# SPRAWOZDANIE Z DZIAŁALNOŚCI
# PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
# w ROKU 2025

Sprawozdanie stanowi wykonanie art. 59 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[1].

[1] Sprawozdanie obejmuje działalność Prezesa Urzędu Ochrony Danych Osobowych w okresie od 1 stycznia 2025 r. do 31 grudnia 2025 r.

Zgodnie z art. 59 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2] każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i środków podjętych zgodnie z art. 58 ust. 2 RODO. Sprawozdania te są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem państwa członkowskiego, a także opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych[3]. Powołany przepis jest uzupełniony przez art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[4], w myśl którego Prezes Urzędu Ochrony Danych Osobowych[5] raz w roku, do 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 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z 2016 r. str. 1 ze zm., dalej: „RODO" lub „ogólne rozporządzenie o ochronie danych".
[3] Dalej także jako: „EROD".
[4] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.), dalej: „ustawa o ochronie danych osobowych".
[5] Dalej także jako: „Prezes UODO".

# Spis treści


**I. WPROWADZENIE ..... 7**

*1. ŹRÓDŁA PRAWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH ..... 7*
*2. URZĄD OCHRONY DANYCH OSOBOWYCH ..... 8*
*2.1. Budżet UODO za 2025 r. ..... 8*
*2.2. Pracownicy UODO ..... 9*
*2.3. Struktura organizacyjna ..... 10*
*2.4. Zadania jednostek organizacyjnych UODO ..... 12*

**II. OCHRONA DANYCH OSOBOWYCH OBYWATELI ..... 16**

*1. WYDAWANIE DECYZJI ADMINISTRACYJNYCH ..... 16*
*2. ROZPATRYWANIE SKARG ..... 17*
*3. WSTĘPNA WERYFIKACJA SPRAW SKARGOWYCH ..... 17*
*4. POSTANOWIENIA O ODMOWIE WSZCZĘCIA POSTĘPOWANIA ..... 18*
*5. SKARGI I DECYZJE SKARGOWE ..... 21*
*5.1. Sektor publiczny ..... 22*
*5.2. Sektor prywatny ..... 29*
*5.3. Sektor finansów, ubezpieczeń i telekomunikacji ..... 36*
*5.4. Sektor zdrowia, zatrudnienia i szkolnictwa ..... 52*
*5.5. Skargi na przewlekłość w sprawach skargowych ..... 56*
*6. NARUSZENIA OCHRONY DANYCH OSOBOWYCH ..... 57*
*6.1. Wstępna kontrola naruszeń ochrony danych osobowych ..... 58*
*6.2. Najczęściej zgłaszane naruszenia ochrony danych osobowych ..... 59*
*6.3. Wstępna weryfikacja zgłoszonego naruszenia ochrony danych osobowych ..... 62*
*6.4. Współpraca z administratorami w związku z naruszeniami ..... 63*
*6.5. Statystyka naruszeń ochrony danych osobowych ..... 64*
*7. POSTĘPOWANIA ADMINISTRACYJNE W SPRAWIE NARUSZEŃ ..... 66*
*7.1. Decyzje administracyjne ..... 66*
*7.2. Administracyjne kary pieniężne w związku z naruszeniem ..... 66*
*7.3. Decyzje wydane w związku z kampanią wyborczą ..... 77*
*8. SYGNALIŚCI ..... 78*
*9. WSPÓŁPRACA Z INNYMI ORGANAMI W ZAKRESIE REAGOWANIA NA INCYDENTY BEZPIECZEŃSTWA I NARUSZENIA ..... 80*
*10. KONTROLA PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH ..... 81*
*10.1. Przetwarzanie wizerunków dzieci ..... 83*
*10.2. Dokumentowanie naruszeń ochrony danych osobowych ..... 83*
*10.3. Bezpieczeństwo danych osobowych pacjentów ..... 85*
*10.4. Przetwarzanie danych osobowych w Wielkoskalowych Systemach UE ..... 87*
*10.4.1. Wizowy System Informacyjny (VIS) ..... 87*
*10.4.2. Kontrola w Ministerstwie Rozwoju i Technologii w zakresie IMI ..... 88*
*10.4.3. Kontrola w Urzędzie do Spraw Cudzoziemców ..... 88*
*10.4.4. Wydział Konsularny i Polonii Ambasady RP w Rabacie ..... 88*
*10.4.5. Kontrola u Komendanta Głównego Straży Granicznej ..... 89*
*10.5. Kontrole w wyniku zgłoszonego naruszenia ..... 89*
*10.6. Wystąpienia o przeprowadzenie sprawdzeń ..... 92*
*11. ZAWIADOMIENIA O PODEJRZENIU POPEŁNIENIA PRZESTĘPSTWA ..... 93*
*12. ORZECZNICTWO SĄDÓW ADMINISTRACYJNYCH ..... 96*
*12.1. Orzecznictwo sądów administracyjnych dotyczące postanowień wydanych na etapie wstępnej kontroli skarg ..... 96*
*12.2. Orzecznictwo sądów administracyjnych w sprawach skargowych ..... 98*
*12.3. Przykłady innych wyroków utrzymujących w mocy decyzje Prezesa UODO ..... 110*
*13. EGZEKUCJA ADMINISTRACYJNA – ZAPEWNIENIE WYKONANIA DECYZJI ORGANU NADZORCZEGO ..... 114*
*13.1. Postępowania w zakresie egzekucji decyzji Prezesa UODO ..... 116*
*13.2. Egzekucja obowiązków o charakterze niepieniężnym ..... 119*
*13.3. Egzekucja należności pieniężnych ..... 120*
*14. ADMINISTRACYJNE KARY PIENIĘŻNE ..... 121*

14.1. Administracyjne kary pieniężne za brak współpracy z organem nadzorczym i za niezapewnienie dostępu do informacji niezbędnych do realizacji jego zadań ... 127
14.2. Administracyjne kary pieniężne jako środek naprawczy przymuszający do wykonania nakazu decyzji. ... 129
15. OPINIOWANIE PROJEKTÓW AKTÓW PRAWNYCH DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH ... 129
15.1. Uwzględnienie ochrony danych osobowych na etapie prac legislacyjnych ... 131
15.2. Ocena skutków dla ochrony danych osobowych w procesie legislacyjnym ... 135
15.3. Zasada zgodności z prawem (praworządności, legalności) ... 140
15.4. Rejestry publiczne i systemy teleinformatyczne ... 143
15.5. Role podmiotów w procesach przetwarzania danych osobowych ... 149
15.6. Zasady przetwarzania danych osobowych, dane szczególnych kategorii, PESEL ... 151
15.7. Postęp technologiczny a ochrona danych ... 157
15.8. Nowe kompetencje Prezesa UODO ... 172
15.9. Deregulacja ... 176
15.10. Podsumowanie ... 179
16. UPRZEDNIE KONSULTACJE ... 180
17. KODEKSY POSTĘPOWANIA I MONITOROWANIE ICH PRZESTRZEGANIA ... 183
17.1. Kodeksy postępowania zatwierdzone przez organ nadzorczy ... 185
17.2. Nowe wnioski o ztwierdzenie lub zmianę kodeksów postępowania ... 186
17.3. Postępowania prowadzone w 2025 r. w sprawie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone we wcześniejszych latach ... 186
17.4. Wspieranie branż w pracy nad kodeksami postępowania ... 187
17.5. Wspieranie branż planujących pracę nad kodeksami postępowania ... 188
17.6. Działania zachęcające do pracy nad kodeksami postępowania ... 189
17.7. Akredytacja podmiotów monitorujących kodeksy postępowania ... 190
17.8. Podsumowanie ... 192
18. PYTANIA DOTYCZĄCE WYKŁADNI PRAWA, WNIOSKI O DOSTĘP DO INFORMACJI ... 194
18.1. Pytania dotyczące wykładni prawa ... 194
18.2. Pytania od inspektorów ochrony danych ... 240
18.3. Zapytania innych organów nadzorczych ... 270
18.4. Wnioski o dostęp do informacji publicznej ... 272
18.5. Skargi na działanie UODO ... 274
19. WYSTĄPIENIA PREZESA UODO ... 274

**III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA ... 302**

1. DZIAŁALNOŚĆ EDUKACYJNA ... 303
1.1. Kampanie edukacyjne ... 303
1.2. Współpraca ze szkołami wyższymi ... 308
1.3. Współpraca UODO z ZUS ... 309
1.4. Społeczny Zespół Ekspertów przy Prezesie UODO ... 312
1.5. Grupa robocza ds. sztucznej inteligencji ... 313
1.6. Współpraca z kościołami i związkami wyznaniowymi ... 314
1.7. Szkolenia ... 315
1.8. Projekty, programy ... 319
1.9. Konkursy ... 329
1.10. Porozumienia o współpracy ... 331
1.11. Poradniki ... 335
1.12. Nagroda im. Michała Serzyckiego ... 335
1.13. Konferencje, seminaria, spotkania ... 336
1.14. UODO rusza w kraj ... 352
1.15. Terenowy punkt konsultacyjny w Rzeszowie ... 357
1.16. Cykl wykładów eksperckich ... 357
1.17. Pol'and'Rock Festiwal ... 359
2. DZIAŁALNOŚĆ INFORMACYJNA ... 359
2.1. Komunikaty ... 360
2.2. Social media ... 361
2.3. Multimedia ... 364
2.4. Biuletyn ... 364
2.5. Kontakty z mediami ... 364
2.6. Prosty język w skomplikowanych sprawach ... 366

