SPRAWOZDANIE Z DZIAŁALNOŚCI
PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
w ROKU 2024

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 2024 r. do 31 grudnia 2024 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 jako: „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 jako: „Prezes UODO".

Spis treści

Spis treści

I. WPROWADZENIE 7

1. *ŹRÓDŁA PRAWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH 7*
2. *URZĄD OCHRONY DANYCH OSOBOWYCH 7*
   - 2.1. *Struktura organizacyjna 8*
   - 2.2. *Pracownicy UODO 9*
   - 2.3. *Zadania jednostek organizacyjnych UODO 11*
   - 2.4. *Budżet UODO za 2024 r. 12*

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI 12

1. *WYDAWANIE DECYZJI ADMINISTRACYJNYCH I ROZPATRYWANIE SKARG 12*
   - 1.1. *Sektor publiczny 17*
   - 1.2. *Sektor prywatny 24*
   - 1.3. *Sektor finansów, ubezpieczeń i telekomunikacji 31*
   - 1.4. *Sektor zdrowia, zatrudnienia i szkolnictwa 38*
   - 1.5. *Postępowania o charakterze transgranicznym 44*
   - 1.6. *Skargi na przewlekłość w sprawach skargowych 47*
   - 1.7. *Rewizja stanowisk w sprawach z lat ubiegłych 47*
   - 1.8. *Orzecznictwo sądów administracyjnych w sprawach skargowych 51*
   - 1.9. *Wyroki sądów administracyjnych w sprawach skargowych – wybrane przykłady 52*
2. *KONTROLA PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH 60*
   - 2.1. *Aplikacje mobilne 61*
   - 2.2. *System Informacyjny Schengen, Wizowy System Informacyjny 62*
   - 2.3. *Misja Ewaluacyjna Schengen w UODO 66*
   - 2.4. *Spełnienie obowiązku informacyjnego 66*
   - 2.5. *Kontrole w wyniku zgłoszonego naruszenia 68*
   - 2.6. *Decyzje administracyjne w postępowaniach kontrolnych 68*
   - 2.7. *Wyroki WSA w Warszawie i NSA dotyczące decyzji Prezesa UODO w sprawie kontroli 70*
3. *ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH 72*
   - 3.1. *Statystyka zgłaszanych naruszeń ochrony danych osobowych 73*
   - 3.2. *Wyjaśnienia 77*
   - 3.3. *Wystąpienia o charakterze generalnym 78*
   - 3.4. *Postępowania administracyjne 80*
   - 3.5. *Zawiadomienia o popełnieniu przestępstwa 81*
   - 3.6. *Decyzje administracyjne 81*
   - 3.7. *Administracyjne kary pieniężne w związku z naruszeniem 82*
4. *EGZEKUCJA ADMINISTRACYJNA – ZAPEWNIENIE WYKONANIA DECYZJI ORGANU NADZORCZEGO 90*
   - 4.1. *Postępowania w zakresie egzekucji decyzji Prezesa UODO 92*
   - 4.2. *Egzekucja obowiązków o charakterze niepieniężnym 95*
   - 4.3. *Egzekucja należności pieniężnych 96*
5. *ADMINISTRACYJNE KARY PIENIĘŻNE 97*
   - 5.1. *Administracyjne kary pieniężne za brak współpracy z organem nadzorczym i za niezapewnienie dostępu do informacji niezbędnych do realizacji jego zadań. 101*
   - 5.2. *Administracyjne kary pieniężne jako środek naprawczy przymuszający do wykonania nakazu decyzji. 103*
6. *OPINIOWANIE PROJEKTÓW AKTÓW PRAWNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH 103*
   - 6.1. *Uwzględnienie ochrony danych osobowych na etapie prac legislacyjnych 105*
   - 6.2. *Ocena skutków dla ochrony danych osobowych w procesie legislacyjnym 109*
   - 6.3. *Zasada praworządności, zasada legalności 114*
   - 6.4. *Rejestry publiczne i systemy teleinformatyczne 120*
   - 6.5. *Role podmiotów w procesach przetwarzania danych osobowych 124*
   - 6.6. *Zasady przetwarzania danych osobowych, dane szczególnych kategorii, PESEL 127*

6.7. Postęp technologiczny a ochrona praw podstawowych 131
6.8. Nowe kompetencje Prezesa UODO 135
6.9. Opiniowanie dokumentów dotyczących problemów informatycznych 137
6.10. Sprawy przed sądami powszechnymi 141
6.11. Podsumowanie 144
7. UPRZEDNIE KONSULTACJE 147
8. KODEKSY POSTĘPOWANIA 148
8.1. Kodeksy postępowania zatwierdzone przez organ nadzorczy 150
8.2. Nowe wnioski o zaopiniowanie kodeksów postępowania 150
8.3. Postępowania prowadzone w 2024 r. w sprawie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone we wcześniejszych latach 150
8.4. Współpraca organu nadzorczego z inicjatywami opracowania kodeksów postępowań 151
9. AKREDYTACJA PODMIOTÓW MONITORUJĄCYCH KODEKSY POSTĘPOWANIA 153
9.1. Wnioski o udzielenie akredytacji do monitorowania kodeksów postępowania 154
9.2. Akredytacje udzielone przez organ nadzorczy 154
9.3. Współpraca z Prezesem UODO akredytowanych w 2022 r. i 2023 r. podmiotów monitorujących 154
10. CERTYFIKACJA 155
11. PYTANIA DOTYCZĄCE WYKŁADNI PRAWA, WNIOSKI O DOSTĘP DO INFORMACJI I WYSTĄPIENIA PREZESA UODO 156
11.1. Pytania dotyczące wykładni prawa 156
11.2. Wnioski o dostęp do informacji publicznej 224
11.3. Skargi na działanie UODO 226
11.4. Wystąpienia 226

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA 231

1. DZIAŁALNOŚĆ EDUKACYJNA 231
1.1. Kampanie edukacyjne 232
1.2. Współpraca ze szkołami wyższymi 236
1.3. Społeczny Zespół Ekspertów przy Prezesie UODO 237
1.4. Szkolenia 238
1.5. Projekty i programy 239
1.6. Konkursy 246
1.7. Porozumienia o współpracy 248
1.8. Poradniki 248
1.9. Współpraca krajowa przy Polskim Komitecie Normalizacyjnym (PKN) 249
1.10. Nagroda im. Michała Serzyckiego 249
1.11. Konferencje, seminaria, spotkania 250
1.12. UODO rusza w kraj 257
1.13. Spotkania z JST 258
1.14. Cykl wykładów eksperckich 259
1.15. IV Tour de Konstytucja 259
1.16. Pol'and'Rock Festiwal 260
2. DZIAŁALNOŚĆ INFORMACYJNA 260
2.1. Komunikaty 261
2.2. Pytania dziennikarskie 261
2.3. Zasięg informacji publikowanych w mediach 262
2.4. Pytania od obywateli 263
2.5. Social media 263
2.6. Biuletyn 265
2.7. Współpraca międzynarodowa 266

IV. UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ OCHRONĄ DANYCH OSOBOWYCH 267

1. UDZIAŁ UODO W PRACACH EROD 267
2. WSPÓŁPRACA ORGANÓW I EGZEKWOWANIE PRAWA 268
2.1.1. Współpraca w ramach IMI 269
2.1.2. Sieć Inspektorów Ochrony Danych 270

2.1.3. Skoordynowany nadzór nad wielkoskalowymi systemami 270
2.1.4. Wnioski prejudycjalne 272
2.1.5. Przekazywanie danych osobowych poza EOG 280
2.1.6. Wizyta studyjna 281
2.1.7. Inne sprawy 281
2.1.8. Prokuratura Europejska 282
2.1.9. Międzynarodowe konferencje, seminaria i spotkania 283

V. WNIOSKI WYNIKAJĄCE ZE STANU PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH 288

ZAŁĄCZNIKI 312

ZAŁĄCZNIK NR 1: WYKAZ ADMINISTRACYJNYCH KAR PIENIĘŻNYCH NAŁOŻONYCH PRZEZ PREZESA UODO W 2024 R. 312
ZAŁĄCZNIK NR 2: WYKAZ WYDARZEŃ OBJĘTYCH PATRONATEM PREZESA UODO W 2024 R. 313
ZAŁĄCZNIK NR 3: WYKAZ KONFERENCJI, SEMINARIÓW, SPOTKAŃ I INNYCH WYDARZEŃ KRAJOWYCH I MIĘDZYNARODOWYCH Z UDZIAŁEM PREZESA UODO LUB JEGO PRZEDSTAWICIELI, ZORGANIZOWANYCH W 2024 R. W POLSCE PRZEZ UODO LUB INNE PODMIOTY 316
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 2024 R. 323
ZAŁĄCZNIK NR 5: DZIAŁALNOŚĆ URZĘDU OCHRONY DANYCH OSOBOWYCH W 2024 R. W LICZBACH 336

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 2024. Na mocy art. 59 ogólnego rozporządzenia o ochronie danych sprawozdanie jest także udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

Niniejsze sprawozdanie przedstawia najważniejsze ustalenia dotyczące zrealizowanych przez Prezesa UODO ustawowych zadań, do których należą: rozpatrywanie skarg, prowadzenie kontroli, opiniowanie projektów aktów prawnych, przyjmowanie zgłoszeń naruszeń ochrony danych i podejmowanie czynności wobec administratorów i podmiotów przetwarzających w celu powiadomienia 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 2024 r. minęło sześć lat 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 oraz czy sprosta wymaganiom w świetle wyzwań związanych z nowymi kompetencjami UODO wynikających z Aktu o zarządzaniu danymi (DGA) i gotowości Prezesa UODO do pełnienia funkcji organu właściwego do spraw rejestracji organizacji altruizmu danych oraz organu właściwego do spraw usług pośrednictwa danych.

Analiza spraw, którymi Prezes UODO zajmował się w okresie analizowanego roku 2024, 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.

Zapraszam do lektury sprawozdania z działalności polskiego organu ochrony danych osobowych w roku 2024, 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 i ochrony 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 ogólne rozporządzenie o ochronie danych osobowych (RODO)[8], 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[9],
- ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[10] oraz wydane na jej podstawie akty wykonawcze.

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, w tym prawa Unii Europejskiej i prawa międzynarodowego. Na mocy art. 34 ust. 1 ustawy, Prezes UODO jest organem właściwym w sprawie ochrony danych osobowych.

---

[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] 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 4.5.2016, str. 1 ze zm.).
[9] Dz. Urz. UE L 119 z 4.05.2016 r. s. 89. Dalej: „dyrektywa 2016/680" lub „dyrektywa policyjna".
[10] Dz. U. z 2023 r. poz. 1206.

Zgodnie z art. 34 ust. 2 ww. ustawy, Prezes UODO jest organem nadzorczym w rozumieniu:

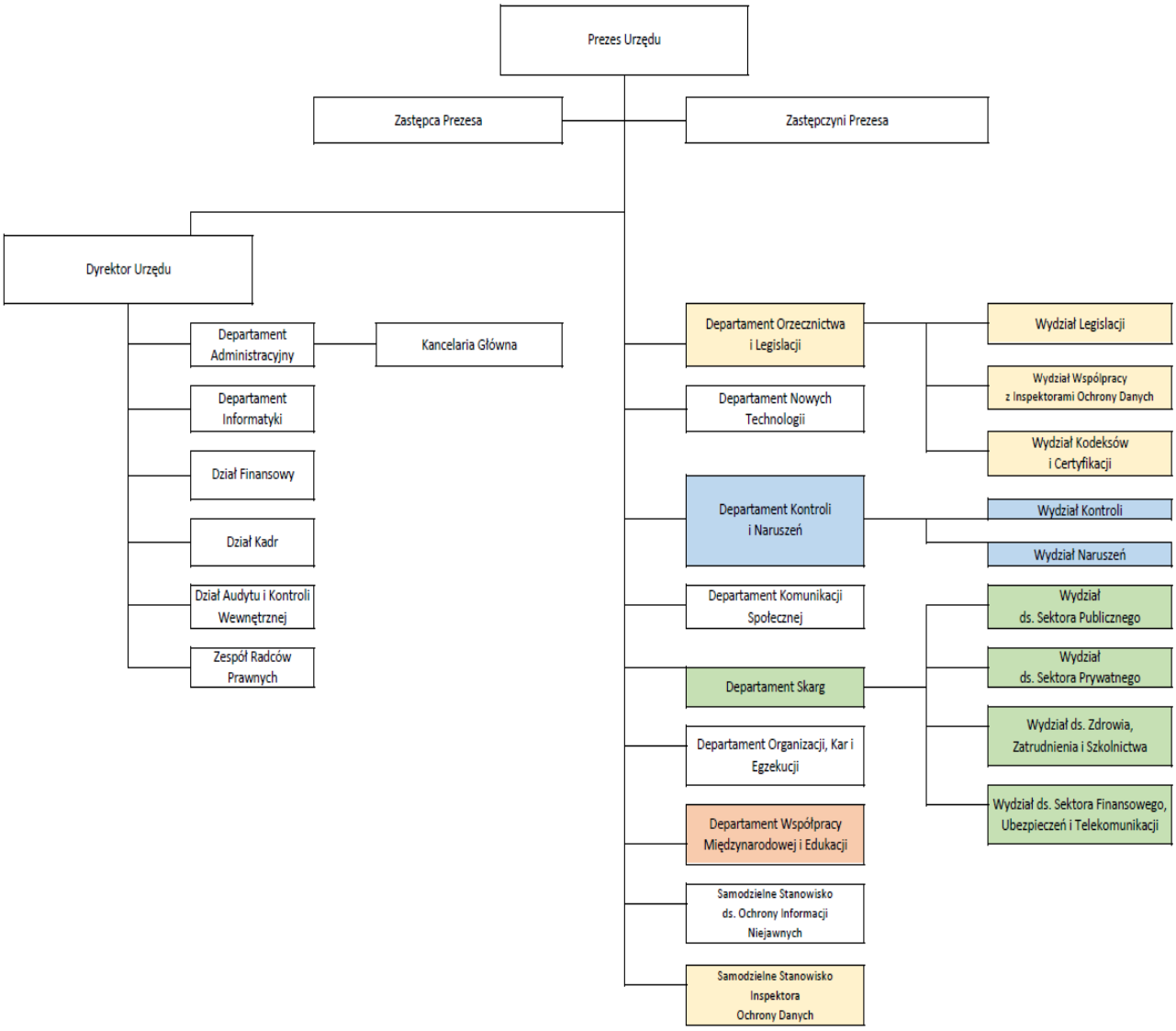
- RODO,
- dyrektywy 2016/680,
- rozporządzenia 2016/794[11].

2.1. Struktura organizacyjna

W skład UODO w 2024 r. wchodziły 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.

[11] 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 jako „rozporządzenie 2016/794".



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 powyższy diagram.

2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2024 r. (nie wliczając Prezesa UODO i jego dwóch zastępców) wynosił 266,25 etatu (tj. 271 osób)[12]. Natomiast zatrudnienie w UODO na dzień 31 grudnia 2024 r. wynosiło 270,45 etatu (tj. 278 osób). Na koniec 2024 r. na stanowiskach merytorycznych

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

zatrudnionych było 245 osób, a na stanowiskach pomocniczych 32 osoby. Wyższe wykształcenie ogółem posiadało 244 pracowników, w tym 149 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2024 r. (bez Prezesa UODO i jego zastępców) przedstawiała się następująco:

1) Departament Orzecznictwa i Legislacji – 33 osoby (32,8 etatu), w tym:
   - Wydział Legislacji – 10 osób (10,0 etatów),
   - Wydział Współpracy z Inspektorami Ochrony Danych – 4 osoby (4,0 etaty),
   - Wydział Kodeksów i Certyfikacji – 5 osób (5,0 etatów);
2) Departament Współpracy Międzynarodowej i Edukacji – 15 osób (14,8 etatów);
3) Departament Kontroli i Naruszeń – 49 osób (48,5 etatu), w tym:
   - Wydział Kontroli – 17 osób (17,0 etatów),
   - Wydział Naruszeń – 25 osób (24,5 etatu);
4) Departament Komunikacji Społecznej – 17 osób (15,95 etatu) – w tym 7 pracowników Infolinii na pełnym etacie;
5) Departament Skarg – 81 osób (80,05 etatu), w tym:
   - Wydział ds. Sektora Publicznego – 14 osób (14 etatów),
   - Wydział ds. Sektora Prywatnego – 22 osoby (22 etaty),
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 16 osób (16 etatów),
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 19 osób (19,0 etatów);
6) Departament Organizacji, Kar i Egzekucji – 15 osób (15,0 etatów);
7) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,33 etatu);
8) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba (1,0 etat);
9) Departament Administracyjny – 28 osób (25,5 etatu);
10) Departament Informatyki – 11 osób (10,42 etatu);
11) Departament Nowych Technologii – 6 osób (5,8 etatów);
12) Dyrektor UODO – 1 osoba (1 etat);
13) Dział Finansowy – 7 osób (7,0 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 – 3 osoby (2,8 etatu);
18) Asystent prezesa UODO – 1 osoba (1 etat).

Liczba pracowników zatrudnionych na stanowiskach merytorycznych i na stanowiskach pomocniczych według stanu na 31 grudnia 2024 r. (bez Prezesa UODO i jego zastępców):

- stanowiska merytoryczne – 245 osób,
- stanowiska pomocnicze – 33 osoby.

Liczba pracowników posiadających wykształcenie wyższe oraz wykształcenie wyższe prawnicze (stan na 31 grudnia 2024 r.):

- wykształcenie wyższe ogółem – 244 osoby,
- w tym wykształcenie wyższe prawnicze – 149 osób.

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 2024 r.

Plan finansowy UODO w 2024 r. w wysokości 54 828 000 zł przedstawiał się następująco:

- wynagrodzenia 35 470 000 zł
- pochodne od wynagrodzeń 6 513 000 zł
- wydatki majątkowe 2 123 000 zł
- pozostałe wydatki 10 722 000 zł

Wydatki zrealizowane przez UODO w 2024 r. objęły:

- wynagrodzenia 35 468 445,33 zł
- pochodne od wynagrodzeń 6 500 980,11 zł
- wydatki majątkowe 2 105 461,49 zł
- pozostałe wydatki 10 640 958,69 zł

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI

1. Wydawanie decyzji administracyjnych i rozpatrywanie skarg

W okresie od 1 stycznia 2024 r. do 31 grudnia 2024 r. w sprawach dotyczących **skarg** obywateli wydanych zostało łącznie **1670 decyzji administracyjnych.** W decyzjach tych Prezes UODO w 876 przypadkach w oparciu o art. 58 RODO zastosował środki naprawcze, w tym:

- w 555 sprawach udzielił upomnienia za naruszenie przepisów RODO, zaś
- w 321 przypadkach zastosował środek naprawczy w postaci nakazu.

Liczba zastosowanych przez organ nadzorczy środków naprawczych w sprawach skargowych nieznacznie spadła w stosunku do roku 2023 r., w którym Prezes UODO zastosował środki naprawcze w 965 sprawach, w tym w 630 sprawach udzielił upomnienia, zaś w 335 przypadkach zastosował środek naprawczy w postaci nakazu.

W roku 2024 Prezes UODO wydał ogółem **1719 decyzji administracyjnych,** na które złożyło się:

- 1670 decyzji w sprawach skargowych;
- 20 decyzji dotyczących naruszeń;
- 7 decyzji dotyczących kontroli.
- 22 decyzje w sprawach nałożenia administracyjnych kar pieniężnych.

Rozpatrywanie skarg, zgodnie z art. 57 ust. 1 lit. f 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) jest jednym z głównych zadań Prezesa Urzędu Ochrony Danych Osobowych[13] jako organu nadzorczego. Wpływ skargi do Prezesa UODO inicjuje postępowanie administracyjne, zmierzające do rozstrzygnięcia sprawy poprzez wydanie decyzji administracyjnej.

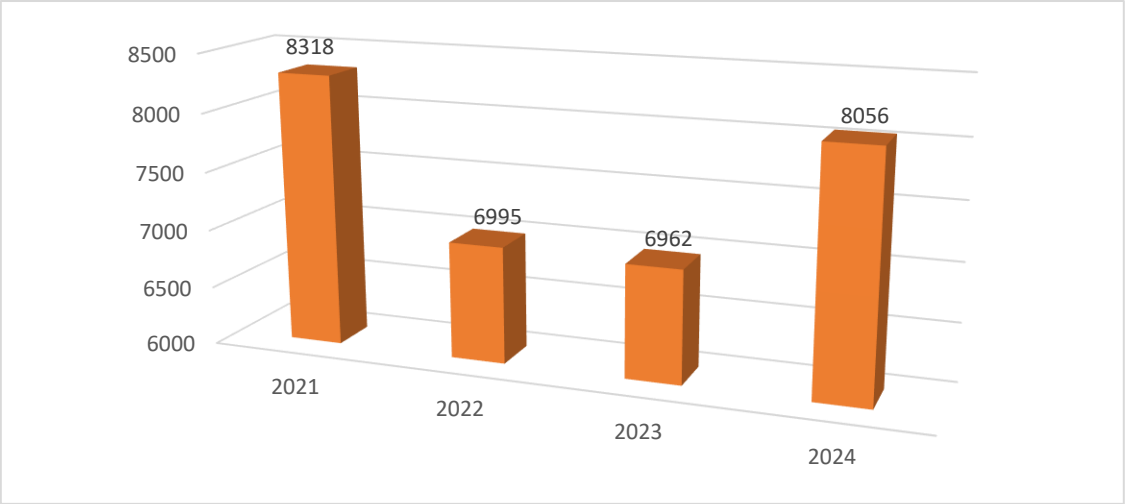
Każda ze skarg analizowana jest na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami ustawy z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[14]. W sytuacji gdy skarga nie spełniała warunków wymaganych przez ww. przepisy prawa, organ właściwy do spraw ochrony danych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

W 2024 r., podobnie jak w latach ubiegłych, 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, w pierwszej kolejności skarżony podmiot wzywany był do złożenia wyjaśnień, przedłożenie dowodów na ich poparcie oraz odniesienie się do zarzutów. O wszczęciu postępowania administracyjnego informowany był zarówno podmiot wzywany, jak i osoba, która złożyła skargę. 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.

W okresie od 1 stycznia 2024 r. do 31 grudnia 2024 r. Prezes Urzędu Ochrony Danych Osobowych prowadził postępowania administracyjne, wszczęte w wyniku skarg wniesionych w roku 2024, jak i w latach poprzednich, które toczyły się zgodnie z przepisami ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz na podstawie przepisów k.p.a., zgodnie z art. 7 ust. 1 ww. ustawy o ochronie danych osobowych.

W roku 2024 r. do Departamentu Skarg Urzędu Ochrony Danych Osobowych wpłynęły 8056 skarg krajowych, a zatem wpływ w stosunku do poprzedniego roku, w którym wpłynęło 6962 skargi, zwiększył się o 16 %.

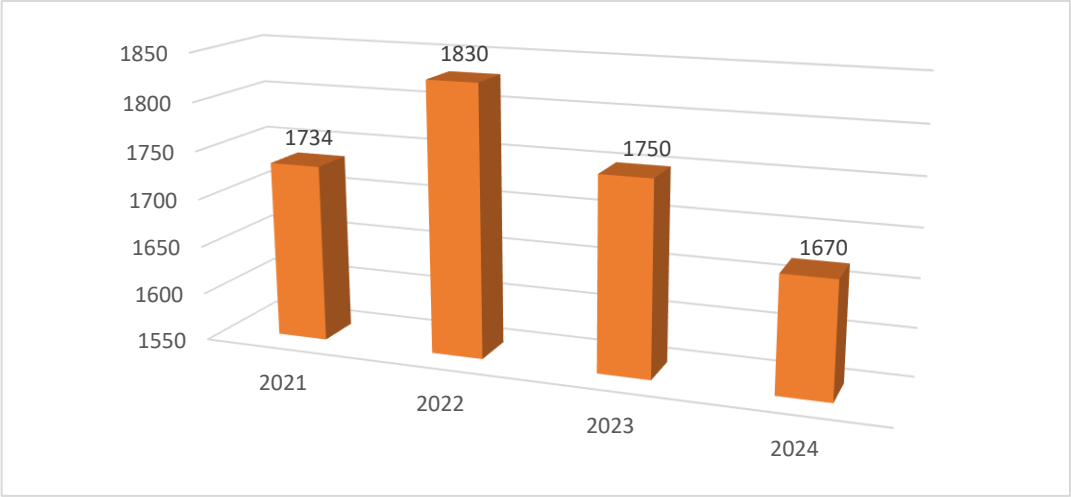
[13] Dalej także „Prezes UODO”.
[14] Dz. U. z 2024 r. poz. 572 ze zm., dalej jako k.p.a.



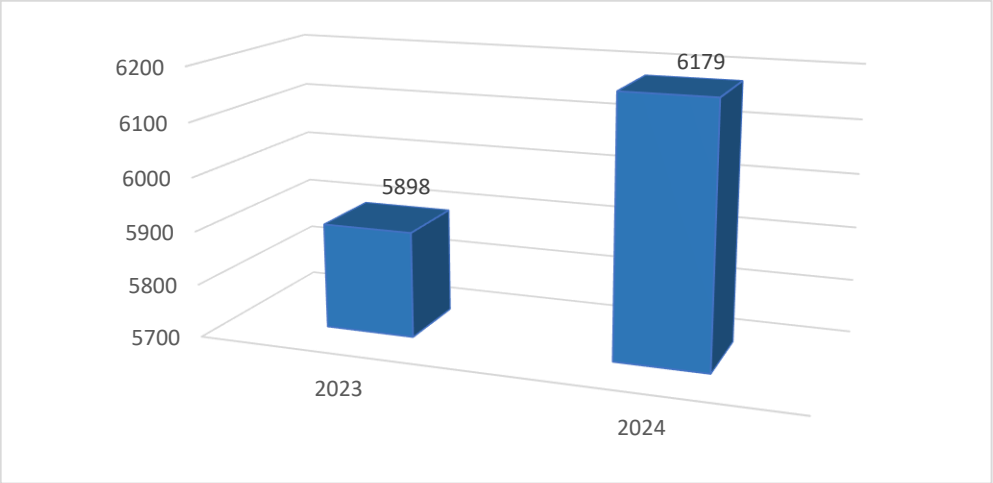
Wykres 1. Liczba skarg krajowych, które wpłynęły do UODO w latach 2021–2024.

W roku 2024 wydaniem decyzji administracyjnych zakończyło się 1670 spraw skargowych. Liczba wydanych przez Prezesa UODO decyzji administracyjnych w sprawach zainicjowanych skargami osób, których dane dotyczą, w 2024 r. nieznacznie spadła w stosunku do ubiegłych lat (w 2023 roku wydanych zostało 1750 decyzji, a w 2022 roku 1830 decyzji). Powyższy spadek nie oznacza jednak zmniejszenia aktywności organu w rozpatrywaniu skarg, gdyż łączna liczba spraw zakończonych w 2024 r. wzrosła w stosunku do roku poprzedniego o 281 spraw i wyniosła 6179 spraw, podczas gdy w roku 2023 zakończono 5898 spraw. Nie wszystkie skargi wnoszone do Prezesa UODO kończą się wydaniem decyzji administracyjnych i jest to niezależne od organu nadzorczego prowadzącego postępowania. Sposób zakończenia postępowania administracyjnego w sprawie skargowej jest uzależniony od konkretnej sprawy, przedmiotu wniesionej skargi, a także od zachowania skarżącego w przypadku, gdy skarga obarczona jest brakami formalnymi. Z tych powodów część spraw kończy się wydaniem postanowienia o odmowie wszczęcia postępowania lub pozostawieniem sprawy bez rozpoznania, np. w związku z nieuzupełnieniem braków formalnych skargi. Oceniając aktywność polskiego organu nadzorczego w sprawach skargowych, nie można pominąć, że w roku 2024 r. liczba wniesionych do tego organu skarg wzrosła o 1094 skargi w stosunku do roku poprzedniego. Wzrost liczby spraw zakończonych w 2024 r., pomimo zwiększonego obciążenia organu liczbą prowadzonych postępowań administracyjnych w ograniczonych warunkach kadrowych, świadczy zatem o poprawie wydajności w rozpatrywaniu spraw skargowych.

W roku 2024 Prezes UODO nie kierował w związku z rozpatrywaniem spraw skargowych zawiadomień o podejrzeniu popełnienia przestępstwa.



Wykres 2. Liczba decyzji administracyjnych wydanych w sprawach zainicjowanych indywidualną skargą, wydanych w latach 2021–2024.

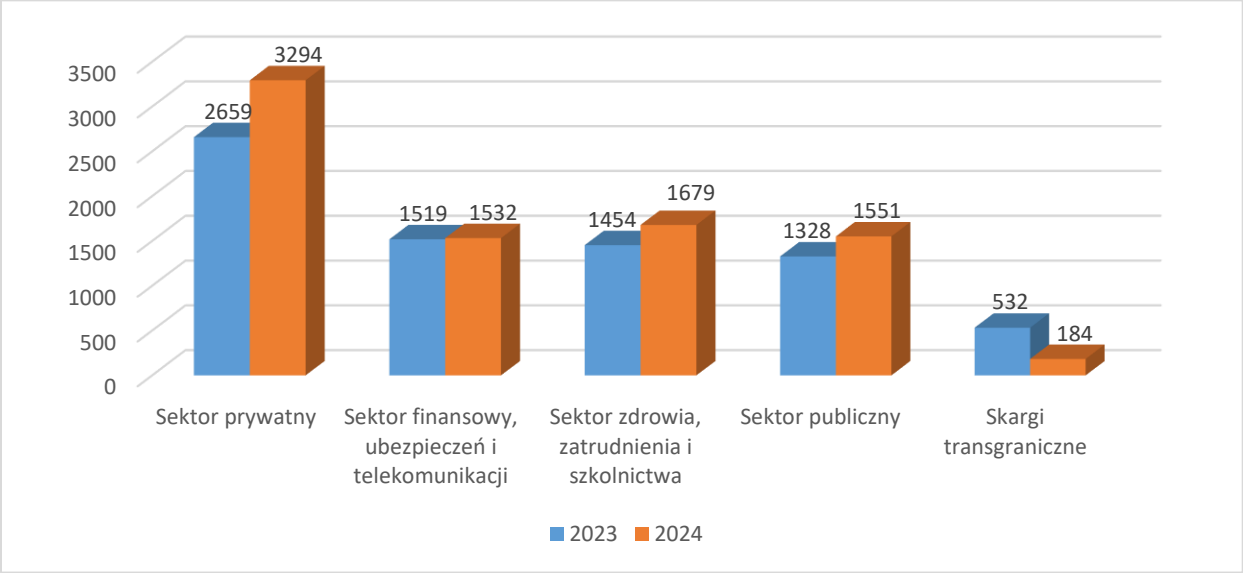


Wykres 3. Liczba spraw zakończonych w latach 2023–2024, zainicjowanych indywidualną skargą.

Uwzględniając podział skarg krajowych, które wpłynęły w 2024 na poszczególne sektory, liczba otrzymanych skarg przedstawia się następująco:

- 3294 skargi na podmioty sektora prywatnego *(z wyłączeniem skarg dot. sektora finansowego, ubezpieczeń i telekomunikacji oraz zdrowia, zatrudnienia i szkolnictwa)* (2659 skarg w roku 2023),
- 1532 skargi na podmioty sektora finansowego, ubezpieczeń i telekomunikacji (1519 skarg w roku 2023),
- 1679 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa (1454 w roku 2023),
- 1551 skarg na podmioty sektora publicznego *(z wyłączeniem skarg dot. sektora zdrowia, zatrudnienia i szkolnictwa)* (1328 w roku 2023).

Ponadto w 2024 roku do Urzędu wpłynęły 184 skargi transgraniczne (532 w roku 2023).



Wykres 4. Liczba skarg, które wpłynęły do UODO w latach 2023–2024 z podziałem na sektory.

W roku 2024 spadek liczby wnoszonych skarg odnotowano jedynie w sektorze transgranicznym, w pozostałych sektorach liczba wnoszonych skarg wzrosła.

Wśród skarg na podmioty z sektora publicznego najwięcej dotyczyło udostępnienia danych osobowych na stronach internetowych Biuletynu Informacji Publicznej (BIP), a także udostępnienia danych osobowych osób zgłaszających nieprawidłowości do organów (np. w zakresie samowoli budowlanych, wycinki drzew) oraz udostępnienia danych osobowych podczas obrad kolegialnych organów jednostek samorządu terytorialnego, a także w nagraniach z takich obrad.

Wśród skarg na podmioty z sektora finansowego niezmiennie w stosunku do lat ubiegłych najwięcej dotyczyło umów zawieranych z bankami i instytucjami kredytowymi.

Skargi na podmioty z sektora zdrowia często dotyczyły wystawiania recept przez lekarzy z wykorzystaniem danych 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.

W każdym spośród wskazanych wyżej sektorów, podobnie jak w latach ubiegłych, osoby, których dane dotyczą, często skarżyły się na przetwarzanie ich danych osobowych bez podstawy prawnej, w tym na 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 także 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 wykazuje zauważalny wzrost świadomości w zakresie ochrony danych osobowych osób wnoszących skargi, Prezes UODO niezmiennie 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 bowiem właściwie określić naruszenia przepisów RODO, przez co zdarzało się, że ich żądania wykraczały poza kompetencje Prezesa UODO. Skarżący w roku 2024 zwracali się do organu m.in. w sprawach dotyczących naruszenia tajemnicy korespondencji, naruszenia dóbr osobistych, ścigania przestępstw, przyznania odszkodowania za naruszenia ochrony danych osobowych. W takich przypadkach organ informował, gdzie dana osoba powinna zgłosić się z żądaniami, których realizacja pozostaje poza jego kompetencjami, wskazując 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.

Ze strony administratorów Prezes UODO również odnotowuje rosnącą świadomość spoczywających na nich obowiązków, zwłaszcza w zakresie obowiązku przetwarzania danych w sposób rzetelny i przejrzysty dla osób, których dane dotyczą. Administratorzy częściej tworzą dokumenty obejmujące politykę przetwarzania danych oraz stosują pisemne klauzule informacyjne o przetwarzaniu danych.

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

Administratorzy danych wzywani do wyjaśnień najczęściej byli w stanie opisać jedynie cel przetwarzania danych; nie zawsze zaś byli w stanie wskazać podstawy prawne, w oparciu o które przetwarzali dane osobowe skarżących.

Prezes UODO podobnie jak w latach poprzednich obserwował, że administratorzy często uchybiali terminowi na spełnienie żądania osoby, której dane dotyczą.

Dodatkowo podmioty, względem których organ skorzystał wcześniej z uprawnień naprawczych, o których mowa w art. 58 ust. 2 RODO z uwagi na stwierdzone nieprawidłowości, podchodziły z większą ostrożnością i dbałością do realizowanych przez siebie operacji przetwarzania danych osobowych.

1.1. Sektor publiczny

Wśród skarg wpływających do organu na podmioty z sektora publicznego, podobnie jak w latach ubiegłych, również w analizowanym okresie sprawozdawczym organ właściwy do spraw ochrony danych osobowych odnotował liczne skargi dotyczące udostępnienia danych osobowych. Najczęściej skargi te dotyczyły

udostępnienia danych osobowych na stronach internetowych Biuletynu Informacji Publicznej[15].

1.1.1. Udostępnienie danych osobowych na stronie internetowej BIP urzędu wojewódzkiego

Prezes UODO w 2024 r. rozpatrywał skargę na udostępnienie przez wojewodę danych osobowych skarżącej w postaci imienia i nazwiska na stronie internetowej BIP urzędu wojewódzkiego. Ustalono, że wojewoda rozpatrywał petycję skarżącej oraz innych mieszkańców gminy. Z uwagi na obowiązek publikacji petycji wojewoda opublikował na stronie internetowej BIP urzędu wojewódzkiego metrykę dotyczącą przebiegu postępowania w sprawie petycji złożonej przez skarżącą, która zawierała jej dane osobowe w postaci imienia i nazwiska. W trakcie prowadzonego postępowania ustalono, że skarżąca pisemnie powiadomiła wojewodę o opublikowaniu jej danych osobowych. Na skutek tego pisma wojewoda usunął dane osobowe skarżącej opublikowane na stronie internetowej BIP urzędu wojewódzkiego. Z zebranego materiału dowodowego wynikało, że skarżąca, składając wraz z innymi mieszkańcami petycję, nie wyraziła zgody na publikację jej danych osobowych na stronie internetowej. Prezes UODO zwrócił uwagę na art. 8 ustawy z 11 lipca 2014 r. o petycjach[16], który zezwala na upublicznienie danych osobowych osoby składającej petycję w postaci imienia i nazwiska pod warunkiem wyrażenia przez tę osobę zgody na publikację jej danych osobowych. W przypadku niewyrażenia takiej zgody brak jest podstaw do upublicznienia danych osobowych wnoszącego petycję. Wobec tego metryka dotycząca przebiegu postępowania w sprawie złożonej przez skarżącą petycji powinna zostać umieszczona na stronie internetowej podmiotu rozpatrującego petycję po uprzedniej anonimizacji danych osobowych skarżącej. W ocenie Prezesa UODO wojewoda, publikując dane osobowe skarżącej, nie legitymował się żadną spośród przesłanek określonych w art. 6 ust. 1 RODO, która stanowiłaby o legalności tego udostępnienia, co przesądza o tym, że ww. udostępnienie danych nastąpiło bez podstawy prawnej. Za powyższe naruszenie Prezes UODO udzielił wojewodzie upomnienia[17].

W innej sprawie, dotyczącej udostępnienia przez wojewodę danych osobowych skarżącego w postaci imienia i nazwiska na stronie internetowej BIP urzędu wojewódzkiego ustalono, że skarżący złożył skargę na radną do rady gminy. Rada gminy podjęła uchwałę o przekazaniu skargi do wojewody. W związku z tą uchwałą wojewoda wydał rozstrzygnięcie nadzorcze i następnie z uwagi na obowiązek ustawowy opublikował je na stronie internetowej BIP urzędu wojewódzkiego. Rozstrzygnięcie nadzorcze zawierało dane osobowe skarżącego w postaci imienia i nazwiska jako osoby, która wniosła skargę do rady gminy. Dane osobowe skarżącego udostępnione na stronie internetowej BIP urzędu wojewódzkiego zostały następnie przez wojewodę zanonimizowane. Prezes UODO uznał w tej sprawie, że przy realizacji

[15] Dalej również jako BIP.
[16] Dz.U. z 2018 r. poz. 870, dalej również jako ustawa o petycjach.
[17] DS.523.1030.2023.

obowiązku opublikowania na stronie BIP urzędu wojewódzkiego rozstrzygnięcia nadzorczego wojewody, w którego treści ujawniono imię i nazwisko skarżącego, nie uwzględniono prawa do prywatności skarżącego. Z materiału dowodowego zebranego w tej sprawie nie wynikało, aby skarżący, wnosząc skargę na radną rady gminy, zrezygnował z prawa do prywatności lub występował jako osoba pełniąca funkcją publiczną. Prezes UODO stwierdził, że przy upublicznieniu dokumentu urzędowego jedynie w celu informacyjnym zbędne było (nieadekwatne do uzyskania celu) ujawnienie danych osobowych skarżącego w postaci jego imienia i nazwiska jako osoby, która wniosła skargę do rady gminy. Publikacja dokumentu, który zawiera dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna była nastąpić po odpowiednim przetworzeniu danych osobowych w nim zawartych. Oznacza to, że rozstrzygnięcie nadzorcze powinno było zostać upublicznione po uprzednim usunięciu z niego danych osobowych skarżącego. W konsekwencji udostępnienie danych osobowych skarżącego w postaci imienia i nazwiska w rozstrzygnięciu nadzorczym wojewody opublikowanym na stronie BIP urzędu wojewódzkiego nie znajdowało oparcia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO oraz naruszyło jedną z podstawowych zasad dotyczących przetwarzania danych, tj. zasadę minimalizacji danych. Za powyższe naruszenie Prezes UODO udzielił wojewodzie upomnienia[18].

1.1.2. Udostępnienie danych osobowych podczas sesji rady gminy, na nagraniu z sesji rady gminy na stronie internetowej oraz w protokole z sesji rady gminy

Przedmiotem skargi było udostępnienie danych osobowych skarżącego przez wójta podczas sesji rady gminy, na nagraniu z sesji rady gminy zamieszczonym na stronie internetowej oraz w protokole z sesji rady gminy oraz udostępnienie danych osobowych przez radę gminy na nagraniu z sesji rady gminy na stronie internetowej. Skarżący wniósł do urzędu gminy za pomocą platformy ePUAP skargi na wójta. Skargi te zostały przekazane radzie na podstawie art. 18b ustawy z 8 marca 1990 r. o samorządzie gminnym[19]. Rada jako organ właściwy rozpatrywała skargi skarżącego na dwóch posiedzeniach. Podczas obu sesji wójt udostępnił nazwisko skarżącego, a przewodniczący rady imię skarżącego. Ww. sesje rady gminy były nagrywane, a nagrania zostały umieszczone przez pracownika urzędu gminy bez anonimizacji na stronach internetowych urzędu gminy. W ocenie Prezesa UODO upublicznienie danych osobowych skarżącego w postaci nazwiska przez wójta podczas dyskusji na sesji rady nad skargami skarżącego nie znalazło oparcia w żadnej z przesłanek wskazanych w art. 6 ust. 1 RODO, ponieważ nie było niezbędne do rozpatrzenia wniesionych skarg.

Obrady sesji mają 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 i dyskutować o nich

[18] DS.523.1369.2023.
[19] Dz.U. z 2024 r. poz. 1465 ze zm. dalej także jako u.s.g.

w sposób zapewniający odpowiedni stopień ochrony danych osobowych w nich zawartych. Skarżący, wnosząc skargi na wójta, nie pełnił funkcji publicznej ani nie zrezygnował ze swojego prawa do prywatności w tym zakresie. Wójt, jako administrator danych osobowych skarżącego zawartych w skardze, zobowiązany był przetwarzać je tak, by nie naruszać przepisów o ochronie danych osobowych, w tym art. 6 ust. 1 RODO oraz zasad przetwarzania danych wyrażonych w RODO, m.in. zasady minimalizacji danych określonej w art. 5 ust. 1 lit. c RODO. W związku z zarzutem upublicznienia przez wójta danych osobowych skarżącego w nagraniach z sesji rady gminy Prezes UODO zwrócił uwagę na art. 5 ust. 2 ustawy z 6 września 2001 r. o dostępie do informacji publicznej[20]. Publikacja nagrań zawierających dane osobowe w zakresie, który może powodować naruszenie prawa do prywatności, powinna nastąpić po odpowiednim przetworzeniu danych osobowych w nich zawartych. Przy upublicznieniu ww. nagrań zbędne było (nieadekwatne do celu) ujawnienie imienia i nazwiska skarżącego, jako osoby składającej skargi na wójta. Prezes UODO uznał za zasadne skorzystanie z instrumentu o charakterze naprawczym przewidzianego w art. 58 ust. 2 lit. b RODO i udzielił upomnienia wójtowi za udostępnienie danych osobowych skarżącego w postaci imienia i nazwiska podczas sesji rady gminy. W pozostałym zakresie Prezes UODO umorzył postępowanie[21].

1.1.3. Udostępnienie przez komendanta powiatowego państwowej straży pożarnej (KPPSP) danych osobowych na stronie internetowej komendy powiatowej państwowej straży pożarnej

Przedmiotem skargi było udostępnienie przez komendanta powiatowego państwowej straży pożarnej[22] danych osobowych skarżącej w postaci imienia i nazwiska na stronie internetowej komendy powiatowej państwowej straży pożarnej. Ustalono, że KPPSP w związku ze złożonym przez skarżącą wnioskiem o udostępnienie informacji publicznej zamieścił na stronie internetowej komendy oraz na stronie internetowej BIP wnioskowane przez skarżącą dokumenty. Opublikowane dokumenty zawierały dane osobowe skarżącej w postaci imienia i nazwiska. Po uzyskaniu informacji od skarżącej o udostępnieniu jej danych osobowych KPPSP usunął zamieszczone na ww. stronach internetowych dokumenty. Prezes UODO uznał, że przedmiotowe udostępnienie danych osobowych skarżącej, które, jak wynikało z wyjaśnień KPPSP, nastąpiło w wyniku pomyłki pracownika komendy powiatowej państwowej straży pożarnej, nie znajdowało oparcia w żadnej spośród przesłanek określonych w art. 6 ust. 1 RODO stanowiących o legalności przetwarzania danych osobowych. Prezes UODO udzielił KPPSP upomnienia w związku z zaistniałym naruszeniem art. 6 ust. 1 RODO[23].

[20] Dz.U. z 2022 r. poz. 902, dalej także jako d.d.i.p.
[21] DS.523.3773.2022.
[22] Dalej także jako KPPSP.
[23] DS.523.2059.2023.

1.1.4. Udostępnienie danych osobowych zawartych w zawiadomieniu powiatowego inspektora nadzoru budowlanego (PINB) o sposobie załatwienia skargi na rzecz podmiotów wskazanych w polu „do wiadomości" tego zawiadomienia

Prezes UODO przeprowadził postępowanie administracyjne w sprawie udostępnienia danych osobowych skarżącej zawartych w zawiadomieniu powiatowego inspektora nadzoru budowlanego[24] (PINB) o sposobie załatwienia skargi, na rzecz podmiotów wskazanych w polu „do wiadomości" tego zawiadomienia. Prezes UODO ustalił, że skarżąca zwróciła się do PINB z wnioskiem o udzielenie informacji, na jakiej podstawie rozpoczęto prace budowlane na działkach położonych w jej miejscowości. Skarżąca poinformowała PINB o nieumieszczeniu tablicy informującej o robotach budowlanych prowadzonych na działkach, nieprawidłowym umieszczeniu skrzynki energii elektrycznej oraz o zmianach w wyznaczeniu granicy tych działek. PINB po otrzymaniu pisma skarżącej przeprowadził kontrolę legalności robót budowlanych prowadzonych na działkach wskazanych w piśmie skarżącej. PINB w „Zawiadomieniu o sposobie rozpatrzenia skargi" poinformował skarżącą o wynikach przeprowadzonej kontroli na ww. działkach. Zawiadomienie to PINB wysłał do podmiotów wymienionych w polu „do wiadomości" – właścicieli nieruchomości, której dotyczyła kontrola przeprowadzona przez PINB. W ocenie Prezesa UODO udostępnienie przez PINB danych osobowych skarżącej, zawartych w skierowanym do niej zawiadomieniu PINB o sposobie załatwienia skargi, na rzecz właścicieli nieruchomości, której dotyczyła kontrola przeprowadzona przez PINB, było nieuzasadnione. Dane osobowe osoby zawiadamiającej organ o potencjalnych nieprawidłowościach powinny co do zasady pozostać poufne w ramach postępowania prowadzonego przez organ z urzędu, w sytuacji gdy nie jest ona stroną postępowania wszczętego na skutek otrzymanego od niej zgłoszenia, i nie mogą być ujawniane w toku postępowania stronom i uczestnikom tego postępowania. Prezes UODO podkreślił, że wysłanie do skarżącej zawiadomienia o sposobie załatwienia skargi nie uzasadniało w żaden sposób udostępnienia zawartych w tym zawiadomieniu danych osobowych skarżącej na rzecz właścicieli nieruchomości, której dotyczyła kontrola przeprowadzona przez PINB. 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 uwagi na powyższe, uwzględniając przede wszystkim wagę stwierdzonego naruszenia oraz jego nieodwracalny charakter, Prezes UODO udzielił PINB upomnienia[25].

1.1.5. Udostępnienie danych osobowych skarżącego w związku z zawiadomieniem powiatowego inspektora nadzoru budowanego o wyznaczeniu kontroli w sprawie stanu technicznego zbiornika na nieczystości ciekłe

[24] Dalej także jako PINB.
[25] DS.523.3975.2020.

Przedmiotem jednej ze skarg, było udostępnienie danych osobowych skarżącego w postaci imienia, nazwiska, adresu zamieszkania i numeru PESEL zawartych we wnioskach skierowanych do PINB o wszczęcie kontroli w sprawie stanu technicznego zbiornika na nieczystości ciekłe na wskazanych przez skarżącego nieruchomościach. Dane osobowe skarżącego jako osoby, która złożyła wniosek o przeprowadzenie kontroli, na skutek którego organ podjął czynności z urzędu, zostały udostępnione na rzecz właścicieli nieruchomości, których dotyczyło zgłoszenie skarżącego. PINB nie wykazał w toku postępowania, aby ujawnienie danych osobowych skarżącego jako osoby, która złożyła wniosek o przeprowadzenie kontroli, na skutek którego PINB z urzędu podjął czynności kontrolne, było niezbędne do ich przeprowadzenia. Prezes UODO stwierdził, że udostępnienie przez PINB danych osobowych skarżącego w postaci imienia i nazwiska, jako osoby, która zawiadomiła organ o potencjalnych nieprawidłowościach, na rzecz właścicieli nieruchomości, których dotyczyło zgłoszenie skarżącego, nie było niezbędne do wypełnienia obowiązku prawnego ciążącego na PINB jako administratorze danych i nie mogło tym samym znaleźć oparcia w art. 6 ust. 1 lit. c RODO. PINB nie legitymował się ponadto żadną z pozostałych określonych w art. 6 ust. 1 RODO przesłanek stanowiących o legalności przetwarzania danych osobowych. Udostępnienie danych osobowych skarżącego nastąpiło bez podstawy prawnej i naruszało zasadę minimalizacji danych (art. 5 ust. 1 lit. c RODO). Prezes UODO skorzystał ze środka przewidzianego w art. 58 ust. 2 lit. b RODO i udzielił PINB upomnienia za ww. naruszenie[26].

1.1.6. Udostępnienie danych osobowych osoby zgłaszającej wycinkę zalesienia

Przedmiotem jednej ze skarg było udostępnienie przez regionalnego dyrektora ochrony środowiska (RDOŚ) danych osobowych skarżącej w postaci imienia i nazwiska, zawartych w odpowiedzi na jej zawiadomienie o wycince zalesienia na terenie NATURA 2000, na rzecz osób, które dokonały tej wycinki. Pracownik RDOŚ udzielił odpowiedzi skarżącej na jej zgłoszenie i wezwał do złożenia wyjaśnień osoby, które według zawiadomienia miały dokonać wycinki. Jednocześnie przesłał ww. osobom za pośrednictwem poczty elektronicznej odpowiedź skierowaną do skarżącej zawierającą jej dane osobowe w postaci imienia i nazwiska. RDOŚ w prowadzonym postępowaniu nie wykazał podstaw prawnych oraz celu udostępnienia danych osobowych skarżącej oraz przyznał, że doszło do niego na skutek omyłki pracownika. Prezes UODO uznał za nieuzasadnione ww. udostępnienie przez RDOŚ danych osobowych skarżącej. Działanie takie nie znajduje podstaw w przepisach k.p.a. Przepisy k.p.a. wyposażają bowiem organ w instrumenty pozwalające na zbadanie sygnalizowanych przez obywateli nieprawidłowości poprzez wszczęcie postępowania z urzędu, które może być przeprowadzone bez konieczności ujawniania źródła informacji. W związku z powyższym Prezes UODO skorzystał z przysługującego mu uprawnienia i udzielił RDOŚ w oparciu o art. 58 ust. 2 lit. b RODO upomnienie za naruszenie art. 6 ust. 1 RODO[27].

[26] DS.523.142.2024.
[27] DS.523.4456.2022.

1.1.7. Udostępnienie przez komornika na kopercie korespondencji informacji o zajęciu wynagrodzenia za pracę

W 2024 r. Prezes UODO prowadził postępowanie administracyjne w sprawie udostępnienia przez komornika sądowego danych osobowych skarżącego w zakresie informacji o zajęciu wynagrodzenia za pracę na kopercie. Prezes UODO ustalił, że komornik sądowy udostępnił na kopercie, której zawartość stanowiło pismo do skarżącego, oprócz imienia, nazwiska i adresu zamieszkania skarżącego również informację o zajęciu wynagrodzenia skarżącego. Prezes UODO uznał, że doszło do naruszenia ochrony danych osobowych skarżącego przez komornika sądowego. Prezes UODO zwrócił uwagę, że zgodnie z przywołanym przez komornika § 17 ust. 3 rozporządzenia Ministra Sprawiedliwości z 18 grudnia 2018 r. w sprawie określenia szczegółowych zasad prowadzenia biurowości, rachunkowości i ewidencji operacji finansowych kancelarii komorniczych[28], jeżeli w jednej sprawie komornik dokonuje doręczenia kilku pism jedną przesyłką, na zwrotnym potwierdzeniu odbioru należy zamieścić informacje pozwalające w sposób jednoznaczny ustalić zawartość przesyłki. Ww. przepis odnosi się zatem do informacji zamieszczanych na zwrotnym potwierdzeniu odbioru w przypadku doręczenia kilku pism jedną przesyłką, natomiast nie dotyczy informacji (danych osobowych) zamieszczanych na kopercie. Dlatego ww. przepisy prawa nie znajdują zastosowania do analizowanego stanu faktycznego i nie stanowiły podstawy do zamieszczenia przez komornika na kopercie adnotacji dotyczącej zawartości przesyłki. Prezes UODO wskazał, że na kopercie powinny być zamieszczone jedynie te dane osobowe, które są niezbędne do dostarczenia korespondencji – za takie dane nie można uznać jednak informacji o zajęciu wynagrodzenia za pracę, która została zamieszczona przez komornika sądowego na kopercie przesyłki skierowanej do skarżącego. Prezes UODO uznał, że skarżone udostępnienie danych osobowych nie miało uzasadnienia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO i udzielił komornikowi sądowemu upomnienie za stwierdzone naruszenie przepisów o ochronie danych osobowych[29].

1.1.8. Udostępnienie danych osobowych w korespondencji e-mail poprzez niezastosowanie opcji „UDW”

Przedmiotem innej skargi było udostępnienie przez powiatowy ośrodek dokumentacji geodezyjnej i kartograficznej (PODGiK) danych osobowych skarżącego w postaci imienia, nazwiska i adresu e-mail, jako jednego z wielu adresatów wiadomości e-mail dotyczącej sposobu przekazywania dokumentacji z wykonania prac geodezyjnych, wysłanej przez dyrektora tego ośrodka do dużej liczby adresatów. Prezes UODO w wydanej decyzji wskazał, że zakres danych i informacji udostępnianych innym adresatom wiadomości e-mail powinien być adekwatny do ich potrzeb związanych ze zgodnym z prawem celem udostępnienia. Prezes UODO stwierdził, że PODGiK nie dochował należytej staranności przy przetwarzaniu danych

[28] Dz. U. poz. 2517.
[29] DS.523.1936.2024.

osobowych skarżącego, naruszając tym samym zasadę minimalizacji danych uregulowaną w art. 5 ust. 1 lit. c RODO. Prezes UODO zwrócił uwagę na charakter przesłanej wiadomości e-mail, która dotyczyła sposobu przekazywania dokumentacji z wykonania prac geodezyjnych. Tego rodzaju korespondencja wystosowana do wielu adresatów, w tym skarżącego, nie wymagała udostępnienia danych osobowych skarżącego w postaci imienia, nazwiska i adresu e-mail. W ocenie Prezesa UODO nie było to działanie niezbędne do realizacji celu, jakim było przedstawienie odbiorcom informacji o formacie, w którym powinny być zapisywane pliki dotyczące wykonania prac geodezyjnych. PODGiK podczas wysyłania korespondencji zbiorczej powinien skorzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie widzą wzajemnie swoich adresów e-mail oraz innych danych przypisanych do tego adresu. Udostępnienie danych osobowych skarżącego w wiadomości e-mail PODGiK nie znajdowało oparcia w żadnej z przesłanek określonych w art. 6 ust. 1 RODO, dlatego korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b RODO, Prezes UODO udzielił PODGiK upomnienie za stwierdzone naruszenie[30].

1.1.9. Przetwarzanie danych osobowych przez Komendanta Głównego Policji (KGP) w wykazie cudzoziemców oraz w Systemie Informacyjnym Schengen (SIS)

Przedmiotem jednej ze spraw było przetwarzanie przez Komendanta Głównego Policji danych osobowych skarżącego w Systemie Informacyjnym Schengen. Dane skarżącego zostały zamieszczone w wykazie cudzoziemców, których pobyt na terytorium Rzeczypospolitej Polskiej jest niepożądany, oraz w SIS do celów odmowy wjazdu na terytorium Schengen na podstawie wpisu szefa urzędu ds. cudzoziemców. Wpis został umieszczony na podstawie wniosku Komendanta Głównego Policji. Podstawą wpisu było uznanie, że wjazd i pobyt skarżącego stanowił zagrożenie dla bezpieczeństwa i porządku publicznego[31]. Ponadto dane osobowe skarżącego zostały przekazane do SIS do celów odmowy wjazdu na okres ich przechowywania w wykazie[32]. Z uwagi na to, że w trakcie postępowania Prezes UODO ustalił, że dane osobowe skarżącego nie są już przetwarzane w SIS, w związku z wygaśnięciem wpisu dokonanego przez szefa urzędu ds. cudzoziemców na skutek upływu terminu figurowania danych w SIS II[33], z uwagi na ich usunięcie, umorzył postępowanie[34].

1.2. Sektor prywatny

1.2.1. Przetwarzanie danych z wykorzystaniem monitoringu wizyjnego

[30] DS.523.3091.2021.
[31] Art. 435 ust. 1 pkt 4 w związku z art. 438 ust. 1 pkt 8 ustawy z 12 grudnia 2013 r. o cudzoziemcach (Dz.U. z 2024 r. poz. 769 ze zm.), dalej także jako ustawa o cudzoziemcach.
[32] Art. 443 ust. 1 pkt 3 ustawy z 12 grudnia 20213 r. o cudzoziemcach.
[33] Rozporządzenie (WE) Nr 1987/2006 Parlamentu Europejskiego i Rady z 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 381/4 z 28.12.2006 r. z późn. zm.).
[34] DS.523.1201.2023.

W jednej ze spraw[35] rodzina złożyła skargę na przetwarzanie danych osobowych bez podstawy prawnej za pomocą monitoringu wizyjnego. Skarżący w godzinach wieczornych zorientowali się, że w wynajmowanym apartamencie zamontowane jest urządzenie przypominające czujkę ruchu wyposażone w rejestrator wideo. Urządzenie zostało zabezpieczone przez policję.

Skarżona wyjaśniła, że zainstalowanie urządzenia miało na celu zapewnienie bezpieczeństwa osobom w nim przebywającym oraz zapobieżenie dokonaniu ewentualnych zniszczeń lub kradzieży. Skarżona wyjaśniła, że nie zna dokładnych właściwości i możliwości technicznych zainstalowanego urządzenia rejestrującego, ponieważ go nie zakupiła ani nie montowała. Prezes UODO nie dał wiary ww. wyjaśnieniom, ze względu na to, że to skarżona zleciła jego montaż oraz otrzymywała zdalnie informacje o obecności w lokalu.

Postępowanie wykazało, że zasięgiem monitoringu wizyjnego objęta była przestrzeń wewnątrz apartamentu przeznaczonego na wynajem. Prezes UODO wskazał, że w związku ze świadczoną usługą wynajmu lokalu – prawa właściciela do swobodnego korzystania z nieruchomości zostają ograniczone, w tym w zakresie możliwości prowadzenia monitoringu wizyjnego. W tym zakresie odwołano się do przepisów kodeksu cywilnego, zgodnie z którymi do ochrony praw najemcy do użytku lokalu stosuje się przepisy o ochronie własności[36]. Skarżona w takiej sytuacji obowiązana była do respektowania praw skarżących, a jej interes w zabezpieczeniu mienia nie przeważał nad ich prawem do ochrony danych osobowych.

Prezes UODO podkreślił, że monitoring wizyjny jest jedną z najbardziej inwazyjnych form ingerencji w podstawowe prawa lub wolności osoby, której dane dotyczą i powinien być wybierany wyłącznie wówczas, kiedy zawiodły inne, alternatywne środki bezpieczeństwa, takie jak systemy antywłamaniowe, zainstalowane zabezpieczenia w oknach i drzwiach, a więc środki, które są mniej inwazyjne w stosunku do podstawowych praw lub wolności innych osób. Sposobem ochrony praw nie mogą być urządzenia, które powodują naruszenie praw innych osób, tak jak to było w niniejszej sprawie. Prezes UODO stwierdził, że przetwarzanie danych osobowych za pomocą monitoringu wizyjnego obejmującego wnętrze wynajmowanego apartamentu nie znajdowało podstaw prawnych.

W innej sprawie[37] skarżący podnieśli, że skarżeni przetwarzają ich dane osobowe za pomocą monitoringu wizyjnego, który częściowo obejmuje ich działkę. Sąsiadów kilkukrotnie wzywano do ograniczenia zasięgu monitoringu, zarówno ustnie, jak i pisemnie.

Prowadzony monitoring – poza obszarem należącym do skarżonych – obejmował swoim zasięgiem również część nieruchomości skarżących oraz drogę publiczną. Wprawdzie zasięg zainstalowanego monitoringu wizyjnego był programowo ograniczony poprzez zastosowanie tzw. strefy (maski) prywatności, to jednak nie była ona zastosowana do pełnego obszaru, który wykraczał poza granicę nieruchomości.

[35] ZWOS.440.4504.2019.

[36] Zgodnie art. 690 ustawy z 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2024 r. poz.1016 ze zm.) do ochrony praw najemcy do użytku lokalu stosuje się przepisy o ochronie własności.

[37] DS.523.2547.2023.

Rejestracja obrazu następowała po rozpoznaniu przez kamerę ruchu w jej zasięgu, a objęcie tym monitoringiem fragmentu działki skarżących wynikało z parametrów technicznych i pola widzenia kamery.

Prezes UODO uznał, że funkcjonowanie monitoringu wiąże się z przetwarzaniem danych osobowych skarżących pomimo zastosowania stref prywatności. Możliwość wielokrotnej zmiany ustawień pola widzenia kamery, a także modyfikowania nałożonej strefy prywatności, nie może być uznana za skuteczne narzędzie, które w sposób trwały zapewni wyłączenie danego obszaru z monitoringu. W konsekwencji nie zapewniono ochrony prywatności osób mogących znaleźć się w jej zasięgu. Prawa i wolności skarżących, w tym ich małoletnich dzieci, były w tym przypadku nadrzędne.

Prezes UODO podkreślił, że nie zakazuje całkowitego stosowania monitoringu jako formy ochrony rodziny i mienia. W ocenie organu dozwolone przetwarzanie danych przez osobę fizyczną w celach o czysto osobistym lub domowym charakterze może mieć miejsce, gdy zasięg monitoringu, z którego pochodzą nagrania, obejmuje tylko nieruchomość stanowiącą własność monitorującego. W niniejszej sprawie taka okoliczność nie zaistniała. Wskazana przez skarżonych potrzeba zapewnienia bezpieczeństwa ich rodzinie oraz ochrony ich mienia jest wystarczającym uzasadnieniem dla wykonywania monitoringu wizyjnego mieszczącego się swoim zasięgiem wyłącznie w granicach ich nieruchomości. Skarżeni w celu zapewnienia bezpieczeństwa nie mogą monitorować terenu stanowiącego przestrzeń prywatną skarżących i przestrzeń publiczną, tj. drogę publiczną.

W ocenie Prezesa UODO jednoznacznym dowodem na nieprzetwarzanie danych za pomocą monitoringu wizyjnego może być zdemontowanie takich urządzeń, względnie skierowanie ich w sposób trwały poza sporny obszar monitorowania.

1.2.2. Przetwarzanie danych osobowych w związku z windykacją

W jednej ze spraw[38] skarżąca zarzuciła spółce udostępnienie jej danych osobowych firmie windykacyjnej bez podstawy prawnej. Skarżąca wskazała, że uiściła naliczoną przez spółkę opłatę dodatkową we wskazanym terminie, a mimo to jej dane osobowe zostały przekazane do firmy windykacyjnej, która kierowała do skarżącej wiadomości SMS w celu wyegzekwowania tej należności.

Zgodnie z praktyką spółki, z chwilą zaksięgowania płatności dane osobowe powinny co do zasady zostać usunięte z systemu. Z przyczyn organizacyjnych, tj. w wyniku przygotowania paczki z danymi osobowymi do windykacji przed zaksięgowaniem dokonanej opłaty, dane skarżącej zostały omyłkowo przekazane do windykacji (powierzenie). Istotną okolicznością sprawy było to, że dane te zostały przekazane do windykacji dopiero po dwóch tygodniach od uregulowania wskazanej należności. Spółka ponownie przeanalizowała wewnętrzne procedury związane z przekazywaniem danych do windykacji. W efekcie wydłużyła czas oczekiwania pomiędzy terminem do zapłaty a przekazaniem danych do windykacji, aby tym samym wydłużyć czas oczekiwania na potwierdzenie zaksięgowania wpłaty dokonanej

[38] DS.523.985.2024.

w ostatnim dniu terminu płatności, co ma zapewnić, że w przyszłości nie będzie dochodzić do podobnych zdarzeń.

W ocenie Prezesa UODO spółka przed przekazaniem danych osobowych skarżącej powinna była zweryfikować, czy należność z tytułu opłaty dodatkowej została uregulowana. Ponieważ dług nie istniał na dzień przekazania danych do egzekucji, nie istniała podstawa do udostępnienia tych danych firmie windykacyjnej. Prezes UODO udzielił upomnienia za udostępnienie bez podstawy prawnej danych osobowych podmiotowi przetwarzającemu w celu prowadzenia nieuzasadnionej windykacji należności.

1.2.3. Przetwarzanie w celach marketingowych i tzw. lista Robinsona

Nieprawidłowości w procesie przetwarzania danych osobowych polegające na przetwarzaniu ich bez podstawy prawnej w celach marketingowych[39], to przykład kolejnej sprawy. Skarżący dokonywał zamówienia w sklepie internetowym przedsiębiorcy, ale nie wyrażał jednak zgody na przesyłanie wiadomości SMS o charakterze marketingowym.

Przedsiębiorca potwierdził otrzymanie żądania skarżącego i poinformował o usunięciu jego numeru telefonu. Pomimo tego zapewnienia skarżący otrzymał kolejną wiadomość marketingową, tym razem na adres e-mail. Przedsiębiorca zaprzeczył, aby doszło do wysłania drugiej wiadomości. Skarżący nie przedstawił wystarczających dowodów, że to przedsiębiorca wysłał tę wiadomość (w szczególności przedstawiony przez skarżącego dowód nie zawierał daty ani adresu e-mail, z którego ta wiadomość została wysłana). Przedsiębiorca oświadczył, że usunął numer telefonu skarżącego następnego dnia po złożeniu żądania, a adres e-mail kilka dniu później. Zdaniem przedsiębiorcy nie potrzebował on zgody na przetwarzanie danych osobowych w celach marketingowych, gdyż posiadał prawnie uzasadniony interes do przetwarzania ich w tych celach z uwagi na dokonywanie przez skarżącego zakupów w jego sklepie.

Kwestia tego, czy informacja pozwala na identyfikację danej osoby, wynika z kontekstu, w jakim informacja ta jest używana. Choć numer telefonu (w przedmiotowym przypadku również adres e-mail) nie określa bezpośrednio tożsamości osoby fizycznej, to jest on informacją, która umożliwia bezpośredni kontakt z określoną osobą. Sama zatem możliwość skontaktowania się z tą osobą może prowadzić do ustalenia jej tożsamości, a więc numer telefonu oraz adres e-mail stanowią dane osobowe w rozumieniu przepisów RODO[40].

Niezależnie od przepisów wspomnianego rozporządzenia, kwestię warunków legalnego prowadzenia marketingu bezpośredniego przy wykorzystaniu połączeń i wiadomości telefonicznych oraz przy wykorzystaniu poczty elektronicznej, regulują

[39] DS.523.7750.2021.

[40] Na gruncie ustawy o ochronie danych osobowych z 1997 r. zob. wyrok WSA w Krakowie z 11.10.2013 r. w sprawie o sygn. akt II SA/Kr 682/13.

także przepisy szczególne[41], tj. Prawo komunikacji elektronicznej. Zgodnie z tą ustawą przesyłanie niezamówionej informacji handlowej za pomocą środków komunikacji elektronicznej, czy też używanie telekomunikacyjnych urządzeń końcowych w celach marketingowych, wymaga uprzedniej zgody. Powyższe przepisy uzależniają zatem możliwość zgodnego z prawem prowadzenia marketingu bezpośredniego oraz przesyłania informacji handlowej dodatkowo od uzyskania odpowiednich zgód w tym zakresie. Przedsiębiorca nie wykazał, aby dysponował którąkolwiek z ww. zgód. Powołanie się na prawnie uzasadniony interes do przetwarzania danych osobowych w tych celach nie był zatem wystarczający, gdyż jest on powiązany z przesłanką zgodności z prawem wynikającą z innych przepisów[42]. Prezes UODO uznał za uzasadnione udzielenie przedsiębiorcy upomnienia za przetwarzanie danych osobowych skarżącego bez podstawy prawnej w celach marketingowych.

Jednocześnie Prezes UODO ustalił, że przedsiębiorca usunął dane osobowe skarżącego w prawem określonym do tego terminie, z wyjątkiem numeru telefonu, który wpisał na tzw. czarną listę, oraz adresu e-mail, który oznaczył w systemie jako „wypisany". Organ uznał, że umieszczenie numeru telefonu na „czarnej liście" nie stanowi już przetwarzania w pierwotnym celu, tj. w celu prowadzenia marketingu bezpośredniego. Ma natomiast zapobiegać wykonywaniu w przyszłości połączeń o charakterze marketingowym do osoby posiadającej ten numer. Jest to równoznaczne z uszanowaniem woli skarżącego – wyrażonego wprost lub pośrednio sprzeciwu wobec przetwarzania jego danych osobowych w celach marketingowych. Przetwarzanie ograniczonego zakresu danych służy zapobieżeniu możliwości naruszenia interesów, praw lub wolności osób, których dane dotyczą. Analogicznie należy potraktować oznaczenie adresu e-mail w systemie przedsiębiorcy jako „wypisany".

Odnośnie do zarzutu dotyczącego niespełnienia obowiązku informacyjnego, Prezes UODO ustalił, że obowiązek ten jest spełniany na stronie internetowej przedsiębiorcy. Prawodawca nie narzuca administratorom szczególnej formy realizacji tego obowiązku. Podanie informacji na stronie internetowej, na której skarżący dokonał zakupu, było prawidłowe.

1.2.4. Prawo do sprostowania danych

Skarżąca złożyła skargę na spółkę[43], która notorycznie wysyła do niej korespondencję na nieaktualny adres, pomimo dwukrotnego żądania sprostowania jej danych. Pomimo zapewnień spółki o poprawieniu adresu, ponownie otrzymywała korespondencję na stary adres. Spółka wyjaśniła, że realizowała prawo skarżącej do sprostowania jej danych poprzez wprowadzenie do systemu właściwego adresu zamieszkania, o czym skarżąca była informowana bezpośrednio przez pracownika.

[41] Artykuł 398 ustawy z 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1221), poprzednio uregulowany w art. 172 ustawy z 16 lipca 2004 r. Prawo Telekomunikacyjne (Dz.U. z 2024 r. poz. 34 ze zm.) oraz art. 10 ustawy z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513 ze zm.)., dalej także jako u.ś.u.d.e.

[42] Wyrok WSA w Warszawie z 18 listopada 2022 r. w sprawie o sygn. akt II SA/Wa 715/22.

[43] DS.523.2744.2022.

Pomimo tego podejmowane działania spółki okazały się nieskuteczne z powodu, jak to określiła, niedopatrzenia pracownika lub przed błąd systemu – nowy adres zamieszkania nie aktualizował się w systemie. Po otrzymaniu wezwania Prezesa UODO do złożenia wyjaśnień spółka ponownie dokonała weryfikacji danych osobowych skarżącej w swoim systemie i tym razem – po wprowadzeniu ponownej zmiany – dokonała sprawdzenia poprawności działania systemu poprzez ponowne wygenerowanie faktury ze zaktualizowanymi danymi.

Okoliczność wystąpienia błędów technicznych systemu czy też zaniedbania przez pracownika nie może wpływać na realizację praw osób, których dane dotyczą. Spółka powinna bowiem dostosować swoje procedury obsługi zgłoszeń w zakresie realizacji praw tak, aby były one skuteczne co do wyniku. Spółka powinna zabezpieczyć realizację prawa do sprostowania danych poprzez właściwą weryfikację skuteczności podjętych czynności już za pierwszym razem. Prezes UODO uznał za uzasadnione udzielenie spółce upomnienia w zakresie stwierdzonego naruszenia, tj. uaktualnienia danych osobowych po upływie przewidzianego prawem terminu oraz nieprzestrzegania wymogu przejrzystej komunikacji, czyli błędnej informacji o zrealizowaniu żądania.

1.2.5. Minimalizacja danych dotyczących dziecka

Wątpliwości skarżącego budziło pozyskanie przez spółkę jego danych osobowych w zakresie daty urodzenia, w celu skorzystania z usług spółki w parku rozrywki[44]. Zdaniem skarżącego spółka naruszyła zasadę minimalizacji danych, gdyż pobieranie dodatkowych danych jest uciążliwe dla klienta, niezasadne, a dodatkowo zwiększa ryzyko wycieku danych. Jego zdaniem identyfikacji klienta można dokonać w wystarczający sposób na podstawie imienia i nazwiska oraz okazania potwierdzenia rezerwacji dostarczonego za pośrednictwem e-maila.

Data urodzenia była niezbędna spółce do identyfikacji lub późniejszej weryfikacji osób korzystających z jej usług. Identyfikacja polegała na porównaniu podanej daty urodzenia z datą zapisaną w bazie i miała na celu ocenę, czy do skorzystania z usług spółki zgłosiła się osoba uprawniona oraz czy zachowane zostały wymogi bezpieczeństwa. Z regulaminu usługi wynikało, że poszczególne grupy wiekowe dzieci mogły przebywać na terenie parku rozrywki tylko pod opieką osoby dorosłej. Spółka wskazała powody przyjęcia takich wymogów, powołując się na konieczność zapewnienia bezpiecznego korzystania z oferowanych atrakcji. Powoływała się na swoje doświadczenie nabyte w trakcie świadczenia usługi, np. osoby małoletnie próbowały korzystać z parku rozrywki pod opieką ich niewiele starszych kolegów. Ponadto ubezpieczyciel wymagał od spółki ustalenia, czy dana osoba faktycznie korzystała z jej usług. Identyfikacja poprzez imię i nazwisko oraz datę urodzenia pozwalała precyzyjnie to ustalić.

Zdaniem Prezesa UODO spółka nie naruszyła zasady minimalizacji danych osobowych i przetwarzała dane osobowe zgodnie z prawem. Zasada minimalizacji oznacza przetwarzanie danych osobowych, które jest adekwatne, stosowne oraz

[44] DS.523.6704.2022.

ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Tym samym zasady minimalizacji nie należy rozpatrywać przez jej literalne brzmienie, a przez przesłanki, które się na nią składają. Dane pozyskane przez spółkę w związku z umową i realizacją usługi spełniają ww. wymóg. Dopóki dane osobowe są używane zgodnie z przeznaczeniem i celem umowy, nie można mówić o bezprawności przetwarzania.

1.2.6. Przetwarzanie danych w celu zawiadomienia organów administracji publicznej

Prawo do ochrony danych osobowych nie jest prawem absolutnym i nie w każdej sytuacji znajduje ono zastosowanie. Przepisy o ochronie danych osobowych nie mają zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze[45]. Należy przez to rozumieć przetwarzanie danych osobowych, które nie jest związane z działalnością zawodową lub handlową. Może ono polegać np. na prowadzeniu korespondencji, przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz aktywności internetowej dokonywanej w ramach takiej działalności[46].

Konflikty sąsiedzkie często eskalują poza zwykłe sprzeczki. W takich sytuacjach strony próbują angażować organy państwowe w swój konflikt poprzez zawiadamianie o podejrzewanych lub zauważonych nieprawidłowościach. Powiadomienie odpowiednich organów, a zwłaszcza reakcja tych organów, powoduje niekiedy zaskoczenie i sprzeciw osoby, wobec której je zgłoszono. W tym również wątpliwości, co do legalności udostępnienia ich danych osobowych w ten sposób.

W jednej z takich spraw[47] przedmiotem skargi było naruszenie przepisów o ochronie danych osobowych przez osobę fizyczną, która udostępniła dane osobowe skarżącego w pismach kierowanych do organów państwowych i samorządowych. Zdaniem skarżącego naruszenie polegało na przetworzeniu jego danych osobowych bez jego wiedzy i zgody. Strony postępowania są sąsiadami. Skarżony pozyskał dane osobowe skarżącego z Elektronicznych Ksiąg Wieczystych w celu dokonania zgłoszenia do organów administracji publicznej o możliwym łamaniu przez niego przepisów o ochronie środowiska oraz przyrody, tj. poprzez nielegalne składowanie odpadów oraz wycinkę drzew.

Prezes UODO uznał, że RODO nie ma zastosowania do przetwarzania danych osobowych w celu powiadomienia odpowiednich organów administracji publicznej o podejrzewanych nieprawidłowościach. Zgłoszenie organom państwowym określonych zdarzeń mających miejsce na sąsiedniej nieruchomości – w celu sprawdzenia, czy ich zaistnienie nie narusza przepisów prawa – nie stanowi naruszenia przepisów o ochronie danych osobowych. Przetwarzanie danych osobowych odbywało się w celu ochrony własności i szeroko pojętego miru

[45] Art. 2 ust. 2 lit. c RODO.
[46] Motyw 16 RODO.
[47] DS.523.856.2024.

domowego, czyli w ramach działalności o czysto osobistym i domowym charakterze, niezwiązanym z jakąkolwiek działalnością zawodową lub handlową.

1.3. Sektor finansów, ubezpieczeń i telekomunikacji

W 2024 roku działalność Prezesa Urzędu Ochrony Danych Osobowych w obszarze sektora finansowego, ubezpieczeń i telekomunikacji skupiała się, podobnie do lat 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. W swoich decyzjach Prezes UODO podkreślał, 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, który mógł wyłącznie ocenić proces przetwarzania danych związany z powyższymi zagadnieniami.

Znaczna część skarg wpływających do Prezesa UODO dotyczyła działalności podmiotów sektora finansowego, takich jak banki, instytucje pożyczkowe, spółdzielcze kasy oszczędnościowo-kredytowe, instytucje utworzone na podstawie art. 105 ust. 4 ustawy z 29 sierpnia 1997 r. – Prawo bankowe[48], związanej z przetwarzaniem danych osobowych w związku z dokonywaniem oceny zdolności kredytowej i analizy ryzyka kredytowego.

1.3.1. Przetwarzanie przez banki informacji stanowiących tajemnicę bankową w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, po wygaśnięciu zobowiązania wynikającego z umowy w oparciu o zgodę osoby, której dane dotyczą

Prezes UODO oceniał także legalność przetwarzania danych osobowych dłużnika w celu oceny zdolności kredytowej i analizy ryzyka kredytowego w oparciu o art. 105a ust. 2 Prawa bankowego, tj. w oparciu o zgodę podmiotu danych. W jednej ze spraw bank przetwarzał, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego w biurze informacji kredytowej, dane w zakresie kilku rachunków dotyczących jednego zobowiązania. Podmiot danych wycofał zgodę na ww. przetwarzanie, co skutkowało zaprzestaniem przetwarzania na tej podstawie. Jednakże wskazał, że jego oświadczenie nie dotyczyło wszystkich rachunków, lecz tylko jednego. W związku z powyższym żądał przywrócenia przetwarzania informacji dotyczących ww. rachunku w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, aby poprawić ocenę swojej zdolności kredytowej. Prezes UODO nie

[48] Dz.U. z 2024 r. poz. 1646 ze zm., dalej także jako Prawo bankowe.

dostrzegł jednak nieprawidłowości w działaniu skarżonych podmiotów, wskazując, że bank i biuro informacji kredytowej, z uwagi na obwiązek przewidziany w art. 105 ust. 4i Prawa bankowego, obowiązane są do dostarczania aktualnych danych o zobowiązaniach i nie mogą działać w tym zakresie w sposób wybiórczy[49].

1.3.2. Przetwarzanie danych przez banki w trakcie oraz po ustaniu relacji umownej

Decyzje wydane w 2024 r. dotyczyły również przypadków przetwarzania danych klientów w trakcie trwającej relacji umownej oraz byłych klientów, po ustaniu tej relacji. Jednym z powodów wnoszenia skarg przez byłych klientów banków było mylne przeświadczenie, że wraz z ustaniem relacji z bankiem, bank powinien natychmiast usunąć dane osobowe byłego klienta. Prezes UODO w wydanych decyzjach wskazywał, że w trakcie obowiązywania umowy bank jest uprawniony do przetwarzania danych osobowych klienta na podstawie art. 6 ust. 1 lit. b RODO[50], natomiast po ustaniu relacji umownych bank przetwarza dane na podstawie art. 6 ust. 1 lit. c RODO w celu wypełnienia obowiązków prawnych[51], wynikających m.in. z art. 74 ustawy z 29 września 1994 r. o rachunkowości[52], art. 49 ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[53] i art. 70 § 1 w zw. z art. 86 § 1 ustawy z 29 sierpnia 1997 r. Ordynacja podatkowa[54].

Powyższe przepisy regulujące obowiązki archiwizacyjne legalizują przetwarzanie danych osobowych w oparciu o przesłankę wskazaną w art. 6 ust. 1 lit. c RODO również w sytuacji, gdy podmiot danych i bank nadal łączy umowa[55].

1.3.3. Udostępnienie danych osobowych innym podmiotom przez banki

Prezes UODO w 2024 r. rozpatrywał skargi na udostępnienie danych osobowych innym podmiotom przez banki. Część z wnoszonych skarg była wynikiem powzięcia przez podmiot danych wiedzy o naruszeniu ochrony danych. W części spraw skarżący oceniali udostępnienie jako nielegalne, jednak po przeprowadzeniu postępowania okazywało się, że udostępnienie znajdowało oparcie w przepisach prawa.

Przykładem jest udostępnienie informacji o stanie rachunku, w przypadku zwrócenia się do banku o informacje stanowiące tajemnicę bankową przez sąd powszechny w związku ze sprawą o podział majątku[56]. Takie udostępnienie następuje

[49] ZSPR.440.1369.2019.
[50] ZSPR.440.1347.2019.
[51] ZSPR.440.1347.2019, ZSPR.440.1523.2018, DS.523.515.2023, ZSPR.440.683.2018, DS.523.2580.2023, DS.523.1342.2022, DS.523.5061.2020, DS.523.4361.2023, DS.523.456.2021, ZSPR.440.1347.2019, ZSPR.440.1523.2018, ZSPR.440.683.2018, DS.523.808.2023, DS.523.2580.2023, DS.523.1342.2022, DS.523.456.2021, DS.523.515.2023, DS.523.2580.2023, DS.523.5061.2020, DS.523.4361.2023.
[52] Dz.U. z 2023 r. poz. 120 ze zm., zwana dalej ustawą o rachunkowości.
[53] Dz.U. z 2023 r. poz. 1124 ze zm., zwana dalej także AML.
[54] Dz.U. z 2025 r. poz. 111.
[55] DS.523.515.2023, ZSPR.440.683.2018, DS.523.808.2023.
[56] DS.523.4413.2023.

na rzecz sądu, a nie stron lub uczestników tego postępowania. Bank nie był przy tym uprawniony do kwestionowania zakresu danych, których udostępnienia zażądał sąd.

Prezes UODO rozpatrywał również sprawy, w których stwierdził, że doszło do nieuprawnionego udostępnienia danych osobowych przez bank na rzecz innych podmiotów. Przykładami takiego udostępnienia są: błędne skierowanie korespondencji zawierającej dane osobowe do osoby trzeciej[57], przesłanie korespondencji elektronicznej na adres e-mail innego klienta banku[58] czy też przekazanie przez bank do podmiotu, z którym współpracuje w zakresie przeprowadzania badań, nadmiarowych danych osobowych klienta w zakresie salda rachunku[59].

1.3.4. Powierzenie przetwarzania danych osobowych innemu podmiotowi przez bank w celach windykacyjnych

Od nieuprawnionego udostępnienia danych należy odróżnić przekazanie danych przez bank na rzecz podmiotu przetwarzającego. W swoich decyzjach wydanych w roku 2024 Prezes UODO stwierdzał, że oparcie w przepisach RODO ma powierzenie przetwarzania danych osobowych zgodne z art. 28 ust. 3 RODO, gdy ma ono na celu dochodzenie roszczeń w imieniu banku przez podmiot wyspecjalizowany w dochodzeniu roszczeń[60]. Przetwarzanie danych osobowych w celu dochodzenia istniejących roszczeń względem byłych klientów ma oparcie w art. 6 ust. 1 lit. f RODO[61]. Prezes UODO wskazywał również, że zgodnie z art. 6a ust. 1 pkt 1 lit. l Prawa bankowego, bank może, w drodze umowy zawartej na piśmie, powierzyć przedsiębiorcy lub przedsiębiorcy zagranicznemu, z zastrzeżeniem art. 6d tej ustawy, wykonywanie w imieniu i na rzecz banku pośrednictwa w zakresie czynności wymienionych w art. 5 i 6 Prawa bankowego w zakresie windykacji należności banku[62].

1.3.5. Dochodzenie wierzytelności przez podmioty sektora finansowego

Podobnie jak w latach poprzednich, tak i w roku 2024 Prezes UODO wydał decyzje odnoszące się do przetwarzania danych w celach windykacyjnych, wskazując, że proces taki w przypadku istniejącej wierzytelności znajduje oparcie w przesłance wskazanej w art. 6 ust. 1 lit. f RODO[63].

Zgodnie z art. 509 § 1 k.c. wierzyciel może bez zgody dłużnika przenieść wierzytelność na osobę trzecią (przelew), chyba że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania. Cesja wierzytelności wiąże się z uprawnieniem do przekazania nabywcy danych osobowych dłużnika umożliwiających podjęcie względem niego stosownych działań zmierzających do odzyskania należności. Powyższa dopuszczalność przelewu wierzytelności nie

[57] DS.523.3309.2021, DS.523.1266.2024.
[58] DS.523.6017.2021.
[59] ZSPU.440.794.2019.
[60] DS.523.4120.2023.
[61] DS.523.4846.2022.
[62] DS.523.2765.2023.
[63] ZSPR.440.1537.2019, DS.523.5831.2022, DS.523.5294.2023.

podlega ograniczeniom umownym ani ustawowym. Nie jest również wymagana zgoda dłużnika (podmiotu danych) na przelew wierzytelności. Prezes UODO w swoich decyzjach wskazywał, że pozyskanie danych przez firmy windykacyjne nie stanowi naruszenia przepisów o ochronie danych osobowych i odbywa się na podstawie art. 6 ust. 1 lit. f RODO[64]. Dłużnik musi liczyć się z tym, że gdy popadanie w zwłokę w spełnianiu zobowiązania, jego prawo do prywatności może zostać ograniczone ze względu na realizację prawnie uzasadnionego interesu wierzyciela związanego z dochodzeniem roszczeń[65].

Prezes UODO rozpatrywał również sprawy dotyczące przetwarzania danych osobowych przez podmioty zarządzające portfelami wierzytelności nabytych przez fundusze inwestycyjne. W tego typu sprawach Prezes UODO stwierdzał, że przekazanie danych osobowych przez fundusze na rzecz ww. podmiotów odbywało się na podstawie umowy powierzenia zawartej zgodnie z art. 28 ust. 3 RODO[66].

1.3.6. Zamieszczanie na kopercie informacji o wezwaniu do zapłaty

Za niedozwoloną formę udostępnienia danych osobowych w jednej ze spraw Prezes UODO uznał umieszczenie na kopercie informacji, że zawiera ona wezwanie do zapłaty wraz z danymi korespondencyjnymi dłużnika – stanowi to ujawnienie danych osobowych dłużnika w zakresie jego sytuacji finansowej. Prezes UODO wskazał, że na kopercie powinny być zamieszczone jedynie te dane osobowe, które są niezbędne do dostarczenia korespondencji – za takie dane nie można uznać ww. adnotacji dotyczącej zawartości koperty[67].

1.3.7. Udostępnianie kopii danych osobowych podlegających przetwarzaniu przez podmioty z sektora telekomunikacyjnego

W 2024 r. Prezes UODO wydawał decyzje dotyczące żądania udostępnienia przez podmioty z sektora telekomunikacyjnego kopii danych osobowych podlegających przetwarzaniu, utrwalonych na nagraniach rozmów telefonicznych[68].

Skarżący, kierując do administratorów żądania wydania kopii danych, powoływali się na przepis art. 15 RODO. W części rozpatrywanych spraw administratorzy, pomimo odmowy realizacji żądań, nie wskazywali na podstawy prawne, które zwalniałaby ich ze spełnienia tego obowiązku. W związku z przetwarzaniem danych osobowych pozyskiwanych za pomocą nagrań rozmów telefonicznych, administrator powinien przewidzieć procedury zapewniające realizację spoczywającego na nim obowiązku zagwarantowania osobom, których dane są przetwarzane, możliwości realizowania ich uprawnień wynikających z przepisów RODO, w tym prawa dostępu do tych danych osobowych oraz uzyskania ich kopii. Prezes UODO wskazywał także na treść art. 46

[64] DS.523.3431.2023.
[65] DS.523.4135.2021.
[66] DS.523.3230.2024.
[67] DS.523.5255.2020.
[68] DS.523.49.2023, DS.523.3684.2023, DS.523.1195.2022.

ust. 2a ustawy z 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[69].

1.3.8. Udostępnienie danych podmiotom nieuprawnionym przez podmioty sektora telekomunikacyjnego

Prezes UODO w 2024 r. zajmował się również sprawami dotyczącymi udostępnienia danych osobowych podmiotom nieuprawnionym przez operatorów telekomunikacyjnych. W tego rodzaju postępowaniach badana była kwestia tego, czy operatorzy telekomunikacyjni dopuścili się naruszenia ochrony danych w szczególności na skutek udostępnienia danych skarżących innym swoim klientom lub osobom trzecim[70]. W większości tych spraw naruszenia ochrony danych polegały na przesłaniu danych skarżących innemu klientowi operatora na błędny adres zamieszkania lub adres e-mail.

Przedmiotem jednej ze spraw było także zdarzenie polegające na udostępnieniu osobie trzeciej przez operatora telekomunikacyjnego danych skarżącego umieszczonych na jednym z akcesoriów, jakie zakupił, a następnie zareklamował w salonie[71]. Pozostawiony u operatora artykuł został oznaczony danymi skarżącego i odnaleziony w miejscu publicznym – trafił w ręce osoby trzeciej. Prezes UODO ustalił, że doszło do udostępnienia podmiotowi nieuprawnionemu danych osobowych skarżącego zawartych na reklamowanym towarze, uprzednio pozostawionym przez niego w salonie spółki. Dowody przedłożone przez skarżącego potwierdziły zaistnienie ww. zdarzenia. Prezes UODO zauważył, że operator zobowiązany był zabezpieczyć dane osobowe skarżącego umieszczone na tym produkcie. Prezes UODO uznał, że operator poza własnym oświadczeniem nie przedstawił żadnego dowodu, który podważyłby dowody przedstawione przez skarżącego. W związku z tym Prezes UODO stwierdził, że doszło do udostępnienia przez operatora danych osobowych skarżącego na rzecz osoby nieuprawnionej, co nie znajdowało oparcia w żadnej z przesłanek legalizujących proces przetwarzania danych osobowych, wyrażonych w art. 6 ust. 1 RODO.

1.3.9. Przetwarzanie danych osobowych pochodzących z dowodu osobistego przez operatorów telekomunikacyjnych.

Wśród spraw dotyczących operatorów telekomunikacyjnych Prezes UODO rozpoznawał skargi dotyczące kwestii związanych z pozyskaniem danych z dowodów osobistych[72]. W większości tych spraw ocenie podlegała kwestia spisania danych z dowodów osobistych w celu zawarcia umowy z operatorem, a także okoliczność dotyczącą utrwalenia obrazu takiego dokumentu[73].

---

[69] Dz. U. z 2024 r. poz. 1034), dalej także jako u.f.i.
[70] DS.523.1265.2023, DS.523.4161.2023, DS.523.440.10.2019, DS.523.29.2024, DS.523.2412.2022, DS.523.6832.2023, DS.523.135.2023, DS.523.33.2021.
[71] DS.523.3734.2023.
[72] DS.523.2891.2021, ZSPR.440.1406.2018, DS.523.3802.2022.
[73] ZSPR.440.1406.2018.

Skarżący wyraził zgodę na utrwalenie obrazu dokumentu tożsamości oraz na przetwarzanie danych w nim zawartych łącznie z wizerunkiem i rysopisem, w związku z zawarciem umowy o świadczenie usług telekomunikacyjnych. Operator przedłożył oświadczenie klienta z zaznaczonymi zgodami na utrwalanie obrazu jego dokumentu tożsamości oraz przetwarzanie danych w nim zawartych. Skarżący zakwestionował zasadność wykonania kopii dowodu osobistego i następnie cofnął zgodę na przetwarzanie jego danych osobowych w tym zakresie. Prezes UODO, przywołując obowiązujące w czasie zawierania umowy pomiędzy skarżącym i spółką przepisy prawa telekomunikacyjnego, uznał, że operator nie legitymował się innymi niż zgoda skarżącego przesłankami uzasadniającymi przetwarzanie jego danych osobowych zawartych w kopii dowodu osobistego, które wykraczają poza to, co faktycznie niezbędne do dalszego wykonywania przez niego umów. Za dane niezbędne do wykonania tych umów należy uznać imię i nazwisko, adres oraz nr PESEL. Dane osobowe zawarte w dowodzie osobistym takie jak obywatelstwo, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, płeć, wzrost w centymetrach, kolor oczu, nazwa organu wydającego dowód osobisty, data wydania i termin ważności, seria i numeru dowodu osobistego oraz wizerunek twarzy i wzór podpisu nie są danymi, które mogą być przetwarzane w celu wykonania umowy o świadczenie usług telekomunikacyjnych. W sytuacji braku zgody skarżącego na przetwarzanie w tak szerokim zakresie jego danych przez spółkę uznano to za złamanie zasady minimalizacji, o której mowa w art. 5 ust. 1 pkt c RODO.

1.3.10. Nieuwzględnienie przez administratora wniosku o usunięcie danych osobowych

Podmiot świadczący usługi internetowe[74] przetwarzał dane osobowe skarżącego, pomimo że zażądał on usunięcia jego danych osobowych, ponieważ pomiędzy stronami nie doszło do zawarcia umowy. W toku prowadzonego postępowania Prezes UODO ustalił, że operator pozyskał dane osobowe skarżącego w celu zawarcia z nim umowy o świadczenie usługi internetowej. Przetwarzanie danych osobowych skarżącego było niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy i jako takie znajdowało podstawę legalizującą w postaci art. 6 ust. 1 lit. b RODO. Do zawarcia umowy między stronami ostatecznie jednak nie doszło. Mimo tego administrator kontynuował przetwarzanie danych osobowych skarżącego, podając jako podstawę swojego działania art. 6 ust. 1 lit. c RODO. Prezes UODO zauważył, że zdaniem spółki, przetwarzanie danych skarżącego było niezbędne do realizacji obowiązków spółki wynikających z przepisów Prawa telekomunikacyjnego. Niemniej jednak Prezes UODO uznał, że taka wykładnia przytoczonych przepisów nie jest właściwa. Przepis art. 168 Prawa telekomunikacyjnego dotyczył obowiązku rejestracji danych o wykonanych usługach telekomunikacyjnych. Z treści tego przepisu wynika obowiązek przechowywania przez przedsiębiorcę telekomunikacyjnego tzw. danych transmisyjnych w okresie nie dłuższym niż 12 miesięcy. W sprawie tej Prezes UODO ustalił, że nie mamy do

[74] DS.523.1518.2020.

czynienia ani z wykonaną usługą, ani z danymi transmisyjnymi. Skarżący był więc uprawniony do żądania usunięcia jego danych osobowych na podstawie art. 17 ust. 1 lit. a RODO, ponieważ nie zaistniała żadna z przesłanek uprawniających administratora do przetwarzania danych osobowych skarżącego po zakończeniu działań związanych z zawarciem umowy, w innym celu niż ten, dla którego dane te zostały zebrane.

1.3.11. Udostępnienie danych osobowych podmiotowi nieuprawnionemu przez podmiot sektora ubezpieczeniowego

Prezes UODO oceniał kwestię legalności[75] udostępnienia danych osobowych skarżącego przez ubezpieczyciela na rzecz innego podmiotu zajmującego się wynajmem samochodów zastępczych. Ubezpieczyciel przetwarzał dane osobowe skarżącego między innymi w zakresie niezbędnym do realizacji umowy ubezpieczenia komunikacyjnego. Po zgłoszeniu ubezpieczycielowi przez skarżącego potrzeby uzyskania pomocy przy wynajmie pojazdu zastępczego konsultant ubezpieczyciela wyszukał podmiot współpracujący z ubezpieczycielem i miał nawiązać ponowny kontakt ze skarżącym w celu przedstawienia mu warunków wynajmu takiego samochodu. Jednak nie uczynił tego. Ubezpieczyciel przekazał dane osobowe skarżącego na rzecz innego podmiotu, który z nim współpracował i działał jako podmiot przetwarzający dane w jego imieniu. W sprawie tej Prezes UODO stwierdził jednak, że ubezpieczyciel nie miał podstaw do przekazania danych osobowych skarżącego na rzecz innego podmiotu, ponieważ ostatecznie skarżący nie wskazał, że chce skorzystać z usługi wynajmu pojazdu zastępczego, a jedynie, że chce poznać warunki tego wynajmu. Prezes UODO zaznaczył, że kwestionowane w skardze przetwarzanie danych osobowych skarżącego polegające na ich udostępnieniu przez ubezpieczyciela na rzecz podmiotu nieuprawnionego nie znajdowało uzasadnienia w przesłankach w wynikających z art. 6 ust. 1 RODO.

1.3.12. Udostępnienie danych osobowych przez ubezpieczyciela na cele postępowania sądowego

Prezes UODO oceniał również sprawy związane z udostępnieniem danych osobowych skarżących na cele postępowania sądowego przez podmioty z sektora ubezpieczeń. Udostępnienie przez ubezpieczyciela danych osobowych znajdowało podstawy legalizujące w art. 6 ust. 1 lit. f RODO – było bowiem niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora[76].

W jednej ze spraw ustalono, że część dokumentów zawierających dane osobowe skarżącego stanowiła załączniki do pozwu ubezpieczyciela przed sądem powszechnym. Co istotne, sam skarżący został również zgłoszony w pozwie jako świadek zdarzenia oraz procesu likwidacji szkody. Kwestionowane przez skarżącego przetwarzanie jego danych osobowych przez ubezpieczyciela, polegające na

[75] DS.523.6895.2023.
[76] DS.523.1724.2024.

udostępnieniu tych danych na rzecz sądu nastąpiło w związku z toczącym się postępowaniem. Dlatego przeprowadzając ocenę tego procesu, Prezes UODO uznał, że przetwarzanie to znajdowało podstawy legalizujące w art. 6 ust. 1 lit. f RODO, było bowiem niezbędne do celów polegających na dochodzeniu zapłaty w postępowaniu regresowym.

1.3.13. Przetwarzanie przez ubezpieczyciela danych osobowych skarżącego, który nie był stroną umowy

W roku 2024 organ nadzorczy wydał decyzje w sprawach, w których ocenie podlegała kwestia użycia w umowie przez ubezpieczycieli danych osobowych skarżących. W jednej z tego typu spraw[77] przetwarzanie danych nastąpiło na skutek pomyłki pracownika ubezpieczyciela, który podczas rejestracji danych osobowych ubezpieczającego pojazdy pomylił się w zapisie jego numeru PESEL, wpisując do systemu informatycznego numer PESEL należący do skarżącego. W konsekwencji rejestrowane wówczas pojazdy przypisane zostały do osoby skarżącego. Prezes UODO stwierdził, że ubezpieczyciel dopuścił się naruszenia przepisów o ochronie danych osobowych, ponieważ przetwarzanie danych osobowych skarżącego w związku z umowami ubezpieczenia komunikacyjnego, których nie był stroną, nie znajdowało oparcia w żadnej z przesłanek wskazanych w art. 6 ust. 1 RODO.

1.4. Sektor zdrowia, zatrudnienia i szkolnictwa

1.4.1. Przetwarzanie przez lekarza danych osobowych pozyskanych za pośrednictwem PUE ZUS

Dostęp lekarzy do danych osobowych znajdujących się na platformie PUE ZUS[78] polega na tym, że lekarz, logując się do PUE ZUS pacjenta celem wystawienia zwolnienia lekarskiego, wprowadza w wyszukiwarkę numer PESEL lub imię i nazwisko. Następnie system prezentuje osobie mającej dostęp do niego dane osobowe ubezpieczonego. Znacząca liczba lekarzy, na których wnoszone są skargi, zdaje się działać w przeświadczeniu, że samo posiadanie uprawnień do uzyskania dostępu do danych osób znajdujących się na PUE ZUS wystarcza do prawidłowego uzasadnienia korzystania z tego dostępu. Lekarze często zbyt swobodnie korzystają z posiadanych uprawnień dostępu do danych znajdujących się na PUE ZUS, realizując w ten sposób własne cele niemające związku z wykonywaniem działalności leczniczej, pozyskując dane osób, z którymi łączą ich relacje prywatne bądź zawodowe, np. dane byłych partnerów bądź też byłych pracowników. Czasami są to osoby, z którymi lekarze uwikłani są w procesy sądowe.

Tymczasem Prezes UODO wielokrotnie podkreślał, że przetwarzanie danych pacjentów w PUE ZUS jest dopuszczalne wyłącznie w celu wystawienia, anulowania lub sprostowania zwolnienia lekarskiego. Jakiekolwiek inne wykorzystanie tych danych, niezależnie od motywacji, stanowi naruszenie RODO.

[77] ZSPR.440.1844.2019.
[78] Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych, dalej także jako PUE ZUS.

W jednej z rozpatrywanych w 2024 r. spraw[79] skarżący zarzucił, że lekarka bezprawnie uzyskała dostęp do jego danych osobowych na PUE ZUS, mimo że nie wystawiła ani nie anulowała ona zwolnienia lekarskiego. Ponadto lekarka nie odpowiedziała na jego prośbę o wyjaśnienie przyczyn tego dostępu. Lekarka argumentowała, że jej działanie miało charakter osobisty, ponieważ było związane z jej rodziną i trwającym procesem sądowym między nią a skarżącym. Korzystając z uprawnień zawodowych, lekarka chciała sprawdzić, czy skarżący rzeczywiście przebywa na zwolnieniu lekarskim i unika rozpraw.

Prezes UODO uznał, że działanie lekarki nie miało charakteru prywatnego, lecz zawodowy, ponieważ uzyskała ona dostęp do danych jako osoba uprawniona do wystawiania zaświadczeń lekarskich w systemie PUE ZUS. W związku z bezprawnym przetwarzaniem danych osobowych skarżącego Prezes UODO udzielił lekarce upomnienia.

W innej sprawie[80] skarżąca zgłosiła, że lekarka, u której nigdy się nie leczyła, bezprawnie uzyskała dostęp do jej danych osobowych w PUE ZUS, mimo że nie wystawiła ani nie anulowała zwolnienia lekarskiego. Lekarka wyjaśniła, że dostęp nastąpił w wyniku błędu – omyłkowego wpisania numeru PESEL pacjentki o niemal identycznym numerze, różniącym się jedynie dwiema cyframi od numeru PESEL skarżącej.

Prezes UODO podkreślił, że nie istnieją przepisy zezwalające lekarzom na przeglądanie danych pacjentów w PUE ZUS w innym celu niż wystawienie, anulowanie lub sprostowanie zwolnienia lekarskiego. W opisywane sprawie lekarka naruszyła przepisy RODO, w szczególności dotyczące legalności przetwarzania danych i ich odpowiedniego zabezpieczenia. W efekcie została upomniana.

Prezes UODO zajmował się także sprawą, w której skarżący zgłosił, że lekarze, z którymi wcześniej łączyły go relacje rodzinne, wykorzystali swoje uprawnienia oraz znajomość jego numeru PESEL, by uzyskać dostęp do jego danych w PUE ZUS. Nie zakończyło się to jednak wystawieniem ani anulowaniem zwolnienia lekarskiego. Ustalono, że skarżący nie był pacjentem żadnego z lekarzy. Jeden z nich, były małżonek skarżącego, wykorzystał jego dane w celach niezwiązanych z udzielaniem świadczeń medycznych. Ponadto druga lekarka – prywatnie siostra pierwszego – uzyskała dostęp do danych skarżącego w celu ustalenia jego miejsca pracy i zamieszkania. Prezes UODO stwierdził, że lekarze bezprawnie wykorzystali dane skarżącego w celach prywatnych i nie byli do tego uprawnieni.

Prezes UODO upomniał decyzją wydaną w innej sprawie[81] lekarza za jednorazowe, nieuprawnione uzyskanie dostępu do danych skarżącej w PUE ZUS. Skarżąca nigdy nie była jego pacjentką, a ich relacja miała charakter osobisty – byli małżeństwem w trakcie rozwodu. Lekarz twierdził, że nie logował się na konto skarżącej w PUE ZUS, lecz jedynie korzystał z platformy w celu sprawdzenia danych

[79] DS.523.6557.2022.
[80] DS.523.267.2024.
[81] DS.523.3695.2023.

ich wspólnych dzieci. Analiza informacji pozyskanych od ZUS-u wykazała jednak, że faktycznie uzyskał on dostęp do danych skarżącej, co stanowiło naruszenie przepisów RODO.

1.4.2. Przetwarzanie przez lekarza danych osobowych na potrzeby wystawiania recept

Skarżący w jednej ze spraw[82] zgłosił, że otrzymał drogą e-mailową oraz w wiadomości SMS informację o wystawieniu recept przez lekarza, którego nie zna. Recepty te widniały w systemie jako zrealizowane, choć sam z nich nie skorzystał. W toku postępowania ustalono, że recepty zostały wystawione i wydane w ramach teleporady udzielonej osobie trzeciej, która nie została prawidłowo zidentyfikowana przez lekarza.

Prezes UODO uznał, że w tej sprawie administrator naruszył obowiązki wynikające z przepisów o ochronie danych osobowych, przetwarzając dane skarżącego bez podstawy prawnej w związku ze świadczeniem usług medycznych na rzecz innej osoby. Biorąc pod uwagę działania podjęte przez administratora po ujawnieniu naruszenia oraz nieodwracalny charakter skutków przetwarzania, Prezes UODO udzielił lekarzowi upomnienia.

1.4.3. Przetwarzanie przez podmiot leczniczy danych osobowych w celu wystawienia recepty, skutkujące pozyskaniem tych danych przez osobę trzecią

W wyniku pomyłki pracownika podmiotu leczniczego, który nie zweryfikował tożsamości skarżącej, wystawiono receptę na dane osoby trzeciej – członka rodziny skarżącej. W efekcie osoba ta uzyskała dostęp do informacji o lekach skarżącej i jej stanie zdrowia[83]. Prezes UODO stwierdził naruszenie przepisów o ochronie danych osobowych i udzielił podmiotowi leczniczemu upomnienia.

1.4.4. Udostępnienie przez pracodawcę danych o stanie zdrowia współpracownikom osoby, której dane dotyczą

Prezes UODO zajmował się także skargą[84], w której skarżąca zarzuciła, że jej pracodawca udostępnił na forum pracowników informacje o jej stanie zdrowia i leczeniu. Była ona długotrwale nieobecna w pracy z powodu zwolnienia lekarskiego. W jego trakcie współpracownicy, po uzyskaniu informacji od przełożonych, kontaktowali się z nią telefonicznie z pytaniami o stan zdrowia. Pracodawca wyjaśnił, że początkowo informacje o chorobie skarżącej były udostępniane jedynie przełożonym odpowiedzialnym za organizację pracy w oddziale, w którym była zatrudniona. Następnie jedna z przełożonych przekazała je innym pracownikom, uzasadniając to koniecznością reorganizacji pracy z powodu długotrwałej

[82] DS.523.5415.2023.
[83] DS.523.3043.2024.
[84] DS.523.5475.2023.

nieobecności skarżącej. Pracodawca argumentował, że działanie to wynikało z troski oraz relacji koleżeńskich.

Prezes UODO stwierdził, że ujawnienie tych danych nie miało podstawy w żadnej z przesłanek art. 9 ust. 2 RODO i było nieuprawnione. Przełożona powinna była jedynie poinformować zespół o nieobecności skarżącej oraz zasadach organizacji pracy w jej zastępstwie, bez podawania szczegółowych informacji o stanie zdrowia.

1.4.5. Prawo do uzyskania kopii danych, zawartych w notatkach, testach psychologicznych oraz zapiskach psychologa

Poradnia Psychologiczno-Pedagogiczna odmówiła skarżącej udostępnienia notatek, testów psychologicznych oraz zapisków psychologa sporządzonych podczas terapii jej córki, uznając je za dokumentację poufną, niedostępną w takim zakresie jak opinia końcowa[85].

Prezes UODO uznał, że skarżąca miała prawo uzyskać wierną kopię danych osobowych swojej córki, zawartych we wszelkiej dokumentacji. Odmowa poradni była nieprawidłowa, przez co skarżąca nie miała świadomości, jakie dane jej córki są przetwarzane. W związku z tym Prezes UODO nakazał poradni udostępnienie pełnej kopii danych zgodnie z wnioskiem skarżącej.

1.4.6. Udostępnienie przez byłego pracodawcę danych osobowych byłego pracownika zawartych w dokumentach dotyczących postępowań dyscyplinarnych, cywilnych i administracyjnych

W jednej ze spraw[86] procedowanych w 2024 r. ustalono, że instytut ujawnił nowemu pracodawcy skarżącej jej dane osobowe zawarte w dokumentach dotyczących postępowań dyscyplinarnych, cywilnych i administracyjnych, w tym zarzutów plagiatu w rozprawie doktorskiej. Dane te zostały przekazane podczas spotkania dziekanów obu instytucji oraz udostępnione do wglądu. Instytut naruszył prawo do prywatności skarżącej, gdyż przekazane informacje mogły wpłynąć na jej zatrudnienie. Ujawnienie danych osobowych nie miało podstawy prawnej, a argumentacja instytutu, że szczegóły postępowania dyscyplinarnego są jawne, została odrzucona. W konsekwencji instytut otrzymał upomnienie.

1.4.7. Udostępnienie przez szkołę danych uczennicy rodzicom innych uczniów

Szkoła pozyskała od uczennicy – córki skarżących – informacje o jej problemach osobistych, zarówno z zeznań podczas spotkania z psychologiem, jak i wiadomości wymienianych między uczennicami[87]. Szkoła, próbując rozwiązać konflikt rówieśniczy, ujawniła te dane podczas spotkania z rodzicami innych uczniów. Informacje dotyczyły m.in. stanu emocjonalnego córki skarżących oraz jej relacji z rodzicami. Prezes UODO uznał, że szkoła naruszyła prywatność dziecka, ujawniając dane osobowe osobom

[85] DS.523.4391.2023.
[86] DS.523.3263.2023.
[87] DS.523.4264.2023.

trzecim. Cel przetwarzania – rozwiązanie konfliktu – nie uzasadniał takiego działania. Szkoła, udostępniając dane, nie dokonała odpowiedniego wyważenia swojego interesu i prawa do prywatności dziecka, za co otrzymała upomnienie.

1.4.8. Zamieszczenie w skierowaniu na badania okresowe adnotacji o stanie zdrowia pracownika

Przedmiotem jednego z postępowań[88] było przetwarzanie przez spółkę (pracodawcę) danych o stanie zdrowia skarżącej, zawartych w skierowaniu na okresowe badania lekarskie. W toku postępowania administracyjnego Prezes UODO wskazał, że wzór skierowania na badania profilaktyczne (wstępne, okresowe, kontrolne) został określony w przepisach prawa. Wśród informacji przewidzianych w tym wzorze nie znajdują się dane dotyczące stanu zdrowia pracownika. Umieszczenie na skierowaniu informacji o tym, że skarżąca miewa omdlenia (bez względu na prawdziwość tej informacji), stanowiło nadmiarowe przetwarzanie danych, do którego pracodawca nie był uprawniony.

Przepisy Kodeksu pracy nie uprawniają pracodawcy do weryfikowania rodzaju przeprowadzanych badań ani ich wyników. W decyzji stwierdzono zatem, że pracodawca bezpodstawnie zamieścił na skierowaniu na badania okresowe adnotację dotyczącą zaobserwowanych u skarżącej omdleń. Prezes UODO zwrócił również uwagę, że choć pracodawca nie może dopuścić pracownika do pracy bez aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do wykonywania obowiązków na określonym stanowisku w warunkach opisanych w skierowaniu, to jednak przepisy Kodeksu pracy przewidują jedynie wydanie pracodawcy zaświadczenia potwierdzającego brak przeciwwskazań do pracy lub informującego o ich istnieniu.

Spółka, kierując skarżącą na badania okresowe, nie miała zatem dowolności w zakresie kształtowania treści skierowania.

1.4.9. Realizacja prawa do sprostowania danych przez podmiot medyczny

Skarżący zgłosił w jednej ze spraw[89], że podmiot medyczny przetwarzał jego nieaktualne dane osobowe dotyczące drugiego imienia, mimo złożenia wniosku o ich sprostowanie. Skarżący skorzystał z przysługującego mu na podstawie art. 16 RODO prawa do sprostowania danych, zgłaszając zmianę imienia i adresu zamieszkania. Z powodu błędu lub niezrozumienia zakresu zmian przez pracownika podmiotu medycznego, drugie imię skarżącego nie zostało usunięte z kartoteki. W efekcie podmiot przetwarzał nieaktualne dane od momentu zgłoszenia zmiany do dnia ich poprawienia po wniesieniu skargi.

Prezes UODO stwierdził, że dalsze przetwarzanie nieaktualnych danych osobowych nie miało podstawy w art. 6 ust. 1 RODO i naruszało zasadę prawidłowości danych określoną w art. 5 ust. 1 lit. d RODO. W związku z tym podmiot medyczny otrzymał upomnienie.

---

[88] DS.523.5504.2024.
[89] DS.523.238.2024.

1.4.10. Przetwarzanie danych osobowych dziecka sprzed jego adopcji w dokumentacji medycznej

W jedne ze skarg[90] skarżąca zarzuciła, że podmiot medyczny nadal przetwarzał stary numer PESEL jej małoletniego dziecka, mimo posiadania nowego numeru nadanego w wyniku adopcji. Dodatkowo w zaświadczeniu lekarskim znalazł się stary numer PESEL, co skutkowało ujawnieniem informacji o procedurze adopcji. Po adopcji dziecka skarżąca poinformowała podmiot medyczny o nowym numerze PESEL i złożyła nową deklarację wyboru lekarza i pielęgniarki POZ. W dokumentacji medycznej, w tym w zaświadczeniu lekarskim, nadal jednak widniał stary numer PESEL.

Prezes UODO uznał, że nie istnieją przepisy zobowiązujące podmiot medyczny do usuwania lub aktualizacji dokumentacji medycznej sporządzonej przed adopcją. Dokumentacja ta stanowi zapis historii leczenia pacjenta, a jej archiwizacja w dotychczasowym kształcie jest zgodna z prawem. W związku z tym organ odmówił uwzględnienia skargi w zakresie przetwarzania starego numeru PESEL. W części dotyczącej rzekomego ujawnienia danych o adopcji postępowanie zostało umorzone, ponieważ nie doszło do bezprawnego udostępnienia informacji.

1.4.11. Przetwarzanie przez pracodawcę danych biometrycznych

Skarżąca złożyła skargę[91] na pracodawcę, który stosował system ewidencji czasu pracy oparty na czytnikach linii papilarnych. Zarzuciła, że jej dane biometryczne były przetwarzane bez podstawy prawnej, oraz że nie spełniono wobec niej obowiązku informacyjnego. Pracodawca twierdził, że system nie przechowuje danych biometrycznych, a jedynie porównuje wzór odcisku palca zakodowanego na karcie z odciskiem faktycznym. Prezes UODO uznał jednak, że pracodawca pełni rolę administratora danych biometrycznych, ponieważ to on decydował o sposobie ich przetwarzania i wykorzystywał je w systemie kontroli dostępu.

Wobec braku podstawy prawnej do przetwarzania takich danych Prezes UODO nakazał ich usunięcie.

1.4.12. Realizacja przez szkołę prawa do uzyskania kopii danych

W jednej z procedowanych spraw[92] Prezes UODO ustalił, że ojciec dziecka, które miało wypadek w szkole, zwrócił się do placówki z żądaniem udostępnienia nagrania monitoringu. Szkoła odmówiła, powołując się na ochronę prywatności innych osób oraz regulamin, zgodnie z którym nagrania mogą być udostępniane wyłącznie w przypadku przestępstwa i tylko instytucjom publicznym, np. policji. Prezes UODO wskazał, że regulamin szkoły nie może ograniczać praw wynikających z RODO.

[90] DS.523.2075.2024.
[91] DS.523.2629.2023.
[92] DS.523.2071.2024.

Szkoła została zobowiązana do udostępnienia kopii danych dziecka w zakresie danych znajdujących się nagraniu po uprzednim zapewnieniu poufności danych innych osób.

1.5. Postępowania o charakterze transgranicznym

Prezes Urzędu Ochrony Danych Osobowych uczestniczy w ramach współpracy w egzekwowaniu 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. Co prawda 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. Niemniej 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.

Komunikacja z administratorem w ramach rozpatrywania skarg, których przedmiotem jest transgraniczne przetwarzanie danych, zależy w dużej mierze od współpracy z wiodącym organem nadzorczym, tj. organem właściwym do rozpatrzenia sprawy ze względu na siedzibę administratora.

Prezes UODO w 2024 r. zarówno przekazywał skargi innym organom do ich rozpatrzenia jako wiodącym organom nadzorczym, jak i przyjmował skargi do prowadzenia od innych organów nadzorczych, jeżeli siedziba domyślnego administratora znajdowała się na terytorium Polski. W 2024 r. Prezes UODO otrzymywał wiele skarg, które sklasyfikowano jako transgraniczne od osób, których dane dotyczą, m.in. nieprawidłowości w procesie przetwarzania ich danych przez Uber B.V. (Holandia), Meta Platforms z siedzibą w Irlandii (Facebook), Zalando SE (Niemcy), Amazon czy też linie lotnicze Ryanair z siedzibą w Irlandii. Skargi te w większości dotyczyły naruszenia praw osób, których dotyczą dane zawarte w rozdziale III RODO. Większość z prowadzonych tego typu postępowań przekazanych do prowadzenia innym organom nadzorczym jest nadal w toku, a skargi nie zostały jeszcze rozpatrzone przez organy nadzorcze prowadzące te postępowania, z uwagi na skomplikowany charakter prowadzenia spraw transgranicznych. W roku 2024 zaobserwowano także wzrost skarg i współpracy transgranicznej w obszarach dotyczących sztucznej inteligencji (tzn. duże modele językowe).

Prowadzenie spraw transgranicznych i współpraca z innymi organami nadzorczymi ma za zadanie zwiększyć ochronę praw osób, których dane dotyczą, w całej Unii Europejskiej, co pomaga w przestrzeganiu i stosowaniu przepisów RODO przez administratorów w całej UE i egzekwowaniu praw osób, których dane dotyczą, przez administratorów danych, co zdaniem Prezesa UODO ma ogromne znaczenie w zakresie dalszego skutecznego stosowania RODO.

1.5.1. Udostępnienie nieprawdziwych danych w reklamach wyświetlanych na portalach społecznościowych (deepfake)[93]

Do Prezesa UODO wpłynęły w 2024 r. skargi[94] prezesa jednej ze spółek i jego żony, na nieprawidłowości w procesie przetwarzania ich danych osobowych przez Meta Platforms Ireland Limited (dalej: Meta), polegające na udostępnianiu danych osobowych skarżących, w tym nieprawdziwych informacji na ich temat (odpowiednio: a) informacji dotyczących skarżącej, z których wynika, jakoby została aresztowana, łamała prawo, a także była bita przez swojego męża, oraz informacji o jej rzekomej śmierci; b) informacji dotyczących skarżącego, z których wynika, jakoby reklamował nowe platformy inwestycyjne i zachęcał do korzystania z nich w celu szybkiego pomnożenia środków), w reklamach wyświetlanych na portalach społecznościowych: Facebook oraz Instagram bez podstawy prawnej. Część danych osobowych udostępnionych na ww. portalach była modyfikowana przy użyciu technologii deepfake.

Prezes UODO zidentyfikował sprawę jako mającą charakter transgraniczny zgodnie z art. 4 pkt 23 RODO i przekazał ją irlandzkiemu organowi nadzorczemu Data Protection Commission (dalej: DPC) jako właściwemu do rozpatrzenia skargi zgodnie z art. 56 ust. 1 RODO. 5 sierpnia 2024 r. Prezes UODO wydał postanowienia, mocą których zobowiązał Meta do ograniczenia przetwarzania danych osobowych skarżących poprzez zakazanie ich udostępniania na rzecz innych podmiotów w reklamach wyświetlanych na portalach społecznościowych: Facebook oraz Instagram, na terytorium Rzeczypospolitej Polskiej przez okres trzech miesięcy od dnia doręczenia tych postanowień Meta. Postanowienia zostały wydane w trybie art. 70 ust. 1 i 2 ustawy z 10 maja 2018 r. o ochronie danych osobowych w zw. z art. 66 ust. 1 RODO na skutek udostępniania przez Meta danych osobowych skarżących – w zakresie ich wizerunku, imienia i nazwiska, w tym nieprawdziwych informacji na ich temat w reklamach wyświetlanych na portalach społecznościowych: Facebook oraz Instagram. Reklamy te wyświetlane były mimo skierowanych przez skarżących do Meta wezwań do usunięcia reklam i materiałów sponsorowanych oraz zaprzestania wyświetlania reklam, które wykorzystują ich wizerunek.

Pełnomocnicy Meta za pośrednictwem Prezesa UODO wnieśli skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie oraz do Prezesa UODO o wstrzymanie wykonania ww. postanowień. 23 października 2024 r. Prezes UODO wydał postanowienia w przedmiocie odmowy wstrzymania wykonania ww. postanowień z 5 sierpnia 2024 r. i przekazał do Wojewódzkiego Sądu Administracyjnego w Warszawie akta spraw wraz z ww. skargami Meta oraz odpowiedziami Prezesa UODO na podniesione w nich zarzuty.

WSA w Warszawie, postanowieniami z 10 grudnia 2024 r. odmówił wstrzymania zaskarżonych postanowień Prezesa UODO wskazując, że pełnomocnik strony skarżącej nie uprawdopodobnił zaistnienia przesłanek, o których mowa w art. 61 §

[93] DS.523.4486.2024, DS.523.4480.2024.
[94] DS.523.4486.2024, DS.523.4480.2024.

3 ustawy Prawo o postępowaniu przed sądami administracyjnymi, w odniesieniu do zaskarżonych postanowień, tj. niebezpieczeństwa wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków. Zdaniem WSA argumentacja strony skarżącej ograniczyła się do ogólnych wywodów i stwierdzeń. Strona skarżąca nie przedstawiła żadnych dowodów bądź argumentów obrazujących konkretne relacje między brakiem wstrzymania wykonania zaskarżonego postanowienia a wystąpieniem zagrożeń z art. 61 § 3 p.p.s.a. Powyższe uniemożliwiło sądowi określenie prawdopodobieństwa wystąpienia zdarzeń objętych dyspozycją ww. przepisu. W konsekwencji, jak stwierdził WSA, brak było podstaw do zastosowania wobec strony skarżącej ochrony tymczasowej w ww. zakresie[95].

DPC, który zgodnie ze stanowiskiem Prezesa UODO przyjął sprawę do prowadzenia w charakterze wiodącego organu nadzorczego, w ramach współpracy przedstawił dotyczące możliwości zastosowania w niniejszych sprawach przepisów DSA. W ocenie Prezesa UODO, z uwagi na utrzymujący się w sprawie stan naruszenia, konieczne jest ustalenie przez DPC, jako wiodący organ nadzorczy, zakresu obowiązków Meta jako współadministratora danych osobowych skarżących w kontekście potencjalnego zbiegu zastosowania w sprawie norm wynikających z DSA i RODO oraz komunikowanych w tym zakresie przez DPC wątpliwości. Współpraca z DPC trwa, a DPC jeszcze nie ustosunkowała się do ww. oceny Prezesa UODO, przedstawionej 4 grudnia 2024 r.

Powyższa sprawa ma charakter precedensowy i przełomowy. Ze względu na odbicie się szerokim echem w Europie wydanych przez Prezesa UODO postanowień, do Urzędu zaczęły wpływać skargi dotyczące przetwarzania danych osobowych w reklamach na platformach społecznościowych, w tym osób publicznie rozpoznawalnych (np. skarga lekarza dot. reklamowania produktu na stawy za pomocą technologii deepfake wykorzystującej jego wizerunek[96]). W sprawach tych Prezes UODO prowadzi dalsze działania o charakterze indywidualnym oraz systemowym.

1.5.2. Inne sprawy o charakterze transgranicznym

W postępowaniach o charakterze transgranicznym pojawiły się skargi na wykorzystanie danych osobowych przez duże platformy mediów społecznościowych w celu trenowania sztucznej inteligencji, np. skargi wniesione przez NOYB dotyczące Twitter/X (narzędzie GROK)[97] czy Meta (narzędzie AI)[98]. Skargi na te platformy dotyczyły w większości braku istnienia podstawy prawnej dla przetwarzania danych przez modele uczenia maszynowego, braku wypełnienia obowiązków informacyjnych wobec osób, których dane zostały wykorzystane do trenowania sztucznej inteligencji oraz braku możliwości skutecznego wyegzekwowania niektórych uprawnień osób, których dane dotyczą np. prawa do bycia zapomnianym. Wszystkie organy nadzorcze UE koordynowały i konsultowały ze sobą działania w sprawie tych skarg. W zakresie

[95] Sygn. akt II SA/Wa 1700/24, sygn. akt II SA/Wa 1701/24. Zob. też informacja opublikowana na stronie Urzędu, gdzie opisany jest wyrok w tej sprawie, który zapadł w 2025 r.: https://uodo.gov.pl/pl/138/3601.
[96] DS.523.7407.2024.
[97] DS.523.4861.2024.
[98] DS.523.3372.2024.

spraw przytoczonych powyżej można m.in. wskazać informację o wycofaniu przez Meta narzędzia Meta AI w wersji, która objęta była przedmiotem skargi (https://noyb.eu/en/preliminary-noyb-win-meta-stops-ai-plans-eu).

Natomiast w sprawie GROK, DPC wezwał NOYB do przedstawienia kopii korespondencji skarżącego z Twitter/X. NOYB nie odebrał przedmiotowego wezwania oraz nie udzielił na nie odpowiedzi, o czym Prezes UODO poinformował DPC.

1.6. Skargi na przewlekłość w sprawach skargowych

W roku 2024 skierowanych zostało łącznie 51 skarg na przewlekłość oraz bezczynność organu nadzorczego w postępowaniach administracyjnych prowadzonych w sprawach skargowych. Skargi te wraz z odpowiedzią na nie Prezesa UODO przekazane zostały do rozpatrzenia przez Wojewódzki Sąd Administracyjny w Warszawie.

W analizowanym roku do Prezesa Urzędu Ochrony Danych Osobowych wpłynęło 14 prawomocnych wyroków Wojewódzkiego Sądu Administracyjnego w Warszawie, stwierdzających bezczynność lub przewlekłość w prowadzonym przez organ nadzorczy postępowaniu oraz 16 wyroków tego sądu, w których skarga na bezczynność organu nie została uwzględniona. W tym samym okresie do organu wpłynęły 4 wyroki Naczelnego Sądu Administracyjnego w Warszawie, stwierdzające bezczynność lub przewlekłość oraz 4 wyroki tego sądu, w których nie stwierdzono bezczynności lub przewlekłości organu.

Niemniej podkreślić należy, że Prezes UODO podejmuje różnorodne działania, mające na celu usprawnienie rozpatrywania wpływających do niego spraw skargowych. Działania te podejmowane są jednak w ramach możliwości organizacyjnych organu, który nie posiada jednostek zamiejscowych i rozpatruje skargi napływające z całego kraju, a liczba tych skarg stale rośnie. Wpływ na liczbę rozpatrzonych spraw skargowych ma również budżet przeznaczony na zatrudnienie, który w danym roku zostaje przyznany organowi nadzorczemu i który przekłada się również na liczbę pracowników zatrudnionych w Departamencie Skarg. Poza ograniczonymi możliwościami kadrowymi również liczba wnoszonych skarg wpływa na czas trwania postępowań, prowadzonych przez Prezesa UODO. Należy podkreślić, że dzięki podjętym działaniom, pomimo wzrostu liczby skarg wniesionych do Prezesa UODO w 2024 r. wzrosła również liczba postępowań skargowych, które zostały w tym roku zakończone.

1.7. Rewizja stanowisk w sprawach z lat ubiegłych

Wskutek wniosku Rzecznika Praw Obywatelskich z 22 grudnia 2020 r.[99], przed Prezesem Urzędu Ochrony Danych Osobowych zostało wszczęte z urzędu postępowanie administracyjne w przedmiocie naruszenia przepisów o ochronie danych osobowych dotyczące przetwarzania danych dotyczących zdrowia skarżącej przy okazji wykonywania testu diagnostycznego w kierunku SARS-CoV-2. Brak zgody

[99] DS.523.6513.2020.

skarżącej na prowadzenie postępowania z urzędu w sprawie z ww. wniosku Rzecznika Praw Obywatelskich, brak możliwości uzyskania takiej zgody przez Prezesa UODO z uwagi na niedysponowanie adresem zamieszkania skarżącej oraz brak trybu postępowania, w którym Prezes UODO mógłby skutecznie wezwać Rzecznika Praw Obywatelskich do uzupełnienia ww. adresu, wypełniły w ocenie ówczesnego Prezesa UODO przesłankę z art. 61a § 1 k.p.a., przesądzającą o niedopuszczalności prowadzenia przez organ postępowania w niniejszej sprawie. Znalazło to odzwierciedlenie w postanowieniu z 19 stycznia 2021 r. w przedmiocie odmowy wszczęcia postępowania. Wojewódzki Sąd Administracyjny w Warszawie (WSA) wyrokiem z 29 września 2021 r.[100] uchylił postanowienie Prezesa UODO z 19 stycznia 2021 r. Od wyroku tego Prezes UODO złożył skargę kasacyjną. Jednakże w 2024 r., po ponownym przeanalizowaniu niniejszej sprawy przez obecnego Prezesa UODO, organ ten uznał za zasadne stanowisko Rzecznika Praw Obywatelskich wyrażone w odpowiedzi na ww. skargę kasacyjną, dotyczące konieczności zbadania niniejszej sprawy w szerszym zakresie, tj. w zakresie legalności przekazania danych osobowych skarżącej dziennikarzom przez administratora jej danych osobowych, a także prawidłowości przetwarzania jej danych w systemie teleinformatycznym udostępnionym przez jednostkę podległą ministrowi właściwemu do spraw zdrowia, właściwą w zakresie systemów informacyjnych ochrony zdrowia zgodnie z ówcześnie obowiązującym § 2 ust. 5 rozporządzenia Rady Ministrów z 21 grudnia 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[101], jak również przez podmiot, w którym wykonany został test diagnostyczny w kierunku SARS-CoV-2. Prezes UODO dysponuje już adresem zamieszkania skarżącej, który został wskazany przez Rzecznika Praw Obywatelskich w skardze do WSA na ww. postanowienie Prezesa UODO. W konsekwencji Prezes 23 kwietnia 2024 r. cofnął skargę kasacyjną z 1 grudnia 2021 r. od wyroku WSA z 29 września 2021 r.[102] i Naczelny Sąd Administracyjny postanowieniem z 24 maja 2024 r.[103] z tego powodu umorzył postępowanie kasacyjne.

Kolejnymi sprawami, w których Prezes UODO zrewidował swoje dotychczasowe stanowisko, były sprawy dotyczące tzw. wyborów kopertowych. Pierwszą z nich była sprawa[104] ze skargi dotyczącej nieprawidłowości w procesie przetwarzania danych osobowych przez Ministra Cyfryzacji oraz Pocztę Polską S.A. w związku z organizacją wyborów Prezydenta Rzeczypospolitej Polskiej w 2020 r. W sprawie tej postanowieniem z 7 lipca 2020 r. Prezes UODO odmówił wszczęcia postępowania. Wojewódzki Sąd Administracyjny w Warszawie wyrokiem z 23 kwietnia 2021 r.[105] uchylił ww. postanowienie. Prezes UODO 24 czerwca 2021 r. złożył skargę kasacyjną od ww. wyroku WSA z 23 kwietnia 2021 r. Niemniej jednak 13 marca 2024 r. zapadł

[100] Sygn. akt II SA/Wa 778/21.
[101] Dz. U. poz. 2316 ze zm.
[102] Sygn. akt II SA/Wa 778/21.
[103] Sygn. akt III OSK 7740/21.
[104] DS.523.2298.2020.
[105] Sygn. akt II SA/Wa 1750/20.

wyrok Naczelnego Sądu Administracyjnego[106], wobec którego, w ocenie Prezesa UODO, cofnięcie ww. skargi kasacyjnej było konieczne i uzasadnione. W konsekwencji w sprawie tej Prezes UODO cofnął skargę kasacyjną Prezesa UODO z 24 czerwca 2021 r. od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie[107] uchylającego postanowienie Prezesa UODO z 7 lipca 2020 r. w przedmiocie odmowy wszczęcia postępowania i wniósł o umorzenie postępowania. Naczelny Sąd Administracyjny postanowieniem z 9 kwietnia 2024 r.[108] umorzył postępowanie. Cofnięcie ww. skargi kasacyjnej przez Prezesa UODO nastąpiło z uwagi na to, że w dniu 13 marca 2024 r. Naczelny Sąd Administracyjny, rozpatrując skargę kasacyjną Poczty Polskiej S.A. od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 26 lutego 2021 r. (sygn. akt II SA/Wa 1817/20), oddalił przedmiotową skargę, wskutek czego ww. wyrok WSA z 26 lutego 2021 r. stał się prawomocny. Natomiast w ww. wyroku WSA w sprawie ze skargi Rzecznika Praw Obywatelskich na czynność Ministra Cyfryzacji w przedmiocie udostępnienia spółce Poczta Polska S.A. danych osobowych żyjących obywateli polskich z rejestru PESEL, stwierdził bezskuteczność tej czynności, albowiem została ona wydana z naruszeniem przepisów prawa, obowiązujących w dacie jej dokonania. Stanowisko Prezesa UODO zaprezentowane zarówno w zaskarżonym postanowieniu z 7 lipca 2020 r., jak i w skardze kasacyjnej – gdzie wskazano, że z uwagi na istniejące **w obrocie prawnym, w czasie przekazywania danych osobowych z rejestru PESEL, rozstrzygnięcie Prezesa Rady Ministrów z 16 kwietnia 2020 r., nakładające na Pocztę Polską S.A. obowiązek,** o którym mowa w art. 99 ustawy z 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2[109], **dla realizacji którego potrzebne jest pozyskanie danych osobowych przez operatora pocztowego, istniała podstawa prawna do udostępnienia tych danych operatorowi pocztowemu** i pozyskanie danych osobowych przez Pocztę Polską S.A. miało oparcie w art. 6 ust. 1 lit. c RODO w zw. z art. 99 ustawy u.s.i.w. jako będące wynikiem wykonania obowiązku jednoznacznie określonego w przepisach prawa – było wadliwe. Dlatego też ww. skarga kasacyjna została cofnięta.

W pozostałych analogicznych sprawach dotyczących wyborów kopertowych, skargi kasacyjne Prezesa UODO również zostały przez niego cofnięte, wobec czego postępowania w sprawie skarg skierowanych do Prezesa UODO, dotyczących tzw. wyborów kopertowych, zostały podjęte.

W 2024 r. zmiana stanowiska Prezesa UODO nastąpiła również w sprawie postępowania z urzędu[110] wszczętego na skutek wniosku Rzecznika Praw Obywatelskich z 9 marca 2020 r. dotyczącego naruszenia przepisów o ochronie danych osobowych w związku z realizacją obowiązku składania przez sędziów i prokuratorów oświadczeń o członkostwie w zrzeszeniu (stowarzyszeniu) i ich

[106] Sygn. akt II OSK 1630/21.
[107] Sygn. akt II SA/Wa 1750/20.
[108] Sygn. akt III OSK 6133/21.
[109] Dz. U. z 2023 r. poz. 201 ze zm.
[110] DS.523.1470.2020.

upubliczniania. W sprawie tej Prezes UODO wcześniej umorzył postępowanie, stwierdzając, że kwestionowane przez RPO przetwarzanie danych osobowych sędziów i prokuratorów było wynikiem wykonania przez ww. osoby obowiązku jednoznacznie określonego w przepisie prawa i miało oparcie w art. 6 ust. 1 lit. c RODO. Decyzja ta została utrzymana w mocy przez WSA wyrokiem z 15 lutego 2021 r.[111], który następnie został zakwestionowany przez Rzecznika Praw Obywatelskich skargą kasacyjną z 10 maja 2021 r.

W 2024 r., w związku z wyrokiem Trybunału Sprawiedliwości z 5 czerwca 2023 r. w sprawie C-204/21, *Komisja Europejska przeciwko Rzeczypospolitej Polskiej*, Prezes UODO zmienił swoje dotychczasowe stanowisko prezentowane w tej sprawie. W piśmie procesowym z 22 maja 2024 r. skierowanym do NSA wskazał, że aktualnie nie może podtrzymać stanowiska zaprezentowanego w zaskarżonej decyzji z 6 kwietnia 2020 r.[112], jak i w odpowiedzi na skargę kasacyjną. W ww. wyroku z 5 czerwca 2023 r. Trybunał Sprawiedliwości stwierdził bowiem, że przyjmując i utrzymując w mocy art. 88a ustawy z 27 lipca 2001 r. Prawo o ustroju sądów powszechnych[113] (p.u.s.p.) w brzmieniu nadanym ustawą z 20 grudnia 2019 r. o zmianie ustawy Prawo o ustroju sądów powszechnych, ustawy o Sądzie Najwyższym oraz niektórych innych ustaw[114], art. 45 § 3 ustawy o Sądzie Najwyższym z 8 grudnia 2017 r.[115] w brzmieniu nadanym wspomnianą wcześniej ustawą z 20 grudnia 2019 r. i art. 8 § 2 ustawy Prawo o ustroju sądów administracyjnych z 25 lipca 2002 r.[116] (p.u.s.a.) w brzmieniu nadanym tą samą ustawą z 20 grudnia 2019 r., Rzeczpospolita Polska uchybiła prawu do poszanowania życia prywatnego i prawu do ochrony danych osobowych zagwarantowanym w art. 7 i art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz w art. 6 ust. 1 akapit pierwszy lit. c oraz lit. e, art. 6 ust. 3 i art. 9 ust. 1 RODO. Prezes UODO w ww. decyzji z 6 kwietnia 2020 r. uznał, że z powołanych przepisów p.u.s.p., p.u.s.a., a także art. 70 ustawy z 21 sierpnia 1997 r. Prawo o ustroju sądów wojskowych[117], ustawy o Sądzie Najwyższym i art. 103 a § 1 ust. 1 i 2 ustawy z 28 stycznia 2016 r. Prawo o prokuraturze[118], wynika obowiązek złożenia przez sędziów i prokuratorów oświadczeń o członkostwie w organizacjach w nich wymienionych, przed powołaniem na stanowisko, a także upublicznienia ww. oświadczeń w Biuletynie Informacji Publicznej.

Wyrok Trybunału Sprawiedliwości odnoszący się wprost do ww. przepisów krajowych, będących podstawą kwestionowanego rozstrzygnięcia Prezesa UODO. i jednocześnie zawierający ich ocenę pod kątem zgodności z prawem unijnym, ma istotne znaczenia dla niniejszej sprawy. Trybunał Sprawiedliwości w wyroku z 5 czerwca 2023 r., C-204/21 uznał ww. przepisy prawa krajowego za naruszające art. 7 i art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 6 ust. 1 akapit

[111] Sygn. akt II SA/Wa 1264/20.
[112] DS.523.1470.2020.AZ.I.
[113] Dz. U. z 2024 r. poz. 334 ze zm.
[114] Dz. U. z 2020 r. poz. 190.
[115] Dz. U. z 2023 r. poz. 1093 ze zm.
[116] Dz. U. z 2022 r. poz. 2492 ze zm.
[117] Dz. U. z 2022 r. poz. 2250 ze zm.
[118] Dz. U. z 2024 r. poz. 390.

pierwszy lit. c oraz lit. e, art. 6 ust. 3 i art. 9 ust. 1 RODO. Zdaniem Prezesa UODO ww. wyrok Trybunału Sprawiedliwości, jak również wyrok Europejskiego Trybunału Praw Człowieka z 22 lutego 2024 r. w sprawie Kaczmarek przeciwko Polsce (16974/14), jako potwierdzające słuszność stanowiska Rzecznika Praw Obywatelskich wyrażonego w opisanej wyżej skardze kasacyjnej, nie mogły zostać pominięte przy rozpatrywaniu niniejszej sprawy przez NSA.

W ich świetle zasadne jest bowiem stanowisko Rzecznika Praw Obywatelskich dotyczące naruszenia zarówno przez WSA, jak i organ, art. 6 ust. 1 lit. c oraz lit. e RODO w zw. z art. 6 ust. 3 RODO. Artykuł 6 ust. 3 RODO *in fine* stanowi, że prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu. Jak wskazał Rzecznik, kluczowe znaczenie w niniejszej sprawie ma to, że ustawodawca unijny nie poprzestał, w odniesieniu do przepisu prawa krajowego, który stanowić ma podstawę przetwarzania danych osobowych w zw. z art. 6 ust. 1 lit. c RODO, na formalnym wymaganiu jego uchwalenia i obowiązywania. Taki przepis krajowy musi spełniać kryteria jakościowe, to jest służyć realizacji celu leżącego w interesie publicznym oraz być proporcjonalny do wyznaczonego, prawnie uzasadnionego celu. W przypadku przetwarzania, o którym mowa w art. 6 ust. 1 lit. e RODO, musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Jak zauważył Rzecznik, WSA powinien był wziąć pod uwagę i zastosować wymagania jakościowe, dotyczące przede wszystkim niezbędności i proporcjonalności, wynikające z prawa Unii Europejskiej.

Oparcie rozstrzygnięcia na przepisie krajowym, nieokreślającym celu przetwarzania danych pozyskiwanych w drodze ww. oświadczeń o członkostwie m.in. w zrzeszeniach czy stowarzyszeniach, w tym ich publicznego udostępnienia w BIP, jak i okresu przechowywania udostępnionych danych, było niewystarczające.

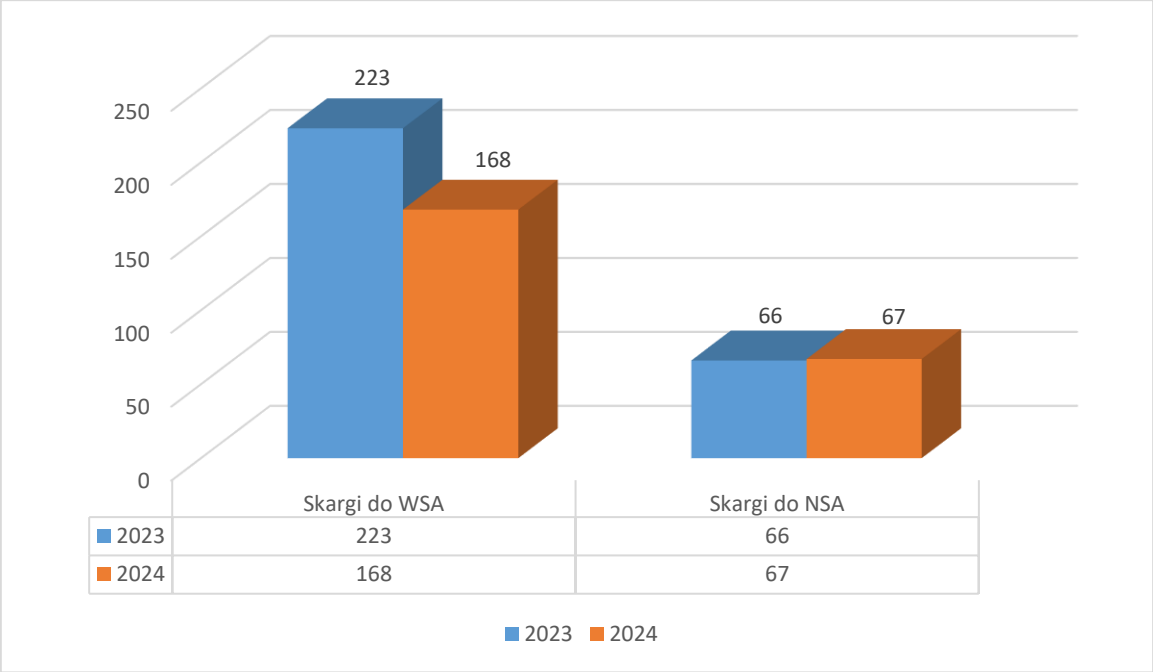
Naczelny Sąd Administracyjny wyrokiem z 29 kwietnia 2025 r.[119], uwzględnił skargę kasacyjną Rzecznika Praw Obywatelskich od wyroku WSA, który wcześniej podtrzymał decyzję Prezesa Urzędu Ochrony Danych Osobowych z 6 kwietnia 2020 r. w sprawie tzw. ustawy kagańcowej. NSA uchylając wyrok sądu niższej instancji, przychylił się tym samym do stanowiska RPO, zgodnego z nowym stanowiskiem organu nadzorczego w tej sprawie. Uchylenie wyroku WSA i decyzji Prezesa UODO oznacza, że organ nadzorczy musi przeprowadzić postępowanie administracyjne wszczęte na żądanie Rzecznika Praw Obywatelskich[120].

1.8. Orzecznictwo sądów administracyjnych w sprawach skargowych

W roku 2024 odnotowano spadek liczby skarg wniesionych na decyzje organu do Wojewódzkiego Sądu Administracyjnego w Warszawie. W roku 2024 skarga taka została wniesiona w **168 przypadkach**, zaś w roku 2023 r. odnotowano 223 takie skargi. Na podobnym poziomie pozostała natomiast zaskarżalność wyroków

[119] Sygn. akt. III OSK 5037/21.
[120] https://uodo.gov.pl/pl/138/3659.

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 2024 wniesiono **67,** podczas gdy w roku 2023 wniesiono ich 66.



Wykres 5. Decyzje wydane w postępowaniach skargowych, zaskarżone do WSA i skargi do NSA w sprawach wyroków WSA dotyczących decyzji wydanych przez Prezesa UODO w latach 2023–2024.

1.9. Wyroki sądów administracyjnych w sprawach skargowych – wybrane przykłady

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

Podobnie jak w latach poprzednich, również w roku 2024 sądy administracyjne rozstrzygały w sprawie skarg na decyzje Prezesa UODO, które dotyczyły przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego.

W jednym z wyroków Naczelny Sąd Administracyjny w Warszawie uchylił zaskarżony wyrok Wojewódzkiego Sądu Administracyjnego i oddalił skargę banku na decyzję Prezesa UODO, potwierdzając aktualność na gruncie przepisów RODO stanowiska Prezesa UODO w zakresie wykładni art. 105a ust. 3 Prawa bankowego, zgodnie z którym przedstawienie dowodu na wysłanie pisma z informacją o zamiarze przetwarzania danych na podstawie ww. przepisu nie jest równoznaczne z przedstawieniem dowodu na poinformowanie przez bank swojego klienta o zamiarze takiego przetwarzania[121]. Naczelny Sąd Administracyjny w 2024 r. wydał następnie kolejne wyroki, w których potwierdził słuszność stanowiska Prezesa UODO odnośnie

[121] Wyrok NSA z 16 stycznia 2024 r., sygn. akt III OSK 3233/21.

do przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego[122].

Naczelny Sąd Administracyjny podzielił również argumentację Prezesa UODO zawartą w decyzji. Stwierdzono, że dłużnik nie odebrał korespondencji zawierającej informację dotyczącą zamiaru przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego, niemniej jednak bank przedstawił dowód próby podjęcia doręczenia pisma w formie dwukrotnie awizowanej koperty z korespondencją zawierającą pismo, która została zwrócona do banku. W ocenie Naczelnego Sądu Administracyjnego, zgodnej z oceną Prezesa UODO, oczywiste było, że bank zapewnił osobie, której dane dotyczą realną możliwość zapoznania się z treścią pisma. Bank, który dołożył wszelkiej staranności w zakresie przekazania informacji, o której mowa w art. 105a ust. 3 Prawa bankowego, nie może ponosić konsekwencji nieodebrania przez dłużnika korespondencji, o ile skierował ją na podany przez nią adres do korespondencji i posiada dowód na to, że podjęte zostały próby jej doręczenia. Tym samym sąd podzielił stanowisko Prezesa UODO, że musi istnieć mechanizm, który w sytuacji zachowania przez bank wszelkiej staranności przy wysłaniu zawiadomienia, zgodnego z treścią art. 105a ust. 3 Prawa bankowego i przedstawienia przez dany bank dowodów na powyższe, uchroni bank przed ww. działaniami dłużnika. Przyjęcie w pełni odmiennej interpretacji ww. przepisu determinować może umożliwienie dłużnikom banków uchylania się od negatywnych konsekwencji niespłacenia zobowiązań, poprzez celowe nieodbieranie listów poleconych wysłanych za zwrotnym potwierdzeniem odbioru[123].

W 2024 r. Wojewódzki Sąd Administracyjny w Warszawie wydawał prawomocne wyroki dowodzące słuszności wykładni ww. przepisu przez Prezesa UODO[124]. Wojewódzki Sąd Administracyjny w Warszawie również stanął na stanowisku, że potwierdzenie nadania nie jest równoznaczne z wykazaniem, że poinformowanie nastąpiło w konkretnej dacie[125].

Wojewódzki Sąd Administracyjny w Warszawie potwierdził stanowisko Prezesa UODO w zakresie niedopuszczalności przetwarzania danych osobowych na zapas przez banki w celu obrony przed ewentualnymi roszczeniami. Sąd wskazał, że z uwagi na fakt, że bank nie wskazał roszczenia, którego zaspokojenia domaga się od uczestniczki, jak również brak jest sporu toczącego się między nią a bankiem dotyczącego stosunku zobowiązaniowego, Prezes UODO zasadnie przyjął, że brak jest celu uzasadniającego przetwarzanie ww. danych osobowych uczestniczki, w rozumieniu art. 6 ust. 1 lit. f RODO[126]. Wojewódzki Sąd Administracyjny w Warszawie wskazał również, że przesłanka określona w art. 6 ust. 1 lit. f RODO nie jest ukierunkowana na ochronę interesów sektora bankowego czy też gospodarczego.

[122] Wyroki NSA z 17 grudnia 2024 r. sygn. akt III OSK 1763/24, z 17 grudnia 2024 r. sygn. akt III OSK 2714/23, z 17 grudnia 2024 r. sygn. akt III OSK 2672/23, z 17 grudnia 2024 r., sygn. akt III OSK 1428/24, z 17 grudnia, sygn. akt III OSK 1763/24, z 17 grudnia 2024 r., sygn. akt III OSK 7477/21, z 17 grudnia 2024 r., sygn. akt III OSK 251/23.
[123] Wyrok NSA z 13 czerwca 2024 r., sygn. akt III OSK 2334/22.
[124] Wyrok WSA w Warszawie z 25 kwietnia 2024 r., sygn. akt II SA/Wa 1641/23.
[125] Wyrok WSA w Warszawie z 15 kwietnia 2024 r., sygn. akt II SA/Wa 1661/23.
[126] Wyrok WSA w Warszawie z 26 lutego 2024 r., sygn. akt II SA/Wa 1631/23.

Podobnie jak pozostałe przesłanki wymienione w art. 6 ust. 1 RODO stanowi przesłankę zgodności z prawem procesu przetwarzania. Tym samym chroni przede wszystkim osobę, której proces ten dotyczy przed nieuprawnionym przetwarzaniem jej danych osobowych[127].

Wojewódzki Sąd Administracyjny w Warszawie oddalił również skargę na decyzję Prezesa UODO, w której organ udzielił bankowi upomnienia za naruszenie art. 6 ust. 1 RODO polegające na przetwarzaniu danych osoby skarżącej w zakresie informacji o opóźnieniach w spłacie umowy w bazie biura informacji kredytowej. W przedmiotowej decyzji Prezes UODO podkreślił, że dane gromadzone przez biuro informacji kredytowej powinny odzwierciedlać rzeczywisty stan zobowiązań kredytowych. Tymczasem bank pomimo udzielenia zabezpieczenia przez sąd powszechny poprzez wstrzymanie obowiązku dokonywania spłat rat kredytu do czasu uprawomocnienia się orzeczenia kończącego ww. postępowanie sądowe przekazał do biura informacji kredytowej informacje dotyczące opóźnień w spłacie umowy. W ocenie sądu Prezes UODO słusznie uznał, że to bank nieprawidłowo przetwarzał dane osobowe klientów, gdyż nie przekazał do biura informacji kredytowej w terminie wynikającym z przepisów prawa, informacji o postanowieniu o zabezpieczeniu i tym samym aktualizacji informacji o opóźnieniach w spłacie rat kredytu. Jednocześnie sąd zauważył, że biuro informacji kredytowej nie dokonuje samodzielnie aktualizacji danych o zobowiązaniach, ale przetwarza te informacje zgodnie z treścią otrzymaną od banków, zatem to od działania lub zaniechania banku uzależniona jest prawidłowość danych przetwarzanych w ww. instytucji utworzonej na podstawie art. 105 ust. 4 Prawa bankowego.

Wojewódzki Sąd Administracyjny w Warszawie podzielił również stanowiska Prezesa UODO w kwestii ścigania przestępstw, określonych przepisami prawa karnego, prowadzenia postępowań mających na celu wykrycie sprawców tych przestępstw, określonych przepisami prawa karnego czy też prowadzenia postępowań mających na celu wykrycie sprawców tych przestępstw, wskazując, że leżą one poza kompetencjami Prezesa UODO. W powyższych sprawach właściwymi są organy ścigania, takie jak policja czy prokuratura. Prezes UODO wskazuje na powyższe kwestie wielokrotnie w decyzjach oraz na wielu etapach postępowania w ramach informacji przekazywanych jego stronom.

1.9.2. Wyrok w sprawie decyzji dotyczącej udostępnienia danych osobowych podczas przeprowadzania czynności terenowych przez komornika

W 2024 r. Wojewódzki Sąd Administracyjny w Warszawie wydał wyrok, w którym oddalił skargę na decyzję Prezesa UODO odmawiającą uwzględnienia wniosku skarżących dotyczącego nieprawidłowości w procesie przetwarzania ich danych osobowych przez komornika sądowego, polegających na udostępnieniu danych osobowych skarżących w postaci imienia i nazwiska na rzecz ich pracownika poprzez okazanie ww. osobie dokumentów egzekucyjnych. Skarżący byli wspólnikami spółki

[127] Wyrok WSA w Warszawie z 25 kwietnia 2024 r., sygn. akt II SA/Wa 1641/23.

jawnej, wobec której komornik prowadził postępowanie egzekucyjne. Dane osobowe skarżących w postaci imienia i nazwiska zostały udostępnione podczas prowadzenia przez komornika czynności terenowych pracownikowi ww. spółki jawnej poprzez okazanie tej osobie tytułu wykonawczego. Jak wynikało z materiału dowodowego, czynności egzekucyjne podjęte w siedzibie spółki spowodowane były zarzutami dłużnika dotyczącymi niemożności wypłaty wynagrodzeń pracownikom. Komornik weryfikował m.in. rodzaj płatności – czy stosowane są płatności wyłącznie gotówkowe, czy także obrót bezgotówkowy. Pracownik spółki podczas wykonywania czynności przez komornika był obecny w siedzibie spółki. Komornik zwrócił się do pracownika o udzielenie informacji dotyczących majątku spółki. Pracownik wniósł o przedłożenie dokumentów uprawniających do dokonania tej czynności – tytułu wykonawczego. Z przeprowadzonych czynności terenowych sporządzono protokół. Zgodnie art. 761 § 1^1 ust. 13 k.p.c. komornik ma prawo zażądać od innych instytucji i osób nieuczestniczących w postępowaniu informacji dotyczących stanu majątkowego dłużnika lub umożliwiających identyfikację składników jego majątku oraz danych adresowych w zakresie niezbędnym do zapewnienia prawidłowego toku postępowania. Komornik miał prawo w celu określenia, czyjego majątku poszukuje, udostępnić dane osobowe skarżących w zakresie imienia i nazwiska jako wspólników dłużnej spółki, osobie, do której się zwrócił o informacje dotyczące stanu majątkowego spółki. Komornik, prowadząc czynności terenowe i zwracając się do innych osób (w niniejszej sprawie do pracownika spółki) o informacje dotyczące stanu majątkowego dłużnika, musi zidentyfikować go w takim stopniu, jaki pozwoli to osobie, do której się zwróci, na udzielenie stosownych informacji. Nazwa dłużnika lub jego imię i nazwisko należy do zakresu minimalnych danych, które go identyfikują. W omawianej sprawie dłużnikiem była spółka jawna, jednak skarżący byli jej wspólnikami i osobami uprawnionymi do jej reprezentacji. Powyższe stanowisko podzielił Wojewódzki Sąd Administracyjny w Warszawie, oddalając skargę na ww. decyzję Prezesa UODO.

1.9.3. Wyrok w sprawie decyzji dotyczącej udostępnienia przez wojewodę danych osobowych zawartych w wystąpieniach pokontrolnych na stronie BIP urzędu wojewódzkiego

Wojewódzki Sąd Administracyjny w Warszawie wydał także wyrok oddalający skargę na decyzję Prezesa UODO, w której udzielił on upomnienia wojewodzie za udostępnienie bez podstawy prawnej danych osobowych skarżącej na stronie internetowej BIP urzędu wojewódzkiego w wystąpieniach pokontrolnych skierowanych do jednego z prezydentów miast oraz ośrodka pomocy społecznej. Wojewoda przeprowadził kontrole w sprawie skarżącej, która korzystała z pomocy ośrodka pomocy społecznej. Kontrole te miały na celu zbadanie zgodności działań podejmowanych przez zespół interdyscyplinarny w sprawie skarżącej z przepisami ustawy o przeciwdziałaniu przemocy w rodzinie oraz obowiązującym wówczas rozporządzeniem w sprawie procedury „Niebieskiej Karty”[128], zbadanie adekwatności

[128] Rozporządzenie Rady Ministrów z 13 września 2011 r. w sprawie procedury „Niebieskiej Karty” oraz wzorów formularzy „Niebieska Karta” (Dz.U z 2023 r. poz. 1870).

prowadzonych działań oraz udzielenie pomocy, także w formie pracy socjalnej, rodzinie skarżącej przez ośrodek pomocy społecznej. Na podstawie informacji pozyskanych w toku kontroli sporządzono dwa protokoły kontroli, które przekazano do podpisania prezydentowi miasta oraz dyrektorowi ośrodka pomocy społecznej. Na podstawie podpisanych protokołów sporządzono wystąpienia pokontrolne z ww. kontroli. Wojewoda udostępnił na stronie internetowej BIP urzędu ww. wystąpienia pokontrolne, które nie zostały zanonimizowane i zawierały dane osobowe skarżącej. Wojewoda wyjaśnił, że obowiązek ich publikacji wynika z realizacji prawa dostępu do informacji publicznej określonego u.d.i.p. Prezes UODO ustalił, że obecnie wojewoda nie udostępnia danych osobowych skarżącej na stronie BIP, znajdujące się tam wystąpienia pokontrolne zostały zanonimizowane poprzez zamianę danych umożliwiających identyfikację osoby fizycznej na szereg znaków „xxxxxxxxxx". Prezes UODO zaznaczył, że prawo do informacji publicznej nie jest prawem nieograniczonym. Zgodnie z art. 5 ust. 2 u.d.i.p. prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. W niniejszej sprawie nie zaistniała żadna z tych okoliczności, tym samym wojewoda, publikując dane osobowe skarżącej, naruszył jej prawo do prywatności, a w przypadku tego udostępnienia nie zaistniała żadna z przesłanek określonych w art. 6 ust. 1 RODO. Stanowisko to podzielił WSA w Warszawie, oddalając skargę na ww. decyzję Prezesa UODO.

1.9.4. Wyrok w sprawie decyzji dotyczącej udostępnienia danych osobowych poprzez przekazanie pisma złożonego do urzędu miejskiego na rzecz ochotniczej straży pożarnej oraz wywieszenia ww. pisma w oknie sali ochotniczej straży pożarnej

W 2024 r. do UODO wpłynął wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie, którym oddalił on skargę na decyzję Prezesa UODO, w której Prezes UODO udzielił upomnienia burmistrzowi za udostępnienie przez burmistrza danych osobowych skarżącego w postaci imienia i nazwiska, adresu oraz wzoru podpisu, zawartych w jego piśmie skierowanym do urzędu miejskiego poprzez przekazanie ww. pisma ochotniczej straży pożarnej, oraz przez ochotniczą straż pożarną poprzez wywieszenie ww. pisma w miejscu ogólnodostępnym[129]. W ww. sprawie skarżący skierował do burmistrza pismo w sprawie działalności ochotniczej straży pożarnej. Burmistrz wyjaśnił, że udostępnił dane osobowe skarżącego zawarte w jego piśmie skierowanym do urzędu miejskiego jednostce ochotniczej straży pożarnej na podstawie art. 65 k.p.a. w celu ustosunkowania się przez tę jednostkę do podniesionych w piśmie zarzutów związanych z działalnością operacyjną i gospodarczą jednostki. Burmistrz nie przedstawił jednak dowodów potwierdzających przekazanie pisma skarżącego dotyczącego działalności ochotniczej straży pożarnej

[129] Wyrok WSA w Warszawie z 16 lutego 2024 r. sygn. akt II SA/Wa 755/23.

organowi właściwemu zgodnie z art. 65 k.p.a. Prezes UODO zauważył ponadto, że ochotnicza straż pożarna nie jest organem administracji publicznej, a ww. przepis art. 65 k.p.a. ma zastosowanie do przekazywania podań przez organ administracji publicznej, do którego wpłynęło podanie do innego organu. Ponadto burmistrz wskazał, że przekazał ww. pismo w celu ustosunkowania się jednostki ochotniczej straży pożarnej do podniesionych w piśmie zarzutów związanych z działalnością operacyjną i gospodarczą jednostki. Przetwarzanie danych osobowych osób zgłaszających nieprawidłowości podlega szczególnej ochronie. Jak stanowi art. 225 § 1 k.p.a., nikt nie może być narażony na jakikolwiek uszczerbek lub zarzut z powodu złożenia skargi lub wniosku albo z powodu dostarczenia materiału do publikacji o znamionach skargi lub wniosku, jeżeli działał w granicach prawem dozwolonych. Prezes UODO zwrócił uwagę na ogólny charakter pisma skarżącego, fakt, że nie wniósł w nim o podjęcie działań w indywidualnej (własnej) sprawie, a jego intencją było zwrócenie uwagi burmistrza na istniejące, zdaniem skarżącego, nieprawidłowości w prowadzonej przez ochotniczą straż pożarną działalności. Udostępnienie na rzecz ochotniczej straży pożarnej danych osobowych skarżącego zawartych w ww. piśmie, jako osoby, która złożyła skargę, nie znajdowało podstaw w przepisach prawa. Przepisy m.in. k.p.a. wyposażają organ w instrumenty pozwalające na zbadanie sygnalizowanych przez obywateli nieprawidłowości poprzez wszczęcie postępowania, które może być przeprowadzone bez konieczności ujawniania źródła informacji. Podniesione w skardze zarzuty w stosunku do ochotniczej straży pożarnej nie wymagały udostępniania danych osobowych osoby, która złożyła skargę na działalność ochotniczej straży pożarnej. Natomiast ochotnicza straż pożarna wywiesiła ww. pismo w miejscu ogólnodostępnym na szybie okna w sali ochotniczej straży pożarnej w celu udostępnienia zarzutów co do działalności ochotniczej straży pożarnej pozostałym mieszkańcom. Ochotnicza straż pożarna nie wykazała, aby legitymowała się odnośnie do udostępnienia w powyższy sposób ww. danych osobowych skarżącego, zawartych w piśmie skierowanym do urzędu miejskiego, którąkolwiek z wymienionych w art. 6 ust. 1 RODO przesłanek stanowiących o legalności przetwarzania (w tym udostępniania) danych osobowych skarżącego. WSA w Warszawie wskazał w wydanym wyroku, że Prezes UODO zasadnie przyjął, że zarówno burmistrz, jak i ochotnicza straż pożarna naruszyli art. 6 ust. 1 RODO poprzez udostępnienie bez podstawy prawnej danych osobowych skarżącego w postaci imienia i nazwiska, adresu oraz wzoru podpisu, zawartych w jego piśmie. Sąd stwierdził, że Prezes UODO udzielając zarówno burmistrzowi, jak i ochotniczej straży pożarnej, stosownie do art. 58 ust. 2 lit. b RODO, upomnień za wykazane uchybienia, nie naruszył prawa, a zastosowany przez Prezesa UODO instrument prawny jest adekwatny do wagi stwierdzonych naruszeń.

1.9.5. Wyrok w sprawie decyzji dotyczącej udostępnienia przez spółdzielnię mieszkaniową danych osobowych na rzecz pracodawcy skarżącego

Naczelny Sąd Administracyjny[130] oddalił skargę kasacyjną złożoną przez spółdzielnię mieszkaniową od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie[131] oddalającego skargę na decyzję Prezesa UODO dotyczącą udostępnienia przez spółdzielnię danych osobowych skarżącego w zakresie jego imienia, nazwiska i adresu zamieszkania wojewódzkiemu szpitalowi specjalistycznemu. Spółdzielnia pozyskała dane osobowe skarżącego w związku ze skierowaną przez niego do spółdzielni korespondencją w sprawach dotyczących rozliczeń finansowych oraz uchwał podjętych przez radę nadzorczą spółdzielni. Spółdzielnia odpowiedziała skarżącemu na skierowaną przez niego korespondencję, a odpowiedź skierowała także do wiadomości pracodawcy skarżącego – wojewódzkiego szpitala specjalistycznego. Spółdzielnia nie wykazała podstawy prawnej udostępnienia danych osobowych skarżącego wojewódzkiemu szpitalowi specjalistycznemu, wyjaśniając jedynie, że powodem udostępnienia danych osobowych skarżącego było wykorzystanie przez skarżącego służbowego adresu e-mail dla celów niezwiązanych z obowiązkami służbowymi. Naczelny Sąd Administracyjny podzielił stanowisko Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Prezesa UODO, że działanie spółdzielni polegające na przesłaniu pracodawcy skarżącego jego danych osobowych wyczerpuje znamiona przetwarzania danych osobowych w rozumieniu RODO, a tym samym podlega określonym zasadom przetwarzania danych, których nieprzestrzeganie skutkuje naruszeniem przez spółdzielnię w niniejszej sprawie art. 6 ust. 1 i art. 5 ust. 1 lit. b i lit. c RODO. Działanie spółdzielni, polegające na przekazaniu informacji o sposobie załatwienia sprawy skarżącego pismem przekazanym do wiadomości jego pracodawcy, tj. szpitala, stanowiło niezgodne z prawem przetwarzanie danych osobowych skarżącego. Przetwarzanie danych osobowych skarżącego nie mieści się w realizacji pierwotnego celu przetwarzania jego danych osobowych przez spółdzielnię, tj. jako członka spółdzielni na podstawie art. 6 ust. 1 lit. c RODO w związku z art. 30 ustawy Prawo spółdzielcze[132] oraz art. 4 ust. 2 i art. 4^1 ustawy o spółdzielniach mieszkaniowych[133]. Ww. działanie nie było niezbędne dla udzielenia odpowiedzi skarżącemu na jego pytania związane ze sprawami finansowymi spółdzielni. Tym samym udostępnienie danych skutkowało naruszeniem zasady wyrażonej w art. 5 ust. 1 lit. b i lit. c RODO, tj. celowości (związania celem) przetwarzania danych oraz adekwatności (minimalizacji danych).

1.9.6. Wyrok w sprawie decyzji dot. odmowy usunięcia i zaprzestania przetwarzania danych osobowych przez Dyrektora Generalnego Służby Więziennej w Centralnej Bazie Danych Osób Pozbawionych Wolności

W 2024 roku zapadł wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie oddalający skargę wniesioną przez skarżącego na decyzję Prezesa UODO

[130] Wyrok Naczelnego Sądu Administracyjnego z 19 stycznia 2024 r. sygn. akt III OSK 2816/22.
[131] Wyrok Wojewódzkiego Sądu Administracyjnego z 5 lipca 2022 sygn. akt II SA/Wa 3920/21.
[132] Ustawa z 16 września 1982 r. Prawo spółdzielcze (Dz.U. z 2024 r. poz. 593).
[133] Ustawa z 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz.U. z 2024 r. poz. 558).

wydaną w sprawie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego przez Dyrektora Generalnego Służby Więziennej (zwanego dalej Dyrektorem) w Centralnej Bazie Danych Osób Pozbawionych Wolności (dalej jako CBDOPW) polegające na odmowie usunięcia i zaprzestania przetwarzania w CBDOPW danych osobowych skarżącego w zakresie informacji o wyrokach oraz o środku zapobiegawczym w postaci tymczasowego aresztowania. Decyzją Prezes UODO odmówił uwzględnienia wniosku skarżącego, wskazując, że nie ma podstaw do stwierdzenia, że dane osobowe skarżącego w zakresie informacji o wykonywaniu środka zapobiegawczego w postaci tymczasowego aresztowania, skazaniu wyrokiem, wykonywaniu kary pozbawienia wolności są przetwarzane przez Dyrektora w sposób niezgodny z ustawą z 14 grudnia 2018 r. Przetwarzanie ww. danych osobowych skarżącego, jako niezbędne do zrealizowania uprawnienia służby więziennej wynikającego z art. 24 ust. 4 pkt 1 ustawy o służbie więziennej oraz zrealizowania obowiązku określonego w art. 25a ust. 2 ustawy o służbie więziennej, znajdowało oparcie w przesłance określonej w art. 13 ust. 1 ustawy z 14 grudnia 2018 r. Prezes UODO, wiążąc treść tego przepisu z kompetencjami służby więziennej, stwierdził, że przetwarzanie ww. danych osobowych skarżącego w CBDOPW oparte jest na obowiązujących przepisach prawa. Jak zostało wykazane w postępowaniu, dane osobowe skarżącego zostały zgodnie z przepisami poddane stosownej weryfikacji i ocenie ich przydatności, co implikowało dalsze pozostawienie ich w CBDOPW.

1.9.7. Wyrok w sprawie przetwarzania danych kontaktowych prezesa zarządu spółki

W jednej ze spraw Wojewódzki Sąd Administracyjny w Warszawie uchylił decyzję Prezesa UODO[134], uznając, że podany przez skarżącego numer telefonu stanowił dane kontaktowe osoby prawnej, a nie osoby fizycznej. Tym samym w niniejszej sprawie nie mogło być mowy o naruszeniu przepisów RODO. Jak wyjaśnił sąd, to, że do skarżącego – prezesa spółki – skierowano ofertę przeznaczoną dla zarządu spółki, nie zmienia faktu, że wykorzystano do tego dane firmy. W niniejszej sprawie numer telefonu nie mógł zostać uznany za dane identyfikujące osobę fizyczną, ponieważ był wykorzystywany w działalności osoby prawnej. Sąd szeroko odwołał się do przepisów prowadzenia spraw spółek przez osoby ją reprezentujące.

Sąd zaznaczył jednak, że niniejsza sprawa była wyjątkowa, gdyż skarżący był prezesem zarządu spółki i znajdował się w innej sytuacji zawodowej niż osoby posiadające status pracownika, ponieważ wyłącznie on sam zadecydował o tym, że jego dane osobowe mają być wskazane jako dane kontaktowe podmiotu, który reprezentuje. Sąd podkreślił, że w innym stanie faktycznym można założyć, że możliwe byłoby nadanie numerowi telefonu przymiotu danych osobowych.

[134] Wyrok WSA z 10 kwietnia 2024 r. w sprawie o sygn. akt II SA/Wa 1592/23.

1.9.8. Wyrok w sprawie postanowienia o odmowie wszczęcia postępowania, wydanego ze względu na to, że RODO nie znajdowało zastosowania w zgłoszonej sprawie

W jednej ze spraw Wojewódzki Sąd Administracyjny w Warszawie podzielił[135] stanowisko Prezesa UODO wyrażone w zaskarżonym postanowieniu o odmowie wszczęcia postępowania w sprawie przetwarzania danych osobowych skarżącej przez spółkę ze względu na to, że RODO nie znajdowało w niej zastosowania.

W ww. postanowieniu Prezes UODO wskazał, że stosownie do treści art. 3 ust. 1 rozporządzenia 2016/679 ma ono zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w UE, niezależnie od tego, czy przetwarzanie odbywa się w UE, a także, gdy wprawdzie nie ma takich jednostek organizacyjnych w UE, ale czynności przetwarzania wiążą się z oferowaniem towarów lub usług osobom w UE. Do ustalenia takiego zamiaru nie wystarczy sama dostępność w UE strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator. Z kolei czynnikiem pozwalającym na taką ocenę może być posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w UE[136].

Okoliczność, że strona internetowa jest dostępna w państwie członkowskim UE, nie jest równoznaczna ze skierowaniem jej usług do osób znajdujących się na terenie UE. W szczególności nie świadczy o tym fakt, że popularna wyszukiwarka internetowa zwraca wynik wyszukiwania do tej strony. Z powyższym stanowiskiem Prezesa UODO zgodził się Wojewódzki Sąd Administracyjny w Warszawie.

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 planem kontroli lub na podstawie uzyskanych przez niego informacji, a także w ramach monitorowania przestrzegania stosowania przepisów rozporządzenia 2016/679 (RODO).

Prezes UODO przeprowadził w 2024 r. czynności kontrolne w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych **50 podmiotach.** Wymienione działania były realizowane w wykonaniu uprawnień przysługujących organowi nadzorczemu na podstawie art. 58 rozporządzenia 2016/679. Na podstawie

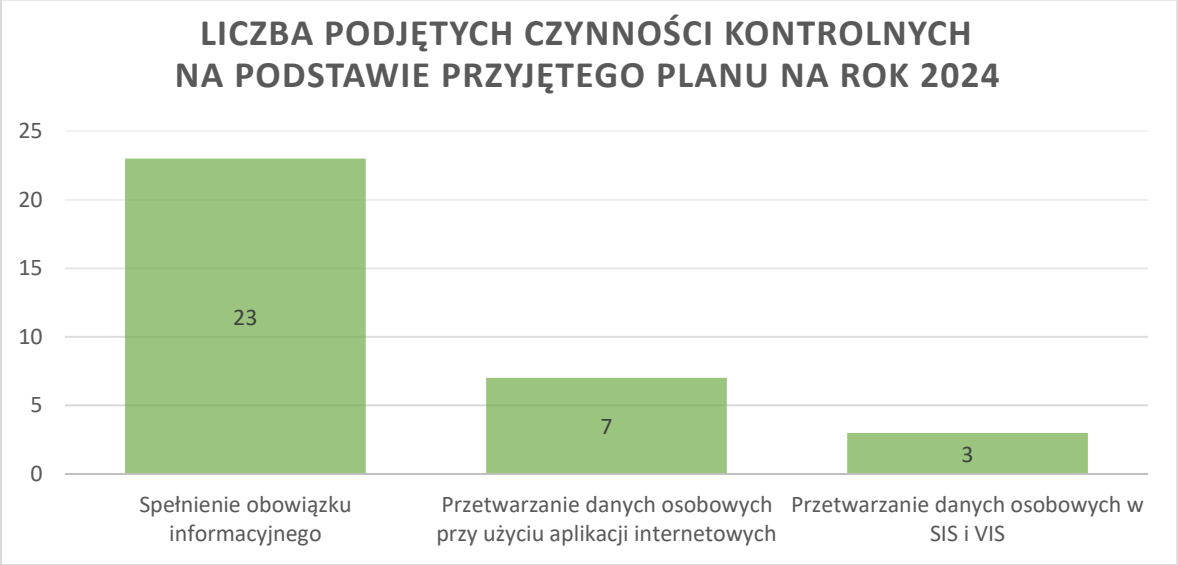
[135] Wyrok WSA z 5 marca 2024 r. w sprawie o sygn. akt II SA/Wa 1242/23.
[136] Motyw 23 i 24 RODO.

przyjętego na 2024 r. planu kontroli sektorowych, przeprowadzono **33 kontrole**, w tym trzy (3) na podstawie art. 34 ustawy z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Dwie (2) kontrole przeprowadzone zostały w związku ze zgłoszonymi Prezesowi UODO przez administratorów naruszeniami ochrony danych osobowych. Pozostałe kontrole zostały podjęte w rezultacie uzyskania przez Prezesa UODO informacji o występujących nieprawidłowościach w związku z przetwarzaniem danych osobowych.

Prezes UODO ponadto przeprowadził **20 sprawdzeń** na podstawie art. 11 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Zgodnie z planem kontroli sektorowych UODO na 2024 r. czynnościami kontrolnymi zostały objęte:

- podmioty prywatne pod kątem sprawdzenia prawidłowości spełniania obowiązku informacyjnego (23 kontrole),
- podmioty przetwarzające dane osobowe przy użyciu aplikacji internetowych (webowych) (7 kontroli),
- organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym (3 kontrole).



Wykres 6. Liczba i zakres przeprowadzonych czynności kontrolnych, podjętych na podstawie planu kontroli sektorowych UODO na 2024 r.

2.1. Aplikacje mobilne

W ramach kontynuacji rozpoczętych w 2023 r. kontroli w zakresie przetwarzania danych w aplikacjach internetowych (webowych), w okresie sprawozdawczym 2024 r. nadal prowadzone były kontrole w podmiotach oferujących użytkownikom takie aplikacje. Jedna z takich kontroli dotyczyła podmiotu reprezentującego sektor banków spółdzielczych i obejmowała prowadzenie serwisu internetowego dla klientów banku. Przeprowadzając kontrolę, dokonano m.in. weryfikacji podstawy prawnej, zakresu,

rodzaju, jak również celu przetwarzania danych. Sprawdzono sposób dopełnienia obowiązków administratora danych, wynikających z art. 13 i 14 rozporządzenia 2016/679 oraz sposobu realizacji praw osób, których dane dotyczą, wynikających z art. 15 ww. rozporządzenia. Zakresem kontroli, bazując na treści przepisów art. 32, art. 24 ust. 2 rozporządzenia 2016/679, objęto również weryfikację, czy administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych objętych ochroną. Kierując się zaś obowiązkiem wskazanym w art. 25 ww. rozporządzenia 2016/679, dokonano sprawdzenia, czy zostały wdrożone odpowiednie środki techniczne i organizacyjne, zarówno na etapie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń. Kontrola miała również na celu sprawdzenie przedmiotowej aplikacji webowej oraz związanych z nią informatycznych zasobów systemowych. Kontrola wykazała, że administrator – jako podmiot kontrolowany – w sposób właściwy dokonuje realizacji obowiązków nałożonych na niego przepisami rozporządzenia 2016/679.

2.2. System Informacyjny Schengen, Wizowy System Informacyjny

System Informacyjny Schengen stanowi zasadnicze narzędzie stosowania postanowień dorobku Schengen, który został włączony w ramy Unii Europejskiej[137]. Wskazany system jest jednym z głównych środków kompensacyjnych, które przyczyniają się do utrzymania wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii poprzez wspomaganie współpracy operacyjnej między właściwymi organami krajowymi, w szczególności strażą graniczną, policją, organami celnymi, organami imigracyjnymi oraz organami odpowiadającymi za zapobieganie przestępstwom, ich wykrywanie, prowadzenie w ich sprawie postępowań przygotowawczych lub ich ściganie albo za wykonywanie kar.

Korzystając z narzędzia, jakim jest System Informacyjny Schengen, właściwe organy powinny zapewnić poszanowanie godności i integralności osoby, której dane są przetwarzane. Unijne przepisy zapewniają pełną ochronę danych osobowych zgodnie z art. 8 Karty praw podstawowych Unii Europejskiej, a jednocześnie dążą do zapewnienia bezpiecznego otoczenia wszystkim osobom przebywającym na terytorium Unii oraz ochrony migrantów o nieuregulowanym statusie, przed wykorzystywaniem i byciem przedmiotem handlu ludźmi. Wpisy zawarte w systemie

[137] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich, Dz.U. UE L 312 z 7.12.2018, str. 1–13;
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006, Dz.U. UE L 312 z 7.12.2018 str. 14–55;
Rozporządzenie 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, Dz.U. UE L 312 z 7.12.2018, str. 56–106.

powinny zawierać wyłącznie informacje niezbędne do zidentyfikowania osób i do podjęcia działań.

System Informacyjny Schengen obejmuje system centralny oraz systemy krajowe. Państwa członkowskie powinny wprowadzić niezbędne rozwiązania techniczne, tak aby za każdym razem, gdy użytkownicy końcowi będą uprawnieni do przeprowadzenia wyszukiwania w krajowej bazie danych policji, mogli równolegle przeprowadzić wyszukiwanie w systemie z zastrzeżeniem zasad określonych w dyrektywie 2016/680 i rozporządzenia 2016/679. Dzięki temu system może działać jako główny środek kompensacyjny na obszarze bez kontroli na granicach wewnętrznych i lepiej uwzględniać transgraniczny wymiar przestępczości i mobilność przestępców.

Do przetwarzania danych osobowych przez państwa członkowskie w systemie ma zastosowanie rozporządzenie 2016/679, z wyjątkiem sytuacji, gdy takiego przetwarzania dokonują właściwe organy krajowe do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom. W takim przypadku służby te podlegają przepisom dyrektywy 2016/680 transponowanym do prawa krajowego, w szczególności monitorowaniu przez krajowe organy nadzorcze, o których mowa w dyrektywie 2016/680. W związku z tym, działając na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[138], która dokonuje wdrożenia dyrektywy 2016/680, Prezes UODO wystąpił do inspektorów ochrony danych wytypowanych **20 jednostek policji** o przeprowadzenie sprawdzenia w zakresie realizowania obowiązku informacyjnego w odniesieniu do Systemu Informacyjnego Schengen.

W związku z wystąpieniami Prezesa UODO inspektorzy ochrony danych jednostek policji sprawdzili, czy podmiotom danych w systemie udostępniane są, zgodnie ze ww. ustawą grudniową, informacje na temat nazwy, siedziby i danych kontaktowych administratora danych krajowego Systemu Informacyjnego Schengen, danych kontaktowych inspektora ochrony danych, celu, do których służą dane osobowe w systemie, prawa wniesienia do organu nadzorczego skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych oraz danych kontaktowych Prezesa UODO, oraz prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych, lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby.

Powyższe informacje powinny być udostępnione na stronie internetowej, w Biuletynie Informacji Publicznej lub w jednostce policji. Ponadto podmiotom danych, w konkretnych przypadkach, przysługuje prawo do informacji na temat:

- podstawy prawnej przetwarzania danych w Systemie Informacyjnym Schengen,
- okresu przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteriów służących określeniu tego okresu,

[138] Art. 11 ust. 1 ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

- odbiorców lub kategorii odbiorców, którym dane osobowe zostały ujawnione, w szczególności odbiorcy w państwach trzecich lub organizacjach międzynarodowych.

Zgodnie z ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, podmiotowi danych przysługuje również prawo do uzyskania na jego wniosek od administratora informacji, czy jego dane są przetwarzane, a w sytuacji ich przetwarzania prawo do informacji o celu i podstawie prawnej ich przetwarzania, kategorii danych osobowych i danych, które są przetwarzane, odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych, okresie przechowywania danych osobowych lub, gdy nie jest to możliwe, o kryteriach służących określeniu tego okresu, możliwości wniesienia wniosku do administratora o sprostowanie lub usunięcie danych osobowych, lub ograniczenie przetwarzania danych osobowych dotyczących tej osoby, prawie wniesienia do organu nadzorczego skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych oraz danych kontaktowych Prezesa UODO i źródle pochodzenia danych. Czynności nadzorcze Prezesa UODO w związku z przeprowadzonymi sprawdzeniami będą kontynuowane w 2025 r.

2.2.1. Kontrola u wojewody

Realizacja obowiązku informacyjnego była również przedmiotem kontroli[139] u jednego z wojewodów. Zakres kontroli obejmował realizację obowiązku informacyjnego w związku z dostępem do Systemu Informacyjnego Schengen (SIS) oraz Wizowego Systemu Informacyjnego (VIS). Kontrola ta obejmowała ustalenie, czy w przypadku osób ubiegających się o wizę i osób zapraszających lub odpowiedzialnych, za poniesienie kosztów utrzymania osoby ubiegającej się o wizę podczas pobytu, Wojewoda przekazuje zgodnie z rozporządzeniem w sprawie VIS[140] informacje o:

- tożsamości administratora krajowego VIS,
- celach przetwarzania danych w ramach VIS,
- kategoriach odbiorców danych, w tym o organach ścigania i o Europolu,
- fakcie, że państwa członkowskie i Europol są uprawnione do dostępu do VIS do celów ochrony porządku publicznego,
- okresie przechowywania danych,
- obowiązku uzyskania danych do celów rozpatrzenia wniosku wizowego,
- fakcie, że dane osobowe przechowywane w VIS mogą zostać przekazane państwu trzeciemu lub organizacji międzynarodowej zgodnie z art. 31 rozporządzenia w sprawie VIS,
- istniejącym prawie do żądania dostępu do danych ich dotyczących, prawie do żądania sprostowania nieprawidłowych danych, uzupełnienia niekompletnych

[139] DKN.5112.60.2024.
[140] Art. 37 ust. 1 rozporządzenia 767/2008.

danych osobowych, usunięcia danych osobowych, które były przetwarzane niezgodnie z prawem lub ograniczenia ich przetwarzania, a także o prawie do otrzymania informacji o procedurach wykonywania tych praw, w tym do otrzymania danych kontaktowych Prezesa UODO, który rozpatruje skargi dotyczące ochrony danych osobowych.

W toku kontroli weryfikowano, w jakim terminie oraz w jaki sposób i w jakiej formie obowiązek informacyjny był realizowany. W szczególności, czy powyższe informacje przekazywane są w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie pisemnej, przy użyciu jasnego i prostego języka osobie ubiegającej się o wizę w momencie pozyskiwania danych, wizerunku twarzy i danych daktyloskopijnych[141]. Kontrola miała również na celu ustalenie, czy w przypadku obywateli państwa trzeciego, których przedmioty podlegają zatrzymaniu, udzielane były informacje na temat możliwości korzystania przez nich z prawa do dostępu do danych, do sprostowania nieprawidłowych danych i usuwania danych przechowywanych niezgodnie z prawem, w ramach praw przysługującym im na mocy przepisów Schengen[142].

2.2.2. Kontrole w urzędach konsularnych RP

Czynnościami kontrolnymi[143] objęto również dwa urzędy konsularne Rzeczypospolitej Polskiej, w związku z ich 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 w ich sprawach.

Ustanowienie Wizowego Systemu Informacyjnego (VIS) stanowi jedną z podstawowych inicjatyw podejmowanych w ramach polityk Unii Europejskiej, które służą tworzeniu przestrzeni wolności, bezpieczeństwa i sprawiedliwości. VIS powinien służyć lepszej realizacji wspólnej polityki wizowej, poprawie współpracy konsularnej i procesu konsultacji pomiędzy centralnymi organami wizowymi poprzez ułatwienie wymiany pomiędzy państwami członkowskimi danych o wnioskach i o związanych z nimi decyzjach w celu uproszczenia procedury składania wniosków wizowych, handlowi wizami, ułatwienia walki z nadużyciami oraz w celu usprawnienia odpraw w przejściach granicznych na granicach zewnętrznych i na terytorium państw członkowskich. VIS powinien również pomóc w identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium państw członkowskich, lub które przestały spełniać te warunki, oraz ułatwić rozpatrywanie wniosku o azyl, a także przyczynić się do zapobiegania zagrożeniom bezpieczeństwa wewnętrznego każdego z państw członkowskich.

[141] Art. 37 ust. 2 rozporządzenia 767/2008.
[142] Art. 53 ust. 1 rozporządzenia 2018/1861.
[143] DKN.5112.25.2024, DKN.5112.57.2024.

Przetwarzanie danych zawartych w VIS powinno być proporcjonalne do zamierzonych celów i niezbędne do wykonania zadań przez właściwe organy. Korzystając z VIS, właściwe organy powinny zapewnić poszanowanie godności ludzkiej i prywatności osób, których dane są wymagane, i nie powinny dyskryminować osób ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną.

2.3. Misja Ewaluacyjna Schengen w UODO

W kwietniu 2024 r. w Urzędzie Ochrony Danych Osobowych miała miejsce misja ewaluacyjna Schengen z udziałem ekspertów wyznaczonych przez państwa członkowskie i Komisję Europejską. Wizyta odbyła się w związku z realizacją mechanizmu oceny prawidłowego wdrażania i stosowania wymogów w zakresie ochrony danych w ramach dorobku Schengen, któremu w tym roku podlegała Polska. Mechanizm ma na celu zapewnienie skutecznego, efektywnego i prawidłowego stosowania przez państwa członkowskie dorobku Schengen, przyczyniając się do utrzymania wzajemnego zaufania między państwami członkowskimi. Pozwala na szybkie stwierdzenie niedociągnięć w stosowaniu dorobku Schengen, które mogłyby zakłócać prawidłowe funkcjonowanie strefy Schengen, zapewnić szybkie ich wyeliminowanie oraz podstawy do dialogu na temat funkcjonowania strefy Schengen jako całości.

Po wizycie w Urzędzie Ochrony Danych Osobowych, a także w pozostałych właściwych organach polskich władz publicznych, zespół ekspertów sporządził sprawozdanie z oceny[144]. Dokument zawiera zalecenia dotyczące działań naprawczych mających na celu wyeliminowanie ewentualnych niedociągnięć i wprowadzenie wymaganych usprawnień zidentyfikowanych podczas oceny. Określa też priorytety realizacji tych działań. Sprawozdanie z oceny przyjmowane jest w formie aktu wykonawczego Komisji Europejskiej, która następnie przekazuje je Parlamentowi Europejskiemu i Radzie. Komisja Europejska wraz z ekspertami państw członkowskich stwierdziła, że Polska zasadniczo spełnia wymogi w zakresie ochrony danych w ramach współpracy Schengen.

2.4. Spełnienie obowiązku informacyjnego

W ramach sektorowych kontroli zgodności przetwarzania danych osobowych z przepisami rozporządzenia 2016/679 oraz ustawy o ochronie danych osobowych w 2024 r. Prezes UODO sprawdzał prawidłowość spełnienia obowiązku informacyjnego przez podmioty prywatne. Kontrole obejmowały ustalenie sposobów dopełnienia obowiązków administratora danych wynikających z art. 13 i art. 14 RODO, w tym rodzaju i zakresu przekazywanych informacji osobom, których dane dotyczą poprzez ustalenie m.in. czy są przekazywane informacje o:

- tożsamości i danych kontaktowych administratora,

[144] Podsumowanie sprawozdania Ewaluatorów Schengen dostępne jest na stronie: https://home-affairs.ec.europa.eu/document/download/aa985c3b-2c11-47e7-99e3-a7459e7c2bc8_en?filename=Schengen%20evaluation%20of%20Poland.pdf

- danych kontaktowych inspektora ochrony danych (jeżeli został powołany),
- podstawie prawnej i celach przetwarzania danych osobowych,
- w przypadku, jeżeli podstawą prawną przetwarzania danych stanowi art. 6 ust. 1 lit. f RODO, to o tym, czy administrator danych wyjaśnia prawnie uzasadniony interes realizowany przez administratora lub przez stronę trzecią,
- wykazie odbiorców danych osobowych lub ich kategorie (jeżeli przetwarzane dane osobowe są przekazywane np. do podmiotów przetwarzających dane lub innych administratorów danych),
- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia,
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – kryteria ustalania tego okresu,
- prawie żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania albo o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- prawie do cofnięcia zgody (jeżeli stanowiła ona podstawę prawną przetwarzania danych),
- prawie wniesienia skargi do organu nadzorczego,
- czy podanie danych osobowych jest wymogiem ustawowym lub umownym albo warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, z uwzględnieniem informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W przypadku pozyskiwania danych niebezpośrednio od osoby, których dane dotyczą, organ nadzorczy sprawdzał, czy osoby te są informowane o źródle pozyskania danych oraz kategorii pozyskanych danych. Przedmiotem kontroli było także ustalenie, w jakim terminie oraz w jakiej formie obowiązek informacyjny jest realizowany, oraz czy w przypadku zmiany celu przetwarzania danych, osoby, których dane dotyczą, informowane są o zmianie celu przetwarzania ich danych osobowych.

Kompleksowa ocena prawidłowości realizacji obowiązku informacyjnego zostanie dokonana w 2025 r. na podstawie wyników wszystkich kontroli przeprowadzanych w tym zakresie.

2.5. Kontrole w wyniku zgłoszonego naruszenia

W 2024 r. Prezes UODO przeprowadził **2 postępowania kontrolne w związku ze zgłoszonym przez administratora naruszeniem ochrony danych.** Kontrole te obejmowały w szczególności sprawdzenie realizacji obowiązków wynikających z rozporządzenia 2016/679, m.in. oceny stosowanych przez administratorów środków bezpieczeństwa, podstaw prawnych przetwarzania danych osobowych, sposobu udostępniania danych osobowych oraz realizacja obowiązku informacyjnego.

2.6. Decyzje administracyjne w postępowaniach kontrolnych

W wyniku nieprawidłowości stwierdzonych w trakcie przeprowadzonych kontroli w 2024 r. Prezes UODO wszczął z urzędu 14 postępowań administracyjnych dotyczących przetwarzania danych osobowych. Po ich zakończeniu wydał 7 decyzji.

Jedna z decyzji[145] została wydana w związku z naruszeniem przez **bank** przepisu art. 38 ust. 3 rozporządzenia 2016/679, polegającego na niezapewnieniu przez bank, jako administratora, by inspektor ochrony danych podlegał bezpośrednio najwyższemu kierownictwu administratora oraz nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Za powyższe naruszenie Prezes UODO nałożył na bank administracyjną karę pieniężną. Postępowanie w sprawie zostało wszczęte na skutek przeprowadzonej przez organ nadzorczy kontroli. Zakresem kontroli objęto przetwarzanie danych osobowych klientów i potencjalnych klientów w związku z ich profilowaniem, poprzez ustalenie, między innymi: zakresu i rodzaju przetwarzanych danych osobowych, celu i czasu przetwarzania danych osobowych, czy zostały opracowane procedury dotyczące profilowania, czy w celu oceny zdolności kredytowej i analizy ryzyka kredytowego podejmuje decyzje oparte na zautomatyzowanym przetwarzaniu, w tym profilowaniu, czy wyznaczony został inspektor ochrony danych, czy administrator prowadzi rejestr czynności przetwarzania danych osobowych i czy uwzględnione są w nim czynności polegające na profilowaniu danych osobowych, czy dokonywana jest ocena skutków dla ochrony danych osobowych, w szczególności w odniesieniu do czynności przetwarzania danych polegających na ich profilowaniu, zasad działania systemów informatycznych wykorzystywanych do przetwarzania danych osobowych, a w szczególności ich profilowania.

W decyzji tej stwierdzone zostało także naruszenie przez bank przepisów art. 30 ust. 1 rozporządzenia 2016/679, polegające na nieuwzględnieniu profilowania w opisie procesów (czynności) przetwarzania danych zawartych w rejestrze czynności przetwarzania danych, oraz art. 35 ust. 1 i ust. 7 rozporządzenia 2016/679, polegające na niedokonaniu oceny skutków dla ochrony danych osobowych w odniesieniu do czynności przetwarzania danych polegających na ich profilowaniu. Za naruszenie ww. przepisów, Prezes UODO nałożył na bank drugą administracyjną karę pieniężną. Sprawa jest jeszcze wciąż przedmiotem postępowania przed Wojewódzkim Sądem Administracyjnym w Warszawie, na skutek skargi na decyzję Prezesa UODO, złożonej przez bank.

[145] DKN.5112.14.2022.

Kolejna decyzja[146] Prezesa UODO dotyczyła jednej z **placówek medycznych**, w której zostało stwierdzone naruszenie przepisów art. 5 ust. 1 lit. f i ust. 2, art. 24 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 polegające na niewdrożeniu: odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą, na podstawie przeprowadzonej analizy ryzyka uwzględniającej stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Niewdrożenie odpowiednich środków technicznych i organizacyjnych polegało również na niezapewnieniu regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia.

Prezes UODO nałożył na placówkę medyczną administracyjną karę pieniężną. Wydał tę decyzję po wszczęciu z urzędu postępowania administracyjnego, w rezultacie uprzedniego przeprowadzenia czynności wyjaśniających oraz kontroli w spółce. Działania te zostały zainicjowane w wyniku zgłoszenia przez spółkę Prezesowi UODO naruszenia ochrony danych osobowych, polegającego na naruszeniu poufności i dostępności przetwarzanych przez spółkę danych osobowych. Sprawa jest przedmiotem postępowania przed Wojewódzkim Sądem Administracyjnym w Warszawie na skutek skargi złożonej przez placówkę medyczną. Wyrokiem z 10 kwietnia 2025 r. Wojewódzki Sąd Administracyjny w Warszawie oddalił w całości skargę na decyzję, przychylając się do uzasadnienia organu nadzorczego. Administrator wniósł skargę kasacyjną od wyroku.

Kolejna decyzja[147] Prezesa UODO wydana po przeprowadzeniu czynności kontrolnych dotyczyła udzielenia upomnienia innej **placówce medycznej** za naruszenie przepisów art. 30 ust. 1 lit. b oraz lit. f rozporządzenia 2016/679. Zakresem kontroli objęto przetwarzanie przez administratora danych osobowych za pomocą środków technicznych umożliwiających rejestrację obrazu w placówkach medycznych (gabinetach stomatologicznych). W toku kontroli ustalono, że w prowadzonym rejestrze czynności przetwarzania danych nie wskazano czynności wykonywanej na danych osobowych w związku z prowadzonym monitoringiem, nie określono też celu przetwarzania danych w zakresie wizerunku osób oraz nie sprecyzowano planowanego terminu usunięcia danych osób monitorowanych. Pomimo że administrator usunął stwierdzone w toku kontroli nieprawidłowości oraz współpracował z organem nadzorczym, to nie ulega wątpliwości, że w terminie przeprowadzenia kontroli miały miejsce nieprawidłowości stanowiące naruszenie art. 30 ust. 1 lit. b oraz lit. f rozporządzenia 2016/679. W ocenie organu nadzorczego nie można było uznać, że działania przedsięwzięte przez administratora po przeprowadzeniu kontroli uchylają

[146] DKN.5112.35.2021.
[147] DKN.5112.17.2023.

niekorzystne dla niego skutki, w postaci przewidzianych w przepisach rozporządzenia 2016/679 sankcji za nieprzestrzeganie przepisów.

W 2024 r. Prezes Urzędu wydał decyzję[148] upominającą i nakazującą dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 wobec jednego z **domów pomocy społecznej**. Decyzja została wydana w wyniku przeprowadzonej kontroli, której celem było ustalenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Kontrolą objęto sposób wypełnienia obowiązków administratora w zakresie realizacji praw osób, których dane dotyczą oraz wdrożenia środków technicznych i organizacyjnych, zapewniających przetwarzanie danych zgodne z rozporządzeniem 2016/679. W ramach czynności kontrolnych stwierdzono nieprawidłowości w realizacji obowiązków administratora skutkujące naruszeniem przepisów rozporządzenia 2016/679 dotyczącym braku przejrzystości w spełnianiu obowiązku informacyjnego w zakresie wskazania odbiorców danych, a w konsekwencji nieprawidłowości w prowadzeniu dokumentacji dotyczącej przetwarzania danych obejmujące brak wskazania odbiorców danych w rejestrze czynności przetwarzania danych dla prowadzonych czynności przetwarzania, naruszenie retencji przetwarzanych danych przez przechowywanie danych ponad okresy wskazane w przepisach prawa lub wynikające z celu przetwarzania oraz nieprawidłowości dotyczące stosowanych środków bezpieczeństwa przetwarzania danych z uwagi na brak procedur lub instrukcji dokonywania okresowych przeglądów przyjętych środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania ich skuteczności dla bezpieczeństwa przetwarzania.

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

Jedną z decyzji[149], wydaną po uchylającym wcześniej decyzję Prezesa UODO wyroku Naczelnego Sądu Administracyjnego, było orzeczenie, w którym organ stwierdził naruszenie przez **Morele.net sp. z o.o**. przepisów art. 24 ust. 1, 25 ust. 1, art. 32 ust. 1 lit. b i lit. d oraz art. 32 ust. 2 rozporządzenia 2016/679. Naruszenie polegało na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych, braku regularnego testowania, mierzenia i oceniania skuteczności tych środków, co skutkowało naruszeniem zasady integralności i poufności oraz zasady rozliczalności. Prezes UODO nałożył ponadto administracyjną karę pieniężną.

Wyrokiem z 16 września 2024 r. Wojewódzki Sąd Administracyjny w Warszawie oddalił w całości skargę na decyzję, przychylając się do uzasadnienia organu nadzorczego. Sąd podniósł, że skoro administrator nie przeprowadził analizy ryzyka wiążącego się z przetwarzaniem danych osobowych w sposób sformalizowany, a więc udokumentowany lub w inny sposób utrwalony oraz ujęty w postaci ściśle określonych,

[148] DKN.5112.11.2023.
[149] ZSPR.421.2.2019.

precyzyjnych formuł wyjaśniających i porządkujących przebieg tego procesu, to nie był zdolny wykazać, że wdrożone przez niego środki techniczne i organizacyjne zapewniają zgodność przetwarzania z rozporządzeniem 2016/679. Administrator wniósł skargę kasacyjną od wyroku.

Kolejną decyzją[150], która została podtrzymana zarówno przez Wojewódzki Sąd Administracyjny, jak i Naczelny Sąd Administracyjny, była decyzja nakładająca administracyjną karę pieniężną na **ClickQuickNow sp. z o.o.,** wskazująca, że w procesie wycofania zgody administrator nie uwzględnił zasady, zgodnie z którą wycofanie zgody powinno być równie łatwe, jak jej wyrażenie. Administrator natomiast działał ze skutkiem odwrotnym, gdyż dla wycofania zgody zastosował skomplikowane rozwiązania organizacyjne i techniczne. Ponadto administrator przetwarzał bez podstawy prawnej dane osób, które nie były jego klientami, a od których otrzymywał żądania zaprzestania przetwarzania danych osobowych. Naczelny Sąd Administracyjny, podobnie jak wcześniej Wojewódzki Sąd Administracyjny w Warszawie, podzielił stanowisko zaprezentowane w decyzji Prezesa UODO oraz uznał argumenty organu nadzorczego zarówno, co do słuszności nałożenia kary, jak również co do jej wysokości.

Oceniając ostateczne rozstrzygnięcie w niniejszej sprawie, należy zauważyć, że zgodę na przetwarzanie danych osobowych definiuje art. 4 pkt 11 rozporządzenia 2016/679, zgodnie z którym „zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych". Odwołanie zgody przysługuje osobie, której dane dotyczą, w każdym czasie, co oznacza, że osoba taka ma prawo w dowolnym momencie wycofać wyrażoną zgodę. Wycofanie zgody musi być tak samo łatwe, jak i jej wyrażenie, a proces wycofania zgody w żadnym przypadku nie powinien być skomplikowany.

W roku sprawozdawczym Wojewódzki Sąd Administracyjny w Warszawie oddalił także skargę **wspólników spółki cywilnej** na decyzję Prezesa UODO[151]. Przedmiotowa decyzja została wydana po przeprowadzeniu kontroli u wspólników spółki cywilnej, celem zbadania zgodności przetwarzania przez nich danych z przepisami o ochronie danych osobowych. Zakresem kontroli objęto przetwarzanie przez wspólników danych osobowych klientów i potencjalnych klientów. W toku kontroli stwierdzono naruszenia przepisów o ochronie danych osobowych, w rezultacie zostało wszczęte postępowanie. W decyzji Prezes UODO stwierdził naruszenie przez wspólników spółki, a także byłego wspólnika, przepisów: art. 6 ust. 1 rozporządzenia 2016/679 polegające na przetwarzaniu danych osobowych swoich potencjalnych klientów bez podstawy prawnej, a w szczególności bez uzyskania ich zgody na przetwarzanie, o której mowa w art. 6 ust. 1 lit. a rozporządzenia 2016/679, z jednoczesnym naruszeniem zasady przetwarzania danych osobowych zgodnie z prawem, o której mowa w art. 5 ust. 1 lit. a rozporządzenia 2016/679, oraz art. 9 ust.

[150] ZSPR.421.7.2019.
[151] DKN.5112.5.2021.

1 w związku z art. 9 ust. 2 rozporządzenia 2016/679 polegające na przetwarzaniu danych dotyczących zdrowia swoich potencjalnych klientów bez podstawy prawnej, a w szczególności bez uzyskania ich wyraźnej zgody na przetwarzanie, o której mowa w art. 9 ust. 2 lit. a rozporządzenia 2016/679, co stanowiło również naruszenie zasady przetwarzania danych osobowych zgodnie z prawem, o której mowa w art. 5 ust. 1 lit. a rozporządzenia 2016/679. W rezultacie Prezes UODO w decyzji nakazał wspólnikom dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679, poprzez zaprzestanie przetwarzania danych osobowych potencjalnych klientów bez podstawy prawnej, tj. bez uzyskania zgody na przetwarzanie ich danych osobowych, o której mowa w art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a rozporządzenia 2016/679. Prezes UODO ww. decyzją nałożył na wspólników oraz byłego wspólnika spółki cywilnej, odpowiadających solidarnie, za naruszenie ww. przepisów, administracyjną karę pieniężną.

Obecnie, po wydaniu przez Wojewódzki Sąd Administracyjny w Warszawie wyroku oddalającego skargę wspólników, postępowanie sądowe w sprawie jest kontynuowane przed Naczelnym Sądem Administracyjnym, w rezultacie skargi kasacyjnej strony.

3. 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 rozporządzenia 2016/679, 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 takiego naruszenia bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po jego stwierdzeniu. 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[152].

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 rozporządzeniu 2016/679, ale także podanie dodatkowych danych umożliwiających organowi nadzorczemu dokonanie analizy naruszenia pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Dotychczasowa praktyka wskazuje, że w przypadku administratorów zgłaszających naruszenia na zaproponowanym formularzu ryzyko przekazania niewystarczających informacji jest mniejsze, niż w przypadku naruszeń przesyłanych przez administratora w innej formie.

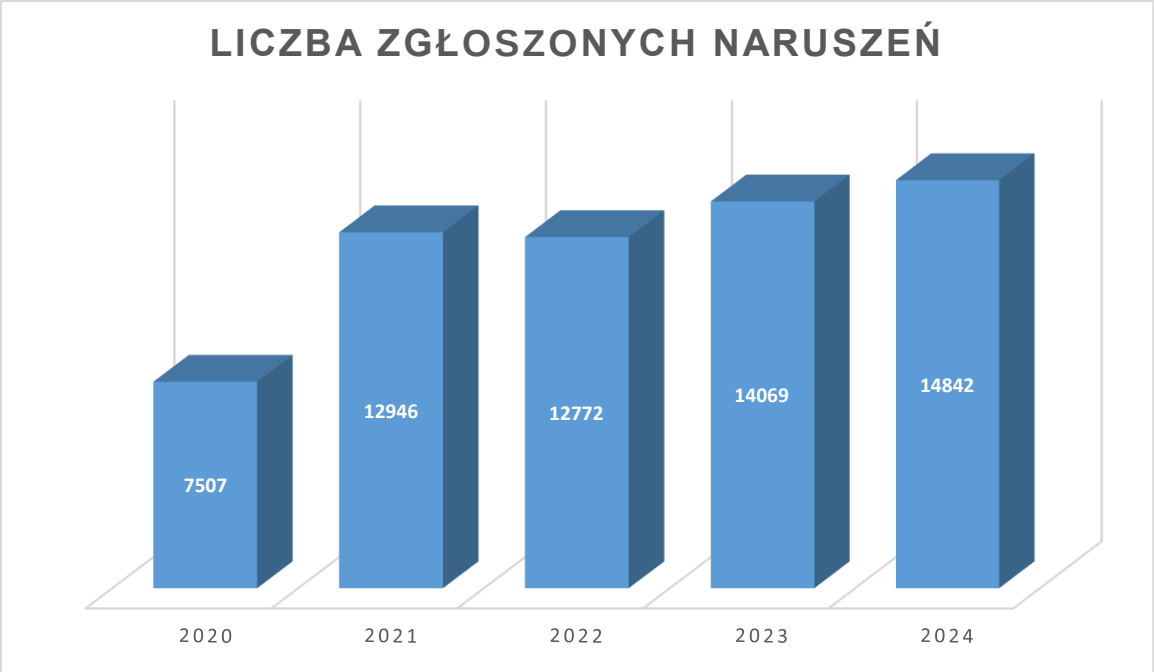
Zgłaszanie naruszeń przez administratorów stanowi skuteczne narzędzie przyczyniające się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych. Zgłaszając naruszenie organowi nadzorczemu, administratorzy informują Prezesa UODO, czy – w ich ocenie – wystąpiło wysokie ryzyko naruszenia praw 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 lit. b rozporządzenia 2016/679. 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 tych objętych zgłoszeniem.

3.1. Statystyka zgłaszanych naruszeń ochrony danych osobowych

W 2024 r. do Urzędu Ochrony Danych Osobowych wpłynęło **14 842 zgłoszenia naruszeń ochrony danych osobowych.**

[152] Rozporządzenie 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 Dz.U.UE.L.2013.173.2



Wykres 7. Liczba naruszeń ochrony danych osobowych, które wpłynęły do UODO w latach 2020–2024.

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

1) **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 zatrudnionego przez administratora danych, a naruszenia miały z reguły charakter jednorazowego incydentu. Zdarzały się jednak naruszenia będące konsekwencją błędów już na etapie gromadzenia danych, 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.

2) **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.

3) 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. Dotyczyło to również udostępniania danych osobowych, w tym wizerunku dzieci, w mediach społecznościowych. Mimo że często udostępniane były w dobrej wierze przez różnego rodzaju placówki czy gminne ośrodki, ich konsekwencją było zagrożenie bezpieczeństwa czy negatywny wpływ na samopoczucie osób małoletnich, które powinny być objęte szczególną ochroną w związku z brakiem świadomości ryzyka, konsekwencji i praw przysługujących im w związku z przetwarzaniem danych osobowych.

4) 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.

5) Nieuprawniony dostęp do baz danych

Naruszenia te 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.

6) Zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej

Były to jednorazowe incydenty, będące 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.

7) Zagubienie lub kradzież nośnika danych

Dochodziło do nich wskutek 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.

8) 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, będącego w strukturze NASK – Państwowego Instytutu Badawczego.

9) 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 dla użytkownika. 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).

3.2. 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 oraz lit. 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 **2036 pisemnych wezwań do złożenia wyjaśnień.** 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 2024 r. Prezes UODO skierował **736 wystąpień (w 2023 r. skierowano 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.

3.3. Wystąpienia o charakterze generalnym

Dodatkowo Prezes UODO skierował do organów państwowych oraz do podmiotu niepublicznego realizującego zadania publiczne **3 wystąpienia** zmierzające do zapewnienia skutecznej ochrony danych osobowych.

W związku z powziętymi przez organ nadzorczy informacjami wskazującymi na występowanie naruszeń ochrony danych osobowych żołnierzy Sił Zbrojnych Rzeczypospolitej Polskiej Prezes UODO skierował pismo do **Ministra Obrony Narodowej**[153] z prośbą o ustalenie oraz przeprowadzenie analizy, jakie dokładnie rozwiązania w obszarze bezpieczeństwa danych osobowych stosowane są przez Siły Zbrojne Rzeczypospolitej Polskiej, w szczególności czy i w jaki sposób przyjęte rozwiązania minimalizują ryzyko naruszenia praw lub wolności żołnierzy w kontekście zdarzeń, które zainicjowały ww. wystąpienie. W odpowiedzi Prezes UODO uzyskał informacje dotyczące przyjętych w resorcie obrony narodowej środków i regulacji służących do zapewnienia bezpieczeństwa przetwarzanych danych osobowych. Jednocześnie Minister Obrony Narodowej poinformował, że w związku z wyłączeniami w dziedzinie obronności stosowania ustawy o ochronie danych osobowych oraz rozporządzenia 2016/679, planuje podjąć kroki celem zmiany ustawy o obronie Ojczyzny poprzez dodanie do niej postanowień przewidujących niezbędne środki ochrony praw i wolności osób, których dane dotyczą.

Kolejne wystąpienie w roku 2024 zostało skierowane do **Komendanta Głównego Policji**[154] z prośbą o podjęcie działań zmierzających do zapewnienia skutecznej ochrony danych osobowych przetwarzanych za pośrednictwem Krajowego Systemu Informacyjnego Policji. W wystąpieniu Prezes UODO zwrócił uwagę na wykorzystywanie przez funkcjonariuszy policji dostępu do ww. systemu w sposób niezgodny z prawem oraz poruszył kwestię utraty przez funkcjonariuszy bloczków mandatowych i notatników służbowych zawierających dane osobowe. Komendant Główny Policji w odpowiedzi wskazał, że problematyka ww. zdarzeń jest mu znana i dokładane są wszelkie starania mające na celu zapewnienie odpowiedniego poziomu wiedzy policjantów i pracowników policji w obszarze ochrony danych osobowych, a zastosowane środki techniczne i organizacyjne oraz wdrożone procedury podnoszą bezpieczeństwo danych osobowych przetwarzanych w Krajowym Systemie Informacyjnym Policji. Jednocześnie w odpowiedzi Komendant Główny Policji

[153] DKN.5101.70.2024.
[154] DKN.5101.66.2024.

poinformował, że zaplanowane zostało zastąpienie notatników służbowych ich elektronicznym odpowiednikiem.

W związku z licznymi przypadkami zagubienia przesyłek przez operatora pocztowego Prezes UODO zwrócił się do **Prezesa Zarządu Poczty Polskiej S.A.**[155] z prośbą o podjęcie działań mających na celu wypracowania rozwiązań w zakresie ograniczenia tego typu zdarzeń oraz wzmocnienia współpracy z nadawcami przesyłek. Występujące liczne przypadki utraty przesyłek lub ich doręczania niewłaściwym odbiorcom przez operatora pocztowego stanowią poważny problem dla administratorów w kontekście obowiązków wynikających z rozporządzenia 2016/679. W wystąpieniu Prezes UODO zwrócił się o informacje, czy Poczta Polska S.A. monitoruje efektywność wdrożonych środków służących wzmocnieniu bezpieczeństwa przesyłek oraz czy wdrożyła lub planuje wdrożyć dodatkowe środki bezpieczeństwa w tym zakresie. W odpowiedzi operator pocztowy poinformował o wdrożeniu licznych działań mających na celu wyeliminowanie lub ograniczenie skali zdarzeń polegających na zagubieniu przesyłek lub ich niewłaściwym doręczeniu. Prezes UODO ocenił pozytywnie kierunek działań podejmowanych przez operatora pocztowego, podkreślając, że Poczta Polska S.A. ma szczególne obowiązki w zakresie zapewnienia bezpieczeństwa danym osobowym znajdującym się w przesyłkach doręczanych przez operatora.

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 wskazanie terminu dokonanego zgłoszenia oraz wyjaśnienia przyczyn opóźnienia powiadomienia organu nadzorczego o naruszeniu,
- sposób realizacji obowiązku zawiadomienia osób, których dane dotyczą,
- wskazanie przez administratorów kategorii i liczby osób oraz danych objętych naruszeniem,
- nakładanie na inspektorów ochrony danych zadań powodujących konflikt interesów.

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 oraz lit. e RODO pozytywnie wpływała na ochronę danych osobowych. Znacznie bowiem skracała proces

[155] DKN.5101.47.2024.

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.

3.4. Postępowania administracyjne

Zgłoszenia naruszenia ochrony danych osobowych stały się dla organu nadzorczego impulsem do dokonywania oceny realizacji przez administratorów i podmioty przetwarzające spoczywających na nich obowiązków wynikających z rozporządzenia 2016/679, dotyczących właściwego zabezpieczenia danych oraz organizacji systemu ochrony danych osobowych.

W 2024 r. Prezes UODO **wszczął z urzędu 18 postępowań administracyjnych** w sprawie naruszenia przepisów o ochronie danych osobowych. W niektórych przypadkach podjęta została decyzja o przeprowadzeniu u administratora 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 oraz lit. d rozporządzenia 2016/679;

c) doboru zabezpieczeń systemu informatycznego oraz testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych objętych naruszeniem, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia;

d) sposobu realizacji przez podmiot przetwarzający postanowień umowy powierzenia przetwarzania uwzględniającej kryteria zawarte w art. 28 ust. 3 rozporządzenia 2016/679, w szczególności dotyczące spełniania obowiązku

przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, podejmowania wszelkich środków wymaganych na mocy art. 32 rozporządzenia 2016/679 oraz – po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych – usuwania lub zwracania administratorowi wszelkich danych osobowych i usuwania wszelkich ich istniejących kopii;

e) treści zawiadomienia osób, których dane dotyczą, o naruszeniu ich danych osobowych pod kątem spełniania wymogów określonych w art. 34 ust. 2 rozporządzenia 2016/679.

3.5. Zawiadomienia o popełnieniu przestępstwa

W analizowanym 2024 r. Prezes UODO złożył zawiadomienie o możliwości popełnienia przestępstwa[156]. Sprawa związana jest z wyciekiem z chińskiej platformy sprzedażowej Pandabuy danych osobowych ponad miliona klientów, w tym kilkudziesięciu tysięcy z Polski. Zawiadomienie złożone do Prokuratury Rejonowej Warszawa Śródmieście-Północ dotyczyło jednak typu czynu zabronionego z art. 107 ust. 1 ustawy o ochronie danych osobowych, czyli bezprawności przetwarzania danych osobowych przez osoby, które wykorzystując dane osobowe klientów platformy z wycieku w postaci imion i nazwisk oraz adresów, sporządziły interaktywną mapę Polski. Prokuratura początkowo odmówiła wszczęcia dochodzenia, wskazując na brak danych dostatecznie uzasadniających popełnienie przestępstwa. Jednak na skutek złożonego przez Prezesa UODO zażalenia, Sąd Rejonowy dla Warszawy – Śródmieścia uchylił postanowienie prokuratury, a sprawę przekazał celem przeprowadzenia postępowania.

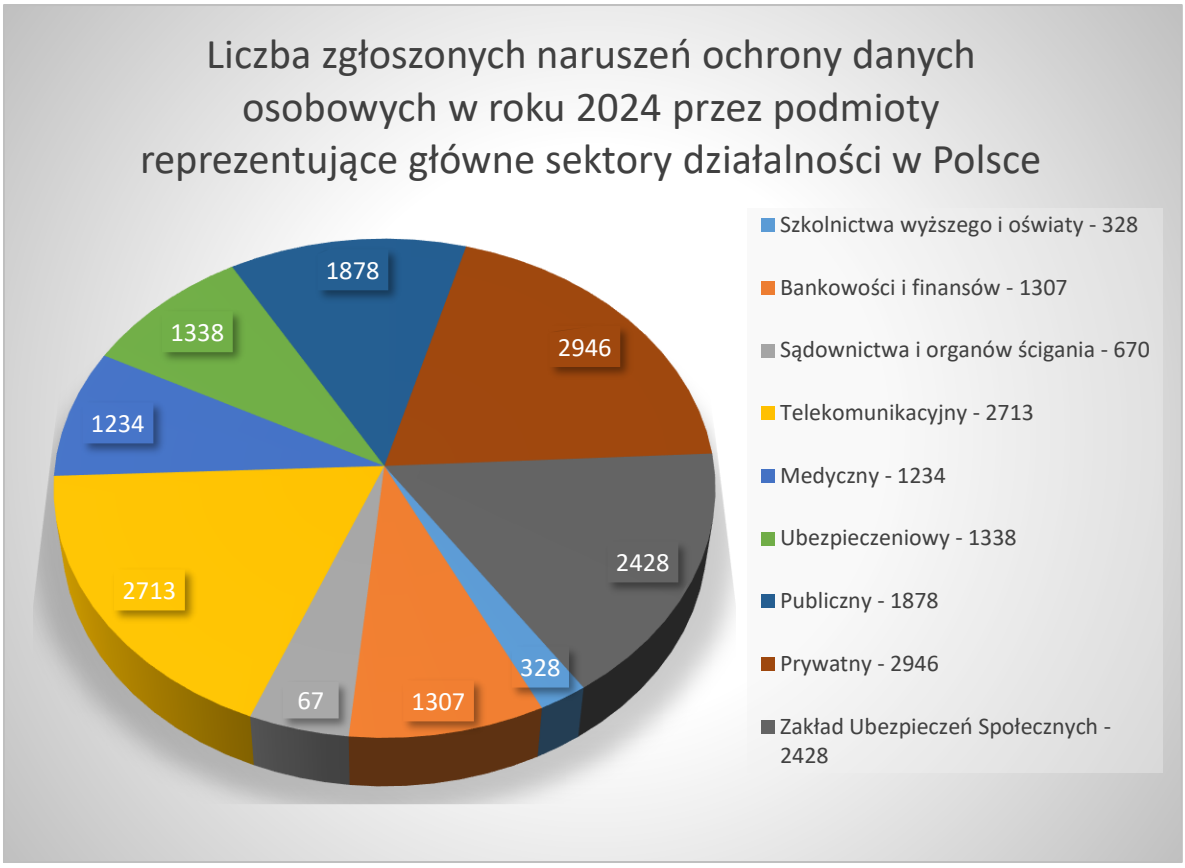
3.6. Decyzje administracyjne

W wyniku prowadzonych przez Prezesa UODO postępowań administracyjnych, które zostały zakończone w 2024 r., wydano **20 decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych (w 2023 r. wydanych zostało 36 takich decyzji).** W 3 decyzjach Prezes UODO udzielił upomnienia administratorowi danych. W przypadku **17 decyzji administracyjnych w związku ze stwierdzeniem naruszenia przepisów o ochronie danych osobowych** Prezes UODO, po przeprowadzeniu postępowań administracyjnych, zdecydował się nałożyć na administratorów danych administracyjne kary pieniężne, w tym w **12 przypadkach** dodatkowo nakazał dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 lub zawiadomienie o naruszeniu osób, których dane dotyczyły, w celu przekazania im informacji wymaganych zgodnie z art. 34 ust. 2 rozporządzenia 2016/679.

3 decyzje Prezesa UODO, wydane po przeprowadzeniu postępowań administracyjnych w związku ze stwierdzeniem naruszenia przepisów o ochronie danych osobowych, zostały zaskarżone do Wojewódzkiego Sądu Administracyjnego w Warszawie.

[156] DKN.5101.151.2024.

Wojewódzki Sąd Administracyjny w Warszawie utrzymał w mocy **6 decyzji, uchylił zaś 3 decyzje Prezesa UODO,** wydane w okresie sprawozdawczym oraz w poprzednich latach po przeprowadzeniu postępowań administracyjnych w związku ze stwierdzeniem naruszenia przepisów o ochronie danych osobowych.



Wykres 8. Liczba zgłoszonych naruszeń ochrony danych osobowych w 2024 r.

3.7. Administracyjne kary pieniężne w związku z naruszeniem

Postępowanie administracyjne prowadzone wobec jednostki **sektora medycznego** zakończone zostało wydaniem decyzji[157] nakładającej na szpital administracyjną karę pieniężną oraz nakazującej zawiadomienie osoby, której została naruszona ochrona danych.

Czynności wyjaśniające zostały przeprowadzone w związku z otrzymaniem z Biura Rzecznika Praw Pacjenta pisma informującego o możliwości wystąpienia naruszenia ochrony danych w wyniku wydania pacjentce oddziału położniczo-ginekologicznego dokumentacji medycznej innej pacjentki. Dokumentacja ta zawierała imię i nazwisko, datę urodzenia, numer PESEL, a także dane dotyczące zdrowia. Szpital dokonał zgłoszenia naruszenia ochrony danych osobowych dopiero po skierowaniu do niego wezwania oraz wszczęciu postępowania administracyjnego. Ostatecznie Prezes UODO stwierdził naruszenie przepisów art. 33 ust. 1 i art. 34 ust.

[157] DKN.5131.6.2024.

1 i 2 rozporządzenia 2016/679 w związku z niezgłoszeniem naruszenia Prezesowi UODO w ciągu 72 godzin od stwierdzenia oraz nieprawidłowym zawiadomieniem osoby, której naruszenie dotyczyło. Nie zawierało ono bowiem opisu środków proponowanych w celu zminimalizowania negatywnych skutków naruszenia.

Decyzja została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie i oczekuje na rozstrzygnięcie.

W kolejnej decyzji[158] Prezes UODO stwierdził naruszenie polegające na udostępnieniu przez **przedsiębiorcę** nieuprawnionemu odbiorcy bazy danych zawierającej dane kilkudziesięciu osób. Do incydentu doszło wskutek wysyłki wiadomości e-mail na niewłaściwy adres. Przeanalizowanie danych, których ochrony dotyczyło zaistniałe naruszenie, pozwoliło stwierdzić, że nieuprawniony odbiorca otrzymał m.in. numery PESEL trzech osób. Prezes UODO nakazał w tej decyzji prawidłowe zawiadomienie tych osób i podkreślił, że w sytuacji udostępnienia nieuprawnionemu odbiorcy bazy danych osobowych, spośród których część można było odnaleźć np. w Internecie, nie zwalnia administratora z obowiązku powiadomienia ich o naruszeniu. Niespełnienie tego obowiązku skutkowało nałożeniem na przedsiębiorcę administracyjnej kary pieniężnej. W sprawie tej Wojewódzki Sąd Administracyjny wydał postanowienie o odrzuceniu skargi.

Następna decyzja[159] dotyczyła **banku.** Naruszenie ochrony danych osobowych wynikało z kradzieży przesyłki zawierającej dokumentację bankową w czasie jej transportu w firmie kurierskiej. Otwarta przesyłka została porzucona w miejscu ogólnodostępnym, w wyniku czego z dokumentacją zapoznała się osoba nieuprawniona. Działania banku – jako 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 (organ powziął informację o jego wystąpieniu na podstawie informacji zamieszczonych na jednej ze stron internetowych) oraz brak zawiadomienia osób, których dane znajdowały się w skradzionej i porzuconej przesyłce. Wszystkie te uchybienia stanowiły łącznie o naruszeniu przez administratora przepisów art. 33 ust. 1 i art. 34 ust. 1 rozporządzenia 2016/679. Prezes UODO uznał, wbrew twierdzeniom banku, że administrator nie wykazał, aby osoba, która odnalazła przesyłkę, mogła zostać uznana za tzw. zaufanego odbiorcę. Była to bowiem osoba trzecia, która zupełnie przypadkowo odnalazła przesyłkę. Biorąc pod uwagę zakres ujawnionych danych, stwierdzono, że w związku z przedmiotowym naruszeniem wystąpiło wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, co w konsekwencji wymagało dokonania zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz powiadomienia o nim osób, których dane dotyczą.

Prezes UODO nałożył na bank administracyjną karę pieniężną, a także nakazał zawiadomienie, w terminie 3 dni od dnia doręczenia niniejszej decyzji, osób, których ochrona danych została naruszona na skutek zdarzenia, i przekazania im

[158] DKN.5131.53.2021.
[159] DKN.5131.59.2022.

wymaganych informacji i środków – zgodnie z art. 34 ust. 2 rozporządzenia 2016/679. Administrator wniósł skargę do Wojewódzkiego Sądu Administracyjnego na tę decyzję oraz złożył wniosek o wstrzymanie wykonania decyzji w punkcie nakazującym administratorowi zawiadomienie osób, których ochrona danych została naruszona. Wojewódzki Sąd Administracyjny po rozpatrzeniu wniosku wydał postanowienie odmawiające wstrzymania wykonania przedmiotowej decyzji. Wskutek zażalenia na powyższe Naczelny Sąd Administracyjny przychylił się do wniosku administratora i wstrzymał wykonanie decyzji w punkcie nakazującym administratorowi zawiadomienie osób, których ochrona danych została naruszona.

Kolejny przykład naruszenia ochrony danych osobowych polegał na udostępnieniu na profilu **stowarzyszenia**, na jednym z portali, listy uczestników amatorskich zawodów sportowych. Lista zawierała nadmiarowe dane osobowe osób biorących udział w tych zawodach i dostępna była dla osób, które pobrały ww. listę z profilu stowarzyszenia na portalu internetowym. Stowarzyszenie miało prawo opublikować dane osobowe uczestników zawodów, jednakże zakres udostępnionych danych osobowych powinien być adekwatny do celu takiej publikacji. W wyjaśnieniach przekazanych organowi nadzorczemu stowarzyszenie przyznało, że w następstwie pomyłki wolontariusza doszło do udostępnienia danych osobowych uczestników zawodów sportowych w nadmiarowym zakresie. Prezes UODO po przeprowadzeniu postępowania administracyjnego nałożył administracyjną karę pieniężną. Kara została uiszczona[160].

Orzeczeniem podkreślającym rolę właściwej identyfikacji zdarzeń oraz realizacji obowiązków przez administratora wynikających z przepisów rozporządzenia 2016/679 była decyzja[161] nakładająca administracyjną karę pieniężną na **bank** za naruszenie przepisu art. 33 ust. 1 rozporządzenia 2016/679, tj. niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Naruszenie ochrony danych osobowych polegało na wysłaniu – w wyniku błędu pracownika banku – przesyłki zawierającej umowę i harmonogram spłaty kredytu do innego klienta banku. Administrator zarejestrował incydent bezpieczeństwa, jednak nie dokonał zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego. Administrator zgłosił naruszenie dopiero po wystąpieniu Prezesa UODO w związku z prowadzonym postępowaniem w sprawie skargi klienta banku – po upływie prawie półtora roku od jego stwierdzenia. Administracyjna kara pieniężna została zapłacona.

Inny **bank** dopuścił się naruszenia przepisów art. 34 ust. 1 i 2 rozporządzenia 2016/679, polegającego na niezawiadomieniu o naruszeniu ochrony danych osobowych bez zbędnej zwłoki osób, których dane dotyczą. Skutkiem tego Prezes UODO nałożył na ten bank administracyjną karę pieniężną oraz nakazał zawiadomienie osób, których dane osobowe zostały ujawnione nieuprawnionemu

[160] DKN.5131.58.2022.
[161] DKN.5131.28.2023.

odbiorcy. W orzeczeniu[162] organ nadzorczy wskazał, że możliwość ujawnienia dużej ilości danych tworzy dla osób, których one dotyczą, ogromne ryzyko. Ponieważ nie zostały o problemie powiadomione, nie mogły przeciwdziałać ewentualnym negatywnym skutkom naruszenia. Bank błędnie rozumował, skupiając się tylko na tym, kto miał dostęp do ujawnionych danych, i bazował na zapewnieniach tych osób, że nic nagannego się nie stało. Przy analizowaniu takiej sytuacji należy jednak zawsze brać pod uwagę prawa osób, których naruszenie dotyczyło oraz to, że przestrzeganie innych tajemnic prawnie chronionych nie zwalnia ze stosowania rozporządzenia 2016/679.

Prezes UODO, stwierdzając w kolejnej decyzji[163] naruszenie przepisów ochrony danych osobowych (art. 5 ust. 1 lit. f, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2, art. 33 ust. 1 i 3 oraz art. 34 ust. 1 i 2 rozporządzenia 2016/679), nakazał **komitetowi** zawiadomienie osób, których dane zostały ujawnione, a także nałożył administracyjną karę pieniężną. Podstawą przeprowadzenia postępowania wyjaśniającego przez Prezesa UODO był brak kontroli i nadzoru komitetu nad wypełnionymi kartami do zbiórki podpisów pod poparciem inicjatywy ustawodawczej. Administrator danych, mimo kilkukrotnych sygnałów ze strony organu nadzorczego oraz prowadzonej z nim korespondencji, nie zdecydował się na zgłoszenie naruszenia ochrony danych osobowych, bezskutecznie próbując wykazać, że wprowadzone przez niego zabezpieczenia były odpowiednie do poziomu ryzyka związanego z przetwarzaniem danych osobowych na listach poparcia. Analiza przypadku wykazała jednak, że gromadzenie tak dużych ilości danych osobowych odbywało się bez nadzoru osób uprawnionych do prowadzenia zbiórki, na skutek czego zostało wykonane zdjęcie list poparcia, a zatem nieuprawniony dostęp oraz skopiowanie znajdujących się na listach poparcia danych osobowych przez co najmniej jedną osobę, która zgłosiła nieprawidłowości. Z prowadzonej z administratorem korespondencji wynikało, że zbiórka podpisów odbywała się bez jakiejkolwiek kontroli ze strony administratora. Listy poparcia udostępnione były na stronie internetowej administratora, a udział w zbiórce podpisów mógł wziąć każdy zainteresowany wsparciem inicjatywy ustawodawczej. Pomimo posiadanej instrukcji zbierania podpisów, administrator nie był w stanie wskazać, czy każdy wolontariusz zapoznał się z jej treścią. Biorąc pod uwagę zasadę rozliczalności określoną w art. 5 ust. 2 rozporządzenia 2016/679, niedopuszczalne było działanie administratora, które pozornie wskazywało na przestrzeganie przepisów o ochronie danych osobowych.

Kolejna sprawa dotyczyła bezpieczeństwa przetwarzania danych osobowych na zewnętrznych nośnikach danych. Postępowanie wyjaśniające i administracyjne wykazało, że **pracodawca** w sposób nieprawidłowy przeprowadził analizę ryzyka, tj. nie przewidział zdarzenia będącego przyczyną wystąpienia naruszenia – zagubienie służbowego pendrive'a. Z przekazanych przez administratora dokumentów wynikało, że obszar dotyczący szyfrowania zewnętrznych nośników pamięci (pendrive) przez pracowników nie był w żaden sposób kontrolowany. W sprawie tej wydana została

[162] DKN.5131.1.2024.
[163] DKN.5131.32.2022.

decyzja[164] nakładająca administracyjną karę pieniężną za naruszenie przepisów art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 oraz nakazująca dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania ich skuteczności w zapewnieniu bezpiecznego przetwarzania. Administrator w całości zaskarżył decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Po przeprowadzeniu wszczętego z urzędu postępowania administracyjnego Prezes UODO wydał kolejną decyzję[165], w której nałożył administracyjne kary pieniężne na dwie **jednostki sektora finansów publicznych** oraz na **podmiot przetwarzający należący do sektora prywatnego**. Miało to związek z niewdrożeniem odpowiednich środków technicznych i organizacyjnych celem zabezpieczenia danych osobowych m.in. pracowników tych dwóch jednostek. Dane tych osób znajdowały się na pendrive, który został zgubiony przez pracownika podmiotu przetwarzającego. W decyzji tej Prezes UODO stwierdził naruszenie przez administratorów przepisów art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679, a także naruszenie zasady poufności (art. 5 ust. 1 lit. f rozporządzenia 2016/679) i zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679). W przypadku obu administratorów Prezes UODO stwierdził naruszenie art. 28 rozporządzenia 2016/679 – lecz w różnym zakresie. W odniesieniu do podmiotu przetwarzającego stwierdził naruszenie przepisów art. 32 ust. 1 i 2 oraz art. 32 ust. 1 i 2 w zw. z art. 28 ust. 3 lit. c oraz lit. f rozporządzenia 2016/679. Różnice w wielkości kar nałożonych na podmioty wynikały m.in. z odmienności w zakresie stwierdzonych nieprawidłowości, choć w pewnych aspektach wszystkie trzy podmioty dopuściły do podobnych zaniedbań. Stwierdzone nieprawidłowości dotyczyły m.in. braków w analizie ryzyka, weryfikacji bezpieczeństwa danych w procesie zmiany oprogramowania kadrowo-płacowego, w którym miały były przetwarzane.

Decyzja ta jest szczególnie istotna w przypadku administratorów przetwarzających dane osobowe za pomocą programów, które z czasem wymagają zmiany, a co za tym idzie, właściwego przygotowania się do tego procesu pod kątem zapewnienia bezpieczeństwa danych osobowych – również przez podmioty przetwarzające, którym zleca się wykonywanie czynności w tym zakresie.

W 2024 r. Prezes UODO wydał kolejną decyzję[166] nakładającą administracyjną karę pieniężną na **podmiot sektora prywatnego**. Przedmiotem decyzji było naruszenie przepisów dotyczących zapewnienia odpowiedniego do ryzyka bezpieczeństwa danych osobowych tj. art. 24 ust. 1, art. 25 ust. 1 art. 32 ust. 1 i 2 oraz art. 5 ust. 1 lit. f i art. 5 ust. 2 rozporządzenia 2016/679. Administrator z jednej strony nie przeprowadził prawidłowo analizy ryzyka, a z drugiej – nie wdrożył zaleceń, co do sposobów zmniejszenia ryzyka. Administrator dla zapewnienia bezpieczeństwa przetwarzania danych osobowych korzystał z urządzenia, którego wersja

[164] DKN.5131.29.2023.
[165] DKN.5131.35.2021.
[166] DKN.5131.21.2022.

oprogramowania sprzętowego (firmware) już w dniu zakupu była nieaktualna, a podatność, którą była obarczona, nie tylko została zakomunikowana przez producenta oprogramowania wraz z zaleceniami, co do jej aktualizacji do nowszych wersji, ale również była szeroko komentowana w mediach. Natomiast administrator w przeprowadzonej analizie ryzyka nie uwzględnił takiej podatności. Efektem powyższego było zmaterializowanie się ryzyka, tj. nastąpiło przełamanie zabezpieczeń systemu informatycznego administratora wykorzystywanego przez niego do przetwarzania danych osobowych, a następnie pobranie i zaszyfrowanie przetwarzanych w nim danych osobowych. Nałożona przez Prezesa UODO administracyjna kara pieniężna na ten podmiot została zapłacona.

Po przeprowadzeniu postępowania administracyjnego wobec **pośrednika w obrocie nieruchomościami**[167] została nałożona administracyjna kara pieniężna za naruszenie przepisów art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1, art. 28 ust. 1 i 3 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. Ponadto administrator zobowiązany został do dostosowania operacji przetwarzania do przepisów rozporządzenia 2016/679 poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania ich skuteczności w zapewnieniu bezpieczeństwa przetwarzania. Do czasu naruszenia ochrony danych osobowych administrator nie przeprowadził analizy ryzyka dla procesów przetwarzania danych osobowych i w sposób dowolny dobierał środki organizacyjne i techniczne, co mogło zwiększać prawdopodobieństwo wystąpienia naruszenia. Nałożona przez Prezesa UODO administracyjna kara pieniężna na ten podmiot została zapłacona.

Kolejną decyzję[168] Prezes UODO wydał wobec **spółki** zajmującej się wynajmem samochodów. Spółka nie wdrożyła odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych, na podstawie przeprowadzonej analizy ryzyka, a rozwiązań, które wprowadziła, nie testowała. Nie oceniała ich skuteczności i dlatego nie wiedziała, że nie są wystarczające. Prezes UODO nałożył administracyjne kary pieniężne zarówno na spółkę, jak i podmiot przetwarzający. Należy podkreślić, że analiza ryzyka oraz zarządzanie ryzykiem są procesami wymagającymi współpracy wszystkich zainteresowanych stron i jako takie wymagają przede wszystkim zaplanowania, zorganizowania, kierowania oraz kontrolowania zasobów wykorzystywanych do przetwarzania, realizacji samych czynności przetwarzania oraz badania i wykrywania ewentualnych podatności oraz luk.

Powodem ukarania administratora reprezentującego **sektor prywatny**[169] było naruszenie przepisów o ochronie danych osobowych, przejawiające się w niewdrożeniu odpowiednich środków bezpieczeństwa przetwarzania danych, którego szczególnie rażącymi przykładami były zaniechanie aktualizacji oprogramowania serwera, brak kontroli administratora nad uprawnieniami pracowników do pracy w jego systemach informatycznych, a także brak szkoleń

[167] DKN.5131.49.2022.
[168] DKN.5130.2415.2020.
[169] DKN.5131.1.2021.

pracowników z zakresu ochrony danych osobowych. Niezależnie od powyższego, administrator, pomimo identyfikacji wysokiego ryzyka dla praw lub wolności swoich byłych oraz obecnych pracowników, ignorując treść wystąpienia organu nadzorczego, nieprawidłowo zawiadomił podmioty danych o naruszeniu. Administrator nie zweryfikował, 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 (co również stanowiło przesłankę nałożenia administracyjnej kary pieniężnej). Prezes UODO stwierdził naruszenie przepisów: art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1, art. 28 ust. 1, art. 32 ust. 1 i 2 oraz art. 34 ust. 2 w związku z art. 33 ust. 3 lit. c oraz lit. d rozporządzenia 2016/679 i nałożył na administratora administracyjną karę pieniężną. Podmiot przetwarzający z kolei – odpowiedzialny za wdrożenie i utrzymanie systemu operacyjnego – został ukarany za uchybienie obowiązkowi wspierania administratora w zapewnieniu przez niego adekwatnych do zagrożeń środków zabezpieczających przetwarzane dane osobowe.

Prezes UODO, stwierdzając naruszenie przepisów art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679 przez jedną z **organizacji młodzieżowych**, nałożył administracyjną karę pieniężną[170] oraz nakazał administratorowi dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679 w terminie 3 miesięcy od dnia doręczenia decyzji. Naruszenie polegało na niezastosowaniu przez administratora odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy wykorzystaniu komputerów przenośnych oraz niezapewnieniu regularnego testowania, mierzenia i oceniania skuteczności tych środków, co skutkowało naruszeniem art. 5 ust. 1 lit. f (zasady integralności i poufności) oraz art. 5 ust. 2 rozporządzenia 2016/679 (zasady rozliczalności). Administracyjna kara pieniężna została przez organizację młodzieżową zapłacona.

Prezes UODO nałożył na **placówkę medyczną**[171] administracyjną karę pieniężną w sprawie, w której w wyniku ataku hakerskiego administrator stracił dostęp do danych pacjentów i pracowników tej placówki. W toku postępowania ustalono, że administrator naruszył przepisy art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 oraz art. 34 ust. 1 rozporządzenia 2016/679 poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą, na podstawie odpowiedniej analizy ryzyka, jak również nie zapewnił regularnego testowania, mierzenia i oceniania skuteczności tych środków, by zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych. Dodatkowo ustalono, że administrator naruszył art. 34 ust. 1 rozporządzenia 2016/679, wobec niezawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. Postępowanie wykazało, że złośliwe oprogramowanie typu ransomware zaszyfrowało dane osobowe około 30 tys. pacjentów i ponad tysiąca pracowników. W związku z zaistniałym zdarzeniem

[170] DKN.5131.9.2024.
[171] DKN.5131.57.2022.

administrator zlecił podmiotowi zewnętrznemu przeprowadzenie ekspertyzy w celu podjęcia próby odszyfrowania danych przetwarzanych na serwerach administratora. Zlecił również przeprowadzenie audytu bezpieczeństwa IT, którego celem była weryfikacja istniejących systemów informatycznych pod kątem określenia podatności na ataki złośliwego oprogramowania, w szczególności oprogramowania typu ransomware. Audyt ten wykazał między innymi, że sprzęt posiadany przez placówkę medyczną nie był odporny na możliwość zaszyfrowania baz danych oprogramowaniem typu ransomware. Administrator nie posiadał również dokumentów potwierdzających sporządzenie i aktualizowanie stosownej analizy ryzyka. Powyższe nie mogło zapewnić należytej kontroli nad bezpieczeństwem danych osobowych.

Poza nałożoną karą pieniężną Prezes UODO zalecił wdrożenie w terminie 30 dni odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych. Nakazał też powiadomić o zdarzeniu osoby, których dane dotyczą, wraz z podaniem imienia, nazwiska i danych do kontaktu z IOD, przedstawieniem opisu charakteru naruszenia ochrony danych osobowych, możliwych konsekwencji zdarzenia i wskazaniem środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu – w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków. Nałożona przez Prezesa UODO administracyjna kara pieniężna na ten podmiot została zapłacona.

Kolejna sprawa dotyczyła niewyznaczenia inspektora ochrony danych (IOD) przez administratora, którym był **organ publiczny**, zobowiązany do tego z mocy ustawy. Konsekwencją niedopełnienia ww. obowiązku był brak publikacji danych do kontaktu z inspektorem ochrony danych oraz zawiadomienia organu nadzorczego, co stanowiło z kolei naruszenie art. 37 ust. 7 rozporządzenia 2016/679. W toku postępowania administrator usiłował wykazać, że podjął stosowne czynności celem wypełnienia ciążących na nim obowiązków, tj. upoważnił do odgrywania roli IOD w swojej organizacji jednego z pracowników działu kadr. W ocenie organu nadzorczego środki dowodowe dostarczone przez administratora były niewystarczające, by wykazać, że należycie wypełnił obowiązki wynikające z art. 37 ust. 1 lit. a oraz art. 37 ust. 7 rozporządzenia 2016/679. W konsekwencji leżących po stronie administratora uchybień Prezes UODO nałożył administracyjną karę pieniężną[172] za niewyznaczenie inspektora ochrony danych, a w konsekwencji brak publikacji jego danych kontaktowych i brak zawiadomienia o tych danych organu nadzorczego.

Skuteczne wyznaczenie i publikacja danych IOD stanowi ważną gwarancję ochrony danych osobowych podmiotów, których dane są przetwarzane. Wynika to z samej roli inspektora ochrony danych i szerokiego wachlarza zadań przypisanych mu na gruncie art. 38 i 39 rozporządzenia 2016/679. Stwierdzonym w niniejszej sprawie naruszeniom art. 37 ust. 1 lit. a oraz art. 37 ust. 7 rozporządzenia 2016/679 należy przypisywać jednak znaczenie szersze, niż by to wynikało z ich formalnego charakteru. Prezes UODO zajął stanowisko, że niewyznaczenie IOD przez administratora może niejednokrotnie utrudniać lub wręcz uniemożliwiać realizację

[172] DKN.5131.7.2024.

praw osobom fizycznym, co nakazuje traktować stwierdzone naruszenie art. 37 ust. 1 lit. a rozporządzenia 2016/679, jako godzące w cały system ochrony danych osobowych, którego istotną część mają stanowić – zgodnie z wolą unijnego ustawodawcy – IOD.

W innym postępowaniu administracyjnym Prezes UODO wydał decyzję[173] nakładającą administracyjną karę pieniężną na **prokuraturę** za naruszenie przepisów art. 6 ust. 1 i art. 9 ust. 1 rozporządzenia 2016/679. Naruszenie polegało na ujawnieniu podczas konferencji prasowej, bez podstawy prawnej, danych osobowych osoby pokrzywdzonej, zawartych w wyroku sądu rejonowego. Skutkowało to naruszeniem art. 5 ust. 1 lit. a rozporządzenia 2016/679, tj. zasady zgodności z prawem i art. 33 ust. 1 rozporządzenia 2016/679, dotyczącego niezgłoszenia Prezesowi UODO naruszenia ochrony danych osobowych oraz art. 34 ust. 1 i ust. 2 RODO, polegającego na niezawiadomieniu o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki, osoby, której dane zostały ujawnione przez prokuraturę podczas konferencji prasowej. W sprawie tej Prezes UODO otrzymał od prokuratury wyjaśnienia, w których wskazano, że opisane zdarzenie nie było przedmiotem analizy administratora pod kątem powstania naruszenia ochrony danych, gdyż w jego ocenie nie było do tego podstaw. Prokuratura tłumaczyła, że dane osobowe, które zostały udostępnione podczas konferencji prasowej, stanowiły część orzeczenia sądu i zostały przytoczone dla zilustrowania zasadniczej rozbieżności pomiędzy przypisanymi osobom skazanym przestępstwami a ustaleniami sądu. A poza tym dane tej osoby zostały już ujawnione w toku postępowania sądowego. Prokuratura prezentowała stanowisko, że ujawnienie danych nie było naruszeniem ochrony danych osobowych, informacje te były bowiem przez Prokuraturę przetwarzane w związku z realizacją ustawowych zadań, a to pozostaje poza kompetencjami Prezesa UODO. W sprawie tej prokuratura zaskarżyła decyzję organu o nałożeniu administracyjnej kary pieniężnej do Wojewódzkiego Sądu Administracyjnego.

4. Egzekucja administracyjna – zapewnienie wykonania decyzji organu nadzorczego

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[174], 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

[173] DKN.5131.33.2023.

[174] Ustawa z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. z 2025 r. poz. 132), zwana dalej także jako „u.p.e.a”.

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)[175]. 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 stronę (zobowiązanego) może polegać w szczególności na: usunięciu uchybień w procesie przetwarzania danych osobowych; spełnieniu żądania osoby, której dane dotyczą (odnoszącego się do jej praw wynikających z przepisów o ochronie danych osobowych); wprowadzeniu czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania danych, zawieszeniu przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej czy wreszcie zawiadomieniu osoby, której dane dotyczą o naruszeniu ochrony jej danych osobowych;
b) **prawomocne decyzje nakładające administracyjne kary pieniężne** – zaskarżenie do sądu administracyjnego takiej decyzji wstrzymuje jej wykonanie i tym samym możliwość wszczęcia egzekucji administracyjnej[176]. Prezes UODO ma prawo nałożyć na podmiot prywatny administracyjną karę pieniężną w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego obrotu, w zależności od tego, która kwota jest wyższa. Natomiast na jednostki sektora finansów publicznych (z wyjątkiem państwowych i samorządowych instytucji kultury), instytuty badawcze i Narodowy Bank Polski, Prezes UODO może nałożyć karę w wysokości do 100 000 zł. Wspomniane wyżej instytucje kultury mogą być ukarane karą do 10 000 zł.

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).

[175] Art. 61 § 1 ustawy z 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2024 r. poz. 935 ze zm.).
[176] Art. 74 ustawy z 10 maja 2018 r. o ochronie danych osobowych.

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 jeszcze na tym etapie sprawy). W przypadku, gdy postępowanie to nie wykaże, że decyzja została wykonana, do zobowiązanego kierowane jest upomnienie[177] 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**[178]. 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.

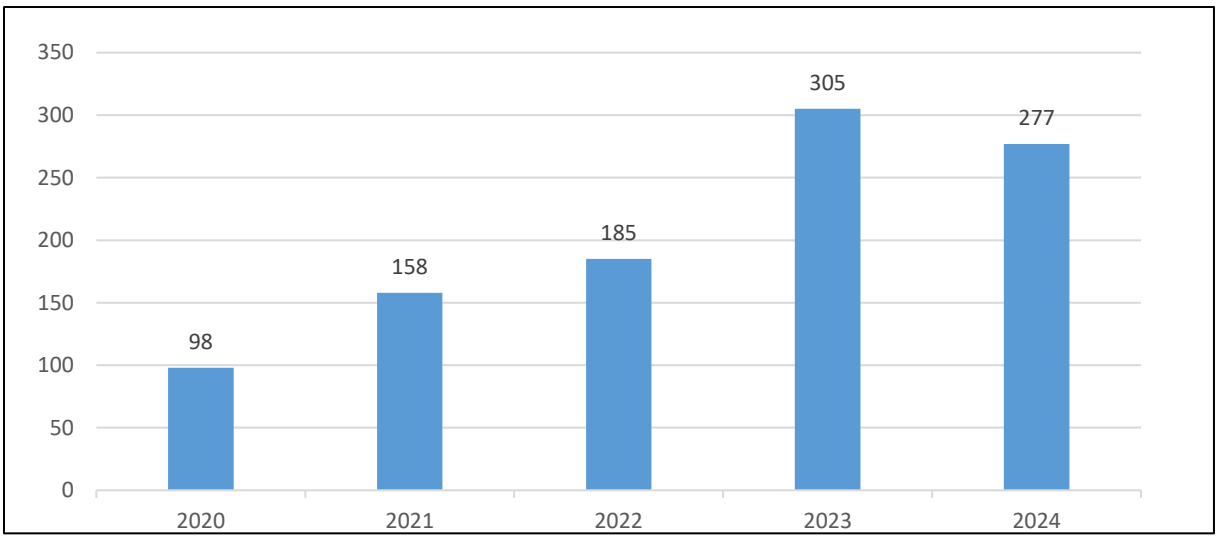
4.1. Postępowania w zakresie egzekucji decyzji Prezesa UODO

W 2024 r. wszczętych zostało **277 postępowań sprawdzających wykonanie decyzji Prezesa UODO** (8 postępowań dotyczyło sprawdzenia wykonania decyzji nakładających administracyjne kary pieniężne, 267 postępowań – decyzji zawierających nakaz, tj. obowiązek o charakterze niepieniężnym, natomiast 2 postępowania dotyczyły sprawdzenia przestrzegania postanowień, wydanych w trybie art. 66 ust. 1 RODO, zobowiązujących do ograniczenia przetwarzania danych osobowych).

Powyższe dane wskazują na **spadek tego rodzaju postępowań o 9 % w stosunku do roku 2023** (w którym wszczęto 305 postępowań sprawdzających). Jednocześnie jednak liczba postępowań zainicjowanych w ostatnich dwóch okresach

[177] Art. 6 § 1 i art. 15 ustawy o postępowaniu egzekucyjnym w administracji.
[178] Dział II u.p.e.a.

sprawozdawczych wskazuje na utrzymującą się tendencję zwyżkową w stosunku do lat 2020–2022, co ilustruje poniższy wykres.



Wykres 9. Zestawienie liczby decyzji i postanowień Prezesa UODO przekazanych do sprawdzenia wykonania i ewentualnej egzekucji administracyjnej w latach 2020–2024.

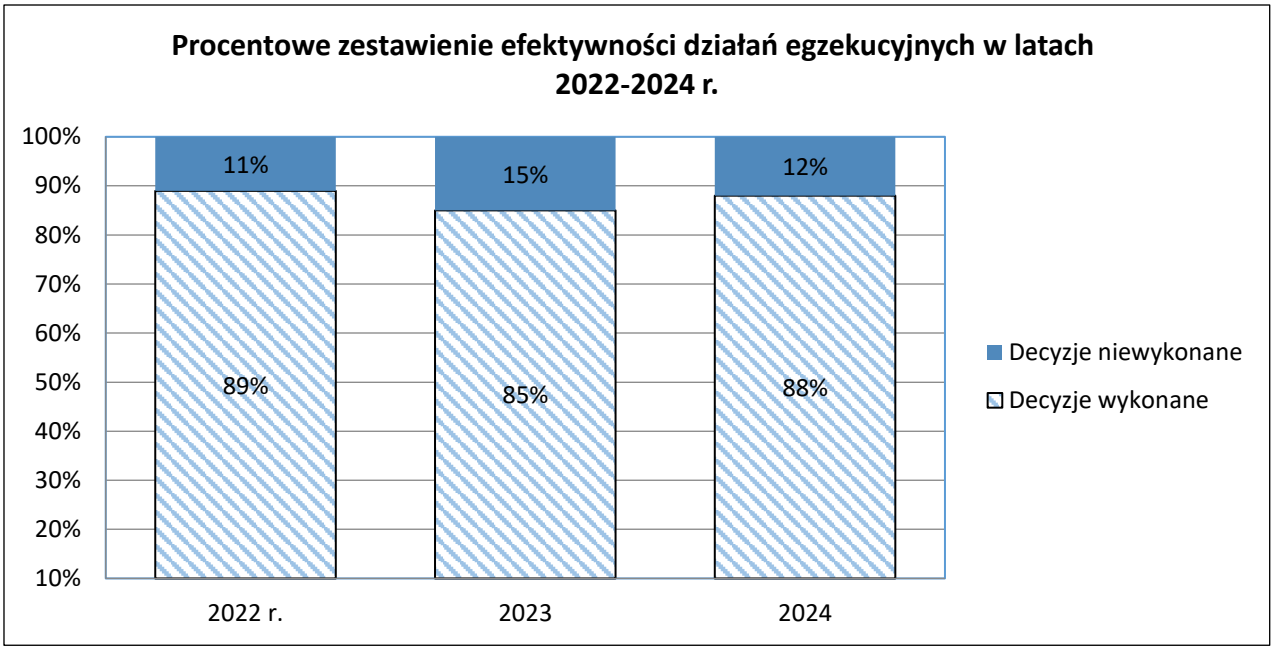
Efektywność prowadzonych przez UODO działań, mających na celu sprawdzenie i spowodowanie wykonania przez zobowiązanych obowiązków nałożonych na nich decyzjami administracyjnymi, przedstawia się następująco:

- spośród 277 decyzji i postanowień, w odniesieniu do których wszczęte zostały postępowania w 2024 r., **zakończonych zostało 244,** natomiast
- 33 decyzje nadal objęte są działaniami UODO.

W 14 przypadkach wszczęta została egzekucja obowiązku o charakterze niepieniężnym, w ramach których na zobowiązanych nałożone zostały grzywny w celu przymuszenia. W stosunku do 1 zobowiązanego Prezes UODO wszczął postępowanie administracyjne w przedmiocie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy.

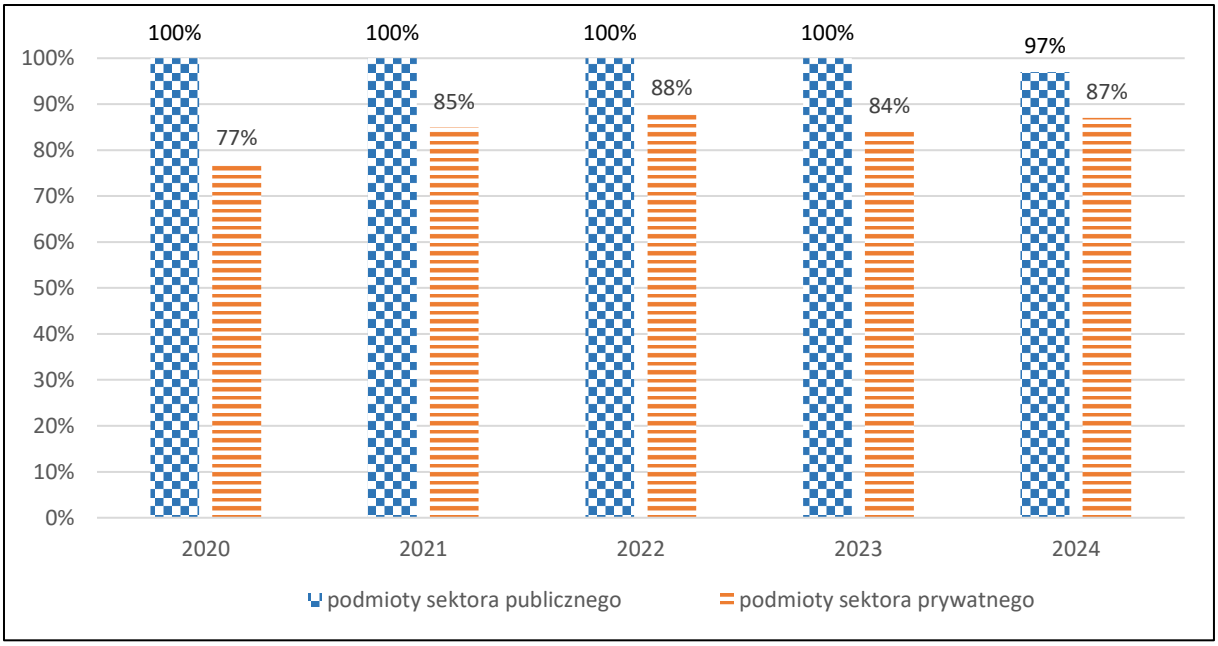
W odniesieniu do pozostałych 18 decyzji prowadzone są w dalszym ciągu działania mające na celu sprawdzenie ich wykonania lub spowodowanie ich dobrowolnego wykonania przez zobowiązanych.

Procentowy wskaźnik efektywności działań w odniesieniu do wszystkich decyzji administracyjnych i postanowień Prezesa UODO, co do których wszczęte zostały w roku 2024 postępowania sprawdzające, wyniósł **88 %**. Porównanie wskaźnika efektywności w latach 2022–2024 obrazuje wykres 10.



Wykres 10. Procentowe zestawienie efektywności działań egzekucyjnych Prezesa UODO w latach 2022–2024.

Podjęte w 2024 r. działania w zakresie sprawdzenia wykonania i egzekucji decyzji administracyjnych oraz postanowień Prezesa UODO dotyczyły w 14 % przypadków podmiotów z sektora publicznego (39 postępowań), a w pozostałych 86 % przypadków – podmiotów prywatnych (238 postępowań). W przeciwieństwie do lat wcześniejszych, w których to wskaźnik wykonalności nakazów orzeczonych przez Prezesa UODO wobec podmiotów należących do sektora publicznego utrzymywał się na stałym poziomie 100 %, w roku 2024 odnotowano 1 postępowanie sprawdzające, w ramach którego zobowiązany nie udowodnił, w czasie trwania okresu sprawozdawczego, wykonania nakazu decyzji. Postępowanie to pozostaje w toku. Pozostałe niewykonane decyzje skierowane były do podmiotów sektora prywatnego.



Wykres 11. Zestawienie efektywności działań egzekucyjnych prowadzonych w latach 2020–2024 w odniesieniu do podmiotów sektora publicznego i sektora prywatnego.

4.2. Egzekucja obowiązków o charakterze niepieniężnym

Wobec stwierdzenia niewykonania przez zobowiązanych nakazów decyzji Prezesa UODO w 2024 r. wszczęte zostały **22 egzekucje obowiązków o charakterze niepieniężnym**. Wystawione w tym okresie tytuły wykonawcze objęły nakazy orzeczone 23 decyzjami administracyjnymi, a łączna kwota grzywien w celu przymuszenia zastosowanych wobec zobowiązanych przez Prezesa UODO w tych postępowaniach wyniosła **155 500 zł**. Spośród 22 wszczętych w 2024 r. egzekucji obowiązków o charakterze niepieniężnym:

1) 15 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 106 500 zł, przy czym w efekcie podjęcia wyżej opisanych działań:

a) 3 postępowania doprowadziły do ustalenia, że zobowiązani wykonali adresowane do nich nakazy decyzji Prezesa UODO – przy tym w 1 przypadku nałożona na zobowiązanego grzywna w celu przymuszenia w kwocie 5 000 zł została wyegzekwowana w całości, zaś w 2 pozostałych sprawach grzywny w łącznej wysokości 4 000 zł zostały umorzone[179],

b) 12 postępowań nie doprowadziło do ustalenia wykonania nakazu decyzji;

2) W trakcie postępowania jest 7 egzekucji, w których nałożono grzywny w celu przymuszenia w łącznej kwocie 49 000 zł.

[179] Art. 125 u.p.e.a.

4.3. Egzekucja należności pieniężnych

W 2024 r. Prezes UODO doprowadził do wszczęcia **30 egzekucji należności pieniężnych** (których łączna wysokość wynosiła **346 945 zł**). Porównując liczbę tego rodzaju spraw z rokiem poprzednim, należy wskazać na 88 % wzrost – w roku 2023 wszczęto bowiem 16 takich postępowań. Tendencja wzrostowa dotyczy również poziomu, na jakim kształtowała się suma należności podlegających egzekucji pieniężnej, która w 2023 r. wyniosła 261 242 zł. W omawianym okresie sprawozdawczym egzekucje należności pieniężnych dotyczyły dwóch rodzajów należności: nałożonych przez Prezesa UODO administracyjnych kar pieniężnych oraz grzywien w celu przymuszenia orzeczonych przez Prezesa UODO jako środków egzekucyjnych w egzekucjach obowiązków o charakterze niepieniężnym. W ujęciu liczbowym postępowania te i ich efekty przedstawiają się następująco:

1) Prezes UODO w bieżącym okresie sprawozdawczym doprowadził do wszczęcia **7 egzekucji**, których przedmiotem były **administracyjne kary pieniężne** w łącznej wysokości **169 445 zł**. Wszystkie egzekwowane w tych postępowaniach kary pieniężne nałożone zostały na podmioty prywatne – 5 spółek prawa handlowego oraz 2 osoby fizyczne prowadzące indywidualną działalność gospodarczą. W przypadku 4 spośród ww. postępowań objęte **nimi administracyjne kary pieniężne w łącznej wysokości 72 125 zł zostały skutecznie wyegzekwowane**. W przypadku 1 postępowania, w którym egzekwowana była kara w wysokości 59 592 zł, organ egzekucyjny (właściwy miejscowo naczelnik urzędu skarbowego) odmówił przystąpienia do egzekucji ze względu na dotyczące zobowiązanego trwające postępowanie o zatwierdzenie układu[180]. W pozostałych przypadkach, dotyczących 2 kar w łącznej kwocie 37 728 zł, właściwe organy egzekucyjne podejmują w dalszym ciągu działania egzekucyjne.
2) Przedmiotem **23 wszczętych przez Prezesa UODO egzekucji** należności pieniężnych były **grzywny w celu przymuszenia** (w łącznej kwocie **177 500 zł**). Wszystkie tego rodzaju środki egzekucyjne orzeczone zostały wobec podmiotów prywatnych – 9 spółek prawa handlowego, 13 osób fizycznych prowadzących indywidualną działalność gospodarczą oraz 1 stowarzyszenia. W przypadku **4 tytułów wykonawczych wystawionych przez Prezesa UODO (na łączną kwotę 50 000 zł)** właściwi naczelnicy urzędów skarbowych wyegzekwowali w całości objęte nimi należności. W przypadku 1 postępowania, w którym egzekwowana była grzywna w wysokości 10 000 zł, organ egzekucyjny odmówił przystąpienia do egzekucji ze względu na brak majątku lub źródła dochodu, z których możliwa byłaby egzekucja. Natomiast w 2 postępowaniach, w których egzekwowane były grzywny w celu przymuszenia w łącznej wysokości 4 000 zł – w związku z ustaleniem, że zobowiązani wykonali adresowane do nich obowiązki o charakterze niepieniężnym – Prezes UODO wydał postanowienia o umorzeniu

[180] Art. 29 § 2 u.p.e.a. w zw. z art. 312 ust. 4 oraz art. 226e ustawy z 15 maja 2025 r. Prawo restrukturyzacyjne (Dz.U. z 2024 r. poz. 1428 ze zm.).

egzekwowanych należności. Pozostałe egzekucje (16 tytułów wykonawczych na łączną kwotę 113 500 zł) nadal są prowadzone przez właściwe organy egzekucyjne.

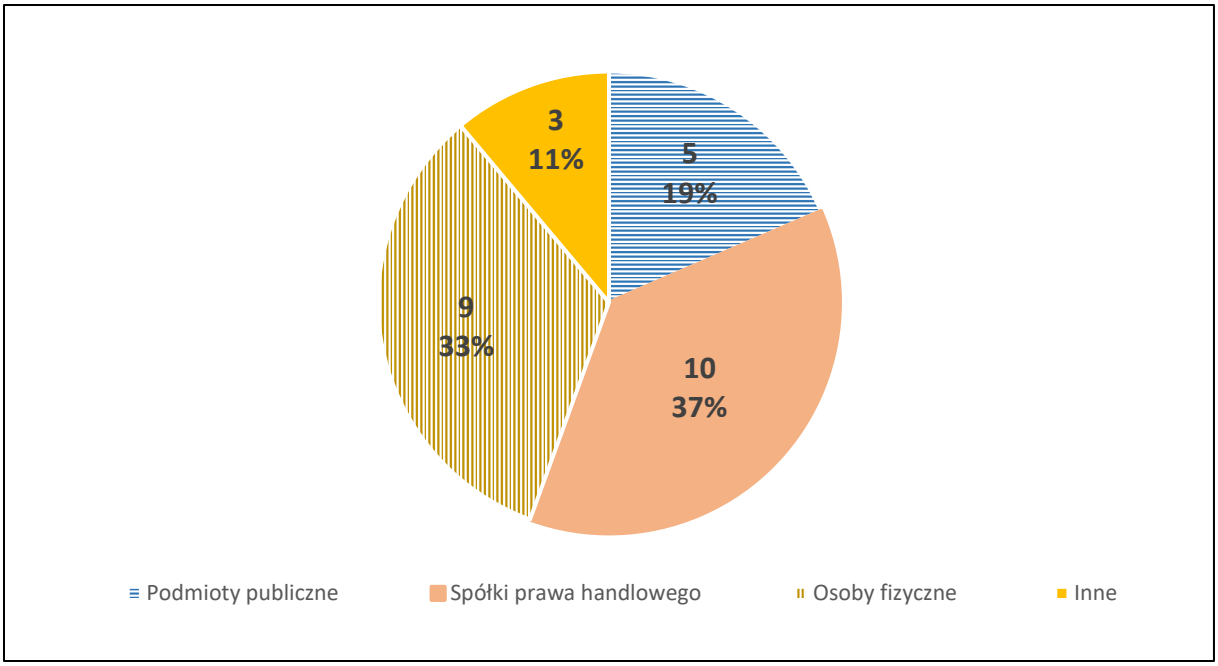
5. Administracyjne kary pieniężne

Stosownie do art. 58 ust. 2 lit. i RODO Prezesowi UODO przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych, zależnie od okoliczności konkretnej sprawy, administracyjnej kary pieniężnej.

Ponadto, w oparciu o art. 210a Prawa Telekomunikacyjnego, Prezes UODO uprawniony jest do nakładania administracyjnych kar pieniężnych za naruszenie niektórych obowiązków przewidzianych przepisami tego aktu prawnego. W omawianym okresie sprawozdawczym Prezes UODO w żadnym przypadku nie skorzystał z tego uprawnienia.

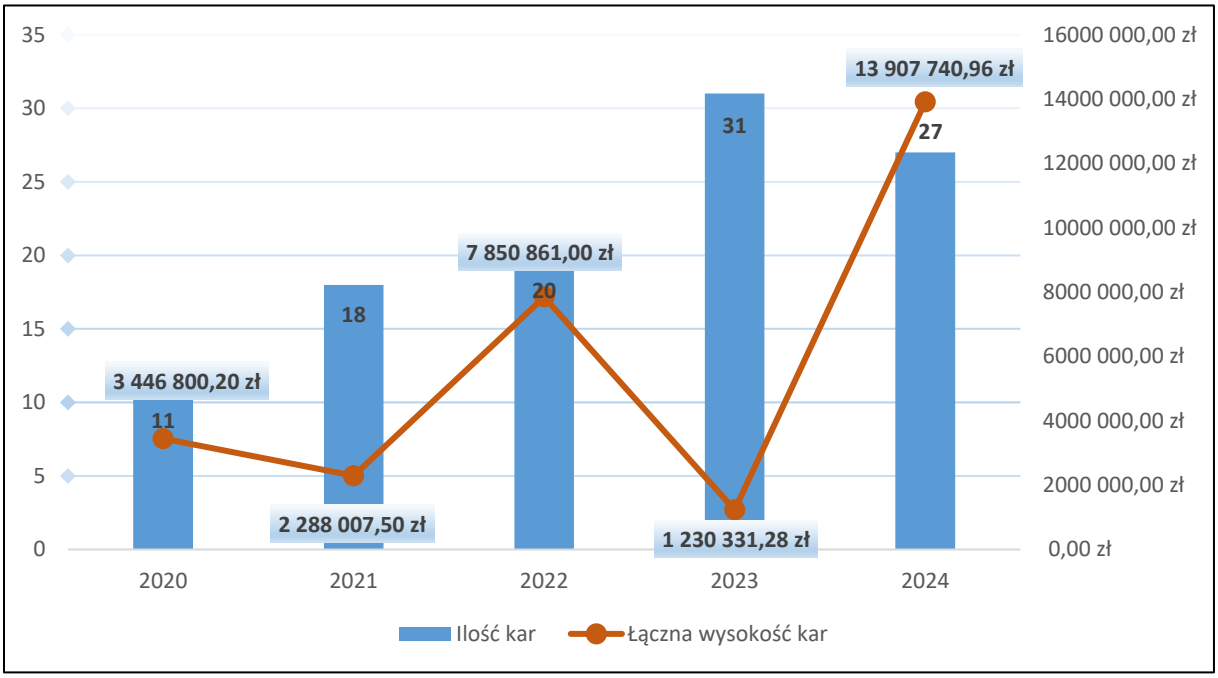
W 2024 r. Prezes UODO skorzystał z uprawnienia do zastosowania administracyjnej kary pieniężnej w przypadkach naruszenia przepisów RODO w 22 sprawach, nakładając na **27 podmiotów** łącznie 27 administracyjnych kar pieniężnych w całkowitej kwocie **13 907 740,96 zł**. W porównaniu z rokiem poprzednim oznacza to **spadek liczby nałożonych kar o 13 %,** przy jednoczesnym **wzroście ich łącznej wysokości o 1030 %** (w 2023 r. orzeczonych zostało 31 administracyjnych kar pieniężnych na łączną kwotę 1 230 331,28 zł). Najwyższa kara nałożona przez Prezesa UODO w analizowanym okresie sprawozdawczym wyniosła 4 053 174 zł (co stanowiło 29 % wartości wszystkich administracyjnych kar pieniężnych wymierzonych w 2024 r.), z kolei najniższa kara została orzeczona w odniesieniu do stowarzyszenia w kwocie 916,71 zł (stanowiącej 0,007 % wartości wszystkich kar).

Spośród 27 ukaranych podmiotów 5 należało do sektora finansów publicznych, natomiast wśród pozostałych 22 podmiotów prywatnych: 10 to spółki prawa handlowego, 9 to osoby fizyczne prowadzące działalność gospodarczą lub będące (obecnie lub w przeszłości) wspólnikami spółki cywilnej, a pozostałe 3 to: komitet inicjatywy ustawodawczej oraz 2 stowarzyszenia.



Wykres 12. Zestawienie podmiotów podlegających w 2024 r. ukaraniu administracyjną karą pieniężną, z podziałem na ich status i formę prawną.

Kolejny wykres przedstawia natomiast liczbę i łączną wysokość administracyjnych kar pieniężnych orzeczonych przez Prezesa UODO w omawianym okresie sprawozdawczym, w porównaniu do lat poprzednich – począwszy od roku 2020.



Wykres 13. Zestawienie liczby i łącznej wysokości administracyjnych kar pieniężnych orzeczonych przez Prezesa UODO w latach 2020–2024

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

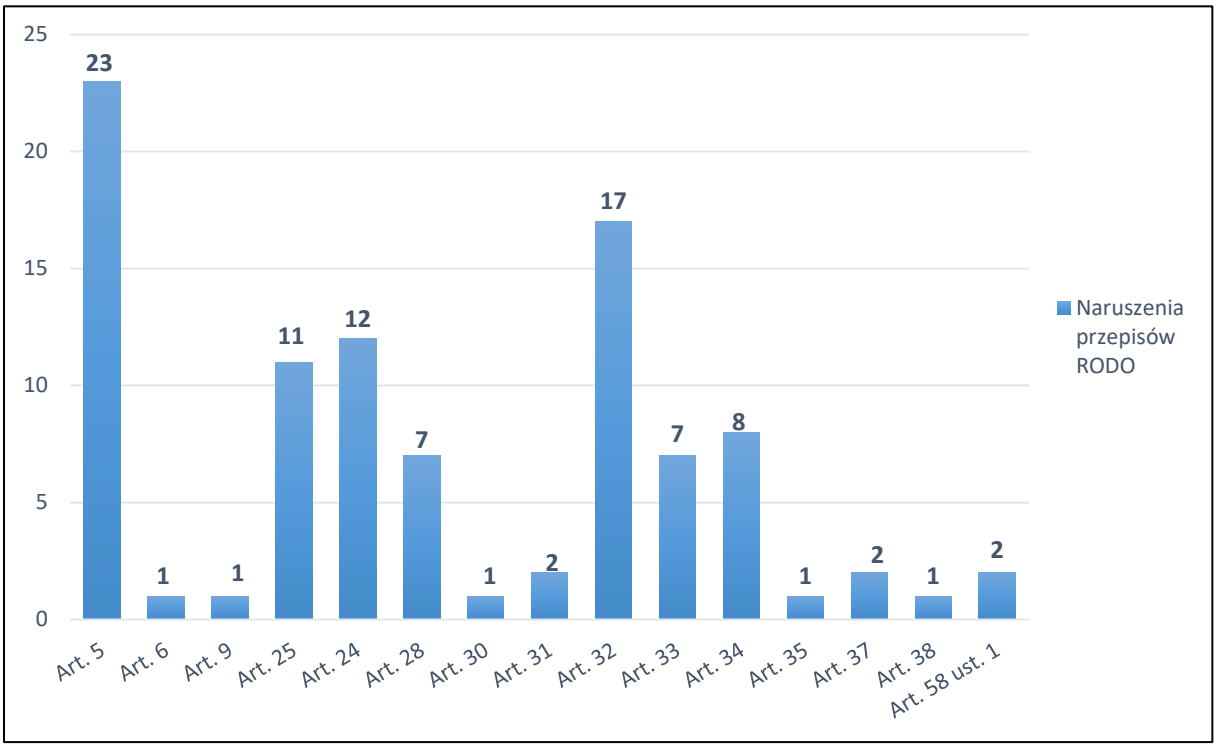
1) **prawomocnych** na dzień 31 grudnia 2024 r. – w całości lub w części, w sytuacji, gdy ukaraniu w jednej decyzji podlegało kilka podmiotów – było (ze względu na ich niezaskarżenie do sądu administracyjnego bądź utrzymanie w mocy na skutek przeprowadzonej kontroli sądowej) **12 decyzji** nakładających w sumie 14 administracyjnych kar pieniężnych w łącznej kwocie **307 994,92 zł**. Spośród tych kar:
   a) 10 kar zapłaconych zostało dobrowolnie przez ukarane podmioty[181],
   b) wobec 1 ukaranego podmiotu wszczęte zostało postępowanie sprawdzające wykonanie decyzji nakładającej administracyjną karę pieniężną[182],
   c) wobec 2 ukaranych podmiotów wszczęta została egzekucja należności pieniężnych, w wyniku której nałożone kary zostały wyegzekwowane[183],
   d) w odniesieniu do jednej kary odstąpiono od działań mających na celu jej wyegzekwowanie wobec ustalenia, że ukarany podmiot utracił byt prawny na skutek rozwiązania go z mocy prawa[184].
2) **nieprawomocnych** na dzień 31 grudnia 2024 r. i **zaskarżonych** do Wojewódzkiego Sądu Administracyjnego w Warszawie – w całości lub w części, w sytuacji, gdy ukaraniu w jednej decyzji podlegało kilka podmiotów – było **10 decyzji** nakładających w sumie 11 administracyjnych kar pieniężnych o łącznej wysokości **13 023 526,04 zł**, z czego:
   a) jedna kara została uchylona przez Wojewódzki Sąd Administracyjny w Warszawie, przy czym zapadłe w tym przedmiocie orzeczenie nie jest prawomocne[185],
   b) w odniesieniu do 10 administracyjnych kar pieniężnych trwa postępowanie sądowo-administracyjne[186].
3) **nieprawomocna** na dzień 31 grudnia 2024 r. i **niezaskarżona** do Wojewódzkiego Sądu Administracyjnego w Warszawie, była **1 decyzja** nakładająca 2 administracyjne kary pieniężne w łącznej wysokości **576 220 zł**, przy czym oczekuje ona na uprawomocnienie się lub wszczęcie egzekucji[187].

Na wykresie 14 przedstawiono z kolei informację o rodzajach naruszeń podlegających ukaraniu administracyjnymi karami pieniężnymi, tj. o przepisach

[181] DKN.5130.2415.2020 (dwie kary orzeczone jedną decyzją, przy czym jedna nie podlegała zaskarżeniu), DKN.5131.35.2021, DKN.5131.21.2022, DKN.5131.49.2022, DKN.5131.57.2022, DKN.5131.58.2022, DKN.5131.28.2023 (trzy kary orzeczone jedną decyzją), DKN.5131.9.2024.
[182] DKN.5131.53.2021.
[183] DOKE.561.1.2024, DOKE.561.4.2024.
[184] DKN.5131.32.2022.
[185] DKN.5131.29.2023.
[186] ZSPR.421.2.2019, DKN.5112.35.2021, DKN.5130.2415.2020 (dwie kary orzeczone jedną decyzją, przy czym jedna podlegała zaskarżeniu), DKN.5131.1.2021 (dwie kary orzeczone jedną decyzją), DKN.5131.59.2022, DKN.5131.33.2023, DKN.5131.1.2024, DKN.5131.6.2024, DKN.5131.7.2024
[187] DKN.5112.14.2022.

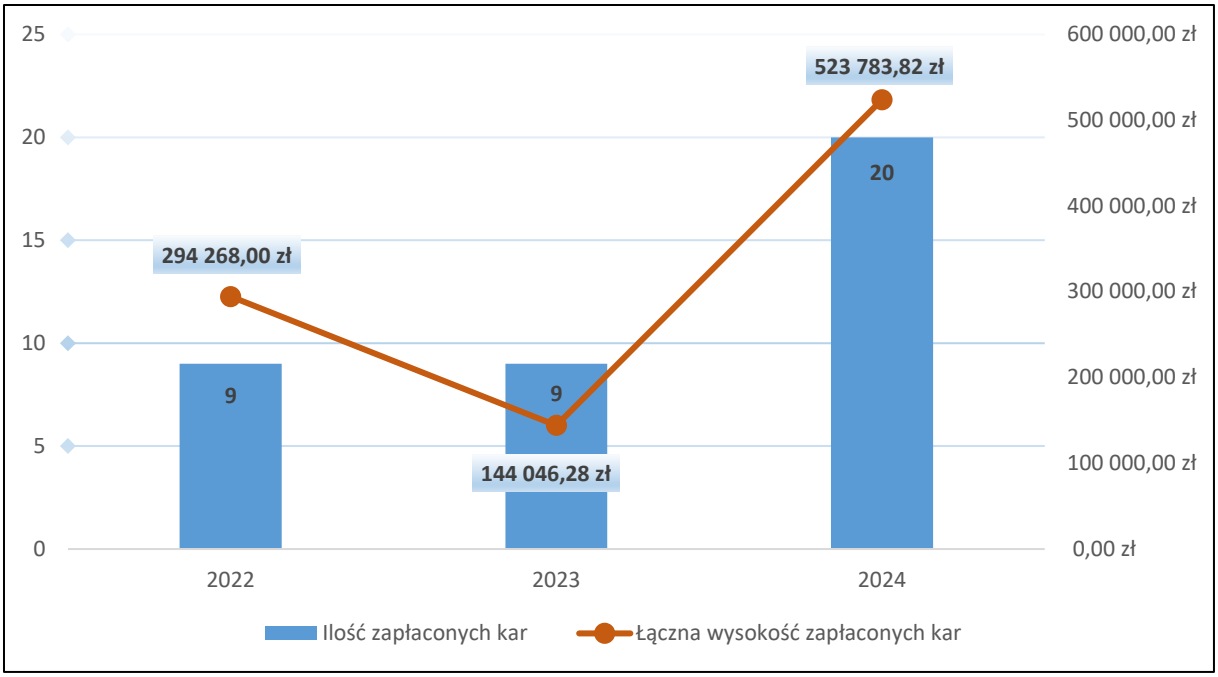
RODO, których naruszenie stwierdzone zostało przez Prezesa UODO w decyzjach nakładających na administratorów lub podmioty przetwarzające administracyjne kary pieniężne w 2024 r.

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.



Wykres 14. Zestawienie naruszeń poszczególnych przepisów RODO podlegających ukaraniu administracyjnymi karami pieniężnym w roku 2024.

W porównaniu do poprzednich lat, w roku 2024 zauważalny był znaczący wzrost liczby zapłaconych (tj. uiszczonych dobrowolnie lub ściągniętych w trybie egzekucji administracyjnej) administracyjnych kar pieniężnych nałożonych w drodze decyzji Prezesa UODO. W analizowanym okresie sprawozdawczym **zapłaconych zostało 20 kar**, w łącznej kwocie **523 783,82 zł**. Oznacza to **wzrost ilościowy o 122 %** w stosunku do lat 2022–2023, w których liczba ta wynosiła rokrocznie 9 kar. Jednocześnie odnotowano wzrost łącznej wysokości zapłaconych administracyjnych kar pieniężnych o 264 % w stosunku do 2023 r. (w którym ich suma wyniosła 144 046,28 zł) oraz o 80 % w stosunku do 2022 r. (w którym ich suma wyniosła 294 268,00 zł).



Wykres 15. Zestawienie liczby i łącznej wysokości administracyjnych kar pieniężnych zapłaconych w latach 2022–2024.

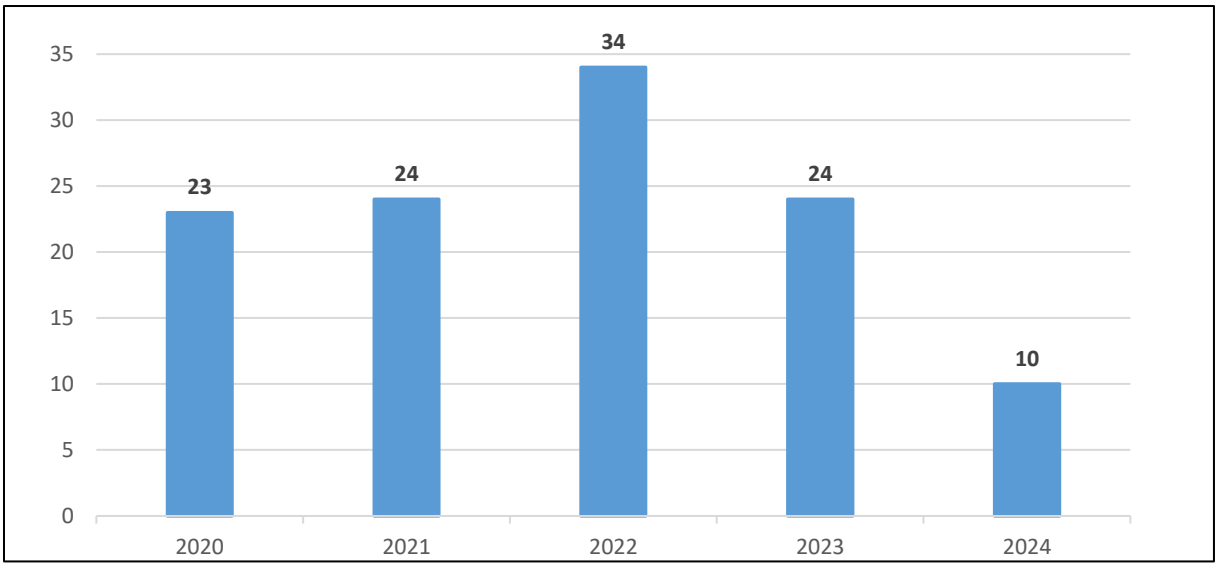
W ramach kompetencji Prezesa Urzędu Ochrony Danych Osobowych do orzekania o sankcjach finansowych przysługuje mu **uprawnienie do nakładania administracyjnych kar pieniężnych o szczególnym dyscyplinującym charakterze**. Kary te mają na celu zdyscyplinowanie administratorów i podmioty przetwarzające, 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.

5.1. 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 oraz lit. 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 też na udzielaniu informacji niepełnych, które nie pozwalały na rozstrzygnięcie sprawy lub wydłużały w sposób nieuzasadniony czas trwania postępowań.

W celu zdyscyplinowania stron postępowań do prawidłowego wypełniania obowiązków procesowych Prezes UODO wszczął w 2024 r. z urzędu **10 postępowań** w przedmiocie nałożenia administracyjnej kary pieniężnej za tego rodzaju naruszenia. Oznacza to spadek liczby tego rodzaju postępowań o 58 % w stosunku do poprzedniego okresu sprawozdawczego, w którym tego rodzaju postępowań wszczętych zostało 24.



Wykres 16. Zestawienie liczby wszczętych w latach 2020–2024 postępowań w przedmiocie nałożenia kary za brak współpracy z Prezesem UODO i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań.

W 4 przypadkach samo wszczęcie postępowania w przedmiocie nałożenia kary okazało się skuteczne i strony zaczęły współpracować z Prezesem UODO – udzieliły żądanych przez Prezesa UODO 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 zakończyły się **2 postępowania**; wysokość nałożonych tymi decyzjami kar wyniosła łącznie

41 471 zł[188]. Do dnia sporządzenia niniejszego sprawozdania obie ww. kary zostały wyegzekwowane w drodze egzekucji należności pieniężnych.

Pozostałe **4 postępowania** w przedmiocie nałożenia kary za brak współpracy z organem i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań wszczętych w 2024 r. **nie zostało zakończonych** do dnia sporządzenia niniejszego sprawozdania.

5.2. 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.

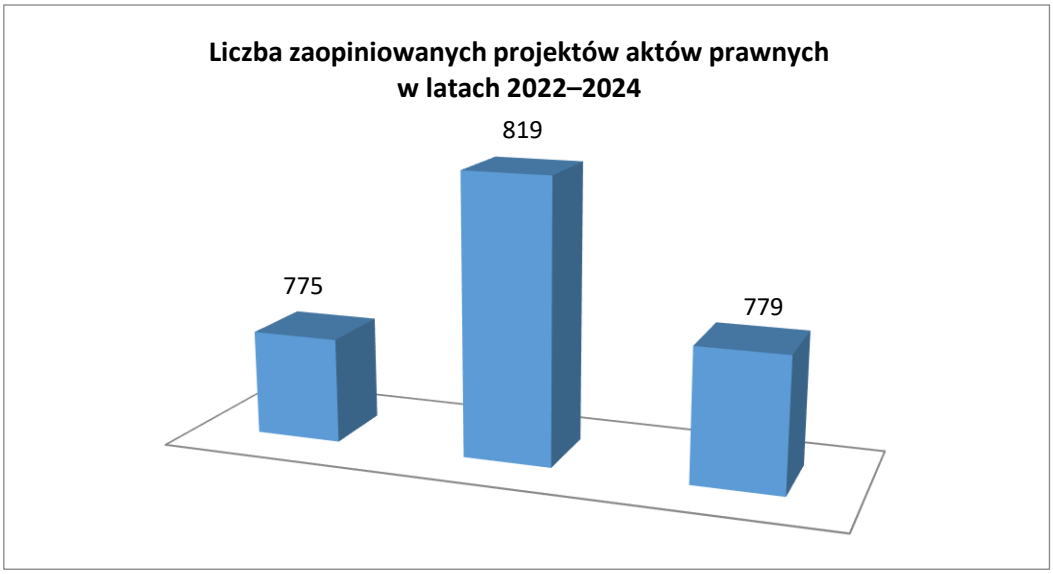
W roku 2024 Prezes UODO wszczął **jedno postępowanie** w przedmiocie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie orzeczonego przez siebie w decyzji administracyjnej nakazu. Do dnia sporządzenia niniejszego sprawozdania postępowanie to nie zostało zakończone.

6. 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 2024 r. do Urzędu Ochrony Danych Osobowych **wpłynęło 570 projektów aktów prawnych** (rządowych, poselskich, obywatelskich i innych), w tym ustaw, rozporządzeń oraz innych aktów krajowych i międzynarodowych.

Łącznie w 2024 r. organ nadzorczy zaopiniował **779 projektów aktów prawnych.** Dla porównania w 2023 r. zaopiniowano 819 projektów aktów prawnych, a w 2022 r.– 775 projektów – co przedstawia wykres 17.

[188] DOKE.561.1.2024, DOKE.561.4.2024.



Wykres 17. Liczba zaopiniowanych projektów aktów prawnych, które wpłynęły do Urzędu Ochrony Danych Osobowych w latach 2022–2024.

Organ nadzorczy nie posiada inicjatywy prawodawczej. Biorąc udział w procesie legislacyjnym, opiniuje projekty przepisów dotyczących przetwarzania danych osobowych jako organ ekspercki celem zapewnienia stosowania w prawie krajowym przepisów o ochronie danych osobowych. Jako rzecznik praw osób, których dane osobowe dotyczą, wskazuje projektodawcom aspekty wymagające uwzględnienia w planowanych regulacjach, konieczne dla prawidłowej realizacji konstytucyjnych praw: do prywatności i do autonomii informacyjnej jednostki, zapewnienia standardów demokratycznego państwa prawa w procesach przetwarzania danych osobowych oraz gwarancji wykonywania uprawnień podmiotów danych wynikających z rozporządzenia ogólnego.

Na podstawie analizy opinii legislacyjnych Prezesa UODO wyróżnić można kwestie, które budzą problemy, a także wskazać powtarzające się nieścisłości. Wiele z nich stanowi powielenie tendencji zauważonych w latach ubiegłych. W roku 2024 uwidoczniły się również liczne nowe trudności, związane głównie z wdrażaniem nowych technologii oraz stałą rozbudową systemów cyfrowych oraz operacji przetwarzania opartych o rozbudowane rejestry państwowe.

Zasadniczymi zagadnieniami pozostającymi w stałym zainteresowaniu organu nadzorczego były przede wszystkim:

- uwzględnienie ochrony danych osobowych w fazie projektowania,
- implementacja testu prywatności jako elementu oceny skutków przyjmowanych regulacji,
- stosowanie zasady praworządności, przyjęcie właściwej konstrukcji podstawy prawnej przetwarzania danych osobowych, zachowanie zasad hierarchii źródeł prawa, rangi aktu prawnego regulującego prawa i obowiązki w przedmiocie przetwarzania danych osobowych,
- procesy przetwarzania w rejestrach państwowych i systemach teleinformatycznych – przetwarzanie danych przez podmioty publiczne, dla

wykonywania zadania publicznego czy w ramach sprawowania władzy publicznej, w szczególności z użyciem nowych technologii,
- rozgraniczenie ról podmiotów biorących udział w procesach przetwarzania danych – normy kierowane do wykonawców regulacji: administratorów, podmiotów działających w ich imieniu czy na ich rzecz,
- stosowanie zasad przetwarzania danych osobowych, zwłaszcza zgodności z prawem, rzetelności i przejrzystości oraz rozliczalności, w tym dla przetwarzania danych szczególnych kategorii oraz identyfikatora PESEL,
- przetwarzanie danych w kontekście procesów cyfryzacji państwa i stosowania nowych technologii,
- kształtowanie zakresu i modelu nowych kompetencji Prezesa Urzędu Ochrony Danych Osobowych wynikających z aktów unijnych oraz przepisów krajowych implementujących czy służących stosowaniu prawa unijnego,
- przetwarzanie danych osobowych w kontekście nowych projektów informatycznych, w szczególności w zakresie testu prywatności, zasad: zgodności z prawem, rzetelności i przejrzystości oraz rozliczalności.

6.1. Uwzględnienie ochrony danych osobowych na etapie prac legislacyjnych

W myśl art. 57 ust. 1 lit. c RODO rolą organu nadzorczego w procesie legislacyjnym jest doradzanie 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 osobowych. Art. 36 ust. 4 RODO stanowi ponadto, że państwa członkowskie konsultują się z organem nadzorczym, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania danych osobowych. Obowiązek przedstawienia do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych projektów i aktów prawnych dotyczących danych osobowych wynika również z art. 51 ustawy o ochronie danych osobowych. Regulamin pracy Rady Ministrów (uchwała nr 190 z 29 października 2013 r.) w § 38 ust. 1 pkt 3, choć nie odnosi się wprost do organu do spraw ochrony danych osobowych, to jednak nakłada prawny obowiązek skierowania projektu dokumentu rządowego do zaopiniowania przez organ państwowy, jeżeli projekt dotyczy zakresu jego działania. Bez wątpienia – stosownie do wskazanych przepisów RODO i u.o.d.o. – w zakresie materii związanej z ochroną danych osobowych takim organem jest Prezes Urzędu Ochrony Danych Osobowych.

Mimo istnienia przywołanego prawnego obowiązku organ nadzorczy w praktyce jest nadal w niektórych przypadkach pomijany w procesie legislacyjnym, a wiele projektów dotyczących ochrony danych osobowych nie jest przedstawianych do jego oceny albo przedstawianych jest dopiero na etapie prac Rządowego Centrum Legislacji i to dzięki temu organowi Prezes Urzędu angażowany jest w proces legislacyjny. W przypadkach nieprzesłania projektu do zaopiniowania Prezes UODO zgłasza swoje uwagi z własnej inicjatywy, działając z urzędu w myśl konstytucyjnej

zasady legalizmu. Niemniej zjawisko to negatywnie oddziałuje na proces prawodawczy. Wielokrotnie projekty aktów prawnych nieprzedstawiane do oceny zawierają wiele uregulowań niezgodnych ze standardami przetwarzania danych osobowych, wynikającymi w szczególności z rozporządzenia ogólnego. Zgodnie z zasadą ochrony danych w fazie projektowania (*privacy by design*) wyrażoną w art. 25 ust. 1 RODO uwzględnienie ochrony danych osobowych powinno odbywać się na jak najwcześniejszym etapie planowania czy podejmowania decyzji o przetwarzaniu. Dotyczy to również procesu legislacyjnego[189]. Przedstawienie projektu do zaopiniowania dopiero na zaawansowanym etapie prac legislacyjnych powoduje znaczne komplikacje po stronie projektodawcy co do możliwości dalszej modyfikacji aktu, celem prawidłowego uwzględniania w regulacji aspektów przetwarzania danych osobowych. Wdrożenie uregulowań nieuwzględniających ochrony danych osobowych wpływa niekorzystnie nie tylko na zapewnienie niezbędnych i wymaganych na gruncie rozporządzenia ogólnego gwarancji dla osób, których dane dotyczą, ale również na wykonawców norm, przede wszystkim administratorów, którzy wobec regulacji niedostatecznych, wadliwych lub niezapewniających stosowania norm RODO pozostają w konfuzji, a często w niezgodności co do sposobu stosowania ustanowionego prawa.

Zauważalnym i wciąż częstym (w porównaniu z latami ubiegłymi) problemem jest brak prawidłowej identyfikacji materii danych osobowych w procesie legislacyjnym. Planując określone regulacje prawne, projektodawca na samym początku powinien rozważyć, jakie skutki w obszarze prywatności obywateli wywrze ich wdrożenie. Tymczasem ten aspekt często jest pomijany lub nie jest dostrzegane, że projektowane rozwiązania będą miały – często bardzo doniosłe – oddziaływanie również na kwestie związane z przetwarzaniem danych osobowych. Brak właściwego rozpoznania zależności pomiędzy projektowanym aktem a obszarem ochrony danych osobowych stwarza wysokie ryzyko wprowadzenia do obiegu prawnego norm naruszających zasady rozporządzenia ogólnego z dalece idącymi negatywnymi skutkami dla obywateli. Uwidacznia się to zarówno w odniesieniu do rozpoczynania procesów przetwarzania danych, ich trwania, jak i kończenia.

Jako przykład aktu, w którym projektodawca nie wyważył wpływu planowanych regulacji na prywatność osób, których dane dotyczą, wskazać należy **projekt ustawy o zmianie ustawy o ochronie zwierząt oraz zmianie niektórych innych ustaw**[190]. Zakłada on liczne regulacje materialno-prawne oraz systemowe dotyczące ochrony zwierząt. Projektodawca nie rozpoznał jednak, że wprowadzenie planowanych trzech rejestrów publicznych o nadzwyczaj szerokim zakresie gromadzonych danych będzie miało swoje wyjątkowo istotne implikacje w odniesieniu do praw i wolności osób, których dane osobowe będą w nich przetwarzane. Projekt zakładał obowiązek oznakowania wszystkich psów i kotów domowych oraz obligatoryjność wpisu ich posiadaczy do Centralnego Rejestru Zwierząt Oznakowanych. Biorąc pod uwagę

[189] Zob. Wytyczne Europejskiej Rady Ochrony Danych nr 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych”.
[190] DOL.401.470.2024.

szacowaną liczbę psów i kotów domowych w Polsce (ponad 12 mln), przetwarzanie danych osobowych miałoby zatem wymiar masowy. Mimo to wprowadzane regulacje w żadnym, choćby podstawowym, stopniu nie odnosiły się do potrzeb uczynienia zadość standardom rozporządzenia 2016/679, stwarzając wiele fundamentalnych ryzyk dla konstytucyjnego prawa do prywatności. Ponadto mimo daleko idącej ingerencji w sferę ochrony danych osobowych, projekt ustawy nie został przedstawiony do oceny Prezesa UODO – opinia została sporządzona i przedstawiona parlamentowi przez organ nadzorczy z własnej inicjatywy.

Za inny przykład tworzonego aktu, w którym projektodawca nie zidentyfikował prawidłowo kwestii związanych z ochroną danych osobowych, może posłużyć **projekt ustawy o wspieraniu rodziców w aktywności zawodowej oraz w wychowaniu dziecka – „Aktywny rodzic”**[191]. Przewidywał on wiele szczegółowych rozwiązań określających warunki nabywania prawa do świadczeń wspierających rodziców w aktywności zawodowej oraz w wychowaniu dziecka, które ściśle wiążą się z przetwarzaniem danych osobowych przez organy publiczne na szeroką skalę, w tym danych szczególnych kategorii oraz pochodzących (uzyskanych, weryfikowanych, wprowadzanych) z rejestrów publicznych. Brak uwzględnienia aspektów związanych z ochroną danych osobowych spowodował liczne istotne konsekwencje i zagrożenia. W swojej opinii Prezes UODO zwrócił uwagę przede wszystkim na brak przeprowadzenia testu prywatności, brak wskazania w ustawie źródeł pochodzenia danych, konstruowanie nieprecyzyjnych norm i otwartych katalogów danych, niezdefiniowanie podmiotów odpowiedzialnych za przetwarzanie danych, brak okresów retencji, korzystanie przez organy ustalające lub weryfikujące prawo do świadczenia z nieokreślonych rejestrów publicznych, blankietowość rozwiązań związanych z wymianą danych. Projekt został przedstawiony do oceny organowi nadzorczemu dopiero na etapie prac parlamentarnych. Do uwag Prezesa UODO nie odniesiono się. Ustawa została uchwalona.

Wynikiem inicjatywy własnej organu nadzorczego była opinia do **projektu ustawy o zmianie ustawy o Krajowej Administracji Skarbowej**[192]**, względem której ustawodawca nie ustosunkował się w toku trwającego procesu legislacyjnego.** Pilna konieczność zmian regulacji związanych z ustawą o KAS była równolegle przedmiotem **wystąpienia Prezesa UODO** (w trybie art. 52 ust. 2 ustawy o ochronie danych osobowych) **skierowanego do Ministra Finansów**[193]. Organ nadzorczy wskazał na wyjątkowo szeroki zakres kompetencji organów skarbowych w zakresie przetwarzania danych osobowych (w tym danych szczególnych kategorii, również poprzez profilowanie i zautomatyzowane podejmowanie decyzji) oraz na sposób sformułowania podstaw przetwarzania budzący poważne wątpliwości w świetle art. 51 Konstytucji RP (prawo do autonomii informacyjnej jednostki) oraz

[191] DOL.401.169.2024.
[192] DOL.401.298.2024.
[193] DOL.413.5.2024.

orzecznictwa międzynarodowego[194]. Minister Finansów, udzielając odpowiedzi na wystąpienie, nie przychylił się do postulatów Prezesa UODO.

Także **projekt ustawy o Krajowej Sieci Kardiologicznej**[195] nie został przedstawiony do zaopiniowania Prezesowi UODO, mimo że wykonywanie przepisów projektowanej ustawy nierozerwalnie związane byłoby z przetwarzaniem danych osobowych, w tym danych dotyczących zdrowia (a więc danych szczególnych kategorii). Efektem braku uwzględnienia przez projektodawcę aspektów związanych z ochroną danych osobowych było nie tylko niedostateczne określenie celów, do jakich służyć ma wprowadzenie elektronicznej Karty Opieki Kardiologicznej (dotyczącej diagnostyki i leczenia kardiologicznego), w sposób nieodpowiadający zasadom zgodności z prawem, rzetelności i przejrzystości, ale także dalsze niedoskonałe ukształtowanie regulacji odnoszących się m.in. do przypisania ról administratora, zasad wymiany informacji za pośrednictwem systemów teleinformatycznych lub systemów łączności, niedookreślenie zakresu przetwarzanych danych oraz nadmiarowe wykorzystywanie numerów PESEL pracowników personelu medycznego. Uwagi organu nadzorczego nie zostały w pełni uwzględnione.

Projekt ustawy o zmianie ustawy o odnawialnych źródłach energii oraz niektórych innych ustaw[196] został przekazany do zaopiniowania dopiero na etapie prac parlamentarnych. Organ nadzorczy zwrócił wówczas uwagę na istotne pominięcie zasad hierarchii aktów prawnych i podkreślił konieczność uregulowania na poziomie ustawy (nie zaś aktu wykonawczego) wzoru sprawozdania potwierdzającego wykonanie obowiązku ograniczenia emisji gazów cieplarnianych lub poprawy efektywności energetycznej – z uwagi na fakt, że dokumenty dołączone do niego zawierać będą dane osobowe. Do przedstawionych uwag projektodawca się nie odniósł. Ustawa została uchwalona.

Brak należytego zastosowania zasady ochrony danych w fazie projektowania uwidoczniony został także w toku prac nad **projektem ustawy o rynku kryptoaktywów**[197]. Mimo że regulowana nim materia dotyczy złożonych relacji pomiędzy uczestnikami obrotu kryptoaktywami, w tym przetwarzania danych osobowych na dużą skalę oraz przekazywania informacji do państw trzecich, projekt nie uwzględnił choćby kierunkowych mechanizmów zarządzania ochroną danych osobowych. Na potrzebę szerszej refleksji nad zapewnieniem zgodności przetwarzanych danych osobowych za pomocą bazowej technologii kryptoaktywów (tj. technologii blockchain i technologii rozproszonego rejestru) z obowiązującymi przepisami i zasadami ochrony danych zwrócił uwagę również Europejski Inspektor Ochrony Danych[198]. Część uwag została uwzględniona przez projektodawcę, proces legislacyjny pozostaje w toku.

---

[194] Zob. wyrok Trybunału Sprawiedliwości UE z 24 lutego 2022 r. w sprawie C-175/20 SS” SIA przeciwko Valsts ieņēmumu dienests.
[195] DOL.401.454.2024.
[196] DOL.401.451.2024.
[197] DOL.401.61.2024.
[198] Zob. opinia EIOD nr 9/2021 w sprawie wniosku dotyczącego rozporządzenia w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937.

Brak uwzględnienia w procesach tworzenia prawa należytych standardów ochrony danych osobowych odbija się w sposób negatywny na jakości stanowionych aktów. Niepokojącym zjawiskiem jest zarówno utrzymująca się nieświadomość projektodawców co do konieczności konsultowania z organem ochrony danych wymagających tego projektów, jak i pomijanie przedstawionych przez niego postulatów, w szczególności w obszarach, które wiążą się z aspektami tak istotnymi, czy wręcz fundamentalnymi jak konstytucyjne zasady hierarchii aktów prawa, przetwarzanie danych sensytywnych, operacje przetwarzania o charakterze masowym, za pośrednictwem rozbudowanych systemów teleinformatycznych czy dotyczących dzieci. Taki stan rzeczy może wiązać się ze szczególnie dotkliwymi konsekwencjami w toku wdrażania i stosowania prawa. Pozytywnie należy odnieść się natomiast do faktu, że w niektórych przypadkach komentarze Prezesa Urzędu są jednak brane pod uwagę na dalszych etapach prac nad projektem i przynajmniej częściowo uwzględniane.

6.2. Ocena skutków dla ochrony danych osobowych w procesie legislacyjnym

Powtarzającym się problemem, dotyczącym zasadniczej części opiniowanych aktów, a mającym kluczowe znaczenie dla prawidłowego stosowania regulacji prawnych dotyczących przetwarzania danych osobowych, jest brak przeprowadzenia oceny skutków dla ochrony danych (Data Protection Impact Assessment – DPIA) jako elementu tzw. testu prywatności. Obecnie ocena skutków w praktyce jest często pomijana, co powoduje negatywne konsekwencje zarówno w odniesieniu do przyszłych wykonawców norm oraz osób, których dane dotyczą, jak i jakości samego procesu prawodawczego. Artykuł 35 ust. 1 RODO stanowi, że w przypadku, 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, dokonać należy oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Z kolei z treści art. 35 ust. 10 RODO wnioskować należy, że ocena ta powinna zostać przeprowadzona w związku z przyjęciem regulacji prawnej państwa członkowskiego – jeżeli przetwarzanie ma odbywać się ze względu na konieczność realizacji ważnego interesu publicznego lub niezbędność dla realizacji obowiązku prawnego administratora – już na etapie tworzenia tej regulacji.

Test prywatności nie jest jedynie obowiązkiem prawnym projektodawcy, ale jest również środkiem kluczowym dla zapewnienia dbałości o poszanowanie prawa do prywatności oraz autonomii informacyjnej w procesie legislacyjnym. Przeprowadzenie przez projektodawcę oceny projektowanych rozwiązań poprzez pryzmat zagrożeń dla prywatności podmiotów danych pozwala na identyfikację i mitygację ryzyk związanych z proponowanym w przepisach przetwarzaniem danych osobowych. Prawidłowo przeprowadzony test prywatności umożliwia wyważenie celów (*ratio legis*) projektowanej regulacji z prawami i wolnościami jednostki. Projektodawca powinien dążyć do zachowania proporcjonalności ingerencji w prawa podmiotów danych

i przyjmować jedynie takie rozwiązania, które są realnie niezbędne dla wypełnienia ważnego zadania realizowanego w interesie publicznym, przewidując jednocześnie środki ochrony praw podstawowych, wolności i interesów podmiotów danych.

Niestety, w wielu przypadkach test prywatności jest często pomijany, także w przypadku projektów dotyczących wielkich rejestrów publicznych czy przetwarzania danych z użyciem nowych technologii. Konieczność implementacji testu prywatności do projektowanych rozwiązań prawnych jest przez organ nadzorczy niezmiennie i stale podnoszona. Pozytywnie należy ocenić, że część resortów dostrzega wagę instrumentu, jakim jest DPIA, a ocena taka jest czasem przeprowadzana po zwróceniu na ten aspekt uwagi przez organ nadzorczy w toku opiniowania. Wciąż jednak w wielu przypadkach DPIA nie jest przeprowadzana w ogóle albo jest sporządzana w sposób pobieżny, fragmentaryczny, bez rzeczywistego odniesienia do treści przepisów. Test prywatności nie powinien być w tym kontekście traktowany jako czysto formalny obowiązek, ale jako integralne narzędzie stanowiące punkt odniesienia dla tworzonych przepisów, pozwalające na dostosowanie tworzonego aktu do standardów ochrony danych osobowych oraz prawa do prywatności.

Nadal zatem w 2024 roku, podobnie jak w latach ubiegłych, Prezes UODO, opiniując projekty aktów prawnych, zwłaszcza ustaw, powoływał istotny aspekt, jakim jest przeprowadzenie w toku procesu legislacyjnego testu prywatności, w tym oceny skutków projektowanych przepisów dla przetwarzania danych osobowych, celem wykonania *ratio legis* planowanych regulacji.

Przykładem niech będzie **projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem operacyjnej odporności cyfrowej sektora finansowego**[199], mający na celu implementację do polskiego systemu prawnego rozporządzenia 2022/2554 (DORA) dotyczącego rozwoju technologii finansowych, ujednoliconych norm bezpieczeństwa cyfrowego w sektorze finansowym, wymiany informacji o cyberzagrożeniach, zasad zarządzania ryzykiem ICT oraz zabezpieczenia przez instytucje finansowe systemów sieciowych i informatycznych. Pomimo wagi regulowanych materii, szerokiego zakresu przetwarzania danych oraz wdrożenia nowego rodzajowo systemu teleinformatycznego, projektodawca nie przeprowadził wysoce zasadnego testu prywatności. W związku z powyższym pominięte w projekcie zostały podstawowe warunki funkcjonowania nowego systemu, sposoby przekazywania danych, zakres i czas przetwarzania czy określenie podmiotów upoważnionych do korzystania z systemu. W opinii Prezes UODO podniósł także kwestie związane z czasem retencji przekraczającym okres dopuszczalny przez rozporządzenie DORA, nieprecyzyjność norm dotyczących przekazywania informacji przez Komisję Nadzoru Finansowego czy też brak przepisów odnoszących się do anonimizowania danych osobowych.

Innym przykładem regulacji, w której test prywatności został pominięty z negatywnymi skutkami dla jej kształtu, był **projekt ustawy o bonie senioralnym**[200], przewidujący wiele unormowań określających warunki nabywania prawa do usług

[199] DOL.401.141.2024.
[200] DOL.401.405.2024.

wsparcia dla rodzin w opiece nad wstępnym seniorem. Rozwiązania te ściśle wiążą się z przetwarzaniem danych osobowych przez organy publiczne upoważnione do realizacji obowiązków nałożonych na nie mocą projektowanych przepisów, w tym także z przetwarzaniem szczególnych kategorii danych osobowych dotyczących zdrowia, na dużą skalę. W opinii wskazano na nadmierny zakres przetwarzania danych osobowych, wątpliwości związane z przepływem danych, a także z przyjętym modelem powszechnej dostępności wykazu, w którym mogą być publikowane informacje identyfikujące przedsiębiorcę (osobę fizyczną prowadzącą działalność gospodarczą), jak również na brak prawidłowego określenia celu przyjmowanych rozwiązań oraz ich korelacji z koniecznością zapewnienia gwarancji wykonywania praw podmiotów danych.

W przypadku **projektu ustawy o zmianie ustawy o narodowym zasobie archiwalnym i archiwach**[201] projektodawca również nie przeprowadził wymaganej oceny skutków. Projekt miał na celu nadanie waloru prawnego, równoważnego oryginałom dokumentów, niektórym odwzorowaniom cyfrowym wykonanym dla dokumentów tradycyjnych (sporządzonych w postaci innej niż elektroniczna). Projektowane przepisy odnosiły się zatem do przetwarzania danych osobowych zawartych w dokumentach elektronicznych, przy użyciu nowych technologii, na szeroką skalę, a co istotne przetwarzanie to mogło dotyczyć różnych kategorii danych, w tym danych podlegających szczególnemu reżimowi przetwarzania (np. danych dotyczących zdrowia, danych dotyczących karalności). Efektem braku przeprowadzenia testu prywatności były liczne luki regulacyjne mające negatywne oddziaływanie na sferę ochrony danych osobowych. Nie przeprowadzono bowiem oceny zaprojektowanych regulacji pod względem zapewnienia właściwej podstawy prawnej dla funkcjonowania systemu teleinformatycznego, nie przewidziano szczegółowych rozwiązań gwarantujących bezpieczeństwo (w tym cyberbezpieczeństwo), integralność i poufność przetwarzanych informacji, nie ustalono standardów wymiany i udostępniania informacji, zabezpieczeń przed stosowaniem niedozwolonego monitoringu pracowników (osób użytkujących system), procedur identyfikacji zagrożeń, mechanizmów odzyskiwania danych czy też regulacji prawidłowo kształtujących sposób, zakres, formę partycypacji i odpowiedzialność poszczególnych podmiotów w procesach przetwarzania danych w systemie. Projekt nie został również przedstawiony organowi nadzorczemu do zaopiniowania.

Projekt ustawy o zmianie niektórych ustaw w celu deregulacji prawa gospodarczego i administracyjnego oraz doskonalenia zasad opracowywania prawa gospodarczego[202] zakładał m.in. zmiany w Kodeksie postępowania administracyjnego wprowadzające możliwość sprawdzenia przez organ administracji publicznej umocowania pełnomocników na podstawie publicznego wykazu, ewidencji lub innego rejestru dostępnego drogą elektroniczną. W opinii Prezes UODO podniósł, że przepisy wdrażające tego rodzaju rozwiązania powinny szczegółowo określać procedurę, formę, zakres i tryb udostępniania danych osobowych. Zwrócił także uwagę

[201] DOL.401.392.2024.
[202] DOL.401.121.2024.

na ryzyka wynikające ze zbyt szerokiego dostępu organów do danych osobowych pełnomocników. Odniósł się także do innych projektowanych zmian, które dotyczyły ustawy Prawo zamówień publicznych. Przewidywały możliwość przeprowadzenia rozpraw lub posiedzeń jawnych na odległość przy użyciu urządzeń technicznych. Zapis obrazu i dźwięku z czynności procesowych odbywających się na sali rozpraw oznacza m.in. przetwarzanie danych osobowych. Proces ten powinien odbywać się więc z poszanowaniem zasad i standardów wynikających z rozporządzenia 2016/679. Przekazywanie tego rodzaju zapisu, ze względu na ryzyko dla naruszenia praw lub wolności osób fizycznych, powinno odbywać się przy zachowaniu najwyższych standardów technicznych, które jednak nie zostały określone w projekcie. Przeprowadzenie testu prywatności w tym przypadku pozwoliłby na dokonanie analizy ryzyk rozwiązań proponowanych w zakresie przetwarzania danych osobowych oraz wypracowanie stosownych rozwiązań je niwelujących. Uwagi organu nadzorczego zostały uwzględnione jedynie w części.

Prezes UODO stale podkreśla, że szczególnej roztropności i staranności wymaga tworzenie regulacji dotyczących przetwarzania danych osób małoletnich, czego wyrazem były m.in. uwagi do **projektu ustawy o zmianie ustawy o systemie oświaty oraz niektórych innych ustaw**[203], wprowadzającego wiele zmian w systemach służących do przeprowadzania egzaminów uczniów oraz wspomagających edukację, w tym z wykorzystaniem wielkoskalowych systemów teleinformatycznych. Ze względu na skalę przetwarzania, ale także jego kontekst oraz wysokie ryzyko naruszenia praw i wolności, w tym osób małoletnich, ocena skutków powinna być traktowana priorytetowo, szczególnie że projekt zakłada inwazyjne formy przetwarzania danych osobowych, w tym danych wrażliwych, takie jak chociażby wykorzystywanie „odpowiedniego sprzętu specjalistycznego" i aplikacji mobilnej służących do monitorowania stanu zdrowia zdającego. Jednocześnie projektodawca nie wykazał niezbędności stosowania takich metod przetwarzania danych osobowych ani nie określił podstawowych warunków takiego przetwarzania, w tym zasad retencji czy administrowania przetwarzanymi danymi. Projektodawca nie wskazał również podmiotu odpowiedzialnego za ocenę stanu zdrowia osoby podlegającej temu monitoringowi oraz sposobu rozstrzygnięcia kolizji z przepisami ustawy o opiece zdrowotnej nad uczniami, w której jasno zostało określone, że badanie stanu zdrowia ucznia należy do podmiotów sprawujących opiekę zdrowotną nad uczniami, a nie do dyrektora szkoły czy komisji egzaminacyjnej. Projektodawca częściowo uwzględnił uwagi Prezesa UODO i zadeklarował przeprowadzenie oceny skutków na dalszym etapie prac legislacyjnych.

Ocena skutków jest równie istotna w przypadku wdrażania procesów przetwarzania z wykorzystaniem nowych technologii, na co zwrócono uwagę w opinii do **projektu uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"**[204], określającej kryteria klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług

[203] DOL.401.294.2024.
[204] DOL.401.181.2024.

przetwarzania w Rządowej Chmurze Obliczeniowej (RChO) lub w Publicznych Chmurach Obliczeniowych (PChO). W wyniku projektowanych zmian w tychże chmurach obliczeniowych mogłyby funkcjonować wszystkie systemy teleinformatyczne administracji rządowej, z wyłączeniem systemów, w których są przetwarzane informacje niejawne. Biorąc pod uwagę wysoce newralgiczny charakter danych przetwarzanych w tych systemach, organ nadzorczy wskazał na konieczność przeprowadzenia testu prywatności, który pozwoliłoby wykazać, czy faktycznie zmiany projektowanej uchwały zwiększą poziom cyberbezpieczeństwa i ochrony danych przetwarzanych w państwowych chmurach obliczeniowych, bez wpływu na ryzyko naruszenia danych zwykłych i szczególnych kategorii przetwarzanych przez administrację publiczną. Projektodawca uwzględnił uwagi organu nadzorczego i zobowiązał się do przeprowadzenia DPIA.

Na nieco inny aspekt realizacji dyspozycji wynikającej z art. 35 ust. 1 rozporządzenia 2016/679 powołano się w opinii do **projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa**[205], wprowadzającym procedurę certyfikacji produktów, usług i procesów ICT. Organ nadzorczy zwrócił uwagę, że rozporządzenie 2016/679 znajdzie zastosowanie do oceny procesów związanych z przetwarzaniem danych osobowych i administratorzy ubiegający się o uzyskanie certyfikatu są zobowiązani do stosowania przepisów o ochronie danych osobowych, w tym do przeprowadzenia oceny skutków dla ochrony danych.

Bardzo dobrym, choć rzadkim, przykładem pozytywnych działań projektodawcy było **podjęcie inicjatywy i dokonanie oceny skutków projektowanych regulacji dla ochrony danych na etapie koncepcyjnych prac resortu**, a następnie jej przedłożenie organowi wraz z **projektem ustawy o zmianie ustawy o ochronie praw nabywcy lokalu mieszkalnego lub domu jednorodzinnego oraz Deweloperskim Funduszu Gwarancyjnym oraz niektórych innych ustaw**[206]. Przeanalizowanie przez projektodawcę poszczególnych zagrożeń i dokonanie oceny ich wpływu na przetwarzane dane osobowe w ramach funkcjonowania tworzonego mocą projektowanych przepisów Portalu Danych o Obrocie Mieszkaniami (DOM) pozwoli przyszłemu administratorowi na zminimalizowanie zidentyfikowanych ryzyk i wdrożenie odpowiednich środków niezbędnych dla zapewnienia bezpieczeństwa danych przetwarzanych w obrocie elektronicznym.

Organ nadzorczy zwrócił jednak uwagę, że realizacji celu regulacji, jakim jest zwiększenie przejrzystości rynku nieruchomości, a w rezultacie opracowanie i udostępnienie statystyk dotyczących cen transakcyjnych na rynku mieszkaniowym, liczby transakcji czy informacji statystycznych dotyczących uczestników tego obrotu, powinna towarzyszyć dodatkowa ocena skutków pod względem ochrony danych osobowych, tym bardziej że przewidywany model przetwarzania zakłada bardzo szerokie wykorzystywanie numerów PESEL.

[205] DOL.401.185.2024.
[206] DOL.401.361.2024.

Innym dobrym przykładem postępowania projektodawcy było przeprowadzenie oceny skutków dla ochrony danych i w oparciu o nią wypracowanie rozwiązań zmieniających dotychczasową treść projektowanych przepisów. W **projekcie ustawy o zawodzie psychologa oraz samorządzie zawodowym psychologów**[207] projektodawca – na skutek istotnego wsparcia przez organ nadzorczy, zarówno w opinii legislacyjnej, jak i w ustaleniach roboczych – uporządkował sposoby przetwarzania danych osobowych w sposób przejrzysty, rzetelny i eliminujący wątpliwości interpretacyjne wykonawców norm oraz podmiotów danych.

Usystematyzowanie materii dotyczącej wykonywania zawodu psychologa zgodnie z proponowanymi rozwiązaniami związane jest z przetwarzaniem danych osobowych, w tym danych szczególnych kategorii (np. danych dotyczących zdrowia, seksualności lub orientacji seksualnej, przekonań religijnych lub światopoglądowych) oraz danych dotyczących karalności, podlegających na podstawie przepisów dotyczących przetwarzania danych osobowych wzmocnionemu reżimowi ochrony. Z tego względu szczególnie istotną kwestią jest zapewnienie zgodności procesów przetwarzania danych regulowanych projektowaną ustawą z rozporządzeniem 2016/679 poprzez dokonanie przez prawodawcę oceny skutków dla ochrony danych. W toku dalszych prac nad projektem projektodawca uwzględnił zdecydowaną większość z przedstawionych uwag, w tym także przeprowadził ocenę skutków dla ochrony danych. Przyczyniło się to do ustalenia regulacji uwzględniającej standardy przetwarzania i ochrony danych osobowych w związku z wykonywaniem zawodu psychologa i w zakresie świadczonych przez niego usług oraz przepisów kształtujących organizację samorządu zawodowego i uprawnienia organów samorządu.

Zasadnicza większość projektów opiniowanych przez Prezesa UODO w roku 2024 nie została jednak wsparta testem prywatności, w tym oceną skutków dla ochrony danych, często pomimo wyraźnych wskazań do konieczności objęcia danej regulacji testem prywatności, a nawet po zwróceniu uwagi na taką powinność przez organ nadzorczy.

Uzasadnione obawy budzi brak uwzględniania tego aspektu w tak istotnych sferach, jak: bezpieczeństwo cyfrowe, przetwarzanie danych w ekstensywnych rejestrach elektronicznych, przy użyciu nowych technologii, usług chmurowych oraz przetwarzanie danych wrażliwych, dotyczących dzieci czy osób starszych.

Nie można tracić z pola widzenia, że w wyniku uwag skierowanych przez Prezesa Urzędu Ochrony Danych Osobowych ocena skutków w niektórych przypadkach była jednak uzupełniania przez projektodawców, co stanowi wciąż rzadki, aczkolwiek pozytywny przykład działań projektodawców.

6.3. Zasada praworządności, zasada legalności

Kwestie materialno-prawne dotyczące praw i obowiązków związanych z przetwarzaniem danych osobowych, zakresu gromadzenia i udostępniania danych

[207] DOL.401.255.2024.

oraz reguł ich przetwarzania mogą być regulowane jedynie przez akt o randze ustawowej. Zasada ta wynika wprost z norm konstytucyjnych. Art. 51 ust. 1 i 2 Konstytucji RP stanowi, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do udostępnienia informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Zgodnie z art. 31 ust. 3 Konstytucji RP ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanowione jedynie w drodze ustawy i tylko przy zachowaniu wyszczególnionych kryteriów konieczności w zgodzie z istotą demokratycznego państwa prawa. Wdrażane przepisy wiążące się z ograniczeniem praw i wolności wynikających z przetwarzania danych osobowych, w szczególności z ich pozyskiwaniem i udostępnianiem, mogą być regulowane w przepisach wyłącznie rangi ustawowej[208].

Praktyka uwidacznia niemalejący w 2024 r. (w stosunku do lat ubiegłych) problem z przenoszeniem przez projektodawców zagadnień związanych z ustaleniem prawnych podstaw pozyskiwania, gromadzenia i udostępnianiem danych osobowych do aktów wykonawczych (rozporządzeń). Nadal obserwowane jest też niepokojące zjawisko – pozostawianie regulowania powyższych kwestii porozumieniom, umowom, aktom wewnętrznym, zarządzeniom, wytycznym czy innego rodzaju instrumentom prawnym o niedookreślonej formie, pozbawionym waloru powszechnie obowiązującego prawa. Taka praktyka stoi w sprzeczności również z normami rozporządzenia 2016/679, które w art. 6 ust. 3 wymienia kryteria legalności, jakie muszą zostać spełnione w przypadku podstawy przetwarzania określonej w art. 6 ust. 1 lit. c i lit. e, czyli dla przetwarzania danych osobowych w oparciu o prawny obowiązek ciążący na administratorze lub przetwarzania w ramach sprawowania władzy publicznej. Organ nadzorczy w kierowanych w 2024 r. opiniach wielokrotnie – podobnie jak w latach ubiegłych – wskazywał, że na projektodawcy ciąży obowiązek uczynienia zadość uregulowaniom RODO, w tym przede wszystkim zasadom określonym w art. 5 i elementom z art. 6 ust. 3, a w przypadku danych zakwalifikowanych do szczególnych kategorii – warunkom przewidzianym w art. 9 ust. 2 i art. 10. Wprowadzanie do porządku prawnego praw i obowiązków w sferze przetwarzania danych osobowych – związanych wszak z ograniczaniem praw i wolności konstytucyjnych podmiotów danych osobowych oraz z nadawaniem szczególnych uprawnień podmiotom przetwarzającym dane osobowe, w tym szczególnych kategorii lub korzystającym z nowych technologii – musi opierać się na konkretnej normie prawnej, która w sposób wyczerpujący, precyzyjny i jasny zarówno dla odbiorcy dyspozycji, jak i dla podmiotów danych, określi, w jakim zakresie przetwarzanie jest legalne, a w jakim jest ono niedozwolone.

Zagadnieniem fundamentalnym dla sformułowania prawnych podstaw i reguł przetwarzania jest określenie przez projektowaną ustawę celów przetwarzania. Nie mogą być one domniemywane, zwłaszcza w przypadku przetwarzania danych przez

[208] Zob. wyroki Trybunału Konstytucyjnego z 18 grudnia 2014 r. sygn. akt K 33/13, z 19 maja 1998 r. sygn. akt U 5/97, z 30 lipca 2014 r. sygn. akt K 23/11 oraz z 19 lutego 2002 r. sygn. akt U 3/01, a także: wyrok TSUE z 2 marca 2021 r. (warunki dostępu do danych dotyczących łączności elektronicznej), sygn. C-746/18.

podmioty publiczne lub w interesie publicznym. Powinny zostać sformułowane w sposób wyczerpujący w relacji do potrzeb *ratio legis* regulacji. W gestii projektodawcy jest wykazanie proporcjonalności przetwarzania dla realizacji zadania realizowanego w interesie publicznym, tj. tego, dlaczego taki akurat model przetwarzania uznano za niezbędny i adekwatny oraz z jakich przyczyn cel regulacji nie może zostać zrealizowany przez inne środki o charakterze mniej ingerującym w prawa i wolności podmiotów danych, zwłaszcza ich prywatność i autonomię informacyjną.

Za przykład niech posłuży **projekt ustawy o zmianie ustawy o wspieraniu rodziny i systemie pieczy zastępczej**[209] zakładający wdrożenie systemu teleinformatycznego umożliwiającego sądom dostęp do danych z Centralnego Rejestru Pieczy Zastępczej. Projektodawca, pomimo stworzenia przepisu kompetencyjnego dla Ministra Sprawiedliwości stanowiącego, że zapewnia on sądom dostęp do systemu teleinformatycznego, nie określił jednak celów i warunków przetwarzania danych osobowych zarówno przez ten organ, jak i przez sądy. Przede wszystkim nie określono celów i sposobów udostępniania danych, czyniąc projektowane przepisy blankietowymi.

Analogiczną argumentację przedstawiono w opinii do **projektu ustawy o Krajowym Rejestrze Osób Pełniących Niektóre Funkcje Publiczne**[210], który zakładał powstanie nowego, co do zasady jawnego rejestru publicznego zawierającego ogromną ilość danych różnych osób (nie tylko osób publicznych, ale również osób trzecich) i wykorzystywanego przez nieokreśloną liczbę osób/podmiotów. Dane zgromadzone w rejestrze miałyby być do niego wprowadzane, udostępniane i wykorzystywane przez kolejne podmioty/organy/osoby w różnych celach, także z użyciem nowych technologii. W przestrzeni publicznej dane te funkcjonowałyby również jako informacje związane z danymi na temat rodziny określonej osoby czy powiązań pomiędzy osobami sprawującymi określone funkcje, także po zakończeniu pełnienia przez nie funkcji publicznej. Mimo to projekt nie sprecyzował dostatecznie celu prowadzenia rejestru, odwołując się jedynie hasłowo do zapewnienia transparentności życia publicznego. Organ nadzorczy podniósł, że z punktu widzenia ingerencji w autonomię informacyjną jednostki i gromadzenia danych w sposób scentralizowany, cele przetwarzania danych osobowych powinny zostać precyzyjnie określone w przepisach rangi ustawy. Zwrócił też uwagę na zbyt dużą ogólność i brak wymaganej precyzyjności norm w zaproponowanym modelu powszechnej dostępności.

Z kolei **projekt ustawy o ochronie ludności i obronie cywilnej**[211] przewidywał, że w celu zapewnienia wykonania zadań ochrony ludności lub obrony cywilnej, poszczególne organy mogą wydawać decyzje lub zawierać porozumienia o współpracy w wykonywaniu zadań, nie wykluczając, że w drodze takich

[209] DOL.401.486.2024.
[210] DOL.401.68.2024.
[211] DOL.401.221.2024.

instrumentów prawnych będą określane również cele i warunki przetwarzania danych o charakterze osobowym, potencjalnie także danych, o których mowa w art. 9 ust. 1 i art. 10 RODO. Jednocześnie nie określono jasnych granic ról i odpowiedzialności poszczególnych podmiotów biorących udział w procesach przetwarzania. Projektodawca, przewidując, że dane z Centralnej Ewidencji Obiektów Zbiorowej Ochrony będą mogły być udostępniane innym podmiotom, nie ustanowił jednak szczegółowego trybu, warunków i powodów kwalifikujących faktyczną zasadność udostępniania czy też środków kontroli tego procesu. Projektodawca nie uzasadnił proponowanego rozwiązania.

Podobne wątpliwości wzbudził **projekt ustawy o zmianie ustawy o obrocie towarami, technologiami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa oraz ustawy o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym**[212] wprowadzający normę, według której minister właściwy do spraw gospodarki może powierzyć określonym instytutom realizację niektórych zadań związanych z utrzymaniem i rozwojem wprowadzanego projektem ustawy systemu teleinformatycznego w drodze niedookreślonego porozumienia. Jednocześnie w uzasadnieniu do projektu wskazano, że w tym zakresie „zdecydowano się na pozostawienie pełnej swobody we wskazaniu konkretnych zadań powierzonych Instytutowi badawczemu". Organ nadzorczy wyraźnie zwrócił uwagę, że prawa i obowiązki związane z przetwarzaniem danych osobowych, zwłaszcza realizowane przez podmioty publiczne, powinny być odpowiednio i wyczerpująco unormowane w przepisach powszechnie obowiązującego prawa, nie zaś w dokumencie pozaustawowym, jak „porozumienie", natomiast powierzenie przetwarzania danych (w myśl art. 28 RODO), z uwagi na zasadę legalizmu i konstytucyjną zasadę praworządności, również wymaga umocowania w ustawie.

Projekt ustawy o unijnej sieci danych dotyczących poziomu zrównoważenia gospodarstw rolnych[213] przewidywał pozyskiwanie danych z gospodarstw rolnych i przekazywanie ich między wojewódzkimi ośrodkami doradztwa rolniczego a agencjami łącznikowymi na podstawie „umowy". Organ nadzorczy podniósł, że z przepisów powszechnie obowiązującego prawa powinno wynikać, a nie z „umowy", jakie obowiązki związane ze zbieraniem danych realizowane są przez podmioty publiczne. Dane osobowe muszą być przetwarzane z poszanowaniem zasad zgodności z prawem, rzetelności i przejrzystości wynikających z art. 5 ust. 1 lit. a) RODO, a także z konstytucyjnej zasady legalizmu. Ponadto nie zostały określone sposoby zbierania i przekazywania danych osobowych, a projekt zakładał, że zakres zbieranych danych osobowych wynikał będzie z umów zawieranych pomiędzy podmiotami, a nie z samego aktu prawnego.

[212] DOL.401.381.2024.
[213] DOL.401.372.2024.

Zasadnicze wątpliwości organu nadzorczego w odniesieniu do przepisów **ustawy o ochronie małoletnich** wzbudził brak właściwych regulacji ustawowych realnie zapewniających standardy ochrony dzieci, efektem czego było skierowanie **wystąpienia do Ministra Sprawiedliwości z wnioskiem o podjęcie stosownych prac legislacyjnych**[214]. Zapewnienie bezpieczeństwa małoletnim poprzez wprowadzenie wysokich standardów ochrony prawnej wymaga zapewnienia równolegle szczególnych środków także w odniesieniu do ich danych osobowych (na co wskazuje także motyw 38 RODO). Tymczasem ustawa nie zapewnia odpowiedniej podstawy prawnej, a podejmowane przez prawodawcę działania prowadzą do zastąpienia jej wytycznymi, które nie mają charakteru norm powszechnie obowiązujących. Ustawodawca pozostawił kwestie związane z przetwarzaniem danych osobowych (w tym danych z art. 9 i 10 RODO) aktom wewnętrznym. Ponadto niedookreśloność przepisów odnoszących się do sfery praw podmiotów danych, w tym nieprecyzyjny zakres podmiotowy i przedmiotowy przepisów dotyczących przetwarzania danych osobowych, brak regulacji przewidujących okres przechowywania i gwarantujących bezpieczeństwo danych – budzi dodatkowe wątpliwości z punktu widzenia poszanowania zasady legalności, rzetelności i przejrzystości, wiążąc się z ryzykiem przetwarzania danych osobowych nadmiarowych, na zapas, a zatem niezgodnie z zasadami ograniczenia celu i minimalizacji danych. W odpowiedzi Ministerstwo Sprawiedliwości poinformowało, że wszczęte zostały prace nad projektem zmiany ustawy, które mają na celu również uczynienie zadość wymogom RODO[215].

Projekt rozporządzenia Prezesa Rady Ministrów zmieniającego rozporządzenie w sprawie pobierania i przekazywania obrazów linii papilarnych i materiału biologicznego oraz utrwalania i przekazywania wizerunku twarzy osoby niebędącej obywatelem Rzeczypospolitej Polskiej[216] zakładał gromadzenie i dalsze przetwarzanie przez policję informacji w formie zdjęć osób, w tym zdjęć sygnalitycznych w postaci elektronicznej w zbiorach danych opartych o system teleinformatyczny. Organ nadzorczy zwrócił uwagę na zbyt ogólny charakter regulacji oraz podniósł, że nie ustanawia ona żadnych sposobów i warunków przetwarzania danych, nie precyzuje zasad funkcjonowania rzeczonego systemu teleinformatycznego, nie stwarzając tym samym wystarczających gwarancji co do trafnego zakwalifikowana danych do odpowiednich, uporządkowanych struktur, pozostawiając znaczną dowolność wykonawcom norm w zakresie przetwarzania danych osobowych, jakimi są przedmiotowe zdjęcia i dane zawarte w opisach wizerunków. Co nie mniej istotne, przepis ustawy o działaniach antyterrorystycznych, stanowiący delegację ustawową do wydania projektowanego rozporządzenia, inne przepisy tej ustawy ani żadne inne przepisy rangi ustawowej nie dają podstawy

[214] DOL.413.9.2024; treść wystąpienia i jego omówienie dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3377.
[215] Projekt ustawy o zmianie ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich oraz niektórych innych ustaw wpłynął do zaopiniowania przez organ nadzorczy w 2025 r. (DPNT.401.128.2025).
[216] DOL.401.208.2024.

prawnej do stanowienia o tych systemach, których dotyczy projekt rozporządzenia. Mimo istotnych uwag dotyczących względów natury podstawowej, stanowisko organu nadzorczego nie zostało uwzględnione.

Inaczej projektodawca postąpił w przypadku **projektu rozporządzenia Rady Ministrów w sprawie ustanowienia Odznaki Honorowej za Zasługi dla Metrologii Rzeczypospolitej Polskiej, ustalenia jej wzoru oraz zasad i trybu nadawania i noszenia**[217]. Organ nadzorczy zwrócił uwagę, że projekt, zakładając wprowadzenie ewidencji osób wyróżnionych Odznaką, prowadzonej przez Główny Urząd Miar, wykracza poza materię ustawowej delegacji, a ewidencja, którą ustanawia projekt, będzie w istocie rejestrem publicznym w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne – zasady prowadzenia takiego rejestru powinny więc wynikać z ustawy. Ponadto projekt rozporządzenia nie ustanawia przynajmniej głównych zasad, na jakich działać ma system ewidencji, a więc w jakim środowisku techniczno-organizacyjnym ma być ona prowadzona, jakie są warunki dostępu do niej, zasady retencji oraz jakie środki, procedury, formy zabezpieczeń zostaną zastosowane dla zapewnienia prywatności i poufności danych. Tym razem jednak uwagi organu nadzorczego zostały uwzględnione w całości.

Odnosząc się do **projektu rozporządzenia zmieniającego rozporządzenie w sprawie programu pilotażowego w zakresie kompleksowej opieki nad świadczeniobiorcą z wczesnym zapaleniem stawów**[218] organ nadzorczy powielił postulaty wyrażone w wielu poprzednich stanowiskach dotyczące niedopuszczalności kształtowania w formie aktu podustawowego przepisów odnoszących się do podstawowych kwestii dotyczących procesu przetwarzania danych osobowych w związku z realizacją programów pilotażowych, szczególnie że procesy te dotyczą w znacznej mierze danych dotyczących zdrowia (danych szczególnych kategorii). Zaznaczono, że to w przepisach rangi ustawy – a nie rozporządzenia wykonawczego – projektodawca wprowadzić powinien odpowiednio i wyczerpująco skonstruowaną podstawę prawną dla określania obowiązku przetwarzania danych osobowych, a co równie istotne – określić cel i zakres niezbędnych dla wykonania tego celu, przetwarzanych danych, ich kategorii oraz określić sposoby przetwarzania danych adekwatnie do tych celów.

Powyższe przykłady stanowią nakreślenie istotnego problemu, jakim jest tworzenie nowych regulacji z pominięciem zasad praworządności oraz konstytucyjnego systemu źródeł praw i obowiązków. Przetwarzanie danych osobowych, szczególnie gdy odbywa się ono na masową skalę w rejestrach publicznych i systemach teleinformatycznych, gdy dotyczy danych szczególnej kategorii, danych dzieci, danych dotyczących karalności czy też danych upublicznianych, zarówno z punktu widzenia gwarancji wynikających z RODO, jak i – przede wszystkim - ustawy zasadniczej, powinno w każdym przypadku opierać się na konkretnie określonej normie wynikającej z aktu rangi ustawy. Mimo wagi

[217] DOL.401.386.2024.
[218] DOL.401.397.2024.

przedmiotowej problematyki uwagi Prezesa UODO dotyczące tego aspektu są wciąż zdecydowanie zbyt często pomijane, z negatywnymi skutkami zarówno z punktu widzenia przyszłych wykonawców norm, jak i niezbędnych gwarancji dla osób fizycznych, których dane dotyczą.

6.4. Rejestry publiczne i systemy teleinformatyczne

W ostatnim roku zauważyć można pogłębiającą się tendencję do wdrażania rozwiązań mających na celu przetwarzanie coraz większej ilości danych osobowych na dużą skalę w państwowych rejestrach i za pomocą systemów teleinformatycznych. Ze względu na kontekst, szeroki zakres przetwarzania oraz wysokie ryzyko naruszenia praw lub wolności osób fizycznych planowanie wdrożenia modeli operacji przetwarzania opartych o takie systemy wymaga szczególnej roztropności oraz dogłębnego i kompleksowego rozważenia pod względem czynienia zadość zasadom i gwarancjom określonym w RODO. Trendem szczególnie niebezpiecznym jest ustawiczne dążenie do budowania systemów opartych o łączenie baz danych lub swobodny dostęp do rejestrów w zakresie ich udostępniania innym podmiotom publicznym. W swoich opiniach legislacyjnych organ nadzorczy nieustannie przywołuje treść motywu 31 rozporządzenia ogólnego, zgodnie z którym łączenie zbiorów danych jest niedozwolone. Udostępnianie danych pomiędzy organami publicznymi nie powinno polegać na udzieleniu dowolnego, niekontrolowanego dostępu do całego rejestru czy zbioru danych, w trybie bezwnioskowym. Organ publiczny występujący z żądaniem udostępnienia danych obowiązany jest przestrzegać przepisów o ochronie danych osobowych. Udostępnienie danych powinno odbywać się w drodze skonkretyzowanego, uzasadnionego wniosku, ograniczonego jedynie do takich danych osobowych, które są realnie niezbędne do realizacji określonego zadania publicznego, z jednoczesnym poszanowaniem dla zasad ograniczenia celu i minimalizacji danych. Nieograniczony dostęp w trybie teletransmisji do rejestru należy uznać za niepożądany również ze względu na zasadę rozliczalności obowiązującą administratora, który jest odpowiedzialny za przetwarzanie danych w rejestrze. Przyjęcie stałego, bezwnioskowego dostępu do rejestru może skutkować brakiem realnej kontroli i nadzoru nad faktycznymi powodami pobrania danych z zasobu oraz nad tym, czy wykorzystywane są one zgodnie z celem ich uzyskania[219].

Równie niepokojąca jest tendencja do tworzenia modeli opartych o jawność lub powszechność dostępu do rejestrów publicznych w oderwaniu od zapewnienia kryteriów celowości czy konieczności takich rozwiązań, które ze swojej istoty stanowią poważną ingerencję w prawo do prywatności i autonomii informacyjnej jednostki. W przypadku zastosowania publicznego rejestru informacje te są wówczas dostępne dla potencjalnie nieograniczonej liczby osób, mogą być swobodnie przeglądane, przechowywane i rozpowszechniane, bez wpływu na słuszność czy zasadność celów takiego przetwarzania, a z punktu widzenia podmiotów danych iluzoryczna staje się

[219] Zob. wyrok Trybunału Sprawiedliwości UE z 1 października 2015 r. w sprawie C-201/14 Smaranda Bara i in., a także: wyrok Naczelnego Sądu Administracyjnego z 3 grudnia 2021 r., sygn. akt III OSK 590/21 dotyczący pozyskiwania danych z rejestru PESEL przez komorników sądowych.

możliwość podjęcia skutecznych środków obronnych przed niewłaściwym wykorzystaniem[220]. Organ nadzorczy podkreśla, że przyjęcie modelu jawności rejestru publicznego, w którym zawarte są dane osobowe, powinno być poprzedzone zarówno rzeczowym wykazaniem, z jakich względów taki model uznano za niezbędny, jak również wszechstronną i wnikliwą analizą szeregu ryzyk dla ochrony danych osobowych, w tym wiążących się z możliwością poddawania danych profilowaniu przez inne podmioty, czy też dalszego ich wykorzystania, w tym z zastosowaniem algorytmów AI.

Obrazowym przykładem powyższej problematyki jest **projekt ustawy o Krajowym Rejestrze Oznakowanych Psów i Kotów**[221], który zakładał obowiązek wpisania każdego właściciela psa lub kota w Polsce do powyższego rejestru. Według treści projektowanych przepisów dostęp do danych kontaktowych właściciela zwierzęcia zawartych w rejestrze mogłaby uzyskać dowolna osoba dysponująca numerem transpondera (chipa umieszczonego w zwierzęciu), w sposób dowolny i pozbawiony jakiejkolwiek kontroli. Jednocześnie projektodawca nie wyjaśnił w żaden sposób, jakiemu słusznemu celowi udzielanie tak szerokiego dostępu do rejestru osobom trzecim miałoby służyć. Ponadto projekt zapewniał wyszczególnionym podmiotom (gminom, policji, straży gminnej/miejskiej, prokuraturze, sądom, inspekcji weterynaryjnej, podmiotom prowadzącym schroniska) nadmiarowo szeroki dostęp do rejestru, poprzez użycie blankietowych sformułowań stwarzających niepożądane domniemywanie kompetencji podmiotów publicznych w przedmiocie przetwarzania danych osobowych, uwzględniając również możliwość swobodnego „przeszukiwania" rejestru. Organ nadzorczy podniósł, że osoba czy podmiot, która chce otrzymać dostęp do danych z rejestru, powinny wykazać co najmniej uzasadniony interes oraz racjonalną potrzebę ściśle związaną z *ratio legis* ustawy. Przed udostępnieniem danych administrator każdorazowo powinien rozpatrywać zasadność interesu osoby wnioskującej, jego podstawę prawną i czy dostęp ma charakter nadrzędny wobec interesów, praw i wolności osoby, której dane dotyczą, a projektodawca powinien ustanawiać staranne, precyzyjne i zawężające określenie granic udostępnienia danych oraz zamknięty katalog podmiotów, którym dane mogą być udostępnianie.

Jako kolejny przykład przytoczyć można **projekt ustawy o zmianie ustawy o szczególnych rozwiązaniach związanych z usuwaniem skutków powodzi oraz niektórych innych ustaw**[222]. Projektowane przepisy przyznawały marszałkowi województwa uprawnienie do pozyskiwania z rejestru PESEL, CEIDG oraz KRS danych w postaci elektronicznej, w sposób automatyczny, przy wykorzystaniu systemów teleinformatycznych prowadzonych przez ministra właściwego do spraw pracy „w celu realizacji zadań ustawowych". Posługując się tak wysoce blankietowym określeniem, projekt przyznawał temu organowi praktycznie nieograniczony i stały

[220] Zob. wyrok Trybunału Sprawiedliwości UE z 22 listopada 2022 r. o sygn. C-37/20 dotyczący uzyskiwania danych z krajowych rejestrów beneficjentów rzeczywistych, a także: wyrok Trybunału Sprawiedliwości UE z 9 listopada 2010 r. w sprawie Volker und Markus Schecke i Eifert o sygn. C-92/09 i C-93/09.
[221] DOL.401.387.2024.
[222] DOL.401.466.2024.

dostęp do danych osobowych zgromadzonych w ww. rejestrach, co wzbudziło poważne wątpliwości z punktu widzenia zasad przetwarzania danych osobowych wynikających z rozporządzenia 2016/679, zwłaszcza zasad minimalizacji danych i ograniczenia celu, a także zgodności z prawem, rzetelności, przejrzystości. Projekt pozostawał również w sprzeczności z dotychczasowymi uregulowaniami ustawowymi – z ustaw regulujących KRS i CEIDG nie wynika możliwość udostępniania danych osobowych w sposób przewidziany w projekcie. Z ustawy o ewidencji ludności wynika konieczność złożenia jednorazowego wniosku o przyznanie dostępu do określonych danych zgromadzonych w rejestrze PESEL, w tym przez organy administracji publicznej, a ewentualna zgoda na dostęp do tych danych jest wydawana w drodze decyzji administracyjnej. Zastrzeżenia organu nadzorczego wzbudziły również postanowienia przewidujące wymianę danych między systemami teleinformatycznymi ministra właściwego do spraw informatyzacji a systemami teleinformatycznymi właściwego ministra kierującego odpowiednim działem administracji rządowej, które w dodatku zakładały udostępnianie danych na potrzeby realizacji danej usługi online na podstawie porozumień pomiędzy ministrem właściwym do spraw informatyzacji a innymi podmiotami. Organ nadzorczy podniósł, że projektowane regulacje powinny wymieniać sprecyzowane cele, w jakich następuje pozyskiwanie danych osobowych z danego rejestru. Przepisy prawa powinny określać tryb oraz sposób udostępnienia danych z rejestru, aby administrator danych osobowych w nim przetwarzanych miał kontrolę nad tym, jakie podmioty i w jakich celach pozyskują dane osobowe. Wskazane unormowania uznano za niedopuszczalne z punktu widzenia podstawowych zasad przetwarzania danych określonych w RODO oraz warunków wymienionych w art. 6 ust. 3 tego aktu. Mimo wagi podnoszonych przez organ nadzorczy kwestii, jego postulaty nie zostały uwzględnione.

Innego rozstrzygnięcia doczekał się **projekt ustawy o rynku pracy i służbach zatrudnienia**[223], który zakładał m.in. szeroką rozbudowę systemów teleinformatycznych w oparciu o bazy życiorysów zawodowych osób bezrobotnych, poszukujących pracy, osób niezarejestrowanych, osób biernych zawodowo, które za pomocą systemu byłyby automatycznie dopasowywane do ofert pracy. Organ nadzorczy zwrócił uwagę na liczne zagrożenia związane z możliwością niedozwolonej integracji rejestrów oraz nadmiarowego przetwarzania danych osobowych w nich zawartych, a także na budzące wątpliwości tryby pozyskiwania danych z KRS czy systemu ZUS przez starostę oraz przez wojewódzkie i powiatowe urzędy pracy. Tym razem znaczna część uwag przedstawionych w opinii została przez projektodawcę wzięta pod uwagę.

Projekt ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw[224] zakładał wprowadzenie dwóch nowych, co do zasady jawnych rejestrów publicznych: rejestru przedsiębiorstw energetycznych oraz rejestru instalacji magazynowych wodoru. Przyjęcie modelu jawności danych osobowych nie zostało

[223] DOL.401.189.2024.
[224] DOL.401.196.2024.

poprzedzone wykazaniem niezbędności powstania takich rejestrów ani nie zostały określone warunki przetwarzania danych osobowych w zakresie retencji, anonimizacji numerów PESEL, trybu udostępniania danych. Organ nadzorczy wskazał na pominięcie uwzględniania mechanizmów wynikających z art. 25 RODO, zwracając uwagę na najwyższe standardy, jakie rejestr państwowy (szczególnie zakładający model jawności) powinien spełniać, w tym przede wszystkim odzwierciedlać walory autentyczności, rozliczalności, niezawodności oraz niezaprzeczalności. Część uwag została uwzględniona przez projektodawcę.

Na zagrożenie łączenia zbiorów danych organ nadzorczy zwrócił uwagę w opinii do **projektu ustawy o zmianie ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy oraz niektórych innych ustaw**[225]. Proponowane w projekcie ustawy rozwiązania związane były m.in. z integracją CEIDG z innymi systemami/rejestrami publicznymi i przekazywaniem danych osobowych, zwłaszcza osób prowadzących działalność gospodarczą. Prezes UODO podniósł, że takie rozwiązanie generuje wiele ryzyk, które nie zostały przez projektodawcę rozstrzygnięte w drodze testu prywatności. Projektodawca nie sprecyzował, z jakich rejestrów administrator będzie pozyskiwał dane, wprowadzając w istocie rozwiązania polegające na zmianie pierwotnych celów prowadzenia rejestrów publicznych, takich jak KRS. Zwrócono również uwagę na brak szczegółowego określenia ról poszczególnych podmiotów w procesach przetwarzania danych.

Na podobny rodzaj zagrożeń zwrócono uwagę w opinii do **projektu ustawy o wsparciu państwa dla rodziców powracających na rynek pracy**[226]. Projekt ten zakładał powstanie nowego rejestru publicznego, obejmującego liczne informacje dotyczące osób nabywających prawo do świadczenia dla rodziców powracających na rynek pracy, które mają być przetwarzane przez wiele upoważnionych na gruncie projektowanej ustawy podmiotów. Przewidywał, że po wpisaniu do formularza wniosku numeru PESEL osoby występującej o przyznanie świadczenia, formularz wniosku może być uzupełniony o dane zgromadzone w rejestrze PESEL w zakresie imion, nazwiska, miejsca urodzenia, daty urodzenia, stanu cywilnego, obywatelstwa i płci osoby. Organ nadzorczy podniósł, że taka redakcja norm prowadzi w istocie do automatycznego łączenia zasobów obu rejestrów. Co więcej, tak ukształtowany przepis wzbudza wątpliwość, czy jego stosowanie nie będzie wiązać się z automatycznym przetwarzaniem danych osobowych, czy nawet profilowaniem.

W **projekcie ustawy o czasowym ograniczeniu cen za energię elektryczną, gaz ziemny i ciepło systemowe oraz o bonie energetycznym**[227] zawarty został przepis umożliwiający wójtowi, burmistrzowi lub prezydentowi miasta (w zakresie, w którym podmioty te weryfikują wnioski o wypłatę bonu energetycznego) bardzo szeroki i niemal dowolny dostęp do wielu różnych zbiorów, potencjalnie w trybie

[225] DOL.401.338.2024.
[226] DOL.401.104.2024.
[227] DOL.401.173.2024.

teletransmisji (z projektowanych przepisów nie wynika, czy ma być w tym zakresie zastosowany jakikolwiek rodzaj trybu wnioskowego). Organ nadzorczy zwrócił również uwagę na fakt, że stosowanie powyższego przepisu może wiązać się z profilowaniem czy też podejmowaniem decyzji w sposób zautomatyzowany.

Konstruowanie procesów przetwarzania opartych o systemy elektroniczne i rejestry państwowe dużej skali powinno być czynione z dalece idącą dbałością o funkcjonalność tych systemów, również pod względem zapewnienia standardów bezpieczeństwa i poufności danych. Wśród opiniowanych projektów dostrzegalny jest niebezpieczny trend do określania warunków działania tego rodzaju rejestrów w sposób zdecydowanie zbyt powierzchowny, a często wręcz dowolny, szczególnie pod względem ustalenia sposobów dysponowania, wymiany i udostępniania danych osobowych, bez zachowania należytych gwarancji dla praw i wolności jednostki.

6.5. Role podmiotów w procesach przetwarzania danych osobowych

Organ nadzorczy w swoich opiniach wielokrotnie zwraca uwagę na problem braku prawidłowego określenia ról podmiotów biorących udział w procesach przetwarzania danych osobowych, zwłaszcza administratora[228]. Prawidłowe rozgraniczenie zakresu kompetencji i odpowiedzialności poszczególnych podmiotów ma szczególnie doniosłe znaczenie w przypadku złożonych modeli przetwarzania, w którym udział biorą liczne podmioty o różnych uprawnieniach, zadaniach i sposobach przetwarzania. Zauważalna jest tendencja do pomijania tego aspektu w ogóle lub też traktowania go w sposób zbyt formalistyczny i powierzchowny. Samo wskazanie określonego podmiotu jako administratora w przepisie normatywnym nie jest wystarczające czy nawet właściwe. O tym, kto jest administratorem danych w konkretnej sprawie, będą bowiem decydowały cele przetwarzania oraz przypisany danemu podmiotowi rodzaj zadań i kompetencji – a zatem to, jaki podmiot jest realnie władny do ustalania celów i sposobów przetwarzania danych osobowych. Rola administratora powinna wynikać z charakteru kompetencji lub też zakresu zadań publicznych, jakie normy prawne mu przypisują. Przepis wprost określający dany podmiot jako administratora powinien zatem pełnić funkcję co najwyżej komplementarną, a przede wszystkim pozostawać w zgodzie z całością regulacji oraz systemu innych relewantnych aktów prawnych[229].

W przypadku tworzenia regulacji prawnych formułujących podstawy procesów przetwarzania najważniejsze jest określenie klarownych i ostrych granic zakresu kompetencji oraz ról poszczególnych podmiotów, w szczególności w przypadku modelu przetwarzania opartego na uczestnictwie wielu współadministratorów lub podmiotów przetwarzających. Jest to zagadnienie kluczowe dla rozstrzygnięcia, który podmiot stanie się odpowiedzialny zarówno za realizację zasad ogólnych RODO (w tym kontekście przede wszystkim zasady rozliczalności), jak i za wykonywanie

[228] Zob. Wytyczne Europejskiej Rady Ochrony Danych nr 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO.
[229] Zob. wyrok Trybunału Sprawiedliwości UE z 11 stycznia 2024 r. o sygn. C-231/22 État belge, a także: wyrok Naczelnego Sądu Administracyjnego z 30 stycznia 2002 r., sygn. akt II SA 1098/01.

wynikających z rozdziału III tego aktu praw osób, których dane dotyczą, czy też rozpatrywanie i zgłaszanie naruszeń.

Ze względu na napływające od administratorów i inspektorów ochrony danych sygnały dotyczące wątpliwości w zakresie stosowania przepisów **ustawy o doręczeniach elektronicznych**, Prezes UODO skierował **wystąpienie do Ministra Cyfryzacji**[230] z wnioskiem o zainicjowanie ich korekty. Jednym z powodów skierowania wystąpienia były właśnie niejednoznaczne przepisy dotyczące ról podmiotów w procesie przetwarzania danych związanych z doręczeniami elektronicznymi powodujące znaczne problemy interpretacyjne i problemy ze stosowaniem ustawy w praktyce przez uczestników procesów przetwarzania. Z przepisów ustawy nie wynika jednoznacznie, jaki status w rozumieniu RODO przypisywać należy operatorowi wyznaczonemu wobec danych osobowych zawartych w treści korespondencji, które przetwarza w związku ze świadczeniem usług PUH (Publicznej Usługi Hybrydowej) oraz PURDE (Publicznej Usługi Rejestrowanego Doręczenia Elektronicznego). Brak jest przepisów wskazujących, czy operator wyznaczony jest administratorem tych danych, czy podmiotem przetwarzającym. Wraz z rozpoczęciem korzystania z doręczeń elektronicznych nadawcy korespondencji powinni mieć jednoznaczną informację o statusie operatora wyznaczonego, albowiem determinuje to przyznane mu obowiązki wynikające z ww. rozporządzenia unijnego i kształtuje zakres jego odpowiedzialności. W odpowiedzi Ministerstwo Cyfryzacji zapowiedziało kolejną nowelizację ustawy o doręczeniach elektronicznych uwzględniającą także kwestie podniesione w wystąpieniu Prezesa Urzędu.

Projekt ustawy o zmianie ustawy o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków oraz niektórych innych ustaw[231] stanowi przykład regulacji, gdzie projektodawca wprost wskazuje tożsamość administratora (którym jest dostawca wody w związku z realizacją zadania polegającego na udzielaniu informacji), lecz nie określa jednocześnie osób, których dane dotyczą ani kategorii przetwarzanych danych osobowych. Stanowiąc, że dostawca wody „przetwarza dane osobowe", powyższa regulacja pozostaje blankietowa i nie stanowi dla wykonawcy normy jasnej informacji co do obowiązku przetwarzania danych osobowych.

Podobne uwagi skierowane zostały wobec **projektu ustawy o zmianie ustawy o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej**[232], w którym rola administratora została określona przez lapidarny przepis stanowiący wprost, że administratorem danych osobowych przetwarzanych w celach związanych z regulacją jest właściwy dyrektor urzędu morskiego. Organ nadzorczy podkreślił, że rola administratora powinna wynikać z charakteru kompetencji lub też zakresu zadań publicznych, jakie przepisy te mu przypisują. Tymczasem projekt ustawy nie dookreślił celów pozyskiwania danych osobowych zgromadzonych w wykazie badań

[230] DOL.413.7.2024.
[231] DOL.401.389.2024.
[232] DOL.401.465.2024.

prowadzonych na polskich obszarach morskich, a więc elementu w dużej mierze konstytuującego również właśnie rolę administratora w procesie przetwarzania. Uwagi Prezesa UODO zostały uwzględnione na etapie rządowego procesu legislacyjnego.

Osobny problem związany z wyznaczeniem roli administratora uwidacznia **projekt ustawy o ogólnym bezpieczeństwie produktów**[233]. Przewidywał on bowiem model, w którym minister właściwy do spraw zdrowia powołuje i odwołuje „administratora systemu monitorowania". Z tak skonstruowanego przepisu nie wynika zatem, jaki podmiot będzie pełnił funkcję administratora w rozumieniu RODO. Organ nadzorczy wielokrotnie zwracał uwagę na wątpliwości, jakie wynikają z zastosowania tego typu konstrukcji. Brak wprowadzenia wyraźnego podziału obowiązków pomiędzy podmiotami uczestniczącymi w procesach przetwarzania danych powoduje, że nie można określić, czy administrator systemu będzie odpowiedzialny za wszystkie obowiązki spoczywające na administratorze w rozumieniu rozporządzenia 2016/679 – zarówno wobec osób, których dane dotyczą, jak i organu nadzorczego. Dodatkowo nie wiadomo, czy administrator sytemu będzie podmiotem publicznym czy też prywatnym, zaś sam sposób jego wyznaczenia oparty na uznaniowej decyzji ministra koliduje z konstytucyjną zasadą legalizmu.

Brak systemowego oraz funkcjonalnego zidentyfikowania i rozróżnienia ról poszczególnych podmiotów może prowadzić również do naruszenia zasad hierarchii aktów prawa, co uwidacznia **projekt rozporządzenia w sprawie przyznawania rekompensaty pieniężnej oraz wyrównania do wysokości rekompensaty wypłacanej strażakowi ratownikowi ochotniczej straży pożarnej**[234]. Przepisy projektu zobowiązywały komendanta wojewódzkiej Państwowej Straży Pożarnej do powołania i wyznaczenia składu Zespołu, który ma ustalać prawo do rekompensaty lub wyrównania za czas niezdolności do pracy strażakowi Ochotniczej Straży Pożarnej. W ten sposób rozporządzenie doprowadziłoby do uprawnienia do przetwarzania danych osobowych innych niż wynikających z delegacji ustawowej osób – mianowicie członków Zespołu, którymi mogą być pracownicy czy strażacy zatrudnieni w komendzie wojewódzkiej Państwowej Straży Pożarnej, ale także inne osoby wyznaczone przez powiatowego komendanta Państwowej Straży Pożarnej czy wójta (burmistrza, prezydenta). Wnioskujący o rekompensatę strażak ochotniczej straży pożarnej również nie jest ani strażakiem, ani pracownikiem PSP. Należy więc podkreślić, że w odniesieniu do tych osób mamy do czynienia z pracownikami odrębnych administratorów.

Jak pokazują powyższe przykłady, aspekt podziału ról poszczególnych podmiotów biorących udział w procesach przetwarzania wciąż pozostaje problematyczny dla projektodawców. W przypadku administratorów, którymi w założeniu nowych regulacji mają być podmioty wykonujące zadania publiczne, kwestia ta staje się niezwykle istotna i to niejedynie z punktu widzenia RODO. W szerszym kontekście pozostaje ona bowiem w ścisłej korelacji z określeniem

[233] DOL.401.299.2024.
[234] DOL.401.308.2024.

przysługujących danym podmiotom kompetencji i władztwa administracyjnego. W tym samym duchu wynikające z RODO zasady rozliczalności i odpowiedzialności administratora pozostają w równoległym związku z zasadą zaufania do władzy publicznej. Brak ustawowego, jasnego podziału kompetencji wpływa ujemnie nie tylko na procesy przetwarzania danych osobowych, ale w szerszym kontekście również na sprawność i jakość funkcjonowania organów władzy publicznej.

6.6. Zasady przetwarzania danych osobowych, dane szczególnych kategorii, PESEL

Powszechnym problemem, do którego organ nadzorczy stale odnosi się w swoich opiniach, jest niedostateczna realizacja zasad przetwarzania określonych w art. 5 RODO. Powszechne jest stosowanie w projektach aktów prawnych pojęć blankietowych, nieostrych, zbyt ogólnych lub niedostatecznych, prowadzących w efekcie do rozszerzającej wykładni kompetencji podmiotów dokonujących operacji przetwarzania, ale także do niedozwolonego profilowania i zautomatyzowanego podejmowania decyzji. Dostrzegalne jest dążenie do wprowadzania otwartych katalogów rodzajów danych, jakie mogą być przetwarzane, albo wprowadzania wymogu udostępniania danych takich, jak numery telefonów lub adresy elektroniczne, mimo braku w polskim porządku prawnym obowiązku posiadania tego rodzaju środków komunikacji. Powyższe zjawiska niekorzystnie wpływają na realizację zasad ograniczenia celu, minimalizacji danych oraz przejrzystości i rzetelności.

Kolejnym problemem były próby wprowadzania ograniczeń praw podmiotów danych na podstawie prawa krajowego z pominięciem warunków przewidzianych w art. 23 RODO. Wyżej wymieniony przepis stanowi, że państwo członkowskie może aktem prawnym ograniczyć zakres niektórych praw i obowiązków wynikających z RODO, ale tylko jeżeli ograniczenie takie nie naruszyłoby istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym np. bezpieczeństwu narodowemu czy zapobieganiu przestępczości. Takim ograniczeniom w każdym przypadku towarzyszyć muszą adekwatne środki zapobiegania nadużyciom lub niezgodnemu z prawem dostępowi albo przekazywaniu danych. Odstępstwo od zasad wymienionych w art. 23 RODO stanowi zatem naruszenie prawa Unii Europejskiej[235].

Problemem jest także brak odnoszenia się do zasady ograniczenia przechowywania. Ustanowienie okresów retencji czy procedur usuwania danych osobowych jest często pomijane przez projektodawców, a w innych przypadkach okresy retencji ustalane są w sposób arbitralny, bez wyjaśnienia konieczności przechowywania danych przez wskazany czas.

Powyższe zagadnienia stają się tym bardziej istotne, gdy brakom stosownych regulacji odpowiadającym zasadom rozporządzenia ogólnego towarzyszy wprowadzanie procesów przetwarzania danych szczególnych kategorii, danych dotyczących karalności czy identyfikatora PESEL. Wymienione rodzaje danych, ze

[235] Zob. Wytyczne Europejskiej Rady Ochrony Danych nr 10/2020 dotyczące ograniczeń wynikających z artykułu 23 RODO.

względu na swoją szczególną charakterystykę, wymagają wyjątkowej dbałości i roztropności przy wdrażaniu podstaw prawnych do ich przetwarzania, obwarowanego szczególnym reżimem wynikającym z art. 9 ust. 2, art. 10 i art. 87 RODO, co niestety, w niemałej części opiniowanych projektów zostało pominięte.

Zbyt często projektodawcy nie uwzględniają także aspektów związanych z bezpieczeństwem i poufnością danych. Zgodnie z art. 32 RODO projektodawca, biorąc pod uwagę kontekst, charakter, cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, powinien już na etapie konstruowania regulacji prawnych przewidzieć środki zapewniające bezpieczeństwo danych. Ciężar tego obowiązku nie powinien być przenoszony w całości na administratorów i podmioty przetwarzające. To projektodawca, odpowiednio rozpoznając przyszłe potencjalne zagrożenia, w drodze stosownej regulacji prawnej dysponuje najlepszą możliwością zapewnienia przyszłym wykonawcom norm adekwatnego zaplecza organizacyjnego, technicznego i finansowego koniecznego dla prawidłowej realizacji zadań publicznych w sposób czyniący jednocześnie zadość wymogom bezpieczeństwa danych osobowych. Nowa regulacja nie powinna ograniczać się jedynie do określenia środków bezpieczeństwa, ale powinna także określać kryteria środków zapewniających bezpieczeństwo.

Przykładem ilustrującym powyższą problematykę jest **projekt ustawy o zdrowiu zwierząt**[236]. Zakładał on utworzenie różnych rejestrów i chociaż projektodawca w sposób szczegółowy określił zakres danych przetwarzanych w każdym z nich oraz wskazał podmioty odpowiedzialne za ich prowadzenie, to nie określił (wynikających z przepisów) sposobów ich prowadzenia, zwłaszcza środków technicznych mających zapewnić bezpieczeństwo danych. W sposób zbyt ogólny i niejasny określone zostały podstawy udostępniania danych z rejestrów między podmiotami. Organ nadzorczy zwrócił uwagę na wymóg zawarcia we wniosku o powołaniu na rzeczoznawcę numeru telefonu lub adresu poczty elektronicznej kandydata na rzeczoznawcę, podkreślając jednocześnie, że polskie prawo nie nakłada powszechnego obowiązku posiadania numeru telefonu i adresu poczty elektronicznej, dlatego ich podanie w ww. wniosku powinno być jedynie fakultatywne. Prezes UODO odniósł się do przepisów nakładających na wymienione podmioty obowiązek zbierania i przekazywania wielu danych i informacji dotyczących m.in. występowania chorób i odzwierzęcych czynników chorobotwórczych. Podniósł, że sposób sformułowania przepisów nie pozwala na stwierdzenie, czy dane i informacje, o których mowa, miałaby obejmować także dane osobowe w rozumieniu rozporządzenia 2016/679.

Na niezgodny, zarówno z rozporządzeniem ogólnym, jak i z orzecznictwem Trybunału Sprawiedliwości UE[237] - model retencji, wskazano w opinii do **projektu ustawy – Prawo komunikacji elektronicznej**[238], który nakłada na przedsiębiorców

[236] DOL.401.203.2024.
[237] Zob. wyroki Trybunału Sprawiedliwości UE z 6 października 2020 r. o sygn. C-511/18, C-512/18 i C-520/18 w sprawie La Quadrature du Net i in. przeciwko Premier ministre i in. oraz wyrok z 6 października 2020 r. o sygn. C-623/17 w sprawie Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs.
[238] DOL.401.60.2024.

telekomunikacyjnych obowiązek przechowywania przez 12 miesięcy danych użytkownika końcowego. Przewiduje też udostępnienie tych danych uprawnionym służbom państwowym i sądom. Organ nadzorczy zwrócił uwagę, że Trybunał Sprawiedliwości UE w swoich orzeczeniach stanął na stanowisku, że niezróżnicowane gromadzenie danych przez przedsiębiorców telekomunikacyjnych o wszystkich użytkownikach jest niezgodne z Kartą praw podstawowych Unii Europejskiej. W ocenie organu nadzorczego obecny model bezwarunkowego gromadzenia danych o wszystkich użytkownikach nie zapewnia stosowania zasad wynikających z przepisów RODO, jak również wynikającej z art. 51 ust. 2 Konstytucji RP zasady ograniczenia gromadzenia informacji o obywatelach przez władze publiczne.

W toku opiniowania **ustawy o zmianie ustawy – Kodeks wyborczy**[239], oceniając zmiany przepisów dotyczące głosowania korespondencyjnego, organ nadzorczy zwrócił uwagę, że co do zasady osoba fizyczna nie powinna być identyfikowana za pomocą danych innych osób (w tym przypadku imienia ojca), jest to bowiem dana osoby trzeciej, w dodatku nadmiarowa (zbędna) wobec możliwości jednoznacznego zidentyfikowania osoby na podstawie innych danych. Krytycznie odniósł się również do wymogu przedłożenia przez wyborcę niepełnosprawnego kopii aktualnego orzeczenia o ustaleniu stopnia niepełnosprawności, zawiera ono bowiem dane szczególnych kategorii, a dla osiągnięcia celu, jakim jest ustalenie niepełnosprawności wyborcy, nie jest konieczne przedstawienie pełnej treści orzeczenia.

Zagadnienia związane z bezpieczeństwem i poufnością danych osobowych były przedmiotem opinii dotyczącej **projektu ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw**[240]. Organ nadzorczy wskazał, że z przyjętym w projekcie modelem udostępniania akt postępowania przygotowawczego w postaci elektronicznej wiążą się liczne ryzyka dla przetwarzania danych osobowych. Istotne jest, aby takie udostępnianie było prowadzone w sposób gwarantujący tym danym integralność i poufność. Projektowane przepisy umożliwiające przekazywanie akt w postaci elektronicznej powinny zostać rozbudowane o procedury przewidujące i minimalizujące owe ryzyka. Jednocześnie Prezes UODO wystąpił z postulatem zmian obecnie obowiązującej konstrukcji art. 156 § 5 k.p.k. w kontekście wyrażonych w orzecznictwie Europejskiego Trybunału Praw Człowieka[241] zastrzeżeń co ww. artykułu i jego zgodności z Konwencją o ochronie praw człowieka i podstawowych wolności.

Do zasad przetwarzania danych szczególnych kategorii organ nadzorczy odniósł się m.in. w opinii do projektu **rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie rodzinnych domów pomocy**[242]. Proponowane rozwiązania w zakresie przetwarzania danych osobowych w związku z kierowaniem osoby

[239] DOL.401.90.2024.
[240] DOL.401.437.2024.
[241] Zob. wyrok Europejskiego Trybunału Praw Człowieka z 22 lutego 2024 r. sygn. 16974/14 w sprawie Kaczmarek przeciwko Polsce.
[242] DOL.401.136.2024.

wymagającej pomocy do rodzinnego domu opieki, wydawaniem decyzji w tej sprawie, przekazywaniem przez kierownika ośrodka lub centrum do rodzinnego domu pomocy informacji dotyczącej stanu zdrowia osoby skierowanej do domu, jak również nadzór i kontrola rodzinnych domów pomocy, nie uwzględniły w sposób prawidłowy wymagań określonych w RODO. Po raz kolejny organ nadzorczy podkreślił, że normy prawne regulujące procesy przetwarzania danych osobowych powinny być określone precyzyjnie i wskazywać na cele przetwarzania, podmioty biorące udział w przetwarzaniu, sposoby przetwarzania oraz na zakres danych podlegających przetwarzaniu. Tymczasem projektowane przepisy przybrały charakter blankietowy i nie wynikało z nich, jakie konkretnie dane osobowe dotyczące osób wymagających pomocy są przetwarzane i z jakich źródeł pochodzą. Świadczenie usług i pomocy podopiecznym rodzinnych domów pomocy jest związane z przetwarzaniem danych dotyczących zdrowia, a zatem danych wrażliwych, którym przepisy rozporządzenia nadają szczególne znaczenie i reżim wykonywania na nich operacji przetwarzania.

Analogiczne zastrzeżenia wzbudził **projekt rozporządzenia Ministra Obrony Narodowej w sprawie orzekania o zdolności do służby w Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, orzekania o inwalidztwie funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego oraz emerytów i rencistów Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego**[243], w którym wprowadzone zostały normy kreujące otwarte katalogi źródeł informacji, w tym danych osobowych, nie wykluczając także danych wrażliwych (dotyczących zdrowia). Orzekanie o zdolności do służby czy o inwalidztwie wiąże się z przetwarzaniem najbardziej intymnych i osobistych informacji o funkcjonariuszu. Z tego powodu tak ważne jest, aby przetwarzanie danych osobowych, w tym szczególnych kategorii dotyczących zdrowia było zgodne z najwyższymi możliwymi standardami w zakresie prawa do prywatności.

Poważne wątpliwości organu nadzorczego wzbudziły przepisy **projektu ustawy o zmianie ustawy o cudzoziemcach oraz niektórych innych ustaw**[244] odnoszące się do automatycznego generowania zaświadczeń, ponieważ w wyniku realizacji przyjętych rozwiązań może dochodzić do zautomatyzowanego przetwarzania danych, w tym profilowania. Mimo to projektodawca pominął wdrożenie właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, o których mowa w art. 22 RODO.

Z zaniepokojeniem organ nadzorczy przyjął zaproponowane w projekcie **ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw**[245] regulacje dotyczące wyłączenia stosowania art. 12–22 RODO. W opinii zwrócił uwagę, że przepisów ogólnego rozporządzenia o ochronie danych nie można całkowicie wyłączyć mocą aktu prawa krajowego, a prawa podmiotów danych wynikające z art.

[243] DOL.401.222.2024.
[244] DOL.401.41.2024.
[245] DOL.401.265.2024.

12–22 RODO można ograniczyć jedynie w celach wskazanych w art. 23 RODO z jednoczesnym uwzględnieniem gwarancji przewidzianych przez ten przepis.

W **wystąpieniu do Ministra Cyfryzacji**[246] Prezes UODO wniósł o podjęcie prac legislacyjnych prowadzących do **zmiany przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej** poprzez przyjęcie rozwiązań, które eliminowałyby ujawnianie numeru PESEL w certyfikacie kwalifikowanego podpisu elektronicznego. Istotne wątpliwości organu nadzorczego wynikają z tego, że numer PESEL jest pozyskiwany przez dostawców usług zaufania publicznego (kwalifikowanego podpisu elektronicznego), a następnie upubliczniany, co z kolei nie wynika ani z przepisów europejskich, ani krajowych. Organ nadzorczy od wielu lat w swoich stanowiskach zwraca uwagę, że numer PESEL jest daną wyjątkową, w sposób unikalny identyfikującą daną osobę, stwarzającą jednocześnie – jako dana referencyjna – wiele ryzyk, w tym tworzenia profili osobowych bez wiedzy osoby, której numer ten dotyczy. Resort cyfryzacji nie przychylił się do uwag Prezesa Urzędu, przyjmując stanowisko, że zmiana legislacyjna w odniesieniu do numeru PESEL w certyfikacie kwalifikowanym nie jest konieczna.

Świadcząc swoje eksperckie wsparcie, organ nadzorczy stale i na bieżąco wskazuje kryteria prawidłowej implementacji standardów, zasad i ograniczeń wynikających z RODO. Niemniej zaobserwować należy, że problem właściwego stosowania zasad przetwarzania nie dotyczy jedynie nowych projektów. Organ nadzorczy dostrzega wiele niekorzystnych zjawisk natury systemowej, które od wielu lat obecne są w obiegu prawnym, a przez nowe regulacje są jedynie powielane, bez podjęcia wymaganej rewizji rozwiązań już funkcjonujących.

6.7. Postęp technologiczny a ochrona praw podstawowych

Stale zwiększająca się (ale i oczekiwana przez obywateli) cyfryzacja życia społecznego niesie ze sobą ogromny potencjał korzyści zarówno dla rozwoju państwa, jak i jego obywateli, ale wiąże się też z równie istotnymi zagrożeniami dla praw jednostki, w tym prawa do prywatności i autonomii informacyjnej. Organ nadzorczy za materię fundamentalną uznaje konieczność roztropnego uregulowania kwestii związanych z rozwojem nowych technologii. Cyfryzacja procesów przetwarzania nie może prowadzić do naruszenia praw i wolności osób fizycznych. Przeciwnie, procesy wdrażania technologii cyfrowych powinny obejmować rozwiązania pozwalające na umocnienie praw i podmiotowości obywateli, sprzyjając rozwojowi społeczeństwa obywatelskiego przy zachowaniu najwyższych standardów demokratycznego państwa prawa, etyki i poszanowania godności ludzkiej.

W związku z opiniowaniem projektów aktów prawnych zauważalna jest tendencja do traktowania cyfryzacji w sposób zbyt powierzchowny, jedynie jako forma digitalizacji dotychczasowych procesów, podczas gdy wdrażanie nowych technologii powinno być każdorazowo poprzedzone dogłębną analizą pod względem wpływu, jakie regulacje te wywrą w sferze praw osób, których dane dotyczą, oraz spełnienia kryteriów

[246] DOL.413.3.2024.

proporcjonalności i niezbędności, zapewnienia odpowiedniego poziomu poufności i bezpieczeństwa, a także zastosowania skutecznych środków kontroli.

Wyrazem aktywnego wspierania organów państwowych w zakresie formułowania długofalowych rozwiązań w tym obszarze jest przedstawiona przez Prezesa UODO opinia do **Strategii Cyfryzacji Polski do 2035 r**.[247] Dążąc do wzmocnienia planowanych rozwiązań strategicznych, organ nadzorczy przedstawił wiele istotnych postulatów odnoszących się nie tylko do zagadnień związanych z ochroną praw podstawowych i konstytucyjnych wartości, ale także rozwojem edukacji, bezpieczeństwa, niezależności cyfrowej państwa, promowania zachowań prozdrowotnych, a w dużej mierze także sposobów uregulowania zagadnień związanych z szeroko rozumianym zastosowaniem sztucznej inteligencji (SI lub AI) w przestrzeni publicznej.

To właśnie zagadnienia związane z rozwojem SI znalazły się w kręgu szczególnego zainteresowania organu nadzorczego w 2024 roku, czego wyrazem była opinia do **projektu ustawy o systemach sztucznej inteligencji**[248]. Prezes UODO zwrócił w niej uwagę, że zapewniając w porządku krajowym stosowanie prawa unijnego dotyczącego sztucznej inteligencji, nie można pomijać uprawnień organu nadzorczego i jego wiodącej roli w zakresie ochrony danych osobowych, wynikających zarówno z RODO, jak i z unijnego aktu w sprawie sztucznej inteligencji (AI Act). Zauważył, że projektowana ustawa nie odzwierciedla szczególnej pozycji organu nadzorczego do spraw ochrony danych osobowych i nie reguluje kompetencji nadzorczych Prezesa UODO, których konieczność wdrożenia w prawie krajowym została określona wprost przez Akt w sprawie sztucznej inteligencji. Wskazał również na istotne zagrożenia związane z nakładaniem się kompetencji nadzorczych Prezesa UODO i projektowanej Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji wynikających z obu regulacji, które potencjalnie mogą negatywnie wpłynąć na niezależność organu nadzorczego oraz stwarzać ryzyko duplikacji i dualizmu rozstrzygnięć.

Na problemy towarzyszące wdrażaniu innego aktu unijnego – aktu o rynkach cyfrowych (rozporządzenie 2022/1925) – Prezes UODO zwrócił uwagę w opinii do **projektu ustawy o zmianie niektórych ustaw w celu zapewnienia stosowania przepisów unijnych poprawiających funkcjonowanie rynku wewnętrznego**[249]. Organ nadzorczy wskazał, że wzajemne powiązania aktu o rynkach cyfrowych oraz rozporządzenia 2016/679 w dalszym ciągu budzą wątpliwości interpretacyjne, a także podkreślił, że opracowanie spójnej interpretacji aktu o rynkach cyfrowych i rozporządzenia 2016/679, przy jednoczesnym poszanowaniu kompetencji każdego z organów regulacyjnych w obszarach, w których rozporządzenie 2016/679 ma zastosowanie, i do których odnosi się akt o rynkach cyfrowych, ma kluczowe znaczenie

[247] DOL.401.502.2024.
[248] DOL.401.354.2024.
[249] DOL.401.138.2024.

dla skutecznego wdrożenia obu regulacji i osiągnięcia ich, uzupełniających się, założeń.

W 2024 roku zauważalna była tendencja do wdrażania również innych niż sztuczna inteligencja nowych technologii – w tym z zastosowaniem biometrii. Przykładem takiej regulacji jest **projekt ustawy o zmianie ustawy o systemie ubezpieczeń społecznych oraz niektórych innych ustaw**[250]**,** zakładający m.in. automatyzację połączeń telefonicznych dotyczących zawiadomienia o terminie badania przy zastosowaniu technologii wykorzystującej automatyczne przetwarzanie danych osobowych, tzw. voicebotów, opartych o algorytmy AI, a zatem przetwarzanie danych biometrycznych w związku z nagrywaniem rozmów telefonicznych. Rozumiejąc chęć usprawnienia procesów kontaktów z klientami ZUS, organ nadzorczy zwrócił jednak uwagę, że zautomatyzowane przetwarzanie danych biometrycznych (jakim jest nagrywanie głosów osób kontaktujących się z ZUS) jest wyjątkowo inwazyjną formą przetwarzania danych osobowych, obarczoną ogromnym ryzykiem naruszenia praw i wolności osób nagrywanych. Analiza unikalnej cechy biometrycznej, jaką jest głos człowieka, pozwala nie tylko dokonać jego identyfikacji, ale określić m.in. jego stany emocjonalne, ustalić choroby, na które cierpi, czy określić wiek i płeć. Podniósł, że dane biometryczne – zgodnie z art. 9 ust. 1 RODO – należą do danych szczególnych kategorii, których przetwarzanie wymaga zachowania szczególnego reżimu. Tymczasem projektodawca nie zawarł w analizowanym dokumencie wymaganych przez art. 9 ust. 2 i 3 RODO gwarancji dotyczących przetwarzania danych biometrycznych.

Podobne uwagi sformułowano w związku z **projektem ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw**[251] zakładającym m.in. upoważnienie operatora infrastruktury krytycznej do żądania od pracownika danych biometrycznych. Organ nadzorczy wskazał, że w przypadku danych biometrycznych, których przetwarzanie obarczone jest wysokim ryzykiem dla podmiotu danych, obowiązek ich podania powinien być niezbędny dla realizacji celu przetwarzania takich danych, a cel ten wymaga dostatecznego uzasadnienia i precyzyjnego sformułowania w przepisie prawa. Jeżeli ma dochodzić do przetwarzania danych biometrycznych (szczególnie w przypadku relacji pracownik – pracodawca) wymagane jest wyczerpujące określenie warunków i granic przetwarzania pozyskanych danych biometrycznych przez pracodawcę.

Projekt ustawy o zmianie ustawy o nieodpłatnej pomocy prawnej, nieodpłatnym poradnictwie obywatelskim oraz edukacji prawnej[252] wprowadzał z kolei możliwość udzielania porad za pośrednictwem środków porozumiewania się na odległość. Organ nadzorczy zwrócił uwagę, że zastosowanie takiej technologii wiąże się z przetwarzaniem różnego rodzaju danych osobowych (w tym potencjalnie również danych dotyczących zdrowia, pochodzenia rasowego, a więc danych szczególnych

[250] DOL.401.430.2024.
[251] DOL.401.265.2024.
[252] DOL.401.396.2024.

kategorii), i w związku z tym konieczne jest zapewnienie uwzględnienia zasad ochrony danych osobowych i prywatności, przede wszystkim poprzez wskazanie w przepisach ustawy stosownych zabezpieczeń w zakresie przetwarzania informacji, prawidłowych okresów retencji oraz właściwego zdefiniowania pojęcia „środków porozumiewania się na odległość".

Organ nadzorczy skierował opinie do **dwóch projektów o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw**[253], których zasadniczym celem była nowelizacja zasad dochodzenia roszczeń z tytułu naruszenia dóbr osobistych, z wykorzystaniem sieci internetowej, przeciwko osobom anonimowym (o tożsamości nieznanej powodowi). Jakkolwiek ideę implementacji do polskiego systemu prawnego instytucji tzw. pozwu ślepego oraz umożliwienie nakazania ujawnienia danych osoby-naruszyciela publikującego zniesławiające treści organ nadzorczy uznaje za słuszną, to jednak zwraca uwagę na wiele problematycznych rozwiązań, które w przypadku wdrożenia zbyt wąsko postrzeganych regulacji, będą miały uboczne, negatywne oddziaływanie w szeroko rozumianym znaczeniu systemowym – również na sferę ochrony praw osób niezwiązanych w ogóle z toczącym się procesem cywilnym. Przykładowo, zawarcie swobodnie ujętego wymogu formalnego, polegającego na dołączeniu do pozwu jedynie zrzutów ekranu, kopii czy wydruków, mających stanowić wystarczającą podstawę do ujawnienia danych, uznać należy za niezgodne ze standardami postępowania dowodowego z dokumentów. Sąd powinien przeprowadzić postępowanie w kierunku weryfikacji prawdziwości takiego dokumentu oraz informacji w nim zawartych przed skierowaniem żądania ujawnienia danych do wskazanego podmiotu. W przeciwnym razie istnieje realne zagrożenie ujawnienia danych użytkownika, który nie ma nic wspólnego z treściami zamieszczonymi w określonej przestrzeni. Dodatkowo projektowane regulacje spowodowałyby, że samo złożenie pozwu (niezależnie od jego zasadności) będzie prowadziło do udostępnienia sądowi oraz powodowi całego szeregu informacji o użytkowniku, którymi nie dysponowałby, gdyby pozew składany był na warunkach ogólnych. Zwrócił także uwagę, że rozwiązania przyjmowane na gruncie k.p.c. wymagają zharmonizowania z celami, zakresem i podstawą prawną przetwarzania określonymi przez ustawę o świadczeniu usług drogą elektroniczną oraz ustawę – Prawo komunikacji elektronicznej, ponieważ na etapie opiniowania wiele z proponowanych rozwiązań pozostawało w istotnej sprzeczności wobec norm przewidzianych w innych aktach prawnych, w sposób godzący w zasady zgodności z prawem, rzetelności, przejrzystości oraz zasady ograniczenia celu i minimalizacji danych. W opiniach podkreślono, że projektowane przepisy powinny być spójne z trybem postępowania z nielegalnymi treściami w Internecie oraz udziałem krajowych organów administracji publicznej w tym procesie wynikającym z aktu o usługach cyfrowych (rozporządzenie 2022/2065).

Rozwój cyfryzacji oraz nowych technologii, ze względu na swój postępowy charakter, pozostaje w szczególnym zainteresowaniu Prezesa Urzędu. Wspierając rozwój tych gałęzi gospodarki i życia społecznego, zwraca uwagę, że postęp w tym

[253] DOL.401.350.2024, DOL.401.468.2024.

zakresie powinien odbywać się w zgodzie z zasadą zrównoważonego rozwoju, mając na względzie wielowektorowe zagrożenia, również dla prywatności obywateli. Projektodawcy nie powinni ulegać presji i trendowi tzw. cyfryzacji za wszelką cenę. Wdrażaniu nowych rozwiązań technologicznych towarzyszyć powinna dogłębna analiza oparta o planowanie strategiczne, mające w szczególności na względzie dobrobyt społeczeństwa, w tym dzieci, młodzieży i osób starszych.

6.8. Nowe kompetencje Prezesa UODO

Wejście w życie nowych regulacji unijnych oraz trwające i przyszłe przygotowania do ich stosowania w prawie krajowym prowadzą do **systematycznego rozszerzania i konieczności realizacji nowych kompetencji Prezesa Urzędu Ochrony Danych Osobowych. Konieczność dostrzeżenia istotnej roli, jaką pełni niezależny organ ds. ochrony danych osobowych przez pryzmat jego nowych zadań**, wiąże się ze stosowaniem regulacji w zakresie:

- przepisów Aktu w sprawie sztucznej inteligencji (AI Act)[254] oraz projektowanej ustawy o systemach sztucznej inteligencji służącej stosowaniu AI Act w obszarze sprawowania nadzoru zgodnie z jego przepisami,
- projektowanej ustawy o zarządzaniu danymi[255],
- projektowanej ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw[256],
- projektowanej zmiany ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[257],
- systemu wjazdu/wyjazdu (EES) obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich[258],

[254] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).

[255] Służącej stosowaniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniającego rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. UE. L. z 2022 r. Nr 152, str. 1 z późn. zm.).

[256] Służącej stosowaniu 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).

[257] Wdrażającej dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).

[258] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz. Urz. UE L 327 z 9.12.2017, str. 20, Dz. Urz. UE L 236 z 19.01.2018, str. 1, Dz. Urz. UE L 258 z 15.10.2018, str. 5, Dz. Urz. UE L 117 z 3.05.2019, str. 14, Dz. Urz. UE L 135 z 22.05.2019, str. 27, Dz. Urz. UE L 248 z 13.07.2021, str. 11, Dz. Urz. UE L 249 z 14.07.2021, str. 15 oraz Dz. Urz. UE L 2024/1356

- zautomatyzowanego przeszukania danych i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej[259],
- wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi[260],
- utworzenia europejskiej przestrzeni danych dotyczących zdrowia EHDS[261],
- decyzji wykonawczej Komisji (UE) 2023/1795 z 10 lipca 2023 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzającej odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA.

Dodatkowo projektowana w przepisach krajowych struktura nadzorcza rynku krajowego w obszarze stosowania aktów unijnych wymaga uwzględnienia celów, ról i uprawnień istniejących organów nadzorczych właściwych dla poszczególnych sektorów oraz horyzontalnych obszarów sprawowanego nadzoru i **przejrzystego ukształtowania zakresu współpracy Prezesa UODO z innymi właściwymi organami,** na co również organ nadzorczy zwracał uwagę w przedkładanych stanowiskach, np. w sprawie projektu ustawy o systemach sztucznej inteligencji[262], projektu ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw[263] czy projektowanej zmiany ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[264].

Wykonywanie nowych kompetencji organu nadzorczego obejmuje również **zadania nieprzewidziane w rozporządzeniu 2016/679** ani w **ustawie o ochronie danych osobowych.** Stanowi o tym **projekt ustawy o zarządzaniu danymi**[265] służący stosowaniu aktu w sprawie zarządzania danymi, zgodnie z którym Prezes Urzędu Ochrony Danych Osobowych ma pełnić funkcję organu właściwego do spraw

z 22.05.2024) oraz służąca jego stosowaniu Ustawa z 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu (Dz.U. poz. 1688).

[259] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/982 z 13 marca 2024 r. w sprawie zautomatyzowanego przeszukania danych i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej oraz zmieniające decyzje Rady 2008/615/WSiSW i 2008/616/WSiSW oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726, (UE) 2019/817 i (UE) 2019/818 (Prüm II).

[260] Projektowana zmiana ustawy o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi wdrażająca dyrektywę Parlamentu Europejskiego i Rady (UE) 2023/977 z 10 maja 2023 r. w sprawie wymiany informacji między organami ścigania państw członkowskich i uchylającej decyzję ramową Rady 2006/960/WSiSW (Dz. Urz. UE L 134 z 22.05.2023, str. 1), DOL.401.306.2024.

[260] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847.

[261] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847.

[262] DOL.401.354.2024.

[263] DOL.401.18.2023.

[264] DOL.401.155.2024.

[265] DOL.401.209.2024.

usług pośrednictwa danych oraz organu właściwego do spraw rejestracji organizacji altruizmu danych, co w przyszłości przełoży się na zasadnicze zwiększenie liczby spraw wnoszonych do organu nadzorczego. Jednocześnie Prezes UODO wyraźnie sprzeciwił się uznaniu go w projektowanych przepisach ww. ustawy za organ właściwy w sprawie **dokonywania oceny dopuszczalności i prawidłowości przekazywania do państw trzecich danych nieosobowych przez osobę fizyczną lub prawną**, której przyznano prawo do ponownego wykorzystywania tych danych nieosobowych.

Wskazane zagadnienia nie zostały na dzień sporządzenia sprawozdania objęte ostatecznie brzmiącymi regulacjami, ze względu na trwające procesy legislacyjne w tym zakresie.

6.9. Opiniowanie dokumentów dotyczących problemów informatycznych

Kompetencje doradcze przewidziane w art. 57 ust. 1 lit. c RODO organ nadzorczy w roku 2024 realizował nie tylko, świadcząc eksperckie wsparcie w procesie legislacyjnym, poprzez opiniowanie projektów ustaw, rozporządzeń i innych aktów krajowych oraz międzynarodowych. W związku z pracami Komitetu Rady Ministrów do spraw Cyfryzacji (KRMC) dokumenty dotyczące problematyki rozpatrywanej przez komitet przesyłane były również do wiadomości Prezesa UODO.

W 2024 r. wpłynęło **66 takich materiałów** (liczba ta została uwzględniona w podanych wyżej ogólnych danych statystycznych dotyczących projektów aktów prawnych przesłanych do zaopiniowania Prezesowi UODO).

Były to przede wszystkim opisy założeń projektów informatycznych (OZPI), protokoły ustaleń z posiedzeń, ustalenia z procesu opiniowania raportów kwartalnych czy raporty końcowe. Mimo że organ nadzorczy nie jest członkiem Komitetu i nie jest uprawniony czy zobowiązany do przedstawiania wiążących opinii, to w granicach przysługujących mu kompetencji podjął się aktywnego udziału w procesie oceny przedłożonych mu projektów informatycznych, przedstawiając opinie o charakterze pomocniczym – eksperckim i doradczym – mające na celu wzmocnienie planowanych rozwiązań o aspekty związane z ochroną danych osobowych.

Jest to tym bardziej istotne, że dokumenty będące przedmiotem analizy KRMC często dotyczą dużych, a przez to doniosłych, projektów informatycznych, których realizacja musi odbywać się z poszanowaniem zasad wynikających z RODO, gdyż przy korzystaniu z nich będzie dochodziło do przetwarzania danych osobowych, często na dużą skalę, w tym danych szczególnych kategorii w rozumieniu art. 9 i 10 RODO.

W przypadku wielu z projektów należało zwrócić uwagę, że w sposób niedostateczny odnoszą się one do problematyki ochrony danych osobowych. Organ nadzorczy każdorazowo podkreśla, że wdrażanie nowoczesnych technologii i narzędzi informatycznych – w myśl zasad domyślnej ochrony danych i uwzględnienia ochrony danych w fazie projektowania – wymaga weryfikacji tego rodzaju systemów również w kontekście przetwarzania danych osobowych, celem wyeliminowania ryzyk naruszenia praw lub wolności osób fizycznych.

Niezwykle istotna jest potrzeba każdorazowej **weryfikacji podstawy prawnej dla realizacji planowanych projektów informatycznych, zakresu oraz celu pozyskiwania i dalszego przetwarzania danych** w odniesieniu do funkcjonalności projektowanych systemów, w rozumieniu rozporządzenia 2016/679, na co organ nadzorczy wielokrotnie zwracał uwagę w stanowiskach przedkładanych resortowi cyfryzacji[266].

Znaczna część projektów objętych wypowiedzią Prezesa UODO zakładała wdrażanie operacji przetwarzania danych o charakterze wymagającym przeprowadzenia DPIA[267]. Dotyczy to zwłaszcza takich obszarów, jak innowacyjne rozwiązania technologiczne, funkcjonowanie rejestrów publicznych czy danych objętych szczególnym reżimem przetwarzania. Beneficjentom i wnioskodawcom zwracano zatem przede wszystkim uwagę na niezbędność włączenia testu prywatności obejmującego ocenę skutków dla ochrony danych jako elementu kluczowego dla wdrażania planowanych założeń.

Na potrzebę przeprowadzenia oceny skutków dla ochrony danych organ nadzorczy wskazał, w związku ze skierowaniem do rozpatrzenia przez Komitet Rady Ministrów do spraw Cyfryzacji, **projekty informatyczne – „Rozwój i zwiększenie dostępności Rejestrów Sądowych – eKRS i EKW (eKRS-EKW)" oraz „Wdrożenie w ST Krajowego Rejestru Karnego 2.0 eUsługi KRK 2.0 i obsługi zapytań systemu ECRIS (eKRK 2.0)"**[268], gdyż ich wdrożenie będzie związane z prowadzeniem licznych operacji przetwarzania danych osobowych, w tym danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych.

Za inny przykład posłużyć może **projekt „Rozbudowa Systemu do Obsługi Postępowań Administracyjnych w Budownictwie i Portalu e-Budownictwo oraz wybranych rejestrów GUNB (SOPAB 1.0)**[269]. W opisie projektu wskazano na szereg systemów, takich jak „Konto użytkownika", które przechowują dane użytkowników wraz z informacjami o realizowanych sprawach i dostępem do dokumentów z postępowań. Ponadto projekt zakładał zmodyfikowanie systemów „Cyfrowa Książka Obiektu Budowlanego" (zawierający m.in. dane o właścicielu czy zarządcy i uwzględniający możliwość podglądu książki poprzez integrację z systemem) czy też system „eBudownictwo Wnioski" służący do generowania i bezpośredniego składania wniosków w procesie budowlanym, z konta użytkownika, na którym wnioski można gromadzić oraz sprawdzać status swojej sprawy. Wobec tych informacji organ nadzorczy zwrócił uwagę na niezbędność przeprowadzenia analizy obowiązujących przepisów prawa, która pozwoliłaby na ustalenie podstawy prawnej przetwarzania, przypominając, że w przypadku przetwarzania danych w zakresie niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze, zastosowanie

[266] DOL.060.25.2024, DOL.060.24.2024, DOL.060.35.2024, DOL.060.39.2024, DOL.060.42.2024.
[267] Zob. komunikat Prezesa Urzędu Ochrony Danych Osobowych z 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 666).
[268] DOL.401.344.2024, DOL.401.345.2024.
[269] DOL.060.36.2024.

znajduje art. 6 ust. 3 RODO, zgodnie z którym podstawa przetwarzania musi być określona w prawie państwa członkowskiego, któremu podlega administrator. Wskazano jednocześnie, że w odniesieniu do procesów przetwarzania danych osobowych ryzyka naruszenia praw lub wolności podmiotów danych określone powinny zostać w drodze testu prywatności. Beneficjent częściowo uwzględnił przedstawione uwagi i zapowiedział przeprowadzenie DPIA w kolejnej wersji projektu założeń.

Analogiczne uwagi przedstawiono w przypadku opiniowania **projektu „Cyfrowe Udostępnienie Zasobów Kultury Studia Filmów Rysunkowych w Bielsku-Białej”**[270]. Z opisu założeń wynikało, że jednym z produktów końcowych projektów będzie „Rejestr użytkowników platformy VOD”. Mimo to w opisie nie określono sposobów technicznych, które wprost odnosiłyby się do zapewnienia bezpieczeństwa danych przetwarzanych w rejestrze. Nie zostało też wyjaśnione, na podstawie jakiej przesłanki legalizującej miałoby się odbywać przetwarzanie danych osobowych. Także w tym przypadku beneficjent zobowiązał się do przeprowadzenia oceny skutków oraz uwzględnił uwagi organu nadzorczego.

Projekt „Usługi cyfrowe dla bezzałogowych statków powietrznych”[271] zakładał uruchomienie systemów teleinformatycznych w podmiotach wykonujących zadania publiczne” – Systemu KSID oraz DTM Autonomia. Zważywszy na możliwe przetwarzanie danych osobowych w powyższych systemach, poddano pod rozwagę przeprowadzenie analizy obowiązujących i projektowanych przepisów prawa oraz stosownej oceny skutków.

Szczególną uwagę organ nadzorczy poświęcił **projektowi „Portfel Aplikacji Zdrowotnych”**[272], mając na uwadze charakter udostępnianego portalu, w przypadku którego może dochodzić do przetwarzania danych dotyczących zdrowia (a więc szczególnych kategorii w rozumieniu art. 9 ust. 1 RODO). Zwrócono uwagę na konieczność określenia właściwej podstawy ustawowej dla przetwarzania danych osobowych użytkowników portalu i aplikacji udostępnianych w tym portalu, a także na rozważenie przyjęcia bardziej kompleksowego podejścia do koncepcji zapewnienia poufności danych, obejmującego poza przyznawaniem zakładanych przez projekt certyfikatów bezpieczeństwa również środków takich jak regularne testy bezpieczeństwa, aktualizacje i monitorowanie potencjalnych zagrożeń.

Na bezwzględną konieczność wprowadzenia ustawowej podstawy prawnej przetwarzania wskazano w opinii do **projektu „eHemofilia”**[273], który mimo dostrzeżenia potrzeby zmian w prawie, błędnie kierunkował na zmiany w rozporządzeniu Ministra Zdrowia z 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, jako na podstawę regulującą dokumentacje medyczne prowadzone dla pacjenta z hemofilią. Organ

[270] DOL.060.45.2024.
[271] DOL.060.9.2024.
[272] DOL.060.35.2024.
[273] DOL.060.54.2024.

nadzorczy zwrócił uwagę, że kwestie związane ze sposobem prowadzenia rejestrów, które wyznaczają zakres ingerencji w autonomię informacyjną jednostki, powinny zostać uregulowane w ustawie.

Na podobny problem zwrócono uwagę przy opiniowaniu projektu **Rejestr Podmiotów Wykonujących Działalność Leczniczą 2.0**[274]. W raporcie z wykonania projektu nie przewidziano konieczności dokonania zmian w prawie. Wskazano natomiast powstanie, jako produktów końcowych projektu, „Zmodyfikowanego Rejestru Podmiotów Wykonujących Działalność Leczniczą" oraz „Zmodyfikowanego Systemu RPWDL obsługującego Rejestr Podmiotów Wykonujących Działalność Leczniczą", który będzie komplementarny względem licznie wymienionych produktów innych projektów – m.in. systemów UEOZ (ePLOZ), REGON, RPM Rejestr Pracowników Medycznych czy Centralna Baza Adresowa. Zważywszy na niedookreślenie pojęcia „komplementarności" systemów oraz możliwe przetwarzanie danych osobowych, organ nadzorczy wskazał, że niezbędne jest przeprowadzenie analizy obowiązujących przepisów prawa w tym zakresie pozwalającej na określenie podstawy prawnej przetwarzania. Zwrócił też uwagę, że przetwarzanie danych osobowych przez podmioty publiczne odbywać powinno się na podstawie przepisów prawa, które w sposób precyzyjny wskazują, jakie dane będą przetwarzane, w jakim celu, przez jaki okres oraz kto będzie za to przetwarzanie odpowiadał.

Na problematykę łączenia zbiorów Prezes UODO zwrócił także uwagę, odnosząc się do **projektu informatycznego „CEZAM – Portal klienta**[275]**"**. System ten zakładał przetwarzanie danych osobowych klientów i interesantów Głównego Urzędu Miar. Ponadto przewidywał powiązanie go za pomocą protokołów API z rejestrami państwowymi, m.in. CEIDG oraz KRS, z których pobierane mają być dane o przedsiębiorcach czy innych osobach. W przekazanej opinii podniósł, że w kontekście planowanego systemu szczególnie istotne jest wykazanie, że przewidywany zakres przetwarzanych danych jest niezbędny do realizacji zadań publicznych wynikających z przepisów ustawy Prawo o miarach, szczególnie w perspektywie planowanej integracji z innymi rejestrami państwowymi. Ponadto zaznaczył, że wymagane jest przyjęcie takich rozwiązań organizacyjnych i technicznych, które ograniczą dostęp jedynie do danych w zakresie realnie adekwatnym do wypełnienia obowiązku prawnego ciążącego na administratorze lub wykonania zadania realizowanego w interesie publicznym.

Organ nadzorczy pozytywnie ocenił dostrzeganie przez niektórych twórców projektów informatycznych zagadnień związanych z włączaniem aspektów ochrony danych osobowych w rozwój usług cyfrowych.

Podsumowując ten rok opisanych relacji z KRMC i beneficjentami projektów informatycznych, Prezes UODO zgłosił do Komitetu postulat, aby w ramach jego prac resorty czy podmioty publiczne odpowiedzialne za poszczególne projekty informatyczne: przeprowadzały ocenę skutków dla ochrony danych na etapie OPZI i kolejnych etapach realizacji projektów informatycznych, właściwie weryfikowały

[274] DOL.060.14.2024.
[275] DOL.060.48.2024.

przyjęcie w procesie legislacyjnym podstawy prawnej przetwarzania danych osobowych dla celów realizacji danego projektu. W odpowiedzi Sekretarz KRMC zapewniła o przyjęciu rozwiązań, które miałyby doprowadzić do zintensyfikowania działań związanych ze stosowaniem i wdrażaniem przepisów ogólnego rozporządzenia o ochronie danych w rozpatrywanych dokumentach. Od beneficjentów i wnioskodawców projektów informatycznych – na skutek tych działań Prezesa UODO – wymagane jest włączanie testu prywatności obejmującego m.in. ocenę skutków dla ochrony danych do opisu założeń danego projektu informatycznego i na poszczególnych etapach jego realizacji i podsumowania. Do przedstawionych deklaracji organ nadzorczy odnosi się bardzo pozytywnie, traktując je jako dobrą prognozę dla opracowywania w przyszłości projektów optymalnych z punktu widzenia zasad określonych w RODO.

6.10. Sprawy przed sądami powszechnymi

Oprócz praw określonych w art. 15–22 RODO oraz prawa wniesienia skargi do Prezesa UODO (na podstawie art. 77 RODO), każdy z podmiotów danych ma również **prawo do wystąpienia z powództwem do sądu cywilnego** oraz do wystąpienia z roszczeniem o wypłatę **odszkodowania za naruszenie przepisów** o ochronie danych osobowych, które spowodowało szkodę majątkową lub niemajątkową (art. 79 i 82 RODO).

Prawo osoby, której dane dotyczą do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu, zostało wprowadzone na podstawie art. 79 i art. 82 RODO i uszczegółowione z punktu widzenia procesowego w przepisach art. 92–99 ustawy z 10 maja 2018 roku o ochronie danych osobowych.

W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 RODO, właściwy jest sąd okręgowy (o czym przesądza art. 93 ustawy o ochronie danych osobowych). Jego obowiązkiem jest (stosownie do art. 94 ust. 1 powołanej ustawy) niezwłoczne zawiadomienie Prezesa UODO o wniesieniu pozwu oraz o prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych. Zgodnie natomiast z art. 94 ust. 2 ustawy, Prezes UODO zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed nim lub przed sądem administracyjnym, albo została zakończona. Prezes UODO niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.

Ustawa o ochronie danych osobowych przewiduje daleko idące konsekwencje procesowe dotyczące sytuacji, w której sąd oraz organ nadzorczy rozpatrują to samo roszczenie o naruszenie przepisów o ochronie danych osobowych:

1) Zgodnie bowiem z art. 95 ustawy o ochronie danych osobowych sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed organem nadzorczym.

2) Ponadto, na podstawie art. 96 ustawy o ochronie danych osobowych, sąd jest zobowiązany do umorzenia postępowania w zakresie, w jakim prawomocna decyzja organu nadzorczego o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a § 3^4 ustawy z 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem.
3) Zgodnie natomiast z art. 97 ustawy o ochronie danych osobowych ustalenia prawomocnej decyzji organu nadzorczego o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi wiążą sąd okręgowy w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.

Rok 2024 był rokiem ponownej oceny realizacji przez sądy obowiązków wynikających z RODO i ustawy o ochronie danych osobowych. Prezes UODO kilkakrotnie na przestrzeni lat występował z prośbą do prezesów sądów apelacyjnych o zasygnalizowanie sądom okręgowym, działającym w obszarze kompetencji właściwego sądu apelacyjnego, konieczności uwzględniania w ich działalności należycie wykonywanego obowiązku wynikającego z art. 94 ust. 1 ustawy o ochronie danych osobowych[276]. Pierwsze wystąpienie miało miejsce w kwietniu 2022 r. Organ nadzorczy zwrócił w nim uwagę m.in. na znikomą liczbę otrzymywanych zawiadomień, a także pewne braki w zakresie przekazywanych informacji, takie jak:

- informowanie tylko o prawomocnym orzeczeniu kończącym postępowanie w sprawie bez uprzedniego przekazania informacji o wniesieniu pozwu w takiej sprawie,
- w razie informacji o wniesieniu pozwu brak wystarczających informacji, które umożliwiałyby zidentyfikowanie powoda. Z reguły jest to tylko imię i nazwisko lub ogólnie określony przedmiot postępowania, co utrudnia, a w praktyce wręcz uniemożliwia stwierdzenie, czy organ nadzorczy prowadzi postępowanie administracyjne na skutek skarg tych samych osób i w tym samym zakresie. To z kolei czyni wysoce utrudnioną lub wręcz niemożliwą do realizacji dyspozycję art. 94 ust. 2 ustawy o ochronie danych osobowych,
- brak wskazania konkretnych przepisów o ochronie danych osobowych, w związku z naruszeniem których doszło do złożenia pozwu, co uniemożliwia organowi nadzorczemu stwierdzenie, czy przedmiot prowadzonego przez niego postępowania administracyjnego jest tożsamy ze zgłoszoną sprawą o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych.

Choć wystąpienie Prezesa UODO spotkało się z pozytywnym przyjęciem ze strony Prezesów Sądów Apelacyjnych, a po jego przekazaniu do sądów okręgowych organ nadzorczy odnotował ich zwiększoną aktywność w realizacji ww. obowiązków

[276] DOL.413.12.2021.

informacyjnych, to po upływie kilku miesięcy liczba przekazywanych zawiadomień o wniesieniu pozwu wróciła do poprzedniego poziomu, zaś liczba zawiadomień o prawomocnych orzeczeniach kończących postępowanie sądowe pozostawała w dalszym ciągu niewielka. Poza tym obowiązki informacyjne wciąż realizowane były fragmentarycznie.

W związku z tym Prezes UODO w maju 2023 r. zdecydował o ponowieniu wystąpienia do sądów apelacyjnych. Dodatkowo zasygnalizował w nim inne problemy zaobserwowane w działalności sądów okręgowych, a związane z wypełnianiem przez nie obowiązków wynikających z art. 94 ust. 1 ustawy o ochronie danych osobowych, głównie w zakresie informacji dotyczących danych identyfikujących strony czy sprawę. Jednocześnie zwrócił się z prośbą o rozważenie podjęcia dodatkowych działań, które umożliwią sądom okręgowym właściwą realizację zadań w tym obszarze.

Opisane powyżej działania nie przyczyniły się do znaczącej zmiany sytuacji, dlatego w 2024 r. w UODO rozpoczęły się prace koncepcyjno-analityczne mające doprowadzić (w porozumieniu ze środowiskiem sądów cywilnych i Ministerstwem Sprawiedliwości) do ustandaryzowania sposobu i zakresu informacji przekazywanych między sądami a Prezesem UODO, co powinno usprawnić wzajemną komunikację.

W ocenie organu nadzorczego jest to bardzo istotne, gdyż wszelkie ułomności w tym zakresie powodują wiele istotnych ryzyk, takich jak m.in.:

- nieprawidłowa realizacja obowiązków określonych rozdziale 10 ustawy o ochronie danych osobowych zarówno przez sądy, jak i Prezesa UODO,
- brak możliwości realizowania przez Prezesa UODO jego uprawnień określonych w art. 98–99 ustawy o ochronie danych osobowych, w tym:
    - wstępowania, za zgodą powoda, do postępowania sądowego o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, w sprawach, które zdaniem Prezesa UODO wymagają jego udziału,
    - przedstawiania istotnego poglądu w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych,
- obarczenie wydanych wyroków wadami prawnymi.

Podkreślić należy, że prawidłowa realizacja przez sądy obowiązku nałożonego na nie mocą art. 94 ust. 1 ustawy o ochronie danych osobowych ma zapewnić równorzędny poziom gwarancji ochrony danych osobom, których dane dotyczą, w sprawach rozpatrywanych przed sądem powszechnym i organem nadzorczym, a przede wszystkim sprzyjać wyeliminowaniu istotnej rozbieżności w ocenie prawnej stanów faktycznych w sprawach o podobne naruszenia rozpatrywanych przez te podmioty.

Realizując natomiast uprawnienie Prezesa UODO wynikające z art. 98 i 99 ustawy o ochronie danych osobowych, poprzez przystępowanie do toczących się postępowań za zgodą powodów w sprawach, które zdaniem Prezesa UODO wymagają jego udziału, czy też przedstawiając istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, Prezes

UODO ma na celu realizację bardziej spójnego stosowania przepisów o ochronie danych osobowych przez sądy, aby prawa osób, których dane dotyczą, były właściwie respektowane. Działania te mają również na uwadze wspieranie sądów w stosowaniu orzecznictwa Europejskiego Trybunału Praw Człowieka (ETPCz) i Trybunału Sprawiedliwości Unii Europejskiej (TSUE), w tym zwłaszcza tych wyroków, które dotyczą wykładni pojęcia i rozmiaru szkody w rozumieniu art. 82 RODO, jak np. wyrok TSUE z 4 maja 2023 r. w sprawie C-300/21; wyrok z 20 czerwca 2024 r. w sprawach połączonych C-182/22 i C-189/22, wyrok z 4 października 2024 r. w sprawie C-507/23).

Realizacja powyższych działań ma tym większe znaczenie, że jak wynika z wystąpienia Prezesa UODO skierowanego do Ministra do spraw Unii Europejskiej[277], nie wszystkie wyroki TSUE zostały odpowiednio transponowane do prawa krajowego.

W związku z brakiem właściwego przepływu informacji między sądami a Prezesem UODO, w 2024 r. organ nadzorczy przesłał pisma informujące o stanie spraw jedynie do 14 sądów okręgowych, które przekazały do UODO niezbędne informacje o toczącym się postępowaniu cywilnym w sprawie o naruszenie danych osobowych.

6.11. 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 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.

Przedstawione w powyższych podrozdziałach zagadnienia nie wyczerpują wszystkich kwestii, które poruszone zostały w minionym roku w czasie opiniowania projektów aktów prawnych przez organ nadzorczy. To materiał poglądowy, punktowo wskazujący problemy, które mają wymiar pierwszoplanowy ze względu na sprawy, których dotyczą. Jakkolwiek wiele z projektów oceniono negatywnie, to należy mieć na względzie, że do organu nadzorczego wpływały również projekty, które jako zgodne ze standardami ochrony danych osobowych nie wymagały jego uwag. Za przykład posłużyć może **projekt ustawy o zmianie ustawy o przetwarzaniu danych dotyczących przelotu pasażera**[278]. Prezes Urzędu Ochrony Danych Osobowych ocenił pozytywnie zaproponowane w nim zmiany mające zapewnić dostosowanie

[277] DOL.413.14.2024; opisane bardziej szczegółowo w części „Wystąpienia”; jednocześnie planowane jest skierowanie kolejnych wystąpień do resortów odpowiedzialnych za wdrożenie poszczególnych wyroków TSUE.
[278] DOL.401.474.2024.

przepisów ustawy o przetwarzaniu danych dotyczących przelotu pasażera do wyroku Trybunału Sprawiedliwości Unii Europejskiej[279].

Analiza spraw prowadzonych w roku 2024 dowodzi, że zaangażowanie organu nadzorczego w sferze tworzenia prawa stale rośnie. Konsekwentne działania podejmowane przez Prezesa UODO odnoszą pozytywne rezultaty i skutkują zwiększeniem wśród projektodawców świadomości co do konieczności wdrażania rozwiązań sprzyjających ochronie danych osobowych. Organ nadzorczy stale poszerza krąg swojego oddziaływania, podejmując aktywne inicjatywy opiniowania z urzędu zarówno projektów aktów prawnych *sensu stricto*, jak i innych aktów o silnym oddziaływaniu w sferze publicznej i społecznej, takich jak plany strategiczne rozwoju państwa czy projekty informatyczne. W opiniach tego drugiego rodzaju organ wypowiada się ze względu na charakter dokumentów – rozłożonych na lata strategii mających horyzontalny wpływ na regulacje prawne, funkcjonowanie państwa, ale i prawa oraz wolności osób, podmiotów praw objętych takimi regulacjami.

W porównaniu z rokiem ubiegłym przede wszystkim pozytywnie należy ocenić odsetek projektodawców decydujących się w dużo większym stopniu niż w latach ubiegłych na uwzględnienie, choćby i częściowo, eksperckich wskazówek przedłożonych przez organ nadzorczy. Widocznej poprawie uległ poziom świadomości co do wagi uwzględniania prawa do prywatności oraz autonomii informacyjnej w procesach legislacyjnych. Znacząco wzrosła także gotowość do podejmowania dialogu i roboczej współpracy celem wypracowania optymalnych rozwiązań – pogodzenia celów projektowanych regulacji ze standardami przetwarzania danych osobowych.

Z drugiej strony nie sposób jednak pominąć aspekty negatywne. Odsetek projektów, w których zdecydowano się na przeprowadzenie testu prywatności jako elementu oceny skutków dla ochrony danych, uznać należy w dalszym ciągu za głęboko niezadowalający, bo nieobejmujący wszystkich przypadków, zważywszy warunki wymagane regulacją RODO – rodzaj przetwarzania, w szczególności z użyciem nowych technologii, wzgląd na charakter, zakres, kontekst i cele oraz duże prawdopodobieństwo możliwego powodowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Co się z tym wiąże również aspekty stosowania zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych są notorycznie pomijane, co w wielu przypadkach ma kaskadowe konsekwencje dla jakości projektowanych aktów pod względem gwarancji dla osób, których dane dotyczą.

Zasadniczym problemem jest jednak wciąż przede wszystkim brak przeprowadzenia gruntownego przeglądu obecnie obowiązujących przepisów pod względem konieczności ich dostosowania do standardów rozporządzenia 2016/679,

[279] Zob. wyrok Trybunału Sprawiedliwości UE z 21 czerwca 2022 r. sygn. C-817/19 w sprawie Ligue de droits humains vs Conseil des ministres. Nadmienić jednocześnie należy, że TSUE zauważył potrzebę implementacji w prawach krajowych państw członkowskich art. 13 dyrektywy 2016/681, który przewiduje możliwość dochodzenia przez pasażera odszkodowania, jak również uprawnia go do dochodzenia roszczeń na drodze sądowej. Kierując się tą wytyczną Trybunału oraz Oświadczeniem EROD 2/2025 w sprawie wdrożenia dyrektywy PNR w świetle ww. wyroku TSUE, w dodatkowej opinii z 2025 r. Prezes UODO zwrócił projektodawcy uwagę na to zagadnienie.

ale również dyrektywy 2016/680[280]. W obiegu prawnym pozostają regulacje, które nie zostały dostosowane do wymogów stawianych przez wymienione akty unijne. Jest to tym bardziej istotne w perspektywie wchodzenia w życie kolejnych aktów unijnych, wymagających roztropnej implementacji do prawa krajowego: aktu o sztucznej inteligencji, rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia czy rozporządzenia w sprawie europejskiego zarządzania danymi. Brak podjęcia koniecznych rozwiązań legislacyjnych w perspektywie kolejnych lat budzi obawy co do dalszego nawarstwiania się problemu, zwłaszcza że nowe akty prawa unijnego nie obniżają standardów ochrony danych i odwołują się do konieczności zapewnienia zgodności z przepisami o ochronie danych osobowych nowych form, sposobów i procesów przetwarzania informacji. Wprowadzanie nowych aktów unijnych oraz nowych sposobów i celów przetwarzania danych osobowych wymaga przeglądu i zmian prawa regulującego korzystanie przez instytucje publiczne z rejestrów państwowych / publicznych. Ma to fundamentalne znaczenie z punktu widzenia ryzyk związanych z profilowaniem danych osobowych i wykorzystywaniem systemów sztucznej inteligencji dla realizacji zadań publicznych.

Efektem braku uwzględnienia uwag organu nadzorczego, zarówno co do projektów z roku 2024, jak i z lat poprzednich, jest funkcjonowanie w obiegu aktów prawa budzących poważne wątpliwości w zakresie ich stosowania, co Prezesowi Urzędu stale sygnalizują podmioty danych, inspektorzy ochrony danych, administratorzy, różnego rodzaju instytucje przedstawicielskie. Niestety, w procesach legislacyjnych dostrzegalna jest tendencja do powielania błędnych rozwiązań i kontynuowania złych praktyk, szczególnie uwidoczniona przy stanowieniu procesów przetwarzania w rejestrach państwowych zakładających łączenie zasobów i opierających przetwarzanie na aktach nieposiadających przymiotu prawa powszechnie obowiązującego, takich jak umowy czy porozumienia. Problem ten, ze względu na rosnące tendencje do digitalizacji procesów państwowych, ulega jedynie nasileniu. Jako przykład braku uwzględnienia zmian, o które od lat postuluje Prezes UODO, wskazać można przepisy dotyczące wdrażania aplikacji mObywatel i jej stosowania dla obsługi kolejnych usług państwa dla obywateli. Uwagi i obawy podnoszone przez organ nadzorczy na gruncie przedstawionych wówczas opinii pozostają bowiem aktualne[281] oraz wymagają dostosowania do kolejnej regulacji europejskiej, jaką jest rozporządzenie eIDAS 2.0[282] określające standardy funkcji europejskiego portfela tożsamości cyfrowej oraz certyfikatu podpisu elektronicznego. Dostrzegając liczne trudności w procesach legislacyjnych, w tym potrzebę horyzontalnych przeglądów i zmian regulacji obowiązujących oraz zapewniania

[280] 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 (Dz.U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.).
[281] DOL.401.169.2022, DOL.401.276.2022.
[282] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.U. UE. L. z 2024, nr 1183 z 2024.04.30).

stosowania regulacji europejskich, Prezes Urzędu, biorąc pod uwagę pozytywne aspekty, na które wskazano w powyższej części sprawozdania, wyraża jednak nadzieję, że perspektywa kolejnych lat zaowocuje dalszym korzystnym wzrostem zaangażowania projektodawców co do wdrażania aspektów związanych z ochroną danych osobowych w procesach tworzenia prawa. Liczy, że drogą kooperacji i dialogu wyzwania nadchodzących lat, związane przede wszystkim z postępującą reformacją cyfrową, uda się przezwyciężyć, wdrażając rozwiązania prawne służące dobrostanowi obywateli oraz sprzyjające pełnemu odzwierciedleniu konstytucyjnych praw do prywatności i autonomii informacyjnej.

7. 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. 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 **2 wnioski o przeprowadzenie uprzednich konsultacji.** W poprzednim roku wpłynęło ich 3, w 2022 – 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, że 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. Zagadnienie to ma podstawowe znaczenie i wymaga uprzedniej prawidłowej oceny. Innymi słowy, ocena skutków dla ochrony danych jest dalszym etapem, do którego można przejść dopiero wtedy, gdy określone przetwarzanie danych osobowych przez wskazany podmiot jest dopuszczalne w świetle przesłanek legalności przetwarzania danych osobowych.

Wniesione w 2024 r. wnioski o uprzednie konsultacje nie zostały poprzedzone przez administratorów analizami w zakresie istnienia podstaw prawnych do planowanego przez nich procesu przetwarzania danych osobowych, co spowodowało, że nie mogły zainicjować postępowania i udzielenia zaleceń. Brak podstawy prawnej do przetwarzania powoduje, że planowane przetwarzanie nie może się odbyć i ani ocena skutków dla ochrony danych, ani procedura uprzednich konsultacji nie będą rozwiązaniem pozwalającym na wyeliminowanie tej przeszkody.

Przykładem takiej sytuacji był wniosek o udzielenie uprzednich konsultacji w przedmiocie wskazania podstaw prawnych do udostępnienia danych[283]. Prezes UODO wyjaśnił, że tego rodzaju wątpliwości powinny być rozstrzygane na podstawie właściwych przepisów określających kompetencje i uprawnienia podmiotu zwracającego się o dostęp do danych, nie zaś w trybie uruchamianym na podstawie art. 36 RODO.

Niezależnie od powyższego Prezes UODO poinformował, że przepisy dotyczące uprzednich konsultacji zawarte zarówno w RODO (art. 36 ust. 1), jak i w ustawie ochronie danych osobowych (art. 57 ust. 1) wskazują, że podmiotem uprawnionym do wystąpienia z wnioskiem o uprzednie konsultacje jest administrator. W analizowanej sprawie podpis wniosku o uprzednie konsultacje budził wątpliwość, gdyż osoba go składająca nie wykazała, że jest uprawniona do reprezentowania wskazanego we wniosku administratora, np. poprzez załączenie stosownego pełnomocnictwa (upoważnienia) do jego reprezentowania.

Inny z wniosków złożony przez podmiot publiczny – również niewłaściwie nazwany przez zgłaszającego „wnioskiem o uprzednie konsultacje" – dotyczył zasadności udostępnienia wszystkich danych osobowych zgromadzonych w konkretnym zbiorze, w związku z realizacją obowiązków związanych z ponownym wykorzystywaniem informacji sektora publicznego[284]. Wniosek ten nie podlegał procedurze uprzednich konsultacji, ponieważ administrator nie miał podstaw prawnych do wskazanego procesu przetwarzania. Dodatkowo wniosek nie spełniał wymogów formalnych, gdyż został złożony przez osobę, która nie przedstawiła stosownego pełnomocnictwa do działania w imieniu administratora w zakresie złożenia wniosku o uprzednie konsultacje.

8. 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

[283] DOL.5100.1.2024.
[284] DOL.5100.2.2024.

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.

Organ nadzorczy nieustannie zachęca do podejmowania prac w zakresie przygotowania kodeksu postępowania. W 2024 r. miało to miejsce m.in.:

- podczas spotkań z przedstawicielami branż/sektorów planujących prace w zakresie przygotowania kodeksów postępowania – pracownicy UODO omawiali zasady przygotowania kodeksów postępowania oraz procedurę ich zatwierdzenia przez Prezesa Urzędu,
- w ramach cyklu webinariów organizowanych przez UODO pt. „Certyfikacja w ochronie danych" – na prośbę uczestników tematem jednego z siedmiu spotkań było omówienie (zestawienie podobieństw i różnic) kodeksów postępowania (art. 40 RODO) i certyfikacji (art. 42–43 RODO), czyli dwóch dobrowolnych narzędzi zgodności przewidzianych w RODO dla administratorów i podmiotów przetwarzających.

Kodeksy postępowania mogą być sporządzone, a następnie przedkładane organowi nadzorczemu do zatwierdzenia przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające.

Procedura zatwierdzenia kodeksu postępowania składa się z kilku etapów. Po złożeniu wniosku w sprawie zatwierdzenia kodeksu postępowania, organ nadzorczy bada, czy przedłożony projekt spełnia **wymogi formalne**[285] **oraz kryteria dopuszczalności**[286], o których mowa w Wytycznych EROD 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, (dalej: Wytyczne EROD 1/2019). Po zakończeniu tej wstępnej oceny, jeśli wniosek lub projekt kodeksu wymaga uzupełnień, organ nadzorczy kieruje do wnioskodawcy pismo, wyznaczając termin na uzupełnienie.

Gdy wniosek i projekt kodeksu nie wymagają zmian lub gdy wnioskodawca uzupełni wskazane braki, możliwe jest przejście do kolejnego etapu, tj. **do pełnej oceny treści przedłożonego projektu w świetle kryteriów zatwierdzania kodeksów**[287]. Etap ten służy wyjaśnieniu treści projektu z wnioskodawcą, umożliwiając mu wprowadzenie ewentualnych modyfikacji. Kończy się on wydaniem przez organ nadzorczy **opinii o zgodności przedłożonego projektu z przepisami RODO**.

Ostatni etap obejmuje **zatwierdzenie kodeksu postępowania w formie decyzji administracyjnej**, o ile organ nadzorczy uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO.

---

[285] Art. 40 RODO, art. 27 ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781), art. 63 i nast. Kodeksu postępowania administracyjnego.

[286] Pkt. 19-31 Wytycznych EROD 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.

[287] Pkt. 32-41 Wytycznych EROD 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.

Zatwierdzone kodeksy postępowania są następnie rejestrowane przez Prezesa UODO i EROD. Do zmiany zatwierdzonego kodeksu postępowania lub jego rozszerzenia stosuje się tę samą procedurę. 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 sektor publiczny, jak i prywatny dostrzega potrzebę i zalety korzystania z tego typu narzędzia, które pozwoli im wykazać rozliczalność, o której mowa w art. 5 ust. 2 RODO. Organ nadzorczy publikuje informacje nt. podmiotów, które złożyły wnioski o zatwierdzenie kodeksu postępowania oraz o inicjatywach, które rozpoczęły prace nad projektami kodeksów.

8.1. Kodeksy postępowania zatwierdzone przez organ nadzorczy

W 2024 roku organ nadzorczy nie zatwierdził żadnego kodeksu postępowania, ale niektóre projekty kodeksów postępowania są na końcowym etapie ich oceny merytorycznej.

8.2. Nowe wnioski o zaopiniowanie kodeksów postępowania

W październiku 2024 r. do Prezesa Urzędu Ochrony Danych Osobowych wpłynął wniosek o zatwierdzenie „Kodeksu postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej”. Wniosek został złożony przez Związek Pracodawców Branży Internetowej Interactive Advertising Bureau Polska[288]. Organ nadzorczy przeprowadził ocenę formalną i w zakresie spełnienia kryteriów dopuszczalności wniosku i projektu kodeksu postępowania.

8.3. Postępowania prowadzone w 2024 r. w sprawie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone we wcześniejszych latach

W okresie sprawozdawczym kontynuowane były postępowania w sprawie zatwierdzenia:

- kodeksu postępowania dla centrów handlowych Polskiej Rady Centrów Handlowych[289],
- kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencje badawcze[290]. Wniosek o zatwierdzenie ww. kodeksu został złożony przez Organizację Firm Badania Opinii i Rynku (OFBOR),
- kodeksu postępowania Krajowej Izby Doradców Podatkowych[291],

[288] DOL.4421.2.2024.
[289] DOL.4421.3.2020.
[290] DOL.4421.2.2020.
[291] DOL.4421.1.2020.

- kodeksu postępowania dla branży hotelarskiej[292]. Wnioskodawcą w postępowaniu w sprawie zatwierdzenia tego kodeksu jest Izba Gospodarcza Hotelarstwa Polskiego.

W 2024 r. na wniosek Sieci Badawczej Łukasiewicz – PORT, Polski Ośrodek Rozwoju Technologii z siedzibą we Wrocławiu[293], Prezes UODO wydał postanowienie w sprawie zawieszenia postępowania dotyczącego zatwierdzenia „Kodeksu postępowania w sprawie przetwarzania danych osobowych dla celów badań naukowych przez biobanki w Polsce". Projekt kodeksu był na etapie oceny merytorycznej.

8.4. Współpraca organu nadzorczego z inicjatywami opracowania kodeksów postępowań

W 2024 r. organ nadzorczy pozostawał również w kontakcie z inicjatywami przygotowującymi projekty kodeksów postępowania, które nie złożyły jeszcze wniosków o ich zatwierdzenie:

1) Odbyło się kilka spotkań z przedstawicielami Związku Pracodawców Innowacyjnych Firm Farmaceutycznych INFARMA, którzy przygotowali projekt kodeksu postępowania dotyczący przetwarzania danych osobowych w branży badań medycznych. Po wstępnych uwagach Urzędu dokument ten ma zostać poprawiony. Jednocześnie na wiosnę 2025 r. planowane jest przeprowadzenie konsultacji społecznych.
2) Pracownicy Urzędu spotkali się także z przedstawicielami Związku Województw Rzeczypospolitej Polskiej oraz Instytutu Szkoleniowo-Doradczego z Łodzi w celu omówienia przebiegu dalszych prac nad kodeksem postępowania z danymi osobowymi w jednostkach samorządu terytorialnego. Rozmowy na temat kodeksu postępowania dla tego sektora były prowadzone również w ramach cyklu spotkań z przedstawicielami i organizacjami zrzeszającymi jednostki samorządu terytorialnego wszystkich szczebli[294]. Uczestniczył w nich Zastępca Prezesa UODO. Więcej informacji na temat tych spotkań znajduje się na stronie internetowej UODO w zakładce Aktualności oraz w Biuletynie UODO Nr 12_01/12_01/24_25 (w artykule pt. „UODO zachęca jednostki samorządu terytorialnego do opracowania kodeksu postępowania").
3) Odbyło się też spotkanie z przedstawicielami środowiska sportowego, które planuje opracowanie kodeksu postępowania dla swojej branży.
4) Grupa organizacji pozarządowych, pod przewodnictwem Fundacji Onkologicznej Alivia, prowadzi z UODO konsultacje w sprawie kodeksu postępowania w zakresie ochrony danych osobowych w sektorze organizacji pozarządowych.

[292] DOL.4421.1.2023.
[293] DOL.4421.1.2021.
[294] Unią Metropolii Polskich, Związkiem Miast Polskich, Związkiem Gmin Wiejskich, Związkiem Województw Rzeczypospolitej Polskiej, Związkiem Powiatów Polskich.

Przydatne informacje dla środowisk planujących prace nad kodeksami postępowania dostępne są na stronie internetowej UODO[295].

Od chwili rozpoczęcia stosowania RODO zatwierdzone zostały jedynie 2 kodeksy postępowania, co dowodzi, że praca nad tymi dokumentami nie jest łatwa. Środowiska podejmujące się ich stworzenia popełniają błędy, które często wpływają na wydłużenie procedury zatwierdzenia kodeksu, zawieszenie prac nad projektem, a nawet całkowite zaniechanie przygotowania takiego dokumentu[296].

Dlatego organ nadzorczy, biorąc pod uwagę kompetencje określone w RODO[297], aktywnie wspiera wszystkie inicjatywy pracujące nad kodeksami postępowania i zachęca kolejne środowiska do podjęcia działań w tym zakresie.

W tym celu:

- przygotowuje materiały informacyjno-edukacyjne i publikuje je na swojej stronie internetowej, w zakładce Kodeksy postępowania, wraz z informacją o: organizacjach pracujących nad kodeksami, wnioskach, które wpłynęły do Prezesa UODO w sprawie zatwierdzenia kodeksów oraz o zatwierdzonych kodeksach postępowania i akredytowanych podmiotach monitorujących,
- z inicjatywy podmiotów zainteresowanych opracowaniem kodeksu postępowania – organizuje spotkania robocze, podczas których pracownicy UODO omawiają warunki, jakim musi odpowiadać projekt kodeksu postępowania i wniosek o jego zatwierdzenie, aby mogła zostać wszczęta procedura w sprawie zatwierdzenia kodeksu przed Prezesem UODO oraz zatwierdzenie kodeksu w formie decyzji administracyjnej. Informacja o takich

[295] https://uodo.gov.pl/pl/p/dla-administratora.

[296] 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, tj. 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 ustępu 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 w kodeksie przepisów RODO lub ustawy o ochronie danych osobowych bez praktycznego wyjaśnienia ich stosowania, niewskazanie w kodeksie przepisów sektorowych oraz 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.

[297] Art. 40 ust. 1 RODO, art. 57 ust. 1 lit. m RODO.

spotkaniach jest publikowana w „Aktualnościach” na stronie internetowej UODO,

- w ramach cyklu webinariów poświęconych certyfikacji, które UODO prowadził w 2024 r., na prośbę słuchaczy, podczas jednego ze spotkań został również omówiony temat dotyczący kodeksów postępowania i certyfikacji, w tym różnice i zalety tych dwóch narzędzi zgodności z RODO.

Warto odnotować, że 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.

9. Akredytacja podmiotów monitorujących kodeksy postępowania

Za monitorowanie przestrzegania kodeksu postępowania adresowanego do podmiotów sektora prywatnego, 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. 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”[298].

Natomiast kodeksy obejmujące podmioty sektora publicznego, choć nie podlegają obowiązkowi wskazania podmiotu monitorującego (art. 41 ust. 6 RODO), to muszą zawierać skuteczny 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.

Zaletą odpowiednio przygotowanego kodeksu jest nie tylko gwarancja pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy, ale także nadzór nad procesami przetwarzania danych osobowych (do których ma zastosowanie zatwierdzony kodeks) przez niezależny podmiot monitorujący, a w przypadku podmiotów publicznych – np. przez audytora lub osoby realizujące zadania kontroli wewnętrznej.

[298] 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 – https://uodo.gov.pl/pl/426/2788.

9.1. Wnioski o udzielenie akredytacji do monitorowania kodeksów postępowania

W 2024 r. do organu nadzorczego nie wpłynął żaden wniosek o udzielenie akredytacji do monitorowania przestrzegania kodeksu postępowania.

9.2. Akredytacje udzielone przez organ nadzorczy

W 2024 r. organ nadzorczy nie udzielił żadnej akredytacji do monitorowania przestrzegania kodeksu postępowania. Należy wskazać, że akredytacja jest udzielana do monitorowania przestrzegania konkretnego kodeksu postępowania. W związku z tym może ona dotyczyć już zatwierdzonego kodeksu postępowania (twórcy kodeksów mogą przewidzieć działalność więcej niż jednego akredytowanego podmiotu monitorującego) albo projektu kodeksu, co do którego została już wydana opinia o zgodności z RODO, albo takiego, co do którego trwają końcowe analizy poprzedzające wydanie takiej opinii.

9.3. Współpraca z Prezesem UODO akredytowanych w 2022 r. i 2023 r. podmiotów monitorujących

Zgodnie z art. 33 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Prezes Urzędu prowadzi publicznie dostępny **Wykaz podmiotów akredytowanych**[299].

W grudniu 2022 r. polski organ nadzorczy udzielił akredytacji RS Jamano spółka z ograniczoną odpowiedzialnością spółka komandytowa, do monitorowania przestrzegania Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych (Porozumienie Zielonogórskie).

Za monitorowanie przestrzegania postanowień Kodeksu postępowania dla sektora ochrony zdrowia (Polska Federacja Szpitali) odpowiada KPMG Advisory spółka z ograniczoną odpowiedzialnością spółka komandytowa, która uzyskała akredytację Prezesa Urzędu w grudniu 2023 r.

Akredytacja do monitorowania przestrzegania kodeksu postępowania jest udzielana na okres **5 lat**, co wynika z treści **Wymogów akredytacji podmiotów monitorujących kodeksy postępowania**. Akredytowany podmiot monitorujący musi być w stanie wykazać spełnienie wymagań wynikających z ww. wymogów akredytacji przez cały okres sprawowania swojej funkcji. Prezes Urzędu cofa akredytację, jeżeli podmiot monitorujący nie spełnia lub przestał spełniać wymogi akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z rozporządzeniem 2016/679.

Zasady komunikacji akredytowanego podmiotu monitorującego z Prezesem Urzędu wynikają z § 3 pkt 6 wspomnianych Wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Akredytowany podmiot monitorujący składa roczne sprawozdanie do organu nadzorczego o wszelkich działaniach prowadzonych przez niego w odniesieniu do kodeksu postępowania. Zarówno RS Jamano sp. z o.o. sp.k., jak i KPMG Advisory sp. z o.o. sp. k. wywiązały się w 2024 r. z tego obowiązku.

[299] https://uodo.gov.pl/pl/426/1111.

W 2024 r. Prezes UODO spotkał się z przedstawicielami KPMG Advisory sp. z o.o. sp. k., między innymi w celu omówienia doświadczeń związanych z funkcjonowaniem Kodeksu postępowania dla sektora ochrony zdrowia (Polska Federacja Szpitali). Rozmawiano też o sposobach zachęcania administratorów i podmiotów przetwarzających do przystępowania do kodeksu, w tym tych z sektora publicznego, do których również skierowany jest kodeks.

W ocenie organu nadzorczego zapewne jedną z przyczyn braku zainteresowania uzyskaniem członkostwa w kodeksie przez podmioty publiczne jest nadal niewystarczająca świadomość znaczenia ochrony danych osobowych w procesach zarządzania jednostką sektora publicznego – w większości podmiotów organizowane są struktury i procedury zapewniające realizację obowiązków m.in. w zakresie zamówień publicznych, kontroli wewnętrznej i audytu czy dostępu do informacji publicznej, a brak właściwego umiejscowienia w strukturze organizacyjnej i opisania zadań związanych z ochroną danych osobowych, a często błędne ich powierzenie do realizacji inspektorowi ochrony danych. Ten problem został dostrzeżony przez organ nadzorczy również podczas wskazanych wyżej spotkań z przedstawicielami jednostek samorządu terytorialnego.

10. 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.

W ramach certyfikacji oceniana jest zgodność operacji przetwarzania danych osobowych z **kryteriami certyfikacji** zatwierdzonymi odpowiednio przez organ nadzorczy lub Europejską Radę Ochrony Danych (EROD). Certyfikacji mogą dokonywać akredytowane podmioty certyfikujące lub organ nadzorczy. Państwa członkowskie podejmują samodzielnie decyzje, jaki model przyjąć – udzielanie certyfikacji nie jest obowiązkowym zadaniem organów nadzorczych[300].

W Polsce certyfikacja może być dokonywana przez podmioty certyfikujące, które będą posiadać akredytację udzieloną przez **Polskie Centrum Akredytacji (PCA)**, m.in. w oparciu o **Dodatkowe wymogi akredytacji podmiotów certyfikujących**, o których mowa w art. 43 ust. 3 RODO[301].

W 2024 r. Prezes Urzędu prowadził działania edukacyjne w ramach cyklu webinariów pn. „Certyfikacja w ochronie danych", które skierowane były przede

[300] Pkt 20 Wytycznych 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia.
[301] https://uodo.gov.pl/pl/427/2303.

wszystkim do podmiotów, które planują opracować własny mechanizm certyfikacji lub które chciałyby uzyskać akredytację do udzielania certyfikacji. Ponieważ webinaria odbywały się za pośrednictwem strony internetowej UODO (online), mogli też w nich uczestniczyć wszyscy zainteresowani tą tematyką. W sumie odbyło się siedem spotkań, podczas których pracownicy Urzędu oraz zaproszeni goście (przedstawiciele PCA oraz niderlandzkiego organu nadzorczego) omówili m.in.: podstawowe pojęcia z zakresu certyfikacji, ramy prawne i dokumenty wydane przez EROD, mechanizm certyfikacji, a także etapy zatwierdzenia kryteriów certyfikacji czy proces akredytacji podmiotów certyfikujących. Nagrania z webinariów są dostępne na stronie internetowej UODO. W związku z działaniami promocyjnymi prowadzonymi przez Polskie Centrum Akredytacji pracownik UODO został zaproszony do udziału w nagraniu podcastu „Jak dbać o bezpieczeństwo danych".

Urząd Ochrony Danych Osobowych był również zaangażowany we współpracę z innymi organami nadzorczymi działającymi w obszarze certyfikacji w ramach EROD – w opiniowanie kryteriów oraz wymianę stanowisk, m.in. jako współrecenzent kryteriów certyfikacji. Wykaz wszystkich mechanizmów certyfikacji dostępny jest na stronie internetowej EROD. Większość z nich to mechanizmy krajowe, ale są i takie, które obowiązują na terenie całego EOG (EU Data Protection Seal).

Mimo tych wszystkich działań edukacyjnych w obszarze certyfikacji (organizacja cyklu webinariów w 2024 r., materiały w Biuletynie UODO, informacje publikowane na stronie internetowej UODO) do końca 2024 r. żaden podmiot nie złożył wniosku do Prezesa UODO o zatwierdzenie kryteriów certyfikacji. Być może podyktowane jest to przebiegiem całej procedury dotyczącej zatwierdzenia kryteriów certyfikacji, w tym konieczności uzyskania opinii EROD, przez co może się ona wydawać niezwykle skomplikowana i czasochłonna.

Polski organ nadzorczy jest gotów do udzielania podmiotom zainteresowanym certyfikacją wszelkich niezbędnych wyjaśnień.

11. Pytania dotyczące wykładni prawa, wnioski o dostęp do informacji i wystąpienia Prezesa UODO

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 powyższego aktu. 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.

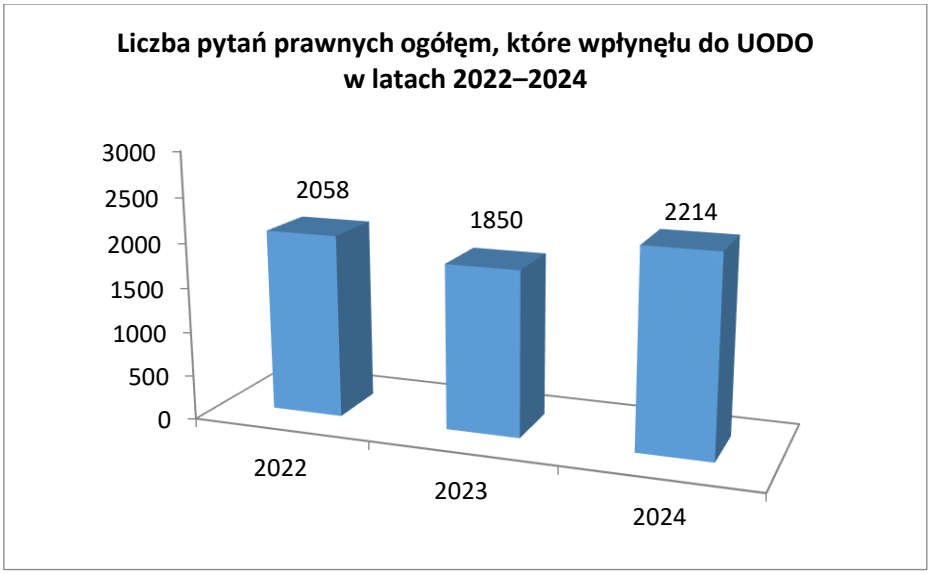
11.1. Pytania dotyczące wykładni prawa

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.

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 2024 **administratorzy oraz osoby fizyczne** skierowali do Urzędu Ochrony Danych Osobowych **1920** pism z **pytaniami prawnymi**, zaś **233** pisma wpłynęły od **inspektorów ochrony danych**. Ponadto w 2024 r. do Prezesa UODO wpłynęło **61** zapytań **organów nadzorczych z innych państw**[302]. Zatem **w sumie** w 2024 r. do UODO wpłynęło **2214 pytań prawnych**. To więcej niż w dwóch poprzednich latach, kiedy wpłynęło ich odpowiednio 1850 w roku 2023 i 2058 w roku 2022.



Wykres 18. Liczba pytań dotyczących wykładni prawa, które wpłynęły do UODO w latach 2022–2024.

Wzrost liczby wpływających pytań może być spowodowany tym, że z każdym rokiem wzrasta świadomość prawna obywateli w zakresie prawa do ochrony danych osobowych i dbałość administratorów o właściwą realizację ich obowiązków. Także wchodzenie w życie nowych przepisów prawa powoduje liczne wątpliwości, a organ nadzorczy proszony jest o ich wyjaśnienie. Do przesyłania pytań skłania zapewne również duża otwartość Prezesa UODO na dialog i współpracę ze wszystkimi interesariuszami.

W roku 2024 rozpatrzonych zostało 1815 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

[302] Więcej na ten temat w części „Współpraca w ramach IMI".

wykonujące tę funkcję mają pełnić w systemie ochrony danych osobowych – podchodzi ze szczególną uwagą. W 2024 r. do UODO wpłynęły 233 pytania od inspektorów ochrony danych (IOD). Odpowiedzi udzielono na 236 pytań od IOD. W poprzednich latach takich pytań wpłynęło: w 2023 r. – 253, a w 2022 r. – 274.

11.1.1. 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:

- stosowanie monitoringu wizyjnego,
- przetwarzanie danych biometrycznych,
- przetwarzanie danych w dokumentacji medycznej oraz danych dotyczących zdrowia,
- przetwarzanie danych w związku z prowadzeniem działalności gospodarczej,
- przetwarzanie danych osobowych w związku z ochroną małoletnich,
- przetwarzanie danych w internecie,
- innych zagadnień.

Ad 1. Stosowanie monitoringu wizyjnego

1) Monitoring wizyjny – legalność stosowania

Podobnie jak w roku ubiegłym, znaczna liczba pytań z 2024 roku odnosiła się do dopuszczalności i oceny prawidłowości stosowania monitoringu wizyjnego, co może być spowodowane brakiem szczegółowych regulacji prawnych w tym zakresie. Wątpliwości dotyczyły m.in. stosowania tzw. monitoringu sąsiedzkiego[303] lub monitoringu wizyjnego we wspólnotach i spółdzielniach mieszkaniowych[304]. Incydentalnie pojawiły się zagadnienia dotyczące stosowania monitoringu audiowizualnego w kabinach maszynistów[305] czy podstaw prawnych pozyskiwania danych z monitoringu przez biura detektywistyczne[306].

W udzielonych odpowiedziach Prezes UODO zaznaczał, że w przypadku wspólnot i spółdzielni mieszkaniowych rozróżnienia wymaga sytuacja, w której monitoring prowadzony jest przez poszczególnych lokatorów na użytek własny oraz sytuacja, w której kamery montuje wspólnota lub spółdzielnia.

Wyjaśniał, że w wielu przypadkach podstawą prawną zapewniającą legalność przetwarzania danych za pośrednictwem monitoringu wizyjnego jest art. 6 ust. 1 lit. f rozporządzenia 2016/679 wskazujący na prawnie uzasadniony interes realizowany przez administratora, jakim w praktyce może być np. konieczność zapewnienia

[303] DOL.023.451.2024, DOL.023.554.2024.
[304] DOL.023.775.2024; DOL.023.846.2024.
[305] DOL.023.903.2024.
[306] DOL.023.821.2024.

bezpieczeństwa osób i mienia w obszarze objętym nadzorem kamer. Jednak, co było podkreślane w stanowiskach Prezesa UODO, dla możliwości zastosowania tej przesłanki legalizującej administrator musi wykazać, że taki rodzaj przetwarzania jest „niezbędny" dla ochrony tego interesu, a także przeprowadzić test równowagi, który wykaże, że interes będący celem takiego przetwarzania ma charakter nadrzędny wobec interesów, praw i wolności osób, których dane będą przetwarzane. Jednocześnie organ przypominał administratorom, że są oni zobowiązani do szczególnego poszanowania prywatności osób w takich obszarach, jak przebieralnie czy toalety, oraz realizowania obowiązków informacyjnych wobec osób obserwowanych.

2) Monitoring audiowizualny w kabinach maszynistów

Warte osobnego omówienia jest pytanie o dopuszczalność nagrywania obrazu przed pojazdami kolejowymi z równoczesną rejestracją głosów w kabinie maszynistów, które miałoby służyć badaniu przyczyn wypadków kolejowych. W odpowiedzi na powyższe pytanie prawne Prezes UODO wskazał, nie negując dążeń do zapewnienia jak najwyższych standardów bezpieczeństwa podróżnych, że przetwarzanie danych osobowych pracowników za pośrednictwem monitoringu zostało uregulowane przepisami Kodeksu pracy[307] i nie może ono być sprzeczne z tymi normami prawnymi. Przepisy Kodeksu pracy stanowią bowiem szczegółowe unormowania przyjęte na mocy tzw. klauzuli otwartości zawartej w przepisie art. 88 rozporządzenia 2016/679 i mają na celu zapewnienie ochrony praw i wolności pracownika w związku z przetwarzaniem danych osobowych dla celów zatrudnienia. Wyłącznie przepisy tam zawarte normują zasady stosowania monitoringu w miejscu pracy i, jak wynika z ich treści, monitoring ma służyć zapewnieniu bezpieczeństwa samych pracowników i mienia. Są to zatem cele odmienne od tych, dla których miałby być stosowany monitoring w kabinie maszynisty. Ponadto przepisy Kodeksu pracy odnoszą się wyłącznie do rejestracji obrazu, a nie dźwięku lub obrazu i dźwięku jednocześnie (art. 22^2 § 1 Kodeksu pracy).

Ad 2. Przetwarzanie danych biometrycznych

1) Tworzenie profili behawioralnych klientów banków w celu zapobiegania przestępstwom finansowym

W 2024 r. Prezes UODO był proszony o ocenę, czy pozyskiwane przez instytucje finansowe dane dotyczące takich zachowań klientów usług płatniczych, jak: sposób użycia myszki komputerowej, klawiatury, ekranu smartfona itp., służące do przygotowania analiz behawioralnych, na podstawie których dokonywane jest ich uwierzytelnianie, co ma umożliwiać ograniczanie transakcji oszukańczych w płatnościach bezgotówkowych, stanowią dane osobowe zwykłe czy też dane

[307] Ustawa 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2025 r. poz. 277).

osobowe szczególnych kategorii[308]. Rozróżnienie to było istotne ze względu na określenie podstaw prawnych przetwarzania danych osobowych.

W odpowiedzi Prezes UODO podniósł w pierwszej kolejności, że należy mieć na względzie to, że korzystanie z technologii opartej na analizie cech behawioralnych osoby fizycznej stanowi głęboką ingerencję w jej prawo do prywatności zagwarantowane w art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej, przepisach art. 47 i art. 51 Konstytucji RP oraz w rozporządzeniu 2016/679. Natomiast pojęcie „dane biometryczne" oznaczają dane, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Przepis art. 9 ust. 1 rozporządzenia 2016/679 ustanawia zasadę zakazu przetwarzania danych biometrycznych i zwolnienie z tego zakazu musi wprost wynikać z regulacji ust. 2 tego przepisu. Przetwarzanie danych behawioralnych mogłoby być uzasadnione w oparciu o art. 9 ust. 2 lit. g rozporządzenia 2016/679 tj. ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. Za podstawę prawną przetwarzania danych behawioralnych dla zapobiegania oszustwom związanym z wykonywanymi usługami płatniczymi nie można uznać przepisu art. 10 ustawy z 19 sierpnia 2011 r. o usługach płatniczych[309], ponieważ przepis ten nie przewiduje odpowiednich gwarancji dla ochrony praw i interesów osób, których dane miałyby być przetwarzane. Prezes UODO wskazał, że jedyną przesłanką, która mogłaby być brana pod uwagę jako podstawa prawna przetwarzania, jest świadoma i wyraźna zgoda osoby, której dane dotyczą, (tj. przesłanka wskazana w art. 9 ust. 2 lit. a rozporządzenia 2016/679). Przy tym jednocześnie powinno istnieć alternatywne rozwiązanie dla podmiotu danych, tak by brak zgody nie wiązał się dla niego z niemożnością skorzystania z usługi banku[310].

2) Pobieranie odcisków palców podczas ubiegania się o wydanie dowodu osobistego

Sprawa ta[311] wiązała się z odmową wydania dowodu osobistego ze względu na brak zgody osoby, której dane dotyczą, na udostępnienie takich danych. Prezes UODO wskazał, że zgoda na przetwarzanie danych biometrycznych nie jest jedyną podstawą prawną legalizującą ich przetwarzanie. W analizowanym przypadku są nią art. 12a ust. 1 pkt 1 lit. i ustawy z 6 sierpnia 2010 r. o dowodach osobistych[312] oraz art. 3 ust. 5 zdanie pierwsze rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1157 z 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów

[308] DOL.023.97.2024; DOL.051.1.2024; DOL.023.138.2024.

[309] Ustawa z 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. z 2024 r. poz. 30).

[310] Temat ten został również opisany w Biuletynie UODO nr 04/04/24 w materiale „Biometryczna weryfikacja tożsamości klientów usług płatniczych".

[311] DOL.023.206.2024.

[312] Ustawa z 6 sierpnia 2010 r. o dowodach osobistych (Dz.U. z 2022 r. poz. 671).

osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się[313]. Jak zaznaczył, dowód osobisty nie stanowi wyłącznie dokumentu stwierdzającego tożsamość osoby fizycznej, ale umożliwia korzystanie z przysługujących obywatelowi Unii Europejskiej swobód czy to w zakresie przemieszczania się na jej terytorium, czy też osiedlania się lub podejmowania zatrudnienia. To z kolei determinuje konieczność stosowania środków zabezpieczających dowody osobiste przed sfałszowaniem czy podrobieniem. Prezes UODO podkreślił także, że przepisy ustawy o dowodach osobistych nie zezwalają na utworzenie bazy danych biometrycznych obejmującej odciski palców (obrazy linii papilarnych) wszystkich osób ubiegających się o dowód osobisty i tych, którym taki dokument wydano.

Ad 3. Przetwarzanie danych w dokumentacji medycznej oraz danych dotyczących zdrowia

Pytania prawne z zakresu przetwarzania danych medycznych (danych o zdrowiu) obejmowały różnorodne zagadnienia. Przesyłały je zarówno osoby fizyczne, jak i osoby prawne. Zgłaszane wątpliwości dotyczyły m.in. podstaw prawnych udostępniania franczyzodawcy danych osobowych zawartych w orzeczeniach lekarskich pracowników do celów sanitarno-epidemiologicznych[314], dopuszczalności udostępnienia danych osobowych personelu szpitala na rzecz jednej z okręgowej izb pielęgniarek i położnych[315] czy też realizacji prawa do usunięcia danych osobowych zawartych w kwestionariuszu medycznym poprzedzającym badanie diagnostyczne, które nie zostało ostatecznie zrealizowane[316].

1) Prawo żądania usunięcia danych z kwestionariusza medycznego w przypadku rezygnacji pacjenta z wykonania badania medycznego

Administrator danych powziął wątpliwości co do obowiązku realizacji przez niego prawa do usunięcia danych w świetle obowiązujących przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[317]. Po uzupełnieniu przez osobę, której dane dotyczą, kwestionariusza osobowego poprzedzającego wykonanie badania diagnostycznego, osoba ta odstąpiła od poddania się badaniu i zażądała usunięcia danych podanych w kwestionariuszu w trybie art. 17 ust. 1 RODO. Wątpliwości administratora dotyczyły tego, czy wypełniony kwestionariusz w związku z rezygnacją z badania można uznać za dokumentację medyczną, co determinuje okres retencji danych. Zgodnie bowiem z art. 23 i następne ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, przechowywanie dokumentacji medycznej ma służyć realizacji prawa pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz

[313] Dz. Urz. UE L 188 z 12 lipca 2019 r., str. 67 z późn. zm.
[314] DOL.023.204.2024.
[315] DOL.023.235.2024.
[316] DOL.023.682.2024.
[317] Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2024 r. poz. 581).

udzielonych mu świadczeń zdrowotnych. Natomiast Rozporządzenie Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania[318] wskazuje (§ 2 ust. 3 pkt 20), że dokumentację [medyczną] indywidualną wewnętrzną stanowią m.in. wyniki badań diagnostycznych wraz z opisem.

Przetwarzanie danych powinno odbywać się w pierwszej kolejności z poszanowaniem zasady ograniczenia przechowywania danych osobowych ustanowionej w art. 5 ust. 1 lit. e RODO. W omawianej sprawie nie zostało wykonane badanie diagnostyczne i całość dokumentacji stanowią wyłącznie dane podane przez pacjenta. W takiej sytuacji administrator danych powinien rozważyć, czy posiadana przez niego dokumentacja stanowi dokumentację medyczną w rozumieniu obowiązujących przepisów prawa i w tym kontekście dokonać oceny, czy spełniona jest przesłanka odmowy realizacji prawa do usunięcia danych z przepisu art. 17 ust. 3 lit. b RODO. Należy także mieć na uwadze, że brak spełniania kumulatywnie warunków określonych w przepisie art. 25 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta stanowi o tym, że nie ma się do czynienia z dokumentacją medyczną w rozumieniu ustawy.

2) Udostępnianie danych osobowych zawartych w orzeczeniach lekarskich do celów sanitarno-epidemiologicznych na żądanie franczyzodawcy

Pytanie dotyczyło podstawy prawnej udostępnienia przez franczyzobiorcę na żądanie franczyzodawcy (w ramach kontroli wewnętrznej) orzeczeń lekarskich pracowników franczyzobiorcy do celów sanitarno-epidemiologicznych. Stanowisko Prezesa UODO w tej sprawie było jednoznaczne – brak jest podstaw prawnych do takiego udostępnienia danych. Przepisy prawa zezwalają na przetwarzanie danych zawartych w orzeczeniach lekarskich do celów sanitarno-epidemiologicznych wyłącznie przez pracodawcę, przy czym status taki względem pracowników ma w tym przypadku franczyzobiorca. Przepisy prawa nie przewidują ponadto obowiązku udostępniania tych danych na rzecz innych podmiotów aniżeli organy urzędowej kontroli żywności, które na podstawie art. 59 ust. 4 ustawy o bezpieczeństwie żywności i żywienia[319] mogą żądać od podmiotów działających na rynku spożywczym udostępnienia orzeczeń lekarskich i innych stosownych dokumentów złożonych do akt pracowniczych.

3) Pozyskiwanie przez pracodawcę danych o niepełnosprawności dziecka pracownika w celu udzielenia pracownikowi urlopu wychowawczego

Pytanie to odnosiło się do legalności żądania przez pracodawcę przedłożenia mu przez pracownika kopii prawomocnego orzeczenia o niepełnosprawności lub stopniu niepełnosprawności dziecka. W ocenie przedstawiciela ustawowego dziecka, pomimo transparentności przepisów prawa co do wymaganych dokumentów w przypadku

[318] Rozporządzenie Ministra Zdrowia z 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2024 r. poz. 798).
[319] Ustawa z 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (Dz.U. z 2023 r. poz. 1448).

wnioskowania o dodatkowy urlop wychowawczy ze względu na niepełnosprawność dziecka, żądane przez pracodawcę dane były nadmiarowe i naruszały przepisy RODO. Przepisy obowiązującego prawa (tj. art. 186 § 3 Kodeksu pracy) uprawniają pracodawcę do pozyskania kopii prawomocnego orzeczenia o niepełnosprawności lub stopniu niepełnosprawności dziecka, na które ma być udzielony urlop wychowawczy, to jest to jednocześnie spełnienie przesłanki z art. 9 ust. 2 lit. b RODO[320]. Bez znaczenia w takim przypadku pozostaje fakt, że Prezes UODO przy opiniowaniu projektu rozporządzenia Ministra Rodziny i Polityki Społecznej w sprawie wniosków dotyczących uprawnień pracowników związanych z rodzicielstwem oraz dokumentów dołączanych do takich wniosków zgłaszał uwagi co do tego, czy kopie zaświadczeń, orzeczeń, decyzji, aktów zawierają wyłącznie informacje niezbędne pracodawcy dla celów przewidzianych przepisami Kodeksu pracy wskazanymi niniejszym rozporządzeniem[321].

4) Udostępnianie danych dotyczących zdrowia dziecka w karcie kwalifikacyjnej wypoczynku

W jednym z pytań prawnych[322] poruszona została kwestia przetwarzania danych dotyczących zdrowia dziecka w karcie kwalifikacyjnej uczestnika wypoczynku (kolonia, zimowisko, biwak, półkolonia itp.), której wzór został ustanowiony rozporządzeniem Ministra Edukacji i Nauki z 21 lipca 2021 r. zmieniającym rozporządzenie w sprawie wypoczynku dzieci i młodzieży[323]. Karta kwalifikacyjna przewidywała podanie przez przedstawiciela ustawowego dziecka m.in. danych o stanie zdrowia dziecka – o tym, czy wymaga specjalnej diety, czy jest na coś uczulone, jakie leki przyjmuje i w jakich dawkach, czy ma jakieś szczególne potrzeby wynikające z niepełnosprawności lub o niedostosowaniu społecznym itp. Przedstawiciel ustawowy dziecka wyraził wątpliwości dotyczące tego, czy nauczyciel szkolny jest uprawniony do przetwarzania danych wrażliwych (tj. dotyczących zdrowia dziecka) oraz czy kierownik wypoczynku jest zobowiązany do poinformowania przedstawiciela ustawowego dziecka o podstawie prawnej przetwarzania danych, okresie ich retencji i kontakcie do inspektora ochrony danych.

Zgodnie z art. 92k ustawy z 7 września 1991 r. o systemie oświaty[324] prowadzona przez organizatora wypoczynku karta kwalifikacyjna zawiera m.in. istotne dane o stanie zdrowia, rozwoju psychofizycznym i stosowanej diecie uczestnika oraz jego numer PESEL w celu potwierdzenia prawa do świadczeń opieki zdrowotnej. Natomiast w myśl art. 13b ust. 2 tej ustawy nauczyciele oraz inne osoby pełniące funkcje lub

[320] Art. 9 ust. 2 lit. b RODO stanowi, że przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne, gdy jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą.
[321] DOL.023.657.2024.
[322] DOL.023.474.2024.
[323] Dz.U. poz. 1548.
[324] Dz.U. z 2024 r. poz. 750 ze zm.

wykonujące pracę w placówkach oświatowych są obowiązani do zachowania w poufności informacji uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą, dotyczących m.in. zdrowia uczniów (z wyjątkiem przypadków wymienionych w ust. 3[325]). Podkreślone zostało przez Prezesa UODO również to, że każde przetwarzanie danych osobowych wiąże się z obowiązkiem informacyjnym administratora określonym w art. 13 RODO.

5) Przekazywanie danych medycznych

Jedna z przychodni zdrowia psychicznego i leczenia uzależnień chciała ustalić podstawę prawną dla przekazywania danych osób uzależnionych na rzecz urzędu miasta. Urząd ten zażądał tych danych ze względu na obowiązek dofinansowywania programów psychoterapii dla osób uzależnionych i współuzależnionych ze środków uzyskanych z dochodów z opłat za korzystanie z zezwoleń na sprzedaż napojów alkoholowych[326].

Dostęp do dokumentacji medycznej reguluje art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, określający katalog instytucji, którym podmiot udzielający świadczeń zdrowotnych może udzielić dostępu do dokumentacji pacjenta, a także przesłanki udzielenia tych informacji. W rozumieniu tego przepisu dostępu do dokumentacji pacjenta można udzielić: organom władzy publicznej, w tym Rzecznikowi Praw Pacjenta, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom w ochronie zdrowia, a także Rzecznikowi Praw Pacjenta Szpitala Psychiatrycznego, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności nadzoru i kontroli. Prezes UODO wskazał przy tym, że art. 53 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych[327] stanowi, że dokumentację medyczną udostępnia się z zachowaniem jej integralności, poufności oraz autentyczności, bez zbędnej zwłoki. Dodatkowo należy mieć na uwadze art. 50 ustawy o ochronie zdrowia psychicznego, z którego wynika obowiązek zachowania tajemnicy przez osoby wykonujące czynności wynikające z ww. ustawy.

Centrum medyczne przedstawiło wątpliwości dotyczące udostępnienia zanonimizowanych danych pacjentów na rzecz podmiotów komercyjnych[328]. Opisując problem, wyjaśniło, że otrzymuje wnioski o udostępnienie danych z dokumentacji medycznej pacjentów na potrzeby rozwoju produktów i usług oferowanych przez podmioty prywatne, działające zazwyczaj w branży produktów leczniczych, wyrobów medycznych, a także w branży oprogramowania, tj. tworzenia algorytmów sztucznej

[325] Przepisu art. 13b ust. 2 ustawy o systemie oświaty nie stosuje się: 1) w przypadku zagrożenia zdrowia ucznia; 2) jeżeli uczeń, a w przypadku ucznia niepełnoletniego jego rodzic, wyrazi zgodę na ujawnienie określonych informacji; 3) w przypadku gdy przewidują to przepisy szczególne.
[326] DOL.023.820.2024.
[327] Dz.U. z 2022 r. poz. 1957 ze zm.
[328] DOL.023.688.2024.

inteligencji i platform wspomagających pracę lekarzy. Wnioskujący podnoszą, że zwracają się o dane medyczne bez informacji identyfikujących pacjentów, które mogłyby być w pełni i w sposób nieodwracalny zanonimizowane. Podmioty komercyjne miałyby prawo do przetwarzania danych na cele określone w umowie, w tym w szczególności prawo do korzystania z otrzymanych danych w zakresie ich utrwalania, organizowania, porządkowania, przechowywania, adaptowania, modyfikowania, przeglądania, wykorzystywania, dopasowywania, łączenia, udostępniania, ograniczania, usuwania. Centrum medyczne zwróciło się o wyjaśnienie, czy dokumentacja medyczna zanonimizowana w zakresie: imion i nazwisk pacjentów, ich numerów PESEL, adresów zamieszkania, informacji o dokumentach tożsamości, miejscach hospitalizacji, godziny zdarzenia medycznego oraz zmieniona w zakresie numerów identyfikacyjnych przypisanych indywidualnie do pacjenta w systemie szpitalnym oraz daty urodzenia (na wskazanie wyłącznie roku urodzenia, by móc określić wiek pacjenta), stanowi nadal dokumentację medyczną w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz czy możliwe jest udostępnienie takiej dokumentacji na rzecz podmiotów komercyjnych. Wskazało, że podmioty komercyjne utrzymują, że udostępnianie zanonimizowanej dokumentacji medycznej nie podlega reżimowi ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a ponadto dane zanonimizowane nie są objęte przepisami RODO (nie można ich uznać za „dane osobowe” w rozumieniu art. 4 pkt 1 tego rozporządzenia, gdyż na ich podstawie nie można bezpośrednio lub pośrednio ustalić tożsamości osoby fizycznej). Centrum medyczne zwróciło się również o określenie relacji pomiędzy przepisami RODO a art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, który reguluje zasady udostępniania dokumentacji medycznej.

Warunki udostępnienia dokumentacji medycznej zostały ściśle określone w przepisach ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w art. 26 tej ustawy. Jednocześnie Prezes UODO podkreślił, że ze względu na wysoce wrażliwy charakter danych dotyczących zdrowia, należy dokonać anonimizacji danych w taki sposób, aby zapewnić nieodwracalność tego procesu i jego realizację z poszanowaniem zasady poufności i integralności, o której mowa w art. 5 ust. 1 lit. f RODO. Jest to także istotne z punktu widzenia poszanowania tajemnic prawnie chronionych (m.in. tajemnicy zawodowej lekarza przewidzianej w art. 13 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta). Każdorazowo ocena udostępnienia dokumentacji medycznej należy do administratora i powinna być poprzedzona dokonaniem analizy ryzyka. To administrator bowiem decyduje, czy istnieją podstawy do przekazania danych i czy odbywa się to w środowisku bezpiecznym dla danych, tak aby ograniczyć ryzyko ich udostępnienia podmiotom/osobom nieuprawnionym, zaginięcia czy uszkodzenia. Przede wszystkim należy zadbać o to, aby proces anonimizacji był skuteczny i nie był mylnie identyfikowany z tzw. pseudonimizacją. Zgodnie z zasadą rozliczalności, administrator wykazuje, że zastosował rozwiązania adekwatne do stwierdzonych ryzyk. Wspierać go w tym procesie może inspektor ochrony danych.

Ad 4. Przetwarzanie danych w związku z prowadzeniem działalności gospodarczej

Prowadzenie działalności gospodarczej łączy się nierozerwalnie z przetwarzaniem danych osobowych klientów, potencjalnych klientów lub zatrudnionych w przedsiębiorstwie pracowników. Następstwem tego jest różnorodność zagadnień przedstawianych w pytaniach prawnych pochodzących zarówno od osób, których dane dotyczą, jak i od przedsiębiorców. W minionym roku pojawiły się pytania związane m.in. z: podstawą prawną przekazywania przez spółdzielnie mieszkaniowe (wspólnoty mieszkaniowe) danych osobowych właścicieli lokali mieszkalnych na żądanie zakładów ubezpieczeń w ramach postępowania likwidacji szkody[329], określeniem tego, czy Booking.com ma status administratora w odniesieniu do danych osób korzystających z usług tego portalu[330].

1) Udostępnianie przez spółdzielnie mieszkaniowe (wspólnoty mieszkaniowe) danych osobowych właściciela lub użytkownika lokalu mieszkalnego na żądanie zakładów ubezpieczeniowych

Spółdzielnie mieszkaniowe (wspólnoty mieszkaniowe) zwróciły uwagę Prezesa UODO na problem dotyczący podstawy prawnej udostępniania danych właścicieli lokali mieszkalnych lub najemców takich lokali, będących sprawcami szkód w nieruchomości, na żądanie zakładów ubezpieczeń w związku z prowadzonymi przez nie postępowaniami likwidacyjnymi. Jako podstawę prawną żądania udostępnienia danych zakłady ubezpieczeń wskazywały art. 42 ustawy o działalności ubezpieczeniowej i reasekuracyjnej[331]. Powołany przepis wskazuje podmioty zobowiązane do udzielenia informacji na wniosek zakładu ubezpieczeń: sądy, prokuratura, policja oraz inne organy i instytucje. Spółdzielnie mieszkaniowe nie są natomiast podmiotami publicznymi i nie można ich zaliczyć do kręgu instytucji, o których mowa w ww. przepisie. Regulacja ta odnosi się do podmiotów prowadzących postępowania związane z wypadkiem ubezpieczeniowym. Wobec tego poprzez „organy” i „instytucje” należy rozumieć przede wszystkim podmioty państwowe i dlatego też przepis ten nie może stanowić podstawy do obligatoryjnego przekazania ubezpieczycielowi żadnych informacji przez spółdzielnię mieszkaniową. Zakłady ubezpieczeń mogą żądać udostępnienia danych sprawców szkód, powołując się na istnienie uzasadnionego interesu w rozumieniu art. 6 ust. 1 lit. f RODO. Niemniej interes podmiotu wnioskującego o udostępnienie danych powinien zostać uprawdopodobniony. Ubezpieczyciel powinien w sposób wyczerpujący wykazać, na podstawie jakich przesłanek wywodzi uzasadnione przypuszczenie, że osoba, której danych żąda, jest faktycznym sprawcą zdarzenia, w jakim konkretnym celu zamierza wykorzystać dane oraz z jakich powodów są mu one niezbędne do realizacji tego celu. Z kolei administrator powinien zbadać, czy nie istnieją okoliczności powodujące, że

[329] DOL.023.805.2024.

[330] DOL.023.171.2024.

[331] Ustawa z 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2024 r. poz. 838).

w wyniku udostępnienia danych naruszone zostaną interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, o charakterze nadrzędnym w stosunku do interesu zakładu ubezpieczeń.

2) Przekazywanie danych osobowych klienta pomiędzy przedsiębiorcami

Kupujący, będący osobą fizyczną, zwrócił się do Prezesa UODO z prośbą o odniesienie się do kwestii przekazania przez jednego z przedsiębiorców jego danych kontaktowych (numer telefonu) innemu przedsiębiorcy celem realizacji zgłoszonej przez niego reklamacji. Nie znając szczegółów, Prezes UODO wskazał, że przekazanie danych na potrzeby rozpatrzenia reklamacji mogło zostać uregulowane w umowie łączącej strony i w pewnych przypadkach może stanowić o tym, że przekazanie danych niezbędnych do realizacji usługi odbywa się z powołaniem na art. 6 ust. 1 lit. c RODO. Taki pogląd jest uzasadniony, jeżeli mamy do czynienia z tzw. umową marketplace. Przekazanie numeru telefonu klienta może być niezbędne dla wykonania umowy, a konkretnie nawiązania przez sprzedawcę zewnętrznego (rzeczywistego sprzedawcę rzeczy) kontaktu z klientem celem pozyskania określonych informacji w związku ze zgłoszoną reklamacją (termin dostarczenia/odbioru rzeczy itp.). Takie przekazanie danych może często mieć charakter warunkowy, co oznacza, że w przypadku braku roszczeń klienta wobec sprzedawcy zewnętrznego, sprzedawca pośredniczący nie ma obowiązku przekazywać danych kontaktowych na jego rzecz[332].

3) Dopuszczalność żądania przez przedsiębiorców z sektora prywatnego przekazania zdjęcia/skanu dowodu osobistego

Wiele pytań dotyczyło żądania udostępnienia skanu dowodu osobistego na rzecz podmiotów zarządzających portalami internetowymi, takimi jak m.in. vinted.pl, inpost, olx.pl, przelewy24.pl[333], z powołaniem się na regulacje ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[334]. Art. 2 ust. 1 powołanej ustawy określa katalog tzw. instytucji obowiązanych, które mają obowiązek stosowania środków bezpieczeństwa finansowego. Z kolei zgodnie z jej art. 34 ust. 4 instytucje obowiązane, na potrzeby stosowania wymienionych środków, mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie. Jednocześnie organ nadzorczy odsyłał do zamieszczonego na stronie internetowej urzędu materiału, zatytułowanego „Czy instytucje finansowe mogą kopiować dowody osobiste?”[335], w którym wskazano, że art. 34 ust. 4 omawianej ustawy, nie upoważnia instytucji finansowych do wykonywania kopii dokumentu tożsamości klienta w każdej sytuacji. Praktyka ta jest dopuszczalna jedynie wtedy, gdy konieczne jest zastosowanie przez wspomniane

[332] DOL.023.754.2024.

[333] DOL.023.588.2024, DOL.023.273.2024.

[334] Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2023 r. poz. 1124 z późn. zm.).

[335] https://uodo.gov.pl/pl/138/2476.

podmioty środków bezpieczeństwa mających na celu przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu. Ryzyko (prawdopodobieństwo) wystąpienia wymienionych zjawisk przestępczych powinno zostać poddane wstępnej ocenie. Należy zwrócić przy tym uwagę na treść art. 35 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, który określa przypadki, w jakich instytucje są zobowiązane do stosowania środków bezpieczeństwa przewidzianych w omawianej ustawie.

4) Odmowa udostępnienia danych właściciela obiektu noclegowego przez Booking.com

W związku z prowadzonym postępowaniem wyjaśniającym, Prezes UOKiK zwrócił się do Prezesa UODO o udzielenie informacji dotyczących zasad udostępniania przez portal Booking.com, jako pośrednika w świadczeniu usług, danych o prywatnym gospodarzu (osobie fizycznej wynajmującej miejsce noclegowe) w sytuacji, gdy konsument dochodzi względem tego gospodarza roszczeń wynikających z niewykonania/nienależytego wykonania umowy. Podniósł, że Booking.com odmówił udostępnienia danych gospodarza, powołując się na brak podstawy prawnej do przetwarzania jego danych osobowych. Konsumentowi powinno zostać zagwarantowane prawo do uzyskania informacji o wynajmującym w sytuacji, gdy chce skorzystać z roszenia dotyczącego realizacji umowy w zakresie potrzebnym do dochodzenia roszczenia, a zatem co najmniej prawo do poznania jego nazwiska, imienia i dokładnego adresu. Przetwarzanie może mieć miejsce m.in., gdy jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b rozporządzenia 2016/679). Jednak kluczowe jest określenie treści umowy i tego, kto w świetle jej postanowień ponosi odpowiedzialność za wykonanie umowy. Podmiot danych, który zawarł umowę z administratorem, ma prawo do uzyskania jego danych osobowych potrzebnych do jej realizacji. Administrator nie może przy tym zasłaniać się brakiem zgody na przetwarzanie jego danych przez drugą stronę umowy (np. wynajmującego). Sytuację prawną konsumenta, który chce uzyskać dane zobowiązanego z umowy do realizacji roszczenia, można także rozpatrywać w świetle regulacji art. 6 ust. 1 lit f RODO. Przepis ten stanowi, że przetwarzanie danych jest zgodne z prawem, jeśli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Ad 5. Przetwarzanie danych osobowych w związku z ochroną małoletnich

1) Nowelizacja ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich

Wejście w życie ustawy z 28 lipca 2023 r. o zmianie ustawy – Kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw[336], nowelizującej m.in. przepisy ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (dalej jako „ustawa o ochronie małoletnich"), wywołało liczne wątpliwości. Dla ułatwienia dostosowania się do znowelizowanych przepisów organ nadzorczy przygotował i zamieścił na stronie internetowej materiał „Jak stosować »ustawę Kamilka« w zgodzie ze standardami ochrony danych osobowych"[337]. Wyjaśnił w nim m.in., na co powinien zwrócić uwagę administrator związany zmienionymi przepisami ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym. Niezależnie od tego udzielał odpowiedzi na indywidualne pytania dotyczące zarówno katalogu osób objętych weryfikacją w rejestrze sprawców przestępstw na tle seksualnym, jak i rodzajów działalności podlegających reżimowi ustawy[338]. Przepis art. 12 ustawy o ochronie małoletnich określa zamknięty katalog podmiotów, którym przysługuje prawo dostępu do Rejestru z dostępem ograniczonym. Obok Rejestru z dostępem ograniczonym istnieją również rejestr publiczny i rejestr osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze.

Prawo dostępu do Rejestru z dostępem ograniczonym przysługuje m.in. pracodawcom przed nawiązaniem z osobą stosunku pracy związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, w zakresie uzyskania informacji, czy dane tej osoby są zgromadzone w tym Rejestrze (art. 12 pkt 6), a także innym organizatorom przed dopuszczeniem osoby do działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi, w zakresie uzyskania informacji, czy dane tej osoby są zgromadzone w tym Rejestrze.

Szkoły to jedne z placówek, które zobowiązane są do wprowadzenia standardów ochrony małoletnich (zgodnie z art. 22b ustawy o ochronie małoletnich) i w tym celu mają prawo pozyskać informacje z ww. Rejestru wobec swoich pracowników, opiekunów czy wolontariuszy przed nawiązaniem z nimi stosunku pracy (współpracy) związanej z czynnościami, o których mowa w art. 12 pkt 6 i 7 ustawy o ochronie małoletnich.

Zadano pytanie, czy placówka edukacyjna zobowiązana jest do weryfikacji przed zatrudnieniem wyłącznie pracowników pedagogicznych, czy również pracowników wykonujących pracę o charakterze niepedagogicznym[339]. Odpowiadając na nie, organ nadzorczy podniósł, że zgodnie z wytycznymi Ministerstwa Edukacji i Nauki[340] przyjąć

[336] Dz.U. poz. 1606.
[337] https://uodo.gov.pl/pl/138/3278
[338] DOL.023.422.2023; DOL.023.663.2024; DOL.023.827.2024.
[339] DOL.023.221.2024.
[340] https://www.gov.pl/web/edukacja/informacja-o-obowiazku-korzystania-z-rejestru-sprawcow-przestepstw-na-tle-seksualnym-z-dostepem-ograniczonym.

należy, że czynnikiem determinującym weryfikację jest zatrudnienie lub powierzanie jakiejkolwiek działalności, nawet jeśli tylko potencjalnie może być ona związana z edukacją i opieką nad dziećmi. W świetle obowiązujących przepisów nie wydaje się uzasadnione dokonywanie ponownej weryfikacji pracowników już zatrudnionych i zweryfikowanych pozytywnie. Należy zauważyć, że w wyniku nowelizacji ustawy o ochronie małoletnich, w przepisie art. 21 ust. 1 ustawy rozszerzono jedynie katalog działalności związanej z pracą z dziećmi poprzez jego poszerzenie o: świadczenia porad psychologicznych, rozwoju duchowego, uprawiania sportu lub realizacji innych zainteresowań przez małoletnich. Ponadto zgodnie z przepisem art. 21 ustawy o ochronie małoletnich, obowiązek sprawdzenia pracodawców odnosi się do momentu przed nawiązaniem stosunku pracy, a także aktualizuje się, gdy rzeczywisty zakres obowiązków osoby, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do działalności, będzie związany co najmniej z jedną z aktywności wymienionych w art. 21 ust. 1 ustawy o ochronie małoletnich. Jeżeli więc dotychczas zatrudnionym pracownikom zmienia się umowa o pracę lub rodzaj działalności, w wyniku czego będą wykonywać obowiązki, o których mowa w znowelizowanych przepisach, należy stosować nowe regulacje.

Wpływające do UODO sygnały świadczące o niedoskonałości ww. przepisów skłoniły Prezesa UODO do skierowania do Ministra Sprawiedliwości wystąpienia z wnioskiem o podjęcie stosownych prac legislacyjnych[341] (o czym więcej w części „Opiniowanie projektów aktów prawnych dotyczących ochrony danych osobowych").

2) Udostępnienie na rzecz wójta gminy orzeczeń i opinii poradni psychologiczno-pedagogicznej dotyczącej uczniów szkoły gminnej

Kolejne z pytań prawnych[342] dotyczyło żądania przez wójta gminy udostępnienia mu przez zespół szkół gminnych orzeczeń i opinii poradni psychologiczno-pedagogicznej dotyczących uczniów. Wójt gminy jest organem publicznym, którego wszelkie działania władcze powinny wynikać wprost z przepisów prawa. Wójt gminy odpowiada za organizację szkoły i wykonuje zadania wynikające z przepisów ustawy z 14 grudnia 2016 r. – Prawo oświatowe[343], ale żądanie udostępnienia danych dotyczących uczniów powinno wynikać z przepisów prawa i podstawa prawna przetwarzania danych osobowych uczniów powinna zostać wskazana przez wójta gminy. Organ prowadzący szkołę ma dostęp (a szkoła mu ten dostęp zapewnia) do danych osobowych przetwarzanych w szkole w związku z realizacją obowiązków wynikających z przepisów prawa. Dostęp organu prowadzącego do danych osobowych musi być adekwatny do celu przetwarzania danych, co oznacza, że zakres udostępnianych danych musi być odpowiedni (bez nadmiaru) do celu przetwarzania (zasada minimalizacji danych). Organ prowadzący szkołę nie powinien mieć dostępu do danych uczniów i ich rodzin zawartych w dokumentacji prowadzonej przez szkołę,

[341] DOL.413.9.2024; treść wystąpienia i jego omówienie dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3377.
[342] DOL.023.947.2024.
[343] Dz.U. z 2024 r. poz.737 ze zm.; dalej jako: Prawo oświatowe.

które odnoszą się do indywidualnych problemów psychologicznych czy pedagogicznych uczniów.

Ad 6. Ujawnianie danych osobowych w Internecie i systemach teleinformatycznych

1) Anonimizacja współrzędnych geograficznych celem udostępnienia na stronie internetowej

Pytanie przedsiębiorcy dotyczyło prawidłowej anonimizacji danych osobowych, by móc zgodnie z prawem ujawniać na mapie internetowej punkty dostaw towarów do klientów w kraju. Miałoby to służyć budowaniu marki przedsiębiorstwa w oczach konsumentów, a jednocześnie odbywać się bez podawania dokładnej lokalizacji dostawy (jedynie ogólne współrzędnie), precyzyjnej wartości zamówienia i danych osobowych klienta. Prezes UODO wskazał, że warunkiem udostępnienia punktów dostaw towarów w Internecie powinna być skuteczna anonimizacja danych. Polegać ona powinna na takiej modyfikacji danych o adresie dostawy, by wykluczyć możliwość ustalenia na podstawie współrzędnych geograficznych tożsamości osoby fizycznej. Można to osiągnąć, np. zmniejszając dokładność danych jedynie do pewnego ogólnego obszaru dostawy. W zależności od uwarunkowań danego miejsca (np. od gęstości zaludnienia) obszar ten może wymagać odpowiedniego rozszerzenia, by zapewnić skuteczność anonimizacji danych. Podobnie należy postąpić również w przypadku danych dotyczących wartości zamówienia. Przeskalowanie tych informacji powinno mieć na tyle szeroki zakres ogólności, aby na podstawie tych danych osoba korzystająca ze strony internetowej nie mogła wywnioskować przybliżonych wartości zamówień dotyczących danej osoby fizycznej będącej kontrahentem[344].

2) Uwierzytelnianie użytkownika przy przeglądaniu ksiąg wieczystych w systemie teleinformatycznym

Minister Rozwoju i Technologii zwrócił się do Prezesa UODO o wyrażenie opinii, czy koncepcja Ministra Sprawiedliwości polegająca na uwierzytelnieniu użytkownika przed dostępem do treści księgi wieczystej prowadzonej w systemie teleinformatycznym (na skutek czego osoba przeglądająca treść księgi wieczystej nie pozostanie anonimowa, a dane tej osoby będą przechowywane w systemie przez określony czas) jest wystarczającym środkiem ochrony danych osobowych, umożliwiającym upublicznienie numerów ksiąg wieczystych gromadzonych w ewidencji gruntów i budynków m.in. na rządowym portalu geoportal.gov.pl.

Planowaną koncepcję odejścia od modelu anonimowej i powszechnej dostępności do danych zawartych w księgach wieczystych na rzecz obowiązku uwierzytelniania się przez użytkowników systemu teleinformatycznego celem dostępu do elektronicznych ksiąg wieczystych Prezes UODO ocenił jako właściwy kierunek zmian. Obowiązek uwierzytelniania się istotnie ograniczyłby bowiem możliwość stosowania tzw. robotów dokonujących automatycznych operacji wyszukiwania

[344] DOL.023.782.2024.

i pobierania danych osobowych z elektronicznych ksiąg wieczystych, z drugiej strony zaś umożliwiłby spełnienie przez administratora wymogu z art. 24 ust. 12 RODO, także w kontekście zasady rozliczalności z art. 5 ust. 2 tego rozporządzenia[345].

Ad 7. Inne zagadnienia

Wielu pytań prawnych nie można przypisać do żadnej z powyższych kategorii, lecz ze względu na to, że dotyczą szczególnie interesujących zagadnień lub często zgłaszanych problemów, niektóre z nich zostały omówione poniżej.

1) Uwiecznianie wizerunku dziecka przez fotografa podczas uroczystości

Rodzic zgłosił zastrzeżenia co do dopuszczalności fotografowania jego dziecka podczas komunii świętej. Jak sam wskazał, nie korzystał on z usług fotografa wynajętego dla całej grupy i nie wyraził zgody na robienie zdjęć swojemu dziecku. Fotograf powołał się jednak na przepis art. 81 ustawy z 4 lutego 1994 r. o prawach autorskich i prawach pokrewnych[346]. Rozpowszechnianie wizerunku osoby fizycznej jest objęte regulacją art. 81 ustawy o prawie autorskim i prawach pokrewnych, który uzależnia rozpowszechnianie wizerunku od zezwolenia osoby przedstawionej na zdjęciu, z uwzględnieniem wyjątków wskazanych w ust. 2 tego przepisu, który wyłącza obowiązek posiadania zezwolenia m.in. w przypadku, gdy wizerunek dotyczy osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza. Przetwarzanie danych osobowych (nawet w postaci wizerunku osoby fizycznej) nie jest tożsame z rozpowszechnianiem wizerunku w rozumieniu ustawy o prawie autorskim i prawach pokrewnych, co skutkuje tym, że wyrażenie zgody na przetwarzanie danych osobowych nie stanowi jednocześnie zgody na rozpowszechnianie wizerunku i odwrotnie. Wskazane zgody mają charakter niezależny, wobec czego zgoda na przetwarzanie danych w rozumieniu rozporządzenia 2016/679 powinna być wyraźnie wyodrębniona od zgody w rozumieniu art. 81 ustawy o prawie autorskim i ustawach pokrewnych. Tym samym należy przyjąć, że podstawą prawną przetwarzania danych osobowych w postaci wizerunku jest zgoda osoby, której dane dotyczą, a nie prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO). W przypadku małoletniego do przetwarzania jego wizerunku wymagane jest uzyskanie zgody przedstawiciela ustawowego.

2) Publikowanie numerów tablic rejestracyjnych pojazdów

Jedno z pytań dotyczyło tego, czy publikacja na portalu internetowym zdjęć samochodów z widocznymi ich numerami rejestracyjnymi, bez zgody właścicieli pojazdów, jest dopuszczalna z punktu widzenia przepisów o ochronie danych osobowych.

W kontekście oceny, czy tablice rejestracyjne samochodu stanowią dane osobowe, kluczowe znaczenie ma możliwość dokonania na ich podstawie pośredniej

[345] DOL.023.1010.2024.

[346] Dz.U. z 2025 r., poz. 24.

identyfikacji osoby fizycznej będącej właścicielem pojazdu. Dysponują nią nie tylko właściwe organy państwowe, ale także inne osoby, które złożą odpowiednio uzasadniony wniosek do Centralnej Ewidencji Pojazdów i Kierowców. Ponadto właściciela pojazdu za pomocą numeru rejestracyjnego pośrednio zidentyfikować mogą również osoby będące np. jego znajomymi, członkami rodzin czy współpracownikami. Ze wskazanych powyżej powodów należy uznać, że tablice rejestracyjne mogą stanowić dane osobowe. Co zaś do publikowania zdjęć pojazdów należących do podmiotów prowadzących działalność gospodarczą należy wskazać, że w przypadku osób fizycznych prowadzących działalność gospodarczą ich dane w zakresie niedotyczącym wprost tej działalności, objęte są przepisami RODO. Dane osób prawnych nie stanowią natomiast danych osobowych[347].

3) Osoba prawna jako inspektor ochrony danych

Interesującym zagadnieniem było zapytanie dotyczące prawnej możliwości wyznaczenia spółki prawa handlowego jako inspektora ochrony danych osobowych. Pytający uznawał taką możliwość, co miało wynikać z treści Wytycznych Grupy Roboczej art. 29 dotyczącej inspektorów ochrony danych (WP 243) oraz tego, że model taki funkcjonuje np. we francuskim prawie ochrony danych osobowych[348]. Prezes UODO został poproszony o wypowiedzenie się w powyższej kwestii oraz o wskazanie czy w takim przypadku odpowiedzialność za wykonywanie obowiązków inspektora obciążałby spółkę (zespół ds. ochrony danych osobowych) czy inspektora ochrony danych wskazanego z imienia i nazwiska.

Odpowiedź Prezesa UODO była w tym temacie jednoznaczna. Na funkcję inspektora ochrony danych może być wyznaczona wyłącznie konkretna osoba fizyczna. Przepisy ustawy o ochronie danych osobowych wymagają, aby administrator i podmiot przetwarzający, którzy wyznaczyli inspektora ochrony danych (IOD), udostępnili imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora na swojej stronie internetowej lub gdy administrator nie posiada własnej strony, w sposób ogólnie dostępny w miejscu prowadzenia działalności (art. 11). Imię i nazwisko konkretnej osoby pełniącej funkcję IOD należy też podać Prezesowi UODO, powiadamiając go o wyznaczeniu takiej osoby (art. 10 ust. 1 ustawy o ochronie danych osobowych). IOD jest punktem kontaktowym dla osób, których dane dotyczą i organu nadzorczego zgodnie z art. 38 ust. 4 i art. 39 ust. 1 lit. e rozporządzenia 2016/679. Zatem zarówno wewnątrz podmiotu będącego administratorem, jak i w relacjach zewnętrznych, dla wszystkich musi być jasne, jaka konkretna osoba fizyczna pełni tę funkcję.

4) Pozyskiwanie danych z Systemu Informacyjnego Schengen

W roku 2024 pojawiło się pytanie o możliwość uzyskania przez podmiot danych informacji o tym, czy dane osobowe jego dotyczące są przetwarzane w SIS (Systemie

[347] DOL.023.162.2024.
[348] DOL.023.698.2024.

Informacyjnym Schengen)[349]. SIS to wielkoskalowy system informatyczny, utworzony jako narzędzie rekompensujące zniesienie kontroli na granicach wewnętrznych i mającym na celu zapewnienie wysokiego poziomu bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej.

Z technicznego punktu widzenia SIS składa się z systemu centralnego, krajowych systemów SIS oraz sieci łączącej te systemy. Za ogólny nadzór nad systemem centralnym odpowiada Komisja Europejska, natomiast za nadzór nad krajowym N.SIS sprawuje centralny organ techniczny KSI, czyli Komendant Główny Policji (art. 26 ust. 1 w zw. z art. 2 ust. 3 ustawy z 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[350]. Osoba niebędąca obywatelem UE, której właśnie wydano decyzję nakazującą powrót lub której odmówiono wjazdu i pobytu, ma prawo otrzymać informację czy w SIS został dokonany wpis na jej temat, a także informację o przechowywaniu jej danych. Informację tę można uzyskać od właściwych w danym kraju organów. W Polsce organem udzielającym informacji w zakresie wpisów w SIS jest Komendant Główny Policji. Każda osoba, której dotyczy wpis w SIS, może wystąpić o dostęp do danych oraz żądać ich usunięcia (art. 53 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1861 z 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006[351] oraz art. 67 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[352]. Każdy, kto uważa, że jego prawa w zakresie ochrony danych osobowych nie są przestrzegane, może wnieść skargę na administratora danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych.

5) Umieszczanie imion i nazwisk pracowników na ubraniach roboczych

Jeden z przedsiębiorców zwrócił się z pytaniem o prawną możliwość umieszczania na odzieży roboczej imion i nazwisk pracowników spółki[353]. W kontekście tego problemu wskazane zostało, że pracodawca ma obowiązek chronić dane osobowe osób, które zatrudnia, zgodnie z przepisami o ochronie danych osobowych. Dane osobowe powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami zgodnie z zasadą ograniczenia celu z art. 5 ust. 1 lit. b rozporządzenia 2016/679. Pracodawca jest odpowiedzialny za przestrzeganie przepisów z art. 5 rozporządzenia

[349] DOL.023.40.2024.
[350] Dz.U. z 2023 r. poz. 1355.
[351] Dz.U. UE. L. z 2018 r. Nr 312, str. 14 z późn. zm.
[352] Dz.U. UE. L. z 2018 r. Nr 312, str. 56 z późn. zm.
[353] DOL.023.360.2024.

2016/679 i musi być w stanie wykazać ich przestrzeganie zgodnie z zasadą rozliczalności z art. 5 ust. 2 rozporządzenia 2016/679. W odniesieniu do zamieszczania imienia i nazwiska na odzieży roboczej pracownika pracodawca powinien nie tylko dokonać analizy czy dysponuje przesłanką uprawniającą go do takiego działania, ale również znać konkretny cel, w jakim miałoby nastąpić udostępnienie danych, które pozyskał w ściśle określonych przepisami prawa pracy celach. Przepisy prawa pracy nie regulują szczegółowo kwestii związanych z ujawnianiem danych osobowych pracownika, w tym na odzieży służbowej, dlatego te kwestie powinny znajdować odzwierciedlenie w wewnętrznych regulowaniach u danego pracodawcy, o ile działania te są niezbędne i usprawiedliwione celem działania zakładu pracy. Zgodnie z art. 104 § 1 Kodeksu pracy regulamin pracy ustala organizację i porządek w procesie pracy oraz związane z tym prawa i obowiązki pracodawcy i pracowników, natomiast na jego elementy wskazuje art. 104^1 tej ustawy.

6) Dopuszczalność utrwalania wizerunku osób fizycznych w związku z naruszaniem przez te osoby zasad bezpieczeństwa i higieny pracy

Pytający zwrócił się o udzielenie wyjaśnień co do legalności utrwalania wizerunku pracowników podlegających kontroli bezpieczeństwa i higieny pracy w związku z nieprawidłowościami, których się osoby te dopuściły. Zapytanie dotyczyło sytuacji, kiedy zdjęcia stanowią dowód i podstawę do wyciągania odpowiedzialności służbowej zgodnie z przepisami Kodeksu pracy lub umów kontraktowych między generalnym wykonawcą a jego podwykonawcami.

Zgodnie ze stanowiskiem Prezesa UODO[354] brak jest przepisu prawa wprost zezwalającego pracodawcy na utrwalanie i wykorzystywanie wizerunku pracownika w sytuacji opisanej w pytaniu. Jednakże należy mieć na uwadze treść przepisów art. 207 § 1 i 234 § 1 Kodeksu pracy odpowiednio z którymi: pracodawca ponosi odpowiedzialność za stan bezpieczeństwa i higieny pracy w zakładzie pracy, a także w razie wypadku przy pracy jest obowiązany podjąć niezbędne działania eliminujące lub ograniczające zagrożenie, zapewnić udzielenie pierwszej pomocy osobom poszkodowanym i ustalić w przewidzianym trybie okoliczności i przyczyny wypadku oraz zastosować odpowiednie środki zapobiegające podobnym wypadkom. Nałożone przez przepisy prawa pracy obowiązki na pracodawcę mogą uzasadniać w pewnych sytuacjach utrwalanie (fotograficzne lub wideo) wizerunku pracowników naruszających bezpieczeństwo pracy, bez konieczności pozyskiwania zgody pracowników na przetwarzanie danych. W tym miejscu należy odwołać się do § 3 rozporządzenia Rady Ministrów w sprawie służby bezpieczeństwa i higieny pracy z 2 września 1997 r.[355], który stanowi, że służba bhp jest uprawniona m.in. do występowania do osób kierujących pracownikami z zaleceniami usunięcia stwierdzonych zagrożeń wypadkowych i szkodliwości zawodowych oraz uchybień w zakresie bezpieczeństwa i higieny pracy, występowania do pracodawcy o zastosowanie kar porządkowych w stosunku do pracowników odpowiedzialnych za zaniedbanie obowiązków w zakresie

[354] DOL.023.385.2024.

[355] Dz.U. Nr 109, poz. 704.

bezpieczeństwa i higieny pracy, niezwłocznego odsunięcia od pracy pracownika, który swoim zachowaniem lub sposobem wykonywania pracy stwarza bezpośrednie zagrożenie życia lub zdrowia własnego albo innych osób.

Rozporządzenie nie wskazuje środków dokumentowania przez służbę bhp powyżej wskazanych okoliczności celem wyciągnięcia konsekwencji wobec pracownika naruszającego zasady bezpieczeństwa pracy. Na uwadze należy mieć to, że dokumentacja zdjęciowa (wideo) sporządzona przez służbę bhp mogłaby stanowić załącznik do protokołu powypadkowego, o ile doszłoby do wypadku przy pracy z przyczyn nieprzestrzegania zasad bezpieczeństwa przez pracownika, a następnie mogłaby być dowodem w postępowaniu przeciwko pracownikowi, który dopuścił się takiego naruszenia np. celem rozwiązania stosunku pracy, nałożenia kary porządkowej etc. Dokumentowanie zdjęciem łamania przez pracowników przepisów bhp i przetwarzanie w tym celu danych pracowników obejmujących także ich wizerunek może zostać za uzasadnione, o ile spełnione są warunki przewidziane przepisami art. 6 i 9 rozporządzenia 2016/679.

11.1.2. Pytania od inspektorów ochrony danych

Rola inspektorów ochrony danych (IOD), co organ nadzorczy konsekwentnie podkreśla, ma fundamentalne znaczenie dla budowy skutecznego systemu ochrony danych osobowych. Przejawia się ona głównie we wspieraniu administratorów w realizacji obowiązków dotyczących ochrony danych osobowych poprzez monitorowanie prowadzonego przetwarzania danych pod kątem jego zgodności z prawem, a także doradzanie w zakresie obowiązków ciążących na administratorach i podmiotach przetwarzających. 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 i udzielanie im wsparcia następowało dotychczas w wielu formach, spośród których jedną z najważniejszych jest udzielanie im indywidualnych konsultacji.

Niezależnie od tego zadaniem UODO jest również rozwijanie współpracy z inspektorami w formule umożliwiającej w jak największym stopniu wymianę poglądów i doświadczeń. W 2024 r. Prezes UODO odbył wiele spotkań z organizacjami reprezentującymi różne środowiska inspektorów ochrony danych, które przedstawiały aktualne wyzwania związane z pełnieniem funkcji IOD, a także wskazywały na brak zrozumienia statusu IOD przez administratorów, co skutkuje tym, że administrator często przerzuca swoje obowiązki na IOD.

Na problem nakładania na IOD obowiązków administratora zwrócono uwagę m.in. w sprawozdaniu EROD z działania CEF DPO przeprowadzonego w 2023 r.[356] Opublikowane w styczniu 2024 r. sprawozdanie EROD składa się ze sprawozdania ogólnego oraz sprawozdań krajowych poszczególnych organów nadzorczych, w tym

[356] https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en.

UODO[357]. Zarówno w sprawozdaniach krajowych, jak i sprawozdaniu ogólnym zostały zaprezentowane wyniki z przeprowadzonych badań, a także płynące z nich wnioski i rekomendacje dla organów nadzorczych, administratorów, podmiotów przetwarzających i inspektorów ochrony danych. Mają one na celu przyczynienie się do właściwego przestrzegania obowiązków administratorów i podmiotów przetwarzających oraz prawidłowego wykonywania zadań przez inspektorów, a także usprawnienie i ujednolicenie sposobu egzekwowania przepisów z zakresu ochrony danych osobowych przez organy nadzorcze.

W sprawozdaniach krajowych zawarto szczegółowe informacje m.in. w zakresie stwierdzonych problemów z przestrzeganiem przepisów dotyczących inspektora ochrony danych. W sprawozdaniu UODO zasygnalizowane zostały w szczególności zidentyfikowane problemy 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.

Stanowisko polskiego organu nadzorczego w ramach CEF DPO zostało zaprezentowane podczas spotkania „Niezależność inspektora ochrony danych w świetle skoordynowanego działania EROD CEF DPO", które odbyło się w siedzibie UODO 9 kwietnia 2024 r.[358] Miało ono na celu upowszechnianie informacji o zeszłorocznym działaniu EROD i sprawozdaniu z tego działania, w tym raportu polskiego organu nadzorczego i przedstawionych w nim zagadnień. Na spotkaniu omówiono standardy w zakresie niezależności IOD wynikające z przepisów o ochronie danych osobowych oraz występujące w praktyce problemy. Dodatkowo po spotkaniu uruchomiony został specjalny adres e-mail, na który można było przesyłać opinie dotyczące tematów omawianych na spotkaniu oraz propozycje działań, jakie mogłyby być pomocne w zapewnieniu inspektorom odpowiedniego statusu i warunków do pełnienia tej funkcji. Nadawcy tych wiadomości dzielili się w nich swoimi doświadczeniami w zakresie pełnienia funkcji IOD (np. przypadki nakładania na IOD zadań administratora, brak świadomości administratorów co do roli, zadań i statusu

[357] Sprawozdanie krajowe polskiego organu nadzorczego w ramach CEF DPO (https://uodo.gov.pl/pl/138/2960).
[358] Podsumowanie efektów tego spotkania można znaleźć w komunikacie pt. „Niezależność IOD musi być standardem – podsumowanie efektów spotkania w UODO" (https://uodo.gov.pl/pl/138/3118).

IOD); przedstawiali też konkretne pytania dotyczące zadań wykonywanych przez inspektora (np. w związku z naruszeniami ochrony danych, realizowaniem roli punktu kontaktowego, przeprowadzaniem audytów czy funkcjonowaniem w centrach usług wspólnych); zgłaszali postulaty co do działań, które mogłyby przyczynić się do poprawy postrzegania roli IOD oraz pełnienia przez niego swojej funkcji (np. ograniczenie możliwości zawierania umów na świadczenie funkcji IOD za 200–300 zł i świadczenia takich usług u dużej liczby administratorów).

Zagadnienia dotyczące roli i niezależnej pozycji IOD oraz współpracy inspektorów ochrony danych z UODO prezentowane były przez UODO w bieżącym okresie sprawozdawczym w ramach akcji „UODO rusza w kraj". Spotkania te były okazją do rozmów na temat aktualnej sytuacji inspektorów w strukturach administratorów (przede wszystkim należących do samorządu terytorialnego oraz terenowych jednostek administracji zespolonej) oraz o praktycznych rozwiązaniach służących zapewnieniu przestrzegania prawa w tym zakresie.

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 2024 roku do UODO wpłynęły **233 pytania od inspektorów ochrony danych.** Udzielono zaś 236 odpowiedzi na pytania od IOD. Wspólny dorobek wypracowany z IOD w zakresie pytań i odpowiedzi sprawia, że liczba pytań od IOD corocznie maleje (w 2023 r. wpłynęły 253 pytania, w 2022 r. - 274 pytania, a w 2021 r. było ich 301). Wynikać to może z tego, że wiele kwestii związanych z właściwym stosowaniem przepisów dotyczących ochrony danych osobowych, w tym pełnienia funkcji IOD, zostało już wyjaśnionych i rozpowszechnionych w poprzednich latach, zarówno w indywidualnej korespondencji z inspektorami, jak i w specjalnej zakładce adresowanej do inspektorów, która była przygotowywana na podstawie wpływających do UODO pytań od inspektorów ochrony danych, a także w newsletterze UODO dla IOD oraz w Biuletynie UODO (https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod). Zamieszczane tam wskazówki nie tylko pozwalają ocenić, jak postąpić w podobnej sprawie, ale również poprzez wskazanie kryteriów i etapów działań podpowiadają np., w jaki sposób dokonać analizy w zakresie określania ról podmiotów, podstaw prawnych czy oceny wniosków o udostępnienie danych. W materiałach tych organ nadzorczy prezentuje również kierunek i zasady interpretacji przepisów pomocne przy rozstrzyganiu wątpliwości z zakresu ochrony danych osobowych.

Pytania przesyłane przez inspektorów w 2024 r. dotyczyły bardzo różnych zagadnień. Zasadniczo można je podzielić na dwie większe grupy, w których pojawia się kilka tematów. Pierwsza grupa pytań obejmuje kwestie, które niezmiennie

pojawiają się w pytaniach IOD, ze względu na to, że związane są z różnorodnością konkretnych sytuacji, w których mogą wystąpić szczegółowe wątpliwości. Odnoszą się one do: występowania konfliktu interesów w związku z pełnieniem funkcji IOD, określenia statusu podmiotów biorących udział w procesie przetwarzania danych osobowych, udostępniania danych osobowych, problemów ze stosowaniem w praktyce zarówno przepisów prawa dotyczących ochrony danych osobowych, jak i przepisów sektorowych.

Natomiast druga, obszerna grupa pytań od IOD dotyczyła wydarzeń i problemów bieżących wynikających m.in. z wprowadzenia nowych przepisów prawa. Były to zagadnienia związane z przetwarzaniem danych osobowych w związku ze stosowaniem przepisów tzw. ustawy Kamilka czy ustawy o doręczeniach elektronicznych, a także dotyczące niezależności IOD w sytuacji nałożenia na niego zadania związanego z obsługą zgłoszeń wniosków dotyczących naruszeń prawa (sygnaliści).

Przekazywane przez IOD informacje o pojawiających się problemach w stosowaniu przepisów o ochronie danych osobowych pozwalają organowi na bieżąco podejmować działania zmierzające do podnoszenia poziomu ochrony danych osobowych, w tym m.in. poprzez:

- udzielanie odpowiedzi na pytania IOD i przygotowywanie wyjaśnień publikowanych na stronie internetowej UODO lub Biuletynie UODO,
- sygnalizowanie właściwym podmiotom zaobserwowanych nieprawidłowości lub potrzeby zmian legislacyjnych.

11.1.3. Udzielanie odpowiedzi na pytania IOD

W omawianym okresie 2024 r. 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.
2) Określenie statusu podmiotów w procesie przetwarzania danych osobowych.
3) Weryfikacja podmiotu przetwarzającego i umowy powierzenia.
4) Udostępnianie danych osobowych.
5) Stosowanie różnych form monitoringu.
6) Przetwarzanie danych osobowych w związku z zatrudnieniem.
7) Przetwarzanie danych osobowych dotyczących dzieci.
8) Przetwarzanie danych osobowych w związku z ochroną małoletnich.
9) Przetwarzanie danych osobowych z wykorzystaniem nowych technologii.
10) Ochrona danych osobowych przetwarzanych z wykorzystaniem rozwiązań informatycznych.
11) Realizacja praw osoby, której dane dotyczą.

Ad 1. Wyznaczanie, status i zadania inspektora ochrony danych

Dla inspektorów ochrony danych kwestie ich niezależnej pozycji oraz prawidłowego, etycznego wykonywania funkcji mają fundamentalne znaczenie. Od lat

dużą wagę przywiązują oni również do właściwego rozróżnienia ich roli od roli organizacji, w których pełnią swoją funkcję.

W 2024 r. wśród sygnałów od IOD często pojawiały się wątpliwości i zastrzeżenia dotyczące praktyki obciążania ich zadaniami, które nie powinny być przez nich wykonywane ze względu na konflikt interesów, o którym mowa w art. 38 ust. 6 RODO. Inspektorzy na konkretnych przykładach wskazywali cedowanie na nich obowiązku zgłaszania naruszeń (w tym również występowania jako pełnomocnik administratora).

Wątpliwości inspektorów dotyczyły tego, że:

- osoba podpisująca formularz zgłoszenia naruszenia zobowiązuje się do realizacji pewnych działań, np. wdrożenia nowych rozwiązań informatycznych związanych z podniesieniem bezpieczeństwa danych (które to działania niejednokrotnie wiążą się z ponoszeniem zobowiązań finansowych), a IOD nie ustala środków organizacyjno-technicznych u administratora, ponieważ o nich nie decyduje,
- IOD na etapie obsługi naruszenia może doradzić pewne działania, które stanowiłyby treść zgłoszenia naruszenia/pism wyjaśniających, a administrator może ich nie wdrożyć lub wdrożyć inne działania,
- gdyby to IOD wykonywał obowiązek zgłoszenia naruszenia i jednocześnie – w ramach swojej funkcji monitorującej – miałby oceniać, czy ten obowiązek jest prawidłowo wykonywany, to prowadziłoby to do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością.

Inspektorzy wskazywali, że wyręczanie administratora przez IOD doprowadzić może do regresu świadomości administratora w zakresie odpowiedzialności, która na nim spoczywa, a także do nasilenia tendencji cedowania na IOD zadań spoczywających na administratorze. Jest to szczególnie ważne ze względu na rosnącą liczbę aktów prawnych, zwłaszcza tych dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa, których stosowanie będzie ogromnym wyzwaniem dla wielu podmiotów z sektora prywatnego oraz publicznego.

Prezes UODO konsekwentnie wskazuje, że do zadań inspektora ochrony danych należy m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk danego administratora, a także nadzorowanie prawidłowego wykonywania wynikających z nich obowiązków, doradzanie i podnoszenie świadomości w tym zakresie. Dlatego IOD nie powinien być osobą, która wyręcza administratora w realizacji należących do niego zadań. Gdy administrator nakłada na IOD zadania, które mogą stać się następnie przedmiotem dokonywanych przez IOD czynności monitorowania (zwłaszcza gdy chodzi o zadania należące do administratora) lub których realizacja prowadziłaby do określania przez niego celów i sposobów przetwarzania, wówczas IOD zmuszony byłby oceniać wyniki swojej pracy. To z kolei może wpłynąć na niezależność i obiektywizm tej oceny, a więc prowadzić do konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO. Konflikt interesów następuje, jeśli nie można pogodzić prawidłowego wykonywania zadań IOD z realizacją innych zadań, gdyż pomiędzy zadaniami występuje sprzeczność uniemożliwiająca odpowiednią ich realizację. Z konfliktem interesów mamy do

czynienia również wtedy, gdy obowiązków nałożonych na IOD jest tak dużo, że IOD musi wybrać, które z nich realizować, a które nie, z powodu braku czasu koniecznego na ich wykonanie.

Dlatego administrator przed powierzeniem inspektorowi innych zadań, niż te przewidziane w RODO, powinien dokonać analizy, czy IOD będzie w stanie prawidłowo i niezależnie wykonywać swoje obowiązki. Nieprzeprowadzenie analizy w tym zakresie może w konsekwencji spowodować naruszenie przepisów o ochronie danych osobowych. 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 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.

Na problem nakładania na IOD obowiązków administratora organ nadzorczy zwracał uwagę również w sprawozdaniu EROD z działania CEF DPO[359].Temat ten został również szeroko omówiony na spotkaniu w dniu 9 kwietnia 2024 r.[360]

Dlatego też w odpowiedzi na pytanie IOD dotyczące **możliwości obsługi i zgłaszania naruszeń przez IOD**[361] Prezes UODO wskazał, że niewłaściwą praktyką jest obarczanie inspektorów ochrony danych odpowiedzialnością za stwierdzanie, kwalifikowanie i zgłaszanie naruszeń ochrony danych osobowych[362].

Na konieczność zapewnienia inspektorowi możliwości niezależnego monitorowania przetwarzania danych osobowych przez administratora zwrócił uwagę również Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 9 lutego 2023 r. w sprawie C-453/21, X FAB Dresden GmbH & Co. KG. TSUE wskazał, że z konfliktem interesów będziemy mieli do czynienia w sytuacji, gdy nie sposób pogodzić prawidłowej realizacji zadań inspektora ochrony danych z wykonywaniem innych zadań, ponieważ między tymi zadaniami istnieje (bądź może istnieć) niezgodność (sprzeczność), która uniemożliwia niezależne wykonywanie zadań IOD, a tym samym nie jest zapewniona skuteczność przepisów RODO. Trybunał stwierdził ponadto, że nie można powierzyć IOD zadań lub obowiązków, które prowadziłyby do określania przez niego celów i sposobów przetwarzania danych osobowych u administratora, ponieważ monitorowanie tych celów i sposobów powinno być prowadzone przez IOD w sposób niezależny.

W odniesieniu do naruszeń ochrony danych rola inspektora ochrony danych powinna ograniczać się przede wszystkim do **doradzania administratorowi**

[359] Sprawozdanie krajowe polskiego organu nadzorczego w ramach CEF DPO (https://uodo.gov.pl/pl/138/2960).
[360] Podsumowanie efektów tego spotkania zawarte są w komunikacie pt. „Niezależność IOD musi być standardem – podsumowanie efektów spotkania w UODO" (https://uodo.gov.pl/pl/138/3118).
[361] DOL.502.178.2024, DOL.502.83.2024.
[362] Takie stanowisko przedstawione zostało zarówno w materiale pt. „Rola kierownictwa administratora w procesie wykonywania przepisów RODO", opublikowanym w Biuletynie UODO - Wydanie 5 (maj 2024) jak również w prezentacji załączonej do materiału „Niezależność IOD musi być standardem – podsumowanie efektów spotkania w UODO", w szczególności w panelach nr 3 i 4.

i monitorowania przyjmowanych przez niego rozwiązań, zaś ostateczna decyzja, np. co do kwalifikacji naruszenia, zgłaszania naruszenia czy wdrożenia nowych środków, powinna należeć do administratora. W taki sposób o roli IOD wypowiedziała się również EROD w Wytycznych 9/2022 w sprawie powiadamiania o naruszeniu ochrony danych osobowych zgodnie z RODO. Wskazała tam, że 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 EROD zaleca, aby był on niezwłocznie informowany o zaistnieniu naruszenia i był zaangażowany w cały proces zarządzania naruszeniami i powiadamiania oraz monitorował, czy wszystkie działania związane z naruszeniem ochrony danych osobowych zostały wykonane prawidłowo.

Co ważne, efektywne i prawidłowe wykonanie przez administratora jego obowiązków związanych z **obsługą naruszenia ochrony danych** (w tym z właściwym ich dokumentowaniem) wymaga wdrożenia przez niego stosownych procedur. Taka procedura pomoże ujednolicić, usprawnić oraz przyśpieszyć działania w przypadku wykrycia naruszenia ochrony danych[363]. Powinna również zawierać postanowienia odnoszące się do roli IOD w obsłudze naruszenia ochrony danych osobowych. Jednak ostateczną decyzję, czy naruszenie zostanie zgłoszone i czy zostaną powiadomione osoby, których dane osobowe uległy naruszeniu, powinien podejmować administrator, co powinno zostać udokumentowane. To administrator również powinien podejmować decyzje dotyczące wdrożenia dodatkowych zabezpieczeń lub innych działań naprawczych, co do których IOD powinien mu doradzać, a następnie sprawdzać, czy zabezpieczenia i działania zostały wdrożone.

Analogicznie należy podejść do **obowiązku prowadzenia rejestru naruszeń**. Z treści art. 33 ust. 5 RODO jednoznacznie wynika, że to do administratora należy obowiązek prowadzenia dokumentacji naruszeń ochrony danych osobowych. Zgodnie z powołanym przepisem administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Mimo że przepis ten nie wskazuje szczególnej formy, w jakiej rejestr naruszeń ma być prowadzony, dokumentacja ta musi być prowadzona w taki sposób, aby pozwolić organowi nadzorczemu na weryfikowanie przestrzegania ww. przepisu RODO przez administratora. Prowadzenie dokumentacji naruszeń pozwala również na monitorowanie, czy administrator dokonuje odpowiednich zgłoszeń naruszeń ochrony danych osobowych Prezesowi UODO.

[363] Punkt 2.1 poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" (https://archiwum.uodo.gov.pl/pl/134/1029).

Wątpliwości dotyczące konfliktu interesów pojawiły się również w związku z wdrożeniem ustawy o ochronie sygnalistów[364]. Pytania IOD dotyczyły tego, **czy IOD może obsługiwać zgłoszenia dotyczące sygnalistów**[365]. Prezes UODO wskazał, że jednym z naruszeń prawa objętym zakresem ustawy o ochronie sygnalistów są naruszenia dotyczące ochrony prywatności i danych osobowych (art. 3 ust. 1 pkt 13). Zatem zgłoszenie sygnalisty procedowane według tej ustawy może dotyczyć materii, która byłaby oceniana również przez IOD w ramach wykonywania przez niego jego zadań określonych w art. 39 ust. 1 lit. b RODO. W takiej sytuacji zasadnie należy uznać, że może dojść do konfliktu interesów. Trudno bowiem sobie wyobrazić, że IOD byłby w stanie zachować bezstronność, gdyby zgłoszenie dotyczyło obszaru ochrony danych osobowych, czyli zagadnień, które wcześniej były przedmiotem jego oceny. Podobnie byłoby również w sytuacji, gdy zgłoszenie dotyczyło naruszenia prawa podczas wykonywania zadań przez samego IOD.

Konflikt interesów może również pojawić się w zakresie realizacji zadania IOD określonego w art. 38 ust. 4 RODO, tj. **pełnienia punktu kontaktowego dla osób, których dane dotyczą,** a więc również dla sygnalistów. Osoby, których dane dotyczą, zgodnie z art. 38 ust. 4 RODO mogą skontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. Tę rolę należy rozumieć jako wsparcie dla osób, których dane dotyczą w sytuacjach, w których zgłosiły one zastrzeżenia, trudności czy wątpliwości co do przetwarzania ich danych osobowych. Angażowanie IOD w procedowanie zgłoszeń sygnalistów może podważyć jego niezależność i obiektywizm w oczach osób, których dane dotyczą, a tym samym doprowadzić do konfliktu interesów i uniemożliwić IOD prawidłowe/niezależne wykonywanie jego zadań.

Nie można również wykluczyć, że na każdym etapie obsługi zgłoszenia sygnalisty może dochodzić do określania celów i sposobów przetwarzania danych osobowych. Zaangażowanie IOD w procedowanie zgłoszeń naruszenia prawa może tym samym prowadzić do konfliktu interesów. Zgodnie z art. 8 ust. 4 ustawy o ochronie sygnalistów podmiot prawny albo organ publiczny po otrzymaniu zgłoszenia przetwarza dane osobowe w zakresie niezbędnym do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego. Dane osobowe, które nie mają znaczenia dla rozpatrywania zgłoszenia, nie są zbierane, a w razie przypadkowego zebrania są niezwłocznie usuwane. Usunięcie tych danych osobowych następuje w terminie 14 dni od chwili ustalenia, że nie mają one znaczenia dla sprawy. IOD jako osoba bezpośrednio zaangażowana w proces obsługi zgłoszenia naruszenia prawa może być zmuszony do dokonania oceny, jakie dane osobowe są niezbędne do przyjęcia zgłoszenia lub podjęcia ewentualnego działania następczego, tj. decydowania o ważnych aspektach przetwarzania danych osobowych. Dodać należy, że ochrona tożsamości sygnalisty również wymaga podejmowania decyzji ad hoc, czy i jakie dane osobowe powinny być przetwarzane, tak aby nie wyjawić tożsamości sygnalisty. Zgodnie z art. 8 ust. 1 ustawy

[364] Ustawa z 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. poz. 928).
[365] DOL.502.161.2024.

o ochronie sygnalisty, dane osobowe sygnalisty, pozwalające na ustalenie jego tożsamości, nie podlegają ujawnieniu nieupoważnionym osobom, chyba że za wyraźną zgodą sygnalisty. A zatem również ze względu na konieczność zapewnienia poufności danych osobowych IOD nie powinien brać udziału w procedowaniu zgłoszenia sygnalisty[366].

Ponadto obsługa zgłoszeń od sygnalistów może wymagać dużych nakładów czasu i pracy. Wobec czego w przypadku próby obciążenia tymi zadaniami IOD może zaistnieć ryzyko zaniedbywania obowiązków IOD wynikających z przepisów RODO, z uwagi na brak czasu na realizację tych zadań.

Organ nadzorczy już poprzednim roku sprawozdawczym odnosił się do zagadnienia dotyczącego **występowania IOD w roli pełnomocnika administratora**. 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 lit. 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.

Prezes UODO w związku z powiadomieniem przez IOD o wyznaczeniu go do pełnienia funkcji IOD na podstawie udzielonego mu pełnomocnictwa do dokonania tej czynności[367] przypomniał, że obowiązek zawiadomienia o wyznaczeniu inspektora ochrony danych ciąży na administratorze, nie zaś na wyznaczonym przez niego inspektorze (art. 37 ust. 7 RODO oraz art. 10 ust. 1 ustawy o ochronie danych osobowych[368]). Wobec powyższego to administrator, a nie IOD, powinien podpisać zawiadomienie o wyznaczeniu IOD. Administrator może ustanowić pełnomocnika do dokonania zgłoszenia dotyczącego IOD (art. 10 ust. 2 ustawy z 10 maja 2018 r. o ochronie danych osobowych), jednak takim pełnomocnikiem nie może być inspektor ochrony danych czy też zastępca IOD[369]. Zawiadomienia dokonanego przez IOD nie

[366] W pkt 40 Wytycznych 07/2020 dotyczących pojęć administratora i podmiotu przetwarzającego zawartych w RODO, EROD uznaje podejmowanie decyzji o tym, jak długo i jakie dane przetwarzać, za kwestie odnoszące się do decydowania o istotnych sposobach przetwarzania danych osobowych. Ta sfera przetwarzania danych osobowych jest zaś zarezerwowana dla administratora.
[367] DOL.5001.97.2024.
[368] Ustawa z 10 maja 2018 r. o ochronie danych osobowych.
[369] Więcej informacji dotyczących tego, że IOD nie powinien być pełnomocnikiem administratora znajduje się w materiale „Za realizację praw osób w zakresie dostępu do dotyczących ich danych odpowiada administrator", zamieszczonym w Biuletynie UODO Wydanie 1 (styczeń 2024) oraz Sprawozdaniu krajowym polskiego organu nadzorczego opracowanym w ramach CEF DPO (str. 9 i 10).

można uznać za prawidłowe i wobec tego powinno zostać ponownie przesłane przez administratora.

W okresie sprawozdawczym wpływały również **pytania dotyczące ustalenia, czy w określonej sytuacji administrator ma obowiązek wyznaczenia IOD w związku z przetwarzaniem przez niego danych osobowych w celu zapobiegania i zwalczania przestępczości.** Na gruncie przepisów dotyczących ochrony danych osobowych administrator może być bowiem zobowiązany do wyznaczenia IOD na podstawie RODO, a jednocześnie również na podstawie ustawy wdrażającej dyrektywę policyjną (DODO), czyli ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Obowiązek wynikający z tej drugiej ustawy dotyczy podmiotów, które przetwarzają dane 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 (art. 1 pkt 1 ustawy z 14 grudnia 2018 r.).

Mimo że Prezes UODO w materiale „Wyznaczenie IOD na podstawie ustawy wdrażającej dyrektywę policyjną (DODO)" wskazał, że podmioty odpowiedzialne za bezpieczeństwo imprez masowych oraz przewoźnicy lotniczy są w grupie administratorów, którzy muszą powołać IOD jako podmioty, do których ma zastosowanie ustawa z 14 grudnia 2018 r., to i tak pojawiły się wątpliwości dotyczące tego, **jakie przepisy sektorowe przewidują, że konkretne podmioty prywatne są zobowiązane wprost do wyznaczania IOD**[370]. Prezes UODO wyjaśnił, że właściwym organem w rozumieniu tej ustawy jest organ władzy publicznej, jednostka organizacyjna lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych (art. 4 pkt 16 ww. ustawy).

Organizator imprezy masowej jest zobowiązany do wyznaczenia IOD na podstawie art. 46 ust. 1 ustawy z 14 grudnia 2018 r. w zw. z art. 35 ustawy o bezpieczeństwie imprezy masowej. Organizator (osoba prawna, osoba fizyczna lub jednostka organizacyjna nieposiadająca osobowości prawnej) przeprowadzający imprezę masową zgodnie z art. 5 ustawy o bezpieczeństwie imprez masowych odpowiada za jej bezpieczeństwo. Bezpieczeństwo imprezy masowej obejmuje spełnienie przez organizatora wymogów w zakresie: zapewnienia bezpieczeństwa osobom uczestniczącym w imprezie (1); ochrony porządku publicznego; zabezpieczenia pod względem medycznym (3); zapewnienia odpowiedniego stanu technicznego obiektów budowlanych wraz ze służącymi tym obiektom instalacjami i urządzeniami technicznymi, w szczególności przeciwpożarowymi i sanitarnymi (4). Zgodnie zaś z art. 35 ust. 1 tej ustawy przetwarzanie informacji, w tym danych osobowych, dotyczących bezpieczeństwa imprez masowych odbywa się w celu zapobiegania przestępstwom i wykroczeniom związanym z tymi imprezami oraz ich zwalczania.

[370] DOL.5101.45.2024.

Przewoźnicy lotniczy są zobowiązani do wyznaczenia IOD na podstawie art. 46 ust. 1 ustawy z 14 grudnia 2018 r. w związku z art. 1 pkt 1 ustawy z 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera[371]. Ustawa o przetwarzaniu danych dotyczących przelotu pasażera określa zasady i warunki przekazywania przez przewoźników lotniczych danych dotyczących przelotu pasażera oraz przetwarzania tych danych w celu wykrywania i zwalczania przestępstw o charakterze terrorystycznym i innych przestępstw lub przestępstw skarbowych oraz zapobiegania im i ścigania ich sprawców, a także podmioty właściwe w tych sprawach. Zgodnie z art. 9 ust. 1 tej ustawy przewoźnik lotniczy, podczas dokonywania rezerwacji lub wystawiania biletu na przewóz lotniczy, informuje w formie pisemnej, w postaci papierowej lub elektronicznej, każdego pasażera o przetwarzaniu jego danych PNR i przekazywaniu ich do JIP (Krajowa Jednostka do spraw Informacji o Pasażerach), w celu określonym w art. 1 ust. 1 ww. ustawy.

Poza wskazanymi wyżej podmiotami (tj. podmioty odpowiedzialne za bezpieczeństwo imprez masowych oraz przewoźnicy lotniczy) podmiotami zobowiązanymi do wyznaczenia IOD, jak wyjaśnił Prezes UODO, będą wszystkie te podmioty, które przetwarzają dane w celach, o których mowa art. 1 pkt 1 ustawy z 14 grudnia 2018 r., co często wynika ponadto z przepisów ustawy regulującej obowiązki takich podmiotów.

W odpowiedzi na pytanie IOD, **czy obowiązek wyznaczenia IOD na podstawie ustawy z 14 grudnia 2018 r. zachodzi w odniesieniu do małej instytucji płatniczej (o której mowa w art. 2 ust. 1 pkt 3 ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu**)[372], organ wskazał, że obowiązek wyznaczenia IOD przez taki podmiot wynika z nałożonych na niego obowiązków określonych przepisami ww. ustawy z 1 marca 2018 r. (art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 i art. 90 ust. 1 i 2). Czynności podejmowane przez małe instytucje płatnicze wiążą się z zapobieganiem m.in. przestępstwom związanym z praniem pieniędzy lub finansowaniem terroryzmu, wobec czego podmiot ten jest zobowiązany do wyznaczenia IOD na podstawie ustawy z 14 grudnia 2018 r.

Innym zagadnieniem dotyczącym powoływania IOD była kwestia **wyznaczenia przez podmioty publiczne jednego, wspólnego IOD**[373]. Prezes UODO przypomniał, że zgodnie z art. 37 ust. 3 RODO, jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych. Prawodawca unijny nie wprowadza obowiązku powołania dla kilku organów/podmiotów publicznych jednego inspektora ochrony danych. Powołanie jednego IOD traktuje jako uprawnienie uzasadnione ekonomicznie i racjonalne z punktu widzenia zapewnienia prawidłowego przetwarzania danych osobowych przez podmioty publiczne, jeżeli spełnione są wskazane w przepisach

[371] Ustawa z 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. z 2022 r. poz. 1441).
[372] DOL.5101.78.2024.
[373] DOL.502.246.2023, DOL.502.136.2024.

RODO warunki. Zapewnieniu efektywności służyć mają uprawnienia i pozycja IOD. Wyznaczenie jednego, a nie wspólnego inspektora ochrony danych, przesądza bowiem o jego umocowaniu. Każdy z administratorów (organów/podmiotów publicznych) realizuje swoje obowiązki względem inspektora ochrony danych i korzysta z jego pracy bez względu na jego zaangażowanie u innych administratorów[374]. Skorzystanie z takiego rozwiązania wymaga jednak dokonania starannej analizy, czy wyznaczona osoba będzie w stanie równolegle prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora. Trzeba przy tym mieć świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. efektywnej dostępności.

Jest tak dlatego, że jednym z zadań IOD jest bieżące monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa oraz udzielanie informacji i rad w zakresie obowiązków wynikających z tych przepisów, zarówno administratorowi, jak i jego pracownikom. Ponadto rodzaj wymaganej od IOD fachowej wiedzy oraz umiejętności może różnić się w zależności od charakteru działalności administratora. Właściwe i efektywne wykonywanie powyższych zadań przez IOD (jak również innych jego zadań) na rzecz każdego z kilku (kilkunastu) administratorów wymaga posiadania przez niego szczegółowej wiedzy na temat sektora, w którym administratorzy działają i obowiązujących ich przepisów, stosowanych przez administratorów procedur administracyjnych, procesów przetwarzania, jakie każdy z administratorów prowadzi, systemów informatycznych oraz zabezpieczeń. A zatem ocena kwalifikacji IOD powinna również uwzględniać znajomość określonego sektora (działu administracji publicznej), w którym działa każdy z administratorów, i dotyczących go przepisów prawa. Z tego względu m.in. w przypadku wyznaczenia jednego IOD dla kilku podmiotów w ramach tej samej gminy zwrócić należy na różnorodność specyfiki podmiotów publicznych, które inspektor miałby obsługiwać, np. ośrodki pomocy społecznej, szkoły.

Trudno jest również wykonywać równolegle w wielu podmiotach zadania w zakresie punktu kontaktowego dla osób, których dane dotyczą, oraz punktu kontaktowego dla organu nadzorczego. Dodatkowo na mocy RODO każda osoba w każdej sprawie dotyczącej jej danych ma prawo kontaktować się z wyznaczonym dla danej organizacji inspektorem. Organ nadzorczy natomiast będzie mógł wymagać od inspektora gotowości do współpracy w związku z realizacją zadań i uprawnień organu w zakresie prowadzonych postępowań.

Kolejną ważną kwestią jest zapewnienie przez każdego z administratorów niezbędnych zasobów do wykonania przez IOD jego zadań. Chodzi tu przede wszystkim o właściwe zasoby czasu niezbędnego do właściwego wykonywania tych zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania (art. 38 ust. 2 RODO).

[374] E. Bielak-Jomaa [w:] *RODO. Ogólne rozporządzenie o ochronie danych*. Komentarz, red. D. Lubasz, Warszawa 2018, art. 37.

Ponadto administrator zobowiązany jest do zapewnienia, aby nie nakładać na IOD zadań, które mogłyby powodować konflikt interesów. Konflikt interesów może być bowiem rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD, jeśli IOD musi wybrać między obowiązkami, jakie będzie realizował, a tymi, którym nie podoła z powodu braku czasu koniecznego na ich wykonanie. Ocena, czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności. Oznacza to, że możliwość zaistnienia konfliktu powinna być stale monitorowana, ponieważ przyczyny zaistnienia takiego konfliktu mogą występować również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD.

Prezes UODO wskazał ponadto, że jeśli administratorzy podejmą decyzję o wyznaczeniu tej samej osoby do pełnienia w ich organizacjach funkcji IOD, wówczas konieczne jest osobne wyznaczenie IOD przez każdego z nich jako osobnych administratorów. Każdy z podmiotów zobowiązanych do wyznaczenia inspektora ochrony danych (niezależnie, czy będzie to jedna, ta sama osoba, czy różne osoby) będzie również zobowiązany – zgodnie z art. 37 ust. 7 RODO – do opublikowania danych kontaktowych inspektora i zawiadomienia o nich organu nadzorczego.

Od czasu wejścia w życie przepisów RODO na stronie internetowej UODO oraz w Newsletterze UODO dla IOD zamieszczane były wskazówki dotyczące tego, jak prawidłowo realizować obowiązek powiadomienia Prezesa UODO o wyznaczeniu, odwołaniu IOD (zastępcy IOD), m.in. z jakiego formularza elektronicznego (odpowiedniego do podstawy powołania IOD) należy skorzystać. W związku z pytaniem IOD dotyczącym potwierdzenia poprawności jego zgłoszenia[375] Prezes UODO jeszcze raz przypomniał, że administratorzy zobowiązani do wyznaczenia lub wyznaczający IOD (bądź jego zastępcę) na podstawie przepisów RODO, powinni skorzystać z formularzy oznaczonych jako „Zawiadomienia na podstawie RODO”[376], natomiast administratorzy zobowiązani do wyznaczenia lub wyznaczający IOD (bądź jego zastępcę) na podstawie ustawy z 14 grudnia 2018 r., powinni skorzystać z formularzy oznaczonych jako „Zawiadomienia na podstawie DODO”[377]. Co istotne, jeżeli zawiadomienie przesłane przez administratora jest nieprawidłowe, powinien on ponownie przesłać zawiadomienie.

Ad 2. Określanie statusu podmiotów w procesie przetwarzania danych osobowych

Zagadnienia dotyczące określenia ról podmiotów uczestniczących w procesie przetwarzania danych osobowych stanowią przedmiot wielu pytań przesyłanych przez inspektorów w każdym okresie sprawozdawczym. Mimo że pomocnych informacji w zakresie określania statusu administratora i podmiotu przetwarzającego można poszukiwać w Wytycznych EROD 07/2020 dotyczących pojęć administratora

[375] DOL.5001.96.2024, DOL.5101.74.2024.
[376] https://uodo.gov.pl/pl/502/2248.
[377] https://uodo.gov.pl/pl/502/2249.

i podmiotu przetwarzającego zawartych w RODO[378] oraz we wskazówkach prezentowanych przez UODO (np. w odpowiedziach na pytania zamieszczone w zakładce IOD/Zadania IOD[379], dostępnych pod linkiem, to i tak kwestia ta wciąż była przedmiotem pytań IOD. Powodem tego może być sposób ujęcia terminu „administrator" w przepisach o ochronie danych osobowych. W odpowiedziach udzielanych inspektorom UODO wskazywał kryteria pomocne w ocenie statusu podmiotów biorących udział w przetwarzaniu danych. W wielu przypadkach odwoływał się do Wytycznych EROD 07/2020, w których znajdują się wskazówki, jak należy identyfikować administratora, a które jednocześnie zwracają uwagę, że administrowanie może wynikać nie tylko z przepisów prawnych, lecz również z faktycznego wpływu na cele i sposoby przetwarzania danych. Istnieją przypadki, w których administrator lub kryteria jego wyznaczania są wprost określone w przepisie prawa, jednak bardziej powszechne są sytuacje, w których status ten wynika z tego, że określony przepis prawa nakłada na dany podmiot zadanie lub obowiązek gromadzenia i przetwarzania określonych danych. Wówczas administratorem jest zwykle organ wyznaczony na mocy prawa do realizacji tego zadania publicznego. W takim przypadku prawo, choć pośrednio, określa, kto jest administratorem. Innymi słowy, prawo może nakładać na podmioty publiczne lub prywatne obowiązek przetwarzania określonych danych, a podmioty te uznawane są zazwyczaj za administratorów w odniesieniu do przetwarzania, które jest niezbędne do wykonania tego obowiązku. Jeżeli administrowanie nie wynika z przepisów prawnych, wówczas kwalifikacja strony jako administratora musi zostać ustalona na podstawie oceny okoliczności faktycznych związanych z przetwarzaniem. Żeby stwierdzić, czy dany podmiot ma decydujący wpływ na przetwarzanie danych osobowych, należy wziąć pod uwagę wszystkie istotne okoliczności faktyczne (pkt. 21–25 ww. Wytycznych).

Przykład sytuacji, w której administrowanie wynika z przepisów prawa, został opisany w odpowiedzi na pytanie dotyczące **określenia statusu inwestora inwestycji niedrogowej i zarządcy drogi**[380]. W celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, czy jednak istnieje konieczność zawarcia umowy powierzenia, należy przede wszystkim dokonać analizy okoliczności faktycznych z uwzględnieniem zadań podmiotów wynikających m.in. z przepisów prawa oraz zawartej między inwestorem inwestycji niedrogowej a zarządcą drogi umowy (na podstawie art. 16 ustawy o drogach publicznych[381]). Rozpatrując status zarówno inwestora inwestycji niedrogowej, jak i zarządcy drogi, należy przede wszystkim wziąć pod uwagę, czy dany podmiot samodzielnie decyduje o sposobach i celach przetwarzania, uwzględniając przy tym ustalony między nimi zakres obowiązków i odpowiedzialności oraz szczegóły wynikające z konkretnych postanowień umownych. Zgodnie z art. 16 ust. 1 ustawy o drogach publicznych, budowa lub przebudowa dróg publicznych spowodowana inwestycją niedrogową

[378] Dostępne pod linkiem https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_pl.
[379] https://archiwum.uodo.gov.pl/p/zadania-iod.
[380] DOL.502.183.2024.
[381] Ustawa z 21 marca 1985 r. o drogach publicznych (Dz.U. z 2024 r. poz. 320 ze zm.).

należy do inwestora tego przedsięwzięcia. Stosownie do art. 16 ust. 2 ustawy o drogach publicznych szczegółowe warunki budowy lub przebudowy dróg, o których mowa w ust. 1, określa umowa między zarządcą drogi a inwestorem inwestycji niedrogowej. W przypadku umowy między zarządcą drogi a inwestorem inwestycji niedrogowej inwestor realizuje własny cel inwestycyjny, a zarządca drogi wykonuje swoje obowiązki ustawowe. Nie ma zatem podstaw do tego, aby między tymi podmiotami mogła zostać zawarta umowa powierzenia przetwarzania danych. Zarządca drogi nie może bowiem działać w imieniu inwestora, bo zakres jego uprawnień określają przepisy prawa. Oba te podmioty są odrębnymi administratorami, gdyż realizują swoje cele oraz mają określone własne podstawy działania, wynikające z przepisów prawa. Sytuacja ta odnosi się zarówno do etapu związanego z przygotowaniem niezbędnej dokumentacji do wniosku o uzyskanie Zezwolenia na Realizację Inwestycji Drogowej (ZRID), jak i do dalszego etapu procedowania zawieranej między stronami umowy, o której mowa w art. 16 ust. 2 ustawy o drogach publicznych.

Innym przykładem dotyczącym wątpliwości co do statusu podmiotu było pytanie IOD o ustalenie, **kto jest administratorem w związku z kontrolą biletową w środkach komunikacji**[382]. Organ nadzorczy wskazał, że przetwarzanie danych osobowych pasażerów w związku z kontrolą biletową w środkach komunikacji reguluje art. 33a Prawa przewozowego[383]. Przepis ten stanowi, że przewoźnik lub osoba przez niego upoważniona, legitymując się identyfikatorem umieszczonym w widocznym miejscu, może dokonywać kontroli dokumentów przewozu osób lub bagażu (ust. 1). W razie stwierdzenia braku odpowiedniego dokumentu przewozu przewoźnik lub organizator publicznego transportu zbiorowego albo osoba przez niego upoważniona pobiera właściwą należność za przewóz i opłatę dodatkową albo wystawia wezwanie do zapłaty (ust. 3). W razie stwierdzenia braku ważnego dokumentu poświadczającego uprawnienie do bezpłatnego albo ulgowego przejazdu przewoźnik lub organizator publicznego transportu zbiorowego albo osoba przez niego upoważniona pobiera właściwą należność za przewóz i opłatę dodatkową, albo wystawia wezwanie do zapłaty. Pobrana należność za przewóz i opłata dodatkowa, po uiszczeniu opłaty manipulacyjnej odpowiadającej kosztom poniesionym przez przewoźnika lub organizatora publicznego transportu zbiorowego, podlegają zwrotowi, a w przypadku wezwania do zapłaty – umorzeniu, w przypadku udokumentowania przez podróżnego, nie później niż w terminie 7 dni od dnia przewozu, uprawnień do bezpłatnego lub ulgowego przejazdu (ust. 4).

Z powołanego przepisu art. 33a Prawa przewozowego wynika zatem, że uprawnieni do pozyskiwania i dalszego przetwarzania danych osobowych podróżnych są przewoźnik lub osoba przez niego upoważniona. Analiza treści tego przepisu prowadzi zatem do wniosku, że o ile przewoźnik powierzy wykonywanie czynności związanych z kontrolą biletową osobie trzeciej, to – w zakresie umocowania – działa ona każdorazowo na jego rzecz. Dotyczy to zwłaszcza pozyskiwania danych

[382] DOL.502.24.2024.
[383] Ustawa z 15 listopada 1984 r. – Prawo przewozowe (Dz.U. z 2020 r. poz. 8 ze zm.).

osobowych pasażerów podczas kontroli i dalszego ich przetwarzania w związku z dochodzeniem należności z tytułu opłat za przejazd bez ważnego biletu. Z takiego ukształtowania przez ustawodawcę relacji między przewoźnikiem a podmiotem, który zostaje przez niego upoważniony do prowadzenia kontroli biletowej, wynika zatem, że decyzje o celach i środkach przetwarzania danych osobowych pasażerów w każdym przypadku należą wyłącznie do przewoźnika. W konsekwencji status administratora danych pasażerów zawsze przysługiwać będzie przewoźnikowi. Z racji tego, że przepis art. 33a Prawa przewozowego ma charakter bezwzględnie obowiązujący, niedopuszczalne jest odmienne ukształtowanie ww. spraw w drodze umowy między przewoźnikiem a osobą trzecią. Stanowisko takie znajduje również odzwierciedlenie w orzecznictwie[384]. Nie jest zatem dopuszczalne zawarcie przez przewoźnika umowy, na podstawie której nastąpiłaby sukcesja prawna na rzecz firmy kontrolującej bilety, przewoźnik może bowiem jedynie upoważnić ją do działania w swoim imieniu. W konsekwencji wszelkie umowy między przewoźnikami a firmami kontrolującymi bilety muszą być rozumiane jako dotyczące powierzenia wykonywania czynności w imieniu przewoźnika. W opinii organu nadzorczego w zakresie dotyczącym przetwarzania danych osobowych pasażerów przepis art. 33a Prawa przewozowego daje podstawę do zawarcia między przewoźnikiem a firmą kontrolującą umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 28 RODO[385].

Inspektorzy sukcesywnie śledzą dorobek UODO i jego rozstrzygnięcia i często nawiązują w swoich pytaniach do prezentowanych przez organ stanowisk i rekomendacji. Na kanwie decyzji Prezesa UODO nakładającej na Burmistrza Aleksandrowa Kujawskiego karę m.in. za nieprzeprowadzenie analizy ryzyka związanego z korzystaniem z kanału YouTube w celu transmisji nagrań z obrad Rady Miasta[386], inspektor zwrócił się z pytaniem, **czy z serwisem YouTube należy zawrzeć umowę powierzenia**[387]. Inspektor zauważył, że w decyzji Prezesa UODO brak umowy powierzenia przetwarzania danych osobowych z serwisem YouTube nie był podstawą do nałożenia kary. W odpowiedzi Prezes UODO potwierdził, że w powołanej decyzji organ nadzorczy nie kwestionował braku umowy powierzenia z właścicielem kanału YouTube. Wyjaśnił natomiast, że kwestie podziału ról i odpowiedzialności za prowadzenie fanpage'a na portalu społecznościowym zostały omówione w orzeczeniach Trybunału Sprawiedliwości Unii Europejskiej (TSUE), zwłaszcza w dwóch sprawach: Wirtschaftsakademie (C-210/16) i Fashion ID (C-40/17). W orzeczeniach tych stwierdzono, że interakcja między portalem społecznościowym a właścicielem fanpage'a może prowadzić do powstania relacji współadministrowania (art. 26 RODO). W wyroku z 5 czerwca 2018 r. (C-210/16) TSUE określił rolę administratora fanpage'a na portalu społecznościowym Facebook, wskazując, że jest on administratorem, w rozumieniu przepisów o ochronie danych osobowych, danych

[384] Np. postanowienie Sądu Najwyższego z 23 października 2003 r., sygn. akt IV KK 265/02.
[385] Identyczne stanowisko było prezentowane wielokrotnie przez organ ochrony danych osobowych w decyzjach jeszcze przed obowiązywaniem RODO (np. decyzja GI-DEC-DS.-35/04, czy GI-DEC-DS.-42/05, dostępne na stronie internetowej www.archiwum.giodo.gov.pl).
[386] ZSPU.421.3.2019.
[387] DOL.502.112.2024.

osób odwiedzających fanpage. Dodatkowo w ocenie TSUE przyjęcie szerokiej definicji „administratora" ma służyć skutecznej i pełnej ochronie osób, których dane dotyczą (wyrok z 13 maja 2014 r., Google Spain i Google, C-131/12, EU:C:2014:317, pkt 34). Ponadto zarówno na gruncie dyrektywy 95/46, jak i RODO, pojęcie administratora nie odsyła każdorazowo do pojedynczego podmiotu i może dotyczyć kilku podmiotów uczestniczących w przetwarzaniu. A zatem z właścicielem serwisu portalu YouTube nie należy zawierać umowy powierzenia. Co istotne, NSA, który podtrzymał decyzję Prezesa UODO[388], wskazał, że administrator – oceniając procesy przetwarzania danych osobowych i przekazując informacje za pośrednictwem serwisów będących własnością innych administratorów – musi pamiętać o konieczności dokonania oceny związanych z tym ryzyk, ale przede wszystkim oceny ról podmiotów występujących w tych procesach, czyli przeprowadzenia wnikliwej analizy ryzyka. Analiza ryzyka może pozwolić administratorowi upewnić się, czy dane z tego serwisu można odzyskać, czy w każdej sytuacji istnieje możliwość zrealizowania prawa osób do dostępu do danych, czy nie należy mieć kopii nagrań w innych miejscach, czy też jakie kategorie danych są w tym miejscu przetwarzane i zastosować odpowiednie środki ochrony, jak np. anonimizacja danych. Przeprowadzenie takiej analizy ryzyka, a także posiadanie odpowiednich polityk związanych z procesami przetwarzania danych pozwala administratorom realizować zasadę rozliczalności, określoną w RODO. Mogą oni wówczas łatwo wykazać, że przetwarzanie danych odbywa się zgodnie z prawem, zasadą celowości, zasadą ograniczenia czasu przetwarzania i zasadą poufności oraz integralności danych.

Ad 3. Weryfikacja podmiotu przetwarzającego i umowy powierzenia

Organ nadzorczy w wydanych decyzjach wielokrotnie podkreślał, że niezwykle istotna jest weryfikacja kompetencji podmiotu przetwarzającego. Obowiązkiem administratora korzystającego z usług podmiotów przetwarzających jest upewnienie się, czy zapewniają one wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Administrator jest zatem odpowiedzialny za ocenę adekwatności gwarancji udzielonych przez podmiot przetwarzający i powinien być w stanie udowodnić, że poważnie wziął pod uwagę wszystkie elementy przewidziane w RODO. Samo podpisanie umowy powierzenia przetwarzania danych osobowych bez dokonania właściwej oceny podmiotu przetwarzającego nie może być uznane za realizację obowiązku przeprowadzenia postępowania weryfikującego podmiot przetwarzający.

Zagadnienie to zostało poruszone w pytaniu IOD, który miał wątpliwość, **czy gotowe wzorce umowy powierzenia przedstawiane przez dostawcę skrzynki elektronicznej w ramach usług oferowanych przez Google, zapewniają zgodność umowy powierzenia z art. 28 RODO**[389]. W odpowiedzi na to pytanie organ nadzorczy przypomniał, że jeśli chodzi o przekazywanie danych do USA (jako państwa trzeciego),

[388] Wyrok NSA z 28 lutego 2024 r. sygn. akt. II OSK 3839/21.
[389] DOL.502.98.2024.

to Komisja Europejska przyjęła decyzję wykonawczą stwierdzającą odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA [Ramy ochrony danych UE–USA" (DPF)][390]. Decyzja ta, zwana nową „Tarczą Prywatności", nie przesądza jednak o zgodności usług Office 365 oferowanych przez Microsoft. Drugą płaszczyzną analizy i oceny zgodności z prawem korzystania przez administratora z usług skrzynki elektronicznej, powinny być wymogi z art. 28 RODO. Każdy administrator zobowiązany jest zapewnić, że podmiot przetwarzający, z usług którego korzysta, daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. O odpowiednie zabezpieczenie spełnienia powyższego wymogu podmiot powinien zadbać w umowie powierzenia bądź w innym instrumencie prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą (art. 28 ust. 3 RODO). Powstałe w czasie analizy wątpliwości co do zgodności usług z powyższymi wymogami należy rozstrzygać na podstawie konkretnych warunków i informacji na temat danej usługi. Administrator ma zatem obowiązek dokonać analizy, czy powierzenie będzie spełniało wymogi z art. 28 RODO, ale także czy spełnione zostaną warunki zgodnego z prawem transferu danych do USA. Przydatne w ocenie może być stanowisko EIOD dotyczące prowadzonego przez ten organ dochodzenia w sprawie wykorzystania przez instytucje Unii Europejskiej produktów i usług Microsoft. W stanowisku tym jest mowa o Microsoft jako podmiocie przetwarzającym[391].

Istotnym problem zgłaszanym w pytaniach IOD były zagadnienia dotyczące praktyk firm hostingowych, które przyjmują we wzorach umów powierzenia nieprawidłowe zapisy umowne dotyczące zwolnienia podmiotu przetwarzającego z odpowiedzialności za ewentualne roszczenia podmiotu danych wytoczone podmiotowi przetwarzającemu w związku z wykonaniem umowy[392]. Prezes UODO wskazał, że art. 79 RODO gwarantuje osobie fizycznej prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu. Z kolei art. 82 RODO rozciąga odpowiedzialność odszkodowawczą również na podmiot przetwarzający oraz wprowadza w tym zakresie odpowiedzialność solidarną, określając jednocześnie możliwość wysuwania roszczeń regresowych oraz wskazując właściwość sądu. Regulacja ta ma charakter cywilnoprawny i stanowi samodzielną podstawę roszczeń odszkodowawczych. Zgodnie z art. 82 ust. 2 RODO każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym rozporządzenie, natomiast podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy

[390] Więcej informacji na ten temat znajduje się pod tym linkiem: https://uodo.gov.pl/pl/526/3247.
[391] Więcej na ten temat w Biuletynie UODO nr 04/04/24.
[392] DOL.502.92.2024.

nie dopełnił obowiązków, które rozporządzenie nakłada bezpośrednio na podmioty przetwarzające lub gdy działał poza zgodnymi z prawem poleceniami administratora lub wbrew tym poleceniom. Zakres odpowiedzialności jest ściśle powiązany z zakresem obowiązków nałożonych na administratora i podmiot przetwarzający. Na podmiocie przetwarzającym dane (na zlecenie administratora) spoczywają ogólny obowiązek przetwarzania danych zgodnie z umową zawartą z administratorem oraz inne obowiązki szczególne, jakie rozporządzenie nakłada na podmioty przetwarzające (np. przewidziany w art. 32 obowiązek należytego zabezpieczenia przetwarzanych danych; wynikający z art. 33 ust. 2 obowiązek zawiadomienia administratora o naruszeniu ochrony danych czy też przewidziany w art. 37 ust. 1 obowiązek wyznaczenia inspektora ochrony danych, jak również obowiązki związane z przekazywaniem danych do państw trzecich i organizacji międzynarodowych, określone w art. 45 i in.). Przepis ust. 4 komentowanego artykułu reguluje solidarną odpowiedzialność podmiotów za wyrządzoną szkodę. Odpowiedzialności solidarnej podlegają administratorzy i podmioty przetwarzające, ponoszący winę za zdarzenia, które doprowadziły do powstania szkody spowodowanej przetwarzaniem naruszającym rozporządzenie, natomiast od tej odpowiedzialności mogą zwolnić się administratorzy i podmioty przetwarzające, jeżeli udowodnią, że w żaden sposób nie ponoszą winy. W motywie 146 zwrócono uwagę na to, że jeżeli administratorzy lub podmioty przetwarzające uczestniczą w tym samym przetwarzaniu, każdy administrator lub podmiot przetwarzający powinien odpowiadać prawnie za całość szkody. Jeżeli jednak zostaną włączeni do jednego postępowania sądowego zgodnie z prawem państwa członkowskiego, odszkodowaniem można obarczyć każdego z administratorów i każdy z podmiotów przetwarzających stosownie do ich winy za szkodę wynikłą z przetwarzania, o ile osobie, której dane dotyczą, zapewnione zostanie pełne i skuteczne odszkodowanie za poniesioną szkodę[393]. Art. 82 ust. 5 RODO przewiduje możliwość roszczeń regresowych w związku z odpowiedzialnością solidarną i zapłatą odszkodowania przez jeden z podmiotów. Jak stanowi art. 92 ustawy z 10 maja 2018 r. o ochronie danych osobowych w zakresie nieuregulowanym w RODO, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 RODO, stosuje się przepisy Kodeksu cywilnego. Zatem jakiekolwiek inne postanowienia umowy powierzenia, które w istocie ograniczały ww. prawa administratora, należałoby uznać za niezgodne z RODO. Dodatkowo zgodnie z art. 28 ust. 1 RODO w ramach powierzenia przetwarzania danych, tj. przetwarzania w imieniu administratora przez inny podmiot, administrator może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Takie brzmienie przepisów RODO

[393] P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022, art. 82.

wskazuje na to, że administrator powinien dokonać uprzedniego zbadania, czy podmiot przetwarzający spełnia wymogi określone w art. 28 ust. 1 RODO. Również motyw 81 RODO stanowi, że administrator powinien korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania. Jak wskazuje EROD w Wytycznych 07/2020, nie należy uznawać braku równowagi w uprawnieniach umownych małego administratora w odniesieniu do dużych dostawców usług za uzasadnienie dla akceptowania przez administratora klauzul i warunków umów, które nie są zgodne z przepisami o ochronie danych, ani nie może zwalniać administratora z obowiązków w zakresie ochrony danych. Administrator musi ocenić te warunki i o ile dobrowolnie je akceptuje i korzysta z usługi, przyjmuje również pełną odpowiedzialność za zgodność z RODO. A zatem – jak wskazał Prezes UODO – administrator powinien zabiegać o przestrzeganie przepisów prawa, szczególnie tych dotyczących obowiązków podmiotu przetwarzającego. Powinien podejmować działania w celu zabezpieczenia przestrzegania tych przepisów na etapie zawierania lub renegocjowania umów powierzenia, a w przypadku trudności – rozważyć podjęcie działań w porozumieniu z innymi administratorami (usługobiorcami) w celu zmiany niewłaściwej praktyki dostawcy.

Ad 4. Udostępnianie danych osobowych

W wielu pytaniach od inspektorów pojawiały się kwestie dotyczące udostępniania danych osobowych. Wątpliwości inspektorów dotyczyły dopuszczalności publicznego udostępnienia określonego zakresu danych osobowych, a także podstawy udostępnienia.

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 występuje o ich udostępnienie. Administrator ponosi odpowiedzialność za wykazanie właściwej staranności w zapewnieniu, aby dane nie były udostępniane bez podstawy prawnej, a jeśli podejmie decyzje o ich udostępnieniu, wówczas powinien zadbać, aby zakres udostępnianych danych był adekwatny do celu udostępniania (zgodnie z zasadą minimalizacji, o której mowa w art. 5 ust. 1 lit. c RODO).

W związku z przepisami ustawy z 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości[394], które dopuszczają zawiadamianie o wygaśnięciu decyzji o rejestracji pojazdu poprzez publiczne

[394] Dz. U. poz. 1394.

obwieszczenie, jeden z IOD zgłosił wątpliwości, **czy w takim obwieszczeniu można podać numery rejestracyjne pojazdów kwalifikujących się do wygaszenia rejestracji**[395]. Na podstawie odpowiedzi udzielonej na to pytanie inspektora przygotowany został materiał zamieszczony w Biuletynie UODO nr 04/04/24. Prezes UODO, odwołując się do definicji danych osobowych zawartej w przepisach RODO, wskazał, że numery tablic rejestracyjnych są informacją, za pośrednictwem której możliwe jest zidentyfikowanie – w sposób pośredni – osoby fizycznej będącej właścicielem pojazdu. Zgodnie z definicją danych osobowych zawartą w RODO każdy identyfikator urządzenia, na przykład numery: VIN, bloku silnika pojazdu lub smartfonu, będą stanowiły dane osobowe, o ile będą one umożliwiały identyfikację posiadacza tak oznaczonego urządzenia. Numery rejestracyjne, którymi właściciele dysponują przez cały czas posiadania pojazdu, mogą pozwolić na identyfikację konkretnych osób nie tylko odpowiednim organom, ale również osobom fizycznym, np. sąsiadom, znajomym, współpracownikom. Są oni w stanie powiązać numer rejestracyjny pojazdu z konkretną osobą. Ponadto inne osoby także mogą na podstawie numeru rejestracyjnego zidentyfikować właściciela pojazdu, składając odpowiednio uzasadniony wniosek do Centralnej Ewidencji Pojazdów i Kierowców.

Biorąc pod uwagę powyższe, organ nadzorczy stoi na stanowisku, że numery rejestracyjne pojazdów stanowią dane osobowe, o ile umożliwiają identyfikację posiadacza pojazdu[396]. Warto jednak dodać, że stanowisko polskiego organu nadzorczego jest zbieżne ze stanowiskiem wielu innych organów ochrony danych w innych krajach, jak np. w Niemczech czy we Włoszech. Także orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, a także sądów w innych krajach, jak choćby w Niemczech, uznaje jednoznacznie numery rejestracyjne pojazdów za dane osobowe. Trzeba dodać, że ostatnio Trybunał Sprawiedliwości Unii Europejskiej orzekł, że nr VIN pojazdu posiada status danej osobowej, jeśli może być użyty do identyfikacji właściciela pojazdu lub innej osoby[397].

Należy jednak pamiętać, że zgodnie z motywem 5 RODO, prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności.

Organy władzy publicznej są zobowiązane działać w granicach i na podstawie obowiązujących przepisów prawa regulujących ich działalność. Zgodnie z art. 6 ust. 1 RODO przetwarzanie danych (w tym ich udostępnianie) jest zgodne z prawem, m.in. wtedy, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (lit. c).

W przedstawionej przez IOD sprawie istnieje ustawowy obowiązek właściwego organu administracyjnego (starosty) zawiadomienia właściciela pojazdu o wygaśnięciu

[395] DOL.502.46.2024.
[396] Stanowisko to znajduje także odzwierciedlenie w orzecznictwie sądów, np. w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 13 kwietnia 2017 r. (sygn. akt VII SA/Wa 1069/16) czy w wyroku WSA z 25 kwietnia 2014 r. (sygn. akt II SA/Wa 30/14), choć ostatnio wydane zostały odmienne orzeczenia w tej kwestii (np. wyrok NSA z 28 czerwca 2019 r. sygn. akt I OSK 2063/17).
[397] Wyrok TSUE z 9 listopada 2023 r. w sprawie C-319/22.

decyzji o rejestracji pojazdu. Zgodnie z art. 17 ust. 1 ustawy o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości, decyzje o rejestracji pojazdu wydane przed 14 marca 2005 r. dotyczące pojazdów nieposiadających ważnego okresowego badania technicznego, w stosunku do których ich posiadacze nie dopełnili obowiązku zawarcia umowy obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych, jeżeli pojazd im podlega, przez okres dłuższy niż 10 lat, przypadający bezpośrednio przed dniem wejścia w życie niniejszej ustawy, wygasają z dniem 10 czerwca 2024 r. Takie zawiadomienie o wygaśnięciu decyzji może odbywać się przez publiczne obwieszczenie (art. 17 ust. 3). Przepisy te nie wskazują jednak, jaka miałaby być treść takiego publicznego obwieszczenia; podobnie jak przepisy Kodeksu postępowania administracyjnego. Te ostatnie określają, że 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 Biuletynie Informacji Publicznej na stronie podmiotowej właściwego organu administracji publicznej (art. 49 ust. 1). Dzień, w którym nastąpiło publiczne obwieszczenie, inne publiczne ogłoszenie lub udostępnienie pisma w Biuletynie Informacji Publicznej wskazuje się w treści tego obwieszczenia, ogłoszenia lub w Biuletynie Informacji Publicznej. Zawiadomienie uważa się za dokonane po upływie czternastu dni od dnia, w którym nastąpiło publiczne obwieszczenie, inne publiczne ogłoszenie lub udostępnienie pisma w Biuletynie Informacji Publicznej (art. 49 ust. 2).

Podkreślić jednak należy, że celem publicznego obwieszczenia, które jest fakultatywne, jest zapewnienie szybkiego skutku doręczenia decyzji adresatowi (tak też mówi wyrok Naczelnego Sądu Administracyjnego z 1 lutego 2023 r., sygn. akt III OSK 1825/21).

W sytuacji braku przepisów regulujących dane zagadnienie (tu zakres danych w obwieszczeniu publicznym) zastosowanie znajdują ogólne zasady z art. 5 RODO. Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”). Niezbędne jest również, w świetle zasady celowości (art. 5 ust. 1 lit. b RODO) i ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO), określenie, jak długo te obwieszczenia publiczne muszą być publikowane w BIP. W przypadkach, w których prawo nie reguluje okresu retencji danych, administrator, po przeprowadzeniu odpowiednich analiz, powinien określić ten okres tak, aby przetwarzanie danych było zgodne z celami, w których je pozyskano[398].

[398] Zasadność tego stanowiska została potwierdzona w orzecznictwie sądów administracyjnych – wyrok Wojewódzkiego Sądu Administracyjnego w Lublinie z 1 marca 2016 r. (sygn. akt II SA/Lu 876/15): „[z] art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych wynika zasada ograniczenia czasowego udostępnienia danych osobowych w Biuletynie Informacji Publicznej. Zasada ta oznacza, że nawet jeśli określone dane odpowiadają celowi, dla którego są zbierane, to nie powinny być przetwarzane, w tym udostępniane innym podmiotom *ad finitum.* Czasowym wyznacznikiem powinno być natomiast osiągnięcie celu przetwarzania”. Wyrok ten zachowuje aktualność także przy obecnie obowiązujących przepisach o ochronie danych osobowych.

Podsumowując, organ wskazał, że to administrator (starosta) powinien dokonać oceny, czy w myśl zasady proporcjonalności, minimalizacji i ograniczenia czasowego publikacja numeru rejestracyjnego pojazdu w publicznym ogłoszeniu jest niezbędna do wykonania obowiązku wynikającego z art. 17 ust. 3 ustawy o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości. Dokonując takiej oceny, należy wziąć pod uwagę, że o ile numer rejestracyjny pojazdu może identyfikować osobę fizyczną, to już imię i nazwisko oraz adres zamieszkania dokonuje wprost takiej identyfikacji. Dlatego można uznać, że publikacja numeru rejestracyjnego pojazdu jest daną osobową mniej ingerującą w prywatność osoby fizycznej, niż publikacja np. jej imienia, nazwiska czy adresu zamieszkania.

Kolejne z pytań od IOD dotyczyło **podstawy udostępnienia przez placówkę ochrony zdrowia dokumentacji medycznej pacjenta ubezpieczycielowi w związku z zawartą elektroniczną polisą**[399], zwłaszcza zaś tego, czy podmiot ochrony zdrowia może udostępniać dane wrażliwe pacjentów na podstawie art. 77(2) i 77(3) Kodeksu cywilnego. Odnosząc się do wskazanych w pytaniu wątpliwości, organ przypomniał, że kwestie udostępniania dokumentacji medycznej oraz informacji dotyczących zdrowia na rzecz zakładów ubezpieczeń regulują przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[400] oraz ustawa o działalności ubezpieczeniowej i reasekuracyjnej[401]. W aktach tych określone zostały zasady, w tym podstawy, na jakich takie dokumenty i dane mogą być udostępniane. Wobec tego administrator przed udostępnieniem takich informacji powinien ustalić, czy spełnione są warunki określone w tych regulacjach. Jednocześnie Prezes UODO zauważył, że wskazane przepisy Kodeksu cywilnego nie mogą stanowić same w sobie podstawy do przetwarzania (w tym udostępniania) danych osobowych pacjentów w rozumieniu art. 6 i art. 9 RODO. Odnoszą się one bowiem jedynie do jednej z form czynności prawnej – do formy dokumentowej. Wobec tego należy przede wszystkim ustalić, na podstawie jakich przepisów prawa zakład ubezpieczeń zwraca się do administratora o udostępnienie dokumentacji medycznej, a następnie czy przepisy te nie wymagają spełnienia dodatkowych warunków dotyczących, np. formy oświadczenia czy czynności prawnej, a jeśli tak, to jakich. Jeżeli jednak wniosek o udostępnienie danych osobowych budzi wątpliwości (nie zawiera uzasadnienia prawnego lub faktycznego), dobrym rozwiązaniem jest zwrócenie się do wnioskodawcy z prośbą o ich wyjaśnienie. Dokładne zbadanie celu i podstawy prawnej wystąpienia z wnioskiem jest niezbędne dla oceny dopuszczalności udostępnienia danych. W przypadku stwierdzenia braku podstawy prawnej do udostępnienia danych osobowych administrator nie powinien takich danych udostępnić.

W 2024 r. analizie poddane zostały także przepisy ustawy – Prawo o ruchu drogowym[402] (art. 73aa, art. 78 ust. 2 pkt 1, art. 140mb), które zobowiązują właścicieli

[399] DOL.502.200.2024.
[400] Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2024 r. poz. 581).
[401] Ustawa z 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2024 r. poz. 838 ze zm.).
[402] Ustawa z 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. z 2024 r. poz. 1251).

pojazdów do złożenia odpowiednio wniosku o ich rejestrację po nabyciu lub zawiadomienia o zbyciu pojazdu. Za niedopełnienie tego obowiązku przewidziane są kary pieniężne nakładane w drodze decyzji administracyjnej. Jednak zgodnie z art. 107 § 1 k.p.a. oraz stanowiskiem UODO[403] decyzje te nie zawierają numeru PESEL karanego. Gdy właściciel pojazdu nie zapłaci nałożonej kary, starosta wszczyna postępowanie egzekucyjne. Jednak stosownie do art. 27 ustawy z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, w tytule wykonawczym wierzyciel (w tym przypadku starosta) musi podać m.in. numer PESEL dłużnika.

W tej sytuacji IOD jednego ze starostw nabrał wątpliwości, **jaka jest podstawa prawna pozyskiwania numeru PESEL dłużnika w celu wystawienia tytułu egzekucyjnego od poszczególnych jednostek organizacyjnych funkcjonujących u administratora**. Czy wydział komunikacji, który przetwarza numer PESEL danej osoby w związku z realizacją zadań określonych w Prawie o ruchu drogowym, może udostępnić go wydziałowi finansowemu w celu wystawienia tytułu wykonawczego?[404] Na podstawie odpowiedzi udzielonej na to pytanie inspektora przygotowany został materiał zamieszczony w Biuletynie UODO nr 10/10/24. Wskazano w nim, że organy administracji publicznej są zobowiązane działać w granicach i na podstawie obowiązujących przepisów prawa regulujących ich funkcjonowanie. Zgodnie zaś z art. 6 ust. 1 RODO przetwarzanie danych (w tym ich udostępnianie) jest zgodne z prawem m.in. wtedy, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (lit. c).

Przepisy ustawy – Prawo o ruchu drogowym (art. 73 i nast.) stanowią, że w sprawie rejestracji pojazdów właściwym organem jest starosta, który na te potrzeby przetwarza dane osobowe ich właścicieli. Wyraźnie wskazują też (art. 80b), jakie dane osobowe są gromadzone w ewidencji pojazdów, wymieniając wśród nich m.in. numer PESEL właściciela czy posiadacza pojazdu. Ponadto określają, jakie podmioty i w jakim zakresie wprowadzają dane do ewidencji (art. 80ba) oraz jakie podmioty mają dostęp do tych danych (art. 80bb), a także komu i w jakim zakresie można je udostępnić (art. 80c). Zgodnie z art. 80c ust. 1 dane zgromadzone w ewidencji udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, m.in. organom właściwym w sprawach rejestracji pojazdów czy administracyjnym organom egzekucyjnym oraz organom podatkowym. Jeśli zaś starosta występuje w roli organu egzekucyjnego, to istnieje podstawa prawna do pozyskania numeru PESEL z ewidencji pojazdów.

Niewykonanie zobowiązania wynikającego z decyzji administracyjnej, tj. niezapłacenie kary, rozpoczyna bieg nowej procedury, zgodnie z przepisami o egzekucji administracyjnej. Stosownie do art. 27 § 1 pkt 2 ustawy o postępowaniu egzekucyjnym w administracji tytuł wykonawczy powinien zawierać m.in. wskazanie

[403] Stanowisko UODO zawarte m.in. w decyzji ZSPU.440.379.2018. (https://uodo.gov.pl/decyzje/ZSPU.440.379.2018) oraz wyrażone w materiale „Czy rozsyłanie »rozdzielników« do uczestników postępowań administracyjnych nie narusza przepisów ustawy o ochronie danych osobowych?" (Biuletyn UODO – Numer specjalny).
[404] DOL.502.132.2024.

imienia, nazwiska lub firmy zobowiązanego i jego adresu, a także NIP-u lub numeru PESEL, jeżeli zobowiązany taki numer posiada. Przepis ten jest przesłanką legalizującą proces przetwarzania danych osobowych w odniesieniu do danych zawartych w wystawionym tytule wykonawczym. Konieczność przetwarzania numeru PESEL w tytule wykonawczym przez organ egzekucyjny (np. starostę) wynikająca z ww. przepisu prawa spełnia jednocześnie przesłankę z art. 6 ust. 1 lit. c RODO.

Także przepisy ustawy z 24 września 2010 r. o ewidencji ludności[405] wskazują, jakim organom i na jakich zasadach oraz w jakim celu można udostępnić dane z rejestru PESEL (art. 46) oraz określają zasady udostępniania danych w drodze teletransmisji danych (art. 48, art. 49). Stanowią (art. 46 ust. 1), że dane z rejestru PESEL oraz rejestrów mieszkańców w zakresie niezbędnym do realizacji ich ustawowych zadań udostępnia się m.in. organom administracji publicznej, sądom i prokuraturze (pkt 1).

Skoro zatem starosta, jako administrator ma prawo przetwarzać numer PESEL w ramach swoich ustawowych zadań wykonywanych jako organ egzekucyjny wobec administracyjnych kar pieniężnych, to kwestia przekazywania danych pomiędzy wydziałami tego administratora nie powinna być rozpatrywana w kategoriach udostępniania danych. Mamy bowiem cały czas do czynienia z przetwarzaniem danych w ramach struktury organizacyjnej jednego administratora.

Ad 5. Stosowanie monitoringu wizyjnego

Monitoring jest zagadnieniem, które – w pytaniach i innych sygnałach od inspektorów ochrony danych – pojawia się w każdym okresie sprawozdawczym. Jednocześnie jest on od dawna przedmiotem szczególnego zainteresowania organu nadzorczego. Niewątpliwie zastosowanie tej technologii jest inwazyjną formą ingerencji w prywatność osób fizycznych i z tego względu powinno mieć miejsce wyłącznie po spełnieniu określonych warunków. Często uzasadnieniem potrzeby zainstalowania monitoringu jest ochrona mienia, ale jak wskazywał organ nadzorczy, administrator powinien w pierwszej kolejności ocenić adekwatność wprowadzenia monitoringu wizyjnego jako metody zapewnienia ochrony mienia i ustalić, czy nie ma innych środków, których zastosowanie mniej ingerowałoby w prywatność osób, których dane dotyczą.

Tego rodzaju wątpliwości zawarł w swoim pytaniu IOD, który zastanawiał się, **czy zainstalowanie monitoringu w szkolnych pomieszczeniach sanitarno-higienicznych jest legalne**[406]. IOD wskazał, że w celu zapobiegania powtarzającym się aktom wandalizmu dyrekcja szkoły planuje zainstalować kamerę pokazującą tylko, kto wchodzi do toalety o danej porze, bez wizji na elementy toalety, co naruszałoby prawa uczniów. W odpowiedzi na te wątpliwości Prezes UODO przypomniał, że zgodnie z art. 108a ust. 3 Prawa oświatowego, monitoring w pomieszczeniach sanitarno-higienicznych może być zainstalowany tylko w wyjątkowych przypadkach, gdy jest to niezbędne do osiągnięcia celów wskazanych w ust. 1 ww. przepisu

[405] Ustawa z 24 września 2010 r. o ewidencji ludności (Dz.U. z 2025 r. poz. 274).
[406] DOL.502.172.2024.

(tj. monitoring jest niezbędny do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia) oraz w taki sposób, że nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób. W pytaniu nie przedstawiono szczegółów planowanego rozwiązania, ale nasunęły się wątpliwości, jak ma ono spełniać warunki z art. 108a ust. 3 Prawa oświatowego, zwłaszcza w zakresie zastosowania technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób, skoro kamera ma rejestrować, kto wchodzi do toalety o określonej porze. Nie jest też wiadome, w jaki sposób rozwiązanie to ma być skuteczne w walce z wandalizmem.

Ad 6. Przetwarzanie danych osobowych w związku z zatrudnieniem

Wiele pytań przesyłanych przez IOD dotyczyło zagadnień związanych zatrudnieniem. Organ nadzorczy podkreślał, że administrator będący pracodawcą musi zapewnić, aby jego działania, w tym przetwarzanie danych osobowych zarówno pracowników, jak i kandydatów do pracy, były zgodne nie tylko z przepisami RODO, ale również z przepisami Kodeksu pracy[407]. Przepisy Kodeksu pracy wskazują bowiem, jakie konkretnie dane można pozyskiwać od osoby ubiegającej się o zatrudnienie, regulują również kwestie pozyskiwania danych osobowych na podstawie zgody od osoby ubiegającej się o zatrudnienie lub pracownika. Odnosząc się natomiast do okresu retencji danych, przywoływał zasadę ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO).

Do tej grupy zagadnień odnosiło się pytanie IOD dotyczące **legalności przetwarzania przez pracodawcę numeru prywatnego telefonu pracownika na podstawie wyrażonej przez niego zgody, w związku z realizacją celów służbowych** (niezbędny kontakt z pracodawcą podczas wykonywania pracy zdalnej lub okazjonalnej pracy zdalnej)[408]. Prezes UODO w odpowiedzi odwołał się do definicji zgody określonej w art. 4 pkt 11 RODO. Przywołał również Wytyczne EROD 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679[409], w których wskazano, że zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody przewidziane w RODO. Jednym z tych wymogów jest zagwarantowanie, aby zgoda była dobrowolna. Co do zasady RODO stanowi, że jeżeli osobie, której dane dotyczą, nie przysługuje rzeczywista możliwość wyboru, czuje się ona zmuszona do wyrażenia zgody lub poniesie negatywne konsekwencje w przypadku jej niewyrażenia, zgoda będzie nieważna (Wytyczne str. 7).

Odnosząc się zaś do kwestii zgody udzielanej przez pracownika, EROD wskazała, że biorąc pod uwagę zależność charakteryzującą stosunek między pracodawcą a pracownikiem, nie jest prawdopodobne, by osoba, której dane dotyczą,

[407] Ustawa z 26 czerwca 1974 r. – Kodeks pracy (Dz.U. z 2025 r. poz. 277).
[408] DOL.502.220.2024.
[409] Dostępne pod linkiem: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl.

mogła odmówić pracodawcy zgody na przetwarzanie danych, nie doświadczając obaw lub faktycznego ryzyka poniesienia niekorzystnych konsekwencji w wyniku odmowy. Nie jest prawdopodobne, by pracownik mógł swobodnie odpowiedzieć na wniosek pracodawcy o wyrażenie zgody na przykład na uruchomienie systemów monitorowania, takich jak nadzór kamer w miejscu pracy lub wypełnienie formularzy oceny, nie odczuwając żadnej presji. EROD uznaje zatem, że w przypadku pracodawców problematyczne jest przetwarzanie danych osobowych obecnych lub przyszłych pracowników na podstawie ich zgody, ponieważ jest mało prawdopodobne, by została ona wyrażona dobrowolnie. W odniesieniu do większości przypadków przetwarzania danych w miejscu pracy zgodną z prawem podstawą nie może i nie powinna być zgoda pracowników (art. 6 ust. 1 lit. a) ze względu na charakter stosunków między pracodawcą a pracownikiem.

W ocenie EROD nie oznacza to jednak, że pracodawcy nigdy nie mogą powoływać się na zgodę jako zgodną z prawem podstawę przetwarzania danych. Mogą się zdarzyć sytuacje, w których pracodawca ma możliwość wykazania, że zgody faktycznie udzielono dobrowolnie. Biorąc pod uwagę brak równowagi sił między pracodawcą a pracownikami, pracownicy mogą wyrazić dobrowolną zgodę wyłącznie w wyjątkowych okolicznościach, w których fakt wyrażenia lub niewyrażenia przez nich zgody nie pociąga za sobą żadnych negatywnych konsekwencji[410].

Organ zauważył, że w przedstawionym przez IOD przypadku przepisy Kodeksu pracy regulujące wykonywanie pracy zdalnej nie przewidują uprawnienia pracodawcy do żądania od pracowników udostępnienia prywatnego numeru telefonu. W takiej sytuacji pracodawca, aby móc przetwarzać w celach służbowych numer prywatnego telefonu komórkowego pracownika, musi uzyskać na to jego zgodę spełniającą warunki z RODO (m.in. zgoda musi być dobrowolna i odwoływalna), a także wymogi z Kodeksu pracy, tj. brak zgody lub jej wycofanie nie może być podstawą niekorzystnego traktowania pracownika, a także nie może powodować wobec niego żadnych negatywnych konsekwencji. Należy z tego wnioskować, że brak zgody na przetwarzanie prywatnego numeru telefonu nie może skutkować brakiem możliwości korzystania z pracy zdalnej.

W 2024 r. Prezes UODO odniósł się również do zagadnienia dotyczącego **okresu przechowywania przez pracodawcę danych osobowych występujących w orzeczeniach o niepełnosprawności** przekazywanych mu dobrowolnie przez pracowników chcących korzystać z uprawnień dla osób z niepełnosprawnością (np. dodatkowe urlopy, skrócony dzień pracy itp.) [411]. Wątpliwości inspektora wynikały m.in. z tego, że część orzeczeń o niepełnosprawności jest orzeczeniami terminowymi (np. wydanymi na 5 lat). Po upływie okresu ich ważności pracownicy dostarczają nowe orzeczenia. W tej sytuacji co do zasady cel, dla którego stare orzeczenie było przetwarzane (dodatkowe uprawnienia pracownika), ustał i należałoby usunąć lub

[410] Wskazówki dotyczące tego zagadnienia w kontekście przepisów Kodeksu pracy zawarte są w materiale UODO pt. „Czy pracodawca może korzystać z prywatnych danych kontaktowych do pracownika?" (https://archiwum.uodo.gov.pl/pl/138/1636).
[411] DOL.502.87.2024.

zanonimizować dane osobowe zawarte w poprzednim orzeczeniu. IOD pytał, co będzie w przypadku kontroli np. Państwowej Inspekcji Pracy. Inspektorzy pracy mogą bowiem chcieć skontrolować akta pracownicze (które są przechowywane 50 lub 10 lat w zależności od daty zatrudnienia pracownika) i podstawę np. udzielania pracownikowi dodatkowego urlopu na podstawie orzeczenia, którego termin, na który zostało wydane, już upłynął. Odpowiedź na pytanie IOD została zamieszona w Biuletynie UODO nr 06/06/24. Wskazano tam, że do przechowywania przez pracodawcę danych osobowych występujących w orzeczeniach o niepełnosprawności odnoszą się właściwe przepisy prawa, tj. przepisy ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych[412]. Zgodnie z art. 2b ust. 7 tej ustawy pracodawcy, podmioty i osoby realizujące zadania wynikające z ustawy przechowują dane osobowe wyłącznie przez okres nie dłuższy, niż jest to niezbędne i w zakresie koniecznym do realizacji celów przetwarzania danych osobowych oraz dokonują przeglądu przydatności przetwarzania danych osobowych nie rzadziej niż co 5 lat. Wynika z tego, że nie ma sztywnego, ustalonego odgórnie okresu przetwarzania ww. danych, a jedynie zostało wskazane, że okres ten powinien być determinowany celem, w jakim dane osobowe są konieczne do ich przetwarzania. Przepis ten stanowi zatem dla administratora wskazówkę, którą ten ma się kierować w przypadku dokonywania oceny (przynajmniej raz na 5 lat), czy przetwarzanie danych osobowych o niepełnosprawności jest nadal konieczne (niezbędne) dla określonych i uzasadnionych celów.

Jeśli zatem uzasadnionym celem administratora będzie konieczność udokumentowania dodatkowych uprawnień pracownika wynikających z niepełnosprawności (np. w przypadku kontroli z PIP), to administrator powinien to wykazać w swoim raporcie z przeprowadzonego przeglądu przydatności przetwarzania danych, o którym mowa w ww. przepisie ustawy. Przy czym należy uwzględnić także przepisy prawa, na podstawie których taka kontrola może być przeprowadzona, w tym okres, w jakim może się ona odbywać. Przykładowo okres taki jest wskazany w art. 30 ust. 3c ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych. Zgodnie z tym przepisem Państwowa Inspekcja Pracy przeprowadza, nie rzadziej niż co 3 lata, kontrolę w zakładach pracy chronionej i w zakładach aktywności zawodowej w zakresie przestrzegania przepisów ustawy, w szczególności art. 28 ust. 1 pkt 2.

Ad 7. Przetwarzanie danych osobowych dotyczących dzieci

Do zagadnienia przetwarzania wizerunku dziecka, w tym jego rozpowszechniania, UODO wielokrotnie odnosił się w materiałach zamieszczanych na stronie internetowej UODO[413]. Organ zwracał również uwagę na konieczność

[412] Ustawa z 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz.U. z 2024 r. poz. 44 ze zm.).
[413] M.in. w komunikacie „Szkolna RODO-wyprawka dla rodziców" zamieszczonym na poprzedniej stronie internetowej UODO (https://archiwum.uodo.gov.pl/pl/138/2164), w poradniku „Ochrona danych osobowych w szkołach i placówkach oświatowych – poradnik"

zapewnienia bezpiecznego przetwarzania danych osobowych w placówkach oświatowych[414]. Niemniej wątpliwości związane z przetwarzaniem wizerunku dzieci pojawiły się również w 2024 r.

W jednym z pytań inspektor ochrony danych zwrócił się z prośbą o ocenę, **czy szkoła może zbierać zgody na przekazywanie zdjęć oraz danych osobowych dzieci do urzędu miasta, w celu promowania inicjatyw szkoły oraz osiągnięć uczniów na stronie internetowej urzędu oraz na profilu urzędu znajdującym się na portalu Facebook**[415]. W odpowiedzi na te wątpliwości Prezes UODO wskazał, że przede wszystkim trzeba określić, czyj cel (jakiego podmiotu) będzie realizowany w związku z przetwarzaniem wizerunku ucznia. Inspektor nie wskazał, jaki i czyj cel realizuje urząd miasta w związku z tym przedsięwzięciem (czy urząd decyduje o konkretnym celu i sposobie przetwarzania danych), niemniej jeżeli udostępnienie przez szkołę danych osobowych uczniów (w tym ich wizerunków) następuje w celach, które samodzielnie kształtuje urząd, a nie w celach własnych udostępniającego, może to wskazywać, że urzędowi miasta (prezydentowi miasta) przysługiwać będzie status administratora. Jest to kluczowa kwestia do ustalenia, to do obowiązków administratora należy bowiem pozyskanie zgody na przetwarzanie danych osobowych (w tym wizerunku).

Wskazówki dotyczące pozyskiwania zgody zawarte są w Wytycznych EROD 05/2020 dotyczących zgody na mocy rozporządzenia 2016/679. Wskazano w nich w szczególności, że zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania. Art. 4 pkt 11 RODO stanowi, że zgoda osoby, której dane dotyczą, oznacza: dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

W pkt 3.3.1 ww. Wytycznych wskazano, że aby móc uznać, że zgoda jest „świadoma", należy poinformować osobę, której dane dotyczą, o określonych elementach kluczowych w celu dokonania wyboru. W związku z tym EROD jest zdania, że do uzyskania ważnej zgody wymagane są przynajmniej następujące informacje: 1) tożsamość administratora; 2) cel każdej operacji przetwarzania, w odniesieniu do

(https://archiwum.uodo.gov.pl/pl/383/479, szczególnie str. 32 i następne) czy w materiale „Wizerunek dziecka" zamieszczonym na poprzedniej stronie internetowej UODO (https://archiwum.uodo.gov.pl/pl/138/1268).

[414] Zagadnienie to zostało poruszone m.in. w materiale przygotowanym przez UODO „Dane osobowe bezpieczne podczas zdalnego nauczania" (dostępnym na stronie internetowej Urzędu pod linkiem: https://archiwum.uodo.gov.pl/pl/383/1475), jak również w Wytycznych dotyczących ochrony danych dzieci w środowisku edukacyjnym (polska wersja wytycznych dostępna https://archiwum.uodo.gov.pl/pl/138/1824).

[415] DOL.502.26.2024.

której prosi się o zgodę; 3) jakie dane (jaki rodzaj danych) będą gromadzone i wykorzystywane; 4) istnienie prawa do wycofania zgody.

EROD zauważa ponadto, że aby uznać, że zgoda jest „świadoma", należy w przypadku gdy na wnioskowanej zgodzie ma się opierać wielu (współ)administratorów lub gdy dane mają zostać przekazane innym administratorom, lub przetwarzane przez innych administratorów, którzy chcą się opierać na pierwotnej zgodzie, wszystkie te organizacje powinny być wymienione. EROD wskazuje, że w zależności od okoliczności i kontekstu sprawy konieczne może być zapewnienie większej ilości informacji, aby umożliwić osobom, których dane dotyczą, rzeczywiste zrozumienie danych operacji przetwarzania. Ze względu na wymóg ujawnienia zgodnej z prawem podstawy, na której opiera się administrator w momencie gromadzenia danych osobowych, administratorzy muszą określić zgodną z prawem podstawę, która będzie miała zastosowanie, jeszcze przed zebraniem danych.

Podkreślić należy, że zgoda na przetwarzanie wizerunku ucznia nie może być ogólna, lecz precyzyjnie określać, jakie dane i w jakim celu mają zostać udostępnione w konkretnym przypadku. Co istotne, celem zgody nie może być wyłącznie operacja związana z przetwarzaniem określonych danych (np. zgoda na udostępnianie czy upublicznianie danych). Cel ten powinien być doprecyzowany, poprzez wskazanie, że dotyczy np. promocji.

W odniesieniu do kwestii udostępniania danych na portalach społecznościowych organ przypomniał, że w takiej sytuacji *de facto* dochodzi do przekazania danych kolejnemu administratorowi. Takie udostępnianie nie tylko powinno być poprzedzone przez administratora pozyskaniem zgód, ale także analizą możliwych ryzyk wynikających z korzystania z danego narzędzia podczas przetwarzania danych osobowych (np. Facebook, kanał YouTube). Na ten aspekt zwrócono uwagę w decyzji Prezesa UODO z 18.10.2019 r.[416] NSA, podtrzymując decyzję Prezesa UODO, wskazał ponadto, że administrator, oceniając procesy przetwarzania danych osobowych i przekazując informacje za pośrednictwem serwisów będących własnością innych administratorów, musi pamiętać o konieczności dokonania oceny związanych z tym ryzyk, ale przede wszystkim oceny ról podmiotów występujących w tych procesach, czyli przeprowadzenia wnikliwej analizy ryzyka. Analiza ryzyka może pozwolić administratorowi upewnić się, czy dane z tego serwisu można odzyskać, czy w każdej sytuacji istnieje możliwość zrealizowania prawa osób do dostępu do danych, czy nie należy mieć kopii nagrań w innych miejscach, czy też jakie kategorie danych są w tym miejscu przetwarzane i zastosować odpowiednie środki ochrony, jak np. anonimizacja danych. Przeprowadzenie takiej analizy ryzyka, jak i posiadanie odpowiednich polityk związanych z procesami przetwarzania danych pozwala administratorom realizować ustanowioną w RODO zasadę rozliczalności. Mogą oni wówczas łatwo wykazać, że przetwarzanie danych odbywa się zgodnie z prawem, zasadą celowości, zasadą ograniczenia czasu przetwarzania i zasadą poufności oraz integralności danych.

[416] ZSPU.421.3.2019.

Administrator, który zamierza przetwarzać dane osobowe, powinien kierować się zasadą minimalizacji (art. 5 ust. 1 lit. c RODO), czyli gromadzić tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Dane powinny być przetwarzane wyłącznie w takich przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami (motyw 39 RODO). Co ważne, oceny, czy dane rzeczywiście są konieczne do osiągnięcia celu, administrator powinien dokonać najpóźniej w momencie ich zbierania. Przetwarzanie danych w zakresie zbędnym dla osiągnięcia celu będzie sprzeczne z RODO.

Podsumowując, organ podkreślił, że administrator powinien w pierwszej kolejności ocenić, czy dla osiągnięcia określonego celu istotnie niezbędne jest pozyskiwanie danych osobowych czy też tego celu nie można osiągnąć innymi sposobami. Niewykluczone bowiem, że zamierzony cel można osiągnąć, niekoniecznie przetwarzając określone dane osobowe (np. poprzez ogólne informacje o inicjatywach, działaniach podejmowanych przez administratora).

Innego rodzaju wątpliwości zostały poruszone w pytaniu IOD dotyczącym **podstawy przekazania danych osobowych uczniów szkoły artystycznej w arkuszu organizacji szkoły do organu prowadzącego, w celu realizacji uprawnień w zakresie kontroli**[417]. Organ nadzorczy przede wszystkim wskazał, że ze względu na to, że organ prowadzący szkołę artystyczną to podmiot publiczny, wszelkie jego działania (w tym przetwarzanie danych osobowych) powinny znajdować podstawę w przepisach. Ponadto Urząd Ochrony Danych Osobowych w poradniku dla szkół[418] wyjaśniał, że „organ prowadzący szkołę ma dostęp (a szkoła mu ten dostęp zapewnia) do danych osobowych przetwarzanych w szkole w związku z realizacją swoich obowiązków wynikających z przepisów prawa", a „dostęp organu prowadzącego do danych osobowych musi być adekwatny do celu przetwarzania danych, co oznacza, że zakres udostępnianych danych musi być odpowiedni (bez nadmiaru) do celu przetwarzania (zasada minimalizacji danych)". Wskazano również, że organ prowadzący szkołę ma dostęp do danych osobowych nauczycieli, które są zawarte w arkuszu organizacyjnym szkoły.

Z rozporządzenia Ministra Kultury i Dziedzictwa Narodowego w sprawie szczegółowej organizacji publicznych szkół i placówek artystycznych[419], regulującego m.in. zakres informacji zawartych w arkuszu organizacyjnym szkoły, nie wynika wprost obowiązek zawarcia w arkuszu danych osobowych uczniów; § 13 rozporządzenia wymienia w tym zakresie dane osobowe nauczycieli. Co również istotne, zgodnie z art. 110 Prawa oświatowego, arkusz organizacji szkoły i przedszkola określa szczegółową organizację nauczania, wychowania i opieki w danym roku szkolnym, a na podstawie zatwierdzonego arkusza dyrektor szkoły ustala tygodniowy rozkład zajęć określający organizację zajęć edukacyjnych. Celem sporządzenia arkusza nie jest zatem

[417] DOL.502.101.2024.
[418] „Ochrona danych osobowych w szkołach i placówkach oświatowych" (s. 19, 20); dostępny pod linkiem https://uodo.gov.pl/pl/383/479.
[419] Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z 22 sierpnia 2019 r. w sprawie szczegółowej organizacji publicznych szkół i placówek artystycznych (Dz.U. poz. 1624 ze zm.).

przekazanie danych osobowych organowi prowadzącemu na potrzeby kontroli szkoły, lecz zapewnienie właściwego funkcjonowania placówki oświatowej. Ponadto szkoła przekazuje arkusz organizacji organowi prowadzącemu w celu jego zatwierdzenia przez ten organ (art. 110 ust. 3 ww. ustawy), a nie w celu udostępnienia danych osobowych w związku z czynnościami kontrolnymi.

W opinii Prezesa UODO zawarcie danych osobowych uczniów w arkuszu organizacji szkoły i przekazanie go w takiej postaci organowi prowadzącemu rzeczywiście może budzić wątpliwości z punktu widzenia zasady minimalizacji danych wyrażonej w art. 5 ust. 1 lit. c RODO, a także zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO). Nie kwestionując uprawnienia tego organu do dokonywania kontroli w placówce oświatowej oraz do przetwarzania danych osobowych w tym celu, należy jeszcze raz podkreślić, że z przepisów prawa nie wynika możliwość żądania przez organ prowadzący przekazania danych osobowych uczniów za pomocą arkusza organizacji szkoły, który służy innym, określonym w przepisach celom.

Ad 8. Przetwarzanie danych osobowych w związku z ochroną małoletnich

Często wprowadzenie nowych regulacji prawnych powoduje liczne wątpliwości w zakresie stosowania obowiązków związanych z ochroną przetwarzanych w tym celu danych osobowych. Przykładem takiej sytuacji było wejście w życie znowelizowanych przepisów o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich[420].

Do UODO wpływały liczne sygnały o problemach w ich interpretacji i stosowaniu, w tym związanych z brakiem kompleksowego uregulowania kwestii dotyczących ochrony danych osobowych. Inspektorzy zwracali przede wszystkim uwagę na trudności w określeniu kategorii osób podlegających sprawdzeniu w rejestrach karnych, ze wskazaniem podmiotów, które mają tych sprawdzeń dokonywać, podstawy przetwarzania danych, okresu retencji danych czy spełnianiu obowiązku informacyjnego. Organ nadzorczy podkreślał, że przepisy wskazanej ustawy powinny być tak precyzyjnie skonstruowane, aby nie budziło wątpliwości, jakie dane osobowe, jakich konkretnych podmiotów danych, w związku z realizacją jakiego celu oraz jak długo miałyby być przetwarzane na podstawie jej przepisów. Ponadto w odpowiedziach kierowanych do inspektorów zachęcał do zgłaszania resortowi uwag na temat zaobserwowanych problemów i wnioskowania o przygotowanie precyzyjnych, niebudzących wątpliwości regulacji związanych z przetwarzaniem danych osobowych w ww. celach. Takie bowiem sygnały kierowane przez praktyków stosujących określone przepisy mogą przyczynić się do szybszego rozwiązania zauważonych problemów przez właściwy resort.

Na każde wpływające do UODO pytanie dotyczące powyższych przepisów inspektorzy otrzymywali wskazówki i wyjaśnienia mające im oraz obsługiwanym przez nich administratorom ułatwić stosowanie tych nieprecyzyjnych przepisów. Dodatkowo

[420] Ustawa z 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (Dz.U. z 2024 r. poz. 560).

na ich podstawie przygotowane zostały i zamieszczone w Biuletynie UODO 09/09/24 materiały „Weryfikowanie pracowników firmy sprzątającej pod względem karalności na tle seksualnym” oraz „Podmiot ustawowo zobowiązany do sprawdzenia niekaralności osób na tle seksualnym sam musi wykonać swoje obowiązki”[421], zawierające podpowiedzi co do stosowania omawianych przepisów.

W odpowiedzi na pytanie inspektora dotyczące podstawy pozyskiwania przez pracodawcę, którego firma świadczy usługi utrzymania czystości na terenie szpitala, informacji o niekaralności za przestępstwa na tle seksualnym, w tym wobec małoletnich, od zatrudnianych w niej osób[422], organ wskazał, że jednym z kluczowych rozwiązań mających chronić dzieci przed wykorzystaniem seksualnym jest obowiązkowa weryfikacja osób, które mają z nimi kontakt w czasie pracy. Odbywa się ona zarówno poprzez pozyskiwanie informacji z Rejestru Sprawców Przestępstw na Tle Seksualnym, jak i poprzez obowiązek przedłożenia zaświadczenia o niekaralności z Krajowego Rejestru Karnego. Rejestr Sprawców Przestępstw na Tle Seksualnym[423] składa się z trzech oddzielnych baz danych: rejestru z dostępem ograniczonym, rejestru publicznego oraz rejestru osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, wydała postanowienie o wpisie w Rejestrze. W Rejestrze z dostępem ograniczonym (zgodnie z art. 6 ww. ustawy) gromadzi się, z zastrzeżeniem art. 9 ust. 1–3, dane o osobach: prawomocnie skazanych za popełnienie przestępstw, o których mowa w art. 2, czyli przeciwko wolności seksualnej wymienionych w rozdziale XXV ustawy z 6 czerwca 1997 r. – Kodeks karny; przeciwko którym prawomocnie warunkowo umorzono postępowanie karne w sprawach o przestępstwa, o których mowa w art. 2; wobec których prawomocnie orzeczono środki zabezpieczające w sprawach o przestępstwa, o których mowa w art. 2; nieletnich, wobec których prawomocnie orzeczono środki wychowawcze, środek poprawczy lub środek leczniczy na podstawie ustawy z 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich w sprawach o czyny karalne, o których mowa w art. 2, z wyłączeniem art. 200 § 1 Kodeksu karnego.

Omawiana ustawa w art. 12 wymienia podmioty, którym przysługuje prawo do uzyskania informacji o osobie ujętej w Rejestrze, której dane zostały zgromadzone w Rejestrze z dostępem ograniczonym. Prawo to przysługuje m.in. pracodawcy przed nawiązaniem z osobą stosunku pracy związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich lub z opieką nad nimi, w zakresie uzyskania informacji, czy dane tej osoby są zgromadzone w tym Rejestrze (art. 12 pkt 6). Zatem skoro przepis wyraźnie określa, w jakich sytuacjach pracodawca może pozyskać informacje z ww. Rejestru, to uprawnienia tego nie można odnieść do pracowników zatrudnionych w innym

[421] DOL.502.124.2024.
[422] DOL.502.114.2024.
[423] Rejestr Sprawców Przestępstw na Tle Seksualnym utworzony został na mocy art. 4 ust. 1 ustawy z 13 maja 2016 r. o przeciwdziałaniu zagrożeniu przestępczością na tle seksualnym i ochronie małoletnich; zwany dalej "Rejestrem".

charakterze. Tym samym pracodawca, którego firma świadczy usługi utrzymania czystości na terenie szpitala, nie ma podstaw, aby pozyskiwać dane z ww. Rejestru.

O ile szpital jest zobowiązany do wprowadzenia standardów ochrony małoletnich, zgodnie z art. 22b ww. ustawy, i w tym celu ma prawo pozyskać informacje z ww. Rejestru, to może to zrobić tylko wobec swoich pracowników przed nawiązaniem z nimi stosunku pracy związanej z tymi czynnościami, o których mowa w art. 12 pkt 6 ustawy. Szczegółowe zasady związane z obowiązkiem pracodawcy w zakresie uzyskania informacji z Rejestru przed zatrudnieniem, a także obowiązek przedłożenia informacji z Krajowego Rejestru Karnego lub rejestru karnego innego państwa określa Rozdział 3 ww. ustawy.

O pomoc w ustaleniu właściwego sposobu postępowania w związku ze stosowaniem przepisów ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich zwrócił się jeden z inspektorów ochrony danych powołany przez uczelnię medyczną. Jak wskazał, uczelnia medyczna jest organizatorem procesu kształcenia, w tym praktyk oraz zajęć klinicznych, które odbywają się w podmiotach leczniczych, na podstawie zawartych z tymi podmiotami umów. W związku z tym, że organizowana działalność spełnia przesłanki z art. 21 ust. 1 wyżej powołanej ustawy, tj. wiąże się z edukacją, leczeniem, opieką nad małoletnimi pacjentami podmiotów leczniczych, uczelnia dokonuje weryfikacji studentów skierowanych na praktyki i zajęcia w podmiocie leczniczym w Rejestrze z dostępem ograniczonym poprzez konto instytucjonalne oraz w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze.

Jeżeli okazałoby się, że student, który ma zostać skierowany na praktykę, widnieje w ww. rejestrach, uczelnia nie może dopuścić go do jej odbycia. Jednocześnie uczelnia zobowiązała studentów do dostarczenia jej informacji z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z 29 lipca 2005 r. o przeciwdziałaniu narkomanii lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego.

Podniesione w pytaniu IOD wątpliwości dotyczyły zwracania się przez podmioty lecznicze, w których studenci będą odbywali praktyki, o: 1) przedkładanie przez uczelnię podmiotowi leczniczemu przed rozpoczęciem praktyki aktualnej informacji, czy dane studenta są zamieszczone w Rejestrze z dostępem ograniczonym lub w Rejestrze osób, w stosunku do których Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 wydała postanowienie o wpisie w Rejestrze, 2) składanie przez uczelnię oświadczeń, że studenci posiadają aktualne zaświadczenie z Krajowego Rejestru Karnego w zakresie przestępstw określonych w rozdziale XIX i XXV Kodeksu karnego, w art. 189a i art. 207 Kodeksu karnego oraz w ustawie z 29 lipca 2005 r. o przeciwdziałaniu narkomanii lub za odpowiadające tym przestępstwom czyny zabronione określone w przepisach prawa obcego, 3) umowne zagwarantowanie podmiotowi leczniczemu uprawnienia do weryfikacji danych zgromadzonych przez uczelnię w wykonaniu obowiązków z art. 21

ww. ustawy poprzez udostępnienie tych danych w formie kopii lub wglądu w oryginały dokumentów[424].

Prezes UODO, odpowiadając na wątpliwości IOD, wskazał, że przepisy ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich określają, jakie podmioty są zobowiązane do pozyskiwania danych osób podlegających sprawdzeniu, o którym mowa w art. 21 tej ustawy.

Zgodnie z ustępem 1 powołanego przepisu przed nawiązaniem z osobą stosunku pracy lub przed dopuszczeniem osoby do innej działalności związanej z wychowaniem, edukacją, wypoczynkiem, leczeniem, świadczeniem porad psychologicznych, rozwojem duchowym, uprawianiem sportu lub realizacją innych zainteresowań przez małoletnich, lub z opieką nad nimi na pracodawcy lub innym organizatorze takiej działalności oraz na osobie, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do takiej działalności, ciążą obowiązki określone w ust. 2-8, w tym obowiązek pozyskania informacji z Rejestru Sprawców Przestępstw na Tle Seksualnym, z Krajowego Rejestru Karnego lub rejestru karnego innego państwa. Pozyskane informacje pracodawca lub inny organizator załącza do akt osobowych pracownika albo dokumentacji dotyczącej osoby dopuszczonej do takiej działalności (art. 21 ust. 9).

Z powyższych przepisów wynika, że każdy z ww. podmiotów zobowiązany jest do odrębnego pozyskania wskazanych informacji w opisany w ustawie sposób. Ustawodawca nie przewidział współdziałania między nimi – ani wymiany, ani udostępniania informacji pozyskanych przez nie na podstawie powołanej ustawy. Jeżeli prawodawca określił katalog działań służących osiągnięciu wskazanego celu, to podmiot go realizujący powinien podejmować jedynie te z nich, które są wskazane w przepisach prawa. Uregulowania te stanowią podstawę prawną legalizującą przetwarzanie danych osobowych przez wskazane w nich podmioty. Natomiast wszelkie porozumienia zawierane pomiędzy takimi podmiotami nie mogą zastępować norm prawnych ani tworzyć niewynikających z nich nowych kompetencji.

W przedstawionej sytuacji przede wszystkim należałoby ustalić, który z podmiotów, czy może oba, zobowiązane są do dokonania sprawdzenia osób, o którym mowa w art. 21 ustawy o ochronie małoletnich. Następnie każdy podmiot zobowiązany powinien samodzielnie wykonać ciążące na nim obowiązki.

Ad 9. Przetwarzanie danych osobowych z wykorzystaniem nowych technologii

Szybki rozwój technologiczny skutkuje nowymi wyzwaniami w zakresie stosowania przepisów RODO w kontekście zagwarantowania właściwej ochrony podmiotom danych. Należy jednak pamiętać, że RODO jest neutralne technologicznie, co oznacza, że dane osobowe muszą być objęte skuteczną ochroną niezależnie od formy ich przetwarzania oraz wybranych przez administratora metod dla realizacji tego celu. Inspektorzy zawracający się z pytaniami do UODO zastanawiali się, jak przy

[424] DOL.502.124.2024.

wykorzystaniu nowych rozwiązań technologicznych zapewnić odpowiednią ochronę danych osobowych.

Jedno z pytań inspektora ochrony danych dotyczyło tego**, czy zaszyfrowane przez administratora (dysponującego kluczami deszyfrującymi) dane osobowe**, tj. zamienione na ciąg cyfr, **stanowią dane osobowe, a tym samym, czy przetwarzanie takich informacji wymaga umowy powierzenia w przypadku ich przekazania firmie świadczącej usługę przechowywania danych w chmurze**[425]. W odpowiedzi organ wyjaśnił, że przepisy RODO przesądzają, że danym osobowym poddanym odwracalnemu procesowi pseudonimizacji (w odróżnieniu od nieodwracalnego procesu anonimizacji), niezależnie od technicznych aspektów tego procesu, takich jak np. zamiany na ciąg cyfr, w dalszym ciągu przysługuje ochrona wynikająca z tego aktu prawnego. Dlatego w opisanej sytuacji należałoby zawrzeć umowę powierzenia.

RODO w art. 4 pkt 5 wprost definiuje, że pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Żeby 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, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby. Motyw 28 RODO w kontekście pseudonimizacji – jako środka, który może ograniczyć ryzyko dla osób, których dane dotyczą – wskazuje zarówno na administratorów, jak i podmioty przetwarzające jako tych, którym środek ten może pomóc wywiązać się z obowiązku ochrony danych. Natomiast na aspekt przechowywania osobno w ramach pseudonimizacji dodatkowych informacji pozwalających przypisać dane osobowe konkretnej osobie, której one dotyczą, zwraca uwagę motyw 29 RODO.

Należy podkreślić, że pseudonimizacja to jedynie technika zabezpieczenia danych osobowych, mająca na celu zmniejszenie ryzyka dla podmiotów danych związanego z przetwarzaniem tych danych.

Do oceny, czy w konkretnym przypadku dokonano anonimizacji, czy pseudonimizacji pomocne mogą być tezy zawarte w Opinii 05/2014 Grupy Roboczej Art. 29 w sprawie technik anonimizacji z 10 kwietnia 2014 r. Wskazano w niej m.in., że: „Konieczne jest zatem zrozumienie, że jeżeli administrator danych nie usunie pierwotnych (umożliwiających identyfikację) danych na poziomie zdarzenia, a przekaże część tego zbioru danych (na przykład po usunięciu lub ukryciu danych

[425] DOL.502.9.2024.

umożliwiających identyfikację), powstały zbiór danych nadal stanowi zbiór danych osobowych. Powstały zbiór danych można zakwalifikować jako anonimowy jedynie w przypadku, gdy administrator danych zagregowałby dane, osiągając poziom, na którym nie istnieje już możliwość zidentyfikowania poszczególnych wydarzeń. Na przykład: jeżeli organizacja gromadzi dane dotyczące przemieszczania się osoby fizycznej, wzorce podróżowania tej osoby na poziomie zdarzenia nadal kwalifikowałyby się jako dane osobowe w odniesieniu do każdej strony, o ile administrator danych (lub jakakolwiek inna strona) nadal ma dostęp do oryginalnych danych pierwotnych, nawet jeżeli ze zbioru udostępnionego osobom trzecim usunięto elementy umożliwiające bezpośrednią identyfikację".

Jeżeli administrator udostępni dostawcy usług spseudonimizowane dane osobowe pozwalające zidentyfikować konkretne osoby, to nadal będzie dochodziło do przetwarzania danych osobowych tych osób. Istotnym aspektem sprawy wskazującym na przetwarzanie danych osobowych pomiędzy tymi podmiotami jest to, że administrator posiada informację pozwalającą na powrotną identyfikację osób.

Kwestia wykorzystania konkretnej techniki przez administratora do procesu, który z założenia może być odwracalny, czyli pseudonimizacji, co do zasady będzie się więc odnosiła do ochrony danych osobowych. Okoliczność, w jaki sposób dokonano pseudonimizacji, jest istotna dla oceny przestrzegania przez administratora i podmiot przetwarzający zasad ochrony danych osobowych, zwłaszcza zasady integralności i poufności (art. 5 ust. 1 lit. a RODO).

Odnosząc się do potrzeby zawarcia umowy powierzenia przez administratora, organ nadzorczy zauważył, że przekazanie danych poddanych pseudonimizacji innemu podmiotowi, jeżeli nie następuje na innej podstawie prawnej, powinno mieć podstawę w postaci takiej umowy.

Jednocześnie Prezes UODO wskazał, że TSUE w wyroku z 26 kwietnia 2023 r. (sprawa T-557/20) dotyczącym sporu między administratorem a Europejskim Inspektorem Ochrony Danych (EIOD) przyjął odmienne niż wyżej przedstawione stanowisko. TSUE w ww. wyroku nie zgodził się ze stanowiskiem EIOD dotyczącym definicji danych osobowych zawartej w art. 3 pkt 1 rozporządzenia 2018/17251 (która odpowiada definicji zawartej w art. 4 pkt 1 RODO). Sprawa dotyczyła przekazania firmie konsultingowej spseudonimizowanych danych.

W opinii EIOD okoliczność, że odbiorca nie miał dostępu do informacji, które posiadał administrator, pozwalających na ponowną identyfikację, nie skutkuje tym, że spseudonimizowane dane przekazane odbiorcy stały się danymi anonimowymi. EIOD twierdzi, że dane pozostają w dalszym ciągu spseudonimizowane nawet wtedy, gdy zostają przekazane osobie trzeciej, która nie dysponuje dodatkowymi informacjami.

TSUE podkreślił natomiast, że kluczowym kryterium przy ocenie kwalifikacji danych jest perspektywa odbiorcy danych. Rozstrzygnięcie TSUE wskazuje, że sama możliwość dostępu administratora do informacji identyfikujących (pozwalających na odwrócenie pseudonimizacji) nie przekłada się na automatyczne uznawanie danych za dane osobowe dla odbiorcy. W ocenie TSUE należy więc każdorazowo zbadać, czy odbiorca ma realną możliwość identyfikacji oznaczonych osób fizycznych, tj. czy informacje przekazane odbiorcy stanowią dla niego dane osobowe. Wyrok TSUE nie

jest prawomocny, został on zaskarżony przez EIOD do Trybunału Sprawiedliwości Unii Europejskiej (zarejestrowany pod sygn. C-413/23 P) i dotychczas nie zapadło rozstrzygnięcie w tej sprawie.

Inne zagadnienie przedstawione przez inspektora dotyczyło tego, czy:

- stosowanie podpisu złożonego z wykorzystaniem narzędzia IC PEN oraz przechowywanie kopii dokumentu opatrzonego takim podpisem stanowi przetwarzanie danych biometrycznych,
- jakie będą odpowiednie środki ochrony danych osobowych oraz
- czy zgoda na przetwarzanie danych osobowych (tj. na użycie IC Pen do podpisania umowy lub innego dokumentu) powinna być odbierana oddzielnie do każdej umowy, czy raczej może mieć charakter ogólny[426].

Organ nadzorczy, odpowiadając na przedstawione pytania, zwrócił uwagę na definicję „danych biometrycznych" zawartą w art. 4 ust. 14 RODO. Jednocześnie EROD w swoich Wytycznych 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo[427] zaleciła rozpatrzenie trzech elementów, aby uznać określone dane za dane biometryczne. Są to: a) charakter danych: dane dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej; b) środki i sposób przetwarzania: wynikają z użycia odpowiedniej technologii; c) cel przetwarzania: dane muszą być przetwarzane w celu jednoznacznej identyfikacji osoby.

Ponadto Grupa Robocza Art. 29 w Opinii 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych[428] zaznaczyła, że jedną z kategorii technik biometrycznych są techniki behawioralne, które obejmują mierzenie zachowania danej osoby na podstawie podpisu odręcznego. Dodano, że „typowymi cechami dynamicznymi mierzonymi przez system biometrii podpisu odręcznego (taki jak tablet graficzny) są: stopień nacisku, kąt nachylenia pisma, prędkość i przyspieszenie narzędzia pisarskiego, kształt liter, kierunek pisma oraz inne niepowtarzalne cechy dynamiczne".

Biorąc pod uwagę powyższe oraz to, że kopia podpisu oraz podpis złożony przy pomocy narzędzia IC PEN, który odczytuje i zapisuje kształt pisma, siłę nacisku, czas zapisu oraz szybkość ruchu ręki składającego podpis, można uznać za „dane biometryczne" w rozumieniu art. 4 ust. 1 i art. 9 RODO, jeżeli administrator używa określonych środków technicznych umożliwiających zidentyfikowanie osoby fizycznej, tj. posiada narzędzia pozwalające na weryfikację tożsamości osoby fizycznej przy pomocy zapisanych danych ze wzorcem biometrycznym i tym samym dysponuje środkami do „specjalnego przetwarzania technicznego".

Prezes UODO przypomniał, że „dane biometryczne" stanowią szczególne kategorie danych wskazane w art. 9 ust.1 RODO i mogą być przetwarzane jedynie

[426] DOL.502.104.2024.
[427] Dostępne pod linkiem: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_pl.
[428] Oryginalny dokument jest dostępny pod linkiem: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf; tłumaczenie na język polski można znaleźć tutaj: https://archiwum.giodo.gov.pl/pl/1520111/4676.

w szczególnych okolicznościach, określonych w ust. 2 powołanego przepisu, np. w sytuacji, gdy „osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, że osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1". Ponadto motyw 51 RODO określa, że „dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności". Z tego powodu wprowadzone techniczne i organizacyjne środki ochrony danych osobowych przez administratora muszą ograniczyć czynniki ryzyka dla ochrony praw i wolności podmiotów danych.

W związku z tym administrator powinien przede wszystkim, przed wprowadzeniem stosowania technologii IC PEN, przeprowadzić ocenę skutków dla ochrony danych (tzw. Data Protection Impact Assessment – DPIA), 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" (art. 35 RODO).

Dodatkowo powinno się również przeprowadzić analizę tego, czy technologia IC PEN i związane z nią przetwarzanie danych biometrycznych są niezbędne do świadczenia określonej usługi, a nie jest to tylko najdogodniejsze rozwiązanie dla administratora, zgodnie z Opinią 03/2012 Grupy Roboczej Art. 29.

Po przeprowadzeniu oceny ryzyka, administrator jest zobowiązany do wprowadzenia odpowiednich środków bezpieczeństwa danych osobowych odpowiadających stopniowi zagrożenia (art. 32 RODO).

Grupa Robocza Art. 29 w Opinii 3/2012 oraz EROD w Wytycznych 3/2019, w celu zapewnienia wysokiego poziomu ochrony technicznej przy przetwarzaniu danych biometrycznych, zalecają m.in. wprowadzenie mechanizmu automatycznego usuwania danych, aby zapobiec zbyt długiemu okresowi przechowywania danych biometrycznych, wprowadzenie systemów weryfikujących autentyczność podpisującego, przechowywanie informacji biometrycznych w postaci zaszyfrowanej oraz w oddzielnej bazie danych, a także kategoryzację danych w trakcie ich przesyłania i przechowywania.

Co więcej, administrator już w czasie projektowania procesów przetwarzania danych powinien uwzględnić wdrożenie odpowiednich środków technicznych i organizacyjnych oraz domyślną ochronę, które zapewnią odpowiednią ochronę praw i wolności podmiotów (*privacy by design* i *privacy by default,* o których mowa w art. 25 RODO). W sytuacji, w której administrator nie wprowadził niezbędnych zabezpieczeń, pomocne może być zaznajomienie się z Wytycznymi EROD 4/2019 dotyczącymi artykułu 25 uwzględniającego ochronę danych w fazie projektowania oraz domyślną ochronę danych[429]. Poza tym Grupa Robocza Art. 29 w Opinii 3/2012 zwraca uwagę, że przetwarzanie danych na podstawie zgody jest ważne, jeżeli udzielona jest

[429] Dostępne pod linkiem: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_pl.

wystarczająca ilość informacji o zastosowaniu danych biometrycznych podmiotowi, którego dane będą przetwarzane. Informacje, które powinny zostać podane takiemu podmiotowi, są opisane w art. 13 ust. 1 i 2 RODO. Z uwagi na szczególny charakter danych biometrycznych, należy zwrócić uwagę na podanie okresu przechowywania danych osobowych oraz informacje o prawie do cofnięcia zgody na ich przetwarzanie. Administrator powinien mieć również na względzie zasadę minimalizacji, ograniczenia przechowywania, integralności i poufności danych (art. 5 RODO).

Organ nadzorczy podkreślił, że zgodnie z art. 4 ust. 11 RODO, „zgoda" powinna być dobrowolna, konkretna, świadoma i powinna zawierać jednoznaczne okazanie woli, w formie wyraźnego działania pozwalającego na przetwarzanie danych osobowych, w tym danych biometrycznych. Motyw 43 RODO stanowi, że „zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych". W motywie 32 doprecyzowano, że „zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele". Ponadto Wytyczne EROD 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679 stanowią, że „usługa może obejmować wiele operacji przetwarzania w więcej niż jednym celu. W takich przypadkach osobom, których dane dotyczą, powinna przysługiwać swoboda wyboru celu, który akceptują, zamiast obowiązku wyrażenia zgody na szereg celów przetwarzania. W danym przypadku zgodnie z RODO uzasadnione może być wyrażenie kilku zgód w celu rozpoczęcia oferowania usługi". W związku z tym administrator powinien umożliwić osobie, której dane dotyczą, wyrażenie zgody/zgód na przetwarzanie danych osobowych, w tym danych biometrycznych, na dokładnie określone cele doprecyzowane w zależności od umowy.

Administrator powinien również pamiętać, że jeżeli chce przetwarzać dane osobowe w innym celu, niż oznajmiono osobie, której dane dotyczą, musi poprosić o zgodę tej osoby na nowy cel albo znaleźć inną podstawę prawną zgodną z art. 6 RODO. Dodatkowo art. 7 ust. 4 RODO oraz Wytyczne 05/2020 podkreślają, że łączenie zgody z akceptacją warunków lub uzależnianie wykonania umowy lub świadczenia usługi od uwzględnienia wniosku o wyrażenie zgody na przetwarzanie danych osobowych, które nie jest konieczne w celu wykonania umowy lub świadczenia usługi, jest uznawane za sytuację niepożądaną i podważającą dobrowolność zgody.

Zgodnie z art. 7 ust. 3 RODO administrator jest zobowiązany zapewnić, aby osoba, której dane są przetwarzane, mogła wycofać zgodę w dowolnym momencie oraz z taką samą łatwością, jak jej udzieliła. Administrator ma także obowiązek poinformowania osoby o prawie do wycofania zgody oraz o tym, jak tego dokonać, jeszcze przed rozpoczęciem przetwarzania danych osobowych, na podstawie art. 13 ust. 2 lit. c RODO. Co więcej, Wytyczne EROD 05/2020 precyzują, że wycofanie zgody nie powinno przynieść żadnych niekorzystnych konsekwencji dla osoby, której dane są przetwarzane. Administrator powinien znaleźć taki sposób wycofania zgody, aby nie powodował on żadnych niekorzystnych skutków dla podmiotu danych.

Ad 10. Ochrona danych osobowych przetwarzanych z wykorzystaniem rozwiązań informatycznych

Wielu inspektorów w 2024 r. zwracało się z prośbą o zajęcie przez organ nadzorczy stanowiska w sprawie korzystania przez pracowników z prywatnych profili zaufanych do celów służbowych[430]. Prezes UODO w odpowiedzi wskazywał, że problem wykorzystywania „prywatnego" profilu zaufanego do celów służbowych był przedmiotem wystąpień i opinii legislacyjnych[431].

Zastrzeżenia organu budziło posługiwanie się przez pracowników profilem/podpisem zaufanym w celach służbowych, zarówno w celu podpisywania korespondencji służbowej, jak i w celu uwierzytelniania się w systemach informatycznych. Zwłaszcza że brak jest możliwości podpisywania podpisem zaufanym bez ujawniania nr PESEL. Organ nadzorczy przedstawiał wiele argumentów, dlaczego ujawnianie numeru PESEL pracownika w sytuacji stosowania podpisu zaufanego jest niezgodne z zasadami wyrażonymi w art. 5 RODO, art. 87 RODO oraz art. 22(1) ustawy z 26 czerwca 1974 r. – Kodeks pracy. Ponadto wskazywał, że wykorzystywanie profilu zaufanego do celów służbowych powinno być dodatkowo przeanalizowane w świetle zasady minimalizacji danych, określonej w art. 5 ust. 1 lit. c RODO. Podstaw prawnych dla ujawniania numeru PESEL pracownika poprzez podpisywanie przez niego dokumentów elektronicznych nie kształtuje także art. 22(1) § 1 k.p. W przywołanej odpowiedzi do RPO organ nadzorczy wskazał również, że w jego ocenie brak jest podstaw prawnych do żądania przez pracodawcę, aby pracownik uwierzytelniał się w systemie wykorzystywanym do realizacji zadań pracodawcy, przy użyciu profilu zaufanego.

Prawidłową praktyką powinno być korzystanie przez pracowników na potrzeby ich identyfikacji oraz składania podpisów ze służbowych narzędzi, które zapewniałyby ochronę przed nieuzasadnioną ingerencją w prywatność zatrudnionych.

Niestety, problemy sygnalizowane przez UODO w powołanych pismach nie znalazły dotychczas rozwiązania, a w niektórych aktach prawnych, w tym np. w ustawie o doręczeniach elektronicznych, jako główny lub alternatywny sposób identyfikacji osoby lub podpisywania dokumentów w celach służbowych wskazywany jest profil zaufany pracownika. Taki sposób ujęcia powyższych zagadnień w przepisach prawa jest problematyczny, dlatego niezbędne jest sygnalizowanie właściwym resortom potrzeby zweryfikowania rozwiązań przyjętych w takich regulacjach i wprowadzenia stosownych zmian.

Ujawnianie numeru PESEL w certyfikacie podpisu zaufanego staje się zatem coraz szerszym problemem poruszanym przez wiele środowisk.

---

[430] M.in. DOL.502.60.2024, DOL.502.44.2024.

[431] Np. opinia Prezesa UODO do projektu ustawy o zmianie ustawy – Kodeks postępowania administracyjnego oraz niektórych innych ustaw dostępna na stronie internetowej Sejmu RP pod adresem: http://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=687; odpowiedź z 4 czerwca 2021 r. skierowana do Rzecznika Praw Obywatelskich co do korzystania przez pracowników GIS z profilu zaufanego podczas wykonywania przez nich obowiązków służbowych (dostępna pod adresem https://bip.brpo.gov.pl/pl/content/pracownicy-sanepidu-profil-zaufany-interwencja-rpo-puodo-odpowiedz-kolejna); wystąpienie Prezesa UODO do Ministra Cyfryzacji (https://archiwum.uodo.gov.pl/pl/138/1072).

W opinii Prezesa UODO, ze względu na systemowy charakter poruszanego zagadnienia, niewątpliwie wymaga ono pogłębionej debaty z udziałem zainteresowanych środowisk celem wypracowania rozwiązań pozwalających pogodzić zapewnienie identyfikacji osoby podpisującej dokumenty elektronicznie z prawem do ochrony danych osobowych oraz z innymi prawami sektorowymi, w tym m.in. przepisami prawa pracy. W odpowiedziach na pytania inspektorów organ nadzorczy zadeklarował ponowne podniesienie tego problemu.

Kwestia wykorzystania prywatnego profilu zaufanego oraz nr PESEL pracowników pojawiła się również w pytaniu inspektora **o wskazanie podstawy prawnej do pozyskiwania od pracowników numeru PESEL, który jest wymagany w związku z utworzeniem adresu do doręczeń elektronicznych (ADE) i wskazywaniem tych osób jako administratora/administratorów oraz użytkowników skrzynki doręczeń**, o których mowa w ustawie o doręczeniach elektronicznych[432]. Osoby te, logując się do skrzynki doręczeń, muszą z kolei skorzystać z aplikacji mObywatel, Profilu Zaufanego, osobistej bankowości elektronicznej itp.[433] Organ nadzorczy wskazał, że obowiązek podawania takich danych wynika z art. 12 ust. 2 pkt 7 ustawy o doręczeniach elektronicznych, zgodnie z którym wniosek o utworzenie adresu do doręczeń elektronicznych powiązanego z publiczną usługą rejestrowanego doręczenia elektronicznego dla podmiotu publicznego zawiera m.in. imię i nazwisko administratora skrzynki doręczeń, jego adres poczty elektronicznej oraz numer PESEL, a jeżeli nie został nadany – niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2015/1501 z 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

Jednocześnie zaznaczył, że do problemu przetwarzania numeru PESEL pracownika podmiotu publicznego do celów służbowych odniósł się w uwagach do projektu ustawy o elektronizacji doręczeń oraz niektórych innych ustaw (poprzedzającego projekt ww. ustawy o doręczeniach elektronicznych). Zgłoszone przez organ nadzorczy wątpliwości dotyczyły zasadności pozyskiwania na potrzeby prowadzenia bazy adresów elektronicznych numeru PESEL osoby działającej w imieniu podmiotu publicznego. Numer PESEL to jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, zawierający datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną. Jest on ściśle powiązany ze sferą prywatną osoby fizycznej, nie zaś z jej czynnościami urzędowymi. Podlega również, jako krajowy numer identyfikacyjny, szczególnej ochronie na gruncie art. 87 RODO. Dlatego w opinii organu nadzorczego ww. rozwiązanie stanowić może naruszenie zasady minimalizacji danych, o której mowa art. 5 ust. 1 lit. c RODO.

[432] Ustawa z 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2024 r. poz. 1045).
[433] DOL.502.225.2023.

Odnosząc się do sygnalizowanego problemu polegającego na zobowiązywaniu pracowników, aby w celu logowania się do skrzynki doręczeń skorzystali z profilu mObywatel, profilu zaufanego lub osobistej bankowości elektronicznej, organ nadzorczy wskazał na wielokrotne działania podejmowane w tym temacie.

Obecny sposób ujęcia przedstawionych zagadnień w przepisach ustawy o doręczeniach elektronicznych jest problematyczny, dlatego niezbędne jest sygnalizowanie właściwemu resortowi potrzeby zweryfikowania przyjętych w tej regulacji rozwiązań i wprowadzenia stosownych zmian. Prezes UODO będzie nadal podejmował działania w tym zakresie.

Ad 11. Realizacja praw osoby, której dane dotyczą

Przepisy RODO przyznają osobom, których dane osobowe dotyczą, liczne uprawnienia związane z przetwarzaniem ich danych. Zostały one zawarte przede wszystkim w rozdziale III RODO. Niemniej właściwe wypełnianie obowiązków administratora w zakresie realizacji praw osób nadal budzi pewne wątpliwości.

W jednym z pytań inspektor zwrócił się z prośbą o interpretację **„liczby żądań”,** o której mowa w art.12 ust. 3 RODO, w związku z wnioskiem o dostęp do danych. Inspektor zastanawiał się, czy „liczba żądań” dotyczy żądań otrzymanych od tego samego podmiotu danych, czy brane są pod uwagę wszystkie żądania, które administrator otrzymał w danym okresie i mogą to być żądania od różnych podmiotów danych[434]. Organ w odpowiedzi wskazał, że z treści przepisów RODO oraz jego motywów nie wynika jasno, czy „liczba żądań”, o której mowa w art. 12 ust. 3 RODO, odnosi się wyłącznie do żądań zgłoszonych administratorowi przez ten sam podmiot danych, czy też chodzi o wszelkie żądania wszystkich podmiotów danych, jakie administrator rozpatruje w danym momencie. Przepis ten reguluje sposób realizacji przez administratora uprawnień podmiotu danych określonych w art. 15–22 RODO, których celem jest zapewnienie jak największej przejrzystości, rzetelności i zgodności z prawem przetwarzania danych osobowych oraz ochrona prawa jednostki do ochrony jej danych osobowych. Wydaje się więc, że analizowany przepis powinien być interpretowany w sposób zapewniający możliwie jak najpełniejszą realizację praw osoby, których dane dotyczą. Jednocześnie obowiązek dochowania terminu wskazanego w art. 12 ust. 3 RODO nie ma charakteru bezwzględnego i w pewnych okolicznościach należy mieć także wzgląd na szczególną sytuację administratora.

Istotne w kontekście tego zagadnienia są również wskazówki zawarte w Wytycznych EROD 01/2022 dotyczących praw osób, których dane dotyczą – Prawo dostępu[435]. Szczególną uwagę należy zwrócić na ten ich fragment, zgodnie z którym fakt otrzymywania przez duże przedsiębiorstwo dużej liczby żądań nie powoduje automatycznego przedłużenia terminu ich wykonania. „Jeżeli jednak administrator otrzymuje tymczasowo dużą liczbę żądań, na przykład ze względu na nadzwyczajne rozpowszechnienie informacji o jego działalności, można to uznać za uzasadniony

[434] DOL.502.137.2024.
[435] Dostępne pod linkiem: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_pl.

powód przedłużenia czasu reakcji. Niemniej administrator, szczególnie gdy zajmuje się dużą ilością danych, powinien dysponować procedurami i mechanizmami umożliwiającymi rozpatrywanie żądań w określonych terminach w normalnych okolicznościach" (pkt 164 wytycznych).

Odnosząc się do przedstawionego zagadnienia, wydaje się więc, że „liczbę żądań" wymienioną w art. 12 ust. 3 RODO i uzasadniającą przedłużenie terminu spełnienia żądania podmiotu danych należy rozumieć jako odnoszącą się do żądań od tego samego podmiotu (np. złożonych w jednym lub podobnym czasie). Wskazuje na to również zastawienie tej przyczyny w jednym szeregu ze „skomplikowanym charakterem żądania". Administrator zatem nie powinien nadużywać wynikającego z tego przepisu uprawnienia do przedłużenia ww. terminu i powinien korzystać z niego jedynie wyjątkowo, przede wszystkim ze względu na wyżej opisane *ratio legis* art. 15–22 RODO. Administrator powinien również zadbać o wdrożenie odpowiednich, właściwych dla skali przetwarzania i liczby otrzymywanych żądań, środków technicznych i organizacyjnych zapewniających jak najszybsze realizowanie tych żądań.

Z kolei w innym pytaniu inspektor przedstawił swoje wątpliwości co do tego, jak zweryfikować, czy **rodzic występujący z żądaniem realizacji praw z RODO faktycznie może działać jako przedstawiciel ustawowy dziecka**, a więc czy ma pełnię władzy rodzicielskiej, czy też została mu ona ograniczona albo został jej pozbawiony[436]. Prezes UODO wyjaśnił, że jeśli chodzi o możliwość żądania dostępu do danych w imieniu dziecka przez rodzica, któremu została ograniczona władza rodzicielska, kluczowe znaczenie mają przepisy prawa rodzinnego i opiekuńczego. Zgodnie z art. 95 § 1 i art. 96 § 1 Kodeksu rodzinnego i opiekuńczego[437] władza rodzicielska obejmuje w szczególności obowiązek i prawo rodziców do wykonywania pieczy nad osobą i majątkiem dziecka oraz do wychowania dziecka, z poszanowaniem jego godności i praw. Rodzice wychowują dziecko pozostające pod ich władzą rodzicielską i kierują nim. Dlatego też w sytuacji, gdy rodzic dziecka nie został pozbawiony władzy rodzicielskiej, ani władza ta nie została ograniczona w sposób uniemożliwiający zasięganie informacji o dziecku, to uprawnienie wynikające z art. 15 RODO będzie przysługiwało rodzicowi jako opiekunowi prawnemu podmiotu danych. Co ważne, ograniczenie władzy rodzicielskiej do pewnych obszarów nie oznacza ograniczenia prawa do informacji o dziecku, gdyż mogłoby spowodować to naruszenie prawa rodzica do uczestniczenia w życiu dziecka. Organ przypomniał, że nawet w przypadku odebrania praw rodzicielskich jednemu z rodziców, w dalszym ciągu przysługują mu pewne uprawnienia (np. prawo do kontaktu z dzieckiem), chyba że sąd te uprawnienia odbierze. Zatem jeżeli administrator nie otrzymał informacji o pozbawieniu rodzica władzy rodzicielskiej nad dzieckiem będącym podmiotem danych, ma on obowiązek spełnić żądanie zgłoszone przez rodzica na podstawie art. 15 RODO.

[436] DOL.502.153.2024.
[437] Ustawa z 25 lutego 1964 r. – Kodeks rodzinny i opiekuńczy (Dz.U. z 2023 r. poz. 2809 ze zm.).

Jednocześnie należy mieć na względzie art. 12 ust. 2 RODO, który stanowi, że administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22. W przypadkach, o których mowa w art. 11 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać prawa przysługujące jej na mocy art. 15–22, chyba że wykaże, że nie jest w stanie zidentyfikować osoby, której dane dotyczą. Jak ponadto wyjaśniono w motywie 59 RODO, należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy tego rozporządzenia, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Zgodnie z art. 12 ust. 6 RODO, 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.

EROD w Wytycznych 01/2022 (sekcje 3.3 i 3.4 Wytycznych) wyjaśniła m.in., że „administrator musi jednocześnie dbać o to, by nie gromadzić większej ilości danych osobowych, niż jest to konieczne do umożliwienia uwierzytelnienia osoby występującej z żądaniem. W związku z tym administrator przeprowadza ocenę proporcjonalności, która musi uwzględniać rodzaj przetwarzanych danych osobowych (np. szczególne kategorie danych lub ich brak), charakter żądania, kontekst, w jakim żądanie jest składane, a także wszelkie szkody, które mogłyby wyniknąć z niewłaściwego ujawnienia. Przy ocenie proporcjonalności należy pamiętać, aby unikać nadmiernego gromadzenia danych przy jednoczesnym zapewnieniu odpowiedniego poziomu bezpieczeństwa przetwarzania” (pkt 70 wytycznych). W kontekście spełnienia żądania uzyskania dostępu do danych osobowych zgłoszonego w imieniu dziecka wyjaśniono również, że należy kierować się przede wszystkim dobrem dziecka oraz wskazano na konieczność wdrożenia przez administratora odpowiednich środków w celu uniknięcia ujawnienia danych osobowych małoletniego osobie nieupoważnionej (pkt 85 i 86 wytycznych).

Weryfikując umocowanie do działania w imieniu innej osoby, administrator powinien wyważyć z jednej strony konieczność zapewnienia ochrony danych osobowych przed ujawnieniem ich osobie do tego nieuprawnionej, z drugiej nie powinien on w tym celu gromadzić danych nadmiarowych czy stosować środków, które w praktyce uniemożliwiałyby uzyskanie dostępu do danych osobie uprawnionej. Dokonując tej oceny, administrator powinien uwzględnić zwłaszcza kategorie przetwarzanych danych osobowych. Od nich zależy bowiem skala ryzyka naruszenia prywatności podmiotu danych w przypadku ujawnienia danych osobie nieupoważnionej.

11.1.4. Podsumowanie tematyki pytań i sygnałów od IOD

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 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. nakładanie na IOD zadań należących do administratora). Inspektorzy z dużym wyczuciem identyfikują zagrożenia dla ochrony danych osobowych wynikające 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 problemy ważne nie tylko z punktu widzenia administratora, u którego zostali wyznaczeni, ale również całego systemu ochrony danych osobowych. Dlatego niejednokrotnie przesyłane przez nich pytania stanowią impuls do podjęcia przez organ nadzorczy interwencji, m.in. w formie wystąpienia.

Z kolei jednym z ważnych zadań organu nadzorczego jest monitorowanie realizacji zidentyfikowanych wcześniej problemów wynikających np. z luk lub nieścisłości w przepisach prawa czy też braku przepisów zapewniających inspektorom właściwe warunki funkcjonowania. Dlatego w bieżącym okresie sprawozdawczym organ nadzorczy – wobec braku przedstawienia mu satysfakcjonujących rozwiązań problemów legislacyjnych – ponownie zwrócił się do właściwych organów o dokonanie odpowiednich zmian[438].

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.

[438] Np. wystąpienia do MZ, MEN oraz Szefa Służby Cywilnej opisane w części „Wystąpienia" niniejszego Sprawozdania.

Również w roku sprawozdawczym sygnały i zagadnienia przekazywane przez IOD zarówno w korespondencji przesyłanej do Urzędu, jak i podczas zorganizowanych przez Prezesa UODO spotkań z inspektorami (np. 9 kwietnia 2024 r. czy w ramach akcji „UODO rusza w kraj") wykorzystane zostały do opracowania różnych materiałów informacyjnych.

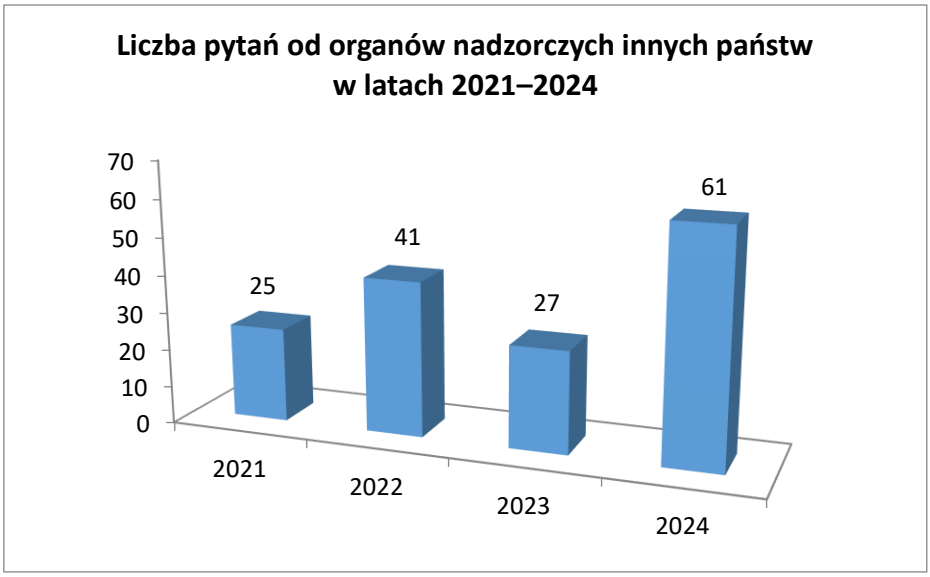
W okresie sprawozdawczym duża grupa pytań dotyczyła funkcjonowania IOD, w tym w szczególności nakładania na inspektora zadań innych niż te, które są przewidziane w RODO, np. zadań należących do administratora. Kwestie te wciąż budzą wątpliwości i dlatego organ nadzorczy w 2024 r. podejmował różne działania 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, zorganizował 9 kwietnia 2024 r. spotkanie, które miało na celu upowszechnianie informacji o zeszłorocznym działaniu EROD w ramach CEF DPO i sprawozdaniu z tego działania, w tym raporcie polskiego organu nadzorczego i przedstawionych w nim zagadnień dotyczących niezależności IOD, a także przeprowadzając szkolenia dla IOD reprezentującymi jednostki samorządu terytorialnego w ramach akcji „UODO rusza w kraj".

Biorąc zatem pod uwagę to, że 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. Pomocne w tym zakresie mogą być wypracowywane przez lata, we współpracy z inspektorami ochrony danych i administratorami, wskazówki dotyczące zgodnego z prawem realizowania obowiązków administratorów wobec IOD, które prezentowane były przez UODO.

11.1.5. *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 2024 r. do Prezesa UODO wpłynęło **61 zapytań organów nadzorczych z innych państw,** w tym m.in. z: Francji, Czech, Słowenii i Słowacji, Szwecji, Finlandii, Bułgarii, Litwy, Łotwy, Irlandii, Estonii i Luksemburga. Dla porównania, w 2023 r. takich pytań wpłynęło 27, w 2022 r. – 41, w 2021 r. – 25, zaś w 2020 r. – 14.



Wykres 19. Liczba pytań od organów nadzorczych innych państw skierowanych do Prezesa UODO w latach 2021–2024.

Organy nadzorcze zwracały się do Prezesa UODO z różnymi zagadnieniami. Pytania dotyczyły m.in. opinii polskiego organu nadzorczego w takich sprawach, jak:

- wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu na podstawie art. 58 ust. 2 lit. a RODO,
- realizacja prawa dostępu do danych,
- interpretacja przepisów RODO, m.in. art. 18, art. 21, art. 22 i art. 27,
- badania naukowe dotyczące zdrowia, tj. czy projekty badawcze są systematycznie sprawdzane przez komisje bioetyczne, czy dostęp do danych dotyczących zdrowia wymaga uprzedniej zgody organu, a w przypadku istnienia tego rodzaju procedury, jakie są zasadnicze kryteria analizowane przez krajowy organ ochrony danych przy ocenie wniosku,
- stosowanie monitoringu wizyjnego, m.in. w szkołach, przez osoby prywatne,
- przetwarzanie danych lokalizacyjnych pojazdów podłączonych do sieci,
- przetwarzanie danych osobowych i ochrona prywatności w sektorze łączności elektronicznej,
- regulacje dotyczące przetwarzania danych osobowych przez przedstawicieli wolnych zawodów, tj. adwokatów, radców prawnych, notariuszy czy doradców podatkowych,
- przetwarzanie danych do celów dowodowych,
- procedura akredytacji jednostek certyfikujących.

Polski organ ochrony danych dokonał wnikliwej 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, jak RODO jest interpretowane w państwach

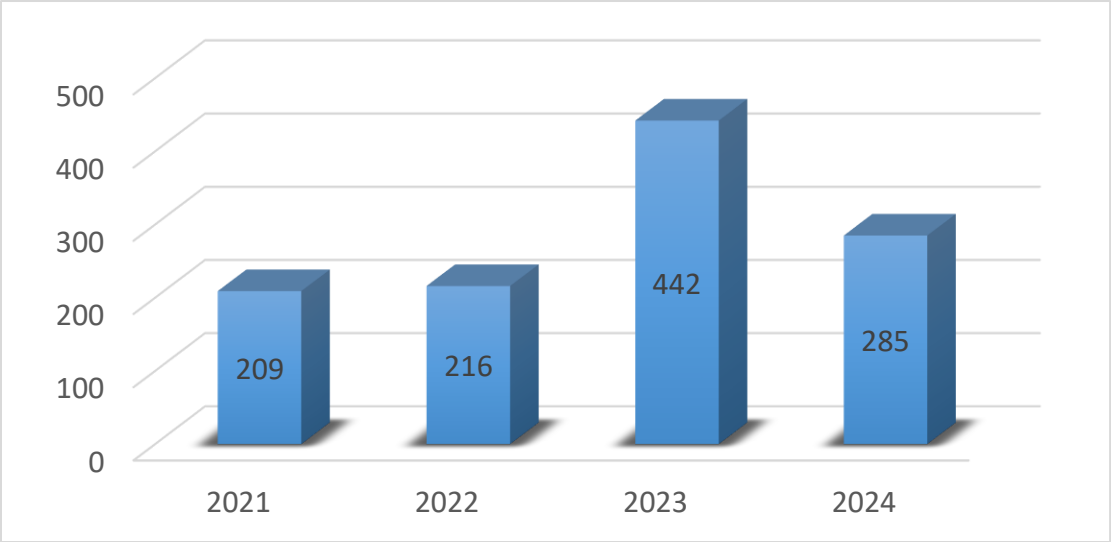
członkowskich UE. Ponadto otrzymywane pytania pozwalają rozeznać się w bieżących zagadnieniach, będących przedmiotem dyskusji innych organów nadzorczych. Pozwala to również na wypracowanie zharmonizowanych, wspólnych stanowisk przy uwzględnieniu ustawodawstwa krajowego.

11.2. Wnioski o dostęp do informacji publicznej

Zgodnie z treścią przepisu art. 61 Konstytucji RP prawo do informacji publicznej obejmuje możliwość uzyskiwania informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne, w zakresie, w jakim podmioty te wykonują zadania władzy publicznej bądź odpowiednio gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Przepis art. 61 Konstytucji umieszczony został w Rozdziale II, zatytułowanym „Wolności, prawa i obowiązki człowieka i obywatela", w podrozdziale „Wolności i prawa polityczne". Usytuowanie prawa do informacji publicznej w grupie wolności i praw politycznych znajduje uzasadnienie w tym, że wiąże się ono ściśle z innymi prawami obywatelskimi, jak czynne prawo wyborcze, prawo równego dostępu do służby publicznej, jak i z fundamentalnymi zasadami ustroju politycznego państwa. Szczegółowe zasady i tryb udzielania informacji określony został w ustawie z 6 września 2001 r. o dostępie do informacji publicznej[439]. Dostęp do informacji publicznej ma na celu umożliwienie obywatelom realny udział w życiu publicznym, ale także ma służyć jawności życia publicznego, określanej potocznie jako przejrzystość działań władzy publicznej oraz osób wykonujących zadania tej władzy.

Od 1 stycznia do 31 grudnia 2024 r. do Urzędu Ochrony Danych Osobowych wpłynęło łącznie **285 wniosków złożonych w trybie ustawy o dostępie do informacji publicznej.** Pytania wnioskodawców dotyczyły również realizacji ustawowych kompetencji Prezesa Urzędu, jak też działalności samego Urzędu w sferze organizacyjnej, finansowej czy kadrowej.

[439] Ustawa z 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz.U. z 2022 r. poz. 902).



Wykres 20. Liczba wniosków o dostęp do informacji publicznej, które wpłynęły do UODO w latach 2021–2024.

Wnioski o informację dotyczyły danych statystycznych, takich jak: liczba postępowań, liczba zgłoszonych skarg i naruszeń ochrony danych osobowych, liczba zawiadomień[440] z sądów powszechnych o wniesionych pozwach, liczba wydanych decyzji, liczba przeprowadzonych kontroli, wysokość nałożonych kar pieniężnych, rodzaj i liczba zastosowanych uprawnień naprawczych, złożonych wniosków o uprzednie konsultacje oraz konkretnych rozwiązań merytorycznych. Wiele pytań dotyczyło decyzji administracyjnych, liczby zgłoszonych Inspektorów Ochrony Danych, planu kontroli sektorowych, kontroli podmiotów przetwarzających dane osobowe przy użyciu aplikacji mobilnych oraz informacji, w jakich podmiotach Prezes Urzędu przeprowadził kontrolę.

Zdarzały się również wnioski o udostępnienie:

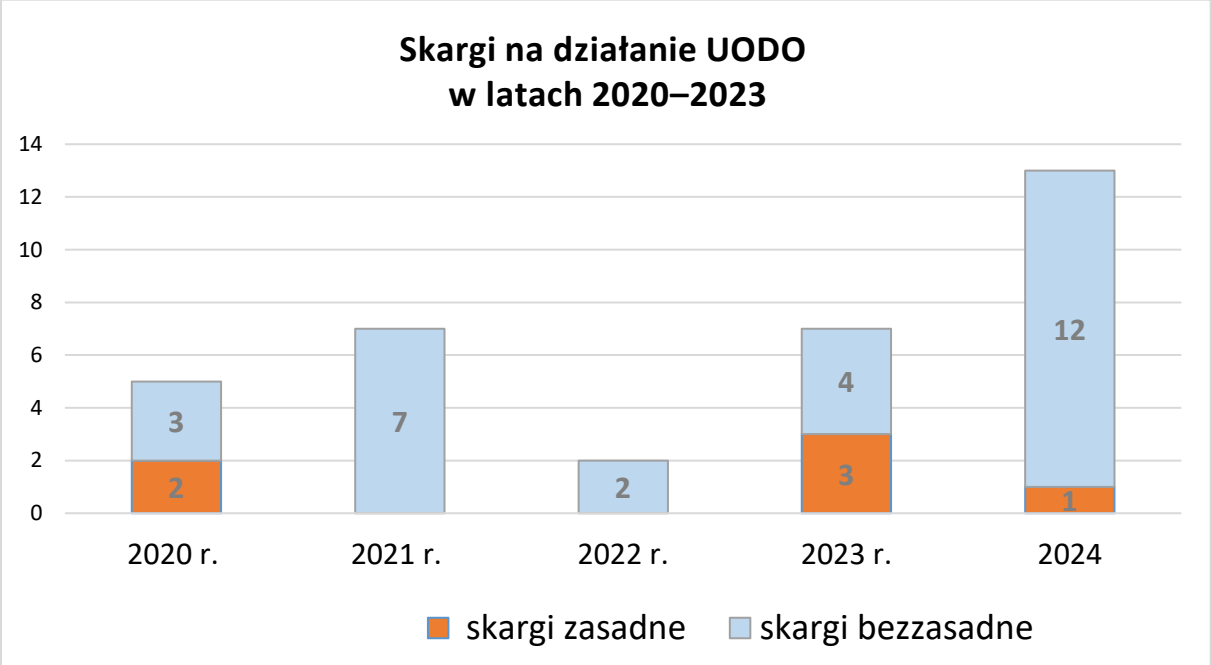
- treści decyzji wydanych przez Prezesa UODO,
- umów zawieranych przez Urząd z podmiotami zewnętrznymi,
- statystyk dotyczących spraw kadrowych.

O dużej transparentności działania organu świadczy także fakt, że Prezes Urzędu Ochrony Danych Osobowych wydał tylko 10 decyzji o odmowie udostępnienia informacji publicznej. Należy podkreślić, że tylko 2 z powyższych decyzji zostały zaskarżone do Wojewódzkiego Sądu Administracyjnego w Warszawie. W jednej z nich sąd utrzymał w mocy decyzję Prezesa UODO, druga nie została dotychczas rozstrzygnięta. Udzielono także 23 informacji poza trybem udostępniania informacji publicznej, najczęściej były to pytania w zakresie współpracy z organami ścigania. Wpłynęło również 12 spraw błędnie skierowanych do Prezesa UODO, które odsyłano do załatwienia właściwym podmiotom zgodnie z art. 65 k.p.a.

[440] Art. 94 ustawy z 10 maja 2018 r. o ochronie danych osobowych.

11.3. Skargi na działanie UODO

W 2024 r. udzielono odpowiedzi na 12 skarg na działanie Urzędu, które dotyczyły najczęściej, zdaniem skarżących, zaniedbania lub nienależytego wykonywania zadań przez Urząd albo przez jego pracowników, naruszenie praworządności lub interesów skarżących, przewlekłego lub biurokratycznego załatwiania spraw lub były wyrazem niezadowolenia z rozstrzygnięć prowadzonych postępowań w UODO. Tylko jedna z nich była zasadna. Wszystkie skargi z działu VIII k.p.a. zostały rozpatrzone w terminie przewidzianym w ustawie. Dwie skargi zostały przekazane zgodnie z właściwością na podstawie art. 234 k.p.a. do rozpatrzenia w toku prowadzonych postępowań.



Wykres 21. Liczba skarg na działanie UODO złożonych w latach 2020–2024.

11.4. 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 może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Podmiot, do którego skierowane zostało wystąpienie, jest zaś obowiązany (zgodnie z art. 52 ust. 3) ustosunkować się do niego na piśmie w terminie 30 dni od daty otrzymania.

Wystąpienia są ważnym instrumentem w kształtowaniu i podnoszeniu poziomu ochrony danych osobowych. Zawarte w nich wnioski o zmianę obowiązujących regulacji prawnych lub o wprowadzenie nowych norm dotyczących przetwarzania danych osobowych albo wskazujące na konieczność zmodyfikowania praktyk stosowanych w podmiotach, do których są skierowane, wskazują na prawidłowy sposób postępowania i zapewniania zgodności z RODO.

W 2024 roku Prezes UODO wystosował **14 wystąpień** z określonymi wnioskami do różnych podmiotów.

Ważniejsze wystąpienia przygotowane w związku z opiniowaniem projektów ustaw zostały omówione w części „Opiniowanie projektów aktów prawnych dotyczących ochrony danych osobowych". Były to wystąpienia do:

- **Ministra Cyfryzacji**[441] o podjęcie prac legislacyjnych prowadzących do **zmiany przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej**,
- **Ministra Finansów**[442] w sprawie **nowelizacji ustawy o Krajowej Administracji Skarbowej** w związku ze **zbyt szerokimi i za bardzo ogólnie określonymi uprawnieniami KAS dotyczącymi dostępu do danych obywateli,**
- **Ministra Cyfryzacji**[443] z wnioskiem o zainicjowanie **korekty ustawy o doręczeniach elektronicznych**,
- **Ministra Sprawiedliwości**[444] z wnioskiem o dostosowanie **ustawy o ochronie małoletnich** do zasad ochrony danych osobowych.

Inne ważne wystąpienie Prezes UODO skierował do Ministra do spraw Unii Europejskiej[445]. Zostało ono przygotowane w związku z tym, że w ocenie organu nadzorczego **nie wszystkie wyroki TSUE zostały odpowiednio transponowane do prawa krajowego**. Dlatego Prezes UODO zwrócił się o przekazanie informacji o planowanych zmianach legislacyjnych, stosownie do treści wyroków TSUE, co do których Prezes UODO wskazywał, że wymagają dokonania zmian w polskim prawie. W odpowiedzi Minister do spraw Unii Europejskiej zaznaczył, że odpowiedzialność za wdrożenie wyroków TSUE spoczywa na ministrach właściwych merytorycznie ze względu na tematykę danej sprawy. Spośród 6 wyroków wskazanych przez Prezesa UODO, tylko w odniesieniu do 2 zidentyfikowano konieczność dokonania zmiany w przepisach krajowych. W związku z tym organ nadzorczy planuje w 2025 r. skierowanie wystąpień bezpośrednio do poszczególnych resortów, wskazując konkretne wyroki, które, w jego opinii, powodują konieczność dokonania zmian legislacyjnych w przepisach krajowych.

Trzy kolejne wystąpienia były reakcją na sygnały otrzymane od inspektorów ochrony danych.

---

[441] DOL.413.3.2024.
[442] DOL.413.5.2024.
[443] DOL.413.7.2024.
[444] DOL.413.9.2024; treść wystąpienia i jego omówienie dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3377.
[445] DOL.413.14.2024.

W wielu przypadkach inspektorzy są dla Urzędu źródłem informacji na temat funkcjonowania przepisów prawa i zidentyfikowanych problemów wynikających np. z luk lub nieścisłości tych przepisów. W takich sytuacjach IOD oczekują od UODO interwencji, np. skierowania odpowiedniego wystąpienia. W wielu przypadkach organ nadzorczy je kieruje i monitoruje ich efekty. 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. Dzięki takiej współpracy możliwe jest wspólne poszukiwanie rozwiązań zauważonych problemów.

Przykładem takiej współpracy był sygnał od inspektora ochrony danych dotyczący konieczności zmiany przepisów prawa w zakresie likwidacji depozytów niepodjętych przez pacjentów. Problem polega na tym, że szpitale, będące jednostkami sektora finansów publicznych, chcąc zlikwidować depozyty niepodjęte przez pacjentów, zobowiązane są m.in. do publikacji danych osobowych tych pacjentów w dzienniku poczytnym w danej miejscowości lub w Biuletynie Informacji Publicznej. Wymaga tego od nich ustawa o likwidacji niepodjętych depozytów[446]. W ten sposób placówka lecznicza (np. szpital psychiatryczny) ujawnia, że określona osoba była jej pacjentem i tym samym pośrednio ujawnia dane dotyczące zdrowia tej osoby. W ocenie Prezesa UODO upublicznienie takich danych prowadzić może do przetwarzania danych osobowych w zakresie nieproporcjonalnym do wyznaczonego celu, jakim jest zwrot depozytu, a zatem do naruszenia zasad ochrony danych, w tym zasady minimalizacji danych. Z tego powodu konieczne jest dostosowanie obowiązujących obecnie regulacji prawnych w **zakresie likwidacji niepodjętych depozytów** do zasad ochrony danych osobowych. O podjęcie działań legislacyjnych w tym zakresie Prezes UODO zaapelował w wystąpieniu skierowanym 26 listopada 2024 r. **do Ministra Zdrowia**[447].

Było to drugie wystąpienie w tej sprawie. Pierwsze wystosowano w 2022 r. i zostało ono przesłane również do wiadomości Rzecznika Praw Pacjenta. W odpowiedzi na to pierwsze wystąpienie Ministerstwo Zdrowia wskazało, że wspólnie z Rzecznikiem Praw Pacjenta prowadzi analizę przedmiotowego zagadnienia. Ponadto Ministerstwo zadeklarowało, że informacja o przygotowanych rozwiązaniach zostanie przekazana po podjęciu ostatecznej decyzji w ramach procesu opiniowania aktów prawnych. Prezes UODO nie otrzymał jednak propozycji rozwiązań legislacyjnych w powyższym zakresie ani też informacji co do ostatecznej decyzji resortu. Dlatego ponowił swoje wystąpienie w tej sprawie.

Prezes UODO ponownie zwrócił się również do **Ministra Edukacji** o podjęcie prac legislacyjnych prowadzących do **zmiany art. 90l ustawy o systemie oświaty** celem dostosowania go do zasad ochrony danych osobowych określonych w art. 5 RODO[448]. Zgodnie z art. 90l ustawy o systemie oświaty, osoby fizyczne i osoby prawne

[446] Ustawa z 18 października 2006 r. o likwidacji niepodjętych depozytów (Dz.U. Nr 208, poz. 1537 ze zm.).
[447] Wystąpienie z 26 listopada 2024 (DOL.413.19.2022), dostępne pod linkiem: https://uodo.gov.pl/pl/138/3454.
[448] DOL.413.4.2023.

inne niż jednostki samorządu terytorialnego, przyznające uczniom ze środków własnych 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.

Przy stosowaniu powołanego przepisu wątpliwości budzi przede wszystkim to, czy i w jakim w 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. W praktyce bowiem, wobec braku regulacji uszczegóławiających procesy przetwarzania danych w przepisach ustawy o systemie oświaty, zasady przetwarzania danych są kształtowane wyłącznie w regulaminach przyznawania stypendiów. Mocą postanowień regulaminowych na szkoły branżowe (np. kolejowe, górnicze) nakładane są zadania polegające na przykład na: dokonywaniu przez nie wyboru stypendystów, wystawianiu uczniom skierowań na badania lekarskie, weryfikowaniu spełniania przez uczniów kryteriów przyznania stypendium za wyniki w nauce lub za osiągnięcia sportowe już po jego przyznaniu.

Działania takie są nierozerwalnie związane z koniecznością przetwarzania danych osobowych przez szkoły w celach innych niż te, które szkoły realizują w związku ze swoimi ustawowymi zadaniami i – co istotne – dotyczą nie tylko przetwarzania danych zwykłych, ale i danych szczególnych kategorii, np. o stanie zdrowia.

Art. 90l o systemie oświaty jest jedynym przepisem krajowym, który odnosi się do ukształtowania procesów przetwarzania danych osobowych związanych z realizacją celu w nim wskazanego. Taka regulacja jest jednak niewystarczająca z punktu widzenia zasad ochrony danych osobowych dla zapewnienia osobom, których dane dotyczą, odpowiednich gwarancji poszanowania ich praw i wolności. Ponadto podstawa prawna powinna zawierać przepisy szczegółowe dostosowujące stosowanie przepisów rozporządzenia 2016/679, 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.

Kwestionowany przepis 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 ustawie o systemie oświaty i ustawie Prawo oświatowe brak jest przepisów, które uprawniałyby szkoły do przetwarzania danych osobowych uczniów w celach związanych z przyznawaniem im stypendiów w trybie art. 90l ustawy o systemie oświaty, w tym udostępniania tych danych na rzecz innych podmiotów i dla realizacji ich celów, co budzi wątpliwości zwłaszcza w kontekście wskazanej wyżej zasady zgodności z prawem. Co więcej, rozporządzenie 2016/679 stawia administratorom przetwarzającym dane osobowe

dzieci szczególne wymagania, zwłaszcza co do warunków ich pozyskania. Jak wskazano w motywie 38 RODO, dzieci wymagają szczególnej ochrony danych osobowych, gdyż mogą być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.

Kolejne istotne zagadnienia to **brak wyodrębnienia IOD w tabeli grup stanowisk urzędniczych odnoszącej się do korpusu służby cywilnej**. Problem ten podnoszony był wielokrotnie podczas spotkań Prezesa UODO z inspektorami ochrony danych odbywających się w 2024 r. Dyrektor Generalna w Ministerstwie Zdrowia zaapelowała o ponowne podjęcie przez Prezesa UODO działań zmierzających do wyodrębnienia stanowiska IOD.

Prezes UODO, kierując kolejne już w tym temacie wystąpienie **do Szefowej Służby Cywilnej**[449]**,** podkreślił, że brak stanowiska inspektora ochrony danych w wykazie stanowisk przede wszystkim utrudnia zatrudnienie na odrębnym stanowisku inspektora ochrony danych, a także powoduje przypisywanie obowiązków IOD w formie dodatkowych zadań już zatrudnionym pracownikom, nawet w sytuacjach, gdy może to powodować konflikt interesów (art. 38 ust. 6 rozporządzenia 2016/679). W takiej sytuacji pracodawcy trudno jest zapewnić, aby IOD podlegał najwyższemu kierownictwu (art. 38 ust. 3 rozporządzenia 2016/679). Dlatego brak stanowiska inspektora ochrony danych w wykazie stanowisk wyklucza lub utrudnia przyjmowanie rozwiązań gwarantujących IOD niezależne i skuteczne wykonywanie tej funkcji. Sytuacja taka może niekorzystnie wpływać na poziom ochrony danych osobowych w podmiotach publicznych (w tym organach administracji rządowej oraz urzędach zatrudniających pracowników należących do korpusu służby cywilnej).

Prezes UODO wskazał, że zamieszczenie określonego stanowiska w wykazie nie oznacza obowiązku jego tworzenia. Natomiast jego brak w wykazie utrudnia zatrudnienie na stanowisku inspektora ochrony danych w większych instytucjach, np. w ministerstwach, urzędach centralnych czy urzędach wojewódzkich. Uzasadniając swoje stanowisko, odwołał się do obowiązku zapewnienia przez administratora niezależnego i prawidłowego wykonywania funkcji IOD, m.in. zapewnienia bezpośredniej podległości IOD najwyższemu kierownictwu oraz zakaz nakładania na inspektora innych zadań i obowiązków, jeśli mogłyby one spowodować konflikt interesów.

Łączenie funkcji IOD z innymi obowiązkami może powodować konflikt interesów (o którym mówi art. 38 ust. 6 RODO), a tym samym utrudniać prawidłowe wykonywanie zadań inspektora oraz realizację innych zadań, gdy wystąpi pomiędzy nimi sprzeczność.

Prezes UODO przypomina, że RODO zobowiązuje kierownictwo podmiotu publicznego w każdej konkretnej sytuacji do starannego przeanalizowania, czy jakiekolwiek inne zadania, czy funkcje, jakimi administrator zamierzałby obarczyć inspektora, nie utrudniłyby mu właściwego wykonywania obowiązków określonych w art. 39 RODO. Konflikt interesów następuje m.in. wtedy, gdy nie można pogodzić

[449] Ponowne wystąpienie dot. wyodrębnienia stanowiska IOD w służbie cywilnej - DOL.413.6.2023, zob. (https://uodo.gov.pl/pl/138/3217).

prawidłowego wykonywania zadań inspektora z realizacją innych zadań, gdyż występuje pomiędzy nimi sprzeczność uniemożliwiająca odpowiednią ich realizację. Konflikt interesów może także wystąpić w związku z nadmiarem obowiązków powierzonych do realizacji IOD.

Problem ten staje się szczególnie istotny w kontekście nowych obowiązków ustawowych nakładanych na podmioty publiczne, z których przynajmniej część może dodatkowo obciążyć IOD.

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[450],
- upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO[451],
- 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[452].

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

Organ nadzorczy był organizatorem wielu inicjatyw, poświęconych aktualnym zagadnieniom związanym ze stosowaniem przepisów RODO w różnych obszarach życia zawodowego i prywatnego obywateli. Organizował punkty konsultacyjno-informacyjne w JST, spotkania, konferencje, nieodpłatne szkolenia, warsztaty czy webinaria z zakresu ochrony danych osobowych, skierowane do instytucji publicznych oraz innych podmiotów zainteresowanych podnoszeniem swoich kwalifikacji w tym obszarze. Prezes UODO angażował się w liczne przedsięwzięcia, udzielając im patronatu (załącznik nr 2), oraz wspierał swoją wiedzą ekspercką wiele wydarzeń krajowych i międzynarodowych, których wykaz znajduje się w załączniku nr 3.

[450] Art. 57.1.b RODO.
[451] Art. 57.1.d RODO.
[452] Art. 57.1.e RODO.

1.1. Kampanie edukacyjne

1) XVIII Dzień Ochrony Danych Osobowych

Przypadające co roku **28 stycznia** święto Dzień Ochrony Danych Osobowych, zostało ustanowione przez Komitet Ministrów Rady Europy dla upamiętnienia rocznicy otwarcia do podpisu Konwencji 108 Rady Europy w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych – pierwszego prawnie wiążącego instrumentu międzynarodowego chroniącego prywatność w erze cyfrowej. Z tej okazji w całej Europie organizowane są różne wydarzenia poświęcone aktualnym zagadnieniom związanym z prawem do prywatności i ochrony danych osobowych, informujące obywateli o zakresie ich praw i obowiązków oraz zagrożeniach związanych z przetwarzaniem dotyczących ich danych osobowych w związku z rozwojem technologicznym.

RODO i technologie były tematem przewodnim XVIII Dnia Ochrony Danych Osobowych.

Przebieg wydarzeń zorganizowanych w 2024 r. przez Urząd Ochrony Danych Osobowych z okazji tego święta przedstawiał się następująco:

1. Warsztaty dla seniorów na temat bezpiecznego korzystania ze zdobyczy nowych technologii podczas codziennych czynności (8.01.2024 r.).
2. Warsztaty dla studentów „Bezpieczna droga przez cyberprzestrzeń: od deepfake'ów po bezpieczeństwo aplikacji mobilnych" (10.01.2024 r.).
3. List otwarty Prezesa Urzędu Ochrony Danych Osobowych do uczestników XIV edycji programu „Twoje dane – Twoja sprawa" w związku z organizowanymi w szkołach obchodami Dnia Ochrony Danych Osobowych (10.01.2024 r.).
4. Cykl debat dotyczących ochrony danych osobowych w sektorze zdrowia w dobie rozwoju nowych technologii, zorganizowanych w Akademii Ekonomiczno-Humanistycznej w Warszawie (16.01.2024 r.):
   - I debata – Kodeksy postępowania,
   - II debata – Monitoring pracowników,
   - III debata – Wykorzystanie nowych technologii w ochronie zdrowia.
5. Punkty konsultacyjne dla Inspektorów Ochrony Danych oraz porady prawne dla obywateli zorganizowane w siedzibie UODO (29.01.2024 r.).
6. Webinarium online z cyklu „Certyfikacja w ochronie danych" (30.01.2024 r.).
7. #ODOlekcja – zajęcia online dla uczniów szkół ponadpodstawowych, pt. „Deepfake: fałszywa rzeczywistość w sieci – czy jesteś na to gotowy?" (30.01.2024 r.).

8. Gra terenowa „O dane dbam codziennie” dla uczniów szkoły podstawowej, zorganizowana przez harcerzy z 200. Grunwaldzkiej Warszawskiej Drużyny Harcerskiej „Leśnicy” w Warszawie i UODO (12.02.2024 r.).

Wzorem lat ubiegłych do współorganizacji tego święta włączyły się szkoły wyższe, z którymi Prezes Urzędu Ochrony Danych Osobowych zawarł porozumienia o współpracy, organizując konferencje z udziałem ekspertów UODO:

- Ogólnopolska Konferencja Naukowa „Aktualne wyzwania ochrony danych” na WPiA UMK w Toruniu[453] (19.01.2024 r.).
- X Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej, podczas którego odbyła się konferencja tematyczna połączona z promocją dobrych praktyk w zakresie ochrony danych osobowych[454] (1.02.2024 r.).
- Akademia Policji w Szczytnie zamieściła na swojej stronie internetowej post o XVIII Dniu Ochrony Danych Osobowych, zachęcając do udziału w wydarzeniach zorganizowanych z okazji tego święta[455].

W wykazie wydarzeń towarzyszących obchodom XVIII Dnia Ochrony Danych Osobowych znalazła się również Konferencja Rzeczowo o Prawie: „Praktyczne aspekty naruszeń ochrony danych osobowych. Wykrycie, ocena, zgłoszenie – badanie i procedury”, zorganizowana przez Lubasz i Wspólnicy – Kancelarię Radców Prawnych sp. k., Fundację Centrum Cyfrowe oraz Aigorithmics sp. z o.o. (25.01.2024 r.).

Ważnym punktem obchodów XVIII Dnia Ochrony Danych Osobowych była wspomniana już uroczystość wręczenia nagrody im. Michała Serzyckiego, Generalnego Inspektora Ochrony Danych Osobowych III kadencji, przyznawanej w uznaniu zasług na polu edukacji i popularyzacji idei ochrony danych osobowych.

Obchody Dnia Ochrony Danych Osobowych stanowią doskonałą okazję do promowania świadomego i odpowiedzialnego korzystania z technologii. Edukacja w tym zakresie jest kluczowa, szczególnie w kontekście coraz większych wyzwań związanych z postępem technologicznym.

2) UODO partnerem kampanii społecznej UOKiK, 15.03.2024 r.

15 marca to Światowy Dzień Konsumenta. Z tej okazji Urząd Ochrony Konkurencji i Konsumentów rozpoczął kampanię społeczną pt. „Inwestujesz? Daj sobie czas. Sprawdzaj, czytaj, pytaj!”, której celem było zwrócenie uwagi społeczeństwa na zjawiska mogące stanowić istotne zagrożenie dla interesów konsumentów. Realizacja kampanii była podyktowana koniecznością przeprowadzenia działań informacyjnych dotyczących produktów finansowych z wykorzystaniem fałszywych wizerunków znanych osób i firm nieuczciwie

[453] https://sknodo.umk.pl/?task=news&action=one&id=7.
[454] https://uodo.gov.pl/pl/138/2982.
[455] https://akademiapolicji.edu.pl/aktualnosci/2203-28-stycznia-dzien-ochrony-danych-osobowych.

obiecujących bezpieczne inwestowanie. Wskutek takich działań konsumenci mogli utracić środki finansowe. Urząd Ochrony Danych Osobowych był partnerem kampanii.

W grudniu 2024 r. UOKiK zaprosił Urząd Ochrony Danych Osobowych do współpracy w ramach kampanii społecznej pod nazwą „Sprawdź, czy Cię stać!", skierowanej głównie do seniorów – grupy najbardziej bezbronnej i podatnej na wszelkiego rodzaju reklamy pseudopromocyjne oraz scam. Celem tej kampanii było zwrócenie uwagi na prawa ludzi starszych do rzetelnej informacji na temat oferowanych produktów i usług oraz uczulenie ich na niebezpieczeństwa związane z możliwością utraty danych osobowych i tożsamości, będących efektem oddziaływania oszukańczych reklam.

3) UODO na 6. Warszawskiej Olimpiadzie Seniorów, 21.09.2024 r.

W czasie 6. Warszawskiej Olimpiady Seniorów zorganizowanej przez Urząd Miasta Warszawy, eksperci UODO udzielali porad prawnych z zakresu ochrony danych osobowych w specjalnym punkcie informacyjnym w Ośrodku Hutnik. Współczesna technologia, która otwiera ogromne możliwości w zakresie dostępu do informacji, kontaktu z bliskimi, korzystania online z usług i wygodnych zakupów, stwarza również ryzyko wyłudzeń danych osobowych, wymyślnych oszustw i cyberataków, które mogą być szczególnie groźne dla seniorów. Podczas spotkania eksperci UODO przekazali wskazówki, które pozwolą seniorom na bezpieczne poruszanie się w cyfrowej rzeczywistości, bez obaw o utratę prywatności[456].

4) UODO na Olimpiadzie dla przedszkolaków, 26.09.2024 r.

Zorganizowane przez Urząd Miasta Warszawy (Społeczne Centrum Sportu Aktywna Warszawa) wydarzenie pod nazwą „Olimpiada dla przedszkolaków", rozpoczęło się od symbolicznego zapalenia znicza olimpijskiego. Przedszkolaki miały okazję sprawdzić swoje umiejętności w licznych konkurencjach sportowych. Równie ważnym elementem tego wydarzenia była edukacja dzieci w zakresie ochrony danych osobowych, którą eksperci Urzędu Ochrony Danych Osobowych dostosowali do wieku najmłodszych uczestników. Przygotowane zostało specjalne stanowisko informacyjne, gdzie dzieci mogły w przystępny sposób dowiedzieć się, czym jest prywatność i jak dbać o dane osobowe. W wydarzeniu wzięło udział około 300 dzieci z 10 przedszkoli[457].

5) Warsztaty dla dzieci poszkodowanych w powodzi, 27.09.2024 r.

Na zaproszenie Fundacji „Odzyskaj siebie" oraz Centrum Reset przedstawicielki Urzędu Ochrony Danych Osobowych spotkały się z dziećmi z Paczkowa, poszkodowanymi w powodzi. Głównym celem tego spotkania była edukacja dzieci w zakresie prawa do prywatności i ochrony danych osobowych. Podczas warsztatów zaprezentowane zostały interaktywne materiały edukacyjne przygotowane przez

[456] https://uodo.gov.pl/pl/138/3358.
[457] https://uodo.gov.pl/pl/138/3371.

Urząd Ochrony Danych Osobowych, które przybliżyły uczestnikom kluczowe zagadnienia związane z nowymi technologiami. W ramach spotkania omówiono zarówno podstawowe, jak i bardziej zaawansowane pojęcia technologiczne, takie jak cyfryzacja, sztuczna inteligencja, big data, czy Internet Rzeczy (IoT). W drugiej części spotkania uczestnicy warsztatów przygotowali plakaty dotyczące szans i zagrożeń związanych ze sztuczną inteligencją. Młodzież analizowała zarówno pozytywne aspekty rozwoju AI, takie jak możliwości automatyzacji i usprawnienia codziennych czynności, jak i potencjalne zagrożenia, w tym ryzyko manipulacji danymi oraz wpływ na prywatność. Na plakatach znalazły się również wskazówki dotyczące bezpiecznego korzystania z nowych technologii, w tym, jak chronić swoje dane osobowe, stosując silne hasła i uważając na to, jakie informacje udostępniamy w sieci. Warsztaty dostarczyły najmłodszym wskazówek, gdzie można szukać pomocy i informacji w razie problemów z naruszeniem prywatności czy cyberzagrożeniami. Temat zajęć edukacyjnych oraz dyskusja z uczestnikami spotkania miały na celu uświadomienie młodym ludziom, czym są dane osobowe oraz to, że dane te stanowią wartość samą w sobie.

6) Warsztaty edukacyjne dla dzieci w ramach programu „Lekcje o finansach", 1,3,18.10.2024 r.

W siedzibie Urzędu Ochrony Danych Osobowych odbyły się zajęcia edukacyjne dla uczniów szkół podstawowych z Wielkopolski, Śląska i Pomorza. Wydarzenie zostało zorganizowane w ramach Programu „Lekcje o finansach" na zaproszenie Ministerstwa Finansów. Celem Programu było wsparcie realizacji działań z zakresu edukacji finansowej wśród uczniów szkół podstawowych. UODO, jako instytucja zaangażowana w edukację, regularnie wspiera tego typu inicjatywy, dzieląc się swoją ekspercką wiedzą z zakresu ochrony danych osobowych. W ramach tego programu Urząd gościł ok. 120 uczniów z różnych stron Polski, którzy mieli okazję uczestniczyć w specjalnie dla nich przygotowanych zajęciach. Podczas spotkania uczniowie dowiedzieli się, jak dużą wartość stanowią dane osobowe, że nie są one jedynie informacjami o nas lub innych ludziach, ale stanowią również nasze dobro osobiste. Zajęcia pozwoliły dzieciom zrozumieć, jak ważne jest dbanie o prywatność oraz jakie prawa przysługują im w zakresie ochrony dotyczących ich danych osobowych.

7) Międzynarodowy Dzień Praw Człowieka, 10.12.2024 r.

Obchodzona co roku 10 grudnia rocznica uchwalenia przez Zgromadzenie Ogólne ONZ Powszechnej Deklaracji Praw Człowieka, w 2024 roku odbywała się pod hasłem „Nasze prawa, nasza przyszłość, już teraz". Motto obchodów nawiązuje do podejmowanych aktywności UODO, w których podkreśla wagę praw jednostki, szczególnie jej prawa do prywatności, oraz wskazuje na konieczność realizacji przez organ nowych zadań i funkcji dotyczących pośrednictwa danych i rejestracji organizacji altruizmu danych.

Dla uczczenia Międzynarodowego Dnia Praw Człowieka, Urząd Ochrony Danych Osobowych zorganizował webinarium „Prawa człowieka i dane osobowe: Co musisz

wiedzieć?”. Webinarium skierowane było do uczniów klas 7-8 szkół podstawowych oraz ponadpodstawowych, uczestniczących w programie „Twoje dane – Twoja sprawa”.

Prezes UODO i jego przedstawiciele uczestniczyli ponadto w innych wydarzeniach zorganizowanych w ramach tego święta:

- w konferencji Rzeczniczki Praw Dziecka zorganizowanej w związku z kampanią „Więcej szacunku dla młodego wizerunku”,
- w XV Warszawskim Seminarium Praw Człowieka poświęconym roli Europejskiej Konwencji Praw Człowieka i Europejskiego Trybunału Praw Człowieka we wzmacnianiu instytucji demokratycznych,
- w spotkaniu inspektorów ochrony danych osobowych (IOD) zorganizowanym przez Kościelnego Inspektora Ochrony Danych przy Konferencji Episkopatu Polski i Instytut „Bona Fama”, podczas którego przedstawiciel UODO przeprowadził szkolenie nt. aktualnych zagadnień związanych z ochroną danych osobowych w obowiązujących przepisach prawa.

8) Kampania „Więcej szacunku dla młodego wizerunku”, 10.12.2024 r.

Celem kampanii Rzecznika Praw Dziecka, w której wziął udział Prezes UODO, było zwrócenie uwagi na problem nadmiernego i nieuważnego publikowania zdjęć młodych osób w sieci. Kampania rozpoczęła się podczas konferencji w Liceum Artes Liberales w Warszawie 10 grudnia 2024 r., w której Prezes UODO podkreślił konieczność prowadzenia szeroko zakrojonych akcji edukacyjnych, uświadamiających młodym ludziom i ich opiekunom wagę ochrony danych osobowych, w tym ich wizerunku, w wirtualnej przestrzeni. W ramach tej kampanii Urząd Ochrony Danych Osobowych zorganizował webinarium „Więcej szacunku dla młodego wizerunku. Ochrona wizerunku młodych osób w sieci” (18.12.2024 r.), w którym z prelekcją wystąpił Inspektor Ochrony Danych UODO. Podczas spotkania poruszono kwestię publikowania zdjęć i nagrań z wizerunkami dzieci i młodzieży oraz legalności takich działań m.in. pod kątem regulacji dot. ochrony dóbr osobistych, danych osobowych i prywatności. Istotne w tym kontekście były próby przyjrzenia się, jak tego rodzaju praktyki postrzegane są z punktu widzenia samych dzieci, m.in. jak wpływają na ich samopoczucie i czy nie podważają ich poczucia bezpieczeństwa i prawa do samostanowienia.

1.2. Współpraca ze szkołami wyższymi

W 2024 r. Prezes Urząd Ochrony Danych Osobowych kontynuował współpracę ze szkołami wyższymi i organizacjami studenckimi. Podczas akcji „UODO rusza w kraj”, dzięki gościnności Uniwersytetu Ekonomicznego w Katowicach, współorganizował w siedzibie tej uczelni konferencję naukową „Bezpieczeństwo informacji i jej zasobów” (20-21.11.2024 r.).

Udzielił patronatu i ufundował nagrody dla finalistów Ogólnopolskiego Konkursu Prawa Europejskiego, którego organizatorami były ELSA Poland i ELSA Łódź. Natomiast 13 grudnia 2024 r. zorganizował w Urzędzie Ochrony Danych Osobowych

konwersatorium dla studentów Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, podczas którego Profesor Agnieszka Grzelak, zastępczyni Prezesa UODO, przedstawiła wyzwania dla ochrony danych osobowych w dobie rozwoju nowych technologii i nawiązała do nowych regulacji w tym zakresie. Studenci wysłuchali też wykładu na temat ochrony danych osobowych w związkach wyznaniowych na tle dotychczasowych doświadczeń UODO i perspektyw na przyszłość.

1.3. Społeczny Zespół Ekspertów przy Prezesie UODO

Prezes Urzędu Ochrony Danych Osobowych powołał 4 czerwca 2024 r. Społeczny Zespół Ekspertów (SZE), który rozpoczął działanie przy Prezesie Urzędu Ochrony Danych Osobowych. Tego samego dnia odbyło się pierwsze spotkanie Zespołu będącego społecznym ciałem opiniodawczo-doradczym Prezesa Urzędu. Uroczyste wręczenie nominacji odbyło się podczas konferencji zorganizowanej przez UODO pt. „Ochrona danych osobowych w UE. Dokąd zmierzamy w przededniu wyborów europejskich?".

Zadaniem nowo powołanego zespołu jest wspieranie Prezesa Urzędu w realizacji jego zadań określonych przepisami prawa, w szczególności w zakresie doradztwa i wyrażania opinii w sprawach przedstawionych Zespołowi, rekomendowanie i inicjowanie działań w obszarze ochrony danych osobowych oraz przygotowywanie – w porozumieniu z Prezesem UODO – ekspertyz i stanowisk w zakresie dotyczącym ochrony danych osobowych. Członkowie Zespołu będą też promowali dobre praktyki oraz wykonywali inne zadania, zlecone przez Prezesa Urzędu, dotyczące ochrony danych osobowych, szczególnie w obszarze nowych technologii.

Jednym z pierwszych zadań SZE, realizowanym równolegle z toczącymi się konsultacjami społecznymi, były prace w zakresie aktualizacji dwóch poradników – o przetwarzaniu danych osobowych w zatrudnieniu oraz o zgłaszaniu naruszeń ochrony danych osobowych. Wśród innych tematów znalazły się kwestie dotyczące przetwarzania danych osobowych w związku ze zbliżającym się wejściem w życie ustawy o sygnalistach oraz rosnące zagrożenia cyberbezpieczeństwa, które są nierozerwalnie związane z przetwarzaniem danych osobowych. Ochronę danych osobowych należy traktować jako istotny element systemu bezpieczeństwa i obronności kraju, dlatego UODO wraz z Zespołem będzie pracować nad propozycjami w tym zakresie, w szczególności dotyczącymi analizy ryzyk, z którymi mogą spotkać się administratorzy w poszczególnych branżach.

W analizowanym 2024 roku członkowie Zespołu uczestniczyli w 38 konferencjach/seminariach i spotkaniach roboczych, byli współorganizatorami 14 wydarzeń, odbyli 6 wykładów w ramach webinariów eksperckich oraz konsultantami 5 dokumentów. Pełny wykaz aktywności Społecznego Zespołu Ekspertów jest opublikowany i na bieżąco aktualizowany w specjalnej zakładce na stronie internetowej UODO[458].

[458] https://uodo.gov.pl/pl/582.

Koncepcja Społecznego Zespołu Ekspertów to wyraz otwarcia Urzędu na środowiska eksperckie i potrzeba stawienia czoła wyzwaniom związanym z ochroną danych osobowych w dobie dynamicznego rozwoju nowych technologii. W skład Społecznego Zespołu Ekspertów, z chwilą jego powstania, wchodziło 15 wybitnych znawców tematu ochrony danych osobowych, specjalizujących się w zagadnieniach prawnych, legislacyjnych, a także nowych technologii i nauki[459]. Przewodniczącym Zespołu został dr Mirosław Gumularz. Udział w pracach SZE ma charakter społeczny.

1.4. Szkolenia

1.4.1. Szkolenie przedstawicieli policji, 30.09.2024 r.

Na zaproszenie Komendanta Głównego Policji, pracownicy Departamentu Kontroli i Naruszeń UODO przeprowadzili 30 września 2024 r. szkolenie dla przedstawicieli policji pt. „Naruszenia ochrony danych – studium przypadku". Podczas prezentacji zagadnień dotyczących tego tematu wskazano najczęstsze błędy popełniane przez administratorów oraz omówiono wybrane decyzje, które organ wydał w związku z naruszeniem przepisów o ochronie danych.

1.4.2. Szkolenie koordynatorów Programu „Twoje dane – Twoja sprawa", 24–25.10.2024 r.

Cyklicznymi szkoleniami organizowanymi od 15 lat przez UODO są szkolenia realizowane w ramach ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa". 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 zajęć tematycznych z uczniami.

Dwudniowe szkolenie dla koordynatorów ogólnopolskiego Programu „Twoje dane – Twoja sprawa", które odbyło się 24–25.10.2024 r. rozpoczęło jego XV edycję. W szkoleniu wzięło udział 150 koordynatorów, nauczycieli i dyrektorów szkół, którzy angażują się w działania edukacyjne na rzecz ochrony danych osobowych, skierowane nie tylko do uczniów, ale również rodziców i lokalnej społeczności[460]. W programie szkolenia znalazły się m.in. wystąpienia dotyczące nauczania o RODO w praktyce, mediacji jako metody rozwiązywania konfliktów wynikających

[459] https://uodo.gov.pl/pl/138/3114. Skład Społecznego Zespołu Ekspertów został powiększony zarządzeniem Prezesa UODO z 23 stycznia 2025 r. o kolejnego członka. W chwili obecnej Zespół liczy 16 członków.
[460] https://uodo.gov.pl/pl/587/3316.

z niewłaściwego postępowania w mediach społecznościowych, prezentacje sceniczne uczniów w ramach konkursu „Twoje dane – Twoja sprawa”. Można też było uzyskać porady od pracownika Infolinii UODO dotyczące ochrony danych osobowych w sektorze oświaty. Szkolenie otwierające XV edycję Programu było okazją do wymiany doświadczeń, wiedzy i sprawdzonych rozwiązań na temat ochrony danych osobowych w edukacji. XV edycja Programu była realizowana w 352 placówkach w całej Polsce.

1.4.3. Szkolenie pełnomocników ds. otwartości danych, 18.12.2024 r.

Tematem szkolenia dla pełnomocników ds. otwartości danych w Ministerstwie Cyfryzacji była „Realizacja zasady poufności danych osobowych w praktyce udostępniania i przekazywania informacji sektora publicznego w celu ponownego wykorzystania”. Podczas tego spotkania przedstawione zostały praktyczne aspekty dokonywania analizy ryzyka dla zapewnienia bezpieczeństwa przetwarzanym danym osobowym, uwzględniające doświadczenia administratorów w związku ze zgłaszanymi incydentami bezpieczeństwa. Wiele uwagi poświęcono opisowi doświadczeń organu nadzorczego w związku z prowadzonymi postępowaniami administracyjnymi, których przedmiotem było zapewnienie bezpieczeństwa przetwarzania danych osobowych, odpowiedniego do ryzyka.

1.5. Projekty i programy

1.5.1. Ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa”

1) XIV edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa” w roku szkolnym 2023/2024 oraz rozpoczęcie XV edycji w roku szkolnym 2024/2025.

Program jest największym systemowym projektem edukacyjnym Prezesa Urzędu Ochrony Danych Osobowych realizowanym na skalę ogólnopolską, w którym uczestniczą szkoły podstawowe, ponadpodstawowe oraz placówki doskonalenia nauczycieli.

Program umożliwia uczniom i nauczycielom zdobywanie oraz rozwijanie praktycznych umiejętności w obszarze ochrony danych osobowych, 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. Uczestnicy otrzymują dostęp do platformy z materiałami edukacyjnymi, a także biorą udział w organizowanych przez UODO wydarzeniach. Praktyczne zajęcia służą budowaniu świadomości i rozumieniu zjawisk związanych z ochroną prywatności i danych osobowych oraz umiejętnemu stosowaniu nabytej wiedzy w życiu.

W roku 2024 Urząd Ochrony Danych Osobowych realizował XIV edycję Programu i rozpoczął jego XV edycję. Każda z nich organizowana jest zgodnie z kalendarzem roku szkolnego.

2) XIV edycja programu „Twoje dane – Twoja sprawa" – rok szkolny 2023/2024

XIV edycja programu edukacyjnego „Twoje dane – Twoja sprawa" była realizowana pod hasłem „Ochrona danych osobowych w mediach społecznościowych i nie tylko". Koncentrowała się na edukacji dzieci i młodzieży w obszarze ochrony prywatności i danych osobowych w mediach społecznościowych, ze szczególnym uwzględnieniem tematu dotyczącego ochrony wizerunku najmłodszych.

W roku szkolnym 2023/2024, w XIV edycji Programu, udział wzięły 303 placówki oświatowe, w tym 197 szkół podstawowych, 99 szkół ponadpodstawowych oraz 7 placówek doskonalenia nauczycieli. Rekrutacja uczestników rozpoczęła się 1 września 2024 r. Najwięcej zgłoszeń wpłynęło z województwa mazowieckiego:

- liczba placówek, które przystąpiły do Programu po raz pierwszy – 137,
- liczba uczestników kontynuujących współpracę kolejny rok – 166,
- liczba inicjatyw edukacyjnych – 4 519, w tym 3 164 lekcje poświęconych ochronie danych osobowych i prywatności,
- liczba uczniów biorących udział w zajęciach – 48 651,
- liczba przeszkolonych nauczycieli – 3 371,
- liczba nauczycieli zaangażowanych w działania – 1796.

3) #ODOlekcje – cykl webinariów dla uczniów

W cyklu zajęć zrealizowanych pod hasłem #ODOlekcje odbyło się 6 ogólnopolskich lekcji dla uczniów szkół podstawowych i ponadpodstawowych, w których udział wzięło blisko 15 000 uczestników z 656 klas. Atutami zajęć była formuła online, przykłady z życia codziennego oraz różnorodność tematów podkreślających rolę ochrony prywatności i danych osobowych w życiu, w szczególności w kontekście zagadnień związanych ze sztuczną inteligencją. Tematyka i sposób realizacji lekcji dostosowane były do wieku i potrzeb uczniów. Zajęcia prowadzili eksperci UODO, przedstawiciele zaproszonych instytucji oraz liderzy Programu.

- „To nie są ślady na piasku – cyfrowa tożsamość i cyfrowa reputacja w kontekście ochrony naszej prywatności i danych osobowych” (20.11.2023 r.),
- „Prawo do ochrony danych osobowych jako prawo człowieka” (8.12.2023 r.),
- „Deepfake: fałszywa rzeczywistość w sieci – czy jesteś na to gotowy?” (31.01.2024 r.),
- „DODO Agencja – biblijna interwencja” (7.02.2024 r.),
- „Nagrywanie oraz montowanie filmu na urządzeniach mobilnych cz. I” (14.03.2024 r.),
- „Nagrywanie oraz montowanie filmu na urządzeniach mobilnych cz. II”; warsztaty przygotowujące do wykonania prac konkursowych zorganizowane przy współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie (21.03.2024 r.),
- „Cyfrowy l@birynt – uważaj na pułapki w sieci” – webinarium odbyło się z udziałem przedstawicieli Urzędu Komunikacji Elektronicznej (16.04.2024 r.).

4) Dodatkowe inicjatywy edukacyjne UODO w ramach XIV edycji programu „Twoje dane – Twoja sprawa”

Szkolenia, materiały edukacyjne, webinaria oraz wsparcie ekspertów UODO przyczyniają się do wzrostu wiedzy oraz podniesienia kompetencji nauczycieli, dyrektorów szkół, pedagogów i inspektorów ochrony danych uczestniczących w Programie. W ramach jego XIV edycji zostały zorganizowane webinaria dla szkolnych koordynatorów Programu:

- dwudniowe szkolenie przygotowujące koordynatorów do realizacji Programu (25–26.10.2023 r.),
- warsztat dla nauczycieli „Jak dobrze zaplanować działania w ramach Programu? Narzędzia coachingu do pracy z celami”, z udziałem 33 uczestników (18.12.2023 r.),
- „RODO w szkolnej ławce. Wykorzystanie wizerunku dziecka – prawo i praktyka” – webinarium z udziałem 455 uczestników, skierowane do dyrektorów placówek oświatowych i nauczycieli. Wydarzenie to zorganizowane zostało przy współpracy z Biurem Rzecznika Praw Dziecka (15.05.2024 r.).

Przez cały rok uczestnicy Programu korzystali z konsultacji telefonicznych, podczas których mogli uzyskać odpowiedzi na nurtujące pytania.

Ponadto szkoły zaangażowały się w obchody Dnia Ochrony Danych Osobowych, organizując w okresie styczeń–luty 2024 r. różnorodne wydarzenia. Wśród nich znalazły się lekcje, apele, spotkania z ekspertami, szkolenia, konkursy, przedstawienia oraz gry i zabawy edukacyjne. Działania były skierowane zarówno do uczniów, jak i do szerszej społeczności, rodziców, nauczycieli oraz osób starszych. Uczniowie przygotowali także materiały edukacyjne, takie jak gazetki szkolne, prezentacje oraz

utwory literackie, poruszające tematykę ochrony danych osobowych i bezpieczeństwa w sieci. W sumie uczestnicy Programu zorganizowali 443 wydarzenia. W niektórych szkołach obchody Dnia Ochrony Danych Osobowych były połączone z Dniem Bezpiecznego Internetu[461].

5) Cykl porad „Warto wiedzieć" dla uczestników Programu

Cykl porad „Warto wiedzieć" skierowany jest do uczniów, uczennic, nauczycieli i rodziców, w celu przybliżenia istotnych kwestii dotyczących ochrony danych osobowych w krótkiej dostępnej i zrozumiałej formie dla uczniów i uczennic. Tematyka poruszona w przygotowanych materiałach w roku 2024 obejmowała następujące materiały:

- 27.02.2024 r. „Udostępnianie przez rodziców zdjęć dzieci w sieci, czyli kilka słów na temat sharenting'u",
- 23.05.2024 r. „Juice Jacking, czyli wyciskanie danych z urządzeń. Uważaj na publiczne porty USB",
- 3.06.2024 r. „Dzień Dziecka w erze cyfrowej: Jak w kilku krokach zadbać o prywatność i bezpieczeństwo najmłodszych online?",
- 27.12.2024 r. „Ryzyko udostępniania wizerunku dzieci w sieci",
- 26.11.2024 r. „Czym jest i jakie prawa daje nam RODO?".

Dzięki przekazanym poradom uczestnicy i uczestniczki mieli okazję zdobyć praktyczne wskazówki dotyczące ochrony swojej prywatności oraz bezpieczeństwa w sieci. Materiały były wykorzystywane podczas lekcji z uczniami i uczennicami oraz do przygotowania gazetek, a także zostały udostępnione na szkolnych stronach internetowych.

6) XV edycja programu „Twoje dane – Twoja sprawa", rok szkolny 2024/2025

Do XV edycji Programu przystąpiły 352 placówki oświatowe, w tym 221 szkół podstawowych, 127 szkół ponadpodstawowych oraz 4 placówki doskonalenia nauczycieli. Najwięcej uczestników pochodziło z województw: śląskiego (80 placówek) i mazowieckiego (67 placówek).

Szkoleniem online, które odbyło się 24–25.10.2024 r. zainaugurowana została XV edycja Programu. Jego celem było przygotowanie szkolnych koordynatorów do realizacji Programu, ze szczególnym uwzględnieniem tematyki związanej z ochroną wizerunku dzieci w Internecie. Eksperci Urzędu Ochrony Danych Osobowych, NASK Państwowego Instytutu Badawczego i Centralnego Biura Zwalczania Cyberprzestępczości omówili szczegóły realizacji Programu oraz kluczowe kwestie związane z cyberbezpieczeństwem i ochroną danych osobowych dzieci. Drugi dzień szkolenia poświęcony był wymianie doświadczeń, dobrych praktyk oraz innowacyjnych pomysłów nauczycieli na realizację działań edukacyjnych oraz odpowiedzi na

[461] Wykaz wydarzeń zorganizowanych przez szkoły i placówki doskonalenia nauczycieli jest udostępniony na stronie internetowej UODO pod adresem: https://uodo.gov.pl/tdts.

najważniejsze pytania dotyczące przetwarzania danych osobowych w sektorze oświaty.

W ramach XV edycji programu „Twoje dane – Twoja sprawa” Urząd Ochrony Danych Osobowych kontynuował również cykl zajęć ogólnopolskich dla uczniów szkół podstawowych i ponadpodstawowych pod hasłem „#ODOlekcje”. W 2024 r. odbyła się kolejna lekcja pt. „Prawa człowieka i dane osobowe: co musisz wiedzieć?” (10 grudnia 2024 r.). Ponadto koordynatorzy Programu wzięli udział w następujących webinariach:

- „Projektowanie prywatności na przykładzie internetu rzeczy (IoT) – perspektywa dostawcy i korzystającego” (6.12.2024 r.),
- „Więcej szacunku dla młodego wizerunku. Ochrona wizerunku młodych osób w sieci”, zorganizowanym przez Rzecznika Praw Dziecka z udziałem eksperta UODO (18.12.2024 r.).

Istotnym elementem działań edukacyjnych skierowanych do uczniów i ich opiekunów XV edycji Programu, było zwrócenie uwagi na kwestie związane z nadmiernym publikowaniem zdjęć i nagrań zawierających wizerunek dzieci.

Szczegóły XV edycji programu „Twoje dane – Twoja sprawa” zostaną opisane w następnym roku sprawozdawczym.

7) Podsumowanie i wnioski

Program „Twoje dane – Twoja sprawa” jest inicjatywą, która przyczynia się do podniesienia świadomości na temat ochrony danych osobowych w środowisku szkolnym, wzrostu zainteresowania tematem ochrony prywatności w życiu każdego człowieka oraz do kształtowania postaw odpowiedzialnego korzystania z technologii wśród młodego pokolenia**.** Uczniowie coraz lepiej rozumieją swoje prawa i obowiązki związane z ochroną danych osobowych oraz stosują zdobytą wiedzę w praktyce. Program umożliwia także podnoszenie kompetencji nauczycieli, dostęp do aktualnej i rzetelnej wiedzy, a także wymianę doświadczeń i najlepszych praktyk w zakresie edukacji o ochronie danych osobowych.

Realizowane działania obejmowały szeroki zakres tematyczny, wykraczający poza podstawę programową szkół i spotkały się z dużym zainteresowaniem zarówno uczniów, jak i nauczycieli. Prawie **49 000 uczniów** wzięło udział w zajęciach, a **ponad 5 000 nauczycieli** zostało przeszkolonych i zaangażowanych w działania. Odbyło się ponad **4 500 zajęć** i wydarzeń na rzecz popularyzacji wiedzy o ochronie danych osobowych, z których najciekawsze zostały wyróżnione i nagrodzone w ramach organizowanych przez Prezesa UODO. Przygotowano ofertę dostosowaną do uczniów w różnym wieku oraz zadbano, aby treści były dostosowane także do uczniów ze szczególnymi potrzebami.

Program został oceniony bardzo pozytywnie zarówno przez uczniów, jak i nauczycieli. Uczestnicy podkreślali jego wartość edukacyjną oraz aktualność poruszanych tematów. Stanowił on doskonałe uzupełnienie podstawy programowej w szkołach, dostarczając wiedzy niezbędnej w świecie cyfrowym. Program aktywnie

angażował uczestników, dzięki różnorodnym materiałom dydaktycznym i formom zajęć, co zwiększyło ich zaangażowanie oraz zainteresowanie.

Uczniowie docenili praktyczny charakter zajęć oraz możliwość dzielenia się własnymi doświadczeniami. Zdobyli praktyczną wiedzę na temat ochrony danych osobowych, co pozwoli im na bezpieczniejsze korzystanie z internetu, natomiast nauczyciele zyskali narzędzia i wiedzę niezbędne do prowadzenia zajęć na ten temat. Podkreślali znaczenie tematyki ochrony danych osobowych w edukacji i wyrażali chęć kontynuowania Programu w kolejnych latach. Program przyczynił się do zmiany postaw uczestników, którzy bardziej świadomie podchodzą do kwestii ochrony prywatności w sieci. Ciekawe i interaktywne formy prowadzenia zajęć, a także organizacja wydarzeń tematycznych, przyczyniły się do zwiększenia zaangażowania uczestników oraz zasięgu Programu.

Wśród rekomendacji znalazły się takie propozycje, jak dostosowanie materiałów do różnych grup wiekowych oraz poszerzenie bazy o dodatkowe materiały dydaktyczne. Sugerowane jest również rozszerzenie tematyki Programu o kolejne zagadnienia związane z bezpieczeństwem dzieci i nowymi technologiami. Ważne jest także zwiększenie zasięgu Programu poprzez współpracę z różnymi instytucjami oraz wsparcie patronów medialnych w promocji działań. Należy uwzględnić treści dla nauczycieli pracujących z uczniami ze specjalnymi potrzebami edukacyjnymi i stale podnosić świadomość zagrożeń cyfrowych. Bezpieczeństwo w sieci wymaga współpracy wszystkich uczestników procesu edukacyjnego: rodziców, nauczycieli, uczniów i środowiska lokalnego. Realizacja tych rekomendacji pozwoli na dalszy rozwój Programu i zwiększenie jego efektywności.

Kontynuacja Programu w kolejnych latach pozwoli na dalsze zwiększenie świadomości społeczeństwa na temat ochrony danych osobowych. Program stanowi cenne źródło aktualnej, niezbędnej i rzetelnej wiedzy oraz dobrych praktyk w zakresie ochrony danych osobowych w szkołach, a także realizacji obowiązków wynikających z ogólnego rozporządzenia o ochronie danych w sektorze oświaty. Ma również wpływ na wzrost zaangażowania nauczycieli w realizację innowacyjnych zajęć z uczniami w obszarze ochrony prywatności. Z uwagi na duże zapotrzebowanie na wiedzę w tym zakresie, program „Twoje dane – Twoja sprawa” będzie kontynuowany w kolejnych latach.

1.5.2. Program szkoleniowy „UODO Tour 2024”

Dwutygodniowy program szkoleniowy w Urzędzie Ochrony Danych Osobowych był Nagrodą Specjalną dla laureatów XII edycji konkursu na esej dla studentów prawa i administracji, zorganizowanego przez UODO we współpracy z Krajową Izbą Radców Prawnych i Kancelarią Kobylańska Lewoszewski Mednis sp. j.[462] Konkurs skupiał się na temacie nowych technologii, w tym wykorzystywania algorytmów sztucznej inteligencji w procesach rekrutacyjnych. W ramach nagrody specjalnej wyróżnieni studenci mogli wziąć udział w dwutygodniowym programie szkoleniowym, który obejmował zapoznanie się ze specyfiką pracy poszczególnych departamentów oraz

[462] https://uodo.gov.pl/pl/589/3112.

z zadaniami, z jakimi mierzą się na co dzień pracownicy UODO. Nakładanie i obliczanie kar administracyjnych, naruszenia i kontrole, w jaki sposób skutecznie złożyć skargę do UODO, proces tworzenia kodeksów i certyfikacji, zagadnienia nowych technologii i bezpieczeństwa informacji – to tylko niektóre z zagadnień, z którym mogli zapoznać się w ciągu dwóch tygodni trwania programu.

Uczestnicy zostali również zaproszeni do dalszej współpracy przy realizacji projektów edukacyjnych i społecznych, podejmowanych przez UODO.

1.5.3. Projekt wizyt studyjnych dotyczący wdrożenia Aktu w sprawie zarządzania danymi (DGA)

W październiku 2024 r. do Komisji Europejskiej został przekazany wniosek o dofinansowanie projektu „Study visits project on DGA implementation in Poland" („Projekt wizyt studyjnych dotyczących wdrażania DGA w Polsce"). Wniosek został złożony w odpowiedzi na konkurs w ramach Instrumentu Wsparcia Technicznego (Technical Support Instrument – TSI, a konkretnie w ramach inicjatywy flagowej dotyczącej wymiany współpracy w zakresie administracji publicznej – PACE – Public Administration Cooperation Exchange). Głównym celem TSI jest wspieranie wysiłków państw członkowskich służących wzmocnieniu ich zdolności instytucjonalnych i administracyjnych, skutecznemu wdrażaniu reform i prawa Unii oraz wsparcie transformacji ekologicznej i cyfrowej. Realizacja projektu zakłada zorganizowanie dwóch wizyt studyjnych pracowników UODO oraz warsztatów online. Na zakończenie projektu zostanie przygotowany raport zawierający podsumowanie przeprowadzonych działań oraz rekomendacje dla Urzędu Ochrony Danych Osobowych dotyczące wdrożenia Aktu w sprawie zarządzania danymi w Polsce. Celem projektu jest zdobycie wiedzy i poznanie doświadczeń państw członkowskich UE w zakresie implementacji Aktu w sprawie zarządzania danymi. W grudniu 2024 r. Ministerstwo Rozwoju i Technologii, które jest instytucją pośredniczącą, oficjalnie poinformowało UODO, że projekt uzyskał wstępną akceptację ze strony Komisji Europejskiej (Dyrekcji Generalnej ds. Wsparcia Reform Strukturalnych – DG REFORM)[463].

1.5.4. Instytut Miast Praw Człowieka

Instytut Miast Praw Człowieka we współpracy z Agencją Praw Podstawowych UE był organizatorem serii spotkań online w ramach projektu „Wzmacnianie systemowego podejścia do włączenia społecznego w samorządzie". Celem projektu było opracowanie metodologii zbierania i oceny danych o odbiorcach programów i usług społecznych realizowanych przez samorządy. Dane te i ich odpowiednia analiza miałyby przyczynić się do lepszego włączenia do udziału w życiu społecznym grup mniejszościowych, takich jak osoby z niepełnosprawnościami, w podeszłym wieku, czy LGBT+.

[463] Oficjalne wyniki naboru ogłoszone zostały w marcu 2025 r. Komisja Europejska podjęła decyzję o przyznaniu finansowania dla projektu PACE – Data Governance Act implementation, zob. https://reform-support.ec.europa.eu/our-projects/country-factsheets/poland_en.

Ekspert reprezentujący UODO w tym projekcie podkreślał, że kluczowe jest wyodrębnienie przedsięwzięć, dla realizacji których rzeczywiście potrzebne są konkretne dane osobowe. Dane ujawniające tożsamość seksualną czy niepełnosprawność podlegają szczególnemu reżimowi ochrony na gruncie RODO. Dlatego też, konstruując programy przewidujące ich przetwarzanie, należy być wyjątkowo ostrożnym. Dane te przetwarzane są na podstawie ustaw szczególnych i nie można zmieniać dowolnie celu, dla realizacji którego zostały zebrane. Nie wyklucza to jednak możliwości konstruowania różnego rodzaju programów przewidujących szeroko rozumianą pomoc dla osób, których dotyczą, na zasadzie ich dobrowolnej partycypacji, po poinformowaniu o zasadach jej udzielania i świadczenia. Konkluzje ze spotkań w ramach tego projektu stały się kanwą do kolejnego spotkań, tym razem dotyczących budowania skutecznych przedsięwzięć zapobiegających wykluczeniu społecznemu.

1.6. Konkursy

W analizowanym 2024 roku organ nadzorczy był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

1) XII Konkurs na esej dla studentów kierunków prawa i administracji

Komisja konkursowa złożona z ekspertów UODO, specjalistów Krajowej Izby Radców Prawnych (KIRP) oraz Kancelarii Kobylańska Lewoszewski Mednis sp. j., po raz dwunasty wyłoniła laureatów w konkursie na esej dla studentów prawa i administracji. Temat kazusu „Sprawdzanie predyspozycji studentów z wykorzystaniem sztucznej inteligencji" dotyczył kwestii związanych z wykorzystaniem narzędzi sztucznej inteligencji do sprawdzania predyspozycji kandydatów do podjęcia studiów na danym kierunku. Zadaniem uczestników było rozwiązanie kazusu w formie eseju, w którym mieli wypowiedzieć się, czy uczelnia ma podstawę prawną do przetwarzania danych osobowych kandydata zawartej w analizie dokonanej z użyciem algorytmów sztucznej inteligencji. Podstawą oceny wniosków sformułowanych przez autorów nadesłanych prac, były m.in. komunikaty i decyzje Prezesa UODO, cytowana literatura, orzecznictwo międzynarodowe, ogólne rozporządzenie o ochronie danych (RODO) oraz rozporządzenie w sprawie sztucznej inteligencji (AI Act). Laureaci konkursu otrzymali nagrody rzeczowe. Wyróżnieni studenci – w ramach nagrody specjalnej – mogli wziąć udział w przygotowanym przez ekspertów UODO **dwutygodniowym programie szkoleniowym w Urzędzie Ochrony Danych Osobowych**[464].

[464] zob. rozdz. 1.5.2. Sprawozdania.

2) Konkursy XIV edycji programu „Twoje dane – Twoja sprawa”

Konkursy organizowane przez Prezesa UODO zachęcają uczniów do głębszego zainteresowania się tematyką ochrony danych osobowych, a szkoły do podejmowania innowacyjnych działań w ramach Programu, dzielenia się wiedzą i opracowywania autorskich materiałów edukacyjnych.

1. Do konkursu dla uczniów **„Dbaj o siebie i swoich bliskich. Ochrona wizerunku w internecie”** wpłynęło 79 zgłoszeń (filmów i plakatów). Komisja konkursowa uhonorowała sześciu zwycięzców w dwóch kategoriach – szkoła podstawowa oraz szkoła ponadpodstawowa.
2. W konkursie na „Inicjatywę edukacyjną roku 2023/2024” spośród 9 zgłoszeń wybrano i nagrodzono trzy inicjatywy edukacyjne zrealizowane w oparciu o autorskie scenariusze zajęć, które wzbogaciły bazę materiałów edukacyjnych Programu. Zespół Szkolno-Przedszkolny w Długołęce otrzymał szczególne wyróżnienie Prezesa UODO – statuetkę „Złotego Pióra” – za zajęcie pierwszego miejsca w konkursie na najlepszą inicjatywę edukacyjną za projekt „Teatrzyk Kamishibai »Pixel, Król Cyberlandii«. Drugie miejsce przyznano Zespołowi Szkół nr 1 im. Stanisława Staszica w Kwidzynie za projekt „Mediacja rówieśnicza jako metoda rozwiązania konfliktu wynikającego z niewłaściwego postępowania w mediach społecznościowych”. Trzecie miejsce zajęła Bursa Szkolna nr 5 w Lublinie za projekt zrealizowany na Dzień Ochrony Danych Osobowych pod tytułem „Konkurs prezentacji scenicznych z zakresu wiedzy o ochronie danych osobowych w mediach społecznościowych”.

Uroczystość wręczenia nagród odbyła się 14 czerwca 2024 r. w Warszawie. Wyróżnione zostały szkoły, nauczyciele i uczniowie, którzy w sposób szczególny przyczynili się do realizacji celów Programu. Spotkanie było okazją do podziękowania uczestnikom Programu za rok owocnej współpracy, uhonorowania laureatów konkursów i zaprezentowania najlepszych praktyk w edukacji, a także – zwrócenia uwagi na istotne kwestie związane z ochroną prywatności dzieci w dobie cyfrowej transformacji.

3) Inne

Prezes UODO objął patronatem honorowym i ufundował nagrody rzeczowe dla finalistów **XXII Ogólnopolskiego Konkursu Prawa Europejskiego**, którego organizatorami byli ELSA Poland i Grupa Lokalna ELSA Łódź. Organizacja tego konkursu w 2024 roku zbiegła się z obchodami dwudziestolecia przystąpienia Polski do UE, wyborami do Parlamentu Europejskiego oraz przygotowaniami do objęcia z początkiem 2025 r. prezydencji RP w Radzie Unii Europejskiej. Uroczystość wręczenia nagród 15 finalistom odbyła się w Łodzi, 7.12.2024 r.

1.7. Porozumienia o współpracy

1) Akademia Ekonomiczno-Humanistyczna w Warszawie, 21.01.2024 r.

Przedmiotem porozumienia Urzędu Ochrony Danych Osobowych z Akademią Ekonomiczno-Humanistyczną w Warszawie było określenie zasad współpracy naukowej, dydaktycznej, badawczej i organizacyjnej związanej z prowadzeniem studiów na Wydziale Nauk Społecznych tej uczelni. Ponadto – inicjowanie i realizowanie wspólnych projektów, w tym praktyk studenckich.

2) Rzecznik Praw Dziecka, 26.04.2024 r.

Porozumienie o współpracy między Prezesem UODO a Rzeczniczką Praw Dziecka w zakresie inicjatyw edukacyjnych i badawczych dotyczących danych osobowych dzieci i młodzieży, zostało podpisane w trakcie wspólnej konferencji „Wyzwania dla ochrony danych osobowych dzieci", która odbyła się 26 kwietnia 2024 r. w siedzibie Urzędu. Obejmuje ono obszary w zakresie realizacji wspólnych projektów, inicjatyw, badań, kampanii, publikacji oraz innych działań edukacyjnych i społecznych. W ramach podpisanego porozumienia obie instytucje mają także wymieniać się specjalistyczną wiedzą.

3) Ogólnopolska Federacja Stowarzyszeń Uniwersytetów Trzeciego Wieku, 20.11.2024 r.

Podczas realizowanej na Śląsku akcji edukacyjnej pod nazwą „UODO rusza w kraj" (20-21.11.2024 r.), Prezes UODO podpisał z Wiesławą Borczyk, Prezeską Ogólnopolskiej Federacji Stowarzyszeń Uniwersytetów Trzeciego Wieku, porozumienie o współpracy. Miejscem tego wydarzenia była siedziba Śląskiego Urzędu Wojewódzkiego w Katowicach. Celem porozumienia jest świadczenie wzajemnej pomocy w działaniach na rzecz promowania zasad ochrony danych osobowych, udział we wspólnych projektach i inicjatywach edukacyjno-informacyjnych, których zadaniem jest pogłębienie świadomości słuchaczy uniwersytetów trzeciego wieku o przysługujących im prawach i środkach ochrony danych osobowych.

1.8. Poradniki

1) Poradnik dotyczący naruszeń ochrony danych osobowych

W okresie od 21 maja do 21 czerwca 2024 r. Prezes UODO przeprowadził były otwarte konsultacje w sprawie aktualizacji poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych", opublikowanego w 2019 r. Z możliwości wniesienia uwag skorzystało 21 podmiotów. W pracach nad przygotowaniem nowego dokumentu uczestniczyli pracownicy UODO we współpracy ze Społecznym Zespołem Ekspertów przy Prezesie UODO. Celem aktualizacji poradnika było wyjaśnienie i uporządkowanie kwestii związanych z zarządzaniem naruszeniami ochrony danych osobowych w ramach

rozporządzenia 2016/679 oraz dostarczenie praktycznych wskazówek z uwzględnieniem aktualnego stanu wiedzy, w tym nowych doświadczeń organów nadzorczych, publikacji Europejskiej Rady Ochrony Danych oraz orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. Zaktualizowana wersja tej publikacji, **„Obowiązki administratorów związane z naruszeniami ochrony danych osobowych. Poradnik na gruncie RODO”**, to wersja 2.0 opublikowana w lutym 2025 r.[465]

2) Poradnik dotyczący ochrony wizerunku dziecka

Efektem współpracy Prezesa UODO z Fundacją Orange jest poradnik „**Wizerunek dziecka w Internecie. Publikować czy nie?**”[466], który opisuje, jakiej ochronie podlega wizerunek i jak poprawnie skonstruować zgodę na jego rozpowszechnianie. Zawiera też listę potencjalnych ryzyk, które wiążą się z publikowaniem wizerunków dzieci w internecie oraz wykaz pytań, które warto sobie zadać przed udostępnianiem online treści z ich udziałem. W poradniku zaakcentowano konieczność wcześniejszego zapytania dziecka o zgodę na publikację jego wizerunku, podkreślając przy tym podmiotowość dziecka w aspekcie jego prawa do decydowania w sprawach, które go bezpośrednio dotyczą.

Poradnik zaprezentowano w czasie konferencji zorganizowanej 8 lipca 2024 r. przez Parlamentarny Zespół Praw Dziecka i UODO, w partnerstwie z Państwową Komisją ds. przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15**,** Biurem Kryminalnym Komendy Głównej Policji oraz partnerami społecznymi[467].

1.9. Współpraca krajowa przy Polskim Komitecie Normalizacyjnym (PKN)

Przedstawiciele Prezesa Urzędu Ochrony Danych Osobowych są reprezentantami 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[468] (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.

1.10. 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

[465] https://uodo.gov.pl/pl/598/3563.
[466] https://uodo.gov.pl/pl/138/3215.
[467] https://uodo.gov.pl/pl/138/3215.
[468] Dz. U. Nr 169, poz. 1386 ze zm.

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 2024 r. nagrodę im. Michała Serzyckiego przyznano już po raz siódmy. Wyróżnienie otrzymała dr Joanna Hałoń-Gnutek, dyplomowana nauczycielka Szkoły Podstawowej nr 4 im. Adama Mickiewicza w Lublinie, która od wielu lat pełni rolę szkolnego koordynatora programu „Twoje dane – Twoja sprawa". Liderka Programu chętnie dzieli się wiedzą i doświadczeniami, a przygotowane przez nią scenariusze zajęć zostały włączone do bazy materiałów edukacyjnych programu „Twoje dane – Twoja sprawa" i stanowią wsparcie dla kolejnych uczestników Programu do organizowania interesujących lekcji z uczniami.

1.11. Konferencje, seminaria, spotkania

W analizowanym roku sprawozdawczym organ nadzorczy organizował konferencje i seminaria, jak również brał aktywny udział w różnych wydarzeniach organizowanych w kraju przez inne podmioty (załącznik nr 3) oraz patronował różnym przedsięwzięciom (załącznik nr 2). Poniżej zaprezentowane zostały wybrane przykłady wydarzeń.

1) III Kongres Bezpieczeństwa Biznesu, 25-26.03.2024 r.

Ochrona danych w czasie zagrożenia była tematem wystąpienia Konrada Komornickiego, zastępcy Prezesa UODO, podczas III Kongresu Bezpieczeństwa Biznesu, które z inicjatywy Stowarzyszenia Bezpieczeństwa Narodowego odbyło się w Spale. Wystąpienie zastępcy Prezesa UODO pt. „Ranga i znaczenie ochrony danych osobowych w czasie wzmożonego cyberzagrożenia i wojny informacyjnej" skupiało się wokół nowych regulacji prawnych (m.in. DSA, DMA, DGA, AI Act i NIS2), które mają na celu przede wszystkim zapewnienie bezpieczeństwa w sieci i zwiększenie przejrzystości działań platform internetowych ze szczególnym uwzględnieniem ochrony danych osobowych. Podkreślił, że Urząd Ochrony Danych Osobowych wychodzi naprzeciw wyzwaniom związanym z rozwojem nowych technologii, sztucznej inteligencji i cyberbezpieczeństwa. Podejmuje działania mające na celu realizację skutecznej ochrony danych osobowych i prawa do prywatności, skupiając się na identyfikacji najważniejszych zagrożeń z obszaru bezpieczeństwa fizycznego, organizacyjnego, technologicznego, osobowego i prawnego, pod kątem wsparcia przedsiębiorców w skutecznym zabezpieczeniu ich działalności.

2) Konferencja „Wyzwania dla ochrony danych osobowych dzieci". Warszawa, 26.04.2024 r.

Organizatorem konferencji był Urząd Ochrony Danych Osobowych we współpracy z Rzeczniczką Praw Dziecka. Podczas konferencji eksperci poruszyli

tematy związane z podmiotowością dziecka, omawiając standardy ochrony dzieci oraz ich prawa w kontekście dynamicznego rozwoju technologicznego. Głównym tematem była publikacja zdjęć dzieci w mediach społecznościowych zarówno przez rodziców, jak i same dzieci. Ponadto zaprezentowano podejście państw członkowskich UE do ochrony danych osobowych najmłodszych, znaczenie wyrażania zgody na przetwarzanie danych dzieci oraz zwrócono uwagę na coraz większą aktywność młodych osób w cyfrowym świecie, który jest środowiskiem stwarzającym wiele zagrożeń. Działania podejmowane na rzecz najmłodszych przez instytucje publiczne i różnego rodzaju organizacje nie zawsze są ze sobą skoordynowane, a wiedza o nich nie jest wiedzą powszechną wśród podmiotów zajmujących się tym zagadnieniem. W programie konferencji znalazły się warsztaty dla dzieci i młodzieży na temat ochrony danych osobowych, przeprowadzone przez ekspertów UODO.

3) XIII Kongres Transportu Publicznego i Technologii Miejskich, 22.05.2024 r.

O tym, że nowoczesne systemy biletowe nie mogą naruszać prywatności pasażerów, mówił Konrad Komornicki, zastępca Prezesa UODO, podczas XIII Kongresu Transportu Publicznego i Technologii Miejskich. Systemy te powinny być tak skonstruowane, aby nie tylko były wygodne i łatwe w obsłudze, ale także zapewniały skuteczną ochronę danych osobowych pasażerów. Dlatego tak ważne jest prawidłowe przeprowadzenie oceny skutków dla ochrony danych przy wdrażaniu w komunikacji nowoczesnych rozwiązań. Natomiast podmioty projektujące i wdrażające nowoczesne systemy biletowe muszą stosować się do wskazanych w RODO zasad *privacy by design* i *privacy by default.* Dzięki temu już na etapie planowania zostanie uwzględniona ochrona danych przetwarzanych w ramach takich rozwiązań, co znacznie ułatwi zapewnienie bezpieczeństwa danych osobowych.

Organizatorem wydarzenia byli: Zespół Doradców Gospodarczych TOR oraz Zarząd Transportu Miejskiego w Warszawie.

4) Konferencja „Ochrona danych osobowych w UE. Dokąd zmierzamy w przededniu wyborów europejskich?”, 4.06.2024 r.

Doświadczenia polskiego i europejskiego prawa ochrony danych osobowych były głównym tematem tego wydarzenia, zorganizowanego przez UODO z okazji 20. rocznicy członkostwa Polski w Unii Europejskiej, 35. rocznicy wolnych wyborów w Polsce, 6. rocznicy stosowania RODO oraz w kontekście zbliżających się wyborów do Parlamentu Europejskiego. Gościem specjalnym konferencji był dr hab. Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych, który w wystąpieniu „Ochrona danych 20 lat temu, ochrona danych za 20 lat – wyzwania przeszłości i przyszłości” przestrzegł m.in. przed zagrożeniami, jakie płyną z prymatu dyskusji o sztucznej inteligencji nad ochroną danych, zaznaczając na tym tle relację między etyką a silnym prawem karnym. W programie konferencji znalazła się uroczystość wręczenia powołań członkom Społecznego Zespołu Ekspertów przy Prezesie Urzędu Ochrony Danych Osobowych. Nowo powstały zespół to inicjatywa, która jest przestrzenią do dzielenia się swoimi przemyśleniami, opiniowania projektów aktów prawnych, doradzania,

rekomendowania i inicjowania działań w zakresie ochrony danych osobowych oraz przedstawiania Prezesowi UODO propozycji zmian prawa w obszarze ochrony danych osobowych.

5) **Konferencja „Ochrona danych osobowych w świetle aktu o sztucznej inteligencji i innych aktów wdrażających europejską strategię danych", 27.06.2024 r.**

Wyzwania dla ochrony danych osobowych wynikające z aktów prawnych przyjętych na podstawie europejskiej strategii w zakresie danych: Aktu o sztucznej inteligencji (AI Act), Aktu w sprawie zarządzaniu danymi (Data Governance Act), Aktu o danych (Data Act) i in. były głównymi tematami dyskutowanymi podczas tego wydarzenia. Poruszone także zostały zagadnienia związane z określeniem właściwości organów stosujących te regulacje, współpracy między nimi oraz sprawowania sądowej kontroli ich działalności. Podczas tego wydarzenia wręczone zostały nagrody laureatom XII edycji konkursu na esej, zorganizowanego przez UODO, Krajową Izbę Radców Prawnych oraz Kancelarię KLM.

Konferencja została zorganizowana przez Urząd Ochrony Danych Osobowych oraz Wydział Prawa i Administracji Uniwersytetu Warszawskiego w Collegium Iuridicium.

6) **Konferencja PINT24 – Prawo i Nowe Technologie, 28–29.06.2024 r.**

Tematyka konferencji skupiała się na zagadnieniach związanych z ochroną prywatności i danych osobowych, sztuczną inteligencją, technologią kwantową i cyberbezpieczeństwem. Prelegenci dyskutowali również na temat nowych regulacji wprowadzanych za sprawą Aktu o sztucznej inteligencji. Wykład Prezesa UODO rozpoczął dyskusję na temat wyzwań dla prywatności i ochrony danych osobowych w kontekście cyfrowym. Wśród panelistów konferencji licznie reprezentowani byli członkowie Społecznego Zespołu Ekspertów przy Prezesie UODO. Organizatorem tego wydarzenia była Okręgowa Izba Radców Prawnych w Krakowie.

7) **Cykl czterech wydarzeń we współpracy UODO – ZUS:**

Organizatorem czterech seminariów, które odbyły się kolejno we Wrocławiu, Gdańsku, Chorzowie i w Warszawie, był Zakład Ubezpieczeń Społecznych (ZUS) we współpracy z Urzędem Ochrony Danych Osobowych.

- **I seminarium UODO – ZUS: „Przetwarzanie danych przez ZUS i płatników składek w związku z realizacją ustawowych obowiązków. Praktyczne aspekty". Wrocław, 19.06.2024 r.**

Seminarium we Wrocławiu zainaugurowany został cykl czterech wydarzeń związanych z tematyką ochrony danych osobowych, których organizatorami były te dwie instytucje. Inspiracją do tego spotkania była potrzeba wymiany doświadczeń w zakresie zapewnienia prawidłowego przetwarzania danych osobowych milionów

płatników składek i wykorzystywania algorytmów sztucznej inteligencji przy realizacji tego zadania. Zaprezentowane zostały najnowsze rozwiązania i najlepsze praktyki wykorzystywane zarówno w podmiotach publicznych, jak i w szeroko rozumianym biznesie.

- **II seminarium UODO – ZUS: „Wdrożenie ustawy o sygnalistach oraz ochrona danych osobowych w miejscu pracy". Gdańsk, 16.09.2024 r.**

Podczas seminarium prelegenci omówili procedury zgłoszeń wewnętrznych i działań następczych – zgodnych z RODO oraz opowiedzieli o ryzykach naruszenia praw i wolności osób w procesie zgłaszania naruszeń prawa. Przybliżyli słuchaczom temat wdrożenia zasad ochrony danych osobowych podczas przetwarzania danych o sygnalistach, a także wątek dopuszczalności stosowania przez pracodawców testów psychometrycznych.

- **III seminarium UODO – ZUS: „Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji". Chorzów, 9.10.2024 r.**

Obowiązki administratorów danych w kontekście projektowania systemów sztucznej inteligencji i możliwości wykorzystania AI w administracji publicznej oraz w biznesie, a także dostosowania organizacji w zakresie cyberbezpieczeństwa do wymogów dyrektywy NIS2 – były głównymi tematami tego seminarium.

- **Konferencja UODO – ZUS: „Wyzwania związane z ochroną danych osobowych. Spojrzenie z perspektywy 2024 roku". Warszawa, 28.11.2024 r.**

Ostatnie i zarazem największe spotkanie w ramach cyklu czterech wydarzeń związanych z ochroną danych osobowych, jakie w 2024 roku zorganizował ZUS we współpracy z UODO, to była konferencja na temat aktualnych wyzwań stojących przed ochroną danych osobowych. Konferencja koncentrowała się na określeniu zadań stojących przed polskim organem nadzorczym w związku z postępującym rozwojem technologicznym oraz koniecznością wprowadzenia nowych regulacji prawnych UE. Dyskutowano nad znaczeniem nowych przepisów (AI Act, dyrektywa NIS2 i in.) i ich wpływie na codzienną praktykę administracji publicznej i pracę inspektorów ochrony danych (IOD).

Inspiracją do serii spotkań UODO z ZUS były liczne pytania dotyczące przetwarzania danych osobowych, jakie stawiano obydwu instytucjom. To właśnie na tej podstawie zrodził się pomysł tematów, które zostały poruszone podczas zrealizowanych wspólnie wydarzeń. Chodziło też o wymianę doświadczeń w zakresie prawidłowego i bezpiecznego przetwarzania danych osobowych tak, aby zagadnienia związane z tym obszarem wiedzy były zrozumiałe nie tylko dla specjalistów.

8) **Seminarium „Praktyczne problemy w stosowaniu przepisów ustawy o ochronie sygnalistów z perspektywy RODO. Przyczynek do dyskusji nad wątpliwościami zgłoszonymi w trakcie konsultacji społecznych", 7.08.2024 r.**

Podczas tego wydarzenia Mirosław Wróblewski, Prezes UODO, wspólnie z pracownikami Urzędu, przedstawicielami Społecznego Zespołu Ekspertów przy PUODO oraz zewnętrznymi ekspertami, omówili uwagi przesłane w ramach konsultacji społecznych i przedstawili propozycje wykładni przepisów ustawy o ochronie sygnalistów w zakresie dotyczącym danych osobowych. Każda uwaga została wnikliwie przeanalizowana i następnie w kolejnych panelach zaprezentowano najbardziej problematyczne kwestie, jakie pojawiły się w ramach konsultacji. Zwrócono uwagę na obowiązki informacyjne i ewentualne wyłączenia w tym zakresie, które wynikają z ustawy o ochronie sygnalistów oraz RODO (w szczególności w kontekście realizacji tych obowiązków względem osób, których dotyczy zgłoszenie), na brak wskazania w ustawie momentu, od którego należy liczyć okres retencji danych osobowych, zastanawiano się, jak odnieść się do zgłoszeń anonimowych (w szczególności w formie ustnej), do praktyki przyjmowania zgłoszeń telefonicznych i wyrażania (lub nie) zgody na nagrywanie i transkrypcję rozmowy i wiele innych ważnych kwestii. Uczestnicy seminarium omówili procedury przyjmowania zgłoszeń wewnętrznych i prowadzenia postępowań wyjaśniających z perspektywy zasad przetwarzania danych osobowych. Polski ustawodawca powierzył Rzecznikowi Praw Obywatelskich rolę centralnego organu wspierającego sygnalistów w korzystaniu z przysługujących im praw, zorganizowanie systemu zgłoszeń zewnętrznych oraz odseparowanie go od systemu zgłoszeń wewnętrznych[469].

9) **Seminarium „Ochrona danych jako element odporności społeczeństwa i państwa", 7.10.2024 r.[470]**

Trendy i kierunki obowiązujące w zakresie ochrony danych osobowych jako elementu odporności społeczeństwa i państwa były głównym tematem tego spotkania. Omówiono na nim zagadnienia dotyczące nowych rodzajów ataków cybernetycznych, wpływu działań wojennych na liczbę naruszeń ochrony danych oraz nowych metod ataków phishingowych i socjotechnicznych w kontekście agresji Rosji na Ukrainę oraz konfliktu na Bliskim Wschodzie. Uczestnicy omówili wyzwania dla ochrony prywatności, jakie niosą ze sobą nowe technologie, takie jak sztuczna inteligencja, uczenie maszynowe i przetwarzanie danych biometrycznych. Dyskutowali nad wykorzystywaniem wycieków danych osobowych do dezinformacji lub ingerencji w procesy demokratyczne. Dużą część spotkania poświęcono na przemyślenia

[469] https://uodo.gov.pl/pl/138/3271.

[470] Seminarium odbywało się w październiku – Europejskim Miesiącu Cyberbezpieczeństwa. To kampania zorganizowana przez ENISA, Agencję Unii Europejskiej ds. Cyberbezpieczeństwa, z inicjatywy Komisji Europejskiej. W tegorocznej edycji tej kampanii szczególną uwagę poświęcono problematyce inżynierii społecznej – różnym metodom socjotechnki, które cyberprzestępcy wykorzystują do manipulacji w oszustwach internetowych nakierowanych na użytkowników sieci. Tematyka seminarium wpisywała się w kampanię ENISA.

dotyczące działań, jakie powinny podjąć organy publiczne w celu zwalczania cyberprzestępczości naruszającej prywatność obywateli. Rozmówcy zastanawiali się, w jaki sposób UODO i CSIRT mogą zacieśnić współpracę w zakresie wymiany informacji o zagrożeniach i naruszeniach ochrony danych oraz jakie konkretne środki techniczne i organizacyjne powinni wdrożyć administratorzy, aby zwiększyć odporność na ataki cybernetyczne. Dyskusja koncentrowała się również na wyzwaniach związanych z wdrażaniem nowych regulacji dotyczących ochrony danych, a także praktycznych aspektach zarządzania bezpieczeństwem informacji w instytucjach publicznych. Cyberbezpieczeństwo wymaga działania zespołowego, współpracy lokalnych instytucji np. wojska czy policji np. z bigtechami, a także kooperacji z instytucjami Unii Europejskiej i państwami członkowskimi. Nie bez znaczenia są tu regulacje prawne (np. dyrektywa NIS2), których prawidłowe wdrożenie ma ogromny wpływ na poziom cyberbezpieczeństwa.

Organizatorem seminarium był Urząd Ochrony Danych Osobowych, Społeczny Zespół Ekspertów przy Prezesie UODO oraz Zakład Ubezpieczeń Społecznych. Oprócz przedstawicieli organizatorów, wśród uczestników seminarium znaleźli się eksperci Centralnego Biura Zwalczania Cyberprzestępczości, Prokuratury Krajowej, Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni (gen. dyw. Karol Molenda), Ministerstwa Obrony Narodowej, Komendy Głównej Policji, Techom Sp. z o.o, Stowarzyszenia Inspektorów Ochrony Danych Osobowych, SABI, UKSW i NASK – Państwowy Instytut Badawczy.

10) Konferencja „Ochrona danych osobowych w robotyce medycznej w dobie AI Act i EHDS", 15.10.2024 r.

Konferencja UODO i Fundacji AI One Health „*Ochrona danych w robotyce medycznej w dobie AI ACT i EHDS*", współorganizowana była przez Izbę POLMED i Ośrodek Przetwarzania Informacji – Państwowy Instytut Badawczy, we współpracy ze Społecznym Zespołem Ekspertów przy Prezesie UODO. W jej ramach odbyły się 4 debaty dotyczące obszaru: kultury ochrony danych medycznych w Polsce, standardów w robotyce medycznej i kierunkach ich dalszego rozwoju oraz robotów medycznych w dobie cyberzagrożeń i wyzwań dla ochrony danych osobowych w chmurze, w dobie AI Act i EHDS. Uczestnicy debat akcentowali konieczność ścisłej współpracy oraz klarownych regulacji między technologią a ochroną danych, kluczowych zarówno dla zapewnienia prywatności pacjentów, jak i dla postępu medycznego. Procedury odnoszące się do przetwarzania danych muszą być zgodne z najwyższymi standardami etycznymi, umożliwiając jednocześnie naukowcom i instytucjom badawczym dostęp do informacji, które mogą prowadzić do przełomowych odkryć i ulepszeń w opiece zdrowotnej. Wskazano również na konieczność rzetelnych pomiarów efektywności zabiegów z użyciem robotów oraz monitorowania wyników pooperacyjnych pacjentów. Skupiono się na temacie rosnącego ryzyka związanego z możliwością ataków cyberprzestępców na roboty medyczne i koniecznością wprowadzenia standaryzacji na poziomie Unii Europejskiej dla ochrony bezpieczeństwa przetwarzanych informacji. Zgodność z przepisami musi

być zachowana na każdym etapie procesu, dlatego tak ważna jest rola IOD w placówkach medycznych.

Skuteczne wdrożenie przepisów, budowanie zaufania w relacjach między pacjentami a personelem oraz zapewnienie odpowiedniego dostępu do danych to najważniejsze wnioski z tego spotkania, zaś działania na rzecz zwiększenia bezpieczeństwa technologii medycznych powinny stać się priorytetem w ochronie zdrowia.

11) Konferencja „AI w medycynie a przetwarzanie danych osobowych pacjentów – przyczynek do dyskusji nad postępującymi zmianami", 17.10.2024 r.

Omówienie kluczowych zagadnień związanych z rozwojem sztucznej inteligencji w medycynie oraz wyzwań, jakie niesie to zjawisko w kontekście przetwarzania danych osobowych, było głównym celem konferencji zorganizowanej na Warszawskim Uniwersytecie Medycznym. Wydarzenie to stworzyło przestrzeń do wymiany wiedzy i doświadczeń ekspertów z różnych dziedzin. Prezes UODO i jego przedstawiciele podkreślali wartość finansową danych medycznych, przez co stały się one atrakcyjnym celem cyberataków. W związku z zaobserwowanym wzrostem liczby incydentów w tym obszarze aktywność organu nadzorczego musi zostać wzmocniona. Przedstawione też zostały wyzwania legislacyjne przed sektorem medycznym, w związku z perspektywą nowych, unijnych regulacji odnoszących się do wykorzystania algorytmów sztucznej inteligencji w medycynie.

12) II edycja International Scientific Workshop – Legal Challengers of Disruptive Technologies, 7.11.2024 r.

Zasadniczym celem warsztatów była wymiana poglądów w zakresie wyzwań prawnych dotyczących przełomowych technologii, w tym sztucznej inteligencji oraz technologii kwantowych, zarówno z perspektywy prawa Unii Europejskiej, jak i innych systemów prawa. Istotna część warsztatów poświęcona była tematyce ochrony danych osobowych, w szczególności w kontekście sztucznej inteligencji, danych medycznych oraz zagrożeń związanych z rozwojem komputerów kwantowych. Prezes UODO wygłosił wykład inaugurujący międzynarodowe warsztaty pt. „Artificial Inteligence & Fundamental Right" oraz objął to wydarzenie patronatem honorowym. Organizatorem warsztatów była Akademia Leona Koźmińskiego w Warszawie.

13) Seminarium „Ochrona zdrowia w zatrudnieniu a RODO", 15.11.2024 r

Seminarium składało się z czterech paneli tematycznych, w ramach których eksperci omówili zagadnienia odnoszące się do przetwarzania danych w profilaktyce zdrowotnej, badań i testów psychologicznych, wsparcia psychologicznego dla pracowników, a także zatrudnienia i aktywizacji zawodowej pracowników z niepełnosprawnościami oraz wypadków przy pracy. Jako wymagające szerszych konsultacji i zmian w przepisach prawa i procedurach, wskazano kwestie dotyczące doprecyzowania trybu, w jakim można byłoby kierować pracownika na wcześniejsze

badania okresowe w związku z pogorszeniem jego stanu zdrowia, wymiany informacji pomiędzy pracodawcą a lekarzem medycyny pracy w szerszym zakresie niż wynikający wprost z treści wzoru skierowania czy orzeczenia, a także zakresu badań medycyny pracy. Podkreślono przy tym brak wyraźnej podstawy prawnej kierowania pracownika na badania psychiatryczne i tym samym możliwości udzielenie mu wsparcia psychologicznego przez pracodawcę. Wzór skierowania na badania okresowe/profilaktyczne opisuje jedynie warunki pracy, wskazując na występowanie (lub nie) czynników niebezpiecznych czy szkodliwych dla zdrowia. Eksperci byli zgodni co do potrzeby systemowych rozwiązań, wskazujących na to, że badania wykonywane w ramach przepisów kodeksu pracy powinny również służyć profilaktyce i kompleksowej ocenie stanu zdrowia, a nie wyłącznie obserwacji tych narządów i układów, które są krytyczne dla występujących w pracy zagrożeń. Należy ujednolicić standardy w medycynie pracy, uporządkować kwestię ochrony danych, tak, by chronić wrażliwe informacje, ale jednocześnie nie utrudniać stawiania zgodnych ze stanem faktycznym diagnoz[471].

Organizatorami seminarium byli: UODO, Społeczny Zespół Ekspertów przy Prezesie UODO oraz Konfederacja Lewiatan.

14) Spotkanie z członkami Koalicji AI w Zdrowiu, 29.11.2024 r.

Podczas spotkania Prezesa UODO z członkami Koalicji AI w Zdrowiu, poruszone zostały tematy związane z przetwarzaniem danych pacjentów, regulacjami prawnymi oraz możliwościami harmonizacji nowoczesnych rozwiązań sztucznej inteligencji z obowiązującymi standardami ochrony prywatności. Spotkanie było okazją do wymiany poglądów i doświadczeń między ekspertami technologicznymi, medycznymi i prawnymi. Podczas wizyty w UODO eksperci podjęli się w szczególności analizy tematów dotyczących wykorzystania danych medycznych do trenowania modeli AI, standardów anonimizacji i pseudonimizacji danych medycznych, a także dostępu do danych w badaniach klinicznych z wykorzystaniem nowych technologii. Nie zabrakło też tematów związanych z legislacją, nowymi przepisami dotyczącymi cyberbezpieczeństwa (NIS2, DORA) i ich relacją z aktem o sztucznej inteligencji. Podczas spotkania poruszono także tematykę skarg wnoszonych do Prezesa UODO w związku z przetwarzaniem danych medycznych z wykorzystaniem systemów AI.

1.12. UODO rusza w kraj

„UODO rusza w kraj” – to inicjatywa Prezesa UODO, której celem jest przybliżenie problematyki ochrony danych mieszkańcom Polski oraz lepszego rozpoznania problemów związanych z ochroną danych osobowych, z jakimi mierzą się w szczególności lokalne społeczności i jednostki samorządu terytorialnego (JST) w różnych regionach naszego kraju. Urząd Ochrony Danych Osobowych nie posiada swoich jednostek terenowych, a dzięki tej

[471] https://uodo.gov.pl/pl/138/3406; https://uodo.gov.pl/pl/138/3429.

akcji sprawy związane z ochroną danych osobowych mieszkańców różnych województw oraz działalność JST w terenie, stały się przedmiotem szczególnego zainteresowania organu i przyczyniły się do lepszego zrozumienia lokalnych problemów ochrony danych osobowych.

Pierwszym kierunkiem akcji „UODO rusza w kraj" była **Małopolska**, gdzie 26 września 2024 r. rozpoczęła się seria spotkań z mieszkańcami oraz władzami wojewódzkimi i samorządowymi tego rejonu. W delegaturze Małopolskiego Urzędu Wojewódzkiego w Tarnowie odbyło się spotkanie z przedstawicielami władz samorządowych, a w Krakowie z mieszkańcami tego miasta. Dodatkowo eksperci UODO przeprowadzili szkolenie dla inspektorów ochrony danych z JST. W Urzędzie Miasta Krakowa działał punkt konsultacyjny, w którym pracownicy Infolinii UODO udzielali konsultacji i porad prawnych z zakresu ochrony danych osobowych i prawa do prywatności.

W ramach tego projektu odbyło się również spotkanie z Kanclerzem Kurii Metropolitarnej w Krakowie, podczas którego nakreślone zostały obszary przyszłej współpracy w zakresie ochrony danych osobowych przetwarzanych przez jednostki kościelne, w szczególności dotyczące współpracy z kościelnymi inspektorami ochrony danych.

Województwo śląskie było kolejnym etapem akcji „UODO rusza w kraj", podczas której odbyło się szereg ważnych wydarzeń. W siedzibie Śląskiego Urzędu Wojewódzkiego w Katowicach odbyło się spotkanie z seniorami, podczas którego podpisane zostało porozumienie pomiędzy UODO a Ogólnopolską Federacją Stowarzyszeń Uniwersytetów Trzeciego Wieku o współpracy w zakresie edukacji na temat ochrony prywatności i danych osobowych oraz pogłębiania świadomości słuchaczy uniwersytetów trzeciego wieku o przysługujących im prawach i środkach ich ochrony (20.11.2024 r.). W tym samych czasie w siedzibie Urzędu Miasta Katowice działał punkt konsultacyjny dla obywateli, w którym eksperci UODO – związani na co dzień z infolinią – udzielali porad prawnych z dziedziny prawa do prywatności i ochrony danych osobowych. Ponadto Urząd Ochrony Danych Osobowych, wspólnie z Katedrą Prawa Gospodarczego Uniwersytetu Ekonomicznego w Katowicach, zorganizowali konferencję naukową „Bezpieczeństwo informacji w organizacji i jej zasobów" (21.11.2024 r.). Partnerami merytorycznymi konferencji byli: czasopismo „Studia Prawnoustrojowe Uniwersytetu Warmińsko-Mazurskiego w Olsztynie" oraz KiHG Radcowie Prawni Sp.p.

Podobne spotkania Prezesa UODO i jego ekspertów odbywać się będą w kolejnych województwach w ramach uzgodnień dokonywanych z władzami wojewódzkimi i samorządowymi.

1.13. Spotkania z JST

Dopełnieniem serii wydarzeń zorganizowanych dla przedstawicieli JST w ramach akcji „UODO rusza w kraj", był zainicjowany przez zastępcę Prezesa UODO cykl VI spotkań z przedstawicielami największych organizacji zrzeszających jednostki samorządu terytorialnego w Polsce: Unię Metropolii Polskich (24.06.2024 r.), Związek

Miast Polskich (6.09.2024 r.), Związek Gmin Wiejskich RP (26.09.2024 r.), Związek Województw RP (21.10.2024 r.), Związek Powiatów Polskich (19.11.2024 r.) oraz Narodowym Instytutem Samorządu Terytorialnego – NIST (25.11.2024 r.). Spotkania te były okazją do wymiany informacji i doświadczeń związanych z ochroną danych osobowych w jednostkach samorządu terytorialnego.

1.14. Cykl wykładów eksperckich

Wykład inauguracyjny Przewodniczącego Społecznego Zespołu Ekspertów przy Prezesie UODO (SZE PUODO) pt. „**Projektowanie prywatności na przykładzie internetu rzeczy (IoT) – perspektywa dostawcy i korzystającego”** wygłoszony online 6 grudnia 2024 r. rozpoczął cykl wykładów eksperckich dla pracowników Urzędu Ochrony Danych Osobowych pn. „Ochrona danych osobowych i technologia”[472]. Wykłady będą odbywały się co do zasady raz w miesiącu i w założeniu mają też być otwarte dla słuchaczy z zewnątrz. Kolejny wykład z tego cyklu zaplanowany został na styczeń 2025 r. jako wydarzenie towarzyszące obchodom XIX Dnia Ochrony Danych Osobowych.

1.15. IV Tour de Konstytucja

Tour de Konstytucja to organizowany od 2021 r. cykl publicznych spotkań w całej Polsce poświęconych prawom zapisanym w Konstytucji. Przygotowują je prawnicy oraz lokalni aktywiści zaangażowani we wspieranie praw człowieka. Celem inicjatywy Tour de Konstytucja jest propagowanie wiedzy nt. praw konstytucyjnych oraz zachęcanie do podejmowania aktywności obywatelskich. Projekt realizowany jest przy wsparciu merytorycznym Urzędu Ochrony Danych Osobowych w zakresie dotyczącym promocji ochrony prywatności oraz danych osobowych.

Prezes UODO na spotkaniu z Prezesem Fundacji Aktywna Demokracja (21.03.2024 r.), organizatorem projektu Tour de Konstytucja, zadeklarował wsparcie Urzędu dla tej inicjatywy w zakresie szerzenia wiedzy na temat ochrony danych osobowych i objął ją swoim patronatem.

Przystanki Tour de Konstytucja z udziałem Prezesa UODO i jego przedstawicieli:

1) **Warsztaty dla uczniów Zespołu Szkół nr 3 im. Marii Skłodowskiej-Curie w Wiskitkach, 25.03.2024 r.** Spotkanie z uczniami dotyczyło tematu sztucznej inteligencji, w szczególności w aspekcie jej codziennego użytkowania. Omówiono temat zagrożeń związanych z rozwojem technologii cyfrowych w kontekście ochrony danych osobowych i praktyczne sposoby zapewnienia bezpieczeństwa cyfrowego.
2) **Koronowo na Plaży Pieczyskiej, 6.08.2024 r.** W trakcie debaty poruszono zagadnienia dotyczące kradzieży danych osobowych oraz niebezpieczeństw związanych ze stosowaniem sztucznej inteligencji. Eksperci UODO podpowiedzieli, co można zrobić w wypadku wystąpienia tego rodzaju nadużyć. Dużo miejsca poświęcili również prewencji – omówili sposoby, które mogą

[472] Nagranie wykładu dostępne jest pod linkiem: https://uodo.gov.pl/pl/592/3478.

minimalizować ryzyko wykorzystania danych osobowych przez przestępców oraz jak chronić się przed niechcianym marketingiem.

3) **Warsztaty dla uczniów Liceum Ogólnokształcącego im. Piotra Skargi w Grójcu, 10.04.2024 r.** Przedstawicielka UODO omówiła zagadnienia związane z Konstytucją, jej znaczeniem dla społeczeństwa, a także z prawami zagwarantowanymi dzieciom i młodzieży przez polskie prawo. Przybliżyła rolę państwa w egzekwowaniu tych praw oraz podkreśliła znaczenie nowych technologii oraz ochrony danych osobowych i prywatności.

IV Tour de Konstytucja „Siła Młodych – Most Pokoleń", koncentrowała się na edukacji młodzieży w zakresie społeczeństwa obywatelskiego, Konstytucji RP i Karty Praw Podstawowych UE. Na spotkaniach z młodzieżą podkreślano znaczenie 20-lecia Polski w Unii Europejskiej i promowanie nadchodzących wyborów do Parlamentu Europejskiego.

1.16. Pol'and'Rock Festiwal

Festiwal Pol'and'Rock, który zwykle kojarzy się z muzyką i zabawą, za sprawą obecności różnych instytucji – w tym Prezesa UODO i jego przedstawicieli – stał się przestrzenią do poważnych rozmów o prawie do prywatności i ochrony danych osobowych, o cyberbezpieczeństwie i o nowych technologiach. Urząd Ochrony Danych Osobowych aktywnie włączył się w edukacyjną część festiwalu, organizując warsztaty na temat sztucznej inteligencji oraz prowadząc punkt konsultacyjny. Obecność Prezesa UODO i jego współpracowników była możliwa dzięki wsparciu Okręgowej Izby Radców Prawnych z Poznania, która udostępniła przestrzeń, w której eksperci Urzędu mogli udzielać porad i dzielić się wiedzą z uczestnikami festiwalu. Połączenie edukacji i zabawy pokazało, że tak ważne tematy, jak ochrona danych osobowych mogą być przedstawiane w sposób przystępny, angażujący i skuteczny – nawet w miejscach o nieformalnym charakterze. Sukces tej inicjatywy dowodzi, że wychodzenie do społeczeństwa i podejmowanie dialogu w niestandardowych miejscach jest efektywne i skuteczne. Dowodzi, że można edukować i budować świadomość społeczną w nowoczesny, otwarty sposób, łącząc to, co ważne z tym, co bliskie ludziom.

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). W szczególności – komunikowano o bieżącej działalności organu nadzorczego, współpracy nawiązanej z innymi instytucjami, programach edukacyjnych, spotkaniach, nałożonych administracyjnych karach pieniężnych i ogólnie – o wszelkich aspektach ochrony danych osobowych.

Rosnące znaczenie danych osobowych dla relacji społecznych i gospodarki sprawiło, że w pracy Urzędu duży nacisk położony został na uproszczenie języka

komunikacji, tak by przekaz Prezesa UODO trafiał do wszystkich, nie tylko do ekspertów, zaś osoby zawodowo zajmujące się danymi osobowymi stały się sojusznikami i partnerami organu w zakresie propagowania ochrony danych osobowych. Prosta komunikacja przyczyniła się zarówno do realizacji prawa osób ze specjalnymi potrzebami, jak i do lepszego zrozumienia zagadnień związanych z danymi osobowymi. Powołany w Urzędzie Zespół ds. Prostego Języka przeprowadził w 2024 r. cykl warsztatów dla pracowników Urzędu, które kontynuowane były także na początku 2025 r.

2.1. Komunikaty

W 2024 r. opublikowanych zostało na stronie internetowej UODO **228 komunikatów**. W podziale na kategorie wygląda to następująco:

- opinie Prezesa UODO – 11,
- wystąpienia – 36,
- komunikaty – 22,
- poradniki – 3,
- „Twoje dane – Twoja sprawa” oraz Dzień Ochrony Danych Osobowych – 10,
- informacje o nałożonych karach – 29,
- naruszenia ochrony danych osobowych – 4,
- plany kontroli – 2,
- informacje o spotkaniach Prezesa UODO – 81,
- informacje o konferencjach – 22,
- inne informacje o działaniach UODO – 8.

2.2. Pytania dziennikarskie

W 2024 roku udzielonych zostało 164 odpowiedzi na pytania od dziennikarzy, w tym od pięciu zagranicznych. Dotyczyły one w sumie 396 szczegółowych zagadnień. Prezes UODO i jego przedstawiciele udzielili 19 wywiadów dla prasy, radia i telewizji. Największe zainteresowania mediów związane były z naruszeniami ochrony danych osobowych w różnych podmiotach. Dziennikarze pytali o to, czy konkretny podmiot zgłosił Prezesowi UODO naruszenie, o szczegóły naruszenia (zwłaszcza, gdy doszło do niego w wyniku działania hakerów), o konsekwencje dla osób, których dane dotyczą, o wysokość kar pieniężnych, które grożą administratorowi w związku z naruszeniem ochrony danych osobowych itd. Dziennikarzy interesowało, czy już wcześniej odnotowano skargi na daną firmę czy instytucję i czy badana była działalność tego podmiotu (np. przeprowadzona została kontrola).

Podmiotem, którego działalność budziła największe zainteresowanie wśród mediów, była spółka Meta. Związane to było z planami spółki dotyczącymi uczenia sztucznej inteligencji z wykorzystaniem danych użytkowników serwisów społecznościowych Facebook i Instagram. Użytkownicy swój sprzeciw wobec takiej praktyki musieli dodatkowo uzasadniać, co budziło wątpliwości z punktu widzenia przepisów RODO. Ponadto Prezes UODO wydał postanowienie zakazujące spółce

Meta publikowania nieprawdziwych postów z wykorzystaniem danych osobowych dwóch osób fizycznych.

Z chwilą pojawienia się na rynku nowej usługi oferowanej przez jakąś firmę, dziennikarze zwracali się z pytaniem do Prezesa UODO, czy badał już wcześniej przetwarzanie danych osobowych u tego podmiotu. Interesowali się też możliwościami wykorzystania algorytmów sztucznej inteligencji do różnych celów.

2.3. Zasięg informacji publikowanych w mediach

1) Informacje o Prezesie UODO

W 2024 r. informacje w mediach dotyczące Prezesa UODO były opublikowane 22 797 razy. Najwięcej materiałów na jego temat pojawiło się w mediach internetowych – stanowiły one 90,4 % wszystkich publikacji. Na kolejnych miejscach znalazły się media radiowe, w których informacje o Prezesie UODO stanowiły 4,48 %, prasa – 3,03 % i telewizje – 2,09 %. Publikacje związane z Prezesem UODO nieco częściej pojawiały się w mediach o charakterze regionalnym – 50,04 %. Natomiast w mediach ogólnokrajowych – 49,96 %. Odnotowane duże zainteresowanie mediów regionalnych miało związek z popularyzacją akcji edukacyjnej pn. „UODO rusza w kraj" i aktywizacją mediów regionalnych w związku z obecnością ekspertów Urzędu w danym województwie.

W przypadku prasy informacje o Prezesie UODO najczęściej pojawiały się w Dzienniku Gazecie Prawnej, Gazecie Podatkowej i w Rzeczpospolitej. Spośród stacji telewizyjnych największą aktywnością w tym zakresie wykazała się TVP Info, a dalej Biznes24 i TVN 24. Z kolei stacje radiowe najczęściej informujące o Prezesie UODO to kolejno: TOK FM, Polskie Radio 24 i Polskie Radio PR 1.

2) Informacje o UODO

W odniesieniu do Urzędu Ochrony Danych Osobowych odnotowano 15 542 informacje. W tym przypadku kolejność mediów pod względem ilości publikacji była nieco inna. Publikacje o UODO w serwisach internetowych stanowiły 92,98 %, w prasowych – 2,9 %, radiowych – 2,57 %, telewizyjnych – 1,55 %. Największe zainteresowanie było w mediach ogólnokrajowych, w których stanowiły one 55,12 informacji na ten temat, a w regionalnych – 44,88 %. Wśród prasy najczęściej o UODO pisały kolejno: Dziennik Gazeta Prawna, Rzeczpospolita, Gazeta Podatkowa.

W przypadku stacji telewizyjnych zainteresowanie w przypadku UODO wyglądało tak samo jak w przypadku Prezesa UODO. Najwięcej materiałów pojawiło się kolejno w: TVP Info, Biznes24 i TVN 24. Nieco inaczej było w przypadku rozgłośni radiowych. O UODO najczęściej informowało Polskie Radio 24 w następnej kolejności Radio TOK FM i Polskie Radio Program 1.

Wniosek: W dobie mediów elektronicznych informacje mają największy zasięg w serwisach internetowych. Zdecydowana większość wpisów o działalności Prezesa UODO i Urzędzie Ochrony Danych Osobowych pojawiła się właśnie w internecie. Wpływ na to miała zarówno liczba takich mediów, łatwość publikacji oraz możliwość

szybkiej reakcji mediów internetowych na komunikaty pojawiające się na stronie internetowej UODO i w mediach społecznościowych, które były później powielane i cytowane. Informacje te często stanowiły pretekst do stworzenia własnych materiałów przez dziennikarzy, którzy odwoływali się do nich bądź je cytowali bezpośrednio[473].

2.4. Pytania od obywateli

W 2024 r. do Departamentu Komunikacji Społecznej wpłynęło ok. **20 zapytań od obywateli**. Najczęściej były w nich poruszane następujące kwestie:

- usterki na stronie internetowej uodo.gov.pl, np. niedziałające linki lub niełądujące się materiały video,
- termin i miejsce zamieszczenia na stronie internetowej materiałów video z wydarzeń organizowanych przez UODO (konferencji, seminariów, webinariów),
- dostępność materiałów zamieszczonych na archiwalnej stronie internetowej UODO,
- odnowienie bazy subskrypcyjnej Biuletynu UODO (trudności z zapisaniem się za pomocą specjalnego formularza, prośby o ręczne dopisanie do listy subskrybentów),
- wnioski o sprostowanie/uzupełnienie treści zamieszczonych w materiałach publikowanych na stronie www.uodo.gov.pl.

Strona internetowa UODO cieszyła się dużym zainteresowaniem. Ponad połowa użytkowników, którzy odwiedzili profil, to nowi odbiorcy, co wskazuje na skuteczne dotarcie do użytkowników oraz duży potencjał w budowaniu zasięgu i zwiększaniu świadomości instytucji. Dane te wskazują, że wiele osób wraca na profil, co można interpretować jako oznaki lojalności i budowania długoterminowego zaangażowania.

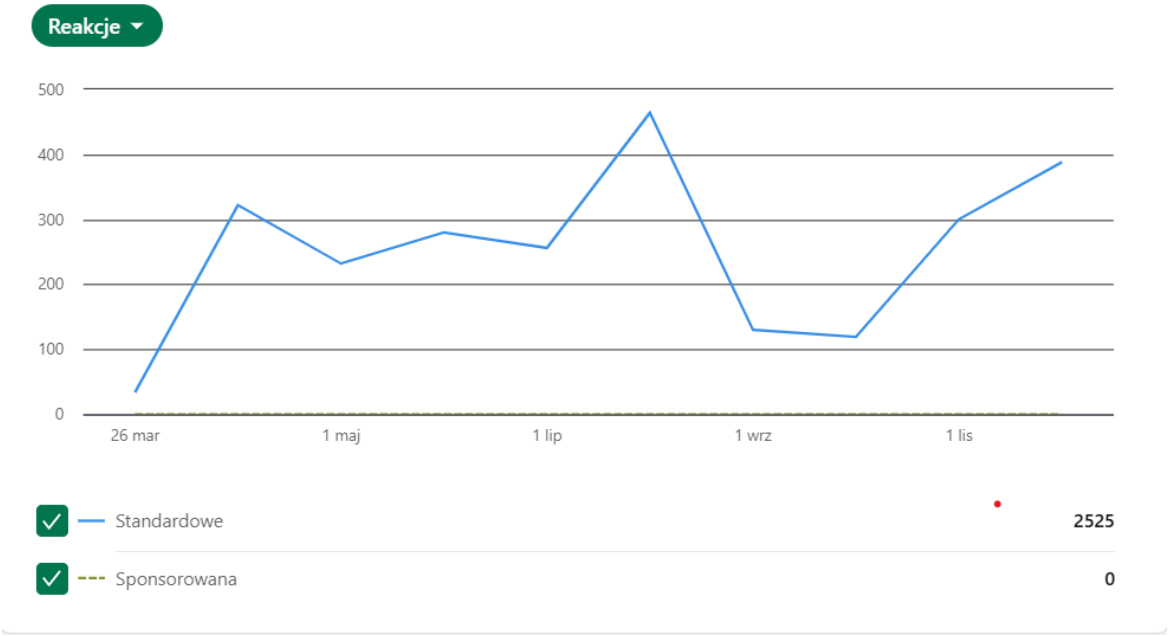
2.5. Social media

Przedstawiamy dane z okresu 27.03.2024 r. – 31.12.2024 r.

2.5.1. LinkedIn

Pierwszy wpis na UODO LinkedIn pojawił się 29.03.2024 r. W sumie, w analizowanym roku 2024 r. na LinkedIn opublikowane zostały 41 wpisy i odnotowano 2525 reakcji użytkowników. Jest to suma wszystkich aktywności, które świadczą o pozytywnym odbiorze publikowanych treści i potwierdzają skuteczne dotarcie do odbiorcy z komunikatem (reakcje „Lubię to”, „Super”, „Gratulacje” itd.).

[473] Źródło danych dotyczących publikacji na temat Prezesa UODO i UODO: PSMM Monitoring & More.



Wykres 22. Dynamika przyrostu liczby obserwujących profil UODO na LinkedIn w okresie 26.03.2024 r. – 31.12.2024 r.

1) Obserwatorzy:

Na koniec roku 2024 UODO miał 4736 obserwujących, w tym nowych – 2018 (przyrost z 281 dni). To bardzo wysoki przyrost biorąc pod uwagę, że Urząd nie prowadzi kampanii reklamowych ani sponsorowanych. Najpopularniejszym postem był wpis informujący o wywiadzie, jakiego Mirosław Wróblewski, Prezes UODO, udzielił kanałowi HRejterzy m.in. na temat kompetencji organu nadzorczego, administracyjnych kar pieniężnych za nieprzestrzeganie RODO i ochrony danych osobowych w Polsce. Wpis wyświetlony został 3543 razy. Inne popularne wpisy dotyczyły projektowania prywatności na przykładzie Internetu rzeczy (2743 wyświetlenia), prywatności jako fundamencie wolności w erze cyfrowej oraz publikacji biuletynu UODO (2728 wyświetleń).

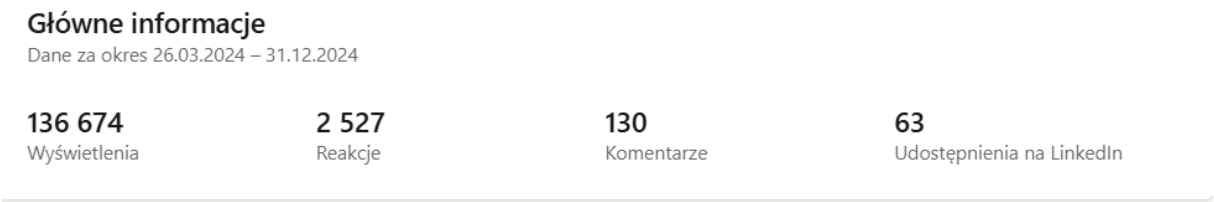
Wskaźnik zaangażowania na podstawie głównych informacji wyniósł 2 %, co jest dobrym wynikiem, jak na profil instytucji publicznej, działającej bez wsparcia płatnych kampanii[474]. Świadczy to, że:

- treści są trafne i wartościowe,
- profil skutecznie zachęca do interakcji,
- użytkownicy realnie wchodzą w interakcje z profilem.

Skuteczność działania pokazuje, że profil UODO nie potrzebuje zasilania płatnymi kampaniami, bo działania organiczne sprawdzają się dobrze. Komentarze i udostępnienia wskazują na to, że treści budzą zainteresowanie, refleksje są

[474] Średni wskaźnik zaangażowania na LinkedIn dla firm i urzędów waha się w przedziale 0,5 – 1 %.

praktyczne i eksperckie, co powoduje, że ludzie chcą się nimi dzielić dalej, podbijając tym samym profesjonalizm samego profilu, co obrazuje poniższe zestawienie:



Wniosek: Treści publikowane na profilu mają wysoką wartość merytoryczną dla odbiorców i są dostosowane do ich oczekiwań. Ich jakość i trafność przyciągają użytkowników, co świadczy o skutecznej strategii obecności UODO w social mediach.

2.5.2. Portal X

Na profilu UODO na X opublikowano 550 wpisów i jest to najlepszy wynik w porównaniu do dwóch ostatnich lat (w 2023 r. – 495 wpisów, w 2022 r. – 536 wpisów).

Wniosek: Wysoki współczynnik zaangażowania potwierdza, że treści trafiają w potrzeby odbiorców. Duża liczba udostępnień i podanych dalej postów (razem ponad 1000) wskazuje, że materiały UODO są postrzegane jako wartościowe.

W okresie od 27 03. do 31.12.2024 r. treści zostały wyświetlone 302,5 tys. razy.

Podsumowanie działań na social mediach:

W 2024 r. aktywność UODO w mediach społecznościowych pokazała, że świadoma, systematyczna i merytoryczna obecność w tych kanałach obiegu informacji, może przynieść wymierne efekty. Social media stają się coraz ważniejszym kanałem komunikacji dla Urzędu Ochrony Danych Osobowych.

2.6. Biuletyn

W czerwcu 2024 roku na łamach „Biuletynu UODO” rozpoczęła się akcja informowania subskrybentów, że od 1 września 2024 r. rozpoczyna się od podstaw proces gromadzenia nowych adresów mailowych subskrybentów tego periodyku. Baza danych subskrybentów „Biuletynu UODO” w szczytowym momencie (koniec sierpnia 2024 r.) liczyła niemal 11 500 tysięcy adresów poczty elektronicznej. Wiele z nich zawierało imię, nazwisko, a domena wskazywała na nazwę organizacji. Zgodnie z zasadą prawidłowości danych – przepisy rozporządzenia 2016/679 wymagają, by dane osobowe były prawidłowe i w razie potrzeby uaktualniane – zaktualizowano dane abonentów, by Biuletyn trafiał wyłącznie do zainteresowanych subskrybentów. 1 września lista dystrybucyjna biuletynu została więc wyzerowana, a proces zbierania subskrybentów ruszył od nowa.

Na koniec 2024 roku liczba subskrybentów wynosiła ok. 2000 osób – tyle osób na nowo zapisało się do subskrypcji Biuletynu.

2.7. Współpraca międzynarodowa

W 2024 roku, w ramach współpracy międzynarodowej odbyło się online **11 Spotkań Sieci Rzeczników (Communications Network Meetings)[475].** Spotkania służą:

1. Informowaniu o bieżących działaniach komunikacyjnych Europejskiej Rady Ochrony Danych.
2. Koordynowaniu działań komunikacyjnych na linii EROD – organy krajowe.
3. Wymianie informacji o bieżących działaniach komunikacyjnych podejmowanych w poszczególnych organach krajowych.

Ad 1. Europejska Rada Ochrony Danych informuje przede wszystkim o działaniach związanych z posiedzeniami plenarnymi oraz o pracach nad wytycznymi, opiniami, zaleceniami oraz nad realizacją strategii EROD. Komunikaty prasowe publikowane są na oficjalnej stronie https://www.edpb.europa.eu/. Do działań komunikacyjnych EROD należą również materiały edukacyjne, materiały informujące o organizowanych wydarzeniach, czy o zmianach w strukturze organizacyjnej EROD. Na stronie internetowej EROD oddzielną sekcję zajmuje zakładka „informacje krajowe" (national news), na której publikowane są komunikaty opracowywane przez krajowe organy ochrony danych, dotyczące ważnych decyzji karowych wydanych w krajach członkowskich.

Materiały EROD opublikowane na stronie internetowej UODO objęły m.in.:

- raport na temat ustaleń w ramach drugiego skoordynowanego egzekwowania prawa, koncentrującego się na wyznaczaniu i pozycji inspektorów ochrony danych (IOD),
- opinia dot. zgody na przetwarzanie danych osobowych do celów reklamy behawioralnej w modelu „zgoda lub zapłata" wdrażanym przez duże platformy internetowe,
- opinia w sprawie wykorzystywania technologii rozpoznawania twarzy do usprawnienia przepływu pasażerów w portach lotniczych (zgodność z art. 5 ust. 1 lit. e i f, art. 25 i art. 32 RODO),
- sprawozdanie z pierwszego przeglądu ram ochrony danych UE–USA,
- określenie priorytetów EROD na lata 2024–2027,
- zatwierdzenie certyfikacji Znaku jakości ochrony danych UE (EU Data Protection Seal),
- oświadczenie dotyczące drugiego raportu Komisji Europejskiej na temat stosowania ogólnego rozporządzenia o ochronie danych (RODO),
- opinia w sprawie wykorzystywania danych osobowych do opracowywania i wdrażania modeli sztucznej inteligencji,
- wytyczne w sprawie pseudonimizacji.

[475] To organizowane raz w miesiącu spotkania prowadzone przez pracowników EROD z Sektora Informacji i Komunikacji (Information and Communications Sector), z udziałem pracowników krajowych organów ochrony danych odpowiedzialnych za działania komunikacyjne.

Ad 2. Koordynacja działań komunikacyjnych polega na wskazywaniu terminu publikacji komunikatu EROD lub innych materiałów po posiedzeniu plenarnym, które następnie są przekazywane w ramach sieci do konsultacji – zgłaszania uwag oraz akceptacji. Do działań koordynacyjnych należy również zapraszanie do wspólnych działań organizowanych przez EROD i informowanie o nich za pośrednictwem krajowych kanałów komunikacji (strony internetowej, media społecznościowe). W organizowanych corocznie Dniach Otwartych Unii Europejskiej uczestniczył przedstawiciel UODO. Wydarzenie odbyło się 4 maja 2024 r. w siedzibie Komisji Europejskiej, w Brukseli, na wspólnym posiedzeniu Europejskiej Rady Ochrony Danych i Europejskiego Inspektora Ochrony Danych. Szczegółowa relacja z wydarzenia została zamieszczona w majowym wydaniu Biuletynu UODO (nr 05/05/24).

Ad 3. Wymiana informacji pomiędzy organami nadzorczymi dotyczyła wzajemnego informowania się o bieżących postępowaniach transgranicznych (one-shop-mechanism cases) lub innych ważnych postępowaniach krajowych, które mogą wiązać się z dużym zainteresowaniem społecznym i medialnym. Spotkania dają możliwość wzajemnego informowania się o otrzymywanych pytaniach dziennikarskich. Zdarza się, że to samo zapytanie rozsyłane było do co najmniej kilku krajów członkowskich. Tematyka odnotowanych w 2024 r. pytań najczęściej dotyczyła:

- legalności przetwarzania danych przez DeepSeek R1 (chatbot bazujący na technologii generatywnej sztucznej inteligencji, oferowany przez spółkę zarejestrowaną w Chinach),
- propozycji spółki Meta Platforms Limited, skierowanej do Komisji Europejskiej i irlandzkiego organu nadzorczego (Data Protection Comission) dot. wprowadzenia płatnej subskrypcji dla użytkowników Europejskiego Obszaru Gospodarczego w zamian za wyłączenie mechanizmu targetowanej reklamy.

Z punktu widzenia polskiego organu ochrony danych duże zainteresowanie wzbudziło wydanie przez litewski organ ochrony danych decyzji nakładającej administracyjną karę pieniężną na spółkę UAB Vinted. Sprawa dotyczyła również polskich użytkowników litewskiej platformy sprzedażowej, którzy wnieśli skargi na niezgodne z przepisami o ochronie danych osobowych przetwarzanie danych przez ten podmiot. Podczas spotkań omawiano też inne tematy, jak dochodzenie w sprawie transferu danych przez TikTok Technology Limitet czy decyzja holenderskiego organu nakładająca karę na Uber.

IV. Uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się ochroną danych osobowych

1. Udział UODO w pracach 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 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. Opracowane stanowiska oraz projekty dokumentów są następnie przedmiotem dyskusji i zostają przyjmowane na comiesięcznych posiedzeniach plenarnych EROD. Porządki obrad i komunikaty z sesji plenarnych są publikowane na stronie internetowej UODO.

W 2024 roku, w ramach prac podgrup i grup zadaniowych EROD, przedstawiciele polskiego organu nadzorczego wraz z reprezentantami pozostałych organów, opracowali w ostatnich latach szereg dokumentów w celu promowania wspólnego zrozumienia rozporządzenia. Polski organ nadzorczy w 2024 r. był współautorem m.in. wymienionych poniżej dokumentów.

Wytyczne:

1. Wytyczne 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f RODO, przyjęte 8 października 2024 r.

Opinie:

1. Opinia 08/2024 w sprawie ważnej zgody w kontekście modeli „zgoda lub zapłata” stosowanych przez duże platformy internetowe, przyjęta 17 kwietnia 2024 r.
2. Opinia 22/2024 w sprawie niektórych obowiązków wynikających z polegania na podmiotach przetwarzających i podprzetwarzających, przyjęta 7 października 2024 r.
3. Opinia 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli AI, przyjęta 17 grudnia 2024 r.

2. 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. 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 2024 r. EROD wybrała obszar „Wdrażanie prawa dostępu przez administratorów". Co roku organy nadzorcze wchodzące w skład EROD w ramach skoordynowanego egzekwowania prawa (Coordinated Enforcement Framework – CEF) przeprowadzają badanie poświęcone ustalonemu wcześniej tematowi. W 2024 r. 30 organów ochrony danych w całym Europejskim Obszarze Gospodarczym (w tym EIOD) wszczęło skoordynowane postępowania, oceniając, czy formalne postępowanie wyjaśniające było uzasadnione, lub przeprowadzając działania mające na celu ustalenie faktów. Na akcję odpowiedziało 1185 administratorów.

2) 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. W 2024 r. EROD zorganizowała warsztaty dotyczące audytu aplikacji mobilnych, w których uczestniczyli przedstawiciele UODO.

2.1.1. Współpraca w ramach IMI

Od 25 maja 2018 r. organy nadzorcze korzystają z systemu wymiany informacji na rynku wewnętrznym[476], 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.

Zgodnie z danymi z systemu IMI w terminie od 1 stycznia do 31 grudnia 2024 r. Urząd Ochrony Danych Osobowych:

1) był organem wiodącym w **12** sprawach w rejestrze spraw IMI,

[476] Ang. *Internal Market Information System*, dalej: „system IMI" lub „IMI".

2) zainicjował i przesłał do innych organów nadzorczych **130** powiadomień, w tym:
   - **20** z art. 56 RODO (identyfikacja wiodącego organu nadzorczego i organu, którego sprawa dotyczy),
   - **1** z art. 60 RODO (w ramach wymiany istotnych decyzji),
   - **109** z art. 61 RODO (dobrowolna wzajemna pomoc);
3) otrzymał łącznie **2 444** wnioski, w tym:
   - **883** z art. 56 RODO (identyfikacja wiodącego organu nadzorczego i organu, którego sprawa dotyczy),
   - **1 092** z art. 60 RODO (współpraca między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy), w tym:
     - **261 projektów decyzji,**
     - **62 w ramach wymiany istotnych decyzji,**
     - **11 zmienionych projektów decyzji,**
     - **497 ostatecznych decyzji,**
   - **434** z art. 61 RODO (dobrowolna wzajemna pomoc),
   - **29** z art. 64 RODO (opinia EROD),
   - **2** z art. 65 RODO (w ramach rozstrzygania sporów przez EROD, procedura pisemna),
   - **4** z art. 65 RODO (w ramach przyjętych środków tymczasowych).

2.1.2. 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.

2.1.3. Skoordynowany nadzór nad wielkoskalowymi systemami

Istotnym obszarem działalności Prezesa UODO w 2024 r. pozostawała współpraca międzynarodowa w ramach art. 62 rozporządzenia 2018/1725[477], która przewiduje skoordynowany nadzór, mający zastosowanie w przypadku, gdy odpowiednie prawo Unii Europejskiej odnosi się do tego artykułu.

Zgodnie z tym przepisem Europejski Inspektor Ochrony Danych (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 Europejskiej. Skoordynowane działania obejmują

[477] 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.

m.in. wspólne kontrole i dochodzenia oraz prace nad wspólną metodologią. Do tego celu powołano Komitet Skoordynowanego Nadzoru (CSC)[478], który obejmuje skoordynowane działania nadzorcze nad:

- Systemem Informacyjny Schengen (SIS),
- Systemem Wjazdu/Wyjazdu (EES),
- Europejskim systemem informacji o podróży oraz zezwoleń na podróż (ETIAS),
- Europejskim systemem przekazywania informacji z rejestrów karnych dotyczącym
- osób niebędących obywatelami UE (ECRIS-TCN),
- Interoperacyjnością systemów EES, ETIAS, ECRIS-TCN, EURODAC, SIS i VIS,
- Agencją Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach
- Karnych (Eurojust),
- Prokuraturą Europejską (EPPO),
- Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (Europol),
- Prüm II,
- Systemem wymiany informacji na rynku wewnętrznym (IMI).

Ważnym zadaniem Komitetu było badanie trudności w interpretacji lub stosowaniu przepisów prawa UE w odniesieniu do wielkoskalowych systemów i organów informacyjnych. Korzystanie z tych systemów musi odbywać się w zgodzie z prawem krajowym, 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 uczestniczyli przedstawiciele UODO, była wymiana doświadczeń i propozycji 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.

Należy podkreślić, że w związku z decyzją Komisji Europejskiej potwierdzającą uczestnictwo Polski we wzmocnieniu współpracy w zakresie ustanowienia Prokuratury Europejskiej[479], Prezes UODO został przyjęty w poczet członków Komitetu Skoordynowanego Nadzoru nad przekazywaniem danych z wykorzystaniem kanałów

[478] Więcej informacji o Komitecie dostępnych jest na stronie EROD: https://edpb.europa.eu/csc/about-csc/who-we-are-coordinated-supervision-committee_pl.

[479] Decyzja Komisji (UE) 2024/807 z 29 lutego 2024 r. potwierdzająca uczestnictwo Polski we wzmocnionej współpracy w zakresie ustanowienia Prokuratury Europejskiej, Dz. U. UE L 2024 poz. 807.

komunikacji Prokuratury Europejskiej (EPPO), które wymaga podjęcia działań na poziomie krajowym.

Przedstawiciele Prezesa UODO uczestniczyli także w posiedzeniach wyspecjalizowanych grup:

- 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 w charakterze eksperta w zespole prowadzącym kontrole w zakresie oceny i monitorowania stosowania dorobku Schengen w obszarze ochrony danych osobowych w jednym z państw Strefy Schengen, zgodnie z rozporządzeniem 2022/922[480]. Kontrola taka polega na dokonaniu ewaluacji, w jaki sposób państwa członkowskie wdrażają i stosują dorobek Schengen, w szczególności w odniesieniu do SIS i VIS w kontekście wymogów ochrony danych. Badaniem obejmuje się również rolę organów ochrony danych w odniesieniu do nadzoru nad organami zarządzającymi i korzystającymi z SIS i VIS. Ocena stanowi gwarancję tego, że państwa członkowskie stosują przepisy dotyczące Strefy Schengen skutecznie i zgodnie z podstawowymi zasadami i normami. Za wdrożenie mechanizmu oceny i monitorowania odpowiadają wspólnie państwa członkowskie i Komisja Europejska przy wsparciu organów i jednostek organizacyjnych Unii Europejskiej uczestniczących we wdrażaniu dorobku Schengen.

2.1.4. 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 uczestników postępowania przed TSUE. Po wydaniu wyroku przez TSUE organ nadzorczy przedstawia swoje stanowisko w sprawie potrzeby zmiany polskiego prawa lub sposobu jego interpretacji.

[480] 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. U. UE L z 2022 r. poz. 160.

Organ nadzorczy dokonuje – niezależnie od powyższego – regularnego przeglądu wszystkich postępowań inicjowanych przez TSUE pod kątem zagadnień z zakresu ochrony danych osobowych.

1) Analiza wniosków prejudycjalnych

Organ nadzorczy dokonał analizy przekazanych przez KPRM wniosków prejudycjalnych. Jako przykłady najbardziej istotnych spraw można wskazać następujące:

- **C-312/24 Darashev** – sprawa dotyczyła kwestii możliwości administratora będącego jednocześnie pracodawcą oraz organem prowadzącym postępowanie karne do przetwarzania danych pochodzących z postępowania karnego przeciwko pracownikowi jako pracodawca – w ocenie organu nadzorczego udział w postępowaniu był zasadny[481].
- **C-374/24 Comdribus** – sprawa dotyczyła systematycznego zbierania danych identyfikacyjnych osób, w odniesieniu do których istniał jeden lub więcej powodów, aby podejrzewać, że popełniły lub usiłowały popełnić przestępstwo. Sprawa dotyczyła także na kwestii dopuszczalności odrębnego ścigania i skazania osoby, która odmówiła poddania się zebraniu danych identyfikacyjnych, nawet jeśli osoba ta nie była ścigana ani skazana za przestępstwo, które stanowiło podstawę zastosowania tego środka – w ocenie organu nadzorczego udział w postępowaniu był zasadny[482].
- **C-414/24 Datenschutzbhörde** – sprawa dotyczyła możliwości wniesienia przez osobę, której dane dotyczą skargi do organu nadzorczego oraz jednocześnie skorzystania przez nią z prawa do skutecznego środka ochrony prawnej przed sądem – w ocenie organu nadzorczego udział w postępowaniu był zasadny[483].
- **C-422/24 Storstockholms Lokaltrafik** – sprawa dotyczyła możliwości przetwarzania danych osobowych pochodzących z kamer nasobnych używanych przez kontrolerów biletów podczas kontroli – w ocenie organu nadzorczego udział w postępowaniu był zasadny[484].
- **C-468/24 Netz Niederösterreich** – sprawa dotyczyła przetwarzania danych osobowych uzyskanych w wyniku działania inteligentnego systemu opomiarowania zużycia energii – w ocenie organu nadzorczego udział w postępowaniu był zasadny[485].
- **C-474/24 NADA Austria e.a.** – sprawa dotyczyła udostępnienia danych osobowych w postaci imion i nazwisk sportowców w związku z naruszeniem

[481] DOL.0623.5.2024.
[482] DOL.0623.7.2024.
[483] DOL.0623.9.2024.
[484] DOL.0623.10.2024.
[485] DOL.0623.12.2024.

przez nich przepisów ustawy antydopingowej – w ocenie organu nadzorczego udział w postępowaniu był zasadny[486].

- **C-661/24 Académie Fiscale e.a.** – sprawa dotyczyła przetwarzania danych osobowych w sektorze łączności elektronicznej, w szczególności proporcjonalności przyjętych w regulacjach krajowych przepisów odnoszących się do zatrzymywania danych o ruchu i lokalizacji w celu zwalczania oszustw i wykorzystania sieci w sposób niedozwolony – w ocenie organu nadzorczego udział w postępowaniu był zasadny[487].

W 2024 r. organ nadzorczy dokonał analizy wpływu na przepisy polskiego prawa 27 wyroków wydanych przez TSUE, z których najważniejsze dotyczyły spraw:

- **C-231/22 État belge** – Trybunał wskazał, że art. 4 pkt 7 RODO należy interpretować w ten sposób, że jednostka lub podmiot prowadzące dziennik urzędowy państwa członkowskiego, które na mocy ustawodawstwa tego państwa są w szczególności zobowiązane do publikowania w niezmienionej postaci aktów i dokumentów urzędowych sporządzonych przez osoby trzecie na ich własną odpowiedzialność z poszanowaniem obowiązujących przepisów, a następnie przekazanych organowi sądowemu, który kieruje je do nich do publikacji, mogą – mimo że nie posiadają one osobowości prawnej – zostać uznane za „administratora" danych osobowych zawartych w tych aktach i dokumentach, jeżeli odnośne prawo krajowe określa cele i sposoby przetwarzania danych osobowych przez ten dziennik urzędowy. Art. 5 ust. 2 RODO w związku z jego art. 4 pkt 7 i art. 26 ust. 1 należy interpretować w ten sposób, że jednostka lub podmiot prowadzące dziennik urzędowy państwa członkowskiego, uznane za administratora w rozumieniu art. 4 pkt 7 tego rozporządzenia, są wyłącznie odpowiedzialne za przestrzeganie zasad, o których mowa w jego art. 5 ust. 1, w odniesieniu do operacji przetwarzania danych osobowych, do których wykonywania są one zobowiązane na mocy prawa krajowego, chyba że z prawa tego wynika wspólna odpowiedzialność z innymi podmiotami w odniesieniu do tych operacji. W ocenie organu nadzorczego wyrok może skutkować koniecznością dokonania zmian w polskim prawie. Za istotne organ nadzorczy uznał podjęcie dyskusji na temat zmiany przepisów ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych.
- **C-118/22 Direktor na Glavna direktsia „Natsionalna politsia" pri Ministerstvo na vatreshnite raboti – Sofia** – TSUE stwierdził, że art. 4 ust. 1 lit. c) i e) dyrektywy 2016/680 w zw. z art. 5 i 10, art. 13 ust. 2 lit. b) oraz art. 16 ust. 2 i 3 tej dyrektywy i art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej należy interpretować w ten sposób, że stoi on na przeszkodzie ustawodawstwu krajowemu przewidującemu przechowywanie przez organy policji do celów

[486] DOL.0623.14.2024.
[487] DOL.0623.18.2024.

zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar danych osobowych, zwłaszcza danych biometrycznych i genetycznych, dotyczących osób, które zostały prawomocnie skazane za umyślne przestępstwo ścigane z oskarżenia publicznego, aż do chwili śmierci osoby, której dane dotyczą, w tym w przypadku zatarcia skazania tej osoby, bez nałożenia na administratora obowiązku okresowego przeglądu, czy takie przechowywanie jest nadal niezbędne, ani przyznania wspomnianej osobie prawa do usunięcia tych danych, od chwili gdy ich przechowywanie nie jest już niezbędne do celów, dla których były one przetwarzane, lub w stosownym przypadku do ograniczenia ich przetwarzania. W ocenie organu nadzorczego wyrok TSUE pociąga za sobą konieczność rozważenia zmiany ustawy z 6 kwietnia 1990 r. o Policji w zakresie uregulowań dotyczących Krajowego Systemu Informacyjnego Policji.

- **C- 61/22 Landeshauptstadt Wiesbaden** – TSUE stwierdził, że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157 z 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się jest nieważne. Skutki rozporządzenia 2019/1157 zostają utrzymane do czasu wejścia w życie, w rozsądnym terminie, który nie może przekroczyć dwóch lat, licząc od dnia 1 stycznia roku następującego po dniu ogłoszenia niniejszego wyroku, nowego rozporządzenia, przyjętego na podstawie art. 77 ust. 3 TFUE, które je zastąpi. W ocenie organu nadzorczego wyrok TSUE pociąga za sobą konieczność dokonania przez polskiego projektodawcę pogłębionej analizy sposobu przetwarzania danych biometrycznych w dowodach osobistych[488].

- **C-470/21 La Quadrature du Net** – w ocenie TSUE 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 (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r., w świetle art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że nie stoi on na przeszkodzie uregulowaniu krajowemu, które zezwala organowi publicznemu odpowiedzialnemu za ochronę praw autorskich i praw pokrewnych przed naruszeniami tych praw, do których dochodzi w Internecie, na dostęp do przechowywanych przez dostawców publicznie dostępnych usług łączności elektronicznej danych dotyczących tożsamości cywilnej odpowiadających adresom IP zbieranym wcześniej przez organizacje zrzeszające uprawnionych, aby ów organ mógł zidentyfikować posiadaczy tych adresów wykorzystywanych do aktywności mogącej stanowić takie naruszenia i aby mógł on w razie

[488] DOL.0623.8.2022.

potrzeby zastosować wobec nich środki, pod warunkiem że na mocy tego uregulowania:

- dane te przechowywane są w warunkach i zgodnie z zasadami technicznymi, które gwarantują, że wykluczone jest, by ich przechowywanie mogło pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego tych posiadaczy, na przykład poprzez ustalenie ich szczegółowego profilu, co można osiągnąć w szczególności poprzez nałożenie na dostawców usług łączności elektronicznej obowiązku przechowywania poszczególnych kategorii danych osobowych, takich jak dane dotyczące tożsamości cywilnej, adresy IP oraz dane o ruchu i dane dotyczące lokalizacji, gwarantującego rzeczywiście szczelne odseparowanie tych poszczególnych kategorii danych, które uniemożliwia na etapie przechowywania wszelkie powiązanie tych poszczególnych kategorii danych, przez okres nieprzekraczający tego, co ściśle niezbędne;
- dostęp tego organu publicznego do takich danych przechowywanych w sposób odseparowany i rzeczywiście szczelny służy wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego i towarzyszą mu gwarancje niezbędne do wykluczenia, by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP, na przykład poprzez ustalenie ich szczegółowego profilu, co wymaga w szczególności, by upoważnionych do posiadania takiego dostępu urzędników owego organu obowiązywał zakaz ujawniania w jakiejkolwiek formie informacji na temat zawartości plików przeglądanych przez tych posiadaczy, z jedynym wyjątkiem wiążącym się z ujawnieniem ich w celu zawiadomienia prokuratury, zakaz śledzenia historii treści przeglądanych przez owych posiadaczy oraz, ogólniej, zakaz wykorzystywania tych adresów IP do celów innych niż zidentyfikowanie ich posiadaczy, aby zastosować wobec nich ewentualne środki;
- możliwość powiązania przez osoby odpowiedzialne w ramach wspomnianego organu publicznego za analizę zdarzeń takich danych z plikami zawierającymi elementy umożliwiające poznanie tytułów utworów chronionych, których udostępnienie w Internecie uzasadniało zebranie adresów IP przez organizacje zrzeszające uprawnionych, jest uzależniona – w przypadkach kolejnego ponowienia aktywności naruszającej prawa autorskie lub prawa pokrewne przez tę samą osobę – od dokonania przez sąd lub niezależny organ administracyjny kontroli, która nie może być w pełni zautomatyzowana i powinna mieć miejsce przed dokonaniem takiego powiązania, ponieważ powiązanie to może w takich przypadkach pozwolić na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego wspomnianej osoby, której adres IP wykorzystano do aktywności mogącej naruszać prawa autorskie lub prawa pokrewne;

- system przetwarzania danych wykorzystywany przez organ publiczny podlega w regularnych odstępach czasu kontroli niezależnego organu mającego status strony trzeciej w stosunku do tego organu publicznego, mającej na celu weryfikację integralności systemu, w tym skutecznych gwarancji chroniących przed ryzykiem takiego dostępu do tych danych lub takiego ich wykorzystywania, które nosiłyby znamiona nadużycia lub byłyby niezgodne z prawem, oraz jego skuteczności i niezawodności w wykrywaniu ewentualnych uchybień.

W ocenie organu nadzorczego wyrok może skutkować koniecznością dokonania zmian w polskim prawie. Na gruncie prawa polskiego brak jest bowiem przepisów, które gwarantowałyby zachowanie wskazanych przez TSUE warunków udostępniania danych osobowych chronionych tajemnicą telekomunikacyjną[489].

- **C-229/23 HYA i in. II** – TSUE stwierdził, że 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 (dyrektywy o prywatności i łączności elektronicznej), rozpatrywany w świetle art. 47 akapit drugi Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że nie stoi on na przeszkodzie przepisom prawa krajowego wymagającym, aby orzeczenie sądowe zezwalające na zastosowanie, bez zgody zainteresowanych użytkowników, kontroli, przejmowania i przechowywania komunikatów samo zawierało wyraźne uzasadnienie na piśmie, niezależnie od istnienia uzasadnionego wniosku organów postępowania karnego. W ocenie organu nadzorczego wyrok może skutkować koniecznością dokonania zmian w polskim prawie. Organ nadzorczy zwrócił uwagę, że z wyroku wynika potrzeba dokonania zmian w stosowaniu przez organy państwa tzw. kontroli operacyjnej dotyczącej danych telekomunikacyjnych[490].
- **C-548/21 CG v Bezirkshauptmannschaft Landeck** – Trybunał wskazał, że w analizowanej sprawie nie znajdują zastosowania przepisy dyrektywy 2002/58, co nie stało na przeszkodzie rozstrzygnięciu sprawy z punktu widzenia przepisów dyrektywy 2016/680. Trybunał wskazał przy tym, że w przypadku, gdy policja zatrzymuje telefon i posługuje się nim w celu pobrania zawartych w nim danych osobowych i zapoznania się z nimi, rozpoczyna się proces przetwarzania danych osobowych w rozumieniu art. 3 ust. 2 dyrektywy 2016/680, nawet jeśli ze względów technicznych policja nie uzyska dostępu do tych danych. W ocenie organu nadzorczego wyrok może skutkować koniecznością dokonania zmian w polskim prawie poprzez podjęcie możliwie pilnych działań legislacyjnych mających na celu zapewnienie skutecznej ochrony prawa do prywatności i ochrony danych osobowych w odniesieniu do przepisów dotyczących stosowania przez organy policji kontroli operacyjnej[491].

[489] DOL.0623.15.2021.
[490] DOL.0623.18.2023.
[491] DOL.0623.29.2021.

- **C-178/22 Procura della Repubblica presso il Tribunale di Bolzano** – TSUE uznał, że artykuł 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 (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z 25 listopada 2009 r., w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że nie stoi on na przeszkodzie przepisowi krajowemu zobowiązującemu sąd krajowy, orzekający w ramach uprzedniej kontroli dokonywanej po przedstawieniu przez właściwy organ krajowy w ramach karnego postępowania przygotowawczego uzasadnionego wniosku o dostęp do zbioru danych o ruchu lub danych o lokalizacji mogących pozwolić na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego użytkownika środka łączności elektronicznej, które to dane są zatrzymywane przez dostawców usług łączności elektronicznej, do wydania zgody na udzielenie tego dostępu, jeżeli zażądano go do celów dochodzenia przestępstw zagrożonych w prawie krajowym karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata, z zastrzeżeniem, że istnieją wystarczające przesłanki popełnienia takich przestępstw i że dane te są istotne dla ustalenia okoliczności faktycznych, pod warunkiem jednak, że ów sąd jest uprawniony do odmowy udzielenia wspomnianego dostępu, jeżeli jest on wnioskowany w ramach dochodzenia dotyczącego przestępstwa, które w sposób oczywisty jest przestępstwem mniejszej wagi w świetle warunków społecznych panujących w danym państwie. TSUE wskazał, że art. 15 ust. 1 dyrektywy 2002/58 stoi na przeszkodzie środkom ustawodawczym przewidującym prewencyjne, tzn. ujęte w sposób generalny i niezróżnicowany, przesłanki zatrzymywania przez dostawców danych o ruchu i danych o lokalizacji. Dostępu do tych danych nie uzasadnia również cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i karaniu ogółu przestępstw, gdyż jest on uzasadniony wyłącznie w przypadku zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego. TSUE uznał, że zdefiniowanie „poważnego przestępstwa” do celów stosowania art. 15 ust. 1 dyrektywy 2002/58 należy do kompetencji państw członkowskich, przy czym uznanie za poważne przestępstwo czynów zagrożonych karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż przewidziany w ustawie okres, jest oparta na kryterium obiektywnym przyznania dostępu do danych. Co istotne, z treści orzeczenia TSUE wynika, że prawo krajowe w przedmiocie uzyskiwania dostępu do danych o ruchu i lokalizacji podmiotu objętego postępowaniem karnym powinno spełniać określone warunki, tj. przepisy krajowe powinny zawierać jasne i precyzyjne przepisy regulujące zakres i przesłanki stosowania dostępu do danych. Co do zasady dostęp powinien być przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o udział w poważnym przestępstwie. Jednocześnie dostęp do danych przez organy krajowe powinien być

uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, które powinny mieć zapewnioną możliwość podjęcia decyzji odmownej. W ocenie organu nadzorczego konieczna jest zmiana właściwych przepisów regulujących dostęp organów prowadzących postępowanie karne do danych osobowych chronionych tajemnicą telekomunikacyjną[492].

2) Ocena wpływu wyroków TSUE na polskie prawo

Organ nadzorczy dokonał analizy wpływu wyroków TSUE na polskie prawo także w sprawach: C-461/22 MK[493], C-590/22 PS[494], C-182/22 i C-189/22[495], C-741/21 juris[496], C-507/23 Patērētāju tiesību aizsardzības centrs[497], C-21/23 Lindenapotheke[498], C-446/21 Maximilian Schrems[499], C-621/22 Koninklijke Nederlandse Lawn Tennisbond[500], C-17/22 i C-18/22 HTB Neunte Immobilien Portfolio i in.[501], C-740/22 Endemol Shine Finland[502], C-200/23 Agencija po vpisvanijata[503], C-65/23 K GmbH[504], C-757/22 Meta Platforms Ireland[505], C-687/21 MediaMarktSaturn (d. Saturn Electro)[506], C-33/22 Österreichische Datenschutzbehörde[507], C-667/21 Krankenversicherung Nordrhein[508], C-604/22 IAB Europe[509], C-46/23 Újpesti Polgármesteri Hivatal[510], C-741/21 juris GmbH[511], C-768/21 Land Hessen[512]. W wymienionych sprawach organ nadzorczy nie stwierdził jednak konieczności dokonania zmian w prawie polskim.

Organ nadzorczy skierował **wystąpienie do Ministra do spraw Unii Europejskiej**[513], w którym zwrócił się o informację odnośnie do planowanych zmian legislacyjnych, stosownie do treści wyroków TSUE, co do których wskazywał, że wymagają dokonania zmian w polskim prawie. W odpowiedzi Minister do spraw Unii Europejskiej wskazał, w kontekście stanowisk przekazanych przez inne resorty, że wyrok C-470/21 La Quadrature du Net powoduje konieczność nowelizacji ustawy – Kodeks postępowania karnego. Minister do spraw Unii Europejskiej podzielił zdanie

[492] DOL.0623.11.2022.
[493] DOL.0623.23.2022.
[494] DOL.0623.24.2022.
[495] DOL.0623.14.2022.
[496] DOL.0623.2.2022.
[497] DOL.0623.27.2023.
[498] DOL.0623.4.2023.
[499] DOL.0623.21.2021.
[500] DOL.0623.26.2022.
[501] DOL.0623.6.2022.
[502] DOL.0623.2.2023.
[503] DOL.0623.11.2023.
[504] DOL.0623.8.2023.
[505] DOL.0623.3.2023.
[506] DOL.0623.1.2022.
[507] DOL.0623.9.2022.
[508] DOL.0623.28.2021.
[509] DOL.0623.25.2022.
[510] DOL.0623.6.2023.
[511] DOL.0623.2.2022.
[512] DOL.0623.4.2022.
[513] DOL.413.14.2024.

organu nadzorczego co do konieczności dokonania zmiany w przepisach krajowych w związku z wyrokiem w sprawie C-231/22 État belge.

2.1.5. Przekazywanie danych osobowych poza EOG

W 2024 r. do Urzędu wpłynęły informacje i zapytania od organów nadzorczych z Europejskiego Obszaru Gospodarczego („EOG") dotyczące wiążących reguł korporacyjnych (dalej WRK) w ponad 60 różnych grupach kapitałowych.
Dotyczyły one przede wszystkim 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[514].

W okresie objętym sprawozdaniem polski organ nadzorczy analizował w charakterze współrecenzenta trzy projekty wiążących reguł korporacyjnych przedstawione przez grupy kapitałowe i zostały w tym zakresie sporządzone stosowne analizy[515]. Dodatkowo wyraził gotowość działania w charakterze współrecenzenta jeszcze w trzech innych procedurach zatwierdzania wiążących reguł korporacyjnych[516].

Polski organ nadzorczy uczestniczył w ramach EROD również w procedurach przyjmowania opinii dotyczących projektów decyzji organów nadzorczych z EOG dotyczących projektów WRK. Współpraca organów nadzorczych z EOG w toku procedury zatwierdzania WRK odbywa się bowiem z uwzględnieniem mechanizmu spójności przewidzianego w art. 63 RODO, po zasięgnięciu opinii Europejskiej Rady Ochrony Danych. W 2024 r. polski organ nadzorczy uczestniczył jako członek zespołów projektowych przygotowujących projekty opinii EROD dot. projektów decyzji organów nadzorczych z EOG w sprawie zatwierdzenia projektów WRK[517].

W 2024 r. Urząd kontynuował **5 (pięć)** postępowań dotyczących WRK – trzy dla administratorów danych osobowych[518], dwa dla podmiotów przetwarzających[519].

W dniach 9–10 kwietnia 2024 r. 3 pracowników Urzędu uczestniczyło w warsztatach dotyczących wiążących reguł korporacyjnych w Wilnie, które zostały zorganizowane przez litewski organ nadzorczy ds. ochrony danych osobowych.

---

[514] ZAS.46.11.2019, DOL.4413.28.2022, DOL.4413.16.2023, DOL.4413.1.2024, DOL.4413.3.2024, DOL.4413.4.2024, DOL.4413.5.2024, DOL.4413.6.2024, DOL.4413.8.2024, DOL.4413.10.2024, DOL.4413.12.2024, DOL.4413.14.2024, DOL.4413.17.2024, DOL.4413.18.2024, DOL.4413.19.2024, DOL.4413.20.2024 DOL.4413.22.2024, DOL.4413.24.2024.
[515] DOL.4413.11.2022, DOL.4413.19.2023, DOL.4413.11.2024.
[516] DOL.4413.10.2022, DOL.4413.16.2022, DOL.4413.13.2024.
[517] DOL.4413.9.2024, DOL.4413.28.2020 i ZAS.46.15.2019 (w tej ostatniej sprawie zgoda polskiego organu nadzorczego na udział w zespole projektowym została wyrażona jeszcze w 2023 r., jednak praca nad projektem opinii miała już miejsce w większości w 2024 r.). Ponadto polski organ nadzorczy zgodził się działać jako członek zespołu projektowego w jeszcze jednej sprawie, jednak w 2024 r. taki zespół projektowy nie rozpoczął prac nad projektami stosownych opinii EROD.
[518] DOL.4413.17.2023, DOL.4413.13.2023, DOL.4413.3.2023.
[519] DOL.4413.7.2023, DOL.4413.14.2023.

2.1.6. Wizyta studyjna

W ramach projektu EU4DigitalUA odbyło się w Warszawie Forum Wymiany Doświadczeń Organów Ochrony Danych (Data Protection Authorities Experience Exchange Forum), współorganizowane przez Urząd Ochrony Danych Osobowych (3–5.03.2024 r.). Celem projektu jest cyfryzacja Ukrainy, w tym wsparcie w dostosowaniu ukraińskich przepisów ochrony danych osobowych do ram prawnych UE. Koordynatorem projektu jest hiszpańska fundacja FIIAPP. W ramach Forum odbyło się szereg spotkań, w których uczestniczyli przedstawiciele Hiszpańskiej Agencji Ochrony Danych (Agencia Espanola de Proteccion de Datos – AEPD) i Komisarza Parlamentu Ukrainy ds. Praw Człowieka.

Tematyka spotkań dotyczyła ochrony wizerunku dzieci, systemów weryfikacji wieku użytkowników internetu oraz nadzoru nad farmakologią. Omówiono także zagadnienia dotyczące międzynarodowego przekazywania danych i europejskich przestrzeni danych. Podczas panelu dot. kodeksów ochrony danych w badaniach klinicznych omówiono perspektywę hiszpańskiego organu nadzorczego i wyzwania stojące przed polską inicjatywą INFARMA. Przedstawiciel Hiszpanii przedstawił specyfikę krajowych przepisów i doświadczeń z przyjmowaniem członków do kodeksu przez podmiot monitorujący. Polski kodeks postępowania ma uregulować podział ról w badaniu klinicznym, gwarancje dla pacjentów i mechanizmy monitorowania jego przestrzegania.

Ostatni dzień spotkania poświęcony był wymianie doświadczeń. Ukraina przygotowuje się do utworzenia niezależnego organu nadzorczego, więc pracownicy UODO podzielili się doświadczeniami w tym obszarze. Przedstawiciele wybranych departamentów UODO omówili zadania i praktyczne aspekty pracy Urzędu w zakresie działalności edukacyjnej, legislacji i współpracy międzynarodowej. Nie zabrakło też tematów związanych z rozpatrywaniem skarg, prowadzeniem kontroli i postępowań w zakresie naruszeń oraz monitoringu i egzekwowania prawa, w tym nakładania administracyjnych kar pieniężnych.

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.

2.1.7. Inne sprawy

W 2024 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.

1) Współpraca UODO w ramach Digital Education Working Group (DEWG)

Inicjatywa powstała w 2009, a jej koordynatorem jest CNIL (francuski organ ochrony danych). Urząd Ochrony Danych Osobowych jest członkiem grupy od samego początku jej działalności. Głównym celem grupy jest promowanie edukacji cyfrowej 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.

W 2024 roku działania DEWG skupiły się na poniższych obszarach:

1. Wspólna publikacja: przygotowanie wielojęzycznej broszury stanowiącej zbiór inicjatyw edukacyjnych państw współpracujących w ramach DEWG, których adresatem są dzieci, rodzice i nauczyciele.
2. Przeprowadzenie ankiety wśród członków DEWG, dotyczącej relacji organów ochrony danych z ministerstwami i szkołami w zakresie podejścia do EdTech. Badanie zostało przygotowane w związku z organizacją the 2024 GPA Side Event on Ed Tech by the DEWG & UNICEF. “Survey on Ed Tech for the GPA Side Event by DEWG & UNICEF”.
3. Zaplanowanie kampanii promocyjnej dotyczącej relacji rodziców z kulturą cyfrową.
4. Rozpoczęcie prac nad powstaniem grupy zadaniowej w zakresie wpływu technologii AI na edukację w odniesieniu do danych i praw dzieci.
5. Wymiana prac i badań dotyczących zapewnienia wieku, współpraca z International Age Assurance Working Group.
6. Przygotowania do obchodów Europejskiego Roku Edukacji Obywatelskiej 2025.

2.1.8. Prokuratura Europejska

W związku z potwierdzeniem uczestnictwa Polski we wzmocnionej współpracy w zakresie ustanowienia Prokuratury Europejskiej, Prezes UODO jako niezależny organ publiczny został przyjęty 19 września 2024 r. w poczet członków Komitetu Skoordynowanego Nadzoru (CSC) nad przekazywaniem danych z wykorzystaniem kanałów komunikacji Prokuratury Europejskiej, które wymaga podjęcia działań na poziomie krajowym.

Europejski Inspektor Ochrony Danych działa w ścisłej współpracy z krajowymi organami nadzorczymi w konkretnych kwestiach wymagających podjęcia działań krajowych. W szczególności, jeżeli Europejski Inspektor Ochrony Danych lub krajowy organ nadzorczy stwierdzi znaczące rozbieżności między praktykami państw członkowskich Unii Europejskiej lub stwierdzi potencjalnie niezgodne z prawem przekazanie danych przy wykorzystaniu kanałów komunikacji Prokuratury Europejskiej, lub w kontekście zapytań zgłoszonych przez co najmniej jeden krajowy organ nadzorczy.

Prokuratura Europejska jest organem właściwym do spraw dochodzenia, ścigania i stawiania przed sądem sprawców i współsprawców przestępstw naruszających interesy finansowe Unii. Jest niepodzielnym unijnym organem o zdecentralizowanej strukturze, działającym jako jeden urząd. Prokuratura

Europejska wszczyna postępowania przygotowawcze, wnosi akty oskarżenia i sprawuje funkcje oskarżyciela publicznego przed właściwymi sądami państw członkowskich aż do ostatecznego zakończenia sprawy.

Za monitorowanie i zapewnienie stosowania przepisów dotyczących ochrony podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania operacyjnych danych osobowych przez Prokuraturę Europejską odpowiada Europejski Inspektor Ochrony Danych (EIOD). Jednakże, w sytuacjach, które wymagają podjęcia działań krajowych, EIOD działa w ścisłej współpracy z krajowymi organami nadzorczymi w ramach Komitetu Skoordynowanego Nadzoru. Może mieć to miejsce np. wtedy, gdy EIOD lub krajowy organ nadzorczy stwierdzi znaczące rozbieżności między praktykami państw członkowskich Unii Europejskiej lub stwierdzi potencjalnie niezgodne z prawem przekazanie danych przy wykorzystaniu kanałów komunikacji Prokuratury Europejskiej,

W tym celu EIOD i krajowe organy nadzorcze mogą wymieniać się odpowiednimi informacjami i pomagać sobie w przeprowadzaniu kontroli, badać trudności dotyczące wykładni lub stosowania przepisów, analizować problemy związane z prowadzeniem niezależnego nadzoru lub korzystaniem z praw przez osoby, których dane dotyczą, sporządzać zharmonizowane wnioski dotyczące wspólnych rozwiązań wszelkich problemów oraz promować wiedzę na temat praw do ochrony danych.

Zgodnie z planem działania Komitetu Skoordynowanego Nadzoru na lata 2022–2024, działania w tym okresie obejmują monitorowanie sposobu wdrażania delegowanych prokuratorów europejskich na szczeblu państw członkowskich oraz wzajemne powiązania między Prokuraturą Europejską a krajowymi bazami danych.

Prezes Urzędu od wielu lat jest aktywnym członkiem Komitetu Skoordynowanego Nadzoru w zakresie nadzoru nad wielkoskalowymi systemami informacyjnymi Unii Europejskiej. Komitet Skoordynowanego Nadzoru przedstawia sprawozdanie ze swoich działań na posiedzeniu plenarnym Europejskiej Rady Ochrony Danych. Następnie Europejska Rada Ochrony Danych przedkłada je Parlamentowi Europejskiemu, Radzie i Komisji Europejskiej.

2.1.9. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2024 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 wydarzeń znajduje się w załączniku nr 4.

Poniżej przedstawione zostały wybrane przykłady niektórych z nich.

1) Konferencja Agencji Praw Podstawowych (FRA). Bruksela, 21–22.02.2024 r.

„NHRIs enhancing the implementation of the EU Charter of Fundamental Rights" („Usprawnienie wdrażania Karty praw podstawowych UE przez krajowe instytucje praw człowieka"), to tytuł konferencji FRA, która z udziałem Prezesa UODO odbyła się w Brukseli. Konferencja zamykała finansowany z funduszy EOG i funduszy norweskich (Norway Grants) projekt współpracy regionalnej pod nazwą „Wspieranie krajowych

instytucji praw człowieka w monitorowaniu praw podstawowych i podstawowych aspektów praworządności". Konferencja miała na celu przedstawienie działań projektowych i inicjatyw dobrych praktyk opracowanych przez krajowe instytucje praw człowieka, by podnieść świadomość i rozumienie roli tych instytucji w zwiększaniu stosowania Karty praw podstawowych UE na szczeblu krajowym i w ramach UE, m.in. w sprawach dotyczących prawa do prywatności i ochrony danych osobowych, a także monitorowanie praworządności. W ramach tego projektu krajowe instytucje praw człowieka w Bułgarii, Chorwacji, na Cyprze, Łotwie, w Polsce, Słowacji i Słowenii oraz Europejska Sieć Krajowych Instytucji Praw Człowieka (ENNHRI) opracowały i wdrożyły działania mające na celu promowanie stosowania Karty praw podstawowych na szczeblu krajowym i wspieranie sprawozdawczości w zakresie praworządności.

2) Spotkanie Grupy Organów Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej (CEEDPA). Tbilisi, 28.02 – 1.03.2024 r.

W konferencji, która po raz pierwszy od pandemicznego 2021 r. odbyła się stacjonarnie w Tbilisi, wzięli udział, oprócz członków CEEDPA, również przedstawiciele EROD, EIOD, Rady Europy, EUROPOL, EUROJUST oraz organów ochrony danych z Austrii, Belgii, Francji, Niemiec, Hiszpanii i Izraela. Polski organ nadzorczy jest pomysłodawcą CEEDPA, zaś UODO pełni w nim funkcję Sekretariatu. Organizatorem spotkania był gruziński organ ochrony danych. CEEDPA jest ważnym forum wymiany doświadczeń w zakresie ochrony danych osobowych i prawa do prywatności. Dzięki spotkaniu w tak szerokim, międzynarodowym gronie, możliwa była wymiana informacji, dobrych praktyk, a tym samym postępująca harmonizacja prawa ochrony danych osobowych. Członkowie CEEDPA mogli korzystać z bogatego doświadczenia i wiedzy instytucji oraz organizacji europejskich oraz bogatych w doświadczenie organów nadzorczych spoza CEEDPA. W ten sposób zbudowany został pomost umożliwiający przepływ wiedzy w zakresie prawodawstwa, zapewniającego globalną ochronę danych osobowych. Wyjątkowy charakter tego spotkania podkreślał udział reprezentantów Mołdawii i Ukrainy, które jest pierwszym po tym, jak kraje te oraz Gruzja zostały oficjalnymi kandydatami do UE. Organizatorzy CEEDPA mieli również powody do świętowania w związku z przyjęciem przez parlament Gruzji nowej ustawy o ochronie danych osobowych, która weszła w życie 1 marca 2024 r. Szczególnie dużo uwagi poświęcono sytuacji też na Ukrainie w związku z trwającą wojną oraz wyrażono zadowolenie z coraz ściślejszej współpracy tego państwa z Unią Europejską – m.in. w ramach programu EU4DigitalUA. Celem tego programu jest rozwój cyfryzacji Ukrainy i wsparcie w dostosowaniu ukraińskich przepisów ochrony danych osobowych do ram prawnych UE. Podczas konferencji CEEDPA Prezes UODO pełnił funkcję moderatora w panelu „Najlepsze praktyki organów ochrony danych osobowych państw Europy Środkowej i Wschodniej oraz innych europejskich organów ochrony danych", zaś jego przedstawiciel wystąpił jako prelegent w panelu zatytułowanym „Zgodność z przepisami i wyzwania regulacyjne: poruszanie się po zawiłościach RODO i innych przepisów regionalnych".

3) Wiosenna Konferencja Europejskich Organów Ochrony Danych. Ryga, 14–16.05.2024 r.

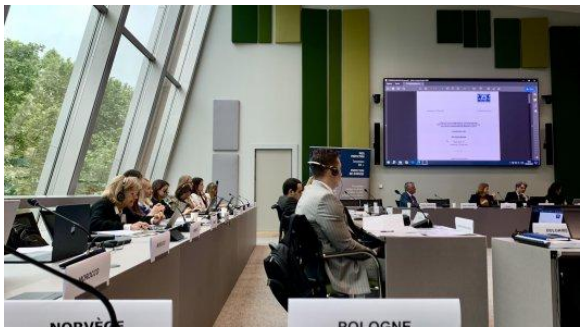
Wiosenne Konferencje są najważniejszym spotkaniem wszystkich rzeczników ochrony danych osobowych z państw członkowskich UE, innych państw europejskich oraz przedstawicieli Komisji Europejskiej, Rady Europy, jak też innych organów zajmujących się ochroną danych osobowych. Podczas tego corocznego wydarzenia organy regulacyjne współpracują w celu poprawy środków ochrony danych. 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. Wydarzenie to, które odbyło się 14-16 maja 2024 r. w Rydze, zostało zorganizowane przez Krajowy Inspektorat Ochrony Danych Łotwy. W konferencji uczestniczył Prezes UODO i jego przedstawiciel z Departamentu Współpracy Międzynarodowej.

W zamkniętych sesjach Wiosennej Konferencji, przeznaczonych wyłącznie dla organów ochrony danych, uczestniczyło 132 delegatów z 45 krajów i 3 organizacje. Natomiast w dniu otwartym dla szerszej publiczności, udział wzięło stacjonarnie około 150 uczestników oraz 200 uczestników w formule online. Głównym tematem wydarzenia była ochrona danych osobowych w obliczu szybko rozwijających się technologii. Kluczowe tematy konferencji obejmowały ewoluującą rolę organów ochrony danych w erze cyfrowej, zagadnienia cyfryzacji usług w obszarze zdrowia, konsekwencje wtórnego wykorzystania danych medycznych, rolę innowacji w sektorze opieki zdrowotnej, wykorzystywanie danych osobowych w badaniach medycznych, a także wspieranie współpracy między podmiotami zajmującymi się ochroną danych. Współpraca międzynarodowa na tych polach to nie jest „opcja”, ale konieczność, jeśli ma być osiągnięty postęp w dziedzinie zapewnienia skutecznej ochrony danych osobowych. Podczas sesji w dniu otwartym konferencji dyskutowano na temat przepisów dotyczących przeciwdziałania praniu pieniędzy i zgodności z RODO, kładąc nacisk na skuteczną współpracę między organami, urzędnikami i przedsiębiorstwami w celu zabezpieczenia procesu przetwarzania danych.

Członkowie i obserwatorzy Wiosennej Konferencji Europejskich Organów Ochrony Danych jednogłośnie przyjęli **Rezolucję w sprawie wzmocnionej współpracy i ustanowienia grup roboczych dla organów ochrony danych**. Europejskie organy ochrony danych potwierdziły swoje zaangażowanie we wspólne wysiłki, przyjmując zasady solidarności, współpracy i wzajemnego wsparcia w dążeniu do skuteczniejszego stawiania czoła wyzwaniom ery cyfrowej i ochrony podstawowych praw i wolności osób fizycznych. Rezolucja została przyjęta w celu sformalizowania i wzmocnienia ich wspólnego podejścia do współczesnych wyzwań związanych z ochroną danych.

Podczas wydarzenia ogłoszono, że gospodarzem 33. Wiosennej Konferencji w 2025 r. będzie organ ochrony danych Gruzji.

4) 46. Posiedzenie plenarne Komitetu T-PD. Strasburg, 5-7.06.2024 r.



Komitet T-PD zdecydowanie zachęca wszystkie Państwa-Strony do jak najszybszego podpisania i ratyfikowania Konwencji 108+. Z tej okazji 7 listopada 2024 r. zaplanowana została konferencja mająca na celu podniesienie świadomości na temat pilnej potrzeby zakończenia procesów podpisywania i ratyfikacji w Państwach-Stronach Konwencji 108. Komitet T-PD przyjął także trzeci moduł wzorcowych klauzul umownych dotyczących przekazywania danych osobowych od podmiotu przetwarzającego do podmiotu przetwarzającego. Dotychczas Komitet T-PD przyjął pierwszy moduł (od administratora do administratora) i drugi moduł (od administratora do podmiotu przetwarzającego). Podczas posiedzenia plenarnego przyjęto również „Wytyczne w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych do celów rejestracji wyborców i ich uwierzytelniania". Sekretariat został zachęcony do promowania Wytycznych i podnoszenia świadomości na temat ich standardów poprzez działania w zakresie współpracy technicznej. Komitet przeprowadził również wymianę poglądów, w oparciu o raport na temat ochrony danych w kontekście neuronauki i podjął decyzję o rozpoczęciu prac nad projektem wytycznych dotyczących neuronauki i ochrony danych[520]. Podczas tego spotkania, przewodnicząca Komitetu T-PD wręczyła zwycięzcom tegorocznej edycji konkursu nagrodę im. Stefano Rodotà, odpowiednio w kategorii „Praca doktorska" za rozprawę „Technologie regulacyjne w badaniu mocy danych i platform w gospodarce aplikacji" i „Artykuły", za publikację „Badanie oszukańczego projektowania w uzasadnionym interesie GDPR".

5) Międzynarodowa konferencja High-Level Policy Dialogue on Data Governance. Montevideo, 30.09 – 1.10.2024 r.

Zastępca Prezesa UODO, Konrad Komornicki, reprezentował Polskę na międzynarodowej konferencji High-Level Policy Dialogue on Data Governance, która odbyła się w Montevideo. W panelu pn. Data Governance: Different Regional Models, Regulations, and Components to Consider, przedstawił prezentację dotyczącą doświadczeń polskiego organu nadzorczego w budowaniu skutecznej ochrony danych osobowych. Uczestniczył w debacie na temat modeli zarządzania danymi na poziomie krajowym, jako instrumentu polityki publicznej, który ustanawia zestaw norm, polityk, standardów, ról i obowiązków w zakresie zarządzania danymi. Ma to na celu wykorzystanie danych zgodnie z prawami człowieka, koncentrując się na jednostkach i ułatwiając innowacje.

6) 47. Posiedzenie plenarne Komitetu T-PD. Strasburg, 4-6.11.2024 r.

[520] Więcej informacji o 46. Posiedzeniu plenarnym T-PD, zob. https://rm.coe.int/t-pd-2024-46rapabr-en-final/1680b05d84

Komitet T-PD zapoznał się ze stanem wewnętrznego procesu podpisywania/ratyfikacji przez Państwa-Strony Konwencji 108 i zdecydowanie zachęcał do jak najszybszego podpisania i ratyfikowania Konwencji 108+. Kontynuował prace nad dokumentem dotyczącym interpretacji art. 11 Konwencji 108+ i polecił Sekretariatowi wprowadzenie, wraz ze sprawozdawcą i Grupą roboczą ds. Art. 11, dalszych zmian w tekście dokumentu, do dyskusji i ewentualnego przyjęcia na kolejnym posiedzeniu plenarnym. Po zapoznaniu się z prezentacją na temat kwestii prywatności i ochrony danych w kontekście federacyjnego uczenia maszynowego i dużych modeli językowych (LLM), Komitet uznał wagę i znaczenie tego tematu, wprowadzając go jako punkt do Planu Działań 2022 – 2025, którym zajmie się Komitet. Podczas tego spotkania odbyła się również wymiana poglądów na temat projektu wytycznych dotyczących neuronauki i ochrony danych, które będą omawiane na kolejnych posiedzeniach. Komitet zapoznał się z informacjami przekazanymi przez Sekretariat na temat zmian w regulaminie konkursu Stefano Rodotà Award, przeprowadził wymianę poglądów i polecił Sekretariatowi, aby wraz z Biurem sfinalizował nowy regulamin i przygotował się do ogłoszenia konkursu w 2025 r.

7) Spotkanie ze studentami European Centre on Privacy and Cybersecurity w Maastricht, 25.11.2024 r.

Prezes UODO, Mirosław Wróblewski, spotkał się ze słuchaczami studiów na Uniwersytecie w Maastricht, gdzie w ramach sesji “Shaping Data Protection Enforcement Strategy in the Times of Artificial Intelligence,” podzielił się doświadczeniem polskiego organu nadzorczego w obszarze ochrony danych osobowych. Sesja odbyła się w ramach Advanced Master on Privacy, Cybersecurity and Data Management i była częścią osobistego tygodnia poświęconego przywództwu i budowaniu strategii w zakresie ochrony danych, z naciskiem na spory sądowe, komunikację i znaczenie osobistego przywództwa. Prezentacja oraz dyskusja toczyła się wokół poniższych tematów:

- strategie egzekwowania RODO (i Aktu o sztucznej inteligencji) w kontekście szybkiego rozwoju technologicznego, widziane z perspektywy organu ochrony danych,
- najlepsze praktyki w zakresie dostosowywania ram egzekwowania i zgodności z nowymi technologiami,
- zmieniająca się rola krajowych organów ochrony danych w globalnym krajobrazie regulacyjnym,
- strategie równoważenia innowacji ze zgodnością z przepisami w organizacjach,
- wgląd w transgraniczną współpracę i harmonizację w egzekwowaniu ochrony danych.

8) 47. Posiedzenie plenarne Komitetu T-PD. Strasburg, 4–6.11.2024 r.

Komitet przyjął informacje dostarczonych przez Sekretariat na temat wzorcowych klauzul umownych, konieczności opracowania większej liczby narzędzi lub instrumentów ułatwiających swobodny przepływ danych oraz o planowanej organizacji pierwszego forum na temat interoperacyjności i konwergencji (pierwszy kwartał 2025

r.). Kontynuował też prace nad dokumentem dotyczącym interpretacji art. 11 Konwencji 108+ oraz zapoznał się z kwestiami dot. prywatności i ochrony danych w kontekście federacyjnego uczenia maszynowego i dużych modeli językowych (LLM), uznając ten temat za bardzo ważny. Zapoznał się też z projektem wytycznych dotyczących neuronauki i ochrony danych, które były tematem kolejnych posiedzeń Komitetu. Zaakceptował zamiany w regulaminie konkursu Stefano Rodotà Award, polecił Sekretariatowi, aby wraz z Biurem sfinalizował nowy regulamin i przygotował się do ogłoszenia konkursu w 2025 r.[521]

V. Wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych

Rok 2024 był rokiem intensyfikacji działań Prezesa UODO, które były podejmowane w wielu obszarach i w różnych formach. Miały one służyć osiągnięciu takich celów, jak:

- przyjmowanie w krajowym porządku prawnym przepisów prawa w jak największym stopniu uwzględniających standardy ochrony danych osobowych, szanujących prawa podstawowe, w tym prawo do prywatności oraz prawo do autonomii informacyjnej obywateli,
- podnoszenie poziomu świadomości podmiotów danych, administratorów i podmiotów przetwarzających oraz wspierających ich IOD,
- zapewnianie właściwego funkcjonowania inspektora ochrony danych w zakresie wykonywania przez niego zadań,
- zachęcanie do tworzenia kodeksów postępowania i wspieranie inicjatyw pracujących nad stworzeniem takich dokumentów,
- zwiększanie zaangażowania Prezesa UODO w postępowania sądowe w sprawach cywilnych,
- właściwe wdrażanie wyroków TSUE do prawa krajowego,
- uspójnienie wykładni przepisów prawa dotyczących ochrony danych osobowych,
- przekazanie administratorom jasnych wskazówek, jak w praktyce stosować RODO bez podejmowania działań nadmiernie ich obciążających.

Analiza działań podjętych w 2024 roku pozwala stwierdzić, że wiele w tym zakresie już udało się osiągnąć.

Konsekwentne działania organu nadzorczego, zapewniające wielu różnym środowiskom wsparcie eksperckie na etapie tworzenia oraz stosowania prawa, przynoszą zamierzone rezultaty i skutkują zwiększeniem świadomości, co do konieczności wdrażania rozwiązań sprzyjających ochronie danych osobowych.

[521] Więcej informacji o 47. Posiedzeniu plenarnym T-PD, zob. https://rm.coe.int/t-pd-2024-47rapabr-en/1680b25e51

Organ nadzorczy stale poszerza krąg swojego oddziaływania, otwierając się na dialog z różnymi środowiskami, a także podejmując aktywne inicjatywy opiniowania z urzędu zarówno projektów aktów prawnych *sensu stricto*, jak również innych aktów o silnym oddziaływaniu w sferze publicznej i społecznej, takich jak plany strategiczne rozwoju państwa czy projekty informatyczne. W opiniach tego drugiego rodzaju organ wypowiada się ze względu na charakter dokumentów – rozłożonych na lata strategii mających horyzontalny wpływ na regulacje prawne, funkcjonowanie państwa, ale i prawa i wolności osób, podmiotów praw objętych takimi regulacjami.

Odnotować należy, że wzrósł odsetek projektodawców decydujących się na uwzględnienie, choćby częściowo, eksperckich wskazówek przedłożonych przez organ nadzorczy. Widocznej poprawie uległ poziom świadomości co do wagi uwzględniania prawa do prywatności oraz autonomii informacyjnej w procesach legislacyjnych. Znacząco wzrosła także gotowość do podejmowania dialogu i roboczej współpracy mającej na celu wypracowanie optymalnych rozwiązań, dzięki którym możliwe jest pogodzenie celów projektowanych regulacji ze standardami przetwarzania danych osobowych.

W efekcie tego typu działań przynajmniej w części przypadków udało się zapobiec wejściu w życie lub wyeliminować z obrotu prawnego przepisy nieprzejrzyste, niezapewniające poszanowania gwarantowanych przez RODO praw osób, których dane są przetwarzane, po części tak wpłynąć na kształt norm, aby ich wykonawcy stosowali rozwiązania niekolidujące ze standardami i zasadami RODO.

Przykładowo w projekcie ustawy o rynku pracy i służbach zatrudnienia[522] projektodawca zakładał m.in. szeroką rozbudowę systemów teleinformatycznych w oparciu o bazy życiorysów zawodowych osób bezrobotnych, poszukujących pracy, osób niezarejestrowanych, osób biernych zawodowo, które za pomocą systemu byłyby automatycznie dopasowywane do ofert pracy. Organ nadzorczy zwrócił uwagę na liczne zagrożenia związane z możliwością niedozwolonej integracji rejestrów oraz nadmiarowego przetwarzania danych osobowych w nich zawartych, a także na budzące wątpliwości tryby pozyskiwania danych z KRS czy systemu ZUS przez starostę oraz przez wojewódzkie i powiatowe urzędy pracy. W efekcie znaczna część tych ryzyk została przez projektodawcę wyeliminowana.

Innym przykładem są prace nad projektem ustawy o zawodzie psychologa oraz samorządzie zawodowym psychologów[523]. W ich toku przeprowadzona została ocena skutków dla ochrony danych, w efekcie której – oraz na skutek istotnego wsparcia przez organ nadzorczy, zarówno w opinii legislacyjnej, jak i w ustaleniach roboczych – projektodawca uporządkował sposoby przetwarzania danych osobowych w sposób przejrzysty, rzetelny i eliminujący wątpliwości interpretacyjne wykonawców norm oraz podmiotów danych.

Z zadowoleniem należy przyjąć wycofanie się projektodawcy z budowy Centralnej Informacji Emerytalnej jako rozwiązania, co do którego na etapie prac legislacyjnych organ nadzorczy zgłaszał poważne wątpliwości[524]. Dlatego przesłany

[522] DOL.401.189.2024.
[523] DOL.401.255.2024.
[524] DOL.401.207.2022.

do zaopiniowania pod koniec 2024 r. projekt ustawy o uchyleniu ustawy o Centralnej Informacji Emerytalnej[525] Prezes UODO ocenił pozytywnie.

Powyższe działania są przykładem na to, że przy tworzeniu prawa możliwe jest wypracowanie norm, które stanowią balans pomiędzy koniecznością uregulowania określonych zagadnień (celu regulacji) a zachowaniem spójności z przepisami o ochronie danych. Niestety, stanowią one niewielką część opiniowanych projektów.

Niepokojącą, obserwowaną od wielu lat, tendencją jest pomijanie Prezesa UODO przez niektóre organy publiczne w procesie uzgodnień i opiniowania projektów aktów normatywnych dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie. Jest to nie tylko zaniechanie stanowiące naruszenie obowiązujących przepisów, ale także utrata okazji do eksperckiego wsparcia projektodawcy przez organ nadzorczy na jak najwcześniejszym etapie procesu legislacyjnego. Angażowanie organu dopiero podczas prac Rządowego Centrum Legislacji i komisji prawniczej należy, niestety, ocenić negatywnie, gdyż jest to zbyt późny moment na dokonywanie ustaleń merytorycznych.

Przedstawienie projektu do zaopiniowania dopiero na zaawansowanym etapie prac legislacyjnych negatywnie oddziałuje na proces prawodawczy. Powoduje znaczne komplikacje po stronie projektodawcy co do możliwości dalszej modyfikacji aktu, celem prawidłowego uwzględniania w regulacji aspektów przetwarzania danych osobowych. Wdrożenie uregulowań nieuwzględniających ochrony danych osobowych wpływa niekorzystnie nie tylko na zapewnienie zagwarantowanych w RODO praw osób, których dane dotyczą, ale również na wykonawców norm, przede wszystkim administratorów, którzy wobec regulacji niedostatecznych, wadliwych lub niezapewniających stosowania norm RODO mają poważne wątpliwości co do sposobu stosowania ustanowionego prawa.

Podkreślić należy, że w przypadkach nieprzesłania projektu do zaopiniowania, Prezes UODO coraz częściej w 2024 r. zgłaszał swoje uwagi z własnej inicjatywy, działając z urzędu w myśl konstytucyjnej zasady legalizmu.

Zauważalnym i wciąż częstym (w porównaniu z latami ubiegłymi) problemem był brak prawidłowej identyfikacji materii danych osobowych w procesie legislacyjnym. Planując określone regulacje prawne, projektodawca na samym początku prowadzonych analiz i prac koncepcyjnych powinien rozważyć, jakie skutki w obszarze prywatności i przetwarzania zindywidualizowanych informacji o osobach wywrze ich wdrożenie. Tymczasem ten aspekt często jest pomijany lub nie jest dostrzegane, że projektowane rozwiązania będą miały – często bardzo doniosłe – oddziaływanie również na kwestie związane z przetwarzaniem danych osobowych. Brak właściwego rozpoznania zależności pomiędzy projektowanym aktem a obszarem ochrony danych osobowych stwarza wysokie ryzyko wprowadzenia do obiegu prawnego norm naruszających zasady rozporządzenia ogólnego z dalece idącymi negatywnymi skutkami dla obywateli. Uwidacznia się to zarówno w odniesieniu do rozpoczynania procesów przetwarzania danych, ich trwania, jak i kończenia.

[525] DOL.401.530.2024.

Zgodnie z zasadą ochrony danych w fazie projektowania (*privacy by design*) wyrażoną w art. 25 ust. 1 RODO, uwzględnienie ochrony danych osobowych powinno odbywać się na jak najwcześniejszym etapie planowania czy podejmowania decyzji o przetwarzaniu. Dotyczy to również procesu legislacyjnego[526].

Dlatego tak ważnym działaniem podjętym przez Prezesa UODO w obszarze legislacji było **rozpoczęcie budowy partnerstw strategicznych** w tej sferze. Na początku 2025 r. podpisane zostały 2 porozumienia o współpracy – z Rządowym Centrum Legislacji oraz z Polskim Towarzystwem Legislacji. Zakładają one podniesienie poziomu technik tworzenia prawa, uwzględniających, na jak najwcześniejszym etapie, ocenę skutków regulacji dla ochrony danych, a także pogłębianie wiedzy i świadomości osób zaangażowanych w proces legislacyjny w zakresie prawa do prywatności i ochrony danych osobowych oraz wymianę doświadczeń i dobrych praktyk związanych z kształceniem prawników, tak by tworzone prawo było precyzyjne oraz w jak największym stopniu zapewnione zostało poszanowanie prawa do ochrony danych osobowych.

Zaznaczyć należy, że problem właściwego stosowania zasad przetwarzania danych osobowych nie dotyczy jedynie nowych projektów. Organ nadzorczy dostrzega wiele niekorzystnych zjawisk natury systemowej, które od lat obecne są w obiegu prawnym, a przez nowe regulacje są jedynie powielane, bez podjęcia wymaganej rewizji rozwiązań już funkcjonujących.

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.

Powyższy problem był wielokrotnie i systematycznie poruszany przez organ nadzorczy przy okazji opiniowania projektów aktów prawnych, jak i w toku realizacji innych jego zadań. W 2024 r. Prezes UODO w wystąpieniu do Ministra Cyfryzacji[527] wniósł o podjęcie prac legislacyjnych prowadzących do zmiany przepisów ustawy o usługach zaufania oraz identyfikacji elektronicznej poprzez przyjęcie rozwiązań, które eliminowałyby ujawnianie numeru PESEL w certyfikacie kwalifikowanego podpisu elektronicznego. Istotne wątpliwości organu nadzorczego wynikają z tego, że numer PESEL jest pozyskiwany przez dostawców usług zaufania publicznego (kwalifikowanego podpisu elektronicznego), a następnie upubliczniany, co z kolei nie wynika ani z przepisów europejskich, ani krajowych. Organ nadzorczy od wielu lat w swoich stanowiskach zwraca uwagę, że numer PESEL jest daną wyjątkową, w sposób unikalny identyfikującą konkretną osobę, stwarzającą jednocześnie – jako dana referencyjna – wiele ryzyk, w tym tworzenia profili osobowych bez wiedzy osoby, której numer ten dotyczy. Niestety, resort cyfryzacji nie przychylił się do uwag Prezesa

[526] Zob. Wytyczne Europejskiej Rady Ochrony Danych nr 4/2019 dotyczące artykułu 25 „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych".
[527] DOL.413.3.2024.

Urzędu, przyjmując stanowisko, że zmiana legislacyjna w odniesieniu do numeru PESEL w certyfikacie kwalifikowanym nie jest konieczna.

Niepokojącym trendem, który stale jest i nadal będzie przedmiotem szczególnego zainteresowania i troski organu nadzorczego, jest tworzenie przepisów przewidujących przetwarzanie coraz większej ilości danych osobowych, często na wielką skalę, w państwowych rejestrach i za pomocą systemów teleinformatycznych, prowadzące do łączenia różnych baz i rejestrów oraz ich udostępniania innym podmiotom publicznym, 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.

Na tego typu zagrożenia Prezes UODO zwrócił uwagę m.in. **w opinii do projektu ustawy o wsparciu państwa dla rodziców powracających na rynek pracy**[528]. Zakładał on powstanie nowego rejestru publicznego, obejmującego liczne informacje dotyczące osób nabywających prawo do świadczenia dla rodziców powracających na rynek pracy, które mają być przetwarzane przez wiele upoważnionych na gruncie projektowanej ustawy podmiotów. Przewidywał, że po wpisaniu do formularza wniosku numeru PESEL osoby występującej o przyznanie świadczenia, formularz wniosku może być uzupełniony o dane zgromadzone w rejestrze PESEL w zakresie imion, nazwiska, miejsca urodzenia, daty urodzenia, stanu cywilnego, obywatelstwa i płci osoby. Organ nadzorczy podniósł, że taka redakcja norm prowadzi w istocie do automatycznego łączenia zasobów obu rejestrów. Co więcej, tak ukształtowany przepis wzbudza wątpliwość, czy jego stosowanie nie będzie wiązać się z automatycznym przetwarzaniem danych osobowych czy nawet profilowaniem.

Innym przykładem budzących zastrzeżenia rozwiązań jest wskazany już projekt rozporządzenia zmieniającego rozporządzenie w sprawie programu pilotażowego w zakresie kompleksowej opieki nad świadczeniobiorcą z wczesnym zapaleniem stawów[529], w przypadku którego Prezes UODO zwrócił uwagę, że to w przepisach rangi ustawy – a nie rozporządzenia wykonawczego – projektodawca powinien wprowadzić odpowiednio i wyczerpująco skonstruowaną podstawę prawną dla przetwarzania danych osobowych, zwłaszcza tych dotyczących zdrowia, a więc danych szczególnych kategorii. W akcie tej rangi powinien określić cel i zakres danych niezbędnych dla jego realizacji.

Stale zwiększająca się i zarazem oczekiwana przez obywateli, cyfryzacja życia społecznego niesie ze sobą ogromny potencjał korzyści zarówno dla rozwoju państwa, jak i jego obywateli, ale wiąże się też z równie istotnymi zagrożeniami dla praw jednostki, w tym prawa do prywatności i autonomii informacyjnej. Organ nadzorczy za materię fundamentalną uznaje konieczność roztropnego **uregulowania kwestii związanych z rozwojem nowych technologii**. Cyfryzacja procesów przetwarzania nie może prowadzić do ignorowania czy naruszenia praw i wolności osób fizycznych. Przeciwnie, procesy wdrażania technologii cyfrowych powinny obejmować rozwiązania pozwalające na umocnienie praw i podmiotowości obywateli, sprzyjając

[528] DOL.401.104.2024.
[529] DOL.401.397.2024.

rozwojowi społeczeństwa obywatelskiego przy zachowaniu najwyższych standardów demokratycznego państwa prawa, etyki i poszanowania człowieczeństwa i godności ludzkiej. Dlatego tak ważne jest, by przetwarzanie danych osobowych w środowisku cyfrowym odbywało się pod kontrolą człowieka, a nie jedynie za pośrednictwem nowych technologii, zwłaszcza sztucznej inteligencji.

W związku z opiniowaniem projektów aktów prawnych zauważalna jest tendencja do traktowania cyfryzacji niekiedy w sposób zbyt powierzchowny, jedynie jako formę digitalizacji dotychczasowych procesów, podczas gdy wdrażanie nowych technologii powinno być każdorazowo poprzedzone dogłębną analizą pod względem ryzyk i wpływu, jaki regulacje te wywrą w sferze praw osób, których dane dotyczą, oraz spełnienia kryteriów proporcjonalności i niezbędności, zapewnienia odpowiedniego poziomu poufności i bezpieczeństwa, a także zastosowania skutecznych środków kontroli.

Wyrazem aktywnego wspierania organów państwowych w zakresie formułowania długofalowych rozwiązań w tym obszarze jest przedstawiona przez Prezesa UODO opinia do **Strategii Cyfryzacji Polski do 2035 r**.[530] Dążąc do wzmocnienia planowanych rozwiązań strategicznych, organ nadzorczy przedstawił wiele istotnych postulatów odnoszących się nie tylko do zagadnień związanych z ochroną praw podstawowych i konstytucyjnych wartości, ale także rozwojem edukacji, bezpieczeństwa, niezależności cyfrowej państwa, promowania zachowań prozdrowotnych, a w dużej mierze także sposobów uregulowania zagadnień związanych z szeroko rozumianym zastosowaniem sztucznej inteligencji w przestrzeni publicznej.

Ponadto UODO aktywnie zaangażował się w inicjatywę Ministerstwa Cyfryzacji dotyczącą rozbudowy systemu S46 – narzędzia wykorzystywanego przez podmioty krajowego systemu cyberbezpieczeństwa do wymiany informacji o incydentach, podatnościach i cyberzagrożeniach. Prace te realizowane są w ramach implementacji dyrektywy NIS 2 do polskiego porządku prawnego.

Celem przedsięwzięcia jest umożliwienie zgłaszania naruszeń ochrony danych osobowych Prezesowi UODO za pośrednictwem systemu S46. Takie rozwiązanie ułatwi realizację obowiązków notyfikacyjnych wynikających zarówno z przepisów o ochronie danych, jak i przepisów o krajowym systemie cyberbezpieczeństwa poprzez jednolity kanał komunikacji. Inicjatywa ta przyczyni się do ograniczenia obciążeń administracyjnych, zwiększenia przejrzystości procesów oraz usprawnienia współpracy pomiędzy organami odpowiedzialnymi za bezpieczeństwo cyfrowe. To także istotny krok w kierunku wzmocnienia zdolności państwa do skutecznego reagowania na zagrożenia w środowisku teleinformatycznym.

Dla organu nadzorczego wyzwaniem w nadchodzących latach będzie weryfikowanie zapewniania, w tym przez prawodawcę, właściwej ochrony danych osobowych przetwarzanych przy użyciu sztucznej inteligencji, chmur, aplikacji, portali, wspólnych systemów czy innych rozwiązań informatycznych. Są one coraz powszechniej stosowane, lecz najczęściej tworzone z pominięciem określonych

[530] DOL.401.502.2024.

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) w fazie projektowania (*privacy by design*), ale 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 ryzyka i wpływ, jaki stosowanie wprowadzanych rozwiązań 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 także 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). 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 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).

W kategorii wyzwań należy również postrzegać wdrożenie **przepisów rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie europejskiej przestrzeni danych dotyczących zdrowia**[531]. Wdrożenie systemu ułatwiającego wymianę danych zdrowotnych w obrębie państw członkowskich UE może przynieść liczne korzyści, w tym poprawę jakości opieki zdrowotnej, lepsze zarządzanie zdrowiem publicznym i wspieranie innowacji w dziedzinie medycyny. Jednak wprowadzenie tak dużego systemu wymiany informacji wiąże się z szeregiem wyzwań technologicznych i ryzyk bezpieczeństwa, w tym tych związanych z pseudonimizacją, łączeniem baz danych, korzystaniem z usług chmurowych. Dlatego istotne będzie

[531] Rozporządzenie parlamentu Europejskiego i Rady UE 2025/327 z 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia i zmiany dyrektywy 2011/24/UE oraz rozporządzenia (UE) 2024/2847, Dz. Urz. UE L 2025/327 (z 05.03.2025), dalej: rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia lub EHDS.

m.in. stworzenie dla tego aktu dobrego otoczenia regulacyjnego w polskim prawodawstwie.

Rok 2024 był rokiem ponownej oceny **realizacji przez sądy obowiązków wynikających z RODO i ustawy o ochronie danych osobowych.**

Prezes UODO już kilkukrotnie na przestrzeni lat występował z prośbą do Prezesów Sądów Apelacyjnych o zasygnalizowanie sądom okręgowym, działającym w obszarze kompetencji właściwego sądu apelacyjnego, konieczności uwzględniania w ich działalności należycie wykonywanego obowiązku wynikającego z art. 94 ust. 1 ustawy o ochronie danych osobowych.

Ponieważ powyższe działania nie przyczyniły się do znaczącej zmiany sytuacji w tym zakresie, w 2024 r. w UODO rozpoczęły się prace koncepcyjno-analityczne mające doprowadzić (w porozumieniu ze środowiskiem sądów cywilnych i Ministerstwem Sprawiedliwości) do **ustandaryzowania sposobu i zakresu informacji przekazywanych między sądami a Prezesem UODO**, co powinno usprawnić wzajemną komunikację.

W ocenie organu nadzorczego jest to bardzo istotne, gdyż wszelkie niedociągnięcia w tym zakresie powodują wiele istotnych ryzyk, takich jak m.in.:

- nieprawidłowa realizacja obowiązków określonych rozdziale 10 ustawy o ochronie danych osobowych zarówno przez sądy, jak i Prezesa UODO,
- brak możliwości realizowania przez Prezesa UODO jego uprawnień określonych w art. 98 – 99 ustawy o ochronie danych osobowych, w tym:
  - wstępowania, za zgodą powoda, do postępowania sądowego o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, w sprawach, które zdaniem Prezesa UODO wymagają jego udziału,
  - przedstawiania istotnego poglądu w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych,
- obarczenie wydanych wyroków wadami prawnymi.

Podkreślić należy, że prawidłowa realizacja przez sądy obowiązku nałożonego na nie mocą art. 94 ust. 1 ustawy o ochronie danych osobowych, ma zapewnić równorzędny poziom gwarancji ochrony danych osobom, których dane dotyczą, w sprawach rozpatrywanych przed sądem powszechnym i organem nadzorczym, a przede wszystkim sprzyjać wyeliminowaniu istotnej rozbieżności w ocenie prawnej stanów faktycznych w sprawach o podobne naruszenia rozpatrywanych przez te podmioty.

Wykonując natomiast uprawnienie Prezesa UODO wynikające z art. 98 i 99 ustawy o ochronie danych osobowych, poprzez przystępowanie do toczących się postępowań za zgodą powodów w sprawach, które zdaniem Prezesa UODO wymagają jego udziału, czy też przedstawiając istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, Prezes UODO ma na celu realizację bardziej spójnego stosowania przepisów o ochronie danych osobowych przez sądy, aby prawa osób, których dane dotyczą, były właściwie respektowane.

Działania te mają również na uwadze wpieranie sądów w stosowaniu orzecznictwa ETPCz i TSUE (w tym zwłaszcza tych wyroków, które dotyczą wykładni pojęcia i rozmiaru szkody w rozumieniu art. 82 RODO, jak np. wyrok TSUE z 4 maja 2023 w sprawie C-300/21; wyrok z 20 czerwca 2024 r. w sprawach połączonych C-182/22 i C-189/22, wyrok z 4 października 2024 r. w sprawie C-507/23).

Realizacja powyższych działań ma tym większe znaczenie, że **nie wszystkie wyroki TSUE zostały odpowiednio transponowane do prawa krajowego**, o czym była już mowa w innej części sprawozdania. Dlatego w 2024 r. Prezes UODO skierował do Ministra do spraw Unii Europejskiej wystąpienie[532], w którym zwrócił się o przekazanie informacji o planowanych zmianach legislacyjnych, uwzględniających wyroki TSUE, w oparciu o które dokonane zostaną zmiany w polskim prawie.

W związku z tym organ nadzorczy planuje w 2025 r. skierowanie wystąpień bezpośrednio do poszczególnych resortów, wskazując konkretne wyroki, które, w jego opinii, powodują konieczność dokonania zmian legislacyjnych w przepisach krajowych.

Prezes UODO za konieczne uznaje **stałe upowszechnianie wiedzy na temat orzecznictwa TSUE, ETPC, sądów krajowych z państw członkowskich UE oraz wytycznych EROD.** Standardy z nich wynikające powinny bowiem być brane pod uwagę zarówno przy stanowieniu prawa, jak i przy jego interpretacji i stosowaniu. Takie podejście powinno jednocześnie przyczynić się do uspójnienia wykładni RODO.

Osiągnięciu tego celu służy m.in. powoływanie się na unijne orzecznictwo i wytyczne EROD w korespondencji z różnymi środowiskami i podmiotami, w tym w opiniach legislacyjnych, wystąpieniach o zmianę przepisów prawa czy w odpowiedziach udzielanych zwłaszcza administratorom i inspektorom ochrony danych.

Niezmiennie dużą wagę – podobnie jak w latach ubiegłych – organ nadzorczy przywiązywał i będzie przywiązywać do **współpracy z inspektorami ochrony danych**, gdyż ich rola ma fundamentalne znaczenie dla budowy skutecznego systemu ochrony danych osobowych. Dlatego 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. Organ nadzorczy – tak jak dotąd – na bieżąco będzie udzielał odpowiedzi na pytania przesyłane przez IOD oraz szybko reagował na sygnalizowane przez IOD problemy, np. poprzez kierowanie do właściwych podmiotów wystąpień postulujących zmianę przepisów prawa bądź stosowanej praktyki. Przykładem takich działań są wystąpienia Prezesa UODO kierowane np. do Szefa Służby Cywilnej[533], Ministra Zdrowia[534] czy Ministra Edukacji[535] opisane w części dotyczącej tej formy aktywności organu nadzorczego.

---

[532] DOL.413.14.2024.

[533] Ponowne wystąpienie dot. wyodrębnienia stanowiska IOD w służbie cywilnej – DOL.413.6.2023 (https://uodo.gov.pl/pl/138/3217).

[534] Wystąpienie z 26 listopada 2024 r. (sygn.. akt: DOL.413.19.2022), dostępne pod linkiem: https://uodo.gov.pl/pl/138/3454.

[535] DOL.413.4.2023.

Ponieważ kwestie dotyczące funkcjonowania IOD, w tym w szczególności nakładania na inspektora zadań innych niż te, które są przewidziane w RODO, np. zadań należących do administratora, wciąż budzą wątpliwości, Prezes UODO w 2024 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, zorganizował 9 kwietnia 2024 r. spotkanie, które miało na celu upowszechnianie informacji o zeszłorocznym działaniu EROD w ramach CEF DPO i sprawozdaniu z tego działania, w tym raporcie polskiego organu nadzorczego i przedstawionych w nim zagadnień dotyczących niezależności IOD[536], a także przeprowadzając szkolenia dla IOD reprezentujących jednostki samorządu terytorialnego w ramach akcji „UODO rusza w kraj". Upowszechnianie wiedzy na temat roli, zadań i pozycji inspektora w organizacjach oraz budowanie świadomości, 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 – jest wciąż aktualnym zadaniem Prezesa UODO. Pomocne w tym zakresie mogą być wypracowywane przez lata, we współpracy z inspektorami ochrony danych i administratorami, wskazówki dotyczące zgodnego z prawem realizowania obowiązków administratorów wobec IOD, które prezentowane były przez UODO.

Jednym z zadań, które polski organ nadzorczy będzie w 2025 r. realizował na rzecz wzmocnienia statusu IOD i ułatwienia przez niego prawidłowej realizacji jego zadań, będzie **udział w pracach nad aktualizacją Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (243 WP)**. Zostały one wydane w 2017 roku i odegrały ważną rolę zarówno w czasie przygotowań, jak w pierwszym okresie stosowania RODO.

Jednak w powołanym sprawozdaniu CEF DPO zalecono aktualizację obecnych wytycznych dotyczących inspektorów ochrony danych ze względu na wyrażone w różnych państwach członkowskich zapotrzebowanie na dodatkowe wytyczne. Potrzeba rozszerzenia Wytycznych 243 WP związana jest m.in. z rozwojem dorobku orzeczniczego organów nadzorczych i sądów[537] oraz zmiany stanu prawnego, a także ze względu na sygnalizowane organom wątpliwości zarówno przez poszczególnych administratorów, inspektorów, jak i reprezentujące ich stowarzyszenia.

W tym miejscu wskazać należy na jeszcze jedną bardzo ważną kwestię związaną ze współpracą organu z IOD-ami i udzielaniem odpowiedzi na pytania dotyczące wykładni prawa. Informacje i wskazówki przekazywane zarówno osobom fizycznym, jak i administratorom oraz podmiotom przetwarzającym są wyrazem realizacji przez Prezesa UODO jego zadań określonych w art. 57 ust. 1 RODO. To eksperckie wsparcie organu nadzorczego przybiera niekiedy szerszy wymiar, zwłaszcza gdy o opinię zwracają się podmioty publiczne. Rolą Prezesa UODO nie jest świadczenie pomocy prawnej, o czym organ nadzorczy wielokrotnie informuje, wskazując, że

[536] Komunikat UODO dotyczący tego działania, treść sprawozdania krajowego UODO oraz link do komunikatu EROD dostępne są pod linkiem: https://uodo.gov.pl/pl/138/2960.
[537] np. w TSUE wyroku w sprawie C-453/21.

wiążące stanowisko co do określonych stanów faktycznych może zająć tylko w decyzji administracyjnej. W pierwszej kolejności wsparcie administratorom i podmiotom przetwarzającym powinni zapewniać inspektorzy ochrony danych. Tymczasem w wielu przypadkach podmioty te, chcąc uzyskać pomoc ze strony UODO, nie przesyłają do organu nadzorczego opinii IOD, co może wskazywać, że albo nie konsultują z nim tych spraw, albo próbują jego stanowisko weryfikować w nieznanym RODO trybie przed organem nadzorczym. Duża liczba **pytań wpływających do UODO wskazuje na konieczność dalszego poszerzania edukacji w obszarze ochrony danych,** tym bardziej że RODO traktowane jest wciąż jako akt nakładający obowiązek tworzenia wielu dokumentów i sformalizowanych procedur, gdy tymczasem takie podejście nie wynika ani z samego RODO, ani z wytycznych Europejskiej Rady Ochrony Danych.

Wytyczne EROD zawierają szczegółowe wyjaśnienia wielu kwestii i przykłady zastosowania przepisów prawa w praktyce. Zapewniają spójną interpretację określonych w RODO praw i obowiązków. Dlatego Prezes UODO często się do nich odwołuje, zwłaszcza w odpowiedziach udzielanych na pytania od IOD, którzy jako fachowcy w dziedzinie ochrony danych osobowych mogą zapewnić administratorom najlepsze wsparcie w zakresie ochrony danych osobowych.

Ważnym działaniem organu jest także kontynuowanie **wsparcia dla inicjatyw pracujących nad kodeksami postępowania**. Kodeksy postępowania to ważny instrument ułatwiający osiąganie zgodności z RODO i podnoszenie poziomu ochrony danych osobowych.

Kodeks, który jest właściwie przygotowany i nie jest powtórzeniem przepisów RODO, oraz doprecyzowuje problemowe kwestie z uwzględnieniem specyfiki danej branży, przynosi wiele korzyści[538]. 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 mogą one liczyć na zbliżony standard ochrony danych oraz obsługę w zakresie realizacji ich praw przez daną branżę.

Zaletą odpowiednio przygotowanego kodeksu jest nie tylko gwarancja pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy. Nadzór nad procesami przetwarzania danych osobowych sprawuje jeszcze niezależny podmiot monitorujący kodeks. Podmioty monitorujące w celu uzyskania akredytacji

[538] 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 sektorze. Z punktu widzenia ochrony danych osobowych kodeksy mogą zatem funkcjonować jako zbiór instrukcji dla administratorów danych i podmiotów przetwarzających, którzy projektują i wdrażają zgodne z RODO czynności przetwarzania danych, nadających znaczenie operacyjne zasadom ochrony danych określonym w prawie europejskim i krajowym (pkt 7 Wytycznych 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, Wersja 2.0, 4 czerwca 2019 r.).

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 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.

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[539].

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.

Ważnym działaniem organu służącym podnoszeniu poziomu ochrony danych osobowych jest **udzielanie odpowiedzi na pytania** zarówno od osób, których dane są przetwarzane, jak i od administratorów i podmiotów przetwarzających oraz od inspektorów ochrony danych. 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.

Analizując treść wpływających do UODO w 2024 r. **pytań od inspektorów ochrony danych** zauważyć można, że z każdym rokiem pojawiające się w nich zagadnienia coraz rzadziej dotyczą kwestii podstawowych, a odnoszą się do coraz bardziej złożonych problemów. Podkreślić należy, że inspektorzy z dużym wyczuciem identyfikują zagrożenia dla ochrony danych osobowych wnikające z luk prawnych lub nieprecyzyjnie skonstruowanych przepisów prawa albo też nieprawidłowej ich interpretacji.

[539] Szerzej o błędach popełnianych podczas prac nad kodeksami postępowania była już mowa w niniejszym opracowaniu, w części poświęconej kodeksom.

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. Praktyka ta będzie kontynuowana w roku 2025.

Niepokojącą tendencją jest natomiast pomijanie przez występujących do organu nadzorczego administratorów (zwłaszcza z sektora publicznego) konsultacji z inspektorami ochrony danych. Z przesyłanych pytań nie wynikało, aby takie konsultacje miały miejsce, a jeśli tak, to jakie były ich wyniki. Dlatego w udzielanych odpowiedziach Prezes UODO zwracał uwagę, że analizy zgłaszanego problemu w pierwszej kolejności powinien dokonać IOD i przedstawić swoją opinię w tym zakresie.

Ważnym działaniem UODO jest **aktualizacja i wydawanie branżowych poradników** dotyczących ochrony danych osobowych. W tym zakresie organ nadzorczy może liczyć na wparcie członków Społecznego Zespołu Ekspertów przy Prezesie UODO.

Analizując kwestię zamierzeń i wyzwań nie można pominąć postępującej cyfryzacji i automatyzacji przetwarzania danych osobowych, które uwidoczniły znaczenie kwestii informatycznych i technologicznych dla oceny rozwiązań prawnych. Otwarte jest wciąż pytanie, jak uczyć sztuczną inteligencję oraz jak „oduczyć" ją, gdy wyciągnie niewłaściwe wnioski. To tylko jeden z przykładowych problemów, z jakimi przyjdzie nam się wkrótce zmierzyć. Dlatego Prezes UODO wielką wagę przywiązuje do uwzględniania w swoich działaniach technologicznego wymiaru ochrony danych, by trafnie identyfikować najnowocześniejsze technologie wykorzystywane do przetwarzania danych osobowych i zachęcać do uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych w procesie innowacji. Ważna jest tu umiejętność analizowania zarówno realnych, jak i potencjalnych zagrożeń oferowanych przez powstające technologie, by w miarę możliwości uprzedzać trendy technologiczne, znajdując **równowagę między innowacjami a prawami człowieka**.

Przed organami nadzorczymi stoi obecnie bardzo ważne zadanie – monitorowanie i wspieranie właściwego wdrożenia do porządku krajowego pakietu przepisów regulujących funkcjonowanie gospodarki cyfrowej oraz zapewnienie ich spójnego stosowania. Nie da się tego zrobić bez zapewnienia – zarówno w wymiarze europejskim, jak i krajowym – spójności przepisów, porozumienia różnych regulatorów (zwłaszcza tych działających w obszarze regulacji cyfrowych czy ochrony praw konsumenta) oraz szerokiego spojrzenia na różne przypadki, w których dochodzi do przetwarzania informacji dotyczących osób. Dla właściwej ich oceny potrzebna jest bowiem wiedza z zakresu prawa, technologii, a nawet etyki. Szkolenia, podnoszenie wiedzy i świadomości oraz otwartość na współpracę i wymianę doświadczeń będą tu miały fundamentalne znaczenie.

W porównaniu z rokiem 2023 przede wszystkim pozytywnie należy ocenić odsetek projektodawców decydujących się w dużo większym stopniu niż w latach

ubiegłych na uwzględnienie, choćby i częściowo, eksperckich wskazówek przedłożonych przez organ nadzorczy. Widocznej poprawie uległ poziom świadomości co do wagi uwzględniania prawa do prywatności oraz autonomii informacyjnej w procesach legislacyjnych. Znacząco wzrosła także gotowość do podejmowania dialogu i roboczej współpracy celem wypracowania optymalnych rozwiązań – pogodzenia celów projektowanych regulacji ze standardami przetwarzania danych osobowych.

Z drugiej strony nie sposób jednak pominąć aspektów negatywnych. Odsetek projektów, w których zdecydowano się na przeprowadzenie testu prywatności jako elementu oceny skutków dla ochrony danych, uznać należy w dalszym ciągu za głęboko niezadowalający, bo nieobejmujący wszystkich przypadków, zważywszy warunki wymagane regulacją RODO – rodzaj przetwarzania, w szczególności z użyciem nowych technologii, wzgląd na charakter, zakres, kontekst i cele oraz duże prawdopodobieństwo możliwego powodowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Co się z tym wiąże również aspekty stosowania zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych są notorycznie pomijane, co w wielu przypadkach ma kaskadowe negatywne konsekwencje dla jakości projektowanych aktów pod względem gwarancji dla osób, których dane dotyczą.

Zasadniczym problemem jest jednak wciąż przede wszystkim brak przeprowadzenia przez ustawodawcę gruntownego przeglądu obecnie obowiązujących przepisów pod względem konieczności ich dostosowania do standardów rozporządzenia 2016/679, ale również dyrektywy 2016/680. W obiegu prawnym pozostają regulacje, które nie zostały dostosowane do wymogów stawianych przez wymienione akty unijne. Jest to tym bardziej istotne w perspektywie wchodzenia w życie kolejnych aktów unijnych, wymagających roztropnej implementacji do prawa krajowego: aktu o sztucznej inteligencji, rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia czy rozporządzenia w sprawie europejskiego zarządzania danymi. Brak podjęcia koniecznych rozwiązań legislacyjnych w perspektywie kolejnych lat budzi obawy co do dalszego nawarstwiania się problemu, zwłaszcza że nowe akty prawa unijnego nie obniżają standardów ochrony danych i odwołują się do konieczności zapewnienia zgodności z przepisami o ochronie danych osobowych nowych form, sposobów i procesów przetwarzania informacji. Wprowadzanie nowych aktów unijnych oraz nowych sposobów i celów przetwarzania danych osobowych wymaga przeglądu i zmian prawa regulującego korzystanie przez instytucje publiczne z rejestrów państwowych / publicznych. Ma to fundamentalne znaczenie z punktu widzenia ryzyk związanych z profilowaniem danych osobowych i wykorzystywaniem systemów sztucznej inteligencji dla realizacji zadań publicznych.

Efektem braku uwzględnienia uwag organu nadzorczego zarówno co do projektów z roku 2024, jak i z lat poprzednich jest funkcjonowanie w obiegu aktów prawa budzących poważne wątpliwości w zakresie ich stosowania, co Prezesowi Urzędu stale sygnalizują podmioty danych, inspektorzy ochrony danych, administratorzy oraz różnego rodzaju instytucje przedstawicielskie. W procesach legislacyjnych dostrzegalna jest tendencja do powielania błędnych rozwiązań

i kontynuowania złych praktyk, szczególnie uwidoczniona przy stanowieniu procesów przetwarzania w rejestrach państwowych zakładających łączenie zasobów i opierających przetwarzanie na aktach nieposiadających przymiotu prawa powszechnie obowiązującego, takich jak umowy czy porozumienia. Ze względu na rosnące tendencje do digitalizacji procesów państwowych, zjawisko to ulega jedynie nasileniu. Dostrzegając liczne trudności w procesach legislacyjnych, w tym potrzebę horyzontalnych przeglądów i zmian regulacji obowiązujących oraz zapewniania stosowania regulacji europejskich, Prezes Urzędu, biorąc pod uwagę pozytywne aspekty, na które wskazano w powyższej części sprawozdania, wyraża jednak nadzieję, że perspektywa kolejnych lat zaowocuje dalszym korzystnym wzrostem zaangażowania projektodawców co do wdrażania aspektów związanych z ochroną danych osobowych w procesach tworzenia prawa. Liczy, że drogą kooperacji i dialogu wyzwania nadchodzących lat, związane przede wszystkim z postępującą reformacją cyfrową, uda się przezwyciężyć, wdrażając rozwiązania prawne służące dobrostanowi obywateli oraz sprzyjające pełnemu odzwierciedleniu konstytucyjnych praw do prywatności i autonomii informacyjnej.

Dla organu nadzorczego wyzwanie stanowi 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 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.**

Obserwowany wzrost liczby **skarg** wnoszonych do Urzędu Ochrony Danych Osobowych przez osoby, których dane dotyczą, 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), z drugiej jednak strony oznacza wzrost świadomości osób, których dane dotyczą, co do przysługujących im praw, co jest bardzo pozytywnym zjawiskiem. W roku 2024 do wzrostu świadomości osób, których dane dotyczą, przyczynił się również polski organ nadzorczy, zwiększając aktywność zmierzającą do szerzenia

wiedzy na ten temat, m.in. podczas licznych spotkań organizowanych na terenie całego kraju, w czasie których osobom, których dane dotyczą, udzielano porad w zakresie ich praw wynikających z RODO.

Podkreślić należy, że wraz ze wzrostem świadomości osób, których dane dotyczą o przysługujących im prawach, a także postępem technicznym, sprawy skargowe prowadzone w UODO są coraz bardziej skomplikowane i wielowątkowe, a ponadto często dotyczą zagadnień związanych z nowymi technologiami. To powoduje konieczność ciągłego aktualizowania przez pracowników UODO 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.

Warto zauważyć, że pomimo większej w stosunku do lat poprzednich liczby prowadzonych spraw, w 2024 r. udało się zwiększyć liczbę spraw zakończonych. W większości spraw sądy administracyjne podzielają stanowiska zajmowane przez organ w sprawach skargowych, oddalając skargi na decyzje Prezesa UODO, co świadczy o wysokiej jakości merytorycznej rozstrzygnięć wydawanych w sprawach skargowych.

Podkreślenia wymaga, 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 i jednocześnie jednym z najważniejszych zadań tego organu 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 osób, których dane dotyczą przed przetwarzaniem tych danych w sposób niezgodny z przepisami RODO.

Wydawane przez Prezesa UODO decyzje odgrywają kluczową rolę w kształtowaniu i wzmacnianiu ochrony danych osobowych w Polsce, a ich pozytywny wpływ można dostrzec w wielu aspektach. Dzięki wyrażonym w decyzjach stanowiskom organu, wskazujących, jak w prawidłowy sposób powinno odbywać się przetwarzane danych, podnoszone standardy ochrony danych osobowych przez administratorów oraz podmioty przetwarzające, skutkujące zwiększeniem dbałości o bezpieczeństwo przetwarzania oraz ich świadomości co do skuteczności dobieranych środków bezpieczeństwa w organizacji w wyniku przeprowadzenia analizy ryzyka dla czynności przetwarzania. W uzasadnieniach decyzji wskazywane jest aktualne orzecznictwo sądów administracyjnych, stanowiska Prezesa UODO oraz standardy w zakresie zapewniania bezpieczeństwa ochrony danych osobowych. Interpretacja przepisów rozporządzenia 2016/679 wyartykułowana w decyzjach stanowi znaczącą pomoc dla podmiotów przetwarzających dane osobowe w lepszym zrozumieniu ciążących na nich obowiązków i dostosowywaniu przyjętych rozwiązań technicznych do dynamicznie rozwijających się technologii. Sankcje i wytyczne skłaniają organizacje do wdrażania skuteczniejszych środków bezpieczeństwa

i procedur ochrony danych, przyczyniając się do zmniejszania ryzyka wycieków i nieuprawnionego dostępu do systemów przetwarzających dane osobowe. Jednocześnie organizacje, które dostosowują swoje działania do zaleceń przedstawionych w decyzjach Prezesa UODO, poprawiają standardy oraz zwiększają zaufanie klientów (osób, których dane dotyczą), wpływając jednocześnie pozytywnie na praktyki biznesowe. Ponadto przytaczane i komentowane w mediach rozstrzygnięcia zawarte w decyzjach dotyczące naruszeń przepisów ochrony danych osobowych zwiększają świadomość społeczeństwa na temat prawa do ochrony danych osobowych. Wszystkie te działania powodują, że ochrona danych osobowych w Polsce staje się coraz bardziej skuteczna – sprzyja to zarówno bezpieczeństwu obywateli, jak i rozwojowi odpowiedzialnego biznesu.

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, szczególnie z uwagi na rozwój technologiczny i związane z nim nowe zagrożenia dla ochrony danych. Dotyczy to w szczególności najmłodszych członków społeczeństwa, którzy mają niewielkie doświadczenia i są najmniej świadomi zagrożeń dla ochrony dotyczących ich danych osobowych, a także praw przysługujących im w związku z przetwarzaniem danych, ale także i osób w wieku podeszłym (stąd m.in. porozumienia o współpracy zawarte w 2024 r. przez Prezesa UODO z Rzecznikiem Praw Dziecka, a także z Uniwersytetami Trzeciego Wieku).

W swojej działalności UODO wielokrotnie podnosił tematy dotyczące zabezpieczenia praw najmłodszych nie tylko w kontekście prawa do ochrony ich danych osobowych, ujętych w RODO. Przykładem są chociażby uwagi Prezesa UODO do **„Strategii Cyfryzacji Polski do 2035 roku”,** w których wskazał m.in. na potrzebę właściwego edukowania dzieci i młodzieży w zakresie bezpiecznego korzystania z narzędzi cyfrowych.

Z tego też m.in. względu – zgodnie z planem kontroli sektorowych na 2025 rok – Urząd Ochrony Danych Osobowych przeprowadza w tym roku kontrole podmiotów/administratorów przetwarzających dane osobowe dzieci. Waga tego zadania wynikała z faktu, że w toku działalności Urzędu Ochrony Danych Osobowych **pojawiło się wiele zgłoszeń odnoszących się do zagadnień cyberbezpieczeństwa w placówkach oświatowych.**

Wśród najczęściej zgłaszanych incydentów wymienić należy m.in.:

- nieuprawniony dostęp do kont nauczycielskich w dziennikach elektronicznych,
- kradzież haseł dostępowych do dzienników elektronicznych przez uczniów,
- udostępnianie dokumentów szkolnych na platformach typu „scribd” i „docer” bez wiedzy administratora, co stwarza wysokie ryzyko wykorzystywania tych platform do współdzielenia i zachowywania dokumentacji, która zostaje automatycznie udostępniona pozostałym użytkownikom danego portalu,

- ataki ransomware, podczas których dochodzi do zaszyfrowania danych osobowych przetwarzanych na serwerach szkolnych, bądź do utraty dostępu do sieci informatycznych szkół.

Analiza ww. incydentów wykazała, że placówki oświatowe są najczęściej narażone na naruszenia bezpieczeństwa danych z powodu braku procedur, niewystarczającego przeszkolenia pracowników oraz wykorzystywania prywatnych zasobów (takich jak adresy e-mail czy skrzynki pocztowe) do celów służbowych. Częste są również nieświadome błędy użytkowników – zapisywanie haseł w przeglądarkach, nieuwaga przy logowaniu czy udostępnianie dokumentów na publicznych platformach. Widać także niski poziom wdrażania podstawowych zabezpieczeń, takich jak dwuskładnikowa weryfikacja tożsamości czy szyfrowanie danych.

Z perspektywy budowania odporności placówek oświatowych kluczowe jest zatem podniesienie świadomości kadry, wprowadzenie polityk bezpieczeństwa informacji, ograniczenie użycia prywatnych kont oraz regularne szkolenia z zakresu ochrony danych i cyberhigieny. Pożądane byłoby utworzenie dla nauczycieli służbowych skrzynek poczty elektronicznej, nad którymi administrator mógłby sprawować kontrolę i zapobiegać ewentualnym atakom phishingowym, mogącym umożliwiać dostęp do danych osobowych znajdujących się w dziennikach elektronicznych. Wzmocnienie zabezpieczeń technicznych i organizacyjnych może znacząco ograniczyć ryzyko wystąpienia podobnych naruszeń w przyszłości.

Urząd Ochrony Danych Osobowych, zgodnie z art. 57 RODO, podejmuje też szereg działań edukacyjno-informacyjnych, które obejmują m.in. upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumieniem tych zjawisk, ze szczególnym uwzględnieniem właśnie dzieci, jako adresatów tych działań[540].

Przykładem jest realizowany od 15 lat ogólnopolski program edukacyjny UODO pn. „**Twoje dane – Twoja sprawa”,** którego uczestnikami są uczniowie i nauczyciele szkół podstawowych, ponadpodstawowych oraz placówki doskonalenia nauczycieli. Co roku na uczestników czekają materiały edukacyjne i specjalistyczne szkolenia, organizowane są konferencje, webinaria, zajęcia lekcyjne, pozalekcyjne, konkursy, porady z cyklu „Warto wiedzieć…” oraz inne wydarzenia tematyczne skierowane do uczniów, nauczycieli i dyrektorów szkół. 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. Od kilkunastu już lat program ten z powodzeniem umożliwia uczniom 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.

[540] Art. 57.1.b RODO.

Szeroki zakres omawianych tematów będących rozwinięciem treści i zagadnień zawartych w podstawie programowej szkół sprawił, że program „Twoje dane – Twoja sprawa" na stałe wpisał się kalendarz działań profilaktyczno – wychowawczych placówek oświatowych. 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 szkół. Wieloletnia realizacja programu w szkołach przyczynia się do kształtowania prawidłowych podstaw i nawyków dzieci i młodzieży w zakresie bezpieczeństwa w internecie i wzrostu ich świadomości na temat ochrony danych osobowych. Program „Twoje dane – Twoja sprawa odgrywa kluczową rolę w kształtowaniu świadomości w zakresie ochrony danych osobowych w polskich szkołach i instytucjach edukacyjnych. UODO będzie dążył do zwiększenia liczby placówek zaangażowanych w ten program oraz do rozwijania jego treści, aby lepiej odpowiadały na aktualne wyzwania związane z rozwojem nowych technologii.

Inicjatywy edukacyjne Prezesa UODO są wielokierunkowe, a ich adresatami są zarówno dzieci i młodzież, jak i ich szersze otoczenie. Daje to gwarancję właściwego przygotowania dzieci i młodzieży do aktywnego, bezpiecznego uczestnictwa w życiu społecznym i w przestrzeni cyfrowej. Program ten to również platforma współpracy z wieloma urzędami i instytucjami na rzecz ochrony prywatności oraz danych osobowych dzieci oraz promocji szkół zaangażowanych i aktywnie działających na rzecz zwiększenia bezpieczeństwa uczniów.

Na szczególną uwagę zasługuje zwłaszcza **współpraca Prezesa UODO z Rzeczniczką Praw Dziecka w zakresie inicjatyw edukacyjnych i badawczych dotyczących danych osobowych dzieci i młodzieży, w tym organizacja konferencji i webinariów.** Efektem tej współpracy są także opracowane materiały edukacyjne w formie fiszek, krzyżówek i testów, które w sposób interaktywny pozwalają dzieciom poznać i utrwalić kluczowe zagadnienia z obszaru ochrony prywatności i danych osobowych oraz bezpiecznego poruszania się w internecie.

Ponadto ekspert UODO zasiada w gronie nowo powołanego w Biurze RPD **Zespołu do spraw etyki badań społecznych z udziałem dzieci**. Celem tej inicjatywy Rzecznika Praw Dziecka jest opracowanie standardów etycznych dla badań z udziałem dzieci w Polsce. Zespół ma za zadanie zapewnienie ochrony dzieciom uczestniczącym w badaniach naukowych, poprzez wypracowanie dobrych praktyk i materiałów edukacyjnych dla badaczy.

W kontekście praw dzieci wydany został przez Urząd Ochrony Danych Osobowych we współpracy z Fundacją Orange **poradnik pt. „Wizerunek dziecka w internecie. Publikować czy nie?".** Poradnik powstał głównie z myślą o osobach pracujących w organizacjach i placówkach, których zadaniem jest troska o dobro i bezpieczeństwo dzieci. Ważnym przesłaniem poradnika jest wspieranie dzieci w budowaniu przekonania, że mają prawo do prywatności i prawo podejmowania decyzji w sprawach, które ich dotyczą.

W ramach współpracy Urzędu Ochrony Danych Osobowych z Fundacją Orange powstały również inne publikacje dotyczące ochrony wizerunku dzieci w internecie:

1) Ochrona wizerunku dzieci – materiał dla klubów sportowych.

2) Ochrona wizerunku dzieci – materiał dla organizacji pozarządowych.
3) Ochrona wizerunku dzieci – materiał dla placówek oświatowych.

Wspomniane poradniki zwracają uwagę na odpowiedzialność placówek działających na rzecz dzieci i młodzieży, które z jednej strony aktywizują i wspierają je w różnych, ważnych dla ich rozwoju działaniach, a z drugiej strony mogą łatwo zgubić z pola widzenia kwestie związane z bezpieczeństwem przetwarzania dotyczących ich danych osobowych. Dlatego już w październiku 2025 r. UODO organizuje wspólnie z Krakowskim Szkolnym Ośrodkiem Sportowym im. Szarych Szeregów i Akademią Wychowania Fizycznego im. Bronisława Czecha w Krakowie konferencję dotyczącą ochrony danych osobowych sportowców, a w szczególności najmłodszych adeptów kultury fizycznej. Jest to o tyle ważne, że właśnie w internecie można znaleźć wiele, często nadmiarowych informacji o młodych sportowcach, które są dostępne publicznie, bez ograniczeń, ujawniając szerokie spektrum danych osobowych małoletnich.

Współpraca Urzędu z innymi podmiotami pozwoliła znaleźć takie rozwiązania, które skutecznie wpływają na zwiększenie ochrony danych osobowych najmłodszych członków społeczeństwa, przy poszanowaniu ich prawa do autonomii informacyjnej i samostanowienia o sobie. Działania te wypracowywane są także we współpracy z innymi środowiskami, z dużym udziałem organizacji pozarządowych oraz ekspertów zrzeszonych w różnych gremiach. UODO ma pełną świadomość, że w dobie wszechobecnego dostępu do internetu ochrona dzieci przed cyberzagrożeniami jest sprawą priorytetową. Dlatego z chwilą powstania w lipcu 2024 r. sejmowej Komisji do Spraw Dzieci i Młodzieży (DIM), UODO aktywnie zaangażował się w jej prace na rzecz stworzenia pakietu standardów ochrony dzieci w środowisku cyfrowym.

Równolegle organ nadzorczy prowadzi działania legislacyjne, analizując i przygotowując opinie do projektów aktów prawnych dotyczące małoletnich. W opiniach legislacyjnych organ nadzorczy odnosił się do kwestii **zapewnienia wieku użytkownika,** która miałaby chronić małoletnich przed treściami szkodliwymi w sieci. Wskazywał w nich na potrzebę stosowania przejrzystych, skutecznych i adekwatnych do wieku środków identyfikacji[541]. Podkreślał przy tym, że skuteczne zapewnienie wieku w środowisku cyfrowym, niezbędne do skutecznej ochrony dzieci, musi być realizowane w sposób zgodny z RODO – w szczególności z **zasadą minimalizacji danych oraz koniecznością stosowania bezpiecznych i proporcjonalnych mechanizmów weryfikacji.**

W tym kontekście ważną rolę odgrywa **nowelizacja rozporządzenia eIDAS2**, które weszło w życie w maju 2024 r. Jego kluczowym elementem jest wprowadzenie Europejskiego Portfela Tożsamości Cyfrowej – narzędzia, które umożliwi obywatelom

[541] W tym kontekście UODO odwołał się do Oświadczenia 1/2025 Europejskiej Rady Ochrony Danych (EROD) zawierającego dziesięć zasad zgodnego z prawem przetwarzania danych osobowych przy zapewnieniu wieku lub przedziału wiekowego danej osoby. Oświadczenie ma na celu zapewnienie spójnego europejskiego podejścia do zapewnienia wieku, aby chronić małoletnich przy jednoczesnym przestrzeganiu zasad ochrony danych. Materiał ten został udostępniony na stronie internetowej https://uodo.gov.pl/pl/537/3624.

potwierdzanie wybranych atrybutów (np. wieku) bez ujawniania pełnych danych osobowych.

Dzięki eIDAS2 możliwe będzie tworzenie zaufanych, zdecentralizowanych rozwiązań do zapewnienia wieku, które działają na zasadzie „tylko tyle informacji, ile to konieczne". Taki model odpowiada postulatom EROD i pozwala realnie pogodzić ochronę dzieci z ochroną prywatności. Nowe ramy prawne eIDAS2 stwarzają więc fundament pod praktyczne wdrażanie skutecznych i bezpiecznych systemów zapewniania wieku w usługach cyfrowych – opartych na interoperacyjnych standardach, pełnej zgodności z RODO i wysokim poziomie zaufania technologicznego.

Temat ten jest niezwykle istotny, zarówno z perspektywy ochrony danych, jak i zapewnienia bezpieczeństwa dzieci w świecie cyfrowym. W związku z tym Urząd planuje organizację kolejnych seminariów poświęconych praktycznym i prawnym aspektom ochrony dzieci w usługach cyfrowych, w świetle wdrażanych rozwiązań wynikających z eIDAS2 oraz wytycznych EROD. Celem tych działań będzie wspieranie administratorów i dostawców usług w opracowywaniu zgodnych z prawem, skutecznych mechanizmów weryfikacji wieku.

W działania na rzecz ochrony danych osobowych dzieci i młodzieży wpisuje się również współpraca UODO z **Ministerstwem Edukacji Narodowej**. Podczas konferencji podsumowującej „Projekt innowacyjno-wdrożeniowy w zakresie oceny funkcjonalnej" (Katowice, 17.04.2024 r.), Konrad Komornicki, zastępca Prezesa UODO, uczestniczył w dyskusji dotyczącej tego, jak skoordynować działania różnych podmiotów, by efektywnie pomagać najmłodszym, ich rodzinom oraz środowisku, w którym funkcjonują na poziomie lokalnym. Dyskusja z udziałem zastępcy Prezesa UODO dotyczyła stworzenia teleinformatycznego systemu centralnego (międzysektorowej bazy danych), która docelowo ma ułatwić dostęp specjalistów do danych osobowych w celu dopasowania usług pomocowych na rzecz dzieci i ich rodzin w potrzebie, przy jednoczesnym poszanowaniu ich prawa do prywatności. Tłumaczył również, jakie podstawy RODO musi spełniać system, by dobrze działać. Zastępca Prezesa UODO zapewnił MEN o pełnym wsparciu i zaangażowaniu UODO w ten projekt, licząc przy tym na współpracę różnych podmiotów, w tym ministerstw. Ważne jest, aby system ten został wdrożony bez zbędnej zwłoki i z zachowaniem bezpieczeństwa danych osobowych.

Z kolei mając na uwadze działania podejmowane przez MEN w związku z wprowadzeniem do szkół nowego przedmiotu **„edukacja zdrowotna",** UODO zwrócił uwagę, aby w przygotowywanym programie nauczania uwzględnić elementy wiedzy na temat ochrony danych osobowych, w tym danych dotyczących szeroko rozumianego zdrowia.

Od 1 września 2025 r. uczniowie będą zdobywać wiedzę na temat ochrony danych osobowych nie tylko w ramach przedmiotów informatyka i etyka, ale także w ramach edukacji obywatelskiej oraz edukacji zdrowotnej. Dlatego wprowadzenie ochrony danych osobowych do podstawy programowej edukacji zdrowotnej i obywatelskiej to bardzo ważny krok w budowaniu świadomości na temat prywatności i bezpieczeństwa cyfrowego. Edukacja w tej dziedzinie pozwoli uczniom skuteczniej

chronić swoje dane, rozpoznawać zagrożenia i świadomie korzystać z narzędzi cyfrowych[542].

Urząd Ochrony Danych Osobowych działa na rzecz edukacji cyfrowej dzieci w ramach **Digital Education Working Group, grupy roboczej funkcjonującej w ramach The Global Privacy Assembly (GPA).** Celem DEWG jest promowanie edukacji cyfrowej różnych podmiotów, z poszanowaniem praw i wolności dzieci, podnoszenie ich świadomości poprzez edukację, a dzieciom – pomaganie w stawaniu się odpowiedzialnymi obywatelami cyfrowymi, korzystającymi z przysługujących im praw, przy jednoczesnym zachowaniu zasady odpowiedzialności rodzicielskiej. Urząd Ochrony Danych Osobowych współpracował z innymi organami nadzorczymi zrzeszonymi w DEWG nad powstaniem tzw. Bookletu – broszury zawierającej wykaz ok. 150 inicjatyw edukacyjnych w obszarze edukacji cyfrowej, realizowanych w ostatnich latach przez 30 organów ochrony danych z całego świata. Poszczególne treści broszury adresowane były do określonej grupy docelowej, począwszy od dzieci, nastolatków, poprzez rodziców, nauczycieli oraz do ogółu społeczeństwa. Broszura została rozdystrybuowana wśród szkół biorących udział w programie „Twoje dane – Twoja sprawa". Stanowi bowiem przydatny materiał, który z powodzeniem można wykorzystać na lekcjach z różnych przedmiotów. Ujęte w broszurze przykłady inicjatyw realizowanych na całym świecie, stanowią doskonałą inspirację dla szkół podejmujących działania edukacyjne w obszarze ochrony danych osobowych i prywatności, w ramach programu „Twoje dane – Twoja sprawa".

W związku z napływającymi do UODO pytaniami w zakresie przetwarzania danych osobowych dla przyjęcia i realizacji standardów ochrony małoletnich, Prezes UODO wskazywał, na jakie aspekty należy zwracać uwagę przy stosowaniu tzw. **ustawy Kamilka**, która weszła w życie 15 lutego 2024 r., aby można było stwierdzić jej zgodność ze standardami ochrony danych osobowych. Na tej podstawie Prezes UODO zwrócił się do Ministra Sprawiedliwości o zainicjowanie zmian przepisów tego aktu prawnego pod kątem dostosowania ich do zasad ochrony danych osobowych.

Lista inicjatyw edukacyjnych Prezesa Urzędu Ochrony Danych Osobowych podejmowanych na rzecz ochrony danych osobowych dzieci jest długa i obejmuje szereg zróżnicowanych i szeroko zakrojonych działań. **W planach na przyszłość** niezmiennie jest zadanie kontynuowania edukacji cyfrowej najmłodszych członków społeczeństwa i ich otoczenia[543].

---

[542] Więcej na temat zadań organu w zakresie ochrony danych osobowych w edukacji i wspólnych działań UODO i Ministerstwa Edukacji, można znaleźć w materiale opublikowanym na stronie internetowej UODO: https://uodo.gov.pl/pl/138/3647.

[543] W kwietniu 2025 r. UODO złożył wniosek o dofinansowanie projektu dotyczącego przeprowadzenia kampanii edukacyjnej w zakresie podnoszenia świadomości na temat praw dzieci i ich ochrony w Internecie. Wniosek został przygotowany w odpowiedzi na nabór „Rights of the child and children's participation CERV-2025-CHILD" prowadzony przez Komisję Europejską w ramach programu Citizens, Equality, Rights and Values Programme (CERV). Celem naboru jest wspieranie, promowanie i wdrażanie kompleksowych polityk mających na celu ochronę i promowanie praw dziecka, w tym prawa do uczestnictwa.

W związku z wytycznymi Strategii UE w zakresie praw dziecka, Europejskiej strategii na rzecz lepszego internetu dla dzieci (BIK+), obowiązkami, jakie nakłada Akt o usługach cyfrowych (DSA) na właścicieli platform internetowych w kontekście dzieci, w ramach projektu zaplanowane zostały kampanie edukacyjne skierowane do dzieci, rodziców, opiekunów i nauczycieli na temat m.in. bezpieczeństwa online i praw cyfrowych. W przypadku pozytywnej oceny wniosku, UODO będzie mógł rozpocząć realizację projektu od 1 stycznia 2026 r. Z uwagi na dotychczas zapoczątkowane już inicjatywy, m.in. we współpracy z Rzeczniczką Praw Dziecka, realizacja projektu wpisuje się w kierunek działań UODO obejmujący ochronę danych osobowych dzieci, w szczególności ich wizerunku.

Prezes UODO będzie nadal wspierać inicjatywy edukacyjne i prowadzić działania na rzecz budowania kultury ochrony danych osobowych wśród uczniów, nauczycieli, rodziców, a także seniorów i środowiska lokalnego. Troska o prawa najsłabszych członków społeczeństwa – dzieci i osób starszych – do prywatności i ochrony ich danych osobowych zostaje jednym z kluczowych kierunków działalności Urzędu Ochrony Danych Osobowych. Walka o podmiotowość i prawa człowieka – w szczególności w odniesieniu do tych najsłabszych grup społeczeństwa – stanowi główny kierunek polityki edukacyjnej realizowanej przez UODO.

Urząd Ochrony Danych Osobowych pokazuje, że ochrona danych osobowych to nie tylko obowiązek wynikający z przepisów prawa, ale również kluczowy element budowania zaufania w relacjach społecznych i zawodowych. Dlatego tak ważna jest współpraca zarówno z sektorem edukacji, jak i z organizacjami pozarządowymi, stowarzyszeniami, organizacjami prawniczymi czy przedsiębiorstwami technologicznymi, które mogą przyczynić się do upowszechniania dobrych praktyk i zwiększania świadomości w tej dziedzinie. Za przykład jednego z wielu takich działań może posłużyć realizacja nagrania z zakresu prawa do prywatności i ochrony danych osobowych oraz struktury i zadań Urzędu Ochrony Danych Osobowych, dla aplikantów radcowskich Krajowej Izby Radców Prawnych, w ramach podpisanego porozumienia o współpracy z tym podmiotem (5.04.2023 r.).

Z kolei pracownicy UODO uczestniczą w szkoleniach przygotowujących ich do nowych zadań. Przykładem jest Agencja Badań Medycznych, która zorganizowała szkolenie pn. „Europejska przestrzeń danych o zdrowiu (EHDS) w badaniach klinicznych: praktyki, regulacje i innowacje” (28.11.2024 r.). Podstawowym celem szkolenia było zwiększenie świadomości na temat EHDS oraz możliwości jej zastosowania w badaniach klinicznych.

Podkreślenia wymaga, że **Data Governance Act (DGA) –** rozporządzenie unijne dotyczące udostępniania i ponownego wykorzystania danych sektora publicznego, które objęte są ochroną, np. ze względu na tajemnicę handlową, zawodową czy własność intelektualną osób trzecich i z tego powodu nie mogą być udostępniane na ogólnych zasadach – przyznaje Prezesowi UODO nowe kompetencje. Urząd Ochrony Danych Osobowych będzie właściwy w zakresie przekazywania danych nieosobowych do państw trzecich, zgłaszania usług pośrednictwa danych, a także rejestrowania organizacji altruizmu danych (podmiotów umożliwiających dobrowolne przekazanie danych i udostępniające je na rzecz interesu społecznego. Prezes UODO będzie

sprawował nadzór w omawianym zakresie i wymierzał kary. Te zmiany wpłyną na przekształcenie Prezesa UODO w organ o nowych dodatkowych kompetencjach, który zajmie się danymi zarówno osobowymi, jak i nieosobowymi. Dla Urzędu oznacza to konieczność ustrojowych zmian, reorganizacji biura, powiększenia aparatu urzędniczego i poszerzenia kompetencji eksperckich pracowników UODO.

Za istotne należy uznać uwagi organu zgłoszone do wspomnianej już w niniejszym sprawozdaniu, **„Strategii Cyfryzacji Polski do 2035 r.”** Wśród uwag organu znalazły się m.in. kwestie niedostatecznego zabezpieczenia danych biometrycznych i danych behawioralnych w regulacjach prawnych, wykonywania usług informatycznych dotyczących obiegu danych osobowych przez podmioty nienależące do Europejskiego Obszaru Gospodarczego, przyspieszonego w ostatnich latach rozszerzania się tzw. Internetu Rzeczy czy wykorzystywania przez sektor prywatny danych osobowych administrowanych przez sektor publiczny.

Jednym z kluczowych kierunków działania organu na najbliższe miesiące będzie też zapewnienie skutecznej ochrony danych osobowych **w służbie zdrowia**, gdyż to właśnie z tego sektora pochodzi ogromna liczba naruszeń, czy głośnych wycieków danych.

Dostosowanie działań Urzędu do zmieniających się potrzeb społeczeństwa, rozwijających się technologii oraz nowych regulacji unijnych wymaga elastyczności, innowacyjności i skuteczności w zarządzaniu zasobami Urzędu.

Zapewnienie skutecznego bezpieczeństwa danym osobowym jest procesem ciągłym, dlatego edukowanie obywateli jest i będzie wciąż aktualnym zadaniem organu.

ZAŁĄCZNIKI

Załącznik nr 1: Wykaz administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2024 r.

Lp.	Data decyzji	Departament UODO prowadzący postępowanie	Sygnatura	Wysokość kary w zł
1	03.01.2024	Departament Kontroli i Naruszeń	DKN.5131.49.2022	4 716,00
2	17.01.2024	Departament Kontroli i Naruszeń	ZSPR.421.2.2019 ZSPR.405.67.2019	3 819 960,00
3	18.01.2024	Departament Kontroli i Naruszeń	DKN.5131.53.2021	9 903,60
4	12.03.2024	Departament Kontroli i Naruszeń	DKN.5131.59.2022	1 440 549,00
5	12.03.2024	Departament Kontroli i Naruszeń	DKN.5131.28.2023	78 575,40
6	24.04.2024	Departament Kontroli i Naruszeń	DKN.5131.32.2022	10 913,00
7	29.04.2024	Departament Kontroli i Naruszeń	DKN.5131.29.2023	238 345,00
8	30.04.2024	Departament Kontroli i Naruszeń	DKN.5131.58.2022	916,71
9	20.05.2024	Departament Kontroli i Naruszeń	DKN.5112.35.2021	1 440 549,00
10	28.05.2024	Departament Kontroli i Naruszeń	DKN.5131.21.2022	17 025,00
11	13.06.2024	Departament Kontroli i Naruszeń	DKN.5131.57.2022	40 000,00
12	10.07.2024	Departament Organizacji, Kar i Egzekucji	DOKE.561.1.2024	21 827,00
13	20.08.2024	Departament Kontroli i Naruszeń	DKN.5131.1.2024	4 053 173,00
14	30.08.2024	Departament Organizacji, Kar i Egzekucji	DOKE.561.4.2024	19 644,00
15	02.09.2024	Departament Kontroli i Naruszeń	DKN.5131.33.2023	85 000,00
16	09.10.2024	Departament Kontroli i Naruszeń	DKN.5131.1.2021	353 589,00
17				9 822,00
18	10.10.2024	Departament Kontroli i Naruszeń	DKN.5131.35.2021	15 000,00
19				20 000,00
20				24 882,21
21	18.10.2024	Departament Kontroli i Naruszeń	DKN.5131.7.2024	25 000,00
22	12.11.2024	Departament Kontroli i Naruszeń	DKN.5131.9.2024	24 555,00
23	12.11.2024	Departament Kontroli i Naruszeń	DKN.5130.2415.2020	1 527 855,00
24				20 037,00
25	26.11.2024	Departament Kontroli i Naruszeń	DKN.5131.6.2024	29 684,04
26	18.12.2024	Departament Kontroli i Naruszeń	DKN.5112.14.2022	261 918,00
27				314 302,00

Załącznik nr 2: Wykaz wydarzeń objętych patronatem Prezesa UODO w 2024 r.

1. Ogólnopolska Konferencja Naukowa „Aktualne problemy ochrony danych osobowych”. Organizator: Centrum Badań nad Cyberprzestępczością, WPiA Uniwersytetu Mikołaja Kopernika w Toruniu, 19.01.2024 r.

2. Konferencja Rzeczowo o Prawie: „Praktyczne aspekty naruszeń ochrony danych osobowych. Wykrycie, ocena, zgłoszenie – badanie i procedury”. Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych Sp. k., 25.01.2024 r.

3. X Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej. Organizator: Akademia WSB w Dąbrowie Górniczej, 1.02.2024 r.

4. I edycja debaty pt. „Jakość usług publicznych i e-administracja”. Organizator: Polskie Towarzystwo Informatyczne. Warszawa, 22.02.2024 r.

5. Spotkanie Manager Business Hub. Trojanów, 7-8.03.2024 r.

6. Konferencja „Akt o usługach cyfrowych okiem autorów komentarzy”. Organizatorzy: Centrum Ochrony Danych Osobowych i Zarządzania Informacją na WPiA Uniwersytetu Łódzkiego, Okręgowa Izba Radców Prawnych w Łodzi oraz Katedra Europejskiego Prawa Gospodarczego, WPiA Uniwersytetu Łódzkiego. Łódź, 15.03.2024 r.

7. 3. Edycja DATA ECONOMY CONGRESS. Organizator: MMC Polska. Warszawa, 25-26.03.2024 r.

8. Ogólnopolska konferencja naukowa online „Granice inwigilacji. W poszukiwaniu optymalnego modelu ochrony prywatności”. Organizatorzy: Katedra Prawa Konstytucyjnego na Wydziale Prawa, Administracji i Ekonomii UWr, Katedra Europejskiego Prawa Konstytucyjnego na WPiA UŁ, Katedra Prawa Administracyjnego i Samorządu Terytorialnego na WPiA UKSW, 23.04.2024 r.

9. IV Ogólnopolska Konferencja Naukowa Prawa Nowych Technologii. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Łódź. WPiA UŁ, 6.05.2024 r.

10. Wykład prof. dr hab. Agnieszki Grzelak, Zastępczyni Prezesa UODO, pt. „Dyrektywa policyjna 2016/680 – (nie)chciana siostra RODO?”. Organizator: Koło Naukowe Prawa Ochrony Danych Osobowych i Sztucznej Inteligencji „Salus Populi”, działające na WPiA Uniwersytetu im. Adama Mickiewicza w Poznaniu. 20.05.2024 r.

11. Konferencja z okazji 6. rocznicy obowiązywania RODO w Polsce, pt. „Ochrona danych osobowych 2018-2024. Wyzwania w cyfrowej rzeczywistości”. Organizator: Lubasz i Wspólnicy Kancelaria Radców Prawnych, 22.05.2024 r.

12. Forum IAB 2024. Organizator: Związek Pracodawców Branży Internetowej IAB Polska. Warszawa, 22-23.05.2024 r.

13. IV edycja Tour de Konstytucja „Siła Młodych – Most Pokoleń" – ogólnopolskie spotkania. Organizator: Fundacja Aktywna Demokracja. Start 2.06.2024 r. Tomaszów Mazowiecki.

14. XVII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. Bielsko-Biała, 3-5.06.2024 r.

15. IV Międzynarodowa Konferencja „AI & MEDTECH CEE. Organizatorzy: Polska Federacja Szpitali, zespół ekspertów wZdrowiu oraz Koalicja AI w Zdrowiu. Warszawa, 11.06.2024 r.

16. Konferencja pt. „Ochrona danych medycznych". Organizator: Akademia WSB w Dąbrowie Górniczej, 19.06.2024 r.

17. Konferencja „PINT 24 – Prawo i Nowe technologie". Organizator: Okręgowa Izba Radców Prawnych w Krakowie. 28-29.06.2024 r.

18. Seminarium pt. „Przetwarzanie danych osobowych przez związki zawodowe. Od teorii do praktyki w kierunku poradnika. Partner merytoryczny: Katedra Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego. 31.07.2024 r.

19. ETH Legal. Panel dyskusyjny „Przyszłość regulacji prawnych w kontekście technologii blockchain". Organizatorzy: Cyber Science, Uniwersytet Śląski w Katowicach. Warszawa, 7.09.2024 r.

20. VII Konferencja z cyklu RODO w zakładzie pracy, pt. „Przetwarzanie danych osobowych a wewnętrzne procedury zgłaszania naruszeń prawa". Organizator: Katedra Prawa Pracy i Polityki Społecznej, WPiA Uniwersytetu Jagiellońskiego. Kraków, 20.09.2024 r.

21. VIII Krajowy Kongres Sekretarzy. Organizatorzy: Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego oraz Krajowa Rada Forów Sekretarzy JST. Warszawa, 24-25.09.2024 r.

22. Międzynarodowa konferencja „Converging Realms: Law, Technology and Society in the Age of Ethical and Multi-Agent AI". Organizatorzy: WPiA Uniwersytetu Jagiellońskiego, Future Law Lab przy Uniwersytecie Jagiellońskim, Fundacja Centrum Cyfrowe. Kraków, 26-27.09.2024 r.

23. Konferencja CYBER24 DAY. Organizator: Grupa Defence24. Warszawa, 2.10.2024 r.

24. Konferencja online „SYGNALIŚCI x RODO – wyzwania po pierwszych tygodniach obowiązywania ustawy". Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp.k. 10.10.2024 r.

25. XIII Konwent Ochrony Danych i Informacji „Zmiany legislacyjne – wpływ na zadania IOD". Organizator: FORSAFE Sp. z o.o. Łódź, 23.10.2024 r.

26. Kampania e-Izba: Bezpieczny Black Friday. Organizator: Izba Gospodarki Elektronicznej w Warszawie. 24.10.2024 r.

27. II edycja International Scientific Workshop – „Legal Challenges of Disruptive Technologies". Organizator: Akademia Leona Koźmińskiego w Warszawie. 7–8.11.2024 r.

28. XXII Ogólnopolski Konkurs Prawa Europejskiego. Organizatorzy: ELSA Poland i Grupa Lokalna ELSA Łódź. Łódź, 7.12.2024 r.

29. Konferencja AI TASK FORCE Innovation Summit. Organizatorzy: WPiA Uniwersytetu Łódzkiego oraz Lubasz i Wspólnicy Kancelaria Radców Prawnych. Warszawa, 11.12.2024 r.

Załącznik nr 3: Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2024 r. w Polsce przez UODO lub inne podmioty

Lp.	Data	Wydarzenie	Miejsce
1.	8.01.2024 r.	Warsztaty dla seniorów na temat bezpiecznego korzystania ze zdobyczy nowych technologii podczas codziennych czynności. Organizator: UODO w ramach obchodów 18. Dnia Ochrony Danych Osobowych 2024.	Warszawa
2.	10.01.2024 r.	Warsztaty dla studentów „Bezpieczna droga przez cyberprzestrzeń: od deepfake'ów po bezpieczeństwo aplikacji mobilnych". Organizator: UODO w ramach obchodów 18. Dnia Ochrony Danych Osobowych 2024.	Warszawa
3.	16.01.2024 r.	Debaty „Ochrona danych osobowych w sektorze zdrowia w dobie rozwoju nowych technologii", w ramach obchodów 18. Dnia Ochrony Danych Osobowych 2024. Organizator: UODO.	Warszawa
4.	19.01.2024 r.	Konferencja Naukowa Ochrona Danych Osobowych, pt. „Aktualne problemy ochrony danych osobowych" w ramach obchodów 18. Dnia Ochrony Danych Osobowych. Organizator: Centrum Badań nad Cyberprzestępczością, WPiA UMK w Toruniu.	Toruń
5.	25.01.2024 r.	Konferencja w ramach obchodów 18. Dnia Ochrony Danych Osobowych 2024, Wykrycie, ocena, zgłoszenie – badanie i procedury". Organizatorzy: Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp. k., Fundacja Centrum Cyfrowe oraz Aigorithmics sp. z o.o.	Warszawa
6.	29.01.2024 r.	Punkty konsultacyjne dla Inspektorów Ochrony Danych oraz porady prawne dla obywateli zorganizowane w siedzibie UODO. Organizator: UODO.	Warszawa
7.	30.01.2024 r.	Webinarium online z cyklu „Certyfikacja w ochronie danych". Organizator: UODO.	Warszawa
8.	31.01.2024 r.	#ODOlekcja – zajęcia online dla uczniów szkół ponadpodstawowych, pt. „Deepfake: fałszywa rzeczywistość w sieci – czy jesteś na to gotowy?" Organizator: UODO.	Warszawa
9.	1.02.2024 r.	X Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej – konferencja tematyczna połączona z promocją dobrych praktyk w zakresie ochrony danych osobowych. Organizator: Akademia WSB w Dąbrowie Górniczej,	Dąbrowa Górnicza
10.	5.02.2024 r.	Spotkanie logistyczno-organizacyjne dotyczące ewaluacji Schengen w MSWiA.	Warszawa
11.	6.02.2024 r.	Wywiad w Radio Dzieciom.	Warszawa
12.	7.02.2024 r.	Spotkanie z Naczelną Izbą Lekarską inaugurujące powstanie zespołu ds. bezpieczeństwa danych medycznych.	Warszawa
13.	7.02.2024 r.	Webinarium dla uczniów pn. „DODO Agencja – biblijna interwencja", w ramach programu „Twoje dane – Twoja sprawa".	online
14.	12.02.2024 r.	Gra terenowa „O dane dbam codziennie" z okazji 18. Dnia Ochrony Danych Osobowych. Organizator: UODO oraz harcerze z 200. Grunwaldzkiej Warszawskiej Drużyny Harcerskiej „Leśnicy" w Warszawie.	Warszawa

Lp.	Data	Wydarzenie	Miejsce
15.	22.02.2024 r.	Wydarzenie: e-Izba Dialog z Biznesem i Administracją Publiczną „Taki Sam Start”.	Warszawa
16.	22.02.2024 r.	1. edycja debaty pt. „Jakość usług publicznych i e-administracja”. Organizator: Polskie Towarzystwo Informatyczne.	Warszawa
17.	26.02.2024 r.	Webinarium „Certyfikacja w ochronie danych”. Organizator: UODO.	online
18.	27.02.2024 r.	Konferencja „Top Trendy Life Sciences”. Organizator: Kancelaria DZP.	Warszawa
19.	28.02.2024 r.	Konferencja pt. „Cyberbezpieczeństwo w zdrowiu”. Organizator: Kancelaria DPZ przy współudziale Ambasady Izraela w Warszawie.	Warszawa
20.	29.02.2024 r.	Debata „Jakość usług publicznych i e-administracja”.	Warszawa
21.	3-5.03.2024 r.	Forum Wymiany Doświadczeń Organów Ochrony Danych (Data Protection Authorities Experience Exchange Forum), współorganizowane przez Urząd Ochrony Danych Osobowych ramach projektu EU4DigitalUA.	Warszawa
22.	7-8.03.2024 r.	Konferencja „Manager Business Hub”.	Trojanów
23.	14.03.2024 r.	Webinarium – warsztaty online dla uczniów „Nagrywanie oraz montowanie filmu na urządzeniach mobilnych”. Organizator: UODO w ramach programu edukacyjnego „Twoje dane – Twoja sprawa”	online
24.	15.03.2024 r.	Konferencja pt. „Akt o usługach cyfrowych okiem autorów komentarzy”. Organizatorzy: Centrum Ochrony Danych Osobowych i Zarządzania Informacją na WPiA UŁ, Okręgowa Izba Radców Prawnych w Łodzi oraz Katedra Europejskiego Prawa Gospodarczego, WPiA UŁ.	Łódź
25.	19.03.2024 r.	Spotkanie Prezesa UODO z Europejskim Inspektorem Ochrony Danych (EIOD).	Warszawa
26.	25.03.2024 r.	Kongres Bezpieczeństwa Biznesu. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych – KSOIN.	Spała
27.	25.03.2024 r.	Wykład w ramach Tour de Konstytucja.	Wiskitki
28.	25.03.2024 r.	3. edycja DATA ECONOMY CONGRESS. Organizator: MMC Polska.	Warszawa
29.	27.03.2024 r.	Webinarium „Certyfikacja w ochronie danych”. Organizator: UODO.	online
30.	9.04.2024 r.	Spotkanie pn. „Niezależność inspektora ochrony danych w świetle działania EROD dotyczącego pozycji i wyznaczania IOD (CEF DPO).	Warszawa
31.	10.04.2024 r.	Wykład w LO im. Piotra Skargi w Grójcu w ramach Tour de Konstytucja.	Grójec
32.	11-12.04.2024 r.	Spotkanie Inspektorów Ochrony Danych Okręgowych Izb Radców Prawnych.	Wrocław
33.	11.04.2024 r.	Szkolenie w Głównym Urzędzie Miar.	Warszawa
34.	15.04.2024 r.	Konferencja „20 lat minęło jak jeden dzień? Prawne aspekty członkostwa Polski w Unii Europejskiej w dwudziestą rocznicę akcesji”.	Warszawa
35.	15.04.2024 r.	Panel ekspertów – wydarzenie Najwyższej Izby Kontroli.	Warszawa
36.	15.04.2024 r.	Ogólnopolska Konferencja Naukowa pt. „Prawo i Kościół”. Organizator: Akademia Katolicka w Warszawie.	Warszawa
37.	16.04.2024 r.	Webinarium „Cyfrowy l@birynt – uważaj na pułapki w sieci”. Organizator: UODO.	online
38.	17.04.2024 r.	Konferencja podsumowująca „Projekt innowacyjno-wdrożeniowy w zakresie oceny funkcjonalnej”. Organizator: Ministerstwo Edukacji Narodowej	Katowice
39.	17.04.2024 r.	III Forum Seniora 2024. Organizator: Polska Press.	Warszawa

Lp.	Data	Wydarzenie	Miejsce
40.	18.04.2024 r.	Webinarium poświęcone zagadnieniu ochrony danych osobowych w kontekście stosowania sztucznej inteligencji. Organizator: UODO.	online
41.	23.04.2024 r.	Ogólnopolska konferencja naukowa pt. „Granice inwigilacji. W poszukiwaniu optymalnego modelu ochrony prywatności". Organizatorzy: Katedra Prawa Konstytucyjnego na Wydziale Prawa, Administracji i Ekonomii UWr, Katedra Europejskiego Prawa Konstytucyjnego na WPiA UŁ, Katedra Prawa Administracyjnego i Samorządu Terytorialnego na WPiA UKSW w Warszawie.	online
42.	24.04.2024 r.	Warsztaty wdrożeniowe dot. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2023/970 z 10 maja 2023 r. w sprawie wzmocnienia stosowania zasady równości wynagrodzeń dla mężczyzn i kobiet za taką sama pracę lub pracę o takiej samej wartości, za pośrednictwem mechanizmów przejrzystości wynagrodzeń oraz mechanizmów egzekwowania. Organizator: Ministerstwo Rodziny, Pracy i Polityki Społecznej.	online
43.	24.04.2024 r.	V webinarium serii „Certyfikacja w ochronie danych". Organizator: UODO.	online
44.	26.04.2024 r.	Spotkanie Zespołu ds. danych równościowych Instytutu Miast Praw Człowieka.	online
45.	26.04.2024 r.	Konferencja „Wyzwania dla ochrony danych osobowych dzieci". Organizatorzy: UODO i RPD.	Warszawa
46.	6.05.2024 r.	IV Ogólnopolska Konferencja Naukowa Prawa Nowych Technologii. Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Łódź, WPiA UŁ.	Łódź
47.	8.05.2024 r.	Konferencja „Forum Bezpieczeństwa Banków". Organizator: Związek Banków Polskich.	Warszawa
48.	8.05.2024 r.	Panel dyskusyjny IAPP „Spersonalizowana reklama i modele Pay or Consent".	Warszawa
49.	10.05.2024 r.	Wydarzenie pn. „Polska w Unii Europejskiej – jakich praw chcemy na co dzień?"	Warszawa
50.	11.05.2024 r.	Szkolenie dla IOD pełniących funkcje w kościołach i innych związkach wyznaniowych. Organizatorzy UODO i Kościelny Inspektor Ochrony Danych,	Łagiewniki
51.	15.05.2024 r.	Webinarium z cyklu RODO w szkolnej ławce, pt. „Wykorzystywanie wizerunku dziecka – prawo i praktyka. Organizator: UODO	online
52.	20.05.2024 r.	Wykład pt. „Dyrektywa policyjna 2016/680 – (nie)chciana siostra RODO?" w ramach projektu naukowego „Czas na RoDoOo – Chroń siebie i swoje dane osobowe! – II edycja", realizowanego na Wydziale Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu.	online
53.	21.05.2024 r.	Konferencja „Kierownictwo organizacji we wdrażaniu bezpieczeństwa informacji". Organizator: Stowarzyszenie Inspektorów Ochrony Danych Osobowych – SIODO.	Warszawa
54.	22.05.2024 r.	Forum IAB 2024. Organizator: Związek Pracodawców Branży Internetowej IAB Polska.	Warszawa
55.	22.05.2024 r.	XIII Kongres Transportu Publicznego i Technologii Miejskich. Organizatorzy: Zespół Doradców Gospodarczych TOR oraz Zarząd Transportu Miejskiego w Warszawie.	Warszawa
56.	22.05.2024 r.	VI webinarium PCA w ramach cyklu „Certyfikacja w ochronie danych".	online
57.	22.05.2024 r.	Konferencja z okazji 6. rocznicy obowiązywania RODO w Polsce, pt. „Ochrona danych osobowych 2018–2024.	online

Lp.	Data	Wydarzenie	Miejsce
		Wyzwania w cyfrowej rzeczywistości". Organizator: Lubasz i Wspólnicy Kancelaria Radców Prawnych sp. k.	
58.	23.05.2024 r.	Forum IAB „25 lat #GenDigital. Dojrzałość i Młodość".	Warszawa
59.	24.05.2024 r.	II spotkanie Zespołu ds. danych równościowych Instytutu Miast Praw Człowieka.	online
60.	24.05.2024 r.	Uroczysty Senat UŁ i doktorat *honoris causa* dla dra hab. Adama Bodnara.	Łódź
61.	28.05.2024 r.	Konferencja „Dostępność dziś i jutro".	Warszawa
62.	28.05.2024 r.	Konferencja „Cyberhigiena i cyberochrona w administracji, biznesie i oświacie". Organizator: Stowarzyszenie Inspektorów Ochrony Danych Osobowych.	Warszawa
63.	2.06.2024 r.	IV edycja Tour de Konstytucja „Siła Młodych – Most Pokoleń" – ogólnopolskie spotkania. Organizator: Fundacja Aktywna Demokracja.	Tomaszów Mazowiecki
64.	3-5.06.2024 r.	XVII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych.	Bielsko-Biała
65.	4.06.2024 r.	Konferencja „Ochrona danych osobowych w Unii Europejskiej. Dokąd zmierzamy w przededniu wyborów europejskich?". Organizator: UODO.	Warszawa
66.	10-11.06.2024 r.	Konferencja Uniwersytetu Jagiellońskiego pt. „Unia Europejska wobec wyzwań XXI wieku".	Gródek
67.	10-11.06.2024 r.	Posiedzenie Komisji ds. Międzynarodowego Prawa Humanitarnego w Ministerstwie Spraw Zagranicznych.	Warszawa
68.	11.06.2024 r.	Konferencja Naukowa pt. „Europejska przestrzeń danych dotyczących zdrowia – ewolucja czy rewolucja?".	Warszawa
69.	11.06.2024 r.	IV Międzynarodowa konferencja „AI & MEDTECH CEE". Organizatorzy: Polska Federacja Szpitali, zespół ekspertów w Zdrowiu oraz Koalicja AI w Zdrowiu.	Warszawa
70.	14.06.2024 r.	Konferencja podsumowująca XIV edycję programu „Twoje dane – Twoja sprawa". Organizator: UODO.	Warszawa
71.	19.06.2024 r.	Seminarium „Przetwarzanie danych przez ZUS i płatników składek w związku z realizacją ustawowych obowiązków. Praktyczne aspekty. Organizator: ZUS we współpracy z UODO.	Wrocław
72.	19.06.2024 r.	Konferencja Naukowa „Ochrona danych medycznych". organizator: Akademia WSB w Dąbrowie Górniczej.	Dąbrowa Górnicza
73.	26.06.2024 r.	Warsztaty z przedstawicielami OpenAI. Organizator: Krajowa Izba Radców Prawnych.	Warszawa
74.	26.06.2024 r.	Spotkanie z inspektorami ochrony danych instytucji kościelnych w siedzibie UODO.	Warszawa
75.	27.06.2024 r.	Konferencja „Ochrona danych osobowych w świetle aktu o sztucznej inteligencji i innych aktów wdrażających europejską strategię danych. Organizatorzy: UODO i WPiA UW.	Warszawa
76.	28-29.06.2024 r.	Konferencja PINT24 – Prawo i Nowe Technologie. Organizator: Okręgowa Izba Radców Prawnych w Krakowie.	Kraków
77.	15.07.2024 r.	III spotkanie Zespołu ds. danych równościowych Instytutu Miast Praw Człowieka.	online
78.	31.07.2024 r.	Seminarium Społecznego Zespołu Ekspertów przy Prezesie UODO, pt. „Przetwarzanie danych osobowych przez związki zawodowe. Od teorii do praktyki w kierunku poradnika". Partner merytoryczny: Katedra Prawa Pracy i Polityki Społecznej Uniwersytetu Jagiellońskiego.	Warszawa
79.	7.08.2024 r.	Seminarium „Praktyczne problemy w stosowaniu przepisów ustawy o ochronie sygnalistów z perspektywy	Warszawa

Lp.	Data	Wydarzenie	Miejsce
		RODO. Przyczynek do dyskusji nad wątpliwościami zgłoszonymi w trakcie konsultacji społecznych". Organizatorzy: UODO i Społeczny Zespół Ekspertów przy Prezesie UODO.	
80.	3-5.09.2024 r.	Spotkanie w ramach Forum Wymiany Doświadczeń Organów Ochrony Danych (Data Protection Authorities Experience Exchange Forum). Wizyta ukraińskiej i hiszpańskiej delegacji w UODO. Współorganizator: UODO.	Warszawa
81.	4.09.2024 r.	XXXIII Forum Ekonomiczne.	Karpacz
82.	7.09.2024 r.	ETH Legal. Panel: Inkubacja innowacji prawniczych w kontekście technologii blockchain. Organizator: Cyber Science, Śląskie Centrum Inżynierii Prawa, Technologii i Kompetencji Cyfrowych, Uniwersytet Śląski w Katowicach.	Warszawa
83.	16.09.2024 r.	Seminarium „Wdrożenie ustawy o sygnalistach oraz ochrona danych osobowych w miejscu pracy". Organizator: ZUS we współpracy z UODO.	Gdańsk
84.	20.09.2024 r.	VII konferencja z cyklu RODO w zakładzie pracy, pt. „Przetwarzanie danych osobowych a wewnętrzne procedury zgłaszania naruszeń prawa". Organizator: Katedra Prawa Pracy i Polityki Społecznej, WPiA Uniwersytetu Jagiellońskiego.	Kraków
85.	21.09.2024 r.	6. Warszawska Olimpiada Seniorów. Organizator: Urząd Miasta Warszawy.	Warszawa
86.	24.09.2024 r.	VIII Krajowy Kongres Sekretarzy. Organizatorzy: Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego oraz Krajowa Rada Forów Sekretarzy JST.	Warszawa
87.	26.09.2024 r.	Olimpiada dla Przedszkolaków. Organizator: Urząd Miasta Warszawy.	Warszawa
88.	26.09.2024 r.	Spotkania z przedstawicielami JST woj. małopolskiego w ramach akcji „UODO rusza w kraj".	Kraków, Tarnów
89.	26.09.2024 r.	Spotkanie Prezesa UODO z Kanclerzem Kurii Metropolitarnej w Krakowie, w ramach akcji „UODO rusza w kraj".	Kraków
90.	26.09.2024 r.	Międzynarodowa konferencja „Converging Realms: Law, Technology, and Society in the Age of Ethical and Multi_Agent AI". Organizatorzy: Future Law Lab przy UJ, WPiA UJ oraz Fundacja Centrum Cyfrowe.	Kraków
91.	30.09.2024 r.	Szkolenie przedstawicieli Komendy Głównej Policji.	Warszawa
92.	1.10.2024 r.	Wykład inauguracyjny Prezesa UODO w związku z otwarciem roku akademickiego 2024/2025 na Politechnice Warszawskiej.	Warszawa
93.	1.10.2024 r.	Spotkanie z uczniami Szkoły Podstawowej z Jerzykowa w ramach programu Ministerstwa Finansów pn. „Lekcja o finansach". Organizator: UODO.	Warszawa
94.	2.10.2024 r.	Konferencja CYBER24 DAY. Organizator: Grupa Defence24.	Warszawa
95.	7.10.2024 r.	Seminarium „Ochrona danych jako element odporności społeczeństwa i państwa". Organizatorzy: UODO, SZE przy Prezesie UODO, ZUS.	Warszawa
96.	8.10.2024 r.	4. Data Economy Congress.	Warszawa
97.	8.10.2024 r.	Inauguracja roku akademickiego w Akademii Katolickiej.	Warszawa
98.	9.10.2024 r.	Seminarium „Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji". Organizatorzy: UODO i ZUS.	Chorzów

Lp.	Data	Wydarzenie	Miejsce
99.	15.10.2024 r.	Konferencja „Ochrona danych w robotyce medycznej w dobie AI Act oraz EHDS". Organizatorzy: UODO, Fundacja AI One Health, Izba POLMED, Ośrodek Przetwarzania Informacji – Państwowy Instytut Badawczy, we współpracy ze Społecznym Zespołem Ekspertów przy Prezesie UODO.	Warszawa
100.	17.10.2024 r.	Konferencja „AI w medycynie a przetwarzanie danych osobowych pacjentów – przyczynek do dyskusji nad postępującymi zmianami". Organizator: Biuro Bezpieczeństwa Warszawskiego Uniwersytetu Medycznego.	Warszawa
101.	17.10.2024 r.	Spotkanie w Ministerstwie Zdrowia dot. rejestru chorób rzadkich.	Warszawa
102.	21.10.2024 r.	Forum Rynku Zdrowia.	Warszawa
103.	21.10.2024 r.	Spotkanie z przedstawicielami Związku Województw RP. Organizator: UODO.	Warszawa
104.	22.10.2024 r.	Konferencja „Dwudziestolecie polszczyzny w Unii Europejskiej: przemiany i wyzwania". Organizator: Przedstawicielstwo KE w Polsce.	Warszawa
105.	22.10.2024 r.	Obchody 15-lecia Rzecznika Praw Pacjenta.	Warszawa
106.	23.10.2024 r.	XIII Konwent Ochrony Danych i Informacji „Zmiany legislacyjne – wpływ na zadania IOD". Organizator: FORSAFE Sp. z o.o.	Łódź
107.	24.10.2024 r.	Gala Jubileuszowa z okazji 90-lecia ZUS.	Warszawa
108.	24.10.2024 r.	Webinarium w ramach kampanii e-Izby: Bezpieczny Black Friday. Organizator: Izba Gospodarki Elektronicznej we współpracy z Federacją Konsumentów.	Warszawa
109.	24-25.10.2024 r.	Inauguracja 15. edycji Programu „Twoje dane – Twoja sprawa".	online
110.	25.10.2024 r.	Forum Fundacji Orange.	Warszawa
111.	29.10.2024 r.	Spotkanie Prezesa UODO ze Związkiem Przedsiębiorstw Finansowych w Polsce.	Warszawa
112.	7.11.2024 r.	II edycja International Scentific Workshop – Legal Challengers of Disruptive Technologies. Organizator: Akademia Leona Koźmińskiego w Warszawie.	Warszawa
113.	8.11.2024 r.	Wizyta delegacji kosowskiego organu ochrony danych.	Warszawa
114.	15.11.2024 r.	Seminarium „Ochrona zdrowia w zatrudnieniu a RODO". Organizatorzy: UODO, SZE przy Prezesie UODO, Konfederacja Lewiatan.	Warszawa
115.	20.11.2024 r.	I Human Rights Cities Conference. Organizator: Instytut Miast Praw Człowieka.	Poznań
116.	21.11.2024 r.	II Konferencja Naukowa pn. „Bezpieczeństwo informacji w organizacji i jej zasobów", w ramach programu „UODO rusza w kraj". Organizatorzy: Katedra Prawa Gospodarczego Uniwersytetu Ekonomicznego w Katowicach, UODO, Czasopismo Studia Prawnoustrojowe UWM w Olsztynie, KiHG Radcowie Prawni Sp. p.	Katowice
117.	28.11.2024 r.	Konferencja „Wyzwania związane z ochroną danych. Spojrzenie z perspektywy 2024 roku". Organizatorzy: UODO, ZUS.	Warszawa
118.	28.11.2024 r.	Ogólnopolska Konferencja Naukowa „Sztuczna Inteligencja w środowisku pracy". Organizator: Zespół badawczy AI Work Team WPiA Uniwersytetu Łódzkiego i Okręgowy Inspektorat Państwowej Inspekcji Pracy w Łodzi.	Łódz

Lp.	Data	Wydarzenie	Miejsce
119.	29.11.2024 r.	Spotkanie Prezesa UODO z członkami Koalicji AI w Zdrowiu.	Warszawa
120.	6.12.2024 r.	Wykład otwarty przewodniczącego Społecznego Zespołu Ekspertów przy Prezesie UODO, pt. „Projektowanie prywatności na przykładzie Internetu Rzeczy (IoT) – perspektywa dostawcy i korzystającego”.	online
121.	9.12.2024 r.	Warsztaty dotyczące wdrożenia i stosowania art. 74 AMLR, zorganizowane w ramach programu Future of Financial Intelligence Sharing (FFIS). Organizatorzy: Generalny Inspektor Informacji Finansowej, RUSI Centre for Financial Security oraz Związek Banków Polskich.	Warszawa
122.	10.12.2024 r.	Konferencja inaugurująca ogólnopolską kampanię informacyjno-edukacyjną pn. „Więcej szacunku dla młodego wizerunku”. Organizator: Rzecznik Praw Dziecka.	Warszawa
123.	10.12.2024 r.	Szkolenie z zakresu ochrony danych osobowych dla kościelnych inspektorów ochrony danych osobowych (IOD). Organizatorzy: Kościelny Inspektor Ochrony Danych przy Konferencji Episkopatu Polski i Instytut Bona Fama.	Warszawa
124.	11.12.2024 r.	Konferencja „AI TASK FORCE Innovation Summit”. Organizatorzy: Lubasz i Wspólnicy Kancelaria Radców Prawnych sp. k., Fundacja Centrum Cyfrowe oraz Aigorithmics sp. z o.o.	Warszawa
125.	11.12.2024 r.	Spotkanie ze spółką Meta dot. nawiązania dialogu na rzecz bezpieczeństwa i prywatności użytkowników.	Warszawa
126.	11.12.2024 r.	Webinarium „Przyjmowanie zgłoszeń zewnętrznych – nowe wyzwanie dla organów publicznych”. Organizator: Rzecznik Praw Obywatelskich.	online
127.	13.12.2024 r.	Konwersatorium dla studentów UKSW zorganizowane w siedzibie UODO. Organizator: UODO.	Warszawa
128.	16.12.2024 r.	Międzynarodowa Konferencja „AI 360. Regulacje, Innowacje, Współpraca”. Organizatorzy: Komisja Cyfryzacji, Innowacji i Nowoczesnych Technologii, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy oraz Uniwersytet Warszawski.	Warszawa
129.	18.12.2024 r.	Szkolenie dla pełnomocników ds. otwartości danych w Ministerstwie Cyfryzacji.	Warszawa
130.	18.12.2024 r.	Webinarium dla grona pedagogicznego w ramach kampanii „Więcej szacunku dla młodego wizerunku”.	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 2024 r.

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	9.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
2.	10.01.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
3.	15.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
4.	16.01.2024 r.	89. Posiedzenie plenarne EROD.	online
5.	17.01.2024 r.	Wspólne spotkanie Podgrupy ekspertów ds. Międzynarodowego przekazywania danych (International Transfers ESG) i Podgrupy ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE) Europejskiej Rady Ochrony Danych.	online
6.	17-18.01.2024 r.	Spotkanie Podgrupy ekspertów ds. Międzynarodowego przekazywania danych (International Transfers ESG) Europejskiej Rady Ochrony Danych.	online
7.	17-18.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	Bruksela
8.	19.01.2024 r.	Spotkanie grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD (CEF DPO).	online
9.	19.01.2024 r.	Spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C).	Bruksela
10.	19.01.2024 r.	European Blockchain Sandbox.	online
11.	19.01.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
12.	22.01.2024 r.	Wspólne spotkanie Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup – CEH) i Podgrupy ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
13.	22.01.2024 r.	Wspólne spotkanie Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) i Podgrupy ekspertów ds. Międzynarodowego przekazywania danych (International Transfers ESG) Europejskiej Rady Ochrony Danych.	online
14.	22.01.2024 r.	Spotkanie Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup – CEH) Europejskiej Rady Ochrony Danych.	online
15.	22.01.2024 r.	Wspólne spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych oraz Podgrupy Ekspertów ds.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
		Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	
16.	22.01.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Taskforce on International Engagement (TF INT).	online
17.	23.01.2024 r.	Spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
18.	24.01.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
19.	24-26.01.2024 r.	Konferencja z okazji 18. Dnia Ochrony Danych – CPDP Data Protection Day.	Bruksela
20.	25.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	online
21.	25.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
22.	29-31.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
23.	30.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
24.	30-31.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
25.	31.01.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
26.	1.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	Bruksela
27.	1.02.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
28.	2.02.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
29.	6.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG).	online
30.	7.02.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
31.	7.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
32.	7-8.02.2024 r,	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	Bruksela
33.	8.02.2024 r.	Spotkanie z Komisją Europejską dot. organizacji Ewaluacji Schengen w zakresie ochrony danych osobowych.	online
34.	12.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
35.	13.02.2024 r.	90. Posiedzenie plenarne EROD.	Bruksela

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
36.	15.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
37.	20.02.2024 r.	Wspólne spotkanie Grupy zadaniowej ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT), Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) i Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	online
38.	20.02.2024 r.	Preparation call for EU Commission High-level roundtable on 4/3 on safe data flows.	online
39.	21.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
40.	21-22.02.2024 r.	Conference „Enhancing the implementation of the EU Charter of Fundamental Rights: Strong and effective NHRIS in the EU”.	Bruksela
41.	22.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	Bruksela
42.	22.02.2024 r.	Spotkanie Technologists Borders & Security Coffee Break.	online
43.	23.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
44.	27-28.02,2024 r.	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	Bruksela
45.	28.02.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
46.	28.02-1.03.2024 r.	Konferencja Grupy Państw Europy Środkowej i Wschodniej - CEEDPA	Tbilisi
47.	29.02.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
48.	1.03.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
49.	4.03.2024 r.	Spotkanie CEF DPO (grupy EROD skoordynowanego działania w zakresie egzekwowania prawa dot. IOD).	online
50.	5.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
51.	5-6.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
52.	6.03.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
53.	7.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
54.	7.03.2024 r.	Workshop in the context of borders and security.	online
55.	11.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
56.	12.03.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
57.	12-13.03.2024 r.	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	online
58.	13.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
59.	14.03.2024 r.	91. Posiedzenie plenarne EROD.	online
60.	18.03.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
61.	19.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
62.	19-20.03.2024 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC).	Bruksela
63.	20.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	Bruksela
64.	20.03.2024 r.	Wspólne spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C) i Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
65.	21.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	Bruksela
66.	21.03.2024 r.	Wspólne spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) i Europejskiej Rady Ochrony Danych.	online
67.	21.03.2024 r.	Wspólne spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
68.	22.03.2024 r.	Spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C).	online
69.	22.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
70.	23.03.2024 r.	Spotkanie Grupy Ekspertów Wspierających EROD (Support Pool of Experts – SPE).	online
71.	25-26.03.2024 r.	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	Bruksela
72.	27.03.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
73.	27.03.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
74.	2-3.04.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
75.	8-10.04.2024 r.	Warsztaty Podgrupy eksperckiej ITS EROD dot. wiążących reguł korporacyjnych.	Wilno

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
76.	9.04.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
77.	10.04.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
78.	10.04.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
79.	11.04.2024 r.	Spotkanie Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup – CEH) Europejskiej Rady Ochrony Danych.	online
80.	12.04.2024 r.	Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
81.	15.04.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
82.	15-16.04.2024 r.	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	Bruksela
83.	16-17.04.2024 r.	92. Posiedzenie plenarne EROD.	online
84.	17.04.2025 r.	Spotkanie Grupy zadaniowej ds. ChatGPT.	online
85.	18.04.2024 r.	Spotkanie ad hoc Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup – CEH) Europejskiej Rady Ochrony Danych.	online
86.	18.04.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
87.	22.04.2024 r.	Spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
88.	23.04.2024 r.	Spotkanie ad hoc Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
89.	24.04.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	Bruksela
90.	24.04.2024 r.	Spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C).	online
91.	24.04.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
92.	29.04.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
93.	29.04.2024 r.	Grupa zadaniowa ds. Bannerów Cookie (TF Cookie Banner)	online
94.	2.05.2024 r.	Wspólne spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych	online
95.	7.05.2024 r.	Spotkanie ad hoc Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
		and Health Expert Subgroup – CEH) Europejskiej Rady Ochrony Danych.	
96.	14.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	Bruksela
97.	14-16.05.2024 r.	Wiosenna Konferencja Europejskich Organów Ochrony Danych (Spring Conference of European Data Protection Authorities). Organizator: Krajowy Inspektorat Ochrony Danych Łotwy.	Ryga
98.	14-15.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG) Europejskiej Rady Ochrony Danych.	online
99.	14.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	Bruksela
100.	15.05.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
101.	15.05.2024 r.	Spotkanie Grupy roboczej ds. ETIAS w ramach Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC).	online
102.	16.05.2024 r.	Grupa zadaniowa ds. wzajemnego oddziaływania prawa ochrony danych, prawa ochrony konkurencji i konsumentów (TF C&C).	online
103.	21.05.2024 r.	Spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
104.	21.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	Bruksela
105.	21.05.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
106.	21.05.2024 r.	Spotkanie pt. „Okrągły stół OECD w sprawie wtórnego wykorzystania danych dotyczących zdrowia dla celów badawczych i związanych ze zdrowiem celów interesu publicznego”.	online
107.	21.05.2024 r.	Spotkanie Grupy roboczej ds. ETIAS w ramach Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC).	Bruksela
108.	22.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
109.	22.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
110.	22.05.2024 r.	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	Bruksela
111.	23-24.05.2024 r.	Konferencja CPDP 2024.	Bruksela
112.	24.05.2024 r.	Conference: „Risk and Compliance in the Age of AI”.	Zagrzeb
113.	26.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
114.	27.05.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
115.	28.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
116.	28.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	online
117.	29.05.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
118.	29.05.2024 r.	Posiedzenie Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee).	online
119.	5-7.06.2024 r.	46. Posiedzenie plenarne Komitetu T-PD.	Strasburg
120.	10.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
121.	11.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
122.	11.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
123.	11.06.2024 r.	Spotkanie DPC Supervision Unit.	online
124.	12.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
125.	13.06.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
126.	14.06.2024 r.	Wspólne spotkanie podgrup: SAESG, ENF, COOP, KEYP. Update from the IE SA concerning Meta Platforms Ireland.	online
127.	17-19.06.2024 r.	73 rd International Working Group on Data Protection in Technology, Berlin Group Meeting.	Oslo
128.	18-19.06.2024 r.	94. Posiedzenie plenarne EROD.	Bruksela
129.	19.06.2024 r.	Spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C).	online
130.	19.06.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
131.	20.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
132.	20.06.2024 r.	European Data Protection Summit: „Rethinking Data in a Democratic Society". Organizator: EDPS.	Bruksela
133.	21.06.2024 r.	Posiedzenie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access)	online
134.	25.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
135.	26.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych. DPO Guidelines meeting.	online
136.	26.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
		and Health – CEH) Europejskiej Rady Ochrony Danych.	
137.	27.06.2024 r.	Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
138.	28.06.2024 r.	Spotkanie punktów kontaktowych Grupy Ekspertów Wspierających EROD (Support Pool of Experts – SPE).	online
139.	1.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych.	online
140.	2-4.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
141.	1.07.2024 r.	Spotkanie Grupy Ekspertów Wspierających EROD (Support Pool of Experts – SPE).	online
142.	1.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
143.	2-3.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
144.	2-3.07.2024 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC).	Bruksela
145.	3-4.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
146.	4.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	Bruksela
147.	4.07.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
148.	4.07.2024 r.	Wspólne Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP), Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) i Podgrupy Doradczej ds. Strategii (Strategic Advisory Expert Subgroup – SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
149.	10.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
150.	11.07.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
151.	11.07.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
152.	16.07.2024 r.	95. Posiedzenie plenarne EROD.	online
153.	18.07.2024 r.	Spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
154.	19.07.2024 r.	Spotkanie Podgrupy ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
155.	21-23.07.2024 r.	Posiedzenie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX.	Bruksela
156.	22.07.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
157.	2-5.09.2024 r.	ENISA Annual Privacy Forum 2024 & Internet Privacy Engineering Network.	Karlstad
158.	9.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
159.	9-11.09.2024 r.	Spotkanie Grupy roboczej Rady UE ds. Wymiany Informacji i Ochrony Danych – DAPIX oraz spotkanie z Prezydencją Węgierską.	Bruksela
160.	9-11.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
161.	9-12.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	Bruksela
162.	11.09.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
163.	12.09.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
164.	16.09.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	Bruksela
165.	17.09.2024 r.	96. Posiedzenie plenarne EROD.	online
166.	17-19.09.2024 r.	Obóz szkoleniowy EROD dot. audytu aplikacji mobilnych(EDPB bootcamp on Mobile Apps Auditing)	Bruksela
167.	18.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	zdalnie
168.	10-11.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
169.	19.09.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
170.	23-25.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	Bruksela
171.	24-27.09.2024 r.	10th Trust Services and eID Forum.	Heraklion
172.	25.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
173.	25.09.2024 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru nad CIS (Coordinated Supervision Committee - CSC).	online
174.	26.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	Bruksela
175.	26.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	online
176.	27.09.2024 r.	Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
177.	30.09-1.10.2024 r.	High-Level Policy Dialogue on Data Governance.	Montevideo
178.	27.09.2024 r.	Spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C).	online
179.	4.10.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
180.	7-8.10.2024 r.	97. Posiedzenie plenarne EROD.	online
181.	8-9.10.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
182.	10.10.2024 r.	Konferencja „Sygnaliści x RODO" Organizator: Lubasz i Wspólnicy. Kancelaria Radców Prawnych.	online
183.	11.10.2024 r.	LeADS Final Conference „Legally Compliant Data – Driven Society".	Pisa
184.	14.10.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
185.	14.10.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
186.	22.10.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
187.	22.10.2024 r.	Spotkanie Podgrupy Ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
188.	23.10.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
189.	24.10.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
190.	30.10.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
191.	4.11.2024 r.	98. Posiedzenie plenarne EROD.	online
192.	4-6.11.2024 r.	47. Posiedzenie plenarne Komitetu T-PD.	Strasburg
193.	5-6.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
194.	5.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
195.	6.11.2024 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru nad CIS (Coordinated Supervision Committee - CSC).	online
196.	6.11.2024 r.	Spotkanie Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup – CEH) Europejskiej Rady Ochrony Danych.	online
197.	6.11.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
198.	7.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE).	online
199.	7.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
200.	8.11.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
201.	10-15.11.2024 r.	Ewaluacja Schengen.	Praga
202.	13.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
203.	15.11.2024 r.	Posiedzenie Grupy Ekspertów Wspierających EROD (Support Pool of Experts – SPE).	online
204.	17-19.11.2024 r.	74 rd International Working Group on Data Protection in Technology, Berlin Group Meeting oraz spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup – CEH) Europejskiej Rady Ochrony Danych.	Bruksela
205.	19.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online
206.	19.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	Bruksela
207.	20.11.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
208.	20-22.11.2024 r.	Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	Bruksela
209.	25.11.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
210.	25.11.2024 r.	Spotkanie ze studentami w ramach Advanced Master on Privacy, Cybersecurity and Data Management.	Maastricht
211.	27.11.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
212.	27-29.11.2024 r.	Warsztaty Podgrupy TECH: Best Practices GDPR Supervision of Algorithms and AI.	Haga
213.	2.12.2024 r.	Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
214.	2-3.12.2024 r.	99. Posiedzenie plenarne EROD.	online
215.	3-4.12.2024 r.	Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	
216.	4.12.2024 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
217.	4-5.12.2024 r.	Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
218.	4-6.12.2024 r.	Warsztaty rozpatrywania spraw (Case Handing Workshop).	Tallinn
219.	6.12.2024 r.	Spotkanie Grupy zadaniowej ds. wzajemnego oddziaływania ochrony danych, ochrony konkurencji i konsumentów (TF C&C).	online
220.	9.12.2024 r.	Szkolenie kościelnych inspektorów ochrony danych. Organizatorzy: Kościelny Inspektor Ochrony Danych przy Konferencji Episkopatu Polski i Instytut „Bona Fama”.	Warszawa
221.	9.12.2024 r.	Spotkanie Grupy zadaniowej ds. administracyjnych kar pieniężnych (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
222.	9-12.12.2024 r.	Wspólne posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych, Komitetu Skoordynowanego Nadzoru oraz Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac.	Bruksela
223.	11.12.2024 r.	Spotkanie Grupy zadaniowej ds. ChatGPT	online
224.	12.12.2024 r.	Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online

Lp.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
225.	13.12.2024 r.	Spotkanie Grupy EROD skoordynowanego działania w zakresie prawa dostępu (CEF Right of Access).	online
226.	16.12.2024 r.	Grupa zadaniowa ds. działalności międzynarodowej Europejskiej Rady Ochrony Danych (Task Force on International Engagement (TF INT).	online
227.	17.12.2024 r.	Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
228.	17.12.2024 r.	100. Posiedzenie plenarne EROD.	online
229.	19.12.2024 r.	Spotkanie Podgrupy Ekspertów ds. (Financial Matters Expert Subgroup – FMES) Europejskiej Rady Ochrony Danych.	online

Załącznik nr 5: Działalność Urzędu Ochrony Danych Osobowych w 2024 r. w liczbach

		2024 r.
1. DECYZJE	**skargowe**	1670
	karowe	22
	dot. naruszeń	20
	dot. kontroli	7
	OGÓŁEM	**1719**
2. SKARGI	**liczba skarg krajowych, które wpłynęły do UODO**	8056
	liczba zakończonych postępowań skargowych OGÓŁEM	6179 (DS) + 27 (DKN) = 6206
Liczba skarg z podziałem na sektory:	**prywatny**	3294
	finansowy, ubezpieczeń i telekomunikacji	1532
	zdrowia, zatrudnienia i szkolnictwa	1679
	publiczny	1551
	skargi o charakterze transgranicznym	184
3. NARUSZENIA	**liczba zgłoszeń naruszeń**	14842
4. ADMINISTRACYJNE KARY PIENIĘŻNE	**liczba administracyjnych kar pieniężnych nałożonych przez Prezesa UODO**	27
	liczba decyzji dot. kar pieniężnych	22
	łączna kwota kar w zł	13 907 740,96
5. KONTROLE	**liczba skontrolowanych podmiotów**	50
	liczba sprawdzeń stosowania przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	20
6. PROJEKTY AKTÓW PRAWNYCH	**liczba zaopiniowanych projektów aktów prawnych**	779
7. Uprzednie konsultacje	**liczba wniosków o uprzednie konsultacje**	2
8. Kodeksy postępowania	**liczba zatwierdzonych kodeksów postępowania**	0
9. Akredytacja	**liczba wniosków o akredytację podmiotów monitorujących kodeksy postępowania**	0
10. Certyfikacja	**liczba wniosków o zatwierdzenie kryteriów certyfikacji**	0
11. PYTANIA dotyczące WYKŁADNI PRAWA	**liczba pytań prawnych od administratorów i osób fizycznych**	1920

		2024 r.
	liczba pytań od IOD	233
	liczba pytań od organów nadzorczych z innych państw	61
	liczba pytań ogółem	2214
12. WNIOSKI PREJUDYCJALNE	**liczba wniosków prejudycjalnych skierowanych do TSUE przez sądy z różnych państw UE, które wpłynęły do polskiego organu nadzorczego**	61
13. WYSTĄPIENIA	**DOL**	11 (DOL) + 3 (DKN)
14. Zawiadomienia o podejrzeniu popełnienia przestępstwa		1 (DKN)
15. SPRAWY PRZED SĄDAMI ADMINISTRACYJNYMI	**liczba decyzji Prezesa UODO zaskarżonych do WSA w Warszawie OGÓŁEM**	168 (DS) + 3 (DKN) = **171**
	liczba decyzji zaskarżonych do NSA	69
	Liczba wyroków uchylających decyzję Prezesa UODO	53
	liczba wyroków utrzymujących w mocy decyzje Prezesa UODO	183