliwość dzielenia się własnymi doświadczeniami. W ocenie uczniów tematyka ochrony danych osobowych jest niezwykle istotna i potrzebna w życiu.

Program stanowi cenne źródło aktualnej i rzetelnej wiedzy oraz dobrych praktyk w zakresie ochrony danych osobowych w szkołach, a także realizacji obowiązków wynikających z ogólnego rozporządzenia o ochronie danych. Ma również wpływ na wzrost zaangażowania nauczycieli w realizację innowacyjnych zajęć z uczniami. Rezultatem podejmowanych przez Urząd Ochrony Danych Osobowych działań edukacyjnych jest większa świadomość uczniów w obszarze ochrony danych osobowych oraz wzrost zainteresowania tematem ochrony prywatności w życiu. Program to okazja do współpracy z wieloma urzędami i instytucjami na rzecz ochrony prywatności oraz danych osobowych dzieci czy promocji szkoły zaangażowanej i aktywnie działającej na rzecz zwiększenia bezpieczeństwa uczniów.

Z uwagi na duże zapotrzebowanie na wiedzę w ww. zakresie program „Twoje dane – Twoja sprawa” będzie kontynuowany w kolejnych latach.

1.2.2. Letnia Akademia Liderów RODO

Letnia Akademia Liderów RODO to inicjatywa edukacyjna Prezesa Urzędu Ochrony Danych Osobowych skierowana do studentów: prawa, administracji, stosunków międzynarodowych oraz informatyki, a także młodych absolwentów tych kierunków. Inicjatywa ma stanowić nowoczesną formę kształcenia, dzięki której młodzi ludzie mogą czerpać z wiedzy i doświadczenia ekspertów z zakresu ochrony danych osobowych. Letnia Akademia Liderów RODO to program, który powstał w związku z 5. rocznicą stosowania RODO w Polsce. Natomiast 30 kwietnia 2023 r. minęło ćwierć wieku obowiązywania w Polsce przepisów o ochronie danych osobowych. W związku z tymi ważnymi rocznicami dla ochrony danych osobowych w Polsce postanowiono zaakcentować te daty uruchomieniem inicjatywy pod nazwą Letnia Akademia Liderów RODO. Celem akademii jest zwiększenie poziomu wiedzy i świadomości młodych ludzi w zakresie ochrony danych osobowych. Uczestnicy I edycji akademii wzięli udział w wykładach prowadzonych przez ekspertów, którzy poruszyli między innymi tematy związane z kontrolami i naruszeniami ochrony danych osobowych, zadaniami inspektorów ochrony danych czy ze współpracą UODO z Europejską Radą

Ochrony Danych. Uczestnicy Letniej Akademii Liderów RODO dowiedzieli się również, jak prawidłowo złożyć skargę do Urzędu Ochrony Danych Osobowych na naruszenie przepisów RODO, jak wygląda procedura nakładania administracyjnych kar pieniężnych przez Prezesa UODO, czy jak zadbać o dane osobowe w dobie postępu technologicznego. W trakcie wykładów przybliżono również zagadnienia związane z ochroną danych osobowych w kontekście cyberbezpieczeństwa i nowych technologii.

Realizacja I edycji projektu odbywała się w okresie 11.07–18.09.2023 r. Przystąpiło do niej 30 studentów i absolwentów kierunków: administracja, prawo, informatyka i stosunki międzynarodowe. Wykładowcami w akademii byli przedstawiciele Urzędu Ochrony Danych Osobowych i Ministerstwa Cyfryzacji, a także zaproszeni eksperci.

Program akademii obejmował siedem dni wykładowych, podczas których były prowadzone wykłady w formie online, a także odbyło się spotkanie finałowe z wykładowcami w siedzibie Akademii Ekonomiczno-Humanistycznej w Warszawie. Uroczystość zakończenia Letniej Akademii Liderów RODO odbyła się 18.09.2023 r. na sali symulacji rozpraw sądowych tej uczelni. Projekt Letnia Akademia Liderów RODO przyczynił się do wzbogacenia studentów i absolwentów studiów kierunkowych o praktyczną wiedzę dotyczącą zasad ochrony danych osobowych.

Letnia Akademia Liderów RODO została objęta patronatem honorowym: Ministra Cyfryzacji, Ministra Edukacji i Nauki, Urzędu Komunikacji Elektronicznej, Rządowego Centrum Legislacji, Instytutu Prawa Ochrony Danych Osobowych, Prezesa Krajowej Izby Radców Prawnych, Naukowej i Akademickiej Sieci Komputerowej oraz Akademii Ekonomiczno-Humanistycznej w Warszawie. Patronat medialny nad inicjatywą objął ogólnopolski dziennik ekonomiczno-prawny „Rzeczpospolita”.

1.3. Program wymiany pracowników

Na podstawie art. 70 ust. 1 lit. v) RODO Europejska Rada Ochrony Danych uruchomiła w 2019 r. program wymiany pracowników „European Data Protection Board Secondments Programme”. Wspomniany przepis nakłada na EROD obowiązek zapewnienia spójnego stosowania RODO. W tym celu, z własnej inicjatywy lub w stosownych przypadkach na wniosek Komisji, EROD podejmuje działania w celu upowszechniania wspólnych programów szkoleń oraz ułatwienia wymiany personelu między organami nadzorczymi, a w stosownych przypadkach – z organami nadzorczymi państw trzecich lub organizacji międzynarodowych.

Celem programu obejmującego lata 2022–2023 było upowszechnienie wspólnych programów szkoleń oraz ułatwienie wymiany pracowników organów nadzorczych, aby umożliwić dzielenie się doświadczeniami i najlepszymi praktykami.

W ramach programu, w dniach 8–26 maja 2023 r., Urząd Ochrony Danych Osobowych gościł przedstawiciela urzędu Państwowego Rzecznika Ochrony Danych i Wolności Informacji Kraju Związkowego Nadrenia-Palatynat oraz przedstawiciela Urzędu Ochrony Danych Osobowych w Pradze. Goście wizytujący polski organ nadzorczy wymienili doświadczenia z ekspertami UODO odnoszące się do wielu zadań, między innymi w zakresie współpracy międzynarodowej, w szczególności w ramach EROD oraz koordynacji systemu IMI, procedurach rozpatrywania skarg i prowadzenia w tym obszarze postępowań administracyjnych. Omawiano także praktyczne aspekty dotyczące zapewnienia wykonania nakazów decyzji administracyjnych, wypełniania obowiązków związanych: z prowadzeniem kontroli, przyjmowaniem zgłoszeń naruszeń ochrony

danych, opiniowaniem projektów aktów prawnych i ze współpracą z inspektorami ochrony danych. Zapoznali się także z postępami prac nad współpracą z inicjatywami zgłaszającymi projekty kodeksów postępowania, a także prowadzania działań informacyjnych za pośrednictwem infolinii.

1.4. Porozumienia o współpracy

Krajowa Izba Radców Prawnych (KIRP), 5.04.2023 r.

W dniu 5 kwietnia 2023 r. Jakub Groszkowski – Zastępca Prezesa UODO i Włodzimierz Chróścik – Prezes Krajowej Rady Radców Prawnych podpisali porozumienie o współpracy. Na podstawie tego dokumentu Urząd Ochrony Danych Osobowych i Krajowa Izba Radców Prawnych będą wspierać się w działaniach na rzecz promowania oraz ochrony ważnych dla siebie wartości, a także uczestniczyć w projektach oraz podejmować wspólne inicjatywy. Głównym celem porozumienia o współpracy jest pogłębienie świadomości prawnej dotyczącej zasad ochrony danych osobowych wśród członków samorządu radców prawnych i obywateli. Współpraca obu instytucji umożliwi wymianę doświadczeń, współpracę szkoleniową, a także udział w tworzeniu spójnych i przemyślanych przepisów z zakresu ochrony danych osobowych dotyczących obszarów związanych z wykonywaniem przez radców prawnych ich zawodu oraz funkcjonowaniem samorządu.

Główny Inspektorat Farmaceutyczny (GIF), 7.12.2023 r.

Ujawnianie i eliminowanie naruszeń prawa związanych z przetwarzaniem danych osobowych pacjentów oraz pracowników aptek ogólnodostępnych było głównym celem podpisanego 7 grudnia 2023 r. porozumienia o współpracy pomiędzy Prezesem Urzędu Ochrony Danych Osobowych i Głównym Inspektorem Farmaceutycznym. Współpraca skupiać się będzie na edukowaniu przedsiębiorców prowadzących apteki ogólnodostępne, w związku z przetwarzaniem przez nich danych szczególnej kategorii, tj. danych o stanie zdrowia. Przewidziane są wspólne: konferencje, seminaria, szkolenia oraz inne inicjatywy edukacyjne na rzecz poszerzania świadomości w zakresie ochrony danych osobowych. Podpisane porozumienie przyczyni się zarówno do skuteczniejszej ochrony pacjentów, jak i wsparcia administratorów w wykonywanej przez nich pracy. Obie instytucje zobowiązały się do wzajemnego przekazywania informacji i organizowania wspólnych narad związanych z naruszeniami przetwarzania danych osobowych pacjentów oraz pracowników aptek. Porozumienie formalizuje istniejącą już współpracę UODO i GIF, podejmowaną w celu skutecznego wypełniania zadań wynikających z ogólnego rozporządzenia o ochronie danych osobowych i ustawy – Prawo farmaceutyczne.

Naczelna Izba Pielęgniarek i Położnych, 21.12.2023 r.

21 grudnia 2023 r. Urząd Ochrony Danych Osobowych zawarł porozumienie z Naczelną Izbą Pielęgniarek i Położnych, którego założeniem jest współpraca przy inicjatywach mających poszerzać wiedzę z zakresu ochrony danych osobowych. Obie instytucje będą wymieniać się wiedzą, informacjami i doświadczeniami oraz doskonalić umiejętności w celu stworzenia i ulepszania sieci profesjonalistów zajmujących się ochroną danych osobowych. Ponadto będą angażować się wspólnie w kursy i szkolenia oraz wspierać się w badaniach, publikacjach i ekspertyzach, które w przyszłości przysłużą się wypracowaniu spójnych oraz przemyślanych przepisów z zakresu ochrony danych osobowych.

1.5. Publikacje

„Wyzwania dla ochrony danych osobowych związane z rozwojem technologii" pod redakcją Justyny Krzywkowskiej, Jacka Mrozka i Jakuba Groszkowskiego, Olsztyn 2023, ISBN 978-83-61605-79-9.

Publikacja jest podsumowaniem trwającej 17 lat tradycji obchodów Dnia Ochrony Danych Osobowych, która co roku jest świętowana 28 stycznia. Szesnastu ekspertów z zakresu prawa do prywatności i ochrony danych osobowych przedstawiło swoje badania i wnioski na temat wpływu technologii na społeczeństwo i sposób życia jego członków oraz wskazali na niebezpieczeństwa z tym związane. Książka jest zbiorem rozważań nad obecnymi i przyszłymi kierunkami ochrony danych osobowych w dobie rozwoju technologii i respektowania demokratycznych praw, jak prawo: do prywatności, informacji, bezpieczeństwa publicznego, wolności słowa czy wyznania.

„Raport z Forum Nowych Technologii 2023"

Zależność pomiędzy ochroną danych osobowych a sztuczną inteligencją były przedmiotem licznych wystąpień oraz ożywionej dyskusji podczas Forum Nowych Technologii, które z inicjatywy Urzędu Ochrony Danych Osobowych i we współpracy z Akademią Ekonomiczno-Humanistyczną w Warszawie odbyło się 20–21 września 2023 r. w siedzibie tej uczelni. Przygotowane zostały nagrania filmowe i fotorelacje dokumentujące przebieg Forum. Powstała także publikacja pt. „Raport z Forum Nowych Technologii" zawierająca najważniejsze wnioski z przebiegu poszczególnych sesji oraz końcowej debaty eksperckiej poświęconej najważniejszym trendom w kontekście ochrony danych osobowych.

„Ochrona danych osobowych w kampanii wyborczej" – poradnik

O tym, jak zapobiec występowaniu nieprawidłowości i naruszeń związanych z przetwarzaniem danych osobowych w kampanii wyborczej, można było się dowiedzieć z poradnika Urzędu Ochrony Danych Osobowych pt. „Ochrona danych osobowych w kampanii wyborczej". Komitety wyborcze oraz inne podmioty zaangażowane w kampanię wyborczą muszą przestrzegać nie tylko przepisów bezpośrednio regulujących jej przebieg, ale również przepisów o ochronie danych osobowych. Ma to tym większe znaczenie, że przepisy regulujące przebieg wyborów w ograniczonym zakresie odnoszą się do kwestii związanych z ochroną danych osobowych. Dlatego w poradniku omówiono takie kwestie, jak:

- akty prawne regulujące przebieg wyborów, w sposób szczególny akcentując zagadnienia związane z przetwarzaniem danych osobowych wyborców;
- zasady dotyczące przetwarzania danych osobowych w procesie wyborczym;
- obwiązki administratora, administracji wyborczej i komitetów wyborczych;
- prawa wyborców i innych osób, których dane są przetwarzane.

W publikacji czytelnicy znajdą m.in. wskazówki z zakresu: realizacji obowiązku informacyjnego, prowadzenia dokumentacji przetwarzania danych, zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu czy wyznaczania inspektora ochrony danych (IOD). Ważną funkcją poradnika jest również przybliżenie obywatelom ich praw w zakresie ochrony danych osobowych w kontekście aktualnych przepisów prawa

wyborczego. Odrębną część publikacji stanowią odpowiedzi na najczęściej pojawiające się pytania odnośnie do tematu głównego poradnika.

Najnowszy poradnik Urzędu Ochrony Danych Osobowych to zaktualizowana wersja publikacji opracowanej we wrześniu 2018 r.

1.6. Współpraca krajowa przy Polskim Komitecie Normalizacyjnym (PKN)

Dyrektor Departamentu Nowych Technologii, jako przedstawiciel Prezesa Urzędu Ochrony Danych Osobowych, jest reprezentantem UODO w PKN KT 182 ds. Ochrony Informacji w Systemach Teleinformatycznych, który realizuje cele wymienione w art. 3 ustawy z 12 września 2002 r. o normalizacji[354] (poprzez opracowywanie norm i innych dokumentów normalizacyjnych w przyporządkowanych im zakresach tematycznych, między innymi poprzez udział ich przedstawicieli w pracach międzynarodowych i europejskich organizacji normalizacyjnych). Do zadań członka KT należy m.in. aktywne uczestnictwo w pracach KT oraz opiniowanie projektów Polskich Norm, Norm Europejskich i Norm Międzynarodowych oraz innych dokumentów normalizacyjnych.

1.7. Nagroda im. Michała Serzyckiego

Nagroda im. Michała Serzyckiego jest wyróżnieniem Prezesa Urzędu Ochrony Danych Osobowych dla tych, którzy przyczyniają się do poszerzania świadomości na temat prywatności i roli ochrony danych osobowych w wielu dziedzinach oraz środowiskach. Od 2018 r. nagroda ta jest wręczana co roku podczas obchodów Dnia Ochrony Danych Osobowych. Nazwa nagrody 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 2023 r. nagrodę im. Michała Serzyckiego przyznano już po raz szósty. Wyróżnienie otrzymali: dr Edyta Bielak-Jomaa – pracownik naukowy Uniwersytetu Łódzkiego oraz Prezes Urzędu Ochrony Danych Osobowych w latach 2015–2019; dr Urszula Góral – IOD Sejmu RP, Pani Iwona Niedzielska-Taźbier – nauczycielka ze Szkoły Podstawowej Nr 17 z Oddziałami Integracyjnymi im. 21. Brygady Strzelców Podhalańskich w Rzeszowie. Nagrodzonych wyróżniono za działania na rzecz edukacji w dziedzinie ochrony danych osobowych. Uroczystość wręczenia nagród odbyła się w Ełku, 31 stycznia 2023 r., podczas konferencji zorganizowanej przez UODO w ramach obchodów XVII Dnia Ochrony Danych Osobowych.

1.8. 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 oraz patronował różnym przedsięwzięciom (załącznik nr 2).

Poniżej przedstawione zostały wybrane przykłady wydarzeń krajowych lub międzynarodowych z udziałem Prezesa UODO bądź jego przedstawicieli, które odbyły się w Polsce w 2023 r. Ich pełny wykaz zawiera załącznik nr 3.

[354] Dz. U. Nr 169, poz. 1386 ze zm.

1) XVII Dzień Ochrony Danych Osobowych – 28 stycznia 2023 r.

Przypadające co roku **28 stycznia** święto, jakim jest 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 ogólnopolską konferencję naukową „Przyszłość ochrony danych w świetle rozwoju technologii" we współpracy z prezydentem miasta Ełku oraz Uniwersytetem Warmińsko-Mazurskim w Olsztynie – Filia w Ełku. Celem konferencji było spotkanie z ekspertami zajmującymi się prawem ochrony danych osobowych, a także przedstawienie uczestnikom najważniejszych wyzwań w tym obszarze na 2023 rok. Podczas pięciu sesji tematycznych poruszono zagadnienia związane z zapewnieniem skutecznej ochrony danych osobowych w różnych obszarach funkcjonowania człowieka, przede wszystkim w tych, w których obserwujemy coraz większą tendencję do wykorzystywania najnowszych osiągnięć technologii do kształtowania procesów przetwarzania tych danych. Ważnym punktem tej konferencji było wręczenie nagrody im. Michała Serzyckiego, Generalnego Inspektora Ochrony Danych Osobowych III kadencji, przyznawanej w uznaniu zasług na polu edukacji i popularyzacji idei ochrony danych osobowych.

Konferencja odbyła się w formule hybrydowej 31 stycznia 2023 r. w siedzibie Uniwersytetu Warmińsko-Mazurskiego w Olsztynie – Filia w Ełku.

W tym samym dniu, w siedzibie uczelni, odbyły się warsztaty ze studentami pnnt. „Ochrona danych osobowych w kontekście cyberzagrożeń" oraz warsztaty z seniorami na temat ochrony danych osobowych podczas korzystania z nowych technologii. Natomiast w Urzędzie Miasta Ełku eksperci UODO udzielali konsultacji z zakresu ochrony danych osobowych, a przedstawiciel urzędu przeprowadził szkolenie dla kadry zarządzającej jst województwa warmińsko-mazurskiego pt. „Projektowanie ochrony danych osobowych przez jednostki samorządu terytorialnego związku z wyzwaniami technologicznymi".

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. Wśród nich znalazły się też uczelnie wyższe, z którymi UODO ma zawarte porozumienie o współpracy. Wśród zaplanowanych na ten dzień wydarzeń z udziałem ekspertów UODO znalazły się:

- **Warsztaty na Uniwersytecie Jagiellońskim, 10.02.2023 r.**

W ramach obchodów 17. Dnia Ochrony Danych Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego zorganizował w Krakowie warsztaty pod nazwą „Sankcje finansowe w świetle przepisów o ochronie danych osobowych w praktyce". Przedstawiciele UODO wystąpili z prelekcją w dwóch sesjach: „Prawo do informacji publicznej" oraz „Kary i naruszenia RODO w perspektywie dotychczasowych doświadczeń".

- **IX Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej, 15.02.2023 r.**

Akademia Wyższej Szkoły Biznesu w Dąbrowie Górniczej po raz kolejny aktywnie zaangażowała się w obchody Dnia Ochrony Danych Osobowych, przygotowując konferencję tematyczną połączoną z promocją dobrych praktyk w zakresie ochrony danych osobowych. Prezes Urzędu Ochrony Danych Osobowych objął to wydarzenie patronatem honorowym oraz udzielił wsparcia merytorycznego w postaci udziału ekspertów UODO w sesjach tematycznych konferencji.

- **XVII Dzień Ochrony Danych Osobowych w szkołach**

Na coroczne obchody Dnia Ochrony Danych Osobowych składają się m.in. liczne wydarzenia lokalne, podejmowane głównie przez szkoły i placówki doskonalenia nauczycieli uczestniczące w programie edukacyjnym UODO „Twoje dane – Twoja sprawa". W analizowanym 2023 r., w różnych regionach kraju, odbyło się 305 inicjatyw edukacyjnych, m.in.: lekcji, apeli, spotkań, konkursów, happeningów, przedstawień oraz gier edukacyjnych, które były okazją do popularyzowania wiedzy nie tylko wśród uczniów, ale także wśród seniorów, rodziców i nauczycieli. Uczniowie ponadto przygotowali gazetki szkolne dotyczące ochrony danych osobowych i bezpieczeństwa w Internecie.

W ramach obchodów Dnia Ochrony Danych Osobowych Urząd Ochrony Danych Osobowych zorganizował webinarium dla uczniów pt. „DODO Agencja – mitologiczna interwencja", które odbyło się 26 stycznia 2023 r. W zajęciach udział wzięły 73 klasy ze szkół podstawowych i ponadpodstawowych.

2) Konferencja pt. „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów", 31.03.2023 r.

Zwiększenie świadomości i zrozumienia dla znaczenia ochrony danych osobowych we współczesnym, szybko rozwijającym się technologicznie świecie oraz zwrócenie uwagi na konieczność wzmocnienia ochrony osób fizycznych było jednym z celów tej konferencji.

Wydarzenie stało się okazją do szerszej dyskusji na temat wyzwań dla ochrony danych osobowych obywateli w świetle orzecznictwa sądów. Brak spójności przepisów krajowych z RODO omówiono na przykładzie prawa do prywatności w odniesieniu do realizacji prawa dostępu do informacji

publicznej. Przedstawiono także wpływ orzecznictwa sądów administracyjnych w zakresie administracyjnych kar pieniężnych na skuteczność ochrony danych osobowych w Polsce. Decyzje podejmowane przez organ nadzorczy powinny być istotne dla polskiego wymiaru sprawiedliwości, wzmacniając w ten sposób pozycję i rolę jedynego w Polsce niezależnego organu, który jest właściwy w sprawie ochrony danych osobowych. Konsekwencje rozbieżności orzecznictwa sądów z treścią decyzji podejmowanych przez Prezesa UODO są dotkliwe dla obywateli – urząd traci możliwość ochrony osób fizycznych we wskazanym zakresie, co godzi w ich prawa podstawowe.

Konferencja została zorganizowana przez Urząd Ochrony Danych Osobowych we współpracy z Akademią Ekonomiczno-Humanistyczną w Warszawie, pod patronatem: Urzędu Komunikacji Elektronicznej, Urzędu Ochrony Konkurencji i Konsumentów, Krajowego Rejestru Długów i serwisu chronPESEL.pl.

3) Międzynarodowa konferencja naukowa „Aktualne problemy ochrony danych osobowych w Kościele i państwie", Kraków, 11.05.2023 r.

Celem konferencji było zgłębienie wykładni kościelnego Dekretu ogólnego regulującego ochronę danych osobowych w Kościele katolickim w kontekście przepisów RODO. Prelegenci przedstawili wyzwania w zakresie ochrony danych osobowych w działalności Kościoła z perspektywy prawa państwowego, spraw będących w kompetencji władz kościelnych i państwowych (*res mixtae*) oraz prawa kanonicznego. Konferencję rozpoczęło wystąpienie na temat współpracy Prezesa UODO z Kościelnym Inspektorem Ochrony Danych w ramach podpisanego w 2019 r. porozumienia. Natomiast w panelu dotyczącym wyzwań w zakresie ochrony danych osobowych z perspektywy prawa państwowego ekspertka UODO przedstawiła zagadnienia związane z ochroną danych osobowych w Kościele z perspektywy skarg wpływających do Prezesa UODO.

Organizatorem wydarzenia był Wydział Prawa Kanonicznego Uniwersytetu Papieskiego Jana Pawła II w Krakowie we współpracy z Prezesem UODO, Kościelnym Inspektorem Ochrony Danych oraz Fundacją Instytut Ochrony Danych Osobowych w Kościele Katolickim Bona Fama.

4) e-Izba Dialog z Biznesem i Administracją Publiczną, 30.05.2023 r.

Tematem spotkania online zorganizowanego przez Izbę Gospodarki Elektronicznej była prezentacja stanowisk z kampanii „Taki Sam Start" oraz „Polska Cyfrowa. Pakiet Zmian" w kwestii danych osobowych wypływających poza Unię Europejską, głównie do Azji. Zasygnalizowane zostały problemy polskich e-sprzedawców z konkurentami z Azji i wynikające z tego wyzwania dla biznesu oraz administracji publicznej. Ważnym zagadnieniem była kwestia zapewnienia skutecznej ochrony danych osobowych trafiających do e-przedsiębiorców azjatyckich i przeciwdziałania nierównym standardom ochrony danych osobowych zarówno na obszarze EOG, jak i w państwach trzecich – w szczególności w kontekście równości ram prawnych dla konkurencji. Zastępca Prezesa UODO wystąpił w panelu pn. „Styk prawa konsumenckiego z ochroną danych osobowych", w którym przedstawił Wytyczne bawarskiego organu nadzorczego dotyczące przekazywania danych do państw trzecich oraz zasygnalizował konieczność wprowadzenia równych ram prawnych konkurencji z azjatyckimi e-przedsiębiorcami.

5) Forum Nowych Technologii, Warszawa, 20–21.09.2023 r.

Celem konferencji było zgłębienie roli i opisanie wpływu postępu digitalizacji na ochronę danych osobowych. Ponad 40 ekspertów podzieliło się z uczestnikami wiedzą na temat aktualnych wyzwań i przyszłych kierunków rozwoju w zakresie nowych technologii i ochrony prywatności. Specjaliści przedstawili trendy i wyzwania związane ze sztuczną inteligencją, z chmurą obliczeniową czy technologią blockchain i technologią śledzenia – w kontekście zapewnienia bezpieczeństwa informacji w erze cyfrowej. Poruszono także temat etyki i odpowiedzialności w tworzeniu i stosowaniu technologii, gdzie przyszłe strategie i działania na tym polu powinny równoważyć innowacyjność z etycznymi i prawnymi aspektami ochrony prywatności. Organizatorem Forum Nowych Technologii był Urząd Ochrony Danych Osobowych we współpracy ze Stowarzyszeniem Prawa Nowych Technologii i Akademią Ekonomiczno-Humanistyczną w Warszawie.

6) Spotkanie z przedstawicielami szkół wyższych, 15–16.11.2023 r.

Prezes UODO zorganizował spotkanie z przedstawicielami 28 szkół wyższych, z którymi zawarł porozumienia o współpracy. Pierwsze z tych spotkań odbyło się stacjonarnie w siedzibie UODO, drugie zaś – głównie dla uczelni spoza Warszawy – przebiegało w formule online. Podczas spotkań przedstawiona została prezentacja dotycząca działań edukacyjnych Urzędu Ochrony Danych Osobowych oraz prowadzone były rozmowy na temat kierunków dalszej współpracy.

7) Konferencja „Nowe technologie a ochrona danych osobowych", Warszawa, 22.11.2023 r.

Najnowsze trendy i wyzwania stojące przed ochroną danych osobowych w erze cyfrowej oraz stworzenie przestrzeni do dialogu i współpracy między różnymi podmiotami zajmującymi się tymi zagadnieniami były głównymi obszarami tematycznymi konferencji zorganizowanej przez Centralę ZUS w Warszawie. Moderatorami konferencji oraz uczestnikami sesji dyskusyjnych byli przedstawiciele Urzędu Ochrony Danych Osobowych. Konferencja była częścią obchodów jubileuszu 90-lecia Zakładu Ubezpieczeń Społecznych. Patronat honorowy nad tym wydarzeniem objął Prezydent Rzeczypospolitej Polskiej Andrzej Duda.

8) Webinarium nt. „Kodeksów postępowania i akredytacji podmiotów monitorujących", 11.12.2023 r.

Webinarium zostało zorganizowane 11.12.2023 r. – w dniu zatwierdzenia przez Prezesa Urzędu Ochrony Danych Osobowych „Kodeksu postępowania dla sektora

ochrony zdrowia" przygotowanego przez Polską Federację Szpitali[355]. Dokument ten to pierwszy w Europie kodeks obejmujący podmioty publiczne i prywatne z sektora medycznego. Przewiduje odrębne mechanizmy monitorowania przestrzegania jego postanowień dla publicznych placówek medycznych, W trakcie webinarium eksperci przedstawili szczegóły prac nad projektem i zakres stosowania kodeksu. W prezentacji „RODO w sektorze medycznym" omówione zostały warunki ubiegania się o przystąpienie do kodeksu, zaś w prezentacji „Kodeks postępowania dla sektora ochrony zdrowia" – zadania KPMG Advisory sp. z o.o. sp.k., podmiotu monitorującego przestrzeganie tego kodeksu. Spółka ta została wpisana do „Wykazu podmiotów akredytowanych" prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych.

9) Webinarium z cyklu „Certyfikacja w ochronie danych", 12.12.2023 r.

W związku z zatwierdzeniem 8 grudnia 2023 r. przez Prezesa Urzędu Ochrony Danych Osobowych „Dodatkowych wymogów akredytacji podmiotów certyfikujących" i ich opublikowaniem na stronie internetowej UODO – podjęto działania edukacyjne poświęcone tematowi certyfikacji w zakresie ochrony danych osobowych w rozumieniu RODO. Pierwszy z cyklu webinariów pn. „Certyfikacja w ochronie danych" odbył się 12.12.2023 r. W trakcie wydarzenia przedstawiciele UODO: omówili ramy prawne certyfikacji i jej celu, wyjaśnili najważniejsze pojęcia, określili rodzaje mechanizmów certyfikacji oraz kryteria przyznania certyfikatu, znaku jakości i oznaczenia, a także wskazali podmioty uprawnione do udzielania certyfikacji i rodzaje mechanizmów certyfikacji (europejski znak jakości danych oraz krajowe mechanizmy certyfikacji). Przedstawiciele UODO omówili również rolę organów nadzorczych w procesie udzielania certyfikacji i procedurę zatwierdzania kryteriów certyfikacji w oparciu o procedurę RODO.

10) V konferencja z cyklu „RODO w zakładzie pracy", 15.12.2023 r.

Wydział Prawa Pracy i Administracji Uniwersytetu Jagiellońskiego po raz kolejny zorganizował konferencję na temat ochrony danych osobowych w miejscu pracy. Piąta edycja konferencji, która z udziałem przedstawiciela UODO odbyła się 15.12.2023 r., poświęcona została zagadnieniom z obszaru zakładowych źródeł prawa pracy i przetwarzania danych osobowych w postępowaniach, takich jak sprawy antymobbingowe, dyscyplinarne czy procedury związane z aktywnością związków zawodowych i komisji socjalnych.

2. Działalność informacyjna

Działalność informacyjna UODO opiera się na informowaniu społeczeństwa o zadaniach organu nadzorczego, odnoszących się do monitorowania i przestrzegania przepisów ogólnego rozporządzenia o ochronie danych (RODO). Komunikowano o bieżącej działalności organu nadzorczego, nawiązanych z innymi instytucjami współpracach, programach edukacyjnych, spotkaniach. Dużą popularnością cieszyły się

[355] „Kodeks postępowania dla sektora ochrony zdrowia" – przygotowany przez Polską Federację Szpitali i zatwierdzony 11.12.2023 r. przez Prezesa Urzędu Ochrony Danych Osobowych. Jest to drugi z kolei kodeks dla branży medycznej. Pierwszym był kodeks dla małych placówek medycznych, zatwierdzony 4.12.2022 r. przez Prezesa UODO.

komunikaty dotyczące administracyjnych kar pieniężnych. Informowano też o wszelkich aspektach ochrony danych osobowych.

Wzorem lat poprzednich w 2023 r. działania informacyjne obejmowały:

- prowadzenie akcji informacyjno-edukacyjnych poprzez media własne, w tym inicjowanie i redagowanie komunikatów oraz tekstów problemowych czy poradnikowych udostępnianych na stronie internetowej UODO,
- obecność i obsługę profili UODO w mediach społecznościowych (Twitter, aktualnie X),
- współpracę z mediami m.in. poprzez udzielanie odpowiedzi na pytania dziennikarzy mediów tradycyjnych i elektronicznych, aranżowanie wywiadów z przedstawicielami UODO i ich wystąpień medialnych,
- promocję medialną programu edukacyjnego „Twoje dane – Twoja sprawa" i Letniej Akademii Liderów RODO,
- opracowywanie i cykliczną publikację „Newslettera UODO dla IOD", który w marcu zmienił swoją formułę i zaczął ukazywać się jako „Biuletyn UODO".

2.1. Strona internetowa i media społecznościowe

Rok sprawozdawczy 2023 był kolejnym, w którym UODO za pośrednictwem strony internetowej www.uodo.gov.pl komunikował się ze społeczeństwem, stawiając na rozwój tzw. mediów własnych. Publikowane materiały kierowane były do różnych grup społecznych i zawodowych, mając na uwadze szerokie spektrum popularyzacji wiedzy o ochronie danych osobowych. Na stronie WWW zamieszczono **85 komunikatów,** wśród których znalazły się również informacje o konferencjach, webinariach oraz seminariach.

W okresie sprawozdawczym, wraz z rozpoczęciem 2023 r., powstała odsłona strony WWW w nowej szacie graficznej. Zaktualizowano wiele materiałów, dokonano przeglądu treści pod kątem retencji danych osobowych w nich zawartych, co wpłynęło na decyzję o ograniczeniu niektórych zasobów. Strona internetowa organu nadzorczego – dostępna pod adresem: www.uodo.gov.pl – powinna odgrywać znaczącą rolę informacyjną i edukacyjną. Wśród publikowanych na niej treści dużym zainteresowaniem opinii publicznej cieszyły się informacje o nakładanych na administratorów w drodze decyzji administracyjnych karach pieniężnych, a także materiały związane z ewentualnymi późniejszymi postępowaniami przed sądami administracyjnymi i wydawanymi wyrokami.

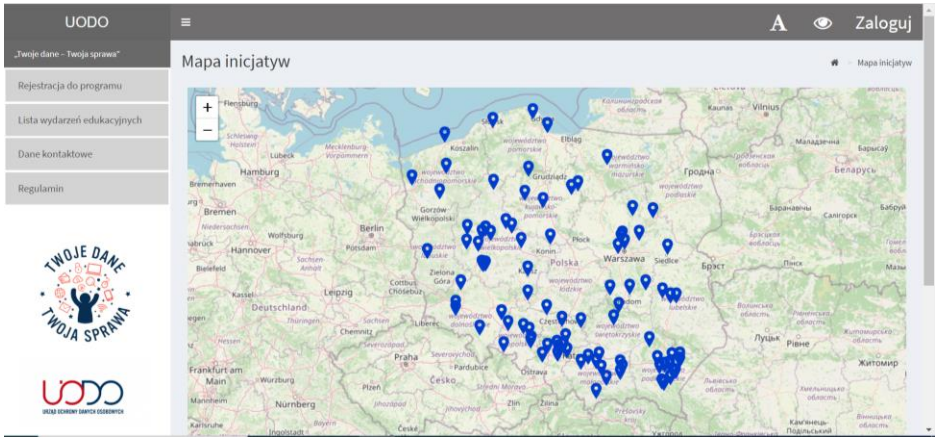
Dużą popularnością cieszyły się również komunikaty o charakterze edukacyjnym, które UODO przygotował i opublikował na swojej stronie internetowej, aby wspierać uczestników systemu ochrony danych.

W 2023 r. UODO podjął kolejne inicjatywy służące podnoszeniu świadomości społeczeństwa na temat bezpieczeństwa danych osobowych. Przykładem takiego działania była m.in. akcja informacyjna z okazji Dnia Bezpiecznego Internetu na temat wpływu nowych technologii na prywatność, do internautów (luty 2023 r.). Urząd Ochrony Danych Osobowych przypomniał osiem dobrych praktyk, opracowanych z tej okazji rok wcześniej, propagując wśród internautów sposoby bezpiecznego zachowania w Internecie.

Inny przykład, o którym była już mowa wcześniej, to wspólna inicjatywa UODO i UKE, webinarium pod hasłem „Na jaką przynętę dasz się złapać?" dla nauczycieli oraz uczniów

klas 7–8 szkół podstawowych oraz szkół ponadpodstawowych. Wydarzenie zorganizowano w ramach programu „Twoje dane – Twoja sprawa”, jednak do udziału w tym webinarium zaproszeni zostali również uczniowie ze szkół, które nie przystąpiły do XIII edycji programu edukacyjnego UODO.

Urząd Ochrony Danych Osobowych stworzył również interaktywną mapę inicjatyw XIII edycji programu „Twoje dane – Twoja sprawa”. Osoby zainteresowane wydarzeniem mogły zapoznać się z krótkimi opisami minionych i aktualnych wydarzeń szkolnych. W materiale przedstawiono zbiór wszystkich zgłoszonych do XIII edycji programu inicjatyw.



OCHRONA DANYCH OSOBOWYCH
W KAMPANII WYBORCZEJ
PORADNIK

Warszawa 2023
www.uodo.gov.pl

Będąc aktywnym członkiem Europejskiej Rady Ochrony Danych (EROD), Urząd Ochrony Danych Osobowych informował o działaniach organów nadzorczych dążących do zharmonizowania przepisów związanych z ochroną danych osobowych, dzięki czemu obywatele Unii Europejskiej zyskali większą świadomość na temat przysługujących im praw. Organ nadzorczy informował na swojej stronie WWW o wytycznych, decyzjach czy opiniach przyjmowanych przez EROD. Oprócz prezentowania podsumowań posiedzeń plenarnych Rady na stronie internetowej na bieżąco publikowane były informacje o ważnych sprawach zarówno dla obywateli, jak i administratorów. W 2023 r. wydano 18 takich komunikatów, co stanowiło 21% wszystkich opublikowanych w tym roku na głównej stronie ogłoszeń.

Sprawą, która w dużej mierze skupiła uwagę opinii publicznej w analizowanym okresie sprawozdawczym, była ogólna dyskusja EROD na temat modelu „pay or ok”. Zdecydowano, że zostanie przygotowany wniosek o udzielenie mandatu na opracowanie wytycznych w tym zakresie.

W kwestii międzynarodowego przekazywania danych EROD podkreśliła znaczenie dalszego opracowywania decyzji stwierdzających odpowiedni stopień ochrony we współpracy z państwami trzecimi i organizacjami międzynarodowymi oraz swoje oczekiwania wobec Komisji Europejskiej dotyczące zakończenia prac nad przeglądem decyzji stwierdzających odpowiedni stopień ochrony przyjętych na mocy dyrektywy 95/46/WE. Ponadto EROD zachęciła Komisję do kontynuowania współpracy międzynarodowej i podkreśliła znaczenie skutecznej współpracy w zakresie egzekwowania prawa z państwami trzecimi.

W 2023 r. strona internetowa organu nadzorczego w dalszym ciągu była poddawana modyfikacji pod względem redagowania prezentowanych na niej treści. Przede wszystkim dopracowano ją pod kątem dostępności cyfrowej, ułatwiając korzystanie ze strony osobom ze szczególnymi potrzebami. Nieodłącznym elementem materiałów filmowych była naniesiona na obraz transkrypcja, co sprawiało, że były one atrakcyjniejsze w odbiorze i bardziej odpowiadające aktualnym potrzebom komunikacyjnym odbiorców. Łącznie UODO przygotował **32 materiały filmowe.** Część z nich zamieszczono na stronie głównej, inne z kolei w sekcji dla administratora. Wiele z nich powstało w ramach programu „Twoje Dane – Twoja Sprawa", pozostałe objęły temat certyfikacji w ochronie danych, kodeksu postępowania dla Polskiej Federacji Szpital, a także konferencji „Forum Nowych Technologii", jak również niezwykle istotnej dla urzędu konferencji „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów". Udostępniono też dwa nagrania w formie wypowiedzi eksperta dla mediów. Publikacje, oprócz informowania o bieżącej działalności urzędu, a także funkcji dydaktycznej, miały na celu wzmacnianie wizerunku UODO.

Istotnym wzmocnieniem działań informacyjnych prowadzonych przez UODO było systematyczne **komunikowanie za pośrednictwem mediów społecznościowych.** Chodzi przede wszystkim o działania informacyjne UODO prowadzone w serwisie **Twitter (obecnie X) – @UODOgov_pl.**

Na platformie opublikowano 495 wpisów, tj. o 41 mniej w porównaniu z rokiem 2022, w którym zamieszczono 536 tweetów. Liczba wyświetleń publikacji w perspektywie całego roku wyniosła 216 200 – wygenerowały one średni miesięczny zasięg na poziomie 18 tys.

Poniższa ilustracja przedstawia oficjalny profil UODO na Twitter (X) – @UODOgov_pl.

Na Twitterze (X) zamieszczano wypowiedzi eksperckie pracowników, a także komunikowano o inicjatywach i wydarzeniach (szkoleniach, debatach, wykładach, webinariach, konferencjach czy seminariach naukowych) organizowanych przez UODO oraz o tych, nad którymi urząd objął patronat honorowy wraz z relacjonowaniem ich na żywo i udostępnianiem zapisów nagrań. Informowano też o podjętych działaniach prawnych. Nie zabrakło także wpisów wzbogaconych o grafiki lub animacje, które uatrakcyjniały prezentowane treści.

Poniżej zaprezentowany został przykładowy post wzbogacony grafiką.

W serwisie Twitter (X) publikowano wskazówki i porady o tematyce edukacyjnej – dotyczące ochrony danych osobowych, przestrzegano przez zagrożeniami bezpieczeństwa danych osobowych, informowano o najnowszych wydaniach „Biuletynu UODO", a także za jego pośrednictwem prowadzono działania promocyjne ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa".

Ilustracja obok przedstawia przykładowy post informujący o najnowszym wydaniu „Biuletynu UODO".

Profil UODO na Twitterze (X) służy jako dodatkowy kanał komunikacji i promocji wydarzeń organizowanych przez UODO. Warto podkreślić, że prowadzenie oficjalnego profilu nie wymaga dodatkowych nakładów finansowych, a osoby zainteresowane danymi treściami mogą je przeglądać o dowolnej porze. Publikowane na nim treści mają charakter głównie informacyjny i merytoryczny, rzadziej wizerunkowy. Zaletą Twittera (X) jest możliwość bezpośredniej komunikacji z obywatelem i budowania zaufania do UODO oraz kierowania krótkich komunikatów zachęcających do zgłębienia tematu na stronie WWW. Za pośrednictwem Twittera (X) 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. Niemal wszystkie treści zamieszczane na oficjalnym profilu na Twitterze (X) odsyłały na stronę www.uodo.pl, która jest podstawowym źródłem informacji o działalności urzędu.

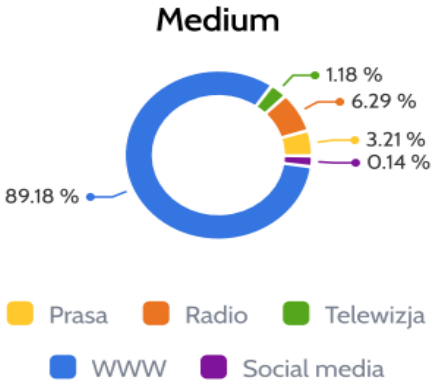
UODO prowadzi również anglojęzyczną stronę internetową – www.uodo.gov.pl/en oraz anglojęzyczny profil na Twitterze (X) – @PDPO_Poland, które są wykorzystywane jako kanały komunikacji w ramach współpracy międzynarodowej, prowadzonej przez UODO. Aktywność kanału na Twitterze (X) – @PDPO_Poland obejmowała informowanie o najważniejszych aktualnościach oraz udostępnianie tweetów zamieszczonych na profilu Europejskiej Rady Ochrony Danych (@EU_EDPB).

2.2. Współpraca z mediami

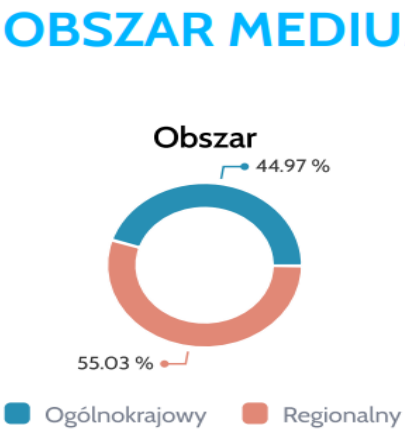
W 2023 r. UODO współpracował z mediami o zasięgu ogólnopolskim, regionalnym oraz lokalnym. Współdziałanie objęło także portale internetowe, w tym serwisy tematyczne. W ramach stałej współpracy z mediami UODO opracował 37 informacji prasowych o tematyce ochrony danych i prywatności. Eksperci UODO udzielili 4 wypowiedzi radiowo-telewizyjnych i 9 wywiadów w prasie. Dotyczyły one tematów związanych z bieżącą działalnością organu nadzorczego oraz były reakcją na zdarzenia wzbudzające zainteresowanie opinii publicznej.

W roku sprawozdawczym 2023 ukazało się w mediach tradycyjnych i na portalach internetowych blisko **18 tys.** informacji, w tym najwięcej odnoszących się do działalności samego UODO (w postaci artykułów, notek lub wzmianek), na co wskazują dane zebrane przez PSSM Monitoring & More. Wskaźnik zasięgu informacji[356] wyniósł 7,4 mld potencjalnych kontaktów, zaś dotarcie informacji wyniosło 241,6 mln realnych kontaktów.

[356] 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,



Wykres 24: Procentowy udział publikacji na temat UODO, które ukazały się w 2023 r., w podziale na media



Wykres 25: Procentowy podział aktywności mediów ogólnopolskich i regionalnych dotyczących UODO

Dominującym środkiem przekazu na temat działalności UODO niezmiennie pozostał Internet, co znalazło odzwierciedlenie w liczbie opublikowanych informacji za pośrednictwem mediów internetowych lub internetowych wydań mediów tradycyjnych. W 2023 r. jednak zauważono wzrost udziału radia i telewizji w procentowym udziale publikacji na temat UODO. Podobnie jak w latach poprzednich zauważalną tendencją pozostało to, że poza prezentowaniem przez dziennikarzy informacji dotyczących

a nie liczbę osób, które mogły się z nią zetknąć. Zasięg wyższy niż liczba mieszkańców Polski oznacza, iż każda osoba mogła spotkać się z daną informacją kilkukrotnie.

[356] 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.

różnorodnych działań związanych z zadaniami i decyzjami Prezesa UODO zwracali się oni do Rzecznika Prasowego UODO z pytaniami odnoszącymi się do bardziej złożonych stanów faktycznych. Co więcej, media relacjonowały wydarzenia z udziałem ekspertów urzędu, a także komunikowały o wielu przedsięwzięciach informacyjno-edukacyjnych podejmowanych przez UODO.

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, z którymi publikowano cykliczne materiały eksperckie.

W 2023 r. uwagę mediów zwróciły m.in. opublikowane na stronie www.uodo.gov.pl teksty problemowe i poradnikowe. W dalszym ciągu szczególnym zainteresowaniem dziennikarzy cieszyły się porady dla inspektorów ochrony danych dostępne na stronie internetowej urzędu oraz artykuły publikowane w „Newsletterze UODO dla Inspektorów Ochrony Danych", przekształconym następnie w „Biuletyn UODO".

Wiele pytań zadawanych przez dziennikarzy odnosiło się do wyroku Naczelnego Sądu Administracyjnego ws. decyzji dotyczącej spółki Morele.net. Efektem tej sprawy była zorganizowana przez urząd konferencja pn. „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów" i powstałe wokół niej komunikaty. Dużą uwagą dziennikarzy, również zagranicznych, cieszył się wątek bota ChatGPT – przetwarzania danych przez OpenAI oraz pierwszej złożonej do UODO skargi w tym zakresie. Dziennikarze byli również zainteresowani tematem ujawnienia danych lekarza przez ówczesnego Ministra Zdrowia[357].

Na skrzynkę rzecznika prasowego przyszło też dużo pytań dotyczących ujawnienia opinii publicznej danych osób, w konsekwencji czego popełniły one samobójstwo[358]. Jedna z tych spraw dotyczyła ujawnienia w mediach społecznościowych danych osoby w kontekście stwierdzenia o rzekomym popełnieniu przez nią czynu o charakterze pedofilskim. Zakres ujawnionych danych obejmował informacje o fakcie pełnienia przez tę osobę posługi kapłańskiej, nazwę zgromadzenia oraz wizerunek. Druga sprawa dotyczyła osoby niepełnoletniej, której dane osobowe zamieszczone w doniesieniach prasowych, dotyczących skazania w 2021 r. byłego pracownika urzędu marszałkowskiego za czyny pedofilskie, pozwalały na pełną identyfikację skrzywdzonego dziecka.

W obu przedstawionych sprawach ówczesny Prezes UODO odmówił ich rozpatrzenia, uznając, że nie ma podstaw prawnych do wszczęcia postępowania. Obecny Prezes Urzędu Ochrony Danych Osobowych podjął czynności mające na celu wyjaśnienie okoliczności upublicznienia danych osobowych tych osób. Postępowania w tych sprawach są w toku i będą przedstawione w sprawozdaniu z działalności organu w 2024 r.[359]

Ciekawy dla mediów był też motyw wycieku danych w laboratorium analitycznym. Atak typu ransomware połączony z wyciekiem danych z firmy świadczącej usługi laboratoryjne poważnie zaniepokoił opinię publiczną, zarówno z uwagi na skalę wycieku,

[357] DKN.5131.32.2023, DKN.5130.9596.2023. Więcej na ten temat zob. w rozdziale „Administracyjne kary pieniężne w związku z naruszeniem" niniejszego sprawozdania.
[358] DOL.023.173.2023, DOL.051.6.2023.
[359] DKN.5101.37.2024.IŁ, DKN.5101.38.2024.IŁ.

jak i potencjalny zakres danych, który obejmował dane o zdrowiu wielu pacjentów. Dlatego Prezes UODO i Rzecznik Praw Pacjenta w ramach porozumienia między organami podjęli wspólne działania w związku z tym wydarzeniem. Połączone wysiłki tych instytucji mogą też przełożyć się na opracowanie w przyszłości rekomendacji, które pozwolą ograniczać ryzyka związane z tak poważnymi naruszeniami ochrony danych oraz niwelować ich negatywne skutki. Chodzi zarówno o złamanie prawa w związku z naruszeniem ochrony danych osobowych, jak i podważenie zaufania pacjentów do podmiotów leczniczych oraz systemu ochrony zdrowia. Prezes UODO zalecał, by pacjenci – przed podjęciem jakichkolwiek działań w związku z zaistniałym naruszeniem ochrony danych – skorzystali z narzędzia udostępnionego przez Ministra Cyfryzacji i zweryfikowali w serwisie bezpiecznedane.gov.pl, czy ich dane są objęte wyciekiem.

Wiele pytań dziennikarzy dotyczyło również takich zagadnień, jak: naruszenia ochrony danych osobowych, ochrona wizerunku, monitoring wizyjny.

Warto podkreślić, że dziennikarze mediów ogólnopolskich, regionalnych i lokalnych byli bardzo zainteresowani wątkami wycieków danych. W wielu takich sprawach zwracali się do UODO w celu potwierdzenia zdarzeń. Równie chętnie korzystali z opracowań UODO, udzielając na ich podstawie wskazówek, jak przeciwdziałać negatywnym skutkom utraty kontroli nad danymi osobowymi.

Współpraca z mediami zaowocowała także patronatami medialnymi nad np. XVII Dniem Ochrony Danych Osobowych oraz XIII edycją programu edukacyjnego „Twoje dane – Twoja sprawa”.

2.3. Odpowiedzi na indywidualne pytania dziennikarzy

W 2023 r. Rzecznik Prasowy UODO udzielił odpowiedzi na **421 pytań zadanych przez dziennikarzy**. Pytania dziennikarzy charakteryzują się coraz większą szczegółowością. Do rzadkości należą przypadki, gdy dziennikarza interesują podstawowe i ogólne kwestie związane z przepisami RODO, jak na przykład: czym są dane osobowe; jakie prawa mają osoby, których dane dotyczą; jakie obowiązki mają administratorzy danych.

Odpowiedzi na pytania mediów często wymagały odwołania się nie tylko do przepisów o ochronie danych osobowych, ale i przepisów szczególnych, pism, czy też zaprezentowania ustaleń z innymi przedstawicielami, np. EROD. Takie sytuacje miały miejsce głównie w przypadku zagadnień dotyczących: pracodawców, przechowywania przez nich danych osobowych, zasad ich zabezpieczania – głównie w zakresie, jakie zabezpieczenia techniczne mają stosować administratorzy w celu skutecznej ochrony danych i analizy ryzyka z tym związanej, czy działalności tzw. gigantów technologicznych i oferowanych przez nich usług.

Do najczęściej zadawanych pytań przez dziennikarzy można zaliczyć te związane z naruszeniami ochrony danych osobowych. Stanowiły one ponad jedną trzecią wszystkich pytań, a związane były z aktualnymi wyciekami danych, o których nierzadko informowali sami administratorzy, realizując ciążące na nich obowiązki związane z powiadamianiem osób, których dotyczyły takie incydenty. Wówczas media najbardziej interesowała kwestia otrzymania przez organ nadzorczy takiego zawiadomienia o naruszeniu, konsekwencji

grożących administratorowi danych i tego, co mogą zrobić osoby, których dane np. zostały ujawnione.

Zauważalna jest jednak różnica w podejściu do tematu naruszeń ochrony danych osobowych wśród mediów ogólnopolskich i regionalnych. Te pierwsze zazwyczaj interesowały się naruszeniami, które miały miejsce w dużych podmiotach. Natomiast wiele pytań od przedstawicieli mediów regionalnych dotyczyło przede wszystkim incydentów, które miały miejsce w ich województwie czy mieście. Tak było nawet w przypadkach, gdy naruszenie dotyczyło jednej bądź kilku osób. Wtedy dziennikarze częściej pytali o podjęte w danej sprawie działania UODO i możliwe decyzje organu nadzorczego.

Kolejnym tematem, który w roku sprawozdawczym cieszył się dużym zainteresowaniem dziennikarzy, był monitoring: w sieci aptek, w szpitalach, przypadek upublicznienia nagrania z wypadku samochodowego, jak również powracające tematy monitoringu sąsiedzkiego i obiektów w obawie przed agresywnym zachowaniem.

W minionym roku 2023 dziennikarze interesowali się także orzecznictwem sądów administracyjnych, związanym z decyzjami Prezesa UODO. Media zazwyczaj ciekawił komentarz UODO do zapadających wyroków, jak i ewentualne dalsze działania organu nadzorczego w przypadku orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie.

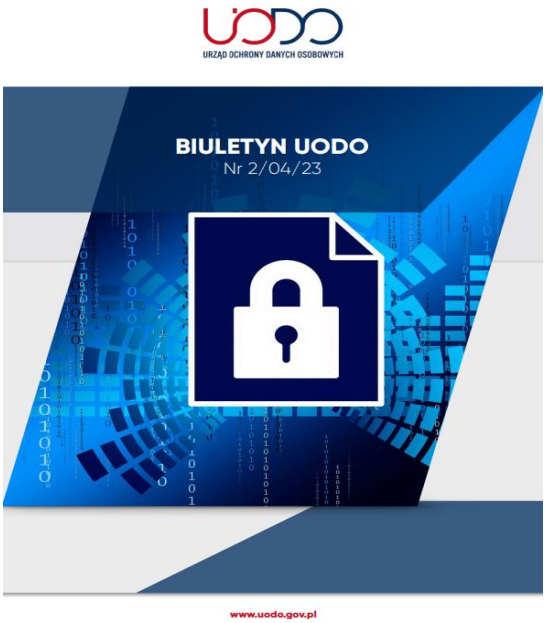
Wśród innych ciekawych dla reprezentantów środków masowego przekazu tematów w roku sprawozdawczym znalazły się m.in.:

- zagadnienia związane z telemarketingiem i pozyskiwaniem danych przez firmy świadczące usługi w tej dziedzinie;
- statystyki związane ze skargami, naruszeniami oraz karami.

2.4. „Newsletter UODO dla IOD" / „Biuletyn UODO"

W 2023 r. kontynuowano wydawanie cyklicznego **„Newslettera UODO dla Inspektorów Ochrony Danych**", który w marcu 2023 r. przekształcono w **„Biuletyn UODO".** W roku sprawozdawczym ukazały się 2 wydania **„Newslettera UODO dla Inspektorów Ochrony Danych"** oraz 9 wydań **„Biuletynu UODO"** (podwójny numer wakacyjny). O jego popularności świadczy stale rosnąca liczba subskrybentów. Na koniec grudnia 2023 r. newsletter trafił do **10 377** subskrybentów (grudzień 2022 r. – **9 257** subskrybentów).

Ilustracje poniżej przedstawiają nagłówki tytułowe „Newslettera UODO dla Inspektorów Ochrony Danych" oraz „Biuletynu UODO".



„Newsletter UODO dla Inspektorów Ochrony Danych”/„Biuletyn UODO” to źródło informacji o działalności urzędu. Początkowo powstał z myślą o bieżącym informowaniu głównie inspektorów ochrony danych, jednak prezentowane w nim materiały miały na tyle ogólny charakter, że okazały się być pomocne w zrozumieniu tematyki ochrony danych osobowych również dla osób spoza tego kręgu. Dużą część subskrybentów stanowią osoby zainteresowane ochroną danych osobowych i prawem do prywatności, w tym dziennikarze oraz przedstawiciele podmiotów prawnych. Publikowane treści wpisują się w działalność informacyjno-edukacyjną UODO. Przekazywane materiały zawierały ogólne wskazówki o stosowaniu przepisów RODO czy wnioski płynące z decyzji administracyjnych. Wraz z przekształceniem newslettera w biuletyn został on znacząco wzbogacony o nowe treści. Powstał dział „Wprowadzenie” ze słowem wprowadzającym od zastępcy prezesa (gościnnie od Prezesa UODO), jak również od rzecznika prasowego, który przybliżał na wstępie, jakie treści znajdą się w numerze. Pojawiło się więcej materiałów o charakterze problemowym i poradnikowym. Publikowane artykuły były odpowiedzią na najczęściej pojawiające się pytania i sygnały, jakie różnymi kanałami urząd otrzymywał od odbiorców. Biuletyn podzielono na stałe sekcje: wprowadzenie, rozmowa z ekspertem, UODO sygnalizuje, wybrane decyzje UODO, naruszenia i kontrole, nowe technologie, sprawy międzynarodowe oraz dwie sekcje ruchome: edukacja oraz partnerzy UODO (w kwietniu zmieniono nazwę na Współpraca z UODO). Zmodyfikowano również szatę graficzną biuletynu zgodnie z aktualnymi trendami.

Biuletyn pozwolił organowi nadzorczemu nie tylko budowanie relacji ze wszystkimi osobami, którym bliska jest tematyka ochrony danych osobowych, ale także na utrzymanie z nimi stałej, comiesięcznej komunikacji.

2.5. Infolinia UODO

Każdego dnia pracownicy infolinii UODO odbierają kilkadziesiąt telefonów od osób zainteresowanych tematyką dotyczącą ochrony danych osobowych. Z pytaniami zwracały

się zarówno osoby fizyczne, jak i podmioty prawne. Pracownicy infolinii upowszechniali wiedzę o ochronie danych osobowych oraz skutecznie informowali obywateli na temat przysługujących im praw i działalności UODO. W szczególności przekazywali informacje o procedurze składania skarg i wniosków, prawidłowym wypełnianiu oraz przesyłaniu formularzy zgłoszeń naruszeń czy 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.

Tematyka przeprowadzonych rozmów w roku sprawozdawczym była bardzo różnorodna. Najczęściej zadawane pytania dotyczyły (oprócz pytań o stan sprawy toczącej się w urzędzie) następujących zagadnień:

- monitoring wizyjny (sąsiedzki, prywatny, wspólnot mieszkaniowych, w placówkach edukacyjnych, w miejscach pracy, w aptekach, w szpitalach, na parkingach);
- przetwarzanie danych osobowych przez spółdzielnie i wspólnoty mieszkaniowe;
- przetwarzanie danych osobowych przez pracodawców (m.in. przechowywanie CV pracownika, dane dotyczące zdrowia, narkotesty i badanie trzeźwości pracownika a RODO, wniosek o pracę zdalną a dane niepełnosprawnego członka rodziny, kontrola pracownika);
- naruszenie w oświacie (nagrywanie ucznia przez nauczyciela, robienie mu zdjęć, ujawnianie danych wrażliwych o dziecku);
- prawidłowe postępowanie w przypadku naruszeń;
- niechciany telemarketing (szczególnie Asmanta);
- żądanie przez internetowe platformy sprzedażowe przesyłania skanów dokumentów tożsamości w celu odblokowania środków otrzymanych ze sprzedaży na kontach użytkowników (m.in. Allegro, Vinted, Olx);
- procedury weryfikacyjne wykorzystywane przez linie lotnicze;

Odnotowano również liczne zapytania dotyczące podszywania się pod UODO.

Techniczne uwarunkowania infolinii nie pozwalają na przedstawienie dokładnej liczby odebranych połączeń. Niemniej łącznie pracownicy infolinii przeprowadzili w 2023 r. **ponad 14,3 tys. rozmów, co stanowi ok. 57 rozmów przeprowadzanych w każdy dzień roboczy.**

Pytania zadawane za pośrednictwem infolinii odnoszą się coraz częściej do bardzo złożonych problemów. Trzeba mieć też na uwadze, że na jedno połączenie często składało się kilka pytań, dotyczących różnych i skomplikowanych prawnie zagadnień.

2.6. Inne

W 2023 r. odbyło się online **11 Spotkań Sieci Rzeczników (Communications Network Meetings),** podczas których omawiane były przede wszystkim bieżące komunikaty publikowane na stronie EROD, projekty koordynowane przez Radę, a także kwestie związane z działaniami prasowymi poszczególnych organów krajowych. Omawiano ponadto sposoby wzmocnienia i usprawnienia współpracy w realizacji zadań komunikacyjnych w sprawach transgranicznych (tzw. one-stop-shop mechanism).

W roku 2023 w ramach Spotkań Sieci Rzeczników podjęto m.in. przygotowanie wkładu do rocznego raportu EROD, w którym znalazł się przegląd najważniejszych decyzji karowych wydanych przez organy nadzorcze, w tym Prezesa UODO. W ramach

wewnętrznego forum stworzonego dla uczestników spotkań organy nadzorcze wymieniały się również informacjami na potrzeby podejmowanych wewnętrznie inicjatyw. Przykładowo, polski organ nadzorczy udzielił odpowiedzi belgijskiemu organowi nadzorczemu na pytanie o wykorzystywanie mediów społecznościowych w swoich działaniach komunikacyjnych oraz czy znajdują się wśród nich komunikatory przeznaczone młodszej grupie odbiorców typu TikTok i Snapchat.

W 2023 r. kontynuowano zainicjowany w roku poprzednim projekt ściślejszej wymiany informacji w sprawach o transgranicznym charakterze. Tego rodzaju informacje mogły być przekazywane w trakcie stałego punktu obrad spotkań Sieci Rzeczników (Communications Network) lub w ramach sieci mailingowej, w której poszczególne organy krajowe przesyłały publikowane na swoich stronach internetowych komunikaty. Posługując się tymi kanałami komunikacji, organy krajowe wymieniały się również informacjami o wpływających do nich pytaniach od dziennikarzy, które mogły budzić zainteresowanie lub angażować pozostałe kraje członkowskie.

W roku 2023 zrealizowano także liczne działania informacyjne, które UODO zainicjował i przeprowadził we współpracy z innymi podmiotami.

Przykładem takiego działania było badanie opinii publicznej pt. **„Dane osobowe – czy wiemy, jak je chronić?”.** Badanie to miało charakter ogólnopolski. Umożliwiło ono rozeznanie się, czy Polacy mają świadomość nowych zagrożeń oraz jakie rozwiązania przyjmują, aby im przeciwdziałać oraz zminimalizować skutki zdarzeń niepożądanych. Wyniki badania pozwoliły ocenić, jak dotychczasowe stosowanie ogólnego rozporządzenia o ochronie danych wpłynęło na zmianę świadomości Polaków odnośnie do dbania o dane osobowe.

Badanie to ma charakter cykliczny – prowadzone jest od 2021 r. we współpracy serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych oraz Instytutu Prawa Ochrony Danych Osobowych. Ankietę przeprowadzono w maju 2023 r. metodą CAWI na reprezentatywnej grupie 1007 respondentów przez IMAS International. W rezultacie tej współpracy powstał raport poświęcony kluczowym wnioskom wynikającym z tego badania. Za każdym razem ankieta uzupełniana jest o nowe pytania, co pozwala diagnozować kolejne zjawiska. Tym razem było to pytanie: **Co zdaniem Polaków zalicza się do zbioru „danych osobowych”?**

Dane osobowe – czy wiemy, jak je chronić? to temat przewodni pierwszej części raportu, który opublikowano w maju 2023 r.[360] Wynika z niego, że blisko 89 % ankietowanych wie, jak zadbać o bezpieczeństwo swoich danych osobowych. 1/3 Polaków potwierdziła, że spotkała się w ciągu ostatniego roku z próbą wyłudzenia ich danych osobowych poprzez fałszywy telefon, link bądź e-mail. 12 % padło ofiarą takiego oszustwa, a drugie tyle nie potrafiło stwierdzić, czy taki fakt miał miejsce. 13,2 % doświadczyło wycieku danych z firm prywatnych i instytucji publicznych, a 22% respondentów nie miało pewności co do tego, czy ich dane nie trafiły stamtąd w ręce przestępców.

86 % Polaków zadeklarowało, że potrafi rozpoznać fałszywy e-mail, sms lub telefon, za pośrednictwem którego przestępcy podszywają się pod znaną firmę lub instytucję, przy czym absolutną tego pewność miał tylko co piąty ankietowany. Znacznie gorzej wypadli badani, odpowiadając na pytanie o reakcję na kradzież danych osobowych. Wiedzę o działaniach, jakie należy podjąć w takiej sytuacji, miało niespełna 56 % respondentów. Co więcej, tylko 45 % badanych wiedziało, jak się zachować w przypadku wycieku danych z aplikacji lub serwisu, na których mieli założone konto.

Odnosząc się do wyników badań ujętych w raporcie, UODO zorganizował webinarium, podczas którego w gronie ekspertów skomentowano zaprezentowane w raporcie wyniki. Podczas debaty z udziałem ekspertów z zakresu ochrony danych osobowych prelegenci omówili również proces budowania świadomości Polaków na temat danych osobowych i wskazali, co wpływa na kształtowanie odpowiednich postaw społeczeństwa. Skomentowali także, jak dotychczasowe stosowanie RODO wpłynęło na zachowania obywateli w zakresie dbania o bezpieczeństwo danych osobowych. Podczas dyskusji przedstawiono wskazówki odnoszące się do działań, jakie należy podjąć w przypadku naruszenia ochrony danych.

W 2023 r. na większą skalę wykorzystywano także **webinaria,** które stały się efektywną formą przekazu w komunikacji, w szczególności z ekspertami oraz młodzieżą. Uwagę mediów przyciągnęły także wydarzenia specjalne, takie jak webinaria tematyczne organizowane przez UODO, zwłaszcza zrealizowane na potrzeby programu edukacyjnego „Twoje dane – Twoja sprawa", m.in. „Na jaką przynętę dasz się złapać?" (webinarium UODO i UKE) czy „Dzień Dziecka z UODO, czyli z Rodusiem chronimy dane osobowe".

Pod koniec 2023 r. urząd – w związku z zatwierdzeniem przez Prezesa UODO „Dodatkowych wymogów akredytacji podmiotów certyfikujących" – zapoczątkował cykl webinariów z serii „Certyfikacja w ochronie danych". W bieżącym roku sprawozdawczym odbyło się pierwsze webinarium z tej serii. Na podstawie tego dokumentu dokonywana jest

[360] Badanie jest kontynuacją poprzedniego bdania zrealizowanego w 2021 r.

akredytacja podmiotów certyfikujących, które weryfikują zgodność operacji przetwarzania danych osobowych prowadzonych przez administratorów i podmioty przetwarzające. Celem certyfikacji jest zwiększenie przejrzystości i poprawa przestrzegania norm ochrony danych osobowych z uwzględnieniem specyfiki branży. Podmioty certyfikujące będą przyznawały certyfikaty ubiegającym się o to firmom z konkretnych sektorów. Posiadanie certyfikatu będzie dobrowolne, a jego zadaniem ma być potwierdzenie najwyższych standardów przestrzegania przepisów o ochronie danych osobowych.

Istotne z edukacyjnego punktu widzenia było również webinarium poświęcone kodeksom postępowania. Prezes UODO zatwierdził „Kodeks postępowania dla sektora ochrony zdrowia" przygotowany przez Polską Federację Szpitali. Podpisany dokument to pierwszy w Europie kodeks obejmujący podmioty publiczne i prywatne z sektora medycznego. Głównym tematem spotkania było przedstawienie stanu prac organu nadzorczego nad kodeksami postępowania w Polsce, o których mowa w art. 40 RODO. Podczas wydarzenia eksperci wskazywali na korzyści przystąpienia do kodeksów postępowania oraz omówili aspekt monitorowania przestrzegania kodeksów postępowania. Spotkania zakończono sesją pytań i odpowiedzi. W 2023 r. UODO zorganizował także kilka innych webinariów, których grafiki przedstawione są powyżej.

IV. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się zagadnieniami 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 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 RODO, ustanowionej przepisami RODO, do której należy Prezes UODO.

Zgodnie z art. 25 regulaminu wewnętrznego EROD działa ona poprzez wewnętrzne podgrupy ekspertów, w skład których wchodzą przedstawiciele organów nadzorczych, EIOD i Komisji Europejskiej. Podgrupy ekspertów wspierają EROD w wykonywaniu jej zadań i dążą do osiągnięcia porozumienia w sprawie każdego przedłożonego wniosku. Pracownicy UODO czynnie reprezentują polski organ nadzorczy, uczestnicząc w pracach wszystkich podgrup eksperckich i grup zadaniowych EROD. W ramach prac podgrup i grup zadaniowych 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. **W 2023 r. EROD zorganizowała ponad 360 spotkań podgrup i grup zadaniowych, podczas których jej członkowie opracowywali stanowiska oraz dokumenty EROD, mające na celu spójne stosowanie przepisów o ochronie danych osobowych.**

Opracowane stanowiska oraz projekty dokumentów są następnie przedmiotem dyskusji i zostają przyjmowane na comiesięcznych posiedzeniach plenarnych EROD. W 2023 r. EROD zorganizowała **15 posiedzeń plenarnych, z czego 5 odbyło się w formie zdalnej, a 1 w formie hybrydowej.** Przedstawiciele UODO wzięli udział we wszystkich posiedzeniach plenarnych EROD. Porządki obrad i komunikaty z sesji plenarnych są publikowane na stronie internetowej UODO.

Zgodnie z ustalonym planem oraz w wyniku potrzeby działania *ad hoc* w 2023 r. EROD przyjęła m.in. niżej wymienione dokumenty.

1.1. Wytyczne i zalecenia

Jedną z podstawowych kompetencji EROD jest wyjaśnianie przepisów RODO poprzez wydawanie wytycznych. W początkowej fazie wdrażania RODO EROD utworzyła dobrze zdefiniowane i kompleksowe repozytorium wytycznych i zaleceń, co gwarantowało, że organy nadzorcze będą konsekwentnie stosować przepisy dotyczące ochrony danych, co z kolei przyczynia się też do zwiększenia przestrzegania przepisów przez zainteresowane strony. Europejska Rada Ochrony Danych w dalszym ciągu opracowuje i rozszerza swoje wytyczne oraz konsekwentnie stara się uwzględnić uwagi zainteresowanych stron, które zbierane są w drodze konsultacji społecznych.

W 2023 r. EROD przyjęła dwa nowe zestawy wytycznych, a także dziewięć zestawów wytycznych wynikających z konsultacji publicznych.

Wytyczne:

1. Wytyczne 03/2022 w sprawie zwodniczych wzorców projektowych w interfejsach platform mediów społecznościowych: jak je rozpoznać i ich unikać;
2. Wytyczne 05/2021 w sprawie wzajemnych zależności między stosowaniem art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V RODO;
3. Wytyczne 7/2022 w sprawie certyfikacji jako narzędzia do przekazywania danych;
4. Wytyczne 9/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO;
5. Wytyczne 01/2022 w sprawie praw osób, których dane dotyczą – Prawo dostępu;
6. Wytyczne 8/2022 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego;
7. Wytyczne 05/2022 w sprawie wykorzystania technologii rozpoznawania twarzy w obszarze egzekwowania prawa;
8. Wytyczne 03/2021 w sprawie stosowania art. 65 ust. 1 lit. a) RODO;
9. Wytyczne 04/2022 w sprawie obliczania administracyjnych kar pieniężnych na mocy RODO;
10. Wytyczne 01/2023 dotyczące art. 37 dyrektywy w sprawie egzekwowania prawa;
11. Wytyczne 2/2023 w sprawie zakresu technicznego art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

Zalecenia:

1. Zalecenia 1/2022 w sprawie wniosku o zatwierdzenie oraz dotyczące elementów i zasad, które powinny znaleźć się w Wiążących Regułach Korporacyjnych Administratora (art. 47 RODO).

1.2. Konsultacje prawodawcze i dokumenty skierowane do instytucji UE lub organów krajowych

1) Wspólna opinia EROD–EIOD 01/2023 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679;
2) Wspólna opinia EROD-EIOD nr 02/2023 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia cyfrowego euro;
3) Wspólny wkład EROD i EIOD w konsultacje publiczne dotyczące projektu szablonu odnoszącego się do opisu technik profilowania konsumentów (art. 15 DMA);
4) Opinia 5/2023 w sprawie projektu decyzji wykonawczej Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA.

1.3. Inne wskazówki i oświadczenia

1) Przewodnik po ochronie danych dla małych firm;
2) Skoordynowane działania w zakresie egzekwowania prawa, korzystanie z usług w chmurze przez sektor publiczny;
3) Nota informacyjna z 10 lipca 2023 r. dotycząca przekazywania danych na podstawie RODO do Stanów Zjednoczonych po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony;
4) Oświadczenie 1/2023 w sprawie pierwszego przeglądu decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Japonii;
5) Dokument EROD dotyczący procedury przyjmowania opinii EROD w sprawie krajowych kryteriów certyfikacji i europejskiego znaku jakości ochrony danych;
6) Sprawozdanie z prac podjętych przez grupę zadaniową ds. banerów cookie;
7) Sprawozdanie z prac podjętych przez organy nadzorcze w ramach grupy zadaniowej ds. 101 skarg;
8) Wzór formularza skargi, ułatwiającego składanie skarg przez osoby fizyczne i ich późniejsze rozpatrywanie przez organy nadzorcze w sprawach transgranicznych.

1.4. Opinie dotyczące spójności

EROD wydaje opinie dotyczące spójności, aby przyczynić się do spójnego stosowania RODO. Organy nadzorcze mogą zwracać się do EROD o opinie dotyczące spójności na mocy art. 64(1) RODO, gdy zamierzają przyjąć określone rodzaje środków. Po wydaniu opinii w sprawie spójności organy nadzorcze przyjmują swoje decyzje krajowe.

W 2023 r. EROD przyjęła następujące opinie dotyczące spójności (art. 64 ust. 1 RODO):

1) Opinie w sprawie projektów decyzji dotyczących wiążących reguł korporacyjnych

Organy nadzorcze mogą zatwierdzać wiążące reguły korporacyjne w rozumieniu art. 47 RODO. Są to polityki ochrony danych wdrożone i przestrzegane w ramach grupy przedsiębiorstw mających siedzibę w EOG – w odniesieniu do przekazywania danych osobowych poza EOG w ramach tej samej grupy. W 2023 r. kilka organów nadzorczych przedłożyło EROD swoje projekty decyzji dotyczących wiążących reguł korporacyjnych administratora lub podmiotu przetwarzającego różnych przedsiębiorstw, zwracając się o wydanie opinii na podstawie art. 64 ust. 1 lit. f). W 2023 r. EROD wydała 27 opinii w sprawie wiążących reguł korporacyjnych.

2) Opinie w sprawie projektu wymogów dotyczących akredytacji podmiotów certyfikujących

Pięć organów nadzorczych przedłożyło swoje projekty decyzji w sprawie wymogów akredytacji dla jednostek certyfikujących na podstawie art. 43 ust. 1 lit. b) RODO do EROD z wnioskiem o wydanie opinii na podstawie art. 64 ust. 1 lit. c) RODO. Wymogi te umożliwiają akredytację jednostek certyfikujących odpowiedzialnych za wydawanie i odnawianie certyfikacji zgodnie z art. 42 RODO. Opinie te mają na celu ustanowienie spójnego i zharmonizowanego podejścia w odniesieniu do wymogów, które organy nadzorcze oraz krajowe jednostki akredytujące stosują podczas akredytacji jednostek certyfikujących na mocy RODO. W tym celu EROD przedstawiła odpowiednim organom zalecenia dotyczące zmian, które należy wprowadzić do projektów opinii. Następnie organy nadzorcze zmieniły swoje projekty zgodnie z art. 64 ust. 7 RODO, uwzględniając w możliwie najszerszym zakresie opinie EROD.

3) Opinie w sprawie kryteriów certyfikacji

Jeżeli organ nadzorczy zamierza zatwierdzić certyfikację zgodnie z art. 42 ust. 5 RODO, rolą EROD jest zapewnienie spójnego stosowania RODO poprzez mechanizm spójności, o którym mowa w art. 63, 64 i 65 RODO. W tych ramach, zgodnie z art. 64 ust. 1 lit. c) RODO, EROD jest zobowiązana do wydania opinii na temat projektu decyzji organu nadzorczego zatwierdzającej kryteria certyfikacji. W 2023 r. EROD wydała jedną opinię w sprawie kryteriów certyfikacji, mającą na celu zapewnienie spójnego stosowania RODO, w tym przez organy nadzorcze, administratorów i podmioty przetwarzające.

4) Opinie w sprawie zatwierdzenia przez organy nadzorcze wymogów akredytacji dla podmiotów monitorujących kodeksy postępowania

Celem opinii w sprawie zatwierdzenia przez organy nadzorcze wymogów akredytacji dla podmiotów monitorujących kodeksy postępowania było zapewnienie spójności i prawidłowego stosowania wymogów wśród organów nadzorczych.

W tym celu EROD przedstawiła organom szereg zaleceń dotyczących zmian, jakie należy wprowadzić do projektu wymogów akredytacji. Na tej podstawie organy nadzorcze zmieniły swoje projekty zgodnie z art. 64 ust. 7 RODO, uwzględniając w jak największym stopniu opinie EROD.

W 2023 r. EROD wydała 5 opinii w sprawie projektów wymogów akredytacji dla podmiotów monitorujących kodeksy postępowania, o które zwróciły się organy nadzorcze, zgodnie z art. 64 ust. 1 lit. c) RODO.

Od 2018 r. EROD przyjęła łącznie 182 opinie dotyczące spójności. W ten sposób, wychodząc od teoretycznego opisu nowych narzędzi zgodności wprowadzonych w RODO, EROD stworzyła ramy dla nowych narzędzi zgodności, takich jak kodeksy postępowania i mechanizmy certyfikacji, aby mogły one funkcjonować w spójny sposób.

EROD poczyniła znaczące postępy w obszarze certyfikacji jako narzędzia zgodności (art. 42 RODO) oraz jako narzędzia przekazywania danych – art. 46 ust. 2 lit. f) RODO. Oprócz ostatecznej wersji Wytycznych 07/2022 dotyczących certyfikacji jako narzędzia do przekazywania danych oraz Dokumentu EROD w sprawie procedury zatwierdzania przez EROD kryteriów certyfikacji skutkującego wspólną certyfikacją, europejskim znakiem jakości ochrony danych, które zostały przyjęte na początku 2023 r., członkowie EROD przeprowadzili również dwa warsztaty certyfikacyjne wiosną i jesienią 2023 r.

Warsztaty odbyły się odpowiednio w Hiszpanii i Luksemburgu, a ich celem było znalezienie synergii, wzmocnienie współpracy między członkami EROD oraz zajęcie się głównymi wyzwaniami i możliwościami, jakie niosą ze sobą te narzędzia. Podczas pierwszego dnia jesiennych warsztatów interesariusze certyfikacji mieli okazję przekazać informacje zwrotne i podzielić się swoimi doświadczeniami.

Europejska Rada Ochrony Danych kontynuuje prace nad tematem certyfikacji, w tym certyfikacji jako narzędzia przekazywania, co potwierdza jej zobowiązanie, odzwierciedlone w strategii na lata 2021–2023, do przyspieszenia harmonizacji i ułatwienia wdrażania mechanizmów zgodności.

1.5. Wiążące decyzje

Egzekwowanie przepisów RODO i nakładanie kar należy do kompetencji organów nadzorczych. Ma to miejsce na szczeblu krajowym oraz w sprawach transgranicznych, w przypadku których organy nadzorcze współpracują ze sobą za pośrednictwem mechanizmu kompleksowej współpracy (*one-stop-shop*, OSS).

W przypadkach, w których organy nadzorcze nie są w stanie osiągnąć konsensusu, EROD przyjmuje decyzję zgodnie z art. 65 RODO. Jest ona wiążąca dla wiodącego organu nadzorczego. Tym samym decyzja ta zmusza wiodący organ nadzorczy do odpowiedniego dostosowania swojej decyzji. Około 1 % decyzji OSS przechodzi przez mechanizm rozstrzygania sporów. Decyzje te często dotyczą dużych podmiotów i przetwarzania danych wszystkich osób fizycznych w Europie. Od 2018 r. wiodące organy nadzorcze nałożyły kary w wysokości ponad 2,5 mld euro, po wydaniu wiążącej decyzji. Stanowi to około 55% całkowitej kwoty kar nałożonych od 2018 r.

W wyjątkowych przypadkach EROD może przyjąć wiążące decyzje w trybie pilnym – zgodnie z art. 66 RODO. Ta pilna procedura została wprowadzona w celu zapewnienia spójności w egzekwowaniu RODO i może być uruchamiana przez organy nadzorcze wyłącznie w sytuacjach, w których stwierdzono pilną potrzebę podjęcia działań.

Wiążące decyzje sporządzane są przez Sekretariat EROD, w ścisłej współpracy z członkami EROD, zanim zostaną przyjęte. Często decyzje stanowią precedens, rozstrzygając spory dotyczące kluczowych kwestii prawnych. Jednocześnie administracyjne kary pieniężne, nakładane w następstwie wiążących decyzji EROD, są zazwyczaj znaczące. W ostatnich latach EROD przekształciła się z organu dostarczającego interpretacji tekstów prawnych w organ decyzyjny, rozpatrujący konkretne sprawy.

Do dnia 23.04.2024 r. EROD wydała łącznie 11 wiążących decyzji. W 2023 r. EROD przyjęła **dwie wiążące decyzje na podstawie art. 65 RODO i jedną pilną decyzję na podstawie art. 66 RODO,** odnoszące się do szeregu kwestii, takich jak: zasada uwzględniania ochrony danych w fazie projektowania i zasada domyślnej ochrony danych, zasada rzetelności, przetwarzanie danych osobowych dzieci, międzynarodowe przekazywanie danych oraz podstawy prawne reklamy behawioralnej.

Wiążące decyzje:

1) **Wiążąca decyzja nr 1/2023 w sprawie sporu przedłożonego przez irlandzki organ nadzorczy, dotyczącego przekazywania danych przez Meta Platforms Ireland Limited na potrzeby jej serwisu Facebook (art. 65 RODO)**

W kwietniu 2023 r. EROD rozstrzygnęła spór dotyczący kary nałożonej na Meta Platforms Ireland Limited (Meta) oraz nakazu zapewnienia zgodności przetwarzania danych w wiążącej decyzji nr 1/2023. W następstwie wiążącej decyzji EROD irlandzki organ nadzorczy nałożył na Meta karę w wysokości 1,2 mld euro. Kara ta została nałożona za przekazywanie przez Meta danych osobowych do USA na podstawie standardowych klauzul umownych od 16 lipca 2020 r. Meta ponadto została zobowiązana do dostosowania swoich transferów danych do RODO. Andrea Jelinek, ówczesna Przewodnicząca EROD, zauważyła: „EROD stwierdziła, że naruszenie Meta jest bardzo poważne, ponieważ dotyczy transferów, które są systematyczne, powtarzalne i ciągłe. Facebook ma miliony użytkowników w Europie, więc ilość przekazywanych danych osobowych jest ogromna. Bezprecedensowa kara jest silnym sygnałem dla organizacji, że poważne naruszenia mają daleko idące konsekwencje". W swojej wiążącej decyzji EROD poleciła irlandzkiemu organowi nadzorczemu zmianę projektu decyzji i nałożenie kary na Meta. Biorąc pod uwagę powagę naruszenia, EROD stwierdziła, że punkt wyjścia do obliczenia kary powinien wynosić od 20 % do 100% obowiązującego ustawowego maksimum. Europejska Rada Ochrony Danych poleciła również irlandzkiemu organowi nadzorczemu, aby nakazał Meta dostosowanie operacji przetwarzania do rozdziału V RODO poprzez zaprzestanie niezgodnego z prawem przetwarzania, w tym przechowywania, w USA danych osobowych użytkowników europejskich przekazanych z naruszeniem RODO, w ciągu 6 miesięcy od powiadomienia o ostatecznej decyzji irlandzkiego organu nadzorczego. Ostateczna decyzja irlandzkiego organu nadzorczego uwzględniała ocenę prawną wyrażoną przez EROD w jej wiążącej decyzji, przyjętej na podstawie art. 65 ust. 1 lit. a) RODO po tym, jak irlandzki organ nadzorczy, jako wiodący organ nadzorczy (LSA), uruchomił procedurę rozstrzygania sporów dotyczących zastrzeżeń zgłoszonych przez kilka organów nadzorczych, których sprawa dotyczy (CSA). Organy te zgłosiły między innymi zastrzeżenia mające na celu nałożenie kary administracyjnej i/lub dodatkowego nakazu zapewnienia zgodności przetwarzania danych.

2) **Wiążąca decyzja nr 2/2023 w sprawie sporu przedłożonego przez irlandzki organ nadzorczy, dotyczącego TikTok Technology Limited (art. 65 RODO)**

W sierpniu 2023 r. EROD rozstrzygnęła spór dotyczący projektu decyzji irlandzkiego organu nadzorczego w sprawie przetwarzania danych osobowych użytkowników w wieku od 13 do 17 lat przez TikTok Technology Limited (TikTok IE).

W decyzji wiążącej nr 2/2023 EROD przeanalizowała praktyki projektowe wdrożone przez TikTok w kontekście dwóch wyskakujących powiadomień, które były wyświetlane dzieciom w wieku 13–17 lat: wyskakującego okienka rejestracji i wyskakującego okienka zamieszczania filmów. Analiza wykazała, że oba wyskakujące okienka nie przedstawiały użytkownikowi opcji w obiektywny i neutralny sposób.

W następstwie wiążącej decyzji EROD irlandzki organ nadzorczy wydał ostateczną decyzję, w której stwierdził w szczególności, że TikTok IE naruszył zasadę rzetelności RODO podczas przetwarzania danych osobowych dotyczących dzieci w wieku od 13 do 17 lat i nałożył upomnienie, nakaz przestrzegania przepisów oraz karę w wysokości 345 mln euro. Anu Talus, Przewodnicząca EDPB, wskazała, że: „Przedsiębiorstwa zajmujące się mediami społecznościowymi mają obowiązek unikać prezentowania użytkownikom, zwłaszcza dzieciom, możliwości wyboru w nieuczciwy sposób – zwłaszcza jeśli taka prezentacja może nakłaniać ludzi do podejmowania decyzji naruszających ich interesy związane z prywatnością. Opcje związane z prywatnością powinny być dostarczane w obiektywny i neutralny sposób, unikając wszelkiego rodzaju zwodniczego lub manipulacyjnego języka, lub projektowania. Dzięki tej decyzji EROD po raz kolejny wyjaśnia, że podmioty cyfrowe muszą zachować szczególną ostrożność i podjąć wszelkie niezbędne środki w celu ochrony praw dzieci do ochrony danych”.

Europejska Rada Ochrony Danych potwierdziła, że administratorzy nie powinni utrudniać osobom, których dane dotyczą, dostosowania ustawień prywatności i ograniczenia przetwarzania. Stwierdziła również, że w wyniku przedmiotowych praktyk TikTok IE naruszył zasadę rzetelności wynikającą z RODO. W związku z tym EROD poleciła irlandzkiemu organowi nadzorczemu, aby w swojej ostatecznej decyzji zawarł stwierdzenie tego dodatkowego naruszenia i nakazał TikTok IE przestrzeganie RODO poprzez wyeliminowanie takich praktyk projektowych. Rada oceniła również, czy środki weryfikacji wieku wdrożone przez TikTok IE między 31 lipca a 31 grudnia 2020 r. były zgodne z wymogami ochrony danych w fazie projektowania (art. 25 ust. 1 RODO). Europejska Rada Ochrony Danych wyraziła poważne wątpliwości co do skuteczności środków weryfikacji wieku wprowadzonych przez TikTok IE w tym okresie, w szczególności biorąc pod uwagę powagę zagrożeń dla dużej liczby dzieci, których dotyczyły. Stwierdziła między innymi, że bramka wiekowa wdrożona przez TikTok IE w celu uniemożliwienia dostępu do platformy użytkownikom poniżej 13. roku życia może być łatwo ominięta, a środki stosowane po uzyskaniu przez użytkowników dostępu do TikTok IE nie były stosowane w wystarczająco systematyczny sposób.

3) Pilna wiążąca decyzja nr 01/2023, przedłożona przez norweski organ nadzorczy w celu przyjęcia środków o charakterze ostatecznym w odniesieniu do Meta Platforms Ireland Ltd (art. 66 ust. 2 RODO)

W następstwie pilnej decyzji wiążącej EROD nr 1/2023 z 27 października 2023 r., irlandzki organ nadzorczy przyjął ostateczną decyzję w dniu 10 listopada 2023 r., nakładając na Meta zakaz przetwarzania danych osobowych do celów reklamy behawioralnej na podstawie umowy i uzasadnionego interesu. Wiążąca decyzja EROD w trybie pilnym została wydana w następstwie wniosku norweskiego organu nadzorczego o podjęcie ostatecznych środków, które obowiązywałyby w całym Europejskim Obszarze Gospodarczym (EOG). Przewodnicząca EROD – Anu Talus – wskazała, że: „Po

dokładnym rozważeniu EROD uznała za konieczne poinstruowanie norweskiego organu nadzorczego, aby nałożył zakaz przetwarzania danych w całym EOG, skierowany do Meta. Już w grudniu 2022 r. Wiążące Decyzje EROD wyjaśniły, że umowa nie jest odpowiednią podstawą prawną do przetwarzania danych osobowych przez Meta w celu reklamy behawioralnej. Ponadto norweski organ nadzorczy stwierdził, że Meta nie wykazała zgodności z nakazami nałożonymi pod koniec ubiegłego roku. Doprowadziło to do zastosowania art. 66 RODO – odstępstwa od zwykłej procedury współpracy, która może być stosowana tylko w wyjątkowych okolicznościach".

Początkowo, 14 lipca 2023 r., norweski organ nadzorczy przyjął zarządzenie nakładające tymczasowy zakaz na mocy art. 66 ust. 1 RODO, w odniesieniu do przetwarzania danych osobowych obywateli Norwegii, których dane dotyczą, do celów reklamy behawioralnej, opierając się na podstawach prawnych umowy lub uzasadnionego interesu. Zakaz ten był ograniczony czasowo i geograficznie: obowiązywał przez 3 miesiące i miał zastosowanie tylko w Norwegii. 26 września 2023 r. norweski organ nadzorczy złożył wniosek do EROD o pilną wiążącą decyzję nakazującą przyjęcie ostatecznych środków mających zastosowanie do użytkowników w całym EOG. Po przeanalizowaniu akt EROD stwierdziła, że dochodzi do ciągłych naruszeń RODO i istnieje pilna potrzeba podjęcia działań w świetle zagrożeń dla praw i wolności osób, których dane dotyczą.

Na podstawie dostarczonych dowodów EROD stwierdziła, że doszło do trwającego naruszenia art. 6 ust. 1 RODO z powodu naruszenia praw i wolności osób, których dane dotyczą, z powodu niewłaściwego wykorzystania podstaw prawnych umowy i uzasadnionego interesu do przetwarzania danych osobowych gromadzonych przez Meta do celów reklamy behawioralnej. Ponadto EROD stwierdziła, że doszło również do ciągłego naruszania przez Meta obowiązku przestrzegania decyzji organów nadzorczych, w szczególności ostatecznych decyzji irlandzkiego organu nadzorczego z grudnia 2022 r. Odnosząc się do pilnego charakteru sprawy, EROD stwierdziła, że zwykłe mechanizmy współpracy nie mogły być stosowane w zwyczajowy sposób oraz że pilna potrzeba zarządzenia środków ostatecznych była oczywista w świetle ryzyka poważnej i nieodwracalnej szkody wyrządzonej osobom, których dane dotyczą.

Współpraca organów i egzekwowanie prawa

1) Oświadczenie w sprawie współpracy w zakresie egzekwowania prawa

Znaczenie spójnego egzekwowania przepisów poprzez współpracę było podkreślane przez EROD od czasu przyjęcia RODO. W 2020 r. EROD ustanowiła skoordynowane ramy egzekwowania prawa (CEF) w celu usprawnienia egzekwowania prawa i współpracy między organami ochrony danych, zgodnie ze swoją strategią na lata 2021–2023. CEF składa się z corocznych wspólnych działań na określony temat, w tym działań, takich jak: wspólne kampanie informacyjne, gromadzenie informacji, kontrole egzekwowania prawa, a także wspólne dochodzenia. Te coroczne skoordynowane wysiłki w zakresie egzekwowania prawa mają na celu poprawę zgodności z przepisami, umożliwienie osobom fizycznym korzystania z ich praw i zwiększenie świadomości na temat kwestii związanych z ochroną danych.

Jako przedmiot skoordynowanego działania służącego egzekwowaniu prawa w 2023 r. EROD wybrała obszar „wyznaczanie i pozycja inspektorów ochrony danych".

Co roku organy nadzorcze wchodzące w skład EROD w ramach skoordynowanego egzekwowania prawa (Coordinated Enforcement Framework – CEF) przeprowadzają badanie poświęcone ustalonemu wcześniej tematowi. W 2023 r. 25 organów ochrony danych w całym Europejskim Obszarze Gospodarczym (w tym EIOD) rozpoczęło skoordynowane działania dotyczące pozycji i wyznaczania inspektorów ochrony danych (CEF DPO). Skontaktowano się z różnymi organizacjami, a także inspektorami ochrony danych w całym EOG, z różnych sektorów (zarówno podmioty publiczne, jak i prywatne), i otrzymano ponad 17 000 odpowiedzi.

2) Sprawozdanie EROD podsumowujące badanie dotyczące wyznaczania i pozycji inspektorów ochrony danych

Zebrano obszerne dane zapewniające cenny wgląd w profil, pozycję i pracę inspektorów ochrony danych 5 lat po wejściu w życie RODO. Organy nadzorcze skonsolidowały swoje ustalenia w raportach krajowych, które następnie – w 2024 r. – zostały połączone w celu stworzenia raportu EROD, wymieniającego przeszkody, z jakimi obecnie borykają się inspektorzy ochrony danych, wraz z szeregiem zaleceń mających na celu dalsze wzmocnienie ich pozycji. Sprawozdanie zachęca między innymi organy nadzorcze do prowadzenia większej liczby działań uświadamiających, informacyjnych i egzekucyjnych. W raporcie zachęca się również organizacje do zapewnienia inspektorom ochrony danych wystarczających możliwości, czasu i zasobów na odświeżenie wiedzy oraz zapoznanie się z najnowszymi rozwiązaniami.

3) Grupa ekspertów wspierających EROD (Support Pool of Experts)

W ramach strategii na lata 2021–2023 EROD w 2020 r. ustanowiła Grupę ekspertów wspierającą EROD (Suport Pool of Experts, dalej SPE). Głównym celem SPE jest pomoc organom nadzorczym w prowadzeniu postępowań i działań w zakresie egzekwowania prawa, będących przedmiotem wspólnego zainteresowania organów. Działania te obejmują m.in. wsparcie analityczne, czy też przygotowywanie raportów na podstawie zebranych w postępowaniu dowodów. Co więcej, SPE ma za zadanie zaspokajanie ewentualnych potrzeb operacyjnych organów. Aby lepiej koordynować pracę SPE, pod koniec 2021 r. EROD utworzyła listę punktów kontaktowych SPE w organach ochrony danych.

Dodatkowo w lutym 2023 r. EROD ogłosiła zaproszenie do wyrażenia zainteresowania „Ustanowieniem listy ekspertów indywidualnych na potrzeby wdrożenia grupy ekspertów wspierających EROD”. Celem tego zaproszenia jest utworzenie listy rezerwowej ekspertów zewnętrznych posiadających wiedzę prawniczą lub techniczną. Pod koniec 2023 r. na liście rezerwowej EROD znajdowało się około 500 ekspertów. Do tej pory uruchomiono łącznie 13 projektów, a niektóre z nich dotyczą kwestii związanych ze sztuczną inteligencją.

W czerwcu 2023 r. EROD zorganizowała warsztaty (*boot camp)* dotyczące kontroli stron internetowych, na które zaprosiła kilku ekspertów ds. ochrony danych. Wydarzenie to było doskonałą okazją do wykorzystania i omówienia nowego narzędzia do audytu stron internetowych EROD opracowanego w ramach SPE, które jest obecnie publikowane jako otwarty kod źródłowy na stronie code.europa.eu. Drugi *boot camp* zostanie zorganizowany w 2024 r.

1.6 Udział UODO w pracach EROD

W ramach prac podgrup i grup zadaniowych EROD przedstawiciele polskiego organu nadzorczego, wraz z reprezentantami pozostałych organów, opracowali w ostatnich latach szereg dokumentów, w tym: opinie, wytyczne, zalecenia i najlepsze praktyki, w celu promowania wspólnego zrozumienia rozporządzenia.

Polski organ nadzorczy w 2023 r. był współautorem m.in. następujących dokumentów:

- Wytyczne 1/2022 dotyczące praw osób, których dane dotyczą – prawo dostępu;
- Wytyczne 03/2022 w sprawie zwodniczych wzorców projektowych w interfejsach platform mediów społecznościowych: jak je rozpoznać i uniknąć;
- Wewnętrzny dokument dotyczący prawa do bycia wysłuchanym i prawo dostępu do akt dotyczących procedur współpracy zgodnie z art. 60 RODO;
- Opinie EROD ws. wymogów akredytacji podmiotu monitorującego kodeksy postępowania na mocy art. 41 RODO oraz podmiotu certyfikującego na mocy art. 43 RODO.

Dnia 10 października 2022 r. EROD przyjęła wykaz aspektów krajowego prawa proceduralnego, które zamierza zharmonizować na szczeblu UE w celu ułatwienia egzekwowania RODO. Opracowanie tego wykazu, tzw. „listy życzeń", było jednym z najważniejszych działań zapowiedzianych w deklaracji wiedeńskiej EROD w sprawie współpracy w zakresie egzekwowania prawa. **Urząd Ochrony Danych Osobowych aktywnie uczestniczył w opracowaniu tego dokumentu, wskazując na aspekty proceduralne, które biorąc pod uwagę jego aktywny udział w licznych postępowaniach transgranicznych (por. statystyki IMI poniżej), wymagają dalszego zharmonizowania na poziomie unijnym.**

Wykaz ten dotyczy m.in.: statusu i praw stron postępowania administracyjnego, terminów proceduralnych, wymogów dotyczących dopuszczalności lub oddalenia skarg, uprawnień w zakresie prowadzenia postępowań wyjaśniających organów ochrony danych oraz praktycznego wdrożenia procedury współpracy.

W wyniku tej inicjatywy EROD 4 lipca 2023 r. Komisja Europejska opublikowała wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679 („wniosek") oraz przeprowadziła formalne konsultacje z EROD i EIOD zgodnie z art. 42 ust. 2 rozporządzenia (UE) 2018/1725. Urząd Ochrony Danych Osobowych brał czynny udział w opracowywaniu wspólnej opinii EROD i EIOD dotyczącej tego wniosku.

W listopadzie 2021 r. **z inicjatywy UODO** utworzono grupę roboczą składającą się z organów nadzorczych z: Francji, Holandii, Litwy i Polski, wspieraną przez Europejską Radę Ochrony Danych (EROD), która rozpatrzyła szereg skarg dotyczących potencjalnych naruszeń ogólnego rozporządzenia o ochronie danych przez Vinted UAB, operatora serwisu sprzedażowego odzieży Vinted.com.

Organy nadzorcze w 2023 r. badały kwestie związane m.in. z przejrzystym informowaniem i przechowywaniem danych związanych z wypłatą środków czy realizacją praw osób, których dane dotyczą. Praca organów koncentrowała się również na przetwarzaniu danych osobowych w kontekście blokowania kont użytkowników. **Organy pracowały nieformalnie, aby pomóc litewskiemu organowi nadzorczemu w przyjęciu**

decyzji nakładającej administracyjną karę pieniężną na Vinted. Efektem tych prac była nałożona przez litewski organ nadzorczy kara pieniężna w wysokości prawie 10 mln zł.

Zaangażowanie organów nadzorczych w prace grupy roboczej do spraw Vinted jest przykładem ścisłej współpracy w zakresie egzekwowania prawa – strategicznego priorytetu dla EROD. Mając za przykład grupę roboczą do spraw Vinted, EROD postanowiła o częstszym korzystaniu z tej formy współpracy w przyszłości.

2. Współpraca w ramach IMI

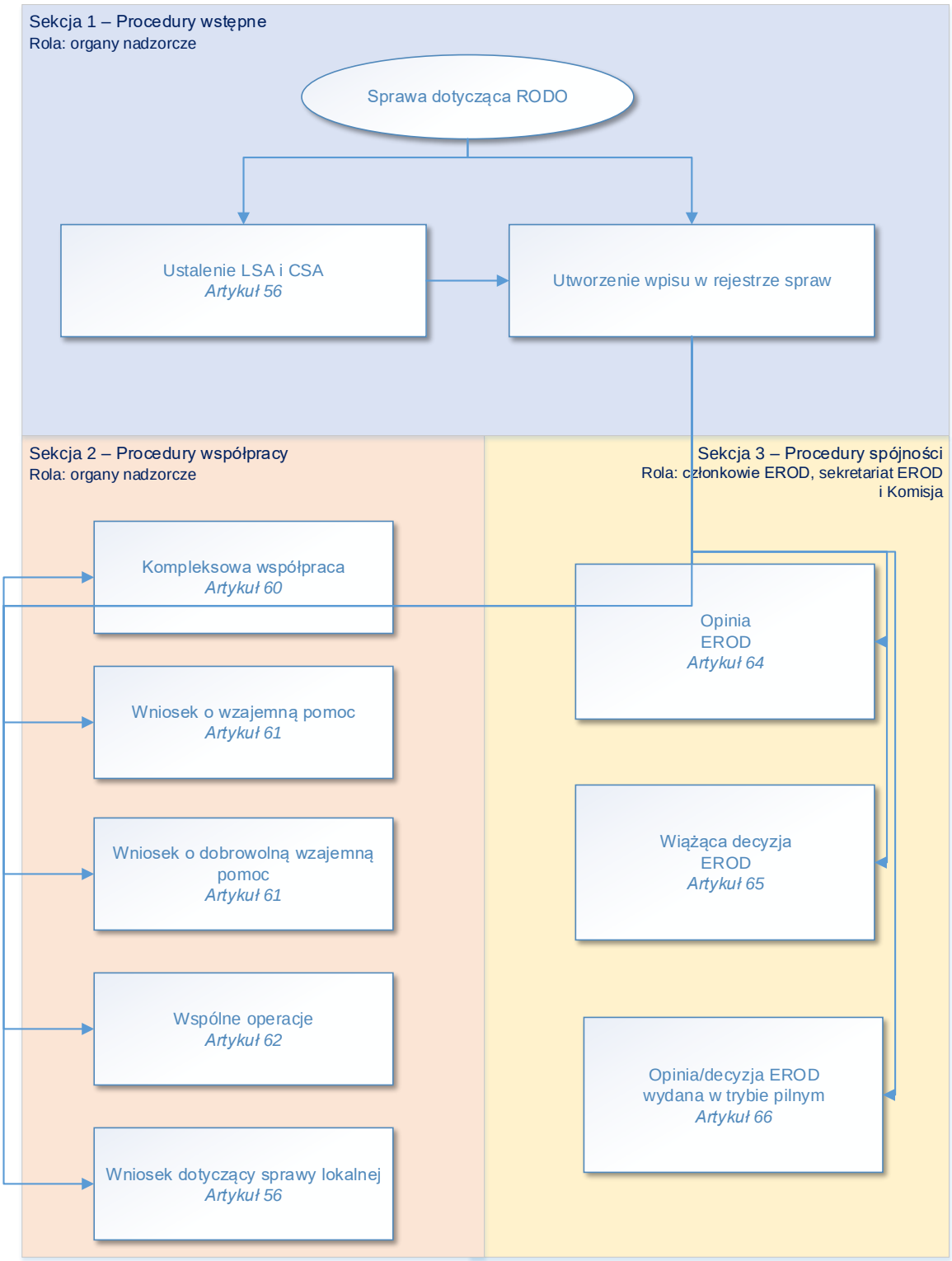
Od 25 maja 2018 r. organy nadzorcze korzystają z systemu wymiany informacji na rynku wewnętrznym[361], w celu wymiany, w sposób bezpieczny i ustandaryzowany, informacji niezbędnych dla realizacji mechanizmów współpracy i spójności, przewidzianych w rozdziale VII RODO, i w tym zakresie prowadzenia postępowań transgranicznych.

System IMI został opracowany przez Dyrekcję Generalną Komisji Europejskiej ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MŚP (DG GROW). Został on dostosowany do potrzeb RODO w ścisłej współpracy z Sekretariatem EROD i organami nadzorczymi. W celu zapewnienia dostosowania systemu do zmieniających się potrzeb organów nadzorczych w ramach EROD działa podgrupa ekspertów 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:

- art. 56 – ustalenie wiodącego organu nadzorczego i organów, których sprawa dotyczy (wniosek dotyczący sprawy lokalnej);
- art. 60 – kompleksowa współpraca;
- art. 61 – wniosek o wzajemną pomoc i dobrowolną wzajemną pomoc;
- art. 62 – wspólne operacje organów nadzorczych;
- art. 64 – opinia EROD;
- art. 65 – wiążąca decyzja EROD;
- art. 66 – opinia/decyzja EROD wydana w trybie pilnym.

[361] Ang. *Internal Market Information System*, dalej: „system IMI” lub „IMI”.



Źródło ilustracji: wewnętrzny podręcznik IMI dla organów nadzorczych, opracowany przez Sekretariat EROD (pisownia oryginalna).

Zgodnie ze statystykami przygotowanymi przez EROD w 2023 r. łącznie w rejestrze spraw EROD utworzono **366** spraw transgranicznych**.**

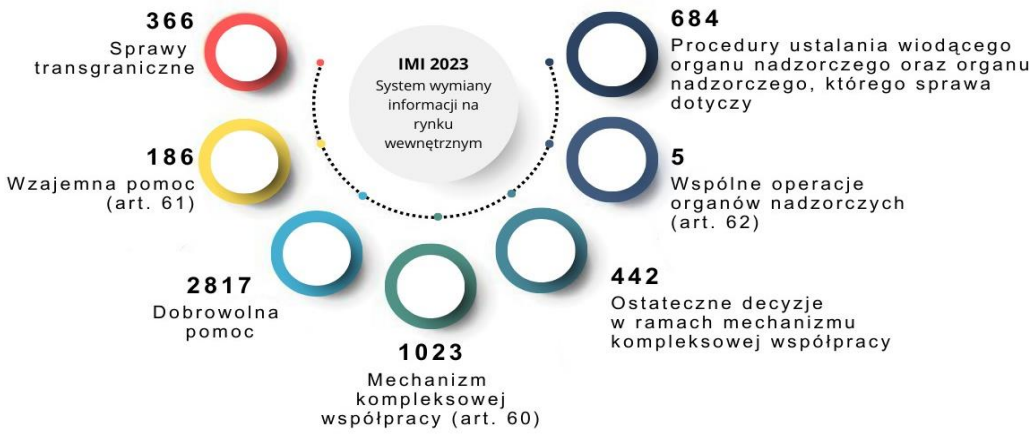
Właściwość wiodącego organu nadzorczego, na mocy art. 56 RODO, względem transgranicznego przetwarzania dokonywanego przez administratora lub podmiot przetwarzający – była rozpatrywana w **684** sprawach.

Uruchomiono **1023** procedury związane z mechanizmem kompleksowej współpracy miedzy wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy (art. 60 RODO), z czego **442** zakończyły się przyjęciem ostatecznej decyzji.

Zgodnie z art. 61 RODO organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania rozporządzenia oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i przeprowadzenie uprzednich konsultacji oraz o przeprowadzenie kontroli i postępowań wyjaśniających. W 2023 r. podjęto współpracę w ramach **186** wniosków o wzajemną pomoc.

Organy nadzorcze prowadzą w stosownych przypadkach wspólne operacje, w tym postępowania i działania egzekucyjne, w których uczestniczą członkowie lub personel organów nadzorczych innych państw członkowskich. W 2023 r. podjęto **5** wspólnych operacji organów nadzorczych.

Poniższa ilustracja przedstawia ww. statystykę ujętą w Sprawozdaniu Europejskiej Rady Ochrony Danych za 2023 r.: „Ochrona praw cyfrowych osób fizycznych”.



<u>Zgodnie z danymi z systemu IMI w terminie od 1 stycznia do 31 grudnia 2023 r. Urząd Ochrony Danych Osobowych</u>:

1) był organem wiodącym w **12** sprawach w rejestrze spraw IMI;
2) zainicjował i przesłał do innych organów nadzorczych **172** powiadomienia, w tym:
   - **33** z art. 56 (identyfikacja wiodącego organu nadzorczego, którego sprawa dotyczy),
   - **3** z art. 60 (**1** – projekt decyzji, **2** – ostateczna decyzja),
   - **136** z art. 61 (dobrowolna wzajemna pomoc);
3) otrzymał łącznie **2 304** wnioski, w tym:
   - **720** z art. 56 (identyfikacja wiodącego organu nadzorczego i organu, którego sprawa dotyczy),
   - **1 041** z art. 60 (współpraca między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy), w tym:
     - **453 projekty decyzji,**

- **107 w ramach wymiany istotnych decyzji,**
- **32 zmienione projekty decyzji,**
- **449 ostatecznych decyzji,**

- **438** z art. 61 (dobrowolna wzajemna pomoc),
- **1** z art. 62 (wspólne operacje organów nadzorczych),
- **39** z art. 64 (opinia EROD),
- **60** z art. 65 (procedura pisemna).

3. 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 r. w celu umożliwienia wymiany najlepszych praktyk pomiędzy inspektorami ochrony danych organów nadzorczych i stworzenia bardziej zharmonizowanego podejścia między nimi. Opracowywane w jej ramach zalecenia są rekomendacjami nieformalnymi, wewnętrznymi i dotyczą wyłącznie organów nadzorczych.

7 marca i 25 września 2023 r. odbyły się dwa spotkanie sieci Inspektorów Ochrony Danych. Praca DPO Network w 2023 r. skupiła się na analizie kwestii, czy dochodzi do współadministrowania między organami nadzorczymi a EROD w kontekście rejestru decyzji ostatecznych, na podstawie art. 60 RODO. Podczas tych spotkań dyskutowano też na temat zasadności utworzenia rejestru przedstawicieli administratorów lub podmiotów przetwarzających, niemających jednostki organizacyjnej w Unii, na podstawie art. 27 RODO. Rozmowy dotyczyły również wykorzystania mediów społecznościowych przez poszczególne organy nadzorcze, a także omówione zostały skoordynowane działania w zakresie egzekwowania prawa dotyczące roli inspektorów ochrony danych. Dyskusja koncentrowała się ponadto na orzeczeniach TSUE zapadłych w sprawach C-487/21 i C-413/23 P. W ramach wymiany informacji i praktyk IOD litewskiego organu nadzorczego przedstawiła prezentację na temat przetwarzania materiału foto/wideo w celu dłuższego przechowywania ze względu na ich wartość historyczną oraz incydentów bezpieczeństwa w sektorze bankowym.

4. Nadzór nad wielkoskalowymi systemami

Istotnym obszarem działalności Prezesa UODO w 2023 r. pozostawała współpraca międzynarodowa w ramach art. 62 rozporządzenia 2018/1725[362], która przewiduje zharmonizowany model skoordynowanego nadzoru, mający zastosowanie w przypadku, gdy odpowiednie prawo Unii Europejskiej odnosi się do tego artykułu.

Zgodnie z ww. przepisem EIOD i krajowe organy nadzorcze czynnie współpracują w ramach swoich obowiązków, aby zapewnić skuteczny nadzór nad wielkoskalowymi systemami informatycznymi oraz organami i jednostkami organizacyjnymi Unii. Skoordynowane działania obejmują m.in. wspólne kontrole i dochodzenia oraz prace nad wspólną metodologią.

[362] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L z 2018 r. poz. 295).

W analizowanym 2023 r. przedstawiciele UODO uczestniczyli w posiedzeniach wymienionych poniżej wyspecjalizowanych grup:

- Grupy ds. Koordynacji Nadzoru nad Systemem Informacji Celnej (CIS), który pomaga w zapobieganiu naruszeniom przepisów prawa celnego i rolnego, ich dochodzeniu i ściganiu;
- Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS), który jest bazą danych mającą ułatwić procedurę rozpatrywania wniosków o wydanie wiz krótkoterminowych;
- Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac, który zawiera odciski palców wszystkich osób ubiegających się o azyl, zarejestrowanych w państwach członkowskich UE i krajach współpracujących.

Przedstawiciel UODO uczestniczył także w pracach Komitetu Skoordynowanego Nadzoru (CSC) obejmujących działania nadzorcze nad Systemem Informacyjnym Schengen (SIS II), a także nad systemem informacyjnym rynku wewnętrznego (IMI), Eurojust i Europol.

Kluczowym obszarem działalności komitetu w 2023 r. były prawa osób, których dane dotyczą. W omawianym roku CSC dążył do podnoszenia świadomości i zapewniania wskazówek, aby pomóc osobom fizycznym w korzystaniu z przysługujących im praw, również z uwagi na wyzwania, jakie niosą ze sobą ramy prawne dotyczące interoperacyjności. Dlatego Komitet Skoordynowanego Nadzoru opracował przewodniki na temat korzystania z praw osób, których dane dotyczą: prawo dostępu, sprostowania i usunięcia danych w Systemie Informacyjnym Schengen (SIS) oraz w systemie informacyjnym Europolu.

Kolejnym zadaniem komitetu było badanie trudności w interpretacji lub stosowaniu rozporządzenia 2018/1725 i innych przepisów prawa UE w odniesieniu do wielkoskalowych systemów oraz organów informacyjnych. Stosowanie niektórych z tych systemów musi pozostawać w zgodzie ze stosowaniem prawa krajowego, które może mieć zastosowanie np. do przetwarzania danych z zakresu ochrony porządku publicznego.

Innym kluczowym zadaniem komitetu było umożliwienie organom nadzorczym wymiany istotnych informacji oraz wzajemnej pomocy w przeprowadzaniu audytów i kontroli. W ramach komitetu odbyły się warsztaty zainicjowane przez jeden z krajowych organów nadzorczych – dotyczące strategii nadzoru nad systemami informacyjnymi UE. Celem warsztatów, w których uczestniczył przedstawiciel UODO, była wymiana doświadczeń i pomysłów na temat tego, w jaki sposób organy ochrony danych podchodzą, pod względem organizacji i interwencji, do swoich zadań nadzorczych w związku z rozszerzeniem systemów informacyjnych UE, wzajemnymi prawami dostępu i przepływem danych oraz interoperacyjnością. Na zaproszenie Europejskiego Inspektora Ochrony Danych przedstawiciel UODO brał udział we wspólnej inspekcji EIOD w siedzibie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) – na podstawie mechanizmu przewidzianego w art. 44 rozporządzenia 2016/794 w sprawie Europolu[363].

[363] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WsiSW (Dz. Urz. UE L z 2016 r. poz. 135).

Ponadto przedstawiciel UODO uczestniczył w charakterze eksperta w zespołach prowadzących kontrole w zakresie oceny i monitorowania stosowania dorobku Schengen w obszarze ochrony danych osobowych, zgodnie z rozporządzeniem 1053/2013[364] i rozporządzeniem 2022/922[365]. W ocenach tych dokonuje się ewaluacji w zakresie tego, w jaki sposób państwa członkowskie wdrażają i stosują dorobek Schengen, w szczególności w odniesieniu do SIS i VIS w kontekście wymogów ochrony danych. Badają one również rolę organów ochrony danych w odniesieniu do nadzoru nad organami zarządzającymi i korzystającymi z SIS oraz VIS. Pozytywna ocena jest gwarancją tego, że państwa członkowskie stosują przepisy Schengen skutecznie i zgodnie z podstawowymi zasadami oraz normami. Za wdrożenie mechanizmu oceny i monitorowania odpowiadają wspólnie państwa członkowskie i Komisja przy wsparciu organów i jednostek organizacyjnych Unii uczestniczących we wdrażaniu dorobku Schengen.

5. 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 TSUE, przekazanych przez KPRM. Wnioski te dotyczą zagadnień z zakresu ochrony danych osobowych. Organ nadzorczy przygotowuje 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 uzyskaniu informacji o stanowiskach innych krajów. Po wydaniu wyroku TSUE organ nadzorczy przedstawia swoje stanowisko w sprawie zasadności zmiany polskiego prawa lub sposobu jego interpretacji.

Organ nadzorczy dokonuje – niezależnie od powyższego – regularnego przeglądu wszystkich postępowań inicjowanych przez TSUE.

W 2023 r. do polskiego organu nadzorczego wpłynęły **23 nowe wnioski prejudycjalne skierowane do TSUE** przez sądy z różnych państw Unii Europejskiej – dla porównania, w 2022 r. było ich 28, a w 2021 r. – 27.

Organ nadzorczy dokonał analizy przekazanych przez KPRM wniosków prejudycjalnych. Jako przykłady najbardziej istotnych spraw można wskazać następujące:

- **C-740/22 *Endemol Shine Finland*** – sprawa dotyczyła ochrony danych osobowych oraz ustnego przekazania danych osobowych jako ich przetwarzania, a także publicznego dostępu do informacji z sądowego rejestru osobowego o wyrokach karnych – w ocenie organu nadzorczego udział w postępowaniu był zasadny[366];

[364] Rozporządzenie Rady (UE) nr 1053/2013 z 7 października 2013 r. w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz uchylenia decyzji komitetu wykonawczego z 16 września 1998 r. dotyczącej utworzenia Stałego Komitetu ds. Oceny i Wprowadzania w Życie Dorobku Schengen (Dz. Urz. UE L z 20213 r. poz. 295).
[365] Rozporządzenie Rady (UE) 2022/922 z 9 czerwca 2022 r. w sprawie ustanowienia i funkcjonowania mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz w sprawie uchylenia rozporządzenia (UE) nr 1053/2013 (Dz. Urz. UE L z 2022 r. poz. 160).
[366] DOL.0623.2.2023.

- **C-46/23 *Újpesti Polgármesteri Hivatal*** – sprawa dotyczyła uprawnienia organu nadzorczego do nakazania administratorowi usunięcia danych przetwarzanych niezgodnie z prawem bez wyraźnego żądania osoby, której dane dotyczą – w ocenie organu nadzorczego udział w postępowaniu był zasadny[367];
- **C-57/23 *Policejní prezidium*** – sprawa dotyczyła przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości oraz pobierania i przechowywania danych genetycznych osób podejrzanych lub oskarżonych – w ocenie organu nadzorczego udział w postępowaniu był zasadny[368];
- **C-169/23 *Másdi*** – sprawa dotyczyła ochrony danych osobowych, obowiązków informacyjnych administratora danych, wyjątków dotyczących istnienia regulacji prawnych przewidujących odpowiednie środki ochronne – w ocenie organu nadzorczego udział w postępowaniu był zasadny[369];
- **C-209/23 *RRC Sports*** – sprawa dotyczyła zasady wykonywania usług pośrednictwa przez agentów piłkarskich, ochrony konkurencji, swobody świadczenia usług oraz ochrony danych osobowych – w ocenie organu nadzorczego udział w postępowaniu był zasadny[370];
- **C-247/23 *Deldits*** – sprawa dotyczyła ochrony danych osobowych, prawa do sprostowania danych oraz sprostowania danych dotyczących płci w rejestrze spraw o udzielenie azylu – w ocenie organu nadzorczego udział w postępowaniu był zasadny[371];
- **C-229/23 *HYA e.a.*** – sprawa dotyczyła ochrony danych osobowych w sektorze łączności elektronicznej, związana była z sądowym zezwoleniem na podsłuchiwanie i nagrywanie rozmów osób podejrzanych oraz wymogiem uzasadnienia zezwolenia – w ocenie organu nadzorczego udział w postępowaniu był zasadny[372];
- **C-394/23 *Mousse*** – sprawa dotyczyła ochrony danych osobowych, niezbędności przetwarzania danych oraz gromadzenia danych na temat płci klientów w zakresie ograniczonym do określeń „pan” lub „pani” – w ocenie organu nadzorczego udział w postępowaniu był zasadny[373];
- **C-492/23 *Russmedia Digital et Inform Media Press*** – sprawa dotyczyła usługi społeczeństwa informacyjnego, ochrony danych osobowych oraz obowiązków dostawcy usług informacyjnych jako administratora danych osobowych – w ocenie organu nadzorczego udział w postępowaniu był zasadny[374].

W 2023 r. organ nadzorczy dokonał analizy wpływu na przepisy polskiego prawa wyroków wydanych przez TSUE w sprawach:

- **C-252/21 *Meta Platforms i in./Facebook e.a.*** – Trybunał stwierdził, że art. 51 RODO oraz art. 4 ust. 3 TUE należy rozumieć w taki sposób, że organ ochrony

[367] DOL.0623.6.2023.
[368] DOL.0623.9.2023.
[369] DOL.0623.10.2023.
[370] DOL.0623.15.2023.
[371] DOL.0623.17.2023.
[372] DOL.0623.18.2023.
[373] DOL.0623.24.2023.
[374] DOL.0623.28.2023.

konkurencji państwa członkowskiego, choć zobowiązany jest do poszanowania obowiązku lojalnej współpracy z organami nadzorczymi, to może w ramach badania nadużycia pozycji dominującej przez przedsiębiorstwo w rozumieniu art. 102 TFUE stwierdzić, że ogólne warunki korzystania z usług tego przedsiębiorstwa dotyczące przetwarzania danych osobowych i ich wdrażanie nie są zgodne z tym rozporządzeniem, jeżeli to stwierdzenie jest konieczne do wykazania istnienia takiego nadużycia. W wyroku TSUE stwierdził także, że art. 9 ust. 1 ROD: „należy interpretować w ten sposób, że w przypadku, gdy użytkownik internetowej sieci społecznościowej przegląda strony internetowe lub aplikacje powiązane z jedną lub kilkoma kategoriami, o których mowa w tym przepisie, i, w stosownym przypadku, zamieszcza w nich dane, rejestrując się na tych stronach lub tych aplikacjach, czy też składając zamówienia online, dokonywane przez operatora tej internetowej sieci społecznościowej przetwarzanie danych osobowych polegające na zbieraniu, za pomocą zintegrowanych interfejsów, plików cookie lub podobnych technologii rejestracji, danych pochodzących z przeglądania tych stron i tych aplikacji oraz danych zamieszczonych przez użytkownika, łączeniu wszystkich tych danych z kontem sieci społecznościowej tego użytkownika i wykorzystywaniu tych danych przez tego operatora, należy uznać za »przetwarzanie szczególnych kategorii danych osobowych« w rozumieniu tego przepisu, które jest co do zasady zakazane, z zastrzeżeniem wyjątków przewidzianych w art. 9 ust. 2 RODO, jeżeli owo przetwarzanie danych może ujawniać informacje należące do jednej z tych kategorii, niezależnie od tego, czy informacje te dotyczą użytkownika tej sieci, czy jakiejkolwiek innej osoby fizycznej”. Zdaniem Trybunału art. 6 ust. 1 lit. b) RODO należy rozumieć w ten sposób, że dokonywane przez operatora internetowej sieci społecznościowej przetwarzanie danych osobowych, polegające na zbieraniu danych użytkowników takiej sieci pochodzących z innych usług grupy, do której należy ten operator, lub pochodzących z przeglądania przez tych użytkowników stron internetowych lub aplikacji osób trzecich, łączeniu tych danych z kontem sieci społecznościowej tych użytkowników i wykorzystywaniu tych danych, może zostać uznane za niezbędne do wykonania umowy, której stroną są osoby, których dane dotyczą, w rozumieniu tego przepisu, tylko wtedy, gdy przetwarzanie to jest obiektywnie niezbędne do osiągnięcia celu, który stanowi integralną część świadczenia umownego na rzecz tych samych użytkowników, skutkiem czego główny cel umowy nie mógłby zostać osiągnięty bez tego przetwarzania. Poza tym zdaniem Trybunału, art. 6 ust. 1 akapit pierwszy lit. f) RODO należy interpretować w ten sposób, że takie przetwarzanie może zostać uznane za niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią w rozumieniu tego przepisu jedynie pod warunkiem, że operator ten wskazał użytkownikom, od których dane zostały pozyskane, prawnie uzasadniony interes, do którego realizacji służy przetwarzanie tych danych, że przetwarzanie to odbywa się w granicach tego, co jest absolutnie niezbędne do realizacji tego prawnie uzasadnionego interesu, oraz że z wyważenia przeciwstawnych interesów w świetle wszystkich istotnych okoliczności wynika, że interesy lub podstawowe prawa i wolności tych użytkowników nie mają pierwszeństwa przed tym prawnie uzasadnionym interesem administratora lub

osoby trzeciej. Art. 6 ust. 1 akapit pierwszy lit. d) i e) RODO należy interpretować w ten sposób, że takie przetwarzanie danych osobowych nie może – co do zasady i z zastrzeżeniem weryfikacji, którą powinien przeprowadzić sąd odsyłający – zostać uznane za niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej w rozumieniu lit. d) lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, w rozumieniu lit. e) tego przepisu. Art. 6 ust. 1 akapit pierwszy lit. a) i art. 9 ust. 2 lit. a) RODO należy interpretować w ten sposób, że okoliczność polegająca na tym, iż operator internetowej sieci społecznościowej zajmuje pozycję dominującą na rynku internetowych sieci społecznościowych, nie stoi sama w sobie na przeszkodzie temu, by użytkownicy takiej sieci mogli skutecznie wyrazić zgodę, w rozumieniu art. 4 pkt 11 tego rozporządzenia, na przetwarzanie ich danych osobowych przez tego operatora. Niemniej okoliczność ta stanowi element istotny dla ustalenia tego, czy zgoda ta została rzeczywiście udzielona skutecznie i – w szczególności – dobrowolnie, czego udowodnienie należy do tego operatora. W ocenie organu nadzorczego wyrok może skutkować koniecznością dokonania zmian w polskim prawie. Za istotne organ nadzorczy uznał podjęcie dyskusji i przyjęcie przepisów prawa krajowego rozstrzygających problematykę współpracy między organem nadzorczym a organem ochrony konkurencji celem uniknięcia sporów kompetencyjnych, dualizmu rozstrzygnięć lub rozstrzygnięć godzących w prawidłową realizację przepisów RODO[375].

- **C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer*** – w wyroku TSUE wskazał, że aby przepis prawny uznać za bardziej szczegółowy, w rozumieniu art. 88 ust. 1 RODO, to musi on spełniać warunki określone w ust. 2 tego artykułu. W konsekwencji TSUE stwierdził, że art. 88 ust. 1 i 2 RODO należy interpretować w ten sposób, że należy odstąpić od stosowania przepisów krajowych przyjętych w celu zapewnienia ochrony praw i wolności pracowników w zakresie przetwarzania ich danych osobowych w związku z zatrudnieniem, jeżeli przepisy te nie spełniają warunków i ograniczeń określonych w tym art. 88 ust. 1 i 2, chyba że przepisy te stanowią podstawę prawną, o której mowa w art. 6 ust. 3 tego rozporządzenia, zgodną z przewidzianymi w nim wymogami. W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[376].
- **C-300/21 *Österreichische Post*** – TSUE stwierdził, że art. 82 ust. 1 RODO należy interpretować w ten sposób, że samo naruszenie przepisów rozporządzenia nie wystarcza do przyznania prawa do odszkodowania. TSUE uznał, że art. 82 RODO należy rozumieć w ten sposób, iż w celu ustalenia kwoty odszkodowania należnego z tytułu ustanowionego w tym artykule prawa do odszkodowania, sądy krajowe powinny stosować wewnętrzne przepisy każdego państwa członkowskiego dotyczące zakresu odszkodowania pieniężnego, pod warunkiem przestrzegania zasad równoważności i skuteczności prawa Unii. W ocenie organu nadzorczego

[375] DOL.0623.10.2021.
[376] DOL.0623.3.2021.

wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[377].

- **C-659/22 *Ministerstvo zdravotnictví*** – zdaniem Trybunału należy uznać, że weryfikacja ważności interoperacyjnych zaświadczeń o szczepieniu, wyniku testu i powrocie do zdrowia w związku z COVID-19 przy użyciu krajowej czeskiej aplikacji „čTečka" stanowi przetwarzanie w rozumieniu art. 4 pkt 2 RODO i jest objęte zakresem zastosowania tego rozporządzenia, zgodnie z jego art. 2 ust. 1. W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[378].
- **C-307/22 FT** – TSUE stwierdził, że art. 12 ust. 5 oraz art. 15 ust. 1 i 3 RODO „należy interpretować w ten sposób, że na administratorze ciąży obowiązek bezpłatnego dostarczenia osobie, której dane dotyczą, pierwszej kopii jej danych osobowych podlegających przetwarzaniu, nawet jeśli jej wniosek jest uzasadniony celem niezwiązanym z celami wskazanymi w motywie 63 zdanie pierwsze wspomnianego rozporządzenia". Odnośnie do drugiego pytania prejudycjalnego TSUE orzekł, że „art. 23 ust. 1 lit. i) RODO należy interpretować w ten sposób, że zakresem stosowania tego przepisu mogą być objęte przepisy krajowe przyjęte przed wejściem w życie tego rozporządzenia. Jednakże taka możliwość nie pozwala na przyjęcie przepisów krajowych obciążających – w celu ochrony interesów gospodarczych administratora – osobę, której dane dotyczą, kosztami pierwszej kopii jej danych osobowych podlegających temu przetwarzaniu". W odpowiedzi na kolejne pytanie TSUE uznał, że „art. 15 ust. 3 zdanie pierwsze RODO należy interpretować w ten sposób, że w ramach relacji lekarz–pacjent prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu oznacza przekazanie osobie, której dane dotyczą, wiernego i zrozumiałego odwzorowania wszystkich tych danych. Prawo to zakłada prawo do uzyskania pełnej kopii znajdujących się w jej aktach medycznych dokumentów, które zawierają między innymi wspomniane dane, jeżeli dostarczenie takiej kopii jest konieczne, aby umożliwić osobie, której dane dotyczą, sprawdzenie ich dokładności i kompletności oraz aby zagwarantować ich zrozumiałość. Co się tyczy danych odnoszących się do zdrowia osoby, której dane dotyczą, prawo to obejmuje w każdym razie prawo do uzyskania kopii danych z dokumentacji medycznej zawierającej informacje, takie jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi w odniesieniu do tej osoby". W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[379].
- **C-683/21 *Nacionalinis visuomenės sveikatos centras*** – w przedmiocie pytań dotyczących art. 4 ust. 7 ogólnego rozporządzenia o ochronie danych TSUE stwierdził, że artykuł ten należy rozumieć w ten sposób, że „za administratora w rozumieniu tego przepisu można uznać podmiot, który zlecił danemu przedsiębiorstwu opracowanie mobilnej aplikacji informatycznej i który w tym kontekście uczestniczył w określaniu celów oraz sposobów przetwarzania danych

[377] DOL.0623.12.2021.
[378] DOL.0623.27.2022.
[379] DOL.0623.18.2022.

osobowych dokonywanego za pośrednictwem tej aplikacji, nawet jeśli ów podmiot sam nie przeprowadził operacji przetwarzania takich danych, nie udzielił wyraźnej zgody na realizację konkretnych operacji takiego przetwarzania lub na publiczne udostępnienie wspomnianej aplikacji mobilnej i nie nabył tejże aplikacji mobilnej, chyba że przed tym publicznym udostępnieniem wspomniany podmiot wyraźnie sprzeciwił się temu udostępnieniu i wynikłemu z niego przetwarzaniu danych osobowych". Ponadto TSUE orzekł, że „uznanie dwóch podmiotów za współadministratorów nie zakłada ani istnienia uzgodnień między tymi podmiotami w przedmiocie ustalania celów i sposobów przetwarzania danych osobowych, ani istnienia uzgodnień ustalających warunki odnoszące się do współadministrowania danymi". Art. 4 pkt 2 RODO, zdaniem TSUE, należy interpretować w ten sposób, że „wykorzystywanie danych osobowych do celów testowania systemów informatycznych zintegrowanych z aplikacją mobilną stanowi „przetwarzanie w rozumieniu tego przepisu, chyba że takie dane zostały zanonimizowane w taki sposób, że osoby, której te dane dotyczą, nie można lub już nie można zidentyfikować, lub chyba że chodzi o dane fikcyjne, które nie odnoszą się do istniejącej osoby fizycznej". Odnośnie do interpretacji art. 83 RODO TSUE stwierdził, że „administracyjna kara pieniężna może zostać nałożona na podstawie tego przepisu wyłącznie wtedy, gdy zostanie wykazane, że administrator dopuścił się, umyślnie lub nieumyślnie, naruszenia, o którym mowa w ust. 4–6 tego artykułu". Ponadto TSUE stwierdził, że „taka kara pieniężna może zostać nałożona na administratora danych w związku z operacjami przetwarzania danych osobowych dokonywanymi przez podmiot przetwarzający w jego imieniu, z wyjątkiem sytuacji, gdy w ramach tych operacji podmiot przetwarzający dokonywał przetwarzania danych do swoich własnych celów lub przetwarzał te dane w sposób niezgodny z ramami lub sposobami przetwarzania określonymi przez administratora lub w taki sposób, że nie można racjonalnie uznać, że administrator ten wyraził na to zgodę". W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[380].

- **C-807/21 *Deutsche Wohnen*** – TSUE w wyroku stwierdził, że art. 58 ust. 2 lit. i) oraz art. 83 ust. 1–6 RODO należy rozumieć w ten sposób, że stoją one na przeszkodzie uregulowaniu krajowemu, na mocy którego administracyjna kara pieniężna może zostać nałożona na osobę prawną działającą w charakterze administratora danych za naruszenie, o którym mowa w art. 83 ust. 4–6 tego rozporządzenia, tylko wtedy, gdy naruszenie to zostało uprzednio przypisane zidentyfikowanej osobie fizycznej. Art. 83 RODO należy interpretować w ten sposób, że administracyjna kara pieniężna może zostać nałożona na podstawie tego przepisu wyłącznie wtedy, gdy zostanie wykazane, że administrator danych, będący jednocześnie osobą prawną i przedsiębiorstwem, dopuścił się, umyślnie lub nieumyślnie, naruszenia, o którym mowa w ust. 4–6 tego artykułu. W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[381].

[380] DOL.0623.27.2021.
[381] DOL.0623.3.2022.

- **C-162/22 *Lietuvos Respublikos generalinė prokuratura*** – TSUE w wyroku wskazuje, iż art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[382], należy interpretować w ten sposób, iż stoi on na przeszkodzie temu, aby dane osobowe dotyczące łączności elektronicznej, które na podstawie środka ustawowego przyjętego na mocy tego przepisu zostały zatrzymane przez dostawców usług łączności elektronicznej, i które zostały następnie udostępnione na podstawie tego środka organom właściwym do zwalczania poważnej przestępczości, mogły być wykorzystywane w ramach dochodzeń dotyczących przewinień dyscyplinarnych związanych z korupcją. W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[383].
- **C-60/22 *Bundesrepublik Deutschland*** – TSUE wskazał, iż naruszenie art. 26 i 30 RODO przez administratora danych nie stanowi „niezgodnego z prawem przetwarzania" w rozumieniu art. 17 ust. 1 lit. d) lub art. 18 ust. 1 lit. b) rozporządzenia w związku z jego art. 5 ust. 1 lit. a) i art. 6 ust. 1 akapit pierwszy, uprawniającego osobę, której dane dotyczą, do żądania usunięcia jej danych lub ograniczenia przetwarzania. Trybunał wskazał, że prawo Unii należy interpretować w ten sposób, że w sytuacji, gdy administrator danych naruszył obowiązki spoczywające na nim na mocy art. 26 i 30 RODO, uwzględnienie przez sąd krajowy takich danych nie jest uzależnione od zgody osoby, której dane dotyczą. W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[384].
- **C-579/21 *Pankki S*** – stanowisko wyrażone przez TSUE wskazuje, iż art. 15 ust. 1 RODO powinien być interpretowany w ten sposób, iż przepis ten nie ustanawia prawa dostępu w odniesieniu do informacji dotyczących tożsamości pracowników administratora danych, chyba że informacje te są niezbędne do umożliwienia osobie, której dane dotyczą, skutecznego wykonywania praw przyznanych jej przez to rozporządzenie i pod warunkiem, że uwzględnione zostaną prawa i wolności pracowników. Ponadto TSUE podkreślił, iż pracowników administratora nie można uznać za „odbiorców" w rozumieniu art. 15 ust. 1 lit. c) RODO. W zakresie kolejnego z pytań prejudycjalnych TSUE stwierdził, że art. 15 ust. 1 RODO należy interpretować w ten sposób, że okoliczność, iż administrator prowadzi działalność bankową regulowaną i że osoba, której dane osobowe jako klienta administratora były przetwarzane, była również pracownikiem tego administratora, nie ma co do zasady wpływu na zakres prawa przysługującego tej osobie na podstawie tego przepisu. TSUE wskazał, iż art. 15 RODO w zw. z art. 99 ust. 2 tego rozporządzenia należy interpretować w ten sposób, że ma on zastosowanie do żądania udzielenia dostępu do informacji, o których mowa w tym przepisie, gdy operacje przetwarzania, których dotyczy to żądanie, zostały dokonane przed datą rozpoczęcia stosowania tego rozporządzenia, ale żądanie zostało złożone po tej dacie. W ocenie organu

[382] Dz. Urz. UE L Nr 201, str. 37.
[383] DOL.0623.12.2022.
[384] DOL.0623.7.2022.

nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[385].

- **C-487/21 *Österreichische Datenschutzbehörde et CRIF*** – TSUE w wyroku uznał, iż pojęcie „kopii" nie dotyczy ścisłej formy dostarczenia kopii danych i powinno być rozumiane szeroko. Prawo do uzyskania od administratora kopii danych osobowych podlegających przetwarzaniu oznacza przekazanie osobie, której dane dotyczą, wiernej i zrozumiałej kopii wszystkich oryginałów tych danych. Prawo to obejmuje prawo do uzyskania kopii fragmentów dokumentów lub całych dokumentów, lub też wyciągów z baz danych, które zawierają między innymi te dane, jeżeli dostarczenie takiej kopii jest niezbędne do umożliwienia osobie, której dane dotyczą, skutecznego wykonywania praw przyznanych jej przez RODO, przy czym wymaga podkreślenia, że należy w tym przedmiocie uwzględnić prawa i wolności innych osób. TUSE orzekł, iż art. 15 ust. 3 zdanie trzecie RODO należy interpretować w ten sposób, że: pojęcie „informacji", o którym mowa w tym przepisie, odnosi się wyłącznie do danych osobowych, których kopię administrator musi dostarczyć, zgodnie ze zdaniem pierwszym tego ustępu, tj. danych osobowych podlegających przetwarzaniu. Podkreślił również, iż żaden przepis RODO nie ustanawia odmiennego traktowania wniosku w zależności od formy, w jakiej został on złożony, w związku z czym zakres prawa do uzyskania kopii nie może różnić się w zależności od tej formy. W ocenie organu nadzorczego wskazany wyrok nie skutkował koniecznością dokonania zmian w polskim prawie[386].

6. Przekazywanie danych osobowych poza EOG

W analizowanym 2023 r. polski organ nadzorczy uczestniczył w ramach EROD w procedurach przyjmowania opinii na temat projektów decyzji organów nadzorczych z Europejskiego Obszaru Gospodarczego (EOG) dotyczących projektów Wiążących Reguł Korporacyjnych (WRK). Współpraca organów nadzorczych z EOG w toku procedury zatwierdzania WRK odbywa się z uwzględnieniem mechanizmu spójności przewidzianego w art. 63 RODO, po zasięgnięciu opinii Europejskiej Rady Ochrony Danych.

W 2023 r. polski organ nadzorczy został członkiem zespołu mającego przygotować opinię EROD dotyczącą projektu decyzji jednego z organów nadzorczych z EOG w sprawie zatwierdzenia projektu WRK. Prace wspomnianego zespołu będą finalizowane w 2024 r.[387]

Przedstawiciele UODO w 2023 r. brali udział w comiesięcznych spotkaniach podgrupy roboczej Europejskiej Rady Ochrony Danych – Transfery Międzynarodowe. Urząd udzielał również wielu odpowiedzi w ramach wymiany opinii z innymi organami nadzorczymi.

W omawianym okresie sprawozdawczym kontynuowane były rozmowy odnośnie do propozycji EROD dotyczącej usprawnień procedur, współpracy transgranicznej i harmonizacji działań krajowych organów ochrony danych osobowych na poziomie

[385] DOL.0623.20.2021.
[386] DOL.0623.24.2021.
[387] ZAS.46.15.2019.

unijnym[388]. Urząd wyraził również opinię na temat decyzji o adekwatności odnośnie do Stanów Zjednoczonych[389].

W 2023 r. Urząd otrzymał jedno zapytanie dotyczące wystąpienia jako organ wiodący (Lead Authority) przy tworzeniu WRK dla administratorów danych osobowych[390]. Kontynuowane były dwa postępowania dotyczące WRK, jedno dla administratorów danych osobowych[391], a drugie dla podmiotów przetwarzających[392].

W jednej ze spraw, po wcześniejszym wyjaśnieniu ewentualnych wątpliwości co do kwestii dotyczących ubiegania się o zatwierdzenie WRK, pewna grupa kapitałowa przedłożyła wnioski o zatwierdzenie wiążących reguł korporacyjnych dla administratorów oraz wiążących reguł korporacyjnych dla podmiotów przetwarzających. Mając na uwadze potrzebę ustalenia organu wiodącego dla tych WRK, polski organ nadzorczy zwrócił się do innych organów nadzorczych z prośbą o zgłaszanie ewentualnych zastrzeżeń co do działania polskiego organu nadzorczego w charakterze organu wiodącego w procedurach mających na celu zatwierdzenie wspomnianych WRK. Ze względu na brak zastrzeżeń, polski organ nadzorczy został organem wiodącym w przedmiotowych procedurach. Pod koniec roku do Urzędu wpłynęły projekty dokumentacji dotyczącej obu wspomnianych wyżej WRK. Obecnie są one analizowane[393].

Organ nadzorczy otrzymał ponadto **21 zapytań od innych organów nadzorczych odnośnie do Wiążących Reguł Korporacyjnych** (w ponad 60 różnych grupach kapitałowych) dla administratorów danych osobowych i podmiotów przetwarzających[394].

Wspomniane wyżej informacje i zapytania od organów nadzorczych z EOG dotyczyły zgłoszenia ewentualnych zastrzeżeń odnośnie do ustanowienia organu wiodącego w ramach danej procedury zatwierdzania WRK, ewentualnych komentarzy do projektu konkretnych wiążących reguł korporacyjnych (ich skonsolidowanego projektu, będącego rezultatem współpracy organu wiodącego i współrecenzentów), czy też ewentualnych komentarzy do zaktualizowanych wersji już zatwierdzonych WRK.

Jak już wspomniano wcześniej, w 2023 r. polski organ nadzorczy analizował w charakterze współrecenzenta[395] projekty wiążących reguł korporacyjnych, przedstawione przez grupy kapitałowe i sporządzał stosowne analizy dokumentacji dotyczącej projektów WRK w ramach dwóch odrębnych procedur zatwierdzania wiążących reguł korporacyjnych prowadzonych przez dwa organy wiodące z EOG[396].

Przedstawiciel Prezesa UODO uczestniczył również w spotkaniach podgrupy EROD dotyczących przekazywania danych osobowych do państw trzecich, w ramach których

[388] DOL.4413.29.2022.
[389] DOL.401.325.2023.
[390] DOL.4413.17.2023.
[391] DOL.4413.13.2023.
[392] DOL.4413.14.2023.
[393] DOL.4413.3.2023, DOL.4413.7.2023, DOL.4413.22.2022.
[394] ZAS.46.16.2018, ZAS.46.11.2019, ZAS.46.15.2019, ZAS.46.53.2019, DOL.4413.20.2020, DOL.4413.25.2020, DOL.4413.11.2021, DOL.4413.4.2022, DOL.4413.2.2023, DOL.4413.4.2023, DOL.4413.5.2023, DOL.4413.6.2023, DOL.4413.8.2023, DOL.4413.9.2023, DOL.4413.10.2023, DOL.4413.11.2023, DOL.4413.15.2023, DOL.4413.16.2023, DOL.4413.18.2023, DOL.4413.22.2023, DOL.614.18.2023.
[395] Ang. *co-reviewer*.
[396] DOL.4413.11.2022 i DOL.4413.19.2023.

wypracowywane były wspólne stanowiska EROD wzmacniające ochronę danych osobowych przekazywanych do państw trzecich.

7. Inne sprawy

W 2023 r. organ właściwy w sprawie ochrony danych osobowych zajmował się również sprawami – zarówno o zasięgu krajowym, jak i międzynarodowym – dotyczącymi innych kwestii niż te wskazane powyżej.

W ramach prac w **podgrupie eksperckiej Social Media**, poza projektami wytycznych dotyczących korzystania z mediów społecznościowych przez organy publiczne i konsultowanymi wcześniej materiałami, omawiano także sprawy związane z portalami społecznościowymi (m.in. TikTok, Facebook, korzystanie z reklamy politycznej, ochrona danych a ochrona konsumentów). Rozpoczęto również prace nad projektem wytycznych o relacji Aktu o usługach cyfrowych (DSA) i RODO. Przedstawiciele UODO aktywnie angażowali się ponadto w prace eksperckiej podgrupy CEH (Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia Europejskiej Rady Ochrony Danych[397]) związane z certyfikacją.

W 2023 r. UODO otrzymywał regularnie różnego rodzaju informacje z ministerstw dotyczące udziału RP w pracach organizacji i organów współpracy międzynarodowej, negocjacji umów wielostronnych itp., które mogły mieć związek z przetwarzaniem danych osobowych. W sprawach tych przekazywał swoje uwagi, jak np. do 9. wersji projektu modelowych klauzul umownych dla transferu danych osobowych między administratorami opracowywanego przez Komitet Konsultacyjny Konwencji 108 Rady Europy[398], czy komentarze do projektu Modułu 2. projektu modelowych klauzul umownych dla transferu danych osobowych między administratorem a podmiotem przetwarzającym opracowywanego przez Komitet Konsultacyjny Konwencji 108 Rady Europy[399].

Udział w pracach Committee of Experts on the Integrity of Online Information (MSI–INF)

Urząd Ochrony Danych Osobowych, jako członek Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, jeszcze w 2022 r. został zaproszony jako obserwator prac **Komitetu Ekspertów ds. Integralności Informacji Online (MSI–INF)** – organu podległemu pod Komitet Sterujący ds. Mediów i Społeczeństwa Informacyjnego Rady Europy, CDMSI – nad projektem wytycznych w sprawie przeciwdziałania rozprzestrzenianiu się nieprawdziwych informacji i dezinformacji w Internecie poprzez weryfikację faktów oraz rozwiązania w zakresie projektowania platform w sposób zgodny z prawami człowieka.

W dniach 27–28 marca 2023 r. odbyło się trzecie spotkanie (w formule hybrydowej) z udziałem online przedstawiciela UODO, podczas którego komitet omówił przyszłe kroki związane z projektem i uzasadnieniem uzupełniającym wytyczne. Jeśli chodzi o projekt wytycznych, MSI–INF zgodził się, że jest on obecnie na bardzo zaawansowanym etapie

[397] Compliance, e-Government and Health – CEH.
[398] DWME.622.2.2023.
[399] DWME.622.3.2023.

i wymaga jedynie drobnych poprawek w brzmieniu niektórych zwrotów. Natomiast, w przypadku uzasadnienia towarzyszącego projektowi wytycznych, uzgodniono, że sprawozdawcy będą kontynuować prace zgodnie z otrzymanymi uwagami i sugestiami.

W dniach 18–19 września 2023 r. odbyło się czwarte posiedzenie, ale już w formule stacjonarnej. Dyskusja koncentrowała się na finalizacji projektu wytycznych w sprawie przeciwdziałania rozprzestrzenianiu się fałszywych informacji i dezinformacji w Internecie poprzez weryfikację faktów i rozwiązania w zakresie projektowania platform w sposób zgodny z prawami człowieka oraz projektu uzasadnienia towarzyszącego wytycznym. Komitet Ekspertów osiągnął porozumienie w sprawie treści obu dokumentów, których przygotowanie zostało mu powierzone.

Na 24. posiedzeniu plenarnym (29 listopada – 1 grudnia 2023 r.) Komitet Sterujący ds. Mediów i Społeczeństwa Informacyjnego (CDMSI) przyjął Wytyczne dotyczące przeciwdziałania rozprzestrzenianiu się dezinformacji i nieprawdziwych informacji w Internecie poprzez weryfikację faktów i rozwiązania w zakresie projektowania platform w sposób zgodny z prawami człowieka oraz uzasadnienie, opracowane przez podległy mu organ, Komitet Ekspertów ds. integralności informacji online (MSI–INF). Instrument ten, oparty na trzech filarach: weryfikacji faktów, rozwiązaniach w zakresie projektowania platform i wzmocnieniu pozycji użytkowników, zawiera praktyczne wskazówki i zalecenia dla decydentów oraz zainteresowanych stron dotyczące przeciwdziałania rozpowszechnianiu dezinformacji i dezinformacji w Internecie.

Udział w pracach Digital Education Working Group

Inicjatywa powstała w 2009, a jej koordynatorem jest CNIL (francuski organ ochrony danych). Urząd Ochrony Danych Osobowych jest członkiem grupy od samego początku działalności. Głównym celem grupy jest promowanie edukacji cyfrowej, która szanuje prawa i wolności wszystkich osób oraz podnoszenie świadomości na temat korzystania z praw cyfrowych przez dzieci. Nadrzędnym celem jest umożliwienie dzieciom rozwijania kompetencji i umiejętności potrzebnych do stania się odpowiedzialnymi cyfrowymi obywatelami.

Ostatnie spotkanie grupy odbyło się online 29.11.2023 r. z udziałem przedstawiciela UODO. W 2023 r. UODO był zaangażowany w realizację planu działań na lata 2023–2024.

Udział w pracach International Age Assurance Working Group

Inicjatywa powstała w 2022 r., a koordynatorem grupy jest ICO (brytyjski organ ochrony danych). Urząd Ochrony Danych Osobowych dołączył do grupy podczas spotkania online, które odbyło się 14.11.2023 r. z udziałem przedstawiciela polskiego organu. Grupa zajmuje się kwestiami dotyczącymi nowych technologii związanymi z weryfikacją wieku, a dokładniej z ochroną prywatności dzieci w Internecie. Podczas listopadowego spotkania wyznaczono na 2024 rok trzy wstępne cele:

- dzielenie się spostrzeżeniami na temat ograniczeń wiekowych;
- promowanie harmonizacji, tam gdzie to możliwe, w celu zapewnienia większej pewności regulacyjnej dla usług online;
- opublikowanie wspólnego oświadczenia w sprawie kontroli wieku.

8. Wizyta studyjna

Urząd Ochrony Danych Osobowych 16 marca 2023 r. gościł przedstawicieli Komisarza Parlamentu Ukrainy ds. Praw człowieka. W spotkaniu wzięli udział także przedstawiciele hiszpańskiego organu nadzorczego i koordynatorka programu EU4DigitalUA, którego celem jest rozwój cyfryzacji Ukrainy, w tym wsparcie w dostosowaniu ukraińskich przepisów ochrony danych osobowych do ram prawnych UE.

Spotkanie to odbyło się w związku z konferencją międzynarodową „Dostosowanie ochrony danych do ram prawnych UE. Otwieranie Ukrainie drogi do bezpieczniejszej przyszłości", zorganizowaną w Warszawie 14 i 15 marca 2023 r. przez Komisarza Parlamentu Ukrainy ds. Praw człowieka, we współpracy z koordynatorami projektu EU4DigitalUA. Konferencja ta miała na celu wsparcie Ukrainy w dostosowaniu jej prawa ochrony danych osobowych do ram prawnych UE.

Polska od ponad 20 lat współpracuje z Ukrainą w ramach Grupy Państw Europy Środkowej i Wschodniej, do której Ukraina, wraz z Mołdawią i Armenią, dołączyła w 2016 r. Wyrazem dobrej współpracy jest także zawarte w 2019 r. porozumienie między ówczesną Komisarz ds. Praw człowieka Parlamentu Ukrainy i Prezesem Urzędu Ochrony Danych Osobowych. Porozumienie zakłada konsolidację wysiłków naszych organów w propagowaniu norm w obszarze praw i podstawowych wolności człowieka, praworządności i rozwoju demokratycznego.

Podczas spotkania w siedzibie UODO uczestnicy wymienili się informacjami dotyczącymi organizacji organu i podejmowanych przez niego działań, a także doświadczeniami związanymi z wdrażaniem RODO. Eksperci UODO podkreślali, że nawet po prawie pięciu latach stosowania RODO w dalszym ciągu istnieje wiele obszarów, które wymagają dalszej pracy. Dlatego konieczne są szkolenia czy współpraca z innymi podmiotami administracji publicznej na rzecz edukacji w zakresie ochrony danych osobowych oraz lepszej jakości nowych regulacji prawnych, które powinny zawierać rzetelnie przeprowadzoną ocenę skutków dla ochrony danych.

9. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2023 r. Prezes UODO i jego przedstawiciele uczestniczyli 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) Spotkania Sieci Inspektorów Ochrony Danych (DPO Network) – online 7.03.2023 r., 25.09.2023 r.

Niezależna sieć inspektorów ochrony danych, której prace koordynuje EROD, składa się z IOD każdego z organów nadzorczych, inspektora ochrony danych EROD i inspektora ochrony danych EIOD. W 2023 r. Sieć IOD spotkała się 2 razy w formule online. W wydarzeniach tych uczestniczył Inspektor Ochrony Danych Urzędu Ochrony Danych Osobowych.

2) 31. Wiosenna Konferencja Europejskich Organów Ochrony Danych, Budapeszt, 10–12.05.2023 r.

Wiosenne Konferencje są najważniejszym, corocznym spotkaniem wszystkich rzeczników ochrony danych osobowych z państw członkowskich UE, innych państw

europejskich oraz przedstawicieli Komisji Europejskiej, Rady Europy, jak też innych organów zajmujących się ochroną danych osobowych. Poszczególne konferencje poświęcone są różnym aspektom ochrony danych osobowych w Europie, a ich uczestnicy podejmują działania ukierunkowane nie tylko na wdrażanie unijnych przepisów, ale również na monitorowanie ich przestrzegania w poszczególnych krajach. Wiosenną Konferencję, która odbyła się 10–12 maja 2023 r. w Budapeszcie, na Węgrzech, zorganizował Krajowy Organ Ochrony Danych i Wolności Informacji Węgier.

Konferencja została podzielona na sesję zamkniętą, na którą zarejestrowało się 138 członków, oraz sesję otwartą, w której udział wzięło 358 uczestników niebędących członkami, z 39 krajów. W wydarzeniu udział wzięła również przedstawicielka Urzędu Ochrony Danych Osobowych. Sesja zamknięta objęła cztery tematy: nowe technologie, prawo konkurencji, orzecznictwo sądowe i najlepsze praktyki/studia przypadków w zakresie współpracy przy egzekwowaniu prawa między krajami EOG i krajami spoza EOG. Po raz pierwszy podczas Wiosennej Konferencji inspektorzy ochrony danych (IOD) mieli możliwość wzięcia udziału w otwartej sesji w formule online lub osobiście. Panele koncentrowały się na relacjach IOD z organem ochrony danych, sieci IOD i szkoleniach IOD oraz roli IOD w organizacji. Konferencja stanowiła doskonałą okazję do wymiany poglądów i doświadczeń. Członkowie przyjęli trzy rezolucje. W ***Rezolucji w sprawie potrzeby wzmocnionej współpracy w dziedzinie ochrony danych i prawa konkurencji*** europejskie organy ochrony danych postanowiły m.in. zobowiązać się do działania w sposób jednolity oraz wzmocnić współpracę w celu osiągnięcia postępów zarówno w zakresie ochrony podstawowych praw: do prywatności, ochrony danych osobowych i uczciwej konkurencji, a także potwierdzić swoje dążenie do wzmocnienia współpracy i wymiany informacji z organami ochrony konkurencji, aby osiągnąć ten cel. Członkowie przyjęli ***Rezolucję w sprawie akredytacji organu ochrony danych San Marino*** jako członka Konferencji Europejskich Organów Ochrony Danych ze statusem krajowego organu ochrony danych oraz ***Rezolucję w sprawie rewizji regulaminu Konferencji.*** Podczas wydarzenia ogłoszono, że gospodarzem 32. Wiosennej Konferencji w 2024 r. będzie organ ochrony danych Łotwy.

3) 44. posiedzenie plenarne Komitetu Konsultacyjnego Konwencji 108 Rady Europy, Strasburg, 14–16.06.2023 r.

14–16 czerwca 2023 r. w Strasburgu odbyło się 44. posiedzenie plenarne Komitetu Konsultacyjnego ds. Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitetu T-PD), z udziałem przedstawiciela UODO. Członkiem Komitetu T-PD z ramienia Rzeczypospolitej Polskiej jest Urząd Ochrony Danych Osobowych.

Posiedzenie zgromadziło przedstawicieli z ponad 70 krajów oraz instytucji krajowych i międzynarodowych w celu kontynuowania prac rozpoczętych w ramach programu prac Komitetu Konwencji 108 na lata 2022–2025, w szczególności w zakresie interpretacji art. 11 Konwencji 108+ oraz Wytycznych dotyczących ochrony danych, w tym danych biometrycznych, w ramach głosowania i wyborów.

Podczas posiedzenia przyjęto dwa ważne dokumenty, które przyczyniają się do wdrożenia Konwencji 108+:

- Wytyczne w sprawie ochrony danych przy przetwarzaniu danych osobowych do celów przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu;

- Wzorcowe Klauzule Umowne dotyczące przekazywania danych osobowych.

Uczestnicy posiedzenia omówili także pierwszy projekt wytycznych w sprawie ochrony danych, w szczególności podczas korzystania z danych biometrycznych, w ramach głosowania i wyborów. Podczas tego spotkania komitet wręczył nagrody laureatom kolejnej edycji nagrody im. Stefano Rodotà 2023: Janis Wong, Dr. Gabriela Zanfir-Fortuna, Sebastiao Bernardo Bruco Geraldes de Barros Vale i Katerina Demetzou, którzy zaprezentowali uczestnikom swoje nagrodzone prace.

4) 45. posiedzenie plenarne Komitetu Konsultacyjnego Konwencji 108 Rady Europy, Strasburg, 16–17.11.2023 r.

15–17 listopada 2023 r. w Strasburgu odbyło się 45. posiedzenie plenarne Komitetu Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Komitet T-PD), w którym uczestniczył przedstawiciel Urzędu Ochrony Danych Osobowych.

Jednym z głównych punktów posiedzenia było dokonanie przez Republikę San Marino ratyfikacji Protokołu zmieniającego Konwencję 108, z okazji 35. rocznicy przystąpienia tego kraju do Rady Europy. Tym samym Republika San Marino stała się 31. państwem, które przystąpiło do zmodernizowanej Konwencji 108+.

Posiedzenie plenarne T-PD, które zgromadziło uczestników z około 70 krajów, instytucji krajowych i międzynarodowych, zaowocowało przyjęciem drugiego modułu wzorcowych klauzul umownych, dotyczącego międzynarodowego przekazywania danych osobowych od administratora do podmiotu przetwarzającego. Dokument uzupełnia pierwszy moduł wzorcowych klauzul umownych, który dotyczył międzynarodowego przekazywania danych osobowych od administratora do administratora, przyjęty przez Komitet T-PD 16 czerwca 2023 r. Dzięki drugiemu modułowi właściwe organy mogą wstępnie zatwierdzać międzynarodowe przekazywanie danych osobowych przy zapewnieniu spójności z globalnymi standardami ochrony danych. Komitet pracuje obecnie nad trzecim modułem poświęconym przekazywaniu danych osobowych od podmiotu przetwarzającego do podmiotu przetwarzającego.

Komitet T-PD kontynuował prace nad wytycznymi dotyczącymi ochrony osób fizycznych w związku z przetwarzaniem danych osobowych do celów rejestracji wyborców i uwierzytelniania, a także nad interpretacją art. 11 zmodernizowanej Konwencji 108+. Podjęto również decyzję o rozpoczęciu prac nad ochroną danych w kontekście neuronauki, w ramach programu prac na lata 2022–2025.

Dodatkowo Komitet T-PD, po rezygnacji jednego z członków biura w październiku 2023 r., wybrał Panią Virpi Koivu, reprezentującą rząd fiński w Komitecie T-PD Finlandii, na pozostałą część kadencji jej poprzednika, tj. do listopada 2024 r.

V. Charakterystyka działalności UODO i wyzwania na przyszłość

Analiza spraw prowadzonych w roku 2023 pozwala na przyjęcie wniosku, że realizowane od chwili rozpoczęcia stosowania RODO konsekwentne działania organu nadzorczego, zapewniające wielu różnym środowiskom wsparcie eksperckie na etapie tworzenia oraz stosowania prawa, przynoszą zamierzone rezultaty.

Z satysfakcją należy odnotować fakt, że dzięki podejmowanym przez urząd działaniom, takim jak przedstawianie opinii w toku **procesów legislacyjnych czy kierowanie wystąpień legislacyjnych,** udało się zapobiec wejściu w życie lub wyeliminować z obrotu prawnego przepisy nieprzejrzyste, niezapewniające poszanowania gwarantowanych przez RODO praw osób, których dane są przetwarzane.

Na skutek uwag organu nadzorczego w toku prac legislacyjnych w przyjmowanych przepisach udało się wprowadzić wiele istotnych zmian. Przykładowo w projekcie ustawy o badaniach klinicznych stosowanych u ludzi[400] projektodawca zgodził się z koniecznością doprecyzowania tworzonych przepisów m.in. w zakresie wyłączeń stosowania przepisów RODO na rzecz jedynie ich ograniczenia, wskazując jednocześnie, na jakim konkretnym etapie badania prawa osób mogą być ograniczone. Omawiana ustawa, która weszła w życie 30 marca 2023 r., stanowi ciekawy przykład godzenia praw z zakresu badań klinicznych i ograniczenia praw osób, których dane mają być przetwarzane.

Uwagi organu nadzorczego zostały również uwzględnione w analizowanym projekcie ustawy o zmianie ustawy – Prawo o notariacie oraz niektórych innych ustaw[401]. Ustawodawca zrezygnował z rozszerzenia katalogu danych osobowych listy notariuszy prowadzonej przez Krajową Radę Notarialną w systemie teleinformatycznym i dodania do niej m.in. numerów PESEL i NIP notariuszy, zastępców notarialnych oraz notariuszy emerytowanych, jak i z wprowadzenia nowego rozwiązania w postaci upublicznienia podstaw prawnych zawieszenia notariusza w czynnościach zawodowych. Uwagi organu zostały uznane także we wprowadzonych przepisach ustawy o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw[402], w których zrezygnowano z przetwarzania danych za pomocą systemu teleinformatycznego prowadzonego przez Szefa Służby Cywilnej. Za pozytywną należy uznać także autorefleksję ustawodawcy w zakresie konieczności wprowadzenia do przepisów ustawy o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli – szczegółowych rozwiązań dotyczących przetwarzania danych osobowych[403], co postulował organ nadzorczy na etapie tworzenia przepisów tej ustawy.

Z kolei inne z zakładanych rozwiązań, co do których organ nadzorczy zgłaszał poważne wątpliwości, w ogóle nie weszły do porządku prawnego, m.in. z powodu zaprzestania prac nad nimi. Jako jeden z przykładów można podać projekt ustawy o aktywności zawodowej[404], który przewidywał przetwarzanie na ogromną skalę danych osobowych szczególnych kategorii oraz danych określonych w art. 10 RODO, które powinny podlegać szczególnemu reżimowi. Projektowane rozwiązania przewidywały

[400] DOL.401.196.2021.
[401] DOL.401.20.2023.
[402] DOL.401.134.2023.
[403] DOL.401.229.2023.
[404] DOL.401.483.2022.

zarówno profilowanie, jak i automatyczne przetwarzanie danych osobowych (bezrobotnych i poszukujących pracy, członków rodzin takich osób, młodzieży wspieranej przez Ochotnicze Hufce Pracy, przedsiębiorców, a także pracowników w publicznych służbach zatrudnienia oraz OHP). Na skutek uwag organu nadzorczego z projektu ustawy usunięto rozwiązania dotyczące scentralizowanej bazy tzw. „rejestru centralnego" i wprowadzono odrębny rozdział poświęcony przetwarzaniu danych osobowych. Niemniej projektowana regulacja wciąż budziła wiele zastrzeżeń, zwłaszcza odnośnie do profilowania i automatycznego przetwarzania.

Powyższe działania są przykładem na to, że przy tworzeniu prawa możliwe jest wypracowanie norm, które stanowią pewien balans pomiędzy koniecznością uregulowania określonych zagadnień (celu regulacji) a zachowaniem spójności z przepisami o ochronie danych. Niestety stanowią one niewielką część opiniowanych projektów.

Ponadto zauważyć należy, że niektóre organy publiczne – poprzez pominięcie procesu uzgodnień i opiniowania – nie przekazują istotnych projektów aktów normatywnych, dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie, do oceny organu nadzorczego. Jest to nie tylko działanie wbrew obowiązującym przepisom i obowiązkom, ale także utrata okazji do eksperckiego wsparcia projektodawcy przez organ nadzorczy na jak najwcześniejszym etapie procesu legislacyjnego. Niewątpliwie korzyści wynikające z takich konsultacji pod kątem ochrony danych pozwoliłyby na ograniczenie ryzyka tworzenia rozwiązań nieprzejrzystych czy niestanowiących gwarancji dla osób, których dane dotyczą.

W opinii organu nadzorczego nadal wiele przepisów oraz kwestii wymaga pogłębionej analizy, dyskusji oraz wprowadzenia stosownych zmian, czego wyrazem są m.in. wciąż sygnalizowane przez IOD problematyczne zagadnienia i luki w przepisach.

Nadal konieczny jest przegląd przepisów dotyczących wykorzystywania i upubliczniania numeru PESEL, który jest krajowym numerem identyfikacyjnym 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. Propozycje projektodawców nie nawiązywały w 2023 r. do tych zabezpieczeń i nie przewidywały w ogóle takich rozwiązań. Tymczasem ujawnienie numeru PESEL może powodować 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 narażone osoby, których PESEL jest powszechnie dostępny w rejestrach publicznych i to bez określenia żadnych dodatkowych warunków jego wykorzystywania. 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. Powyższy problem był wielokrotnie i systematycznie poruszany przez organ nadzorczy przy okazji opiniowania projektów aktów prawnych, jak i w toku realizacji innych zadań organu nadzorczego. W 2023 r. UODO wyraził swoje wątpliwości w tym zakresie, m.in. opiniując projekt ustawy o zmianie ustawy o statystyce

publicznej[405] czy kierując wystąpienie do Prezesa Zarządu Krajowej Rady Izb Rolniczych[406] zawierające wniosek o podjęcie działań mających na celu ograniczenie zakresu danych ujawnianych w spisie członków izby rolniczej uprawnionych do głosowania w wyborach do walnych zgromadzeń izb rolniczych (w tym numeru PESEL), który udostępniony jest do wglądu w siedzibie gminy. Jednocześnie zauważyć należy również, że z jednej strony w wielu przypadkach ta dana osobowa jest uznawana za konieczną do realizacji zakładanego celu i rozpowszechniana bez żadnych ograniczeń, a z drugiej wchodzą w życie przepisy umożliwiające zastrzeżenie numeru PESEL oraz nakładające obowiązek weryfikacji numeru PESEL w rejestrze zastrzeżeń przy zawieraniu określonych umów[407].

Szczególnie istotny, wymagający pogłębionej analizy i debaty w obliczu rozwoju nowych technologii oraz tworzonych nowych regulacji europejskich, jest aspekt ważenia ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze na etapie projektowania rozwiązań krajowych.

Niepokojącym trendem, który stale jest i nadal będzie przedmiotem szczególnego zainteresowania organu nadzorczego, jest tworzenie przepisów przewidujących przetwarzanie danych osobowych 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 rozporządzenia Ministra Cyfryzacji 2023 r. w sprawie szczegółowych warunków uwierzytelnienia z wykorzystaniem profilu mObywatel[408], do którego Prezes UODO, biorąc pod uwagę fakt, że dopuszcza ono uwierzytelnianie użytkownika aplikacji mObywatel przy użyciu danych biometrycznych, stanowiących dane szczególnej kategorii w rozumieniu RODO, zgłosił liczne uwagi podczas procesu legislacyjnego.

Dla organu nadzorczego wyzwaniem na 2024 rok będzie weryfikowanie zapewniania właściwej ochrony danych osobowych przetwarzanych przy użyciu: chmur, aplikacji, portali, wspólnych systemów czy innych rozwiązań informatycznych. Są one coraz powszechniej stosowane i – niestety – coraz częściej tworzone z pominięciem określonych w RODO zasad. Jest to niezwykle istotne, gdyż przepisy ogólnego rozporządzenia wymagają, by każde przetwarzanie danych osobowych było planowane z uwzględnieniem koncepcji ochrony danych (i prywatności) zarówno w fazie projektowania (*privacy by design*), jak i w czasie samego przetwarzania. W sytuacji gdy twórca przepisów przewiduje, że przetwarzanie danych osobowych będzie prowadzone z wykorzystaniem określonych rozwiązań informatycznych, to od samego początku, na każdym etapie projektowania ich wykorzystywania, powinien brać pod uwagę wpływ, jaki ich stosowanie będzie wywierało na prywatność osób, których dane dotyczą. Uwzględniać przy tym powinien także stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych, a jednocześnie tak zaprojektować planowane

[405] DOL.401.276.2022.
[406] DOL.413.8.2023.
[407] Ustawa z 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości (Dz. U. poz. 1394 ze zm.) – opiniowana przez Prezesa UODO pod sygnaturą DOL.401.610.2022.
[408] DOL.401.262.2023.

cyfrowe rozwiązania, by były odpowiednie dla konkretnego przypadku oraz pozbawione na jak najwyższym poziomie ryzyk naruszeń praw i wolności podmiotów danych. Pożądane jest, by **aspekt ważenia ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze brać pod uwagę już na etapie projektowania rozwiązań prawnych.**

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). Rozwiązania prawne powinny być skonstruowane tak, by z jednej strony wypełnianie celów prawodawcy następowało ze spełnieniem wskazanych w RODO funkcjonalności i zasad, a z drugiej strony pozwalało 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 i w związku z jakimi etapami operacji na danych osobowych jest odpowiedzialny za to przetwarzanie (w tym m.in. pozyskiwanie czy udostępnianie danych). Chcąc zwrócić na tę kwestię szczególną uwagę, UODO przygotował materiał „Ustawodawca powinien precyzyjne regulować korzystanie z rozwiązań informatycznych", który został opublikowany w „Biuletynie UODO" nr 2/04/23.

Wyzwaniem w roku 2024 będzie niewątpliwie zaangażowanie organu nadzorczego w postępowania legislacyjne zmierzające do zapewnienia stosowania w porządku krajowym europejskich aktów horyzontalnych – zwłaszcza z tzw. **pakietu cyfrowego** – w szczególności w kontekście potencjalnego odgrywania przez organ nadzorczy nowych ról instytucjonalnych.

Aktem, który wymagał będzie najpilniejszych prac legislacyjnych rządu z udziałem organu nadzorczego, jest **rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (Akt w sprawie zarządzania danymi).** Rozpoczęcie jego stosowania nastąpiło 24 września 2023 r. Organ nadzorczy w 2023 r. uczestniczył w pracach nad zapewnieniem jego stosowania w krajowym porządku prawnym – nowa odsłona tych rozwiązań będzie przedmiotem dalszych prac w roku 2024.

Drugim istotnym aktem jest **rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Akt o usługach cyfrowych).** Rozpoczęcie jego stosowania nastąpiło 17 lutego 2024 r.

W 2023 r. organ nadzorczy był zaangażowany w prowadzony przez rząd (resort cyfryzacji) projekt ustawy, a następnie (w nowej odsłonie) **projekt założeń projektu ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw** wdrażającej rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz

zmiany dyrektywy 2000/31/WE (Akt o usługach cyfrowych)[409]. W toku dalszych prac UODO będzie zabiegał, by zadania i kompetencje, które miałyby na nim spoczywać, były precyzyjnie określone.

Poprawa współpracy organów nadzorczych i harmonizacja stosowania i egzekwowania RODO to kolejne wyzwania na najbliższy czas. Projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania rozporządzenia (UE) 2016/679 będzie w 2024 r. przedmiotem szczególnego zainteresowania Prezesa UODO.

Do innych wyzwań zaliczyć można prawne uregulowanie kwestii ochrony prywatności i danych osobowych w związku ze stosowaniem tzw. *dark patterns,* tworzeniem szczegółowych profili, na podstawie których dobierany jest przekaz reklamowy czy budowa ogólnoeuropejskiego systemu tożsamości cyfrowej.

Po stronie sukcesów warto odnotować zatwierdzenie przez Prezesa UODO pod koniec 2023 r. kolejnego kodeksu postępowania – **Kodeksu postępowania dla sektora ochrony zdrowia** przygotowanego przez Polską Federację Szpitali – i udzielenie akredytacji podmiotowi, który będzie monitorował jego przestrzeganie. Warto podkreślić, że kodeksy postępowania to ważny instrument ułatwiający osiąganie zgodności z RODO i podnoszenie poziomu ochrony danych osobowych.

Dotychczasowe doświadczenia organu nadzorczego, zebrane w toku współpracy z inicjatywami kodeksowymi, dowodzą, że przygotowanie kodeksu postępowania to proces długotrwały i wymagający wytężonej, skrupulatnej pracy. Środowiska podejmujące się stworzenia tych dokumentów popełniają błędy, które często wpływają na wydłużenie procedury zatwierdzenia kodeksu, zawieszenie prac nad projektem, a nawet całkowite zaniechanie przygotowania takiego dokumentu[410].

---

[409] DOL.401.18.2023.

[410] Do najczęstszych błędów popełnianych przez środowiska pracujące nad projektami kodeksów postępowania należą:

- brak jasnego i zwięzłego uzasadnienia, w którym przedstawia się szczegółowe informacje o celu kodeksu, zakresie jego stosowania oraz sposobie, w jaki ułatwi on skuteczne stosowanie RODO;
- wnioskowanie o zatwierdzenie kodeksu przez podmiot, który nie reprezentuje większości sektora;
- brak podmiotu, który podjąłby się roli wnioskodawcy w postępowaniu o zatwierdzenie kodeksu;
- zbyt wąski zakres przeprowadzonych konsultacji (np. nieobejmujący w ogóle osób, których dane dotyczą – użytkowników albo klientów czy organizacji działających na ich rzecz) oraz przedstawianie zbyt szczegółowego sprawozdania z konsultacji;
- zbyt kompleksowe/szerokie podejście do zagadnień przetwarzania danych zamiast rozstrzygnięcia najważniejszych problemów sektora, co powoduje niemożność zatwierdzenia kodeksu ze względu na istnienie zbyt wielu kwestii spornych, które trudno jest rozstrzygnąć w jednym dokumencie (warto w tym miejscu zwrócić uwagę na brzmienie ust. 2 art. 40 RODO – wymieniono w nim zagadnienia, jakie mogą obejmować kodeksy postępowania, ale wyliczenie to ma charakter przykładowy i nie jest wyliczeniem wyczerpującym, tzn. nie wszystkie wskazane w nim zagadnienia muszą być uregulowane w kodeksie);
- przepisanie do kodeksie przepisów RODO lub ustawy o ochronie danych osobowych bez praktycznego wyjaśnienia ich stosowania;
- niewskazanie w kodeksie: przepisów sektorowych, wytycznych, opinii i stanowisk EROD w odniesieniu do konkretnego sektora lub konkretnej czynności przetwarzania, lub tylko ogólne ich wskazanie bez odniesienia się do konkretnych przepisów związanych z przetwarzaniem danych osobowych w sektorze, dla którego powstał kodeks,
- niepowoływanie się przez twórców na istniejące orzecznictwo rozstrzygające zagadnienia regulowane w kodeksie;
- brak wypracowania odpowiednich mechanizmów umożliwiających monitorowanie kodeksu.

Tym bardziej cieszy to, że w Polsce wraz z rozpoczęciem stosowania RODO wiele organizacji zainicjowało prace nad stworzeniem branżowych kodeksów postępowania. Złożone do organu nadzorczego wnioski o zatwierdzenie projektów kodeksów, ale też sygnały od inicjatyw, które rozpoczynają prace związane z opracowaniem tego mechanizmu rozliczalności, wskazują, że zarówno podmioty publiczne (np. sądy, jednostki samorządu terytorialnego), jak i prywatne (np. centra handlowe, hotelarze) dostrzegają potrzebę i zalety korzystania z tego typu narzędzia, które pozwoli im wykazać rozliczalność, o której mowa w art. 5 ust. 2 RODO.

Innym ważnym mechanizmem umożliwiającym wykazanie wywiązania się przez administratora lub podmiot przetwarzający z ciążących na nich obowiązków określonych w RODO jest **certyfikacja,** dokonywana przez podmioty certyfikujące, które będą posiadać stosowną akredytację udzieloną przez Polskie Centrum Akredytacji (PCA).

W związku z przyjętym w Polsce modelem certyfikacji zadaniem organu nadzorczego będzie również zatwierdzanie kryteriów certyfikacji, o których mowa w art. 42 ust. 5 RODO.

Niezmiennie dużą wagę organ nadzorczy będzie przywiązywał do **współpracy z inspektorami ochrony danych.** W jego ocenie niezmiernie ważną kwestią jest zarówno wspieranie IOD we właściwym wypełnianiu przez nich ich funkcji, w tym weryfikowanie przestrzegania przez podmioty powołujące IOD przepisów dotyczących ich funkcjonowania, jak też udzielanie im konsultacji we wszelkich sprawach, którymi się zajmują. Dlatego organ nadzorczy – tak jak dotąd – na bieżąco będzie udzielał odpowiedzi na pytania przesyłane przez IOD oraz reagował na sygnalizowane przez IOD problemy, np. poprzez kierowanie do właściwych podmiotów wystąpień postulujących zmianę przepisów prawa bądź stosowanej praktyki. Przykładem takich działań są opisane w części dotyczącej pytań od IOD wystąpienia UODO kierowane np. do Ministra Rodziny i Polityki Społecznej[411] czy do Ministra Edukacji i Nauki[412].

Na przestrzeni ostatnich lat obserwowany jest utrzymujący się wysoki wskaźnik liczby **skarg** wnoszonych do Urzędu Ochrony Danych Osobowych przez osoby, których dane dotyczą. Taka tendencja z jednej strony wskazuje na problemy z przestrzeganiem przez administratorów prawa tych osób do ochrony danych (co znajduje także odzwierciedlenie w liczbie stosowanych przez Prezesa UODO środków naprawczych), natomiast z drugiej strony oznacza także wzrost świadomości osób, których dane dotyczą, co do przysługujących im praw, co jest bardzo pozytywnym i pożądanym zjawiskiem.

Utrzymująca się od kilku lat duża liczba wpływających skarg stanowi niezmiennie duże wyzwanie dla Urzędu Ochrony Danych Osobowych. Podkreślić należy, że wraz ze wzrostem świadomości osób, których dane dotyczą, o przysługujących im prawach, a także postępem technicznym, sprawy prowadzone w urzędzie są coraz bardziej skomplikowane i wielowątkowe, a ponadto coraz częściej dotyczą zagadnień związanych z nowymi technologiami. Powoduje to konieczność ciągłego aktualizowania przez pracowników wiedzy zarówno z zakresu prawa, jak i różnych innych dziedzin, co jest konieczne do zapewnienia wysokiej jakości merytorycznej ich pracy i przekłada się także na jakość wydawanych rozstrzygnięć.

Pomimo bardzo dużej liczby spraw, którymi zajmował się urząd w analizowanym

[411] DOL.413.9.2023.
[412] DOL.413.4.2023.

2023 r., udało się utrzymać na podobnym do lat poprzednich poziomie liczbę spraw zakończonych wydaniem decyzji administracyjnej, przy zachowaniu wysokiej jakości merytorycznej rozstrzygnięć organu nadzorczego. Warto zauważyć, że w większości spraw także sądy administracyjne podzielały stanowiska zajmowane przez organ w sprawach skargowych, oddalając skargi na decyzje Prezesa UODO.

Należy podkreślić, że dla ochrony osoby, której dane dotyczą, w związku z przetwarzaniem jej danych, kluczowe jest zapewnienie, by mogła ona złożyć skargę do organu nadzorczego, gdy uzna, że przetwarzanie jej danych narusza przepisy RODO. Natomiast rolą Prezesa Urzędu Ochrony Danych Osobowych jest zapewnienie, by skarga złożona przez tę osobę została rozpatrzona w sposób niezależny, prawidłowy i zgodny z przepisami. Rozpatrywanie skarg osób, których dane dotyczą, jest zadaniem, do którego Prezes Urzędu Ochrony Danych Osobowych przykłada szczególną wagę, ponieważ prawidłowa realizacja tego zadania przyczynia się do ochrony tych osób przed przetwarzaniem ich danych w sposób niezgodny z przepisami RODO.

Urząd Ochrony Danych Osobowych nieustannie podejmuje szereg **działań edukacyjnych,** które wpisują się w misję organu nadzorczego – bo choć Polacy są coraz bardziej świadomi zagrożeń w obszarze ochrony danych osobowych, wielu z nich wie, jak zareagować w przypadku utraty danych w związku z naruszeniem i potrafi przewidzieć negatywne konsekwencje takiego zdarzenia, to jednak konieczne jest stałe edukowanie społeczeństwa, z uwagi na rozwój technologiczny i związane z nim nowe zagrożenia dla ochrony danych. Ta ostatnia nie jest dana raz na zawsze. To ciągły proces doskonalenia umiejętności w zakresie skutecznego zapewnienia bezpieczeństwa naszym danym. Dlatego edukowanie obywateli jest i będzie wciąż aktualnym zadaniem organu.

Poprzez edukację i informację upowszechniana jest w społeczeństwie wiedza o ochronie danych osobowych i ryzyku, a także o przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienie tych zjawisk – ze szczególną uwagą poświęconą działaniom skierowanym do dzieci. Efektem takiego podejścia jest realizowany od 14 lat ogólnopolski program edukacyjny dla szkół, uczniów i ośrodków doskonalenia nauczycieli „Twoje dane – Twoja sprawa”. Dużym zainteresowaniem uczestników Programu 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, oraz webinaria. 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 Programu.

Podobnie jak w poprzednich edycjach programu „Twoje dane – Twoja sprawa”, stopień spełnienia oczekiwań uczestników był bardzo wysoki, o czym świadczą bardzo dobre oceny tego przedsięwzięcia przez jego realizatorów – uczniów i nauczycieli. Nauczyciele podkreślają konieczność organizowania zajęć w tym obszarze tematycznym – jako niezbędny element zapewnienia bezpieczeństwa nauczania w szkole. Podkreślają też adekwatność tematyki programu do realiów społeczeństwa informacyjnego, uniwersalny zakres merytoryczny oraz duże zainteresowanie uczniów i nauczycieli tematyką prawa do prywatności i ochrony danych osobowych.

Wieloletnia realizacja programu 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 tematem. Program stanowi ważne źródło aktualnej wiedzy i dobrych praktyk w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty.

Warto również podkreślić ogromną rolę podmiotów współpracujących i popierających działania edukacyjne Urzędu Ochrony Danych Osobowych – m.in. Rzecznika Praw Dziecka, Ministra Edukacji, co 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 edukacji oraz współpracę z inspektorem ochrony danych osobowych.

Działania edukacyjne są kluczowe dla budowania świadomości społeczeństwa. Dlatego Urząd Ochrony Danych Osobowych nie ustaje w popularyzowaniu wiedzy o ochronie danych osobowych poprzez organizację: szkoleń, konferencji, seminariów, debat naukowych i różnych spotkań dotyczących ochrony danych osobowych. Współpracuje ze szkołami wyższymi, a eksperci UODO wspierają swoją wiedzą ważne wydarzenia przeznaczone również dla inspektorów ochrony danych. Podczas webinariów adresowanych do IOD-ów prezentowane były oczekiwania społeczeństwa względem nich oraz obowiązki administratora, takie jak np. wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych i zgodność ich przetwarzania z przepisami RODO. Urząd Ochrony Danych Osobowych opracował poradniki, wytyczne i podręczniki dla IOD w ramach działań prowadzonych wspólnie z organami nadzorczymi innych państw. Jeśli chodzi o zasięg i efektywność podejmowanych działań informacyjno-edukacyjnych urzędu, to jest ona związana z otwartością na potrzeby odbiorców, tj. administratorów, inspektorów ochrony danych oraz wszystkich zainteresowanych tematem ochrony danych osobowych i prywatności. Wielokierunkowość tych działań pozwala docierać do różnych grup odbiorców z konkretnym przekazem, dopasowanym do ich potrzeb.

Podnoszeniu poziomu ochrony danych osobowych służy też **udzielanie odpowiedzi na pytania.** Dla organu nadzorczego są one jednocześnie ważnym sygnałem wskazującym na istnienie problemów w konkretnym obszarze i umożliwiającym szybkie reagowanie na nie, m.in. w formie komunikatów publikowanych na stronie internetowej UODO lub kierowania do właściwych podmiotów wystąpień postulujących zmianę przepisów prawa bądź stosowanej praktyki.

W analizowanym roku 2023 zakres tematyczny pytań prawnych kierowanych do Prezesa UODO był bardzo szeroki i dotyczył różnych aspektów przetwarzania danych osobowych. Wątpliwości dotyczyły nie tylko stosowania RODO, ale także innych, szczególnych przepisów prawa.

Podobnie jak w ubiegłych latach pytania dotyczyły udostępniania danych członków wspólnoty mieszkaniowej na rzecz innych jej członków[413], udostępniania sołtysowi listy

[413] DOL.023.100.2023, DOL.023.101.2023.

osób uprawnionych do głosowania podczas zebrań sołeckich[414], pozyskiwania i udostępniania nagrań z monitoringu wizyjnego na prywatnej posesji oraz we wspólnotach mieszkaniowych[415] czy kwestii związanych ze statusem podmiotów w procesie przetwarzania danych[416].

Wiele pytań wpłynęło także z sektora oświaty. Dotyczyły one m.in. takich zagadnień, jak: legalność zawierania umów powierzenia pomiędzy ubezpieczającym a szkołą jako ubezpieczonym[417], przetwarzanie danych osobowych ucznia w ramach medycyny pracy[418], przechowywanie przez szkoły oryginałów świadectw uczniów potwierdzających ukończenie danego etapu edukacji[419], przetwarzanie wizerunku ucznia[420], przetwarzanie danych absolwentów[421] czy wycofanie przez ucznia zgody na przetwarzanie jego danych osobowych przez szkołę[422].

Jak co roku wpływały również pytania od związków zawodowych, m.in. w kwestii pozyskiwania informacji o pracownikach w celu przeprowadzenia referendum strajkowego[423] czy dostępu do wniosków osób korzystających z Zakładowego Funduszu Świadczeń Socjalnych.

W analizowanym 2023 r. wpływały także pytania, które dotyczyły wprowadzonych zmian legislacyjnych w prawie energetycznym[424]. Wątpliwości dotyczyły przetwarzania danych osobowych w związku z uruchomieniem w Polsce centralnego systemu informacji rynku energii (CSIRE) oraz zasilenia tego systemu danymi o punktach pomiarowych[425].

W porównaniu z latami ubiegłymi można zauważyć znaczny spadek liczby pytań prawnych. Fakt ten może świadczyć o tym, że **działalność edukacyjna,** jaką Prezes UODO prowadzi m.in. poprzez swoją stronę internetową, „Biuletyn UODO" czy szkolenia, przynosi widoczne efekty. Częściej bowiem pytania dotyczą zagadnień związanych z wejściem w życie nowych uregulowań prawnych (np. z pracą zdalną) lub interpretacją tych przepisów, które bywają stosowane okazjonalnie (np. w związku z wyborami parlamentarnymi). Więcej jest też pytań związanych z zastosowaniem nowych technologii.

Niepokojącą tendencją jest pomijanie przez administratorów (zwłaszcza z sektora publicznego) konsultacji z inspektorami ochrony danych, występujących do organu nadzorczego. Z przesyłanych pytań nie wynikało, aby takie konsultacje miały miejsce, a jeśli tak, to jakie były ich wyniki. Jednocześnie podobnych wątpliwości nie zgłaszali IOD u tych administratorów. Dlatego w udzielanych odpowiedziach UODO zwracał uwagę, że analizy zgłaszanego problemu w pierwszej kolejności powinien dokonać IOD i przedstawić swoją opinię w tym zakresie. Organ nadzorczy nie ma bowiem kompetencji do realizacji wobec administratorów zadań IOD.

---

414 DOL.023.592.2023.
415 Np. DOL.023.651.2023, DOL.023.251.2023, DOL.023.320.2023, DOL.023.248.2023, DOL.023.306.2023.
416 Np. DOL.023.401.2023, DOL.023.329.2023.
417 DOL.023.613.2023.
418 DOL.023.350.2023.
419 DOL.023.180.2023.
420 DOL.023.109.2023.
421 DOL.023.665.2023.
422 DOL.023.714.2023.
423 DOL.023.904.2023.
424 Art. 20 (1) ustawy z 20 maja 2021 r. o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (Dz. U. z 2021 r. poz. 1093 z późn. zm.).
425 DOL.023.335.2023, DOL.023.194.2023.

Podsumowując część sprawozdania dotyczącą pytań i sygnałów wpływających do UODO od inspektorów ochrony danych, stwierdzić należy, że zgodnie z przepisami RODO organ nadzorczy oraz inspektorzy ochrony danych zostali zobowiązani do wzajemnej pomocy i współpracy, co w założeniu ma im ułatwić wywiązywanie się z ich obowiązków. W okresie sprawozdawczym w ramach tej współpracy inspektorzy chętnie korzystali z możliwości konsultowania się z organem nadzorczym. Zagadnienia przedstawione w pytaniach były bardzo zróżnicowane. Dotyczyły zarówno spraw związanych z zapewnieniem prawidłowego wykonywania swojej funkcji przez IOD, jak i zagadnień, z którymi inspektorzy spotykają się podczas wypełniania swoich zadań.

Analizując treść wpływających do UODO w 2023 r. pytań od inspektorów, zauważyć można, że z każdym rokiem pojawiające się w nich zagadnienia coraz rzadziej dotyczą kwestii podstawowych, a raczej bardziej złożonych problemów obejmujących nieprawidłowości i zagrożenia, które mogą wpływać na niezależność inspektora oraz skuteczne wykonywanie jego funkcji (np. pełnienie przez IOD funkcji pełnomocnika administratora). Ponadto inspektorzy z dużym wyczuciem identyfikują zagrożenia dla ochrony danych osobowych wnikające z luk prawnych lub nieprecyzyjnie skonstruowanych przepisów prawa albo też nieprawidłowej ich interpretacji.

Sygnalizowane przez IOD zagadnienia i wątpliwości dotyczące stosowania przepisów prawa ochrony danych osobowych są dla organu nadzorczego bardzo ważnym źródłem informacji na temat praktycznego funkcjonowania ochrony danych osobowych, w tym realizacji zadań przewidzianych w RODO, pełnienia funkcji przez IOD, a także problemów z tym związanych. Inspektorzy często identyfikują ważne problemy nie tylko z punktu widzenia administratora, u którego zostali wyznaczeni, ale również całego systemu ochrony danych osobowych. Dlatego w niektórych przypadkach stanowią one impuls do podjęcia przez organ nadzorczy interwencji, np. w formie wystąpienia (np. opisane powyżej wystąpienia do MRiPS, MEN oraz Prezesa Zarządu Krajowej Rady Izb Rolniczych).

Odpowiedzi organu nadzorczego udzielane inspektorom w ramach konsultacji często stanowią podstawę do przygotowywania materiałów służących edukowaniu inspektorów i innych podmiotów zobowiązanych do przestrzegania przepisów o ochronie danych osobowych, ułatwiając im wywiązywanie się z nałożonych przepisami RODO obowiązków i zadań, a także wypracowanie odpowiednich standardów i rozwiązań. Materiały takie zamieszczane są następnie w „Biuletynie UODO" lub na stronie internetowej organu, a także wykorzystywane przy opracowywaniu poradników, wskazówek czy przygotowywaniu szkoleń. Również w roku sprawozdawczym sygnały i zagadnienia przekazywane przez IOD wykorzystane zostały do opracowania różnych materiałów informacyjnych.

W okresie sprawozdawczym duża grupa pytań dotyczyła funkcjonowania IOD, w tym w szczególności nakładania na inspektora zadań innych niż te, które są przewidziane w RODO, np. zadań należących do administratora. Kwestie te wciąż budzą wątpliwości i dlatego organ nadzorczy w 2023 r. podejmował różne działania mające na celu podnoszenie wiedzy i świadomości w zakresie zagadnień związanych z wyznaczaniem, zadaniami i ze statusem IOD: udzielał odpowiedzi na pytania od inspektorów i administratorów oraz prowadził postępowania administracyjne będące następstwem akcji 27 pytań, obejmujących kluczowe kwestie w dziedzinie obowiązków administratorów

związanych z wyznaczaniem i funkcjonowaniem inspektorów ochrony danych (informacje na temat tych pytań opublikowane są na stronie internetowej UODO).

Inną bardzo ważną aktywnością UODO na rzecz IOD w 2023 r. był udział w prowadzonym przez EROD w ramach skoordynowanego egzekwowania prawa (Coordinated Enforcement Framework – CEF) **działaniu, którego tematem była pozycja i wyznaczanie inspektorów ochrony danych (CEF DPO**). W inicjatywie tej uczestniczyło 25 organów ochrony danych w całym Europejskim Obszarze Gospodarczym (w tym EIOD).

Na potrzeby ww. skoordynowanego działania polski organ nadzorczy przygotował sprawozdanie krajowe, w którym m.in. zasygnalizowane zostały problemy zidentyfikowane w zakresie praktyk mogących powodować naruszenie przepisów RODO, takie jak np.:

- obciążanie IOD obowiązkami administratora, np. prowadzeniem rejestru czynności przetwarzania;
- zawieranie umowy powierzenia przetwarzania danych osobowych pomiędzy administratorem a IOD;
- udzielanie IOD pełnomocnictwa do reprezentowania administratora w sprawach z zakresu ochrony danych osobowych;
- świadczenie przez firmy zatrudniające inspektorów ochrony danych usług outsourcingu funkcji IOD i jednocześnie usług polegających na wykonywaniu za administratora tzw. „wdrożenia RODO" oraz innych działań związanych z analizą i oceną ryzyka, zapewnianiem bezpieczeństwa danych osobowych czy obsługą żądań i praw osób, których dane dotyczą, oraz szeroko rozumianym bezpieczeństwem informacji.

W sprawozdaniu krajowym UODO zostały przedstawione również działania edukacyjne podejmowane na rzecz upowszechniania zagadnień dotyczących ochrony danych osobowych oraz tych odnoszących się do pełnienia funkcji przez IOD. Jako przykłady swoich działań edukacyjnych, mających na celu podnoszenie wiedzy fachowej IOD, ale również wzmocnienie jego statusu, polski organ nadzorczy wskazał wytyczne i wskazówki zamieszczane na stronie internetowej UODO bądź w „Newsletterze UODO dla IOD" („Biuletyn UODO").

Na podstawie przenalizowanych w skoordynowany sposób wyników wspólnej inicjatywy w ramach CEF DPO organy ochrony danych będą mogły podejmować decyzje w sprawie ewentualnych dalszych krajowych działań w zakresie nadzoru i egzekwowania prawa. Zagregowanie tych wyników umożliwi głębszy wgląd w temat i ukierunkowane działania następcze na poziomie UE.

Prezes UODO wyraża nadzieję, że wypracowane w ramach powyższych działań stanowiska, opinie i wskazówki przyczynią się do wzrostu świadomości co do rozumienia roli inspektora ochrony danych – i to zarówno przez inspektorów, jak i przez podmioty, w których pełnią oni swoją funkcję.

Jednocześnie zauważyć należy, że w 2023 r. kwestie dotyczące statusu IOD były przedmiotem prac nie tylko EROD, ale również Trybunału Sprawiedliwości Unii Europejskiej (TSUE). W wyroku z 9 lutego 2023 r. w sprawie C-453/21 TSUE orzekł m.in., że IOD może mieć inne obowiązki w ramach swojej roli, jeśli nie występuje konflikt interesów. Trybunał stwierdził również, że sądy krajowe mogą określić, co jest sytuacją

konfliktu interesów. Ustaleń w tym zakresie należy dokonywać odrębnie dla każdego przypadku na podstawie oceny wszystkich istotnych okoliczności, w szczególności struktury organizacyjnej administratora lub jego podmiotu przetwarzającego, oraz w świetle całości obowiązujących przepisów, w tym ewentualnych przepisów wewnętrznych administratora lub podmiotu przetwarzającego. W ocenie TSUE RODO nie ustanawia zasadniczej niezgodności między sprawowaniem funkcji IOD a sprawowaniem innych funkcji u administratora danych lub jego podmiotu przetwarzającego. Trybunał stwierdził, że IOD powinien: „być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny", ale „nie można mu powierzyć zadań lub obowiązków, które prowadziłyby do określania przez niego celów i sposobów przetwarzania danych osobowych u administratora lub jego podmiotu przetwarzającego". Orzeczenie to zostało wydane w sprawie dotyczącej orzeczenia wstępnego niemieckiego Federalnego Sądu Pracy dla x-Fab Dresden i jego byłego IOD, który został zwolniony w wyniku pełnienia również funkcji przewodniczącego rady zakładowej. Informacje na temat powyższego wyroku organ nadzorczy zamieścił w materiale pt. „TSUE: rozstrzygnięto kwestię łączenia funkcji IOD z innymi zadaniami w danej organizacji" opublikowanym w „Biuletynie UODO" nr 1/03/2023.

Biorąc zatem pod uwagę to, iż zagadnienia związane z funkcjonowaniem IOD nadal budzą wiele wątpliwości, wyzwaniem dla UODO na przyszłość powinno być dalsze budowanie świadomości na temat roli, zadań i pozycji inspektora w organizacjach, w tym budowanie świadomości wśród administratorów i podmiotów przetwarzających, że ochrona danych osobowych, to nie jest jedynie zadanie IOD, ale przede wszystkim zadanie i odpowiedzialność administratora bądź podmiotu przetwarzającego, którzy mają być w tym wspierani przez IOD.

Innym ważnym zagadnieniem jest **spójność orzecznictwa sądowego i podejmowana przez Prezesa UODO analiza wniosków w sprawach prejudycjalnych wniesionych do TSUE.** Prezes UODO – na podstawie informacji przesłanych przez Pełnomocnika RP przed TSUE – przygotowuje stanowiska w kwestiach dotyczących zasadności udziału RP w tych postępowaniach, opracowuje pisemne analizy skutków orzeczeń TSUE na ustawodawstwo krajowe, a także przygotowuje odpowiedzi na pytania TSUE na rozprawę czy o zasadności udziału w rozprawach – w zakresie spraw, których przedmiotem jest ochrona danych osobowych. Realizacja tego zadania jest pracochłonna i wymaga analizy wielu aktów prawa krajowego i unijnego. Co jednak ważne, stanowiska organu nadzorczego prezentowane w tym obszarze opierają się również na wytycznych EROD i orzecznictwie, co sprzyja harmonizacji podejścia do kwestii będących przedmiotem postępowań.

Wyroki Trybunału Sprawiedliwości Unii Europejskiej stanowią ważną wskazówkę dla krajowego ustawodawcy co do kierunków zmian legislacyjnych, a także praktyki jednolitego stosowania przepisów wspólnotowych oraz krajowych.

W stosunku do spraw, które wpłynęły do rozstrzygnięcia przez TSUE, organ nadzorczy wielokrotnie dostrzegał potrzebę uczestnictwa w postępowaniu przed Trybunałem. Potrzeba ta wynikała z istotności poruszanego w pytaniu prejudycjalnym tematu oraz możliwości wydania przez Trybunał wyroku, który skutkowałby koniecznością zmiany polskiego prawa lub zmiany interpretacji przepisów.

Choć pytania, które zadawały sądy państw członkowskich Trybunałowi dotyczyły różnorodnej tematyki, to można zauważyć, iż najczęściej związane były z obowiązkami administratora wobec podmiotów danych oraz prawem do usunięcia lub sprostowania danych. Wynikały one w dużej mierze z intensywnego rozwoju społeczeństwa informacyjnego i postępu technologicznego, co przekładało się na pytania o interpretację przepisów RODO w świetle nowych rozwiązań technologicznych.

Ze spraw, które zostały rozstrzygnięte przez TSUE w 2023 r., większość, w ocenie organu nadzorczego, nie wymagała dokonania zmian w polskim prawie, wpływała jednak na interpretację przepisów. Jedynie, odnosząc się do wyroku w sprawie C-252/21 *Meta Platforms i in./Facebook e.a.,* organ nadzorczy stwierdził konieczność dokonania zmiany przepisów. Wyrok w tej sprawie ma charakter precedensowy, ponieważ dotyczy konieczności współdziałania organu ds. konsumentów z organem ds. ochrony danych osobowych w sytuacji, gdy ta sama sprawa dotyczy zarówno ochrony praw konsumentów, jak i danych osobowych. Dlatego w zajętym stanowisku organ nadzorczy za istotne uznał podjęcie dyskusji i rozważenie przyjęcia przepisów prawa krajowego rozstrzygających problematykę współpracy między organem nadzorczym a organem ochrony konkurencji celem uniknięcia sporów kompetencyjnych i dualizmu rozstrzygnięć.

Podsumowując, Prezes UODO za potrzebne uznaje stałe upowszechnianie wiedzy na temat orzecznictwa TSUE, sądów krajowych z państw członkowskich Unii Europejskiej oraz wytycznych EROD, co powinno przyczynić się do spójności wykładni EROD.

ZAŁĄCZNIKI

Załącznik nr 1

Wykaz administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2023 r.

Lp.	Data decyzji	Departament UODO prowadzący postępowanie	Sygnatura	Wysokość kary w zł
1.	11.01.2023 r.	Departament Kar i Egzekucji	DKE.561.35.2022	18 279,00
2.	19.01.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.12.2020	30 000,00
3.	25.01.2023 r.	Departament Kar i Egzekucji	DKE.561.24.2022	22 848,00
4.	07.02.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.31.2021	1 556,28
5.	08.02.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.50.2021	33 012,00
6.				472,00
7.	01.03.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.49.2021	51 876,00
8.	14.03.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.45.2022	20.000,00
9.	20.04.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.31.2022	23 580,00
10.	09.05.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.44.2022	10 000,00
11.	16.05.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.56.2022	30 000,00
12.	31.05.2023 r.	Departament Organizacji, Kar i Egzekucji	DKE.561.37.2022	14 148,00
13.	31.05.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.8.2021	47 160,00
14.	02.06.2023 r.	Departament Organizacji, Kar i Egzekucji	DKE.561.38.2022	18 864,00
15.	21.06.2023 r.	Departament Organizacji, Kar i Egzekucji	DOKE.561.1.2023	33 012,00
16.	12.07.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.43.2022	11 790,00
17.	18.07.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.47.2022	15 000,00
18.	30.08.2023 r.	Departament Organizacji, Kar i Egzekucji	DOKE.561.8.2023	56 592,00
19.	18.10.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.55.2022	103 752,00
20.	16.11.2023 r.	Departament Organizacji, Kar i Egzekucji	DOKE.561.7.2023	14 148,00
21.	30.11.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.6.2023	282 960,00
22.	30.11.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.26.2023	35 000,00
23.	30.11.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.13.2022	117 900,00
24.	06.12.2023 r.	Departament Organizacji, Kar i Egzekucji	DOKE.561.2.2023	14 148,00
25.	07.12.2023 r.	Departament Organizacji, Kar	DOKE.561.5.2023	11 790,00

Lp.	Data decyzji	Departament UODO prowadzący postępowanie	Sygnatura	Wysokość kary w zł
		i Egzekucji		
26.	13.12.2023 r.	Departament Organizacji, Kar i Egzekucji	DOKE.561.18.2023	23 580,00
27.	19.12.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.42.2022	10 000,00
28.	20.12.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.32.2023	100 000,00
29.	20.12.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.34.2022	50 000,00
30.	20.12.2023 r.	Departament Kontroli i Naruszeń	DKN.5131.35.2022	10 000,00
31.	21.12.2023 r.	Departament Organizacji, Kar i Egzekucji	DOKE.561z.14.2023	18 864,00

Załącznik nr 2

Wykaz wydarzeń objętych patronatem Prezesa UODO w 2023 r.

1. IX Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej. Organizator: Akademia WSB w Dąbrowie Górniczej, 15.02.2023 r.

2. Instytut Prawa Ochrony Danych Osobowych na Akademii Ekonomiczno-Humanistycznej w Warszawie, 25.05.2023 r.

3. Konferencja „Adwokat dla przedsiębiorcy 3.0". Organizatorzy: Okręgowa Rada Adwokacka w Warszawie oraz Komisja ds. Sekcji Praktyków Prawa. Warszawa, 28.09.2023 r.

4. IX edycja Ogólnopolskiego Szczytu Gospodarczego OSG 2023 „Państwo – Gospodarka – Bezpieczeństwo: Wojna w Europie. Polska w obliczu nowych wyzwań". Organizator: Europejskie Centrum Biznesu. Lublin, 9–10.10.2023 r.

5. IV edycja Cyber24 Day. Organizator: Grupa Defence24. Warszawa, 10.10.2023 r.

6. V Konferencja „RODO w zakładzie pracy: Zakładowe źródła prawa pracy w przedmiocie przetwarzania danych osobowych. Przetwarzanie danych osobowych w ramach zakładowych postępowań wyjaśniających". Organizator: Katedra Prawa Pracy i Polityki Społecznej, WPiA Uniwersytetu Jagiellońskiego, online 15.12.2023 r.

Załącznik nr 3

Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2023 r. w Polsce przez UODO lub inne podmioty

Lp.	Data	Wydarzenie	Miejsce
1.	10.01.2023 r.	Spotkanie z przedstawicielami KPRM i MEiN w sprawie wspólnego projektu edukacyjnego.	online
2.	23.01.2023 r.	Spotkanie z przedstawicielami Microsoft dot. EU Boundary.	online
3.	26.01.2023 r.	Webinarium „DODO Agencja – mitologiczna interwencja”. Organizator: UODO w ramach #ODOlekcje – cyklu ogólnopolskich lekcji dla uczniów uczestniczących w programie „Twoje dane – Twoja sprawa”.	online
4.	31.01.2023 r.	Ogólnopolska konferencja naukowa pt. „Przyszłość ochrony danych osobowych w świetle rozwoju technologii”. Organizator: UODO we współpracy z Prezydentem Miasta Ełku oraz Uniwersytetem Warmińsko-Mazurskim w Olsztynie – Filia w Ełku.	Ełk
5.	31.01.2023 r.	Szkolenie UODO dla kadry zarządzającej jst woj. warmińsko – mazurskiego pt. „Projektowanie ochrony danych osobowych przez jednostki samorządu terytorialnego w związku z wyzwaniami technologicznymi”. Organizator: UODO we współpracy z Urzędem Miasta Ełku.	Ełk
6.	7.02.2023 r.	Gala Dnia Bezpiecznego Internetu. Organizatorzy: Polskie Centrum Programu Safer Internet i Fundacja Orange.	Warszawa
7.	7.02.2023 r.	Webinarium „Ile warte są Twoje dane? Kilka słów o wyzwaniach związanych z monetyzacją danych osobowych”. Organizator: UODO w ramach #ODOlekcje – cyklu ogólnopolskich lekcji dla uczniów uczestniczących w programie „Twoje dane – Twoja sprawa”.	online
8.	8.02.2023 r.	Spotkanie z przedstawicielami KPRM w sprawie szkolenia.	online
9.	10.02.2023 r.	Warsztaty pt. „Sankcje finansowe w świetle przepisów o ochronie danych osobowych w praktyce”. Organizator: WPiA Uniwersytetu Jagiellońskiego.	Kraków
10.	14.02.2023 r.	IX Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej.	Dąbrowa Górnicza
11.	21.02.2023 r.	Uroczystość podpisania listu intencyjnego UODO z Akademią Ekonomiczno-Humanistyczną w Warszawie.	Warszawa
12.	14–15.03.2023 r.	International Conference „ALIGNING DATA PROTECTION WITH EU LEGAL FRAMEWORK. PAVING UKRAINE’S PATH TO A MORE SECURE FUTURE”.	Warszawa
13.	16.03.2023 r.	Spotkanie w UODO z przedstawicielami ukraińskiego Komisarza Parlamentu Ukrainy ds. Praw Człowieka.	Warszawa
14.	21.03.2023 r.	Spotkanie z przedstawicielami Urzędu Komunikacji Elektronicznej.	Warszawa
15.	23.03.2023 r.	Webinarium „Dane biometryczne – bezpieczeństwo czy ryzyko?”. Organizator: UODO w ramach #ODOlekcje – cyklu ogólnopolskich lekcji dla uczniów uczestniczących w programie „Twoje dane – Twoja sprawa”.	online

Lp.	Data	Wydarzenie	Miejsce
16.	24.03.2023 r.	Szkolenie z zakresu ochrony danych osobowych dla żołnierzy i pracowników Centralnego Wojskowego Centrum Rekrutacji w Warszawie.	Warszawa
17.	31.03.2023 r.	Konferencja „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów". Organizator: UODO we współpracy z Akademią Ekonomiczno-Humanistyczną w Warszawie.	Warszawa
18.	5.04.2023 r.	Uroczystość podpisania porozumienia o współpracy pomiędzy Krajową Izbą Radców Prawnych a Urzędem Ochrony Danych Osobowych.	Warszawa
19.	13.04.2023 r.	Webinarium „Na jaką przynętę dasz się złapać? Organizatorzy: UODO i UKE w ramach cyklu „RODO w szkolnej ławce".	online
20.	17.04.2023 r.	Szkolenie dla Kancelarii Prezesa Rady Ministrów.	online
21.	18.04.2023 r.	Międzynarodowa Konferencja KPRM „The Future is Data. Przyszłość to dane". Organizator: Kancelaria Prezesa Rady Ministrów.	online
22.	27.04.2023 r.	Szkolenie dla Inspektorów Ochrony Danych w Izbach Radców Prawnych. Organizator: KIRP.	Warszawa
23.	28.04.2023 r.	Webinarium „Fake news – czy wiemy, jak sobie z tym radzić? Dane osobowe w świecie manipulacji informacją". Organizator: UODO i OEIiZK w ramach #ODOlekcje – cyklu ogólnopolskich lekcji dla uczniów uczestniczących w programie „Twoje dane – Twoja sprawa".	online
24.	11.05.2023 r.	Międzynarodowa konferencja naukowa „Aktualne problemy ochrony danych osobowych w Kościele i państwie". Organizator: Katedra Norm Ogólnych i Teorii Prawa Wydziału Prawa Kanonicznego Uniwersytetu Papieskiego Jana Pawła II w Krakowie.	Kraków
25.	8–26.05.2023 r.	Wizyta w siedzibie UODO przedstawicieli urzędu Państwowego Rzecznika Ochrony Danych i Wolności Informacji Kraju Związkowego Nadrenia-Palatynat oraz z Urzędu Ochrony Danych Osobowych w Pradze.	Warszawa
26.	11.05.2023 r.	Webinarium dla uczniów klas 7–8 szkół podstawowych i szkół ponadpodstawowych pt. „Dane biometryczne – bezpieczeństwo czy ryzyko?". Organizator: UODO.	online
27.	15.05.2023 r.	Okrągły Stół RODO w NGO. Organizator: Krajowa Izba Radców Prawnych.	Warszawa
28.	15.05.2023 r.	VIII Krajowy Zjazd Pielęgniarek i Położnych – podsumowanie VII kadencji samorządu pielęgniarek i położnych.	Warszawa
29.	16.05.2023 r.	Spotkanie Komisji Ruchu i Systemów Elektronicznych IGKM.	online
30.	22.05.2023 r.	Spotkanie inaugurujące powstanie Instytutu Prawa Ochrony Danych Osobowych.	Warszawa
31.	30.05.2023 r.	e-Izba Dialog z Biznesem i Administracją Publiczną „Taki Sam Start". Organizator: Izba Gospodarki Elektronicznej.	online
32.	1.06.2023 r.	Webinarium dla uczniów edukacji wczesnoszkolnej „Z Rodusiem chronimy dane osobowe". Organizator: UODO w ramach cyklu „RODO w szkolnej ławce".	online
33.	12.06.2023 r.	Szkolenie dla Kancelarii Prezesa Rady Ministrów.	online
34.	27.06.2023 r.	Spotkanie z UNHCR Polska (Wysoki Komisarz Narodów Zjednoczonych do spraw Uchodźców).	online
35.	28.06.2023 r.	Posiedzenie Komisji ds. Międzynarodowego Prawa Humanitarnego.	Warszawa
36.	29.06.2023 r.	Webinarium „Dane osobowe – czy wiemy, jak je chronić?". Organizator: UODO wraz z serwisem ChronPESEL.pl oraz Krajowym Rejestrem Długów BIG S.A.	online

Lp.	Data	Wydarzenie	Miejsce
37.	11–13.07.2023 r.	Wykłady ekspertów UODO podczas Letniej Akademii Liderów RODO.	online
38.	18.07.2023 r.	Spotkanie z przedstawicielami Ministerstwa Cyfryzacji w sprawie projektu rozporządzenia ustanawiającego dodatkowe przepisy proceduralne dotyczące wykonywania RODO. Organizatorzy: UODO i MC.	online
39.	21.07.2023 r.	Spotkanie w MSWiA dot. ewaluacji wdrażania dorobku Schengen.	online
40.	3.08.2023 r.	Wykłady w Letniej Akademii Liderów RODO.	online
41.	29.08.2023 r.	Wykłady w Letniej Akademii Liderów RODO.	online
42.	5–6.09.2023 r.	XXXII Forum Ekonomiczne „Nowe Wartości Starego Kontynentu – Europa u progu zmian". Organizatorzy: Fundacja Instytut Studiów Wschodnich, Miasto Karpacz.	Karpacz
43.	11.09.2023 r.	Obchody 30-lecia PIIT i 20-lecia Sądu Polubownego. Organizator: Centrum Konferencyjne Muzeum POLIN.	Warszawa
44.	11.09.2023 r.	Uroczystość wręczenia dobroczynnych nagród Ministra Kultury i Dziedzictwa Narodowego. Organizator: Ministerstwo Kultury i Dziedzictwa Narodowego.	Warszawa
45.	12.09.2023 r.	Konferencja „Zawody zaufania publicznego: etyka, autonomia i społeczna odpowiedzialność". Organizator: Ogólnopolskie Porozumienie Samorządów Zawodów Zaufania Publicznego.	Warszawa
46.	14–15.09.2023 r.	Spotkanie Inspektorów Ochrony Danych uczelni medycznych. Organizator: Konferencja Rektorów Akademickich Uczelni Medycznych.	Warszawa
47.	14.09.2023 r.	Wykład IOD UODO w Letniej Akademii Liderów RODO.	online
48.	18.09.2023 r.	Konferencja Naukowa „Bezpieczeństwo dokumentów publicznych" połączona z zakończeniem IV edycji studiów podyplomowych „Bezpieczeństwo dokumentów publicznych". Organizator: Akademia Policyjna w Szczytnie.	Szczytno
49.	18.09.2023 r.	Finałowy Dzień Letniej Akademii Liderów RODO. Organizator: UODO.	Warszawa
50.	20–21.09.2023 r.	Forum Nowych Technologii. Organizator: UODO we współpracy ze Stowarzyszeniem Prawa Nowych Technologii oraz Akademią Ekonomiczno-Humanistyczną w Warszawie.	Warszawa
51.	26–28.09.2023 r.	17. Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w Internecie". Organizatorzy: Fundacja Dajemy Dzieciom Siłę, NASK, saferinternet.pl.	Warszawa
52.	28.09.2023 r.	Spotkanie Rady Merytorycznej Konferencji „CYBER & RODO".	online
53.	28.09.2023 r.	Konferencja „Adwokat dla przedsiębiorcy 3.0". Organizator: Okręgowa Rada Adwokacka w Warszawie.	Warszawa
54.	29.09.2023 r.	Inauguracja roku akademickiego 2023/2024 w Wyższej Szkole Administracji Publicznej w Ostrołęce.	Ostrołęka
55.	2.10.2023 r.	Inauguracja roku akademickiego 2023/2024 Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.	Olsztyn
56.	6.10.2023 r.	Inauguracja roku akademickiego 2023/2024 UKSW.	Warszawa
57.	6.10.2023 r.	Spotkanie z przedstawicielką KE dot. uwag do rozporządzenia wykonawczego do RODO.	online
58.	9.10.2023 r.	Inauguracja roku akademickiego 2023/2024 Akademii Leona Koźmińskiego w Warszawie.	Warszawa
59.	9–10.10.2023 r.	IX edycja Ogólnopolskiego Szczytu Gospodarczego OSG. Organizator: Europejskie Centrum Biznesu.	Lublin
60.	10.10.2023 r.	IV edycja Cyber24 Day. Organizator: Defence24 Sp. z o.o.	Warszawa
61.	10.10.2023 r.	Spotkanie z przedstawicielami Ministerstwa Cyfryzacji – omówienie uwag do rozporządzenia wykonawczego do RODO.	online

Lp.	Data	Wydarzenie	Miejsce
62.	14.10.2023 r.	Inauguracja roku akademickiego 2023/2024 studiów podyplomowych Uniwersytetu Jagiellońskiego.	Kraków
63.	11–12.10.2023 r.	XXI Samorządowe Forum Kapitału i Finansów. Organizatorzy: miasto Katowice, województwo śląskie, Górnośląsko-Zagłębiowska Metropolia.	Katowice
64.	14.10.2023 r.	Inauguracja studiów podyplomowych na WPiA Uniwersytetu Jagiellońskiego.	Kraków
65.	16.10.2023 r.	Spotkanie z przedstawicielami Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.	Warszawa
66.	16–17.10.2023 r.	26. Banking & 22. Insurance Forum.	Warszawa
67.	18–19.10.2023 r.	Konferencja Tauron dot. Inspektorów Ochrony Danych.	Osiek k. Oświęcimia
68.	24.10.2023 r.	XIV Warszawskie Seminarium Praw Człowieka. Organizator: MSW we współpracy z Radą Europy.	Warszawa
69.	25–26.10.2023 r.	Szkolenie w ramach XIV edycji programu „Twoje dane – Twoja sprawa”. Organizator: UODO.	online
70.	15–16.11.2023 r.	Spotkanie z przedstawicielami 28 szkół wyższych. Organizator: UODO.	Warszawa/online
71.	20.11.2023 r.	Webinarium „To nie są ślady na piasku – cyfrowa tożsamość i cyfrowa reputacja w kontekście ochrony naszej prywatności i danych osobowych”. Organizator: UODO w ramach #ODOlekcje – cyklu ogólnopolskich lekcji dla uczniów uczestniczących w programie „Twoje dane – Twoja sprawa”.	online
72.	22.11.2023 r.	Uroczystość wręczenia nagród Głównego Inspektora Pracy.	Warszawa
73.	22.11.2023 r.	Konferencja „Nowe technologie a ochrona danych osobowych”. Organizatorzy: UODO i Centrala ZUS w Warszawie.	Warszawa
74.	29.11.2023 r.	Konferencja „Cybersec & RODO z Zdrowiu”. Organizator: Polska Federacja Szpitali.	Warszawa
75.	29.11.2023 r.	Spotkanie dot. powołania członków Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych.	Warszawa
76.	29.11.2023 r.	Konferencja „Konsument w świecie nowych cyfrowych możliwości”. Organizator: Konfederacja Lewiatan.	Warszawa
77.	29.11.2023 r.	Debata „Jakość usług publicznych i e-administracja” z cyklu „Debaty cyfrowe”. Organizator: Polskie Towarzystwo Informatyczne.	Warszawa
78.	30.11.2023 r.	Spotkanie podsumowujące konferencję z ZUS.	Warszawa
79.	30.11.2023 r.	Spotkanie Zastępcy Prezesa UODO z Radą Instytutu Prawa Ochrony Danych Osobowych.	Warszawa
80.	5.12.2023 r.	Gala IAB MIXX Awards 2023.	Warszawa
81.	7.12.2023 r.	Webinarium Warszawskiego Centrum Innowacji Edukacyjno-Społecznych i Szkoleń z okazji Dnia Praw Człowieka.	online
82.	7.12.2023 r.	Jesienna konferencja Programowa PFSz – SAVE THE DATE. Organizator: Polska Federacja Szpitali.	online
83.	8.12.2023 r.	Webinarium dla licealistów „Prawo do ochrony danych osobowych jako prawo człowieka”. Organizator: UODO w ramach #ODOlekcje – cyklu ogólnopolskich lekcji dla uczniów uczestniczących w programie „Twoje dane – Twoja sprawa”.	online
84.	8.12.2023 r.	Gala z okazji jubileuszu 35-lecia Urzędu Rzecznika Praw Obywatelskich oraz wręczenia dorocznej Nagrody Rzecznika Praw Obywatelskich im. Pawła Włodkowica.	Warszawa
85.	10.12.2023 r.	Międzynarodowy Dzień Praw Człowieka. Organizator: WCIES.	online
86.	11.12.2023 r.	Webinarium dot. Kodeksu Polskiej Federacji Szpitali. Organizator: UODO.	online

Lp.	Data	Wydarzenie	Miejsce
87.	12.12.2023 r.	Webinarium „Certyfikacja w ochronie danych”. Organizator: UODO.	online
88.	28.06.2023 r.	Posiedzenie Komisji ds. Międzynarodowego Prawa Humanitarnego.	Warszawa
89.	15.12.2023 r.	V Konferencja z cyklu „RODO w zakładzie pracy”. Organizator: Katedra Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego.	online
90.	18.12.2023 r.	Webinarium dla koordynatorów programu „Twoje dane – Twoja sprawa” pt. „Jak dobrze zaplanować działania w ramach Programu? Narzędzia coachingu do pracy z celami”. Organizator: UODO.	online
91.	21.12.2023 r.	Uroczystość podpisania porozumienia UODO z Naczelną Izbą Pielęgniarek i Położnych.	Warszawa

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 2023 r.

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	10.01.2023 r.	Wspólne posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa oraz Ekspertów ds. Międzynarodowego Przekazywania Danych (Borders, Travel and Law Enforcement Expert Subgroup & International Transfers ESG) Europejskiej Rady Ochrony Danych.	online
2.	10–11.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG).	online
3.	11.01.2023 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
4.	17.01.2023 r.	74. posiedzenie plenarne EROD.	online
5.	18.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
6.	18–19.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
7.	18.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
8.	19.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
9.	23.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
10.	23–28.01.2023 r.	Ewaluacja dorobku Schengen w zakresie ochrony danych osobowych.	Lizbona
11.	24.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa oraz Ekspertów ds. Międzynarodowego Przekazywania Danych (Borders, Travel and Law Enforcement Expert Subgroup & International Transfers ESG) Europejskiej Rady Ochrony Danych – zaproszenie dla podmiotów zewnętrznych (eksperci USA) – EU-US DPF.	online
12.	25.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
13.	26.01.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup).	online
14.	6.02.2023 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101).	online
15.	7.02.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
16.	7.02.2023 r.	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
17.	7–8.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	Bruksela
18.	8–9.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych	Bruksela
19.	9.02.2023 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
20.	10.02.2023 r.	Wspólne posiedzenie *ad hoc* Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa oraz Ekspertów ds. Międzynarodowego Przekazywania Danych (Borders, Travel and Law Enforcement Expert Subgroup & International Transfers ESG) Europejskiej Rady Ochrony Danych.	online
21.	14.02.2024 r.	75. posiedzenie plenarne EROD.	Bruksela
22.	16.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
23.	16.02.2023 r.	Spotkanie grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD – CEF DPO.	online
24.	16.02.2023 r.	Wspólne posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) i Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
25.	16.02.2023 r.	Spotkanie sprawozdawców wytycznych EROD dot. prawa dostępu.	online
26.	20.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
27.	21–22.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
28.	23.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
29.	23.02.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
30.	28.02.2023 r.	76. posiedzenie plenarne EROD *ad hoc* (EU-US DPF).	Bruksela
31.	28.02–1.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
32.	2.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
33.	6.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
34.	6.03.2023 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101).	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
35.	7.03.2023 r.	Spotkanie sprawozdawców wytycznych EROD dot. prawa dostępu.	online
36.	7.03.2023 r.	Sieć Inspektorów Ochrony Danych – posiedzenie podgrupy DPO Network.	online
37.	8–9.03.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	Bruksela
38.	9–10.03.2023 r.	Warsztaty dot. certyfikacji zorganizowane w ramach prac Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	Madryt
39.	12–13.03.2023 r.	Posiedzenie Podgrupy IT Users Europejskiej Rady Ochrony Danych.	Bruksela
40.	13.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
41.	13.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
42.	13–14.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
43.	17.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
44.	21.03.2023 r.	Wspólne posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) oraz Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
45.	21.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
46.	22.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
47.	22.03.2023 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
48.	22.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
49.	22.03.2023 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee) Europejskiej Rady Ochrony Danych.	online
50.	23.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
51.	26–31.03.2023 r.	Wydział Konsularny i Polonii Ambasady RP w Kairze. Czynności kontrolne w zakresie ochrony danych osobowych przetwarzanych w Systemie Informacyjnym Schengen (SIS, VIS).	Kair
52.	27-28.03.2023	3. posiedzenie MSI-INF Committee of Experts on the Integrity of Online Information.	online
53.	28.03.2023 r.	77. posiedzenie plenarne EROD.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
54.	29.03.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
55.	4.04.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
56.	4.04.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
57.	13.04.2023 r.	78. posiedzenie plenarne EROD.	online
58.	17.04.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Audytów Aplikacji Mobilnych.	online
59.	18.04.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
60.	18.04.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
61.	19.04.2023 r	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
62.	19.04.2023 r	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
63.	19.04.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
64.	24.04.2023 r.	Wspólne Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) i Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
65.	25–26.04.2023 r.	79. posiedzenie plenarne EROD.	Bruksela
66.	27.04.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
67.	28.04.2023 r.	Grupa zadaniowa ds. wzajemnego oddziaływania prawa ochrony danych, prawa ochrony konkurencji i konsumentów (Taskforce C&C).	online
68.	4.05.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
69.	5.05.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
70.	10–12.05.2023 r.	31. Wiosenna Konferencja Europejskich Organów Ochrony Danych. Organizator: Krajowy organ Ochrony Danych i Wolności Informacji Węgier.	Budapeszt
71.	16.05.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
72.	17.05.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
73.	17.05.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
74.	22.05.2023 r.	Grupa zadaniowa ds. działalności międzynarodowej (Taskforce on International Engagement – FT INT).	online
75.	22.05.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
76.	22–23.05.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
77.	23.05.2023 r.	Konferencja z okazji 45-lecia CNIL „Działanie na rzecz odpowiedzialnej przyszłości cyfrowej". Organizator: CNIL.	online
78.	23.05.2023 r.	Spotkanie CEF DPO (grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD).	online
79.	24.05.2023 r.	80. posiedzenie plenarne EROD.	online
80.	29.05.2023 r.	Spotkanie z przedstawicielami organu ochrony danych Gruzji w ramach Grupy Państw Europy Środkowej i Wschodniej (CEEDPA).	online
81.	30–31.05.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
82.	31.05.2023 r.	Spotkanie CEF DPO (grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD).	online
83.	31.05.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
84.	1.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG).	online
85.	1–2.06.2023 r.	Annual Privacy Forum – APF.	online
86.	6.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
87.	8.06.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
88.	13.06.2023 r.	Grupa ds. Koordynacji Nadzoru nad Eurodac (Eurodac SCG).	online
89.	13.06.2023 r.	Grupa ds. Koordynacji Nadzoru nad VIS (VIS SCG).	online
90.	13–14.06.2023 r.	Posiedzenie Komitetu Skoordynowanego Nadzoru w celu nadzoru organów nadzorczych nad Systemem Informatycznym Schengen.	Bruksela
91.	13–16.06.2023 r.	44. posiedzenie plenarne Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy (Komitet T-PD).	Strasburg
92.	13–16.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	Bruksela
93.	15.06.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
94.	16.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
95.	19.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
96.	19.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
97.	19–20.06.2023 r.	JOINT EOSC-Life/Healthy Cloud WORKSHOP: Elements of Secure Processing Environments.	online
98.	20.06.2023 r.	81. posiedzenie plenarne EROD.	online
99.	26.06.2023 r.	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
100.	26.06.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
101.	29.06.2023 r.	Spotkanie z Urzędem ds. Europejskich Partii Politycznych i Europejskich Fundacji Politycznych.	online
102.	29.06.2023 r.	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
103.	3.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
104.	4.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG) Europejskiej Rady Ochrony Danych.	online
105.	6.07.2023 r.	Spotkanie CEF DPO (grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD).	online
106.	6.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
107.	7.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup (FMES) Europejskiej Rady Ochrony Danych.	online
108.	10.07.2023 r.	Grupa zadaniowa ds. działalności międzynarodowej (Taskforce on International Engagement – FT INT).	online
109.	11.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
110.	11.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
111.	11.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup (FMES) Europejskiej Rady Ochrony Danych.	online
112.	12.07.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
113.	12.07.2023 r.	Grupa zadaniowa ds. ChatGPT.	online
114.	12.07.2023 r.	Warsztaty Global Privacy Assembly (GPA) „Moving forward on Data Free Flow with Trust”.	online
115.	13.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
116.	17.07.2023 r.	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
117.	18.07.2023 r.	82. posiedzenie plenarne EROD.	online
118.	19.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Audytów Aplikacji Mobilnych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
119.	20.07.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
120.	2.08.2023 r.	83. posiedzenie plenarne EROD.	online
121.	30.08.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup (FMES) Europejskiej Rady Ochrony Danych.	online
122.	31.08.2023 r.	Wspólne spotkanie Podgrupy ekspertów ds. współpracy oraz Podgrupy ekspertów ds. egzekwowania prawa (Cooperation ESG / Enforcement ESG).	online
123.	6.09.2023 r.	Grupa zadaniowa ds. ChatGPT.	online
124.	6.09.2023 r.	Grupa zadaniowa ds. wzajemnego oddziaływania prawa ochrony danych, prawa ochrony konkurencji i konsumentów (Taskforce C&C).	online
125.	7.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
126.	7.09.2023 r.	Posiedzenie Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee – CSC).	online
127.	11.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
128.	12.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
129.	12.09.2023 r.	Spotkanie CEF DPO (grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD).	online
130.	12.09.2023 r.	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
131.	13.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
132.	13.09.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
133.	13.09.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
134.	15.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup).	online
135.	19–20.09.2023 r.	84. posiedzenie plenarne EROD.	Bruksela
136.	25.09.2023 r.	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network) Europejskiej Rady Ochrony Danych.	online
137.	25–26.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
138.	26.09.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
139.	28.09.2023 r.	Posiedzenie Grupy Ekspertów Wspierających EROD (Support Pool of Experts – SPE).	online
140.	1–3.10.2023 r.	Wspólne czynności kontrolne Europolu na zaproszenie EIOD.	Haga
141.	4–5.10.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
		(International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	
142.	8–13.10.2023 r.	Realizacja obowiązku prowadzenia kontroli na miejscu z zakresu oceny stosowania dorobku Schengen.	Ryga
143.	9.10.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
144.	10.10.2023 r.	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
145.	11.10.2023 r.	Posiedzenie Grupy zadaniowej ds. banerów cookie (FT Cookie Banner).	online
146.	11.10.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
147.	11.10.2023 r.	Grupa zadaniowa ds. ChatGPT.	online
148.	12.10.2023 r.	Spotkanie grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD – CEF DPO.	online
149.	13.10.2023 r.	85. posiedzenie plenarne EROD.	online
150.	16.10.2023 r.	Wspólne Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory – SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
151.	17.10.2023 r.	85. posiedzenie plenarne EROD.	online
152.	16.10.2023 r.	Wspólne Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
153.	20.10.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
154.	24.10.2023 r.	Wspólne Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
155.	26.10.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup).	online
156.	26.10.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
157.	27.10.2023 r.	86. posiedzenie plenarne EROD ad hoc.	online
158.	31.10.2023 r.	Conference online Children's Rights: Putting interoperable age verification and parental consent into live operation.	online
159.	2.11.2023 r.	Internet Freedom Summit. Organizator: American Bar Association.	online
160.	7.11.2023 r.	Wspólne posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG) oraz Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup).	online
161.	7.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup).	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
162.	8.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
163.	8.11.2023 r.	Grupa zadaniowa ds. ChatGPT.	online
164.	9.11.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
165.	11.11.2023 r.	Spotkanie International Age Assurance Working Group.	online
166.	14.11.2023 r.	87. posiedzenie plenarne EROD.	Bruksela
167.	14.11.2023 r.	Spotkanie International Age Assurance Working Group.	online
168.	15.11.2023 r.	Posiedzenie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
169.	15.11.2023 r.	Grupa zadaniowa ds. wzajemnego oddziaływania prawa ochrony danych, prawa ochrony konkurencji i konsumentów (Taskforce C&C).	online
170.	15–17.11.2023 r.	45. posiedzenie plenarne Komitetu T-PD Rady Europy.	Strasburg
171.	16.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
172.	16.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
173.	17.11.2023 r.	Spotkanie CEF DPO (grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD).	online
174.	20.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
175.	21–22.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
176.	22.11.2023 r.	Spotkanie dot. ewaluacji Schengen z Komisją Europejską.	online
177.	27.11.2023 r.	Grupa zadaniowa ds. działalności międzynarodowej (Taskforce on International Engagement – FT INT).	online
178.	27–29.11.2023 r.	11. posiedzenie Komitetu Skoordynowanego Nadzoru, posiedzenie VIS i Eurodac (Coordinated Supervision Committee).	Bruksela
179.	28.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup (FMES) Europejskiej Rady Ochrony Danych.	online
180.	29.11.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup – SAESG) Europejskiej Rady Ochrony Danych.	online
181.	29.11.2023 r.	Spotkanie grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF right of access).	online
182.	29.11.2023 r.	Spotkanie Digital Education Working Group.	online
183.	4.12.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
184.	4.12.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
185.	5.12.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
186.	5–6.12.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
187.	6.12.2023 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
188.	7.12.2023 r.	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
189.	13–14.12.2023 r.	OECD conference: Towards an effective and equitable digital education ecosystem.	online
190.	15.12.2023 r.	88. posiedzenie plenarne EROD.	Bruksela
191.	19.12.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
192.	20.12.2023 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online

Załącznik nr 5

Działalność Urzędu Ochrony Danych Osobowych w 2023 roku w liczbach

		2023 r.
1. DECYZJE	**skargowe**	1796 1750(DS) + 43(DKN) + 3(DOL) = 1796
	karowe	30
	dot. naruszeń	36
	dot. kontroli	4
	dot. kodeksu postępowania	3
	dot. akredytacji podmiotu monitorującego kodeks	1
	OGÓŁEM	**1870**
2. SKARGI	**Liczba skarg krajowych, które wpłynęły do UODO**	6962
	Liczba zakończonych postępowań skargowych OGÓŁEM	5942 5898 (DS) + 43 (DKN) + 3 (DOL) = 5942
Liczba skarg z podziałem na sektory:	**Prywatny**	2659
	Finansowy, ubezpieczeń i telekomunikacji	1519
	Zdrowia, zatrudnienia i szkolnictwa	1454
	Publiczny	1328
	Transgraniczny	475
3. NARUSZENIA	**Liczba zgłoszeń naruszeń**	14069
4. ADMINISTRACYJNE KARY PIENIĘŻNE	**Liczba administracyjnych kar pieniężnych nałożonych przez Prezesa UODO**	31 w 1 decyzji nałożono 2 kary
	Liczba decyzji dot. kar pieniężnych	30
	Łączna kwota kar w zł	1 230 331,28
5. KONTROLE	**Liczba skontrolowanych podmiotów**	33
	Liczba sprawdzeń stosowania przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	13
6. PROJEKTY AKTÓW PRAWNYCH	**Liczba zaopiniowanych projektów aktów prawnych**	819
7. Uprzednie konsultacje	**Liczba wniosków o uprzednie konsultacje**	3
8. Kodeksy postępowania	**Liczba zatwierdzonych kodeksów postępowania**	1
9. PYTANIA PRAWNE	**Liczba pytań prawnych**	1850
	Liczba pytań od IOD	253

		2023 r.
	Liczba pytań od organów nadzorczych z innych państw	27
10. WNIOSKI PREJUDYCJALNE	**Liczba wniosków prejudycjalnych skierowanych do TSUE przez sądy z różnych państw UE, które wpłynęły do polskiego organu nadzorczego**	23
11. WYSTĄPIENIA	**DOL**	5
12. Zawiadomienia o podejrzeniu popełnienia przestępstwa		0
13. SPRAWY PRZED SĄDAMI ADMINISTRACYJNYMI	**Liczba decyzji Prezesa UODO zaskarżonych do WSA w Warszawie OGÓŁEM**	236 228 (DS) + 8 (DKN) = 236
	Liczba skarg wniesionych do NSA	74 70 (DS) + 4 (DKN) = 74
	Liczba wyroków uchylających decyzję Prezesa UODO	36 33 (DS) + 3 (DKN) = 36
	Liczba wyroków utrzymujących w mocy decyzje Prezesa UODO	128 124 (DS) + 4 (DKN) = 128