*2.7. Infolinia UODO ... 367*

**IV. UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ OCHRONĄ DANYCH OSOBOWYCH ... 368**

*1. UDZIAŁ UODO W PRACACH EROD ... 368*
*2. WSPÓŁPRACA ORGANÓW I EGZEKWOWANIE PRAWA ... 371*
*3. UDZIAŁ PREZESA UODO W PRACACH NAD PAKIETAMI OMNIBUS ... 374*
*4. PLATFORMY Z CHIN ... 379*
*5. CERTYFIKACJA ... 379*
*6. INNE DZIAŁANIA W ZAKRESIE UREGULOWAŃ DOTYCZĄCYCH DANYCH ... 380*
*7. MONITOROWANIE ROZWOJU NOWYCH TECHNOLOGII ... 380*
*8. WARSZTATY ... 381*
*9. UDZIAŁ UODO W PRACACH ORGANÓW I ORGANIZACJI MIĘDZYNARODOWYCH ... 382*
*9.1. Komitet Konsultacyjny Konwencji nr 108 ... 382*
*9.2. Global Privacy Assembly - GPA ... 382*
*9.3. Grupa Berlińska ... 383*
*9.4. Postępowania transgraniczne ... 384*
*9.5. Współpraca w ramach IMI ... 385*
*9.6. Data Protection Framework ... 386*
*9.7. Rozporządzenie proceduralne ... 387*
*10. MIĘDZYNARODOWE KONFERENCJE, SEMINARIA I SPOTKANIA ... 387*
*11. SKOORDYNOWANY NADZÓR NAD WIELKOSKALOWYMI SYSTEMAMI INFORMACYJNYMI UE ... 395*
*12. WNIOSKI PREJUDYCJALNE ... 399*
*13. OCHRONA DANYCH OSOBOWYCH PRZED SĄDAMI CYWILNYMI ... 412*

**V. WNIOSKI WYNIKAJĄCE ZE STANU PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH ... 416**

**VI. PODSUMOWANIE ... 455**

**ZAŁĄCZNIKI ... 461**

*ZAŁĄCZNIK NR 1:*
*Wykaz administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2025 r. ... 461*
*ZAŁĄCZNIK NR 2:*
*Wykaz wydarzeń objętych patronatem Prezesa UODO w 2025 r. ... 463*
*ZAŁĄCZNIK NR 3:*
*Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2025 r. W Polsce przez UODO lub inne podmioty ... 466*
*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 2025 r. ... 475*
*ZAŁĄCZNIK NR 5:*
*Działalność Urzędu Ochrony Danych Osobowych w 2025 r. w liczbach ... 490*



*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 2025. 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 2025 r. minęło siedem 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 2025, w tym w szczególności zgłaszanych skarg, pytań o wykładnię prawa 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 2025, które jest nie tylko informacją o działalności polskiego organu nadzorczego zawierającą wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych, ale przedstawia również 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 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych oraz wydane na jej podstawie akty wykonawcze,
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[9],
- ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[10] oraz wydane na jej podstawie akty wykonawcze.

W związku z uchwalaniem nowych przepisów prawa unijnego i krajowego, kompetencje Prezesa UODO są sukcesywnie rozbudowywane (także w zakresie danych nieosobowych). Zostały one określone w takich aktach prawnych, jak:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniającego rozporządzenie (UE) 2018/1724,
- ustawa z dnia 27 marca 2026 r. o zarządzaniu danymi,

[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 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 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.

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/900 z dnia 13 marca 2024 r. w sprawie przejrzystości i targetowania reklamy politycznej (trwa proces legislacyjny zainicjowany przez komisję senacką),
- ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 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),
- Ustawa z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji.

## 2. Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych zapewnia wykonanie zadań wynikających z kompetencji Prezesa UODO określonych w RODO i w ustawie z dnia 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.

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. Budżet UODO za 2025 r.

**Plan finansowy UODO w 2025 r. przedstawiał się następująco:**

- wynagrodzenia 40 896 000 zł
- pochodne od wynagrodzeń 7 571 000 zł
- wydatki majątkowe 2 750 000 zł
- pozostałe wydatki 15 108 000 zł

**Wydatki zrealizowane przez UODO w 2025 r.:**

- wynagrodzenia 40 895 548,31 zł
- pochodne od wynagrodzeń 7 442 856,61 zł
- wydatki majątkowe 2 686 546,70 zł
- pozostałe wydatki 13 971 531,93 zł

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 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".

## 2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2025 r. (nie wliczając Prezesa UODO i jego dwóch zastępców) wynosił 268,95 etatu (tj. 275 osób). Natomiast zatrudnienie w UODO na dzień 31 grudnia 2025 r. wynosiło 294,78 etatu (tj. 301 osób). Wzrost ten wynika z nowych zadań nałożonych prawem na Prezesa Urzędu (wynikających m.in. z przepisów o zarządzaniu danymi), a także znaczącym wzrostem otrzymywanych skarg oraz zgłoszeń naruszeń ochrony danych, których ilość wskazuje na dalsze potrzeby Urzędu w tym zakresie. Szczegółowe informacje odnośnie do tych zagadnień zawiera dalsza część sprawozdania.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2025 r. (bez Prezesa UODO i jego zastępców) przedstawiała się następująco:

1) Departament Wstępnej Kontroli Skarg i Naruszeń – 32 osoby (32,0 etaty), z pracownikami infolinii włącznie, w tym:
   - Wydział Wstępnej Kontroli Skarg – 15 osób (15 etatów),
   - Wydział Wstępnej Kontroli Naruszeń – 7 osób (7 etatów);
2) Departament Skarg – 67 osób (66,05 etatu), w tym:
   - Wydział ds. Sektora Publicznego – 16 osób (16 etatów),
   - Wydział ds. Sektora Prywatnego – 18 osób (17,5 etatu),
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 12 osób (12 etatów),
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 14 osób (13,75 etatu);
3) Departament Prawa i Nowych Technologii – 34 osoby (33,4 etatu), w tym:
   - Wydział Legislacji – 13 osób (13,0 etatów),
   - Wydział Współpracy z Inspektorami Ochrony Danych – 4 osoby (4,0 etaty),
   - Wydział Kodeksów i Analiz – 9 osób (9,0 etatów);
4) Departament Kontroli i Naruszeń – 42 osoby (41,5 etatu), w tym:
   - Wydział Kontroli – 8 osób (8,0 etatów),
   - Wydział Naruszeń – 10 osób (9,5 etatu),
   - Wydział Postępowań Administracyjnych – 12 osób (12,0 etatów),
   - Wydział Wsparcia Informatycznego – 6 osób (6,0 etatów);
5) Departament Kar i Egzekucji – 12 osób (12,0 etatów);
6) Departament Komunikacji Społecznej – 10 osób (9,4 etatu);
7) Departament Inicjatyw Edukacyjnych – 10 osób (9,8 etatu);
8) Departament Współpracy Międzynarodowej – 17 osób (17.0 etatów), w tym:
   - Wydział ds. Postępowań Transgranicznych – 5 osób (5 etatów);
9) Departament Projektów Społecznych i Zrównoważonego Rozwoju – 5 osób (4,33 etatu);
10) Departament Informatyki i Cyberbezpieczeństwa – 12 osób (11,42 etatu);
11) Departament Innowacyjności i Zarządzania Danymi – 7 osób (6,8 etatu);
12) Departament Finansów i Kadr – 11 osób (11,0 etatów);
13) Zespół Radców Prawnych – 3 osoby (3 etaty);

14) Departament Organizacyjno-Administracyjny – 33 osoby (31,25 etatu);
15) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,33 etatu);
16) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba (1,0 etat);
17) Główny koordynator ds. wielkoskalowych systemów informacyjnych UE – 1 osoba (1,0 etat);
18) Główny koordynator ds. ochrony danych osobowych w kościołach i związkach wyznaniowych – 1 osoba (1,0 etat);
19) Dział Audytu Wewnętrznego – 1 osoba (0,5 etatu)
20) Dyrektor UODO – 1 osoba (1,0 etat).

Liczba pracowników zatrudnionych na stanowiskach merytorycznych i na stanowiskach pomocniczych według stanu na 31 grudnia 2025 r. (bez Prezesa UODO i jego zastępców):

- stanowiska merytoryczne – 265 osób,
- stanowiska pomocnicze – 36 osób.

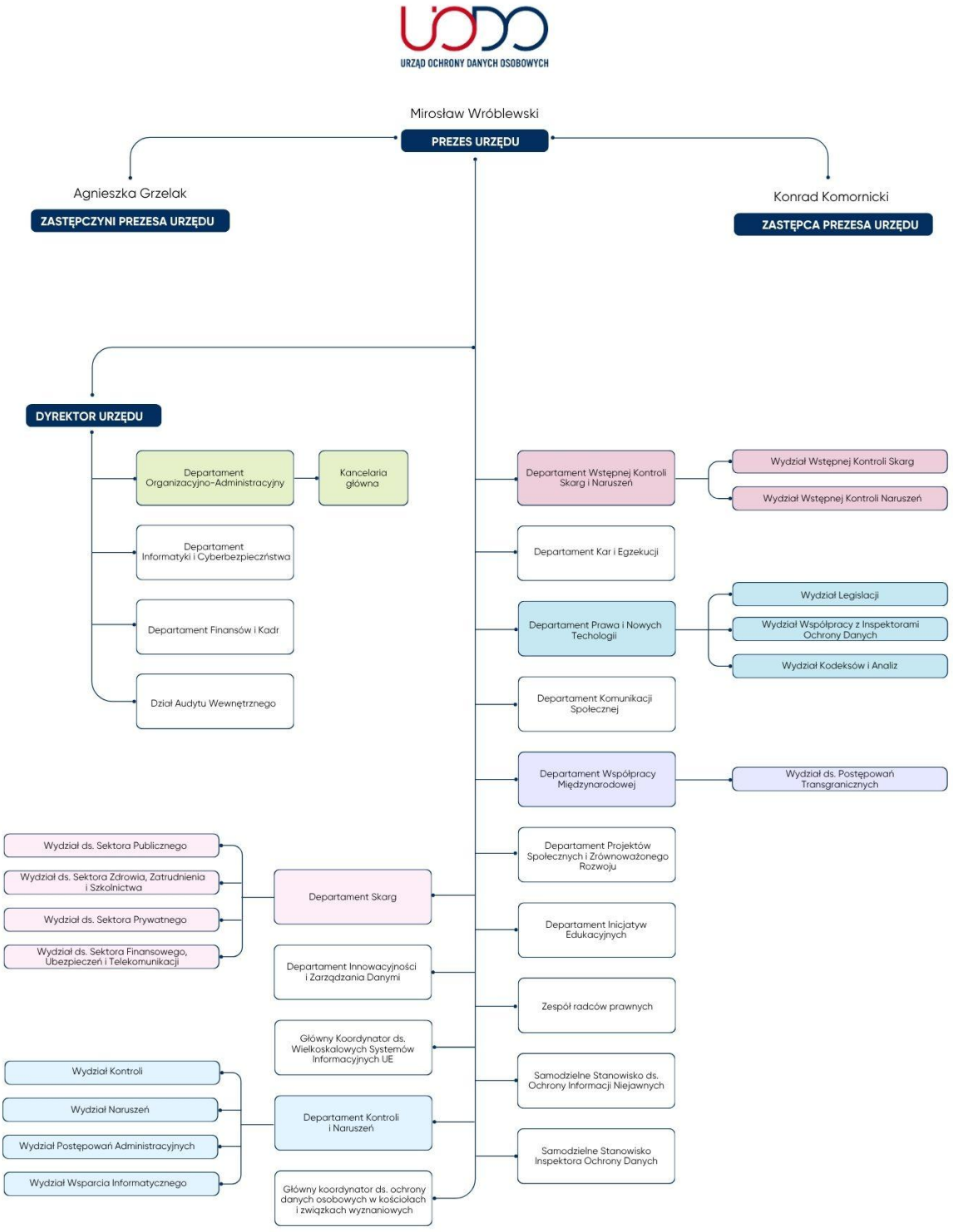
Liczba pracowników posiadających wykształcenie wyższe oraz wykształcenie wyższe prawnicze (stan na 31 grudnia 2025 r.):

- wykształcenie wyższe ogółem – 273 osoby,
- w tym wykształcenie wyższe prawnicze – 163 osób.

### 2.3. Struktura organizacyjna

W strukturze Urzędu działa 19 komórek organizacyjnych, z czego w pięciu z nich wyodrębnione zostały wydziały, które zajmują się sprawami z określonych sektorów. W Departamencie Prawa i Nowych Technologii działają trzy wydziały: Wydział Legislacji, Wydział Współpracy z Inspektorami Ochrony Danych oraz Wydział Kodeksów i Analiz. W Departamencie Kontroli i Naruszeń znajduje się Wydział Kontroli, Wydział Naruszeń, Wydział Postępowań Administracyjnych oraz Wydział Wsparcia Informatycznego, zaś w Departamencie Wstępnej Kontroli Skarg i Naruszeń – Wydział Wstępnej Kontroli Skarg oraz Wydział Wstępnej Kontroli Naruszeń. Z kolei w Departamencie Skarg funkcjonują 4 wydziały: Wydział ds. Sektora Publicznego, Wydział ds. Sektora Prywatnego, Wydział ds. Zdrowia, Zatrudnienia i Szkolnictwa oraz Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji, natomiast w Departamencie Współpracy Międzynarodowej – Wydział ds. Postępowań Transgranicznych.

Strukturę organizacyjną Urzędu Ochrony Danych Osobowych przedstawia poniższa grafika.


URZĄD OCHRONY DANYCH OSOBOWYCH
Mirosław Wróblewski
PREZES URZĘDU
Agnieszka Grzelak
ZASTĘPCZYNI PREZESA URZĘDU
Konrad Komornicki
ZASTĘPCA PREZESA URZĘDU
DYREKTOR URZĘDU
Departament Organizacyjno-Administracyjny
Kancelaria główna
Departament Informatyki i Cyberbezpieczeństwa
Departament Finansów i Kadr
Dział Audytu Wewnętrznego
Departament Wstępnej Kontroli Skarg i Naruszeń
Wydział Wstępnej Kontroli Skarg
Wydział Wstępnej Kontroli Naruszeń
Departament Kar i Egzekucji
Departament Prawa i Nowych Techologii
Wydział Legislacji
Wydział Współpracy z Inspektorami Ochrony Danych
Wydział Kodeksów i Analiz
Departament Komunikacji Społecznej
Departament Współpracy Międzynarodowej
Wydział ds. Postępowań Transgranicznych
Departament Projektów Społecznych i Zrównoważonego Rozwoju
Departament Inicjatyw Edukacyjnych
Zespół radców prawnych
Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych
Samodzielne Stanowisko Inspektora Ochrony Danych
Wydział ds. Sektora Publicznego
Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa
Wydział ds. Sektora Prywatnego
Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji
Departament Skarg
Departament Innowacyjności i Zarządzania Danymi
Główny Koordynator ds. Wielkoskalowych Systemów Informacyjnych UE
Wydział Kontroli
Wydział Naruszeń
Wydział Postępowań Administracyjnych
Wydział Wsparcia Informatycznego
Departament Kontroli i Naruszeń
Główny koordynator ds. ochrony danych osobowych w kościołach i związkach wyznaniowych

## 2.4. Zadania jednostek organizacyjnych UODO

Do zadań jednostek organizacyjnych Urzędu Ochrony Danych Osobowych należy w szczególności: rozpatrywanie skarg w sprawach dotyczących przestrzegania 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 może być konieczne nałożenie administracyjnej kary pieniężnej.

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.

W perspektywie nowych zadań Prezesa UODO wynikających m.in. z przepisów unijnego aktu w sprawie zarządzania danymi (DGA), zaobserwowanych potrzeb związku z obsługą skarg i naruszeń ochrony danych osobowych, współpracy międzynarodowej w ramach skoordynowanego nadzoru, zmieniającego się otoczenia w związku z rozwojem nowoczesnych technologii i koniecznością wsparcia ze strony organu, wybrane jednostki organizacyjne Urzędu poddano reorganizacji, a także utworzono nowe jednostki, których powstanie przyczynić się ma do sprawnego, niezakłóconego wykonywania zadań Prezesa UODO[12]:

1) Departament Innowacji i Zarządzania Danymi (DIZD),
2) Departament Projektów Społeczecznych i Zrównoważonego Rozwoju (DPSZR),
3) Departament Wstępnej Kontroli Skarg i Naruszeń (DWKSN),
4) Główny koordynator ds. Wielkoskalowych Systemów Informacyjnych UE,
5) Główny koordynator ds. ochrony danych osobowych w kościołach i związkach wyznaniowych.

### **2.4.1.** Departament Innowacji i Zarządzania Danymi (DIZD)

W 2025 r. trwały prace na projektem ustawy o zarządzaniu danymi, której celem było wdrożenie do polskiego porządku prawnego unijnego Aktu w sprawie zarządzania danymi (DGA)[13]. Projektowane przepisy przyznawały Prezesowi UODO kompetencje organu właściwego do spraw pośrednictwa danych i rejestracji organizacji altruizmu danych oraz kompetencje dotyczące przekazywania danych nieosobowych do państw trzecich. Aby zapewnić właściwe wykonywanie ww. zadań, utworzono Departament Innowacji i Zarządzania Danymi, składający się ze specjalistów odpowiedzialnych za przygotowanie Urzędu do realizacji zadań wynikających z DGA, którzy jeszcze przed wejściem w życie ustawy aktywnie realizowali zadania przygotowawcze związane z wykonywaniem nowych kompetencji Prezesa UODO. Były to głównie działania informacyjne mające na celu zwiększanie świadomości dotyczącej nowych regulacji oraz kompetencji Prezesa UODO wynikających z DGA, w ramach których odbywały się tematyczne webinaria, konferencja naukowa oraz przygotowano cykl artykułów „DGA w pigułce” publikowanych w Biuletynie UODO.

### **2.4.2.** Departament Projektów Społecznych i Zrównoważonego Rozwoju (DPSZR)

Departament Projektów Społecznych i Zrównoważonego Rozwoju jest jednostką odpowiedzialną za inicjowanie, koordynowanie oraz wdrażanie działań o charakterze społecznym i rozwojowym w obszarze ochrony danych osobowych oraz wyzwań wynikających z dynamicznych zmian technologicznych, w szczególności związanych z wdrażaniem narzędzi opartych na sztucznej inteligencji. Przygotowane przez

[12] Zarządzenie nr 9/2025 Prezesa UODO z dnia 12 marca 2025 r.

[13] Przepisy krajowe uzupełniające regulację unijną w zakresie instytycjonalnym, organizacyjnym, proceduralnym oraz nakładania kar za naruszenia wynikające z DGA, zostały wprowadzone ustawą z dnia 27 marca 2026 r. o zarządzaniu danymi (Dz. U. z 2026 r. poz. 548), która weszła w życie 23 lipca 2026 roku.

departament analizy, rekomendacje czy rozwiązania mają wspierać procesy decyzyjne kierownictwa, służyć identyfikowaniu zagrożeń, inicjowaniu działań prewencyjnych oraz koordynowaniu przedsięwzięć odpowiadających na aktualne potrzeby. Departament ten koordynuje także realizację przez Urząd wielofunkcyjnego programu „UODO rusza w kraj".

### **2.4.3.** Departament Wstępnej Kontroli Skarg i Naruszeń (DWKSN)

Departament Wstępnej Kontroli Skarg i Naruszeń (DWKSN) rozpoczął działalność 1.01.2025 r.[14] W jego ramach utworzono Wydziały Wstępnej Kontroli Skarg i Wstępnej Kontroli Naruszeń. Do tej jednostki organizacyjnej Urzędu w pierwszej kolejności wpływają skargi i zgłoszenia naruszeń ochrony danych osobowych w celu ich weryfikacji pod kątem formalnym oraz oceny wagi problemu. Departament przejął także odpowiedzialność za prowadzenie infolinii Urzędu oraz przyjmowanie zgłoszeń zewnętrznych sygnalistów. Powstanie DWKSN było efektem zaobserwowanych potrzeb oraz zmieniającego się otoczenia Urzędu. Jego utworzenie pomogło lepiej, sprawniej, a przede wszystkim szybciej rozpatrywać skargi osób fizycznych na nieprawidłowości w przetwarzaniu ich danych osobowych oraz zgłaszane przez administratorów naruszenia ochrony danych. Teraz to Departament Wstępnej Kontroli Skarg i Naruszeń zajmuje się selekcją przypadków, które nie rodzą konieczności prowadzenia dalszego postępowania, dzięki czemu pozostałe departamenty prowadzące postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, mogą skupić się na tych sprawach, które wymagają kolejnych działań ze strony organu.

Nowe możliwości rozwoju zyskała też infolinia, która może w większym stopniu czerpać z doświadczeń pracowników rozpatrujących skargi i naruszenia oraz korzystać z ich wiedzy i zgłaszanych potrzeb.

Podstawowymi zadaniami departamentu są:

1) działania związane z uzupełnianiem braków formalnych wpływających do Urzędu skarg, a także wydawanie postanowień o odmowie wszczęcia postępowania w razie zaistnienia przesłanek uniemożliwiających rozpatrzenie skargi,
2) analizowanie zgłaszanych przez administratorów naruszeń ochrony danych osobowych pod kątem formalnym i oceny wagi problemu,
3) przyjmowanie zgłoszeń zewnętrznych sygnalistów i udzielanie im informacji zwrotnej,
4) prowadzenie infolinii Urzędu.

Wobec znacznego wzrostu liczby skarg Urząd przez cały rok 2025 wzmacniał stan osobowy **Wydziału Wstępnej Kontroli Skarg**. W styczniu i lutym w Wydziale tym zatrudnionych było 8 osób, w marcu – 9, w kwietniu – 10, w maju i czerwcu – 11,

[14] Na mocy zarządzenia Prezesa Urzędu Ochrony Danych Osobowych nr 36/2024 z dnia 19 grudnia 2024 r. w sprawie nadania statutu Urzędowi Ochrony Danych Osobowych.

w lipcu i sierpniu – 12, we wrześniu i październiku – 13, w listopadzie i grudniu – 14[15]. Do Wydziału trafiły 3 osoby nowozatrudnione w UODO, natomiast 4 przeszły z innych komórek organizacyjnych, w tym jedna po powrocie z urlopu macierzyńskiego. Nowi pracownicy wymagali odpowiedniego czasu na przeszkolenie i wdrożenie się w zakres powierzonych im obowiązków, ale istotnie wzmocnili skład osobowy Wydziału.

We wstępnej weryfikacji skarg pracowników Wydziału Wstępnej Kontroli Skarg wspierali pracownicy infolinii (5-6 osób).

### **2.4.4.** Główny koordynator ds. Wielkoskalowych Systemów Informacyjnych UE

Istotnym obszarem działalności Prezesa UODO jest współpraca międzynarodowa w ramach art. 62 rozporządzenia 2018/1725[16], która przewiduje skoordynowany nadzór mający zastosowanie w przypadku, gdy odpowiednie prawo Unii Europejskiej odnosi się do tego artykułu. W stukturze organizacyjnej Urzędu powstało więc stanowisko koordynatora ds. wielkoskalowych systemów informacyjnych UE, którego głównym zadaniem jest m.in. zapewnienie uczestnictwa UODO w skoordynowanym nadzorze nad wielkoskalowymi systemami informacyjnymi oraz nad organami, urzędami i agencjami Unii Europejskiej. Zadanie to jest wykonywane w uzgodnieniu z Prezesem UODO i w konsultacji z z komórkami organizacyjnymi Urzędu, w zakresie legislacji, skarg, kontroli, zgłaszanych naruszeń i współpracy międzynarodowej. Koordynator bierze udział w wyznaczonych przez Prezesa UODO kontrolach dotyczących przetwarzania danych osobowych w wielkoskalowych systemach informacyjnych, a także uczestniczy we wspólnych kontrolach EIOD. Ważnym zadaniem jest także opiniowanie rządowych instrukcji dla przedstawiciela RP na posiedzenia Grupy roboczej ds. Schengen, Komitetu Schengen i Rady Schengen.

### **2.4.5.** Główny koordynator ds. ochrony danych osobowych w kościołach i związkach wyznaniowych.

Współpraca Prezesa UODO z niezależnymi organami nadzorczymi powołanymi na podstawie art. 91 RODO legła u podstaw decyzji o utworzeniu w strukturze organizacyjnej Urzędu stanowiska koordynatora ds. ochrony danych osobowych w kościołach i związkach wyznaniowych. Jedym z głównych zadań koordynatora jest monitorowanie zgodności działań kościoła lub związku wyznaniowego z obowiązującymi przepisami dotyczącymi ochrony danych osobowych i współpraca z osobami odpowiedzialnym za przetwarzanie danych w tych podmiotach. Rolą koordynatora jest też inicjowanie wydarzeń, takich jak szkolenia, konferencje, warsztaty i innych działań edukacyjnych mających na celu podnoszenie świadomości

[15] Na koniec wskazanego miesiąca lub drugiego ze wskazanych miesięcy.

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 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. U. UE L z 2018 r. poz. 295.

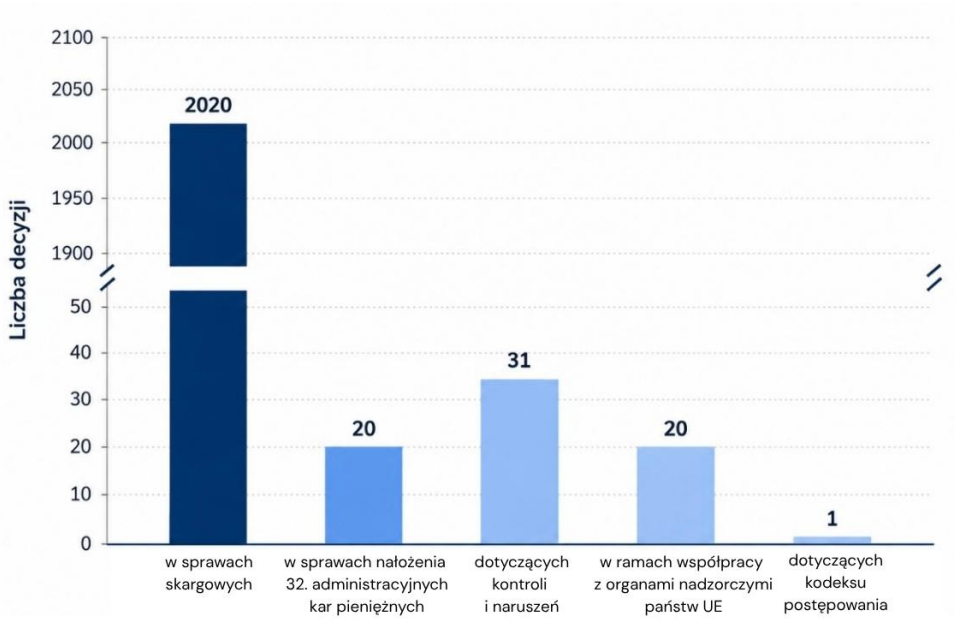
wśród duchowieństwa, pracowników i członków wspólnoty na temat obowiązków związanych z ochroną danych osobowych.

# II. OCHRONA DANYCH OSOBOWYCH OBYWATELI

## 1. Wydawanie decyzji administracyjnych

Postępowanie dotyczące naruszenia przepisów o ochronie danych osobowych, wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej, toczy się według przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, zgodnie z przepisami K.p.a. W przypadku stwierdzenia naruszenia przepisów prawa, postępowanie to może zakończyć się wydaniem **decyzji administracyjnej,** mocą której Prezes Urzędu Ochrony Danych Osobowych m.in.: umarza postępowanie, odmawia uwzględnienia wniosku skarżącego, nakazuje przywrócenie stanu zgodnego z prawem, nakłada karę, upomnienie albo ostrzeżenie na administratora czy podmiot przetwarzający. Pomimo autonomii proceduralnej państw członkowskich UE pewne kwestie proceduralne, zwłaszcza związane z postępowaniami transgranicznymi, zostały bezpośrednio uregulowane w RODO.

W okresie od 1 stycznia 2025 r. do 31 grudnia 2025 r. Prezes Urzędu Ochrony Danych Osobowych wydał ogółem **2092 decyzje administracyjne,** na które złożyło się: **2020** decyzji w indywidualnych sprawach skargowych,
**20** decyzji w sprawach nałożenia 32. administracyjnych kar pieniężnych,
**31** decyzji dotyczących kontroli i naruszeń,
**20** decyzji w ramach współpracy z organami nadzorczymi państw UE,
**1** decyzja dotycząca kodeksu postępowania.




**Wykres 1:** Liczba decyzji administracyjnych wydanych przez Prezesa UODO w 2025 r. z podziałem na sektory.

## 2. Rozpatrywanie skarg

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 jako organu nadzorczego. Wpływ skargi inicjuje postępowanie administracyjne, zmierzające do rozstrzygnięcia sprawy poprzez wydanie decyzji administracyjnej.

W okresie od 1 stycznia 2025 r. do 31 grudnia 2025 r. Prezes Urzędu Ochrony Danych Osobowych prowadził postępowania administracyjne wszczęte w wyniku skarg wniesionych zarówno w roku 2025, jak i w latach poprzednich, które toczyły się zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz na podstawie przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[17].

## 3. Wstępna weryfikacja spraw skargowych

Wstępna weryfikacja skarg i naruszeń wpływających do Prezesa Urzędu Ochrony Danych Osobowych jest zadaniem nowo powołanego do tego zadania Departamentu Wstępnej Kontroli Skarg i Naruszeń.

W 2025 r. do Prezesa UODO wpłynęło **12 827 skarg**[18], o których mowa w art. 77 rozporządzenia 2016/679. W przypadku zaledwie **1 121 (8,7 %)** skarg wstępna weryfikacja nie wykazała braków formalnych i sprawy te zostały od razu przekazane do Departamentu Skarg. Pozostała liczba **11 706 skarg (91,3%)** zawierała braki formalne.

Znacząca liczba 11 706 skarg przeznaczonych do uzupełnienia braków formalnych pokazuje nakład pracy, który Urząd musi wykonać, by wpływające skargi spełniały kryteria i warunki wyznaczone przepisami prawa. W niektórych przypadkach konieczne było jednak zakończenie postępowania bądź pozostawienie skargi bez rozpoznania. Działania te wyraźnie pokazują bardzo istotną rolę nowo powołanej jednostki organizacyjnej, jaką jest Departament Wstępnej Kontroli Skarg i Naruszeń (DWKSN).

[17] Dz. U. z 2025 r. poz. 1691, dalej: K.p.a.

[18] Liczba ta nie obejmuje skarg prowadzonych przez UODO w 2025 r. w ramach współpracy międzynarodowej z innymi organami krajowymi państw UE. W styczniu wpłynęło – 838 skarg, w lutym – 955, w marcu – 983, w kwietniu – 914, w maju – 1055, w czerwcu – 935, w lipcu – 1305, w sierpniu – 970, we wrześniu – 1007, w październiku – 1214, w listopadzie – 1246, w grudniu – 1405.

W ostatnim czasie widoczny jest znaczny wzrost zainteresowania interwencją Prezesa UODO w sprawach indywidualnych względem lat ubiegłych: w 2021 r. wpłynęło 8 318 skarg krajowych, w 2022 r. – 6 995, w 2023 r. – 6 962, w 2024 r. – 8 056, a w 2025 r. – aż 12 827 skarg. **W roku sprawozdawczym 2025 wpłynęło do Prezesa UODO aż 61% więcej skarg indywidualnych niż w 2024 r.** Odzwierciedla to zwiększenie świadomości osób, których dane dotyczą, co do przysługujących im uprawnień, a tym samym świadczy m.in. o skuteczności działalności edukacyjnej UODO i rosnącym zaufaniu społecznym do organu nadzorczego.

Najmniejszy miesięczny wpływ skarg w 2025 r. odnotowano w styczniu – 838. W maju liczba skarg przekroczyła 1 000, w lipcu – 1 300, natomiast w grudniu został odnotowany rekordowy wpływ – ponad 1 400 skarg krajowych.

Wydział Wstępnej Kontroli Skarg w DWKSN w 2025 r. zakończył 5 473 spraw, natomiast po uzupełnieniu braków formalnych 1769 spraw przekazał do Departamentu Skarg, a 286 do innych departamentów. Na 215 wydanych postanowień 196 dotyczyło odmowy wszczęcia postępowania, w 10 przypadkach, gdy realizacja żądań skarżących pozostawała w kompetencji sądów powszechnych – zwrotu skargi[19].

Porównując liczbę spraw załatwionych w Departamencie Skarg w 2024 r. (6176) z liczbą spraw załatwionych w Departamencie Skarg (2291) i Departamencie Wstępnej Kontroli Skarg i Naruszeń (5493) łącznie w 2025 r., **wzrost wydajności Urzędu w zakresie załatwiania spraw skargowych można ocenić na 25 procent**.

## 4. Postanowienia o odmowie wszczęcia postępowania

Tematyka wydawanych przez organ postanowień była różnorodna, a poniżej przedstawiono zagadnienia pojawiające się najczęściej – postanowienia o odmowie wszczęcia postępowania.

Postanowienia wydane przez organ dotyczyły m.in. odmowy wszczęcia postępowań w sytuacjach, w których skarżący zmierzali do nadużycia prawa do ochrony danych osobowych (np. gdy ich rzeczywistym celem było uzyskanie korzyści majątkowej od administratora danych). Znaczną część wydawanych postanowień stanowiły również odmowy wszczęcia postępowania ze względu na żądania skarżących wykraczające poza kompetencje Prezesa UODO, takie jak np. wnioski o nakazanie wypłaty odszkodowania lub zadośćuczynienia. Kolejną liczną grupą postanowień były dotyczące sytuacji przetwarzania danych osobowych w działalności prasowej oraz w celach osobistych, co do których stosowanie przepisów rozporządzenia 2016/679 zostało wyłączone. Organ odmawiał wszczęcia postępowania w odpowiedzi na skargi zawierające sprzeczne żądania, uniemożliwiające zastosowanie uprawnień naprawczych, skargi wystosowane przedwcześnie, a także w sytuacjach, kiedy do przetwarzania danych jeszcze nie doszło. Prezes UODO wydał także wiele postanowień o odmowie wszczęcia

[19] Ponadto wydano 2 postanowienia o połączeniu spraw, 6 w których wyłączono część akt do odrębnego postępowania, 1 odmawiające uzupełnienia postanowienia.

postępowań w odpowiedzi na żądania przeprowadzenia kontroli ogólnych praktyk administratorów danych.

Poniżej przedstawiono grupy tematyczne najczęściej wydawanych w 2025 r. postanowień o odmowie wszczęcia postępowania.

**Nadmierne żądania**

W 2025 r. organ nadzorczy wydał liczne postanowienia o odmowie wszczęcia postępowania w sprawach, w których żądania skarżących zmierzały do nadużycia prawa do ochrony danych osobowych[20], przykładowo do uzyskania określonej korzyści majątkowej[21] lub do nadmiernego obciążenia organu[22] poprzez mobilizację jego zasobów bez uzasadnionego powodu.

Sprawy te obejmowały m.in. przypadki uzależniania wycofania roszczeń wynikających z RODO wobec administratora od wypłaty przez niego określonej sumy pieniężnej na rzecz skarżącego. Należy w tym miejscu wskazać, że skarga składana do organu nadzorczego nie może służyć jako narzędzie do wymuszenia na administratorze działań, które nie wynikają z przepisów RODO. O nadużyciu prawa do ochrony danych osobowych i chęci sparaliżowania organu poprzez zarzucanie go wnioskami może świadczyć formułowanie w nich nadmiernie rozbudowanych i nieprecyzyjnych żądań utrudniających organowi ustalenie stanu faktycznego, częsta modyfikacja okoliczności sprawy czy składanie licznych wniosków dowodowych, szczególnie takich, które merytorycznie nie mają znaczenia dla sprawy, lecz są stale dosyłane, uniemożliwiając jej sprawne załatwienie.

Do stanowiska organu przychylał się Wojewódzki Sąd Administracyjny w Warszawie[23]. Nadużywanie prawa do ochrony danych osobowych powodowało ograniczenie innym podmiotom dostępu do skutecznego realizowania tego prawa przed organem nadzorczym.

**Żądanie dostępu do dokumentów zawierających dane osobowe lub żądanie udostępnienia nośników danych**

Prezes UODO odmawiał wszczęcia postępowania w sprawach skarg zawierających żądania odnoszące się do dokumentów lub nośników danych osobowych (np. nagrań z monitoringu wizyjnego[24]). Żądania te dotyczyły nakazania przez organ administratorowi udostępnienia oryginałów lub kopii[25] dokumentów, wglądu do nich czy ich zwrotu[26]. W kontekście tak sformułowanych żądań istotne było

[20] Art. 57 ust. 4 RODO.

[21] DWKSN.523.4099.2025, DWKSN.523.4544.2025, DWKSN.523.4708.2025, DWKSN.523.4709.2025, DWKSN.523.4710.2025, DWKSN.523.4180.2025, DWKSN.523.4181.2025.

[22] DWKSN.523.3115.2025, DWKSN.523.7493.2025.

[23] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 20 stycznia 2026 r. sygn. akt II SA/Wa 1464/25.

[24] DS.523.5712.2024.

[25] DWKSN.523.7192.2025.

[26] DWKSN.523.1603.2025.

to, że Prezes UODO może podejmować tylko te czynności, które znajdują się w zakresie jego uprawnień określonych m.in. w RODO[27]. Żaden przepis nie uprawnia Prezesa UODO do wydawania nakazów udostępnienia dokumentów, ani nie stanowi podstawy do żądania od administratora danych wydania dokumentów zawierających dane osobowe bądź kopii tych dokumentów, jako nośników danych. Uprawnienie osoby wynikające z RODO[28] odnosi się wyłącznie do uzyskania kopii danych osobowych, a nie ich nośników.

**Przetwarzanie danych osobowych w celach osobistych**

Stale ponawiającym się zagadnieniem wśród spraw, które nie mogą być rozpatrywane przez Prezesa UODO, były sprawy dotyczące przetwarzania danych w ramach czynności o czysto osobistym lub domowym charakterze, co do których przepisy RODO nie mają zastosowania[29]. Zgodnie z RODO[30] do takich czynności należy takie przetwarzanie danych osobowych, które pozostaje bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może polegać między innymi na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Tak samo sprawą osobistą jest m.in. przetworzenie danych osobowych związane z rozpadem pożycia małżeńskiego, w tym dochodzeniem swoich praw osobistych przed sądem powszechnym poprzez wskazywanie dowodów dla stwierdzenia faktów[31], konfliktami rodzinnymi czy aspektami wychowawczymi dzieci osób, których dane dotyczą[32], a także udostępnienie danych osobowych kancelariom prawnym w celu sporządzenia i wysłania pisma[33].

**Sformułowanie sprzecznych żądań wobec organu**

Prezes UOOD odmawiał także wszczęcia postępowania w sytuacjach sprzeczności żądań do niego kierowanych. Sprzeczność żądań występuje, gdy osoba (często mimo pomimo udzielonych jej pouczeń) formułuje żądania w sposób uniemożliwiający rozpoznanie jej sprawy, np. żąda spełnienia obowiązku informacyjnego oraz usunięcia swoich danych osobowych[34] lub oczekuje zarówno uzyskania kopii jej danych osobowych, jak i ich usunięcia[35]. Osoba, której dane dotyczą, nie może żądać podjęcia działań, które wzajemnie się wykluczają. Organ nie może nakazać usunięcia danych osobowych administratorowi, a jednocześnie zobowiązać go w sposób weryfikowalny do spełnienia obowiązku informacyjnego

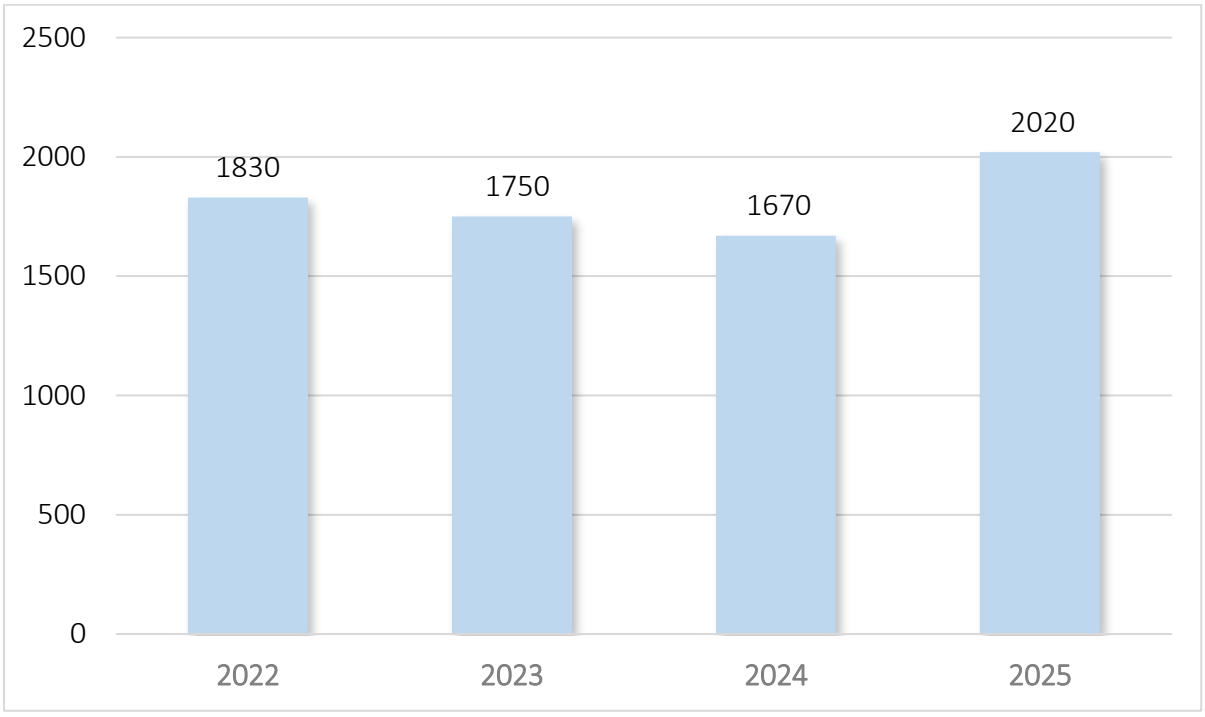
[27] Art. 58 ust. 2 RODO.
[28] Art. 15 ust. 3 RODO.
[29] Art. 2 ust. 2 lit. c RODO.
[30] Motyw 18 zdanie pierwsze RODO.
[31] DWKSN.523.2248.2025, DWKSN.523.2388.2025.
[32] DWKSN.523.3583.2025.
[33] DS.523.5666.2024.
[34] DWKSN.523.791.2025.
[35] DS.523.7150.2024.

wobec wnoszącego skargę. Tak samo nie można żądać zarówno usunięcia danych, jak i ich sprostowania czy ograniczenia przetwarzania. Administrator musi przetwarzać dane, aby taki obowiązek istniał. Nakazanie wykonania żądań w określonej kolejności czyniłoby natomiast rozstrzygnięcie organu niemożliwym do zweryfikowania w kwestii prawidłowości jego wykonania. Stanowisko organu o bezprzedmiotowości postępowania w przypadku zgłoszenia sprzecznych żądań przez stronę znajduje oparcie w orzecznictwie Wojewódzkiego Sądu Administracyjnego w Warszawie[36].

## 5. Skargi i decyzje skargowe

W 2025 r. do procedowania w Departamencie Skarg przekazano – po uprzedniej weryfikacji przez Departament Wstępnej Kontroli Skarg i Naruszeń – **1884 skargi krajowe.** Wydaniem decyzji administracyjnej zakończyło się **2020 spraw**.

Liczba wydanych przez Prezesa UODO decyzji administracyjnych w sprawach zainicjowanych skargami osób, których dane dotyczą wyraźnie wzrosła w stosunku do ubiegłych lat. W porównaniu z rokiem 2024, w którym wydanych zostało 1670 decyzji, liczba decyzji administracyjnych wydanych w 2025 r. w sprawach skargowych wzrosła 20 %.

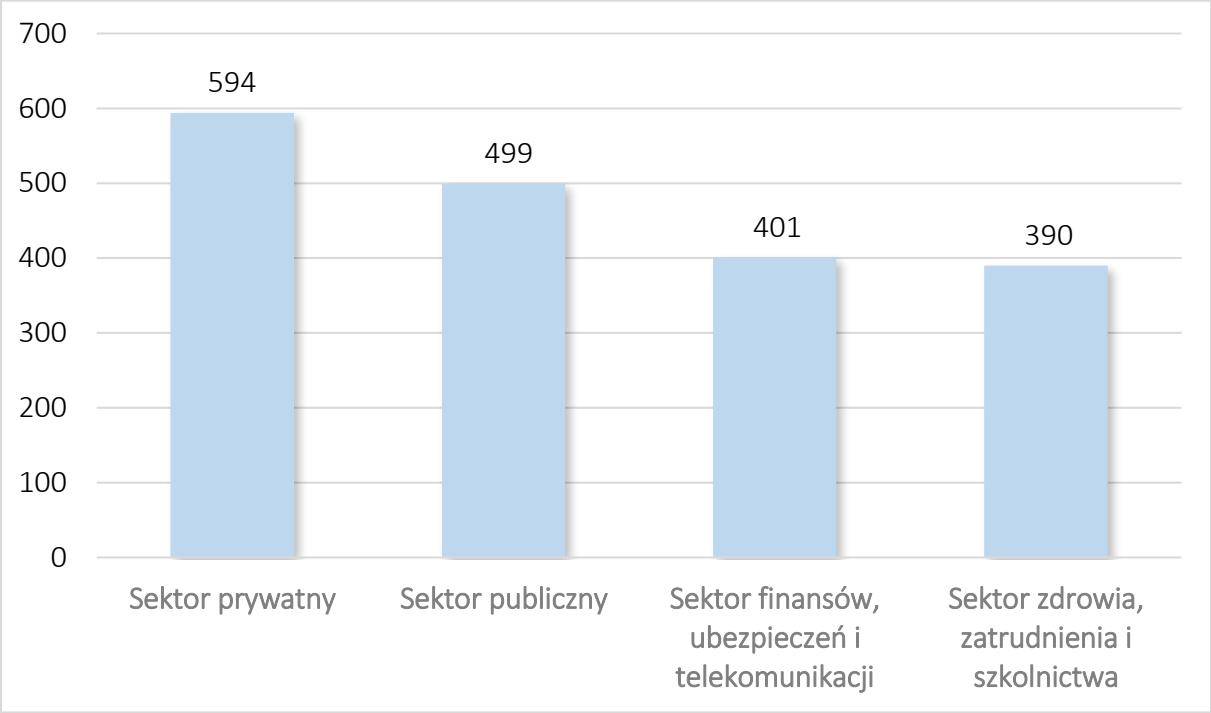



**Wykres 2:** Liczba decyzji administracyjnych wydanych w sprawach zainicjowanych indywidualną skargą, wydanych w latach 2022-2025.

Podział skarg krajowych, które przekazane zostały do Departamentu Skarg w 2025 na poszczególne sektory, przedstawiał się następująco:

[36] Np. wyroki Wojewódzkiego Sądu Administracyjnego w Warszawie: z 26 maja 2020 r. sygn. akt II SA/Wa 554/20, z 4 lutego 2026 r. sygn. akt II SA/Wa 1400/25 z 12 lutego 2026 r. sygn. akt II SA/Wa 2249/25.

- 594 skargi na podmioty sektora prywatnego,
- 499 skarg na podmioty sektora publicznego,
- 401 skarg na podmioty sektora finansowego, ubezpieczeń i telekomunikacji,
- 390 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa.




**Wykres 3:** Liczba skarg przekazanych w 2025 r. do Departamentu Skarg z podziałem na sektory.

Jak już wspomniano, w 2025 r. Departament Skarg wydał łącznie **2020 decyzji administracyjnych.** W decyzjach tych Prezes UODO w:

- **1130** przypadkach w oparciu o art. 58 RODO zastosował środki naprawcze, w tym w **815** przypadkach udzielił upomnienia za naruszenie przepisów RODO,
- **319** przypadkach zastosował środek naprawczy w postaci nakazu.

Łączna liczba zastosowanych w 2025 r. przez organ nadzorczy środków naprawczych w sprawach skargowych wzrosła o 65 % w stosunku do roku 2024 r., w którym Prezes UODO zastosował środki naprawcze w 876 sprawach, w tym w 555 sprawach udzielił upomnienia, zaś w 321 przypadkach zastosował środek naprawczy w postaci nakazu. W roku 2025 w jednej ze spraw skargowych Prezes UODO zastosował również administracyjną karę pieniężną.

### 5.1. Sektor publiczny

**Administracyjna kara pieniężna w związku z udostępnieniem danych osobowych na konferencji prasowej**

Prezes UODO decyzją wydaną w 2025 r. nałożył na **Komendanta Głównego Policji** administracyjną karę pieniężną w wysokości 75 tys. zł za naruszenie art. 6 ust. 1 i art. 9 ust. 1 RODO, poprzez udostępnienie danych osobowych bez podstawy prawnej na konferencji prasowej – związane z odtworzeniem nagrań dotyczących rozmów skarżącej z numerem alarmowym 112 i dyżurnym komendy miejskiej policji[37]. W decyzji stwierdził, że dostępnione dane osobowe dotyczyły również stanu zdrowia skarżącej. Prezes UODO w części umorzył postępowanie w zakresie, w jakim nie wykazało ono zaistnienia kwestionowanego przez skarżącą procesu przetwarzania danych osobowych.

Prezes UODO uznał w tej sprawie, że zastosowanie znajdują przepisy RODO, ponieważ na samym początku dane osobowe skarżącej, a w szczególności informacje utrwalone na ww. nagraniach, nie zostały zebrane, jak również udostępnione podczas konferencji prasowej przez policję w żadnym z celów określonych w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Komendant Główny Policji stwierdził, że materiał udostępniony podczas konferencji prasowej stanowił materiał prasowy w rozumieniu art. 7 ust. 2 pkt 4 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe[38]. Z tą argumentacją nie zgadzał się Prezes UODO wskazując, że prowadzenie przez Komendanta Głównego Policji polityki informacyjnej poprzez udzielanie przez niego środkom masowego przekazu na konferencji prasowej informacji o działalności policji nie jest działalnością Komendanta Głównego Policji polegającą na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu przez niego materiałów prasowych, a zatem działalnością, o której mowa w art. 2 ust. 1 ustawy o ochronie danych osobowych. Uzasadniając tę ocenę Prezes UODO wskazał m.in., że celem art. 14 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.[39] jest zagwarantowanie wolności niezależnym od władzy publicznej środkom masowego przekazu, a nie zagwarantowanie wolności władzy publicznej. Komendant Główny Policji, jako organ władzy publicznej, nie jest również beneficjentem określonej w art. 54 ust. 1 Konstytucji RP wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Przepis ten znajduje się bowiem w rozdziale II Konstytucji RP, zatytułowanym „Wolności, prawa i obowiązki człowieka i obywatela", a zatem wymienione w nim wolności nie są wolnościami organów władzy publicznej. Zatem Komendant Główny Policji, jako organ władzy publicznej, nie może korzystać z przywilejów i ułatwień, które przepisy prawa przewidują dla prasy.

Odnosząc się z kolei do podniesionego w wyjaśnieniach Komendanta Głównego Policji argumentu, że materiał udostępniony podczas konferencji prasowej nie zawierał danych osobowych, lecz wyłącznie informacje o charakterze anonimowym, do których RODO nie ma zastosowania, Prezes UODO wskazał, że dotyczące skarżącej informacje udostępnione podczas konferencji prasowej były udostępnione w pewnym kontekście. Konferencja prasowa została bowiem przeprowadzona w reakcji na

[37] DS.523.4750.2023.
[38] Dz. U. z 2018 r. poz. 1914.
[39] Dz. U. z 1997 r. Nr 78 poz. 483 ze zm.

materiały z udziałem skarżącej wyemitowane przez stacje telewizyjne. Dla osób, które obejrzały ww. materiały przed obejrzeniem konferencji prasowej Komendanta Głównego Policji, odnoszące się do skarżącej informacje udostępniane podczas tej konferencji były informacjami o osobie zidentyfikowanej. Osoby, które nie zapoznały się wcześniej z tymi materiałami, mogły i nadal mogą bez trudu do nich dotrzeć (np. przy użyciu wyszukiwarki internetowej), powiązując tym samym informacje udostępnione w trakcie konferencji prasowej z osobą skarżącej. Dla tych osób, odnoszące się do skarżącej informacje udostępnione w trakcie konferencji prasowej Komendanta Głównego Policji, stanowią zatem informacje o możliwej do zidentyfikowania osobie fizycznej i stanowią dane osobowe w rozumieniu art. 4 pkt 1 RODO.

W decyzji wydanej w tej sprawie Prezes UODO wskazał również, że administracyjna kara pieniężna spełni w tych konkretnych okolicznościach funkcję edukacyjną i prewencyjną. Wskaże bowiem zarówno Komendantowi Głównemu Policji, jak i innym administratorom danych na odpowiedzialność organów władzy publicznej za bezprawne działania podejmowane przez nie z wykorzystaniem swojej władzy oraz możliwości, które ta władza daje.

Wojewódzki Sąd Administracyjny w Warszawie wyrokiem z 28 stycznia 2026 r.[40] oddalił skargę wniesioną przez Komendanta Głównego Policji na ww. decyzję nakładającą administracyjną karę pieniężną.

### Udostępnianie na stronach internetowych Biuletynu Informacji Publicznej danych osobowych zamieszczonych w petycjach

W 2025 r. Prezes UODO wydał liczne decyzje w sprawach skarg na udostępnienie na stronie internetowej **Biuletynu Informacji Publicznej** (BIP) danych osobowych zamieszczonych w petycjach[41]. W jednej z takich spraw[42] udzielił upomnienia burmistrzowi za naruszenie art. 6 ust. 1 RODO poprzez udostępnienie bez podstawy prawnej na stronie internetowej BIP gminy, danych osobowych w zakresie imienia, nazwiska, adresu zamieszkania oraz podpisu, zamieszczonych w petycji skierowanej do rady miejskiej. Prezes UODO wskazał, że art. 8 ust. 1 ustawy z dnia 11 lipca 2014 r. o petycjach[43] wprost stanowi, że jedynymi danymi osobowymi wnoszącego petycję, zamieszczonymi na stronie internetowej BIP przez podmiot właściwy do rozpatrzenia petycji – pod warunkiem wyrażenia zgody wnoszącego petycję na powyższe – jest imię i nazwisko. Ponieważ skarżąca składając petycję nie wyraziła zgody na publikację jej danych osobowych Prezes UODO uznał, że burmistrz publikując na stronie internetowej Biuletynu Informacji Publicznej gminy jej dane osobowe w zakresie jej imienia, nazwiska, adresu zamieszkania oraz podpisu, zawarte w petycji, nie legitymował się żadną z przesłanek określonych w art. 6 ust. 1 RODO, która stanowiłoby o legalności tego udostępnienia. To przesądza o tym, że ww.

[40] Wyrok WSA z 28 stycznia 2026, sygn. akt II SA/Wa 890/25.
[41] DS.523.5060.2022, DS.523.4306.2023, DS.523.139.2023, DS.523.4526.2022, DS.523.261.2025.
[42] DS.523.2913.2021.
[43] Dz. U. z 2018 r. poz. 870.

udostępnienie nastąpiło bez podstawy prawnej. Prezes UODO uznał również, że kwestionowane przetwarzanie naruszyło art. 5 ust. 1 lit. a RODO. W chwili wydawania decyzji w sprawie proces przetwarzania danych osobowych skarżącej w sposób kwestionowany przez nią w skardze nie był kontynuowany, dane osobowe skarżącej zostały usunięte z ww. strony internetowej. Z uwagi na to Prezes UODO uznał za zasadne skorzystanie z instrumentu o charakterze naprawczym przewidzianego w art. 58 ust. 2 lit. b RODO i udzielił burmistrzowi upomnienia.

**Udostępnianie przez organy samorządu terytorialnego i osoby wchodzące w skład tych organów, danych osobowych na portalach społecznościowych**

Przedmiotem skarg, których dotyczyły decyzje wydane przez Prezesa UODO w 2025 r., były również kwestie udostępniania przez organy samorządu terytorialnego lub osoby wchodzące w skład tych organów, danych osobowych na **portalach społecznościowych**[44].

Decyzją wydaną w jednej ze spraw[45] Prezes UODO:

- umorzył postępowanie w zakresie nieprawidłowości w przetwarzaniu danych osobowych skarżącej przez radę miejską, polegających na udostępnieniu przez radnego rady miejskiej wizerunku skarżącej zawartego na zdjęciach na publicznym profilu tego radnego w portalu internetowym Facebook,
- nakazał radnemu rady miejskiej dostosowanie operacji przetwarzania do przepisów RODO poprzez usunięcie wizerunku skarżącej zawartego na zdjęciach opublikowanych pod 4 adresami na publicznym profilu radnego w portalu internetowym Facebook,
- udzielił radnemu rady miejskiej upomnienia za naruszenie art. 6 ust. 1 RODO polegające na udostępnieniu przez niego wizerunku skarżącej zawartego na zdjęciu zamieszczonym w poście na tym portalu.

W uzasadnieniu tej decyzji Prezes UODO wyjaśnił, że rada miasta nie posiada statusu administratora w stosunku do danych osobowych skarżącej w zakresie jej wizerunku, zawartego na zdjęciach upublicznionych w portalu Facebook na profilu radnego, ponieważ jak wynika z wyjaśnień przewodniczącego tej rady, nie udostępniała ona w tym portalu pod wskazanymi adresami wizerunku skarżącej, wskazane w skardze adresy w tym portalu są prywatnym profilem radnego, rada nie posiada publicznego profilu w tym portalu, jak również nie była organizatorem wydarzenia. W sytuacji prowadzenia przez konkretnego radnego swojego profilu na portalu społecznościowym w sieci Internet i publikowania przez niego informacji (w tym danych osobowych), bez związku z działaniami rady, rada nie jest administratorem takich danych osobowych przetwarzanych przez radnego. Prezes UODO uznał, że radny jest administratorem danych osobowych skarżącej upublicznionych przez radnego, w zakresie wizerunku skarżącej, zawartego na zdjęciach na jego profilu w portalu społecznościowym Facebook. Podkreślił również, że zgodnie z art. 47 Konstytucji RP, każda osoba ma prawo do ochrony prawnej życia prywatnego,

[44] DS.523.6929.2022, DS.523.4607.2021, DWKSN.523.3019.2025.
[45] DS.523.5859.2023.

rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, a radny przed publikacją wizerunku skarżącej w przedmiotowy sposób powinien był ustalić ryzyko takiego działania i jego oddziaływanie na konstytucyjne prawa skarżącej, w tym prawo do prywatności.

W innej sprawie[46] Prezes UODO udzielił burmistrzowi upomnienia za naruszenie art. 6 ust. 1 RODO poprzez udostępnienie bez podstawy prawnej danych osobowych skarżącej (byłego pracownika urzędu miejskiego) w postaci imienia i nazwiska w serwisie społecznościowym Facebook. Sprawa ta dotyczyła zamieszczenia na profilu urzędu miejskiego w serwisie społecznościowym Facebook wpisu w związku z udzieleniem odpowiedzi na wniosek o dostęp do informacji publicznej oraz w związku z zapytaniem w komentarzach na tym portalu dotyczącym ujęcia w budżecie odszkodowania wypłaconego skarżącej. Burmistrz wyjaśnił, że wpis ten był skutkiem omyłki pracownika. Błąd ten został jednakże zauważony i dane osobowe skarżącej zostały następnego dnia po ich opublikowaniu usunięte z ww. strony internetowej. Prezes UODO w uzasadnieniu wydanej w tej sprawie decyzji wskazał, że burmistrz nie wykazał w toku postępowania, aby legitymował się którąkolwiek z przesłanek określonych w art. 6 ust. 1 RODO, która stanowiłaby o legalności ww. udostępnienia danych osobowych skarżącej. Prezes UODO uznał w tej sprawie, że żaden przepis prawa nie uprawniał burmistrza do podania do publicznej wiadomości danych osobowych skarżącej w postaci imienia i nazwiska w powyższy sposób.

### Udostępnianie danych osobowych przez wspólnotę mieszkaniową

Do Prezesa UODO wpływa wiele skarg dotyczących przetwarzania danych osobowych przez **wspólnoty mieszkaniowe**, w tym ich udostępniania. Jedna z takich spraw zakończonych decyzją wydaną w 2025 r. dotyczyła skargi na udostępnienie przez wspólnotę mieszkaniową i spółkę, z którą wspólnota zawarła umowę o administrowanie nieruchomością wspólną, danych osobowych właściciela lokalu w e-mailu do członków wspólnoty mieszkaniowej oraz poprzez przekazanie do skrzynek pocztowych w budynku ulotek o tej samej treści co e-mail[47]. Prezes UODO ustalił, że skarżąca opublikowała na portalu Facebook posty dotyczące działań zarządu wspólnoty mieszkaniowej i spółki, z którą wspólnota zawarła umowę o administrowanie nieruchomością wspólną. Natomiast wspólnota, w celu odniesienia się do tych zarzutów, zleciła ww. spółce udzielenie informacji członkom wspólnoty o działalności zarządu wspólnoty i spółki. Wspólnota w wyjaśnieniach podnosiła, że przetwarzała dane osobowe skarżącej, w kwestionowany przez nią sposób, na podstawie art. 6 ust. 1 lit. f RODO, i udostępniła nazwisko skarżącej oraz numer lokalu, w którym zamieszkuje, w celu realizacji przez nią prawnie uzasadnionego interesu, jakim jest przedstawienie członkom wspólnoty rzetelnych informacji w odpowiedzi na publicznie udostępniony przez skarżącą post, zawierający niepełne i wprowadzające w błąd informacje. Prezes UODO w wydanej decyzji wskazał, że w jego ocenie

[46] DS.523.6929.2022.
[47] DS.523.6740.2022.

wspólnota nie spełniła przesłanek wskazanych w art. 6 ust. 1 lit. f RODO, uprawniających ją do kwestionowanego przetwarzania danych skarżącej. Okoliczność istnienia prawnie uzasadnionego interesu nie jest wystarczająca dla możliwości zastosowania tego przepisu, ponieważ niezbędne jest również wyważenie dwóch dóbr chronionych prawem, tj. prawnie uzasadnionego interesu administratora lub strony trzeciej z jednej strony i interesów, podstawowych praw oraz wolności podmiotu danych z drugiej. W tej sprawie dane osobowe skarżącej udostępniane zostały w powiązaniu z oświadczeniem wspólnoty odnoszącym się do ogólnych uwag o funkcjonowaniu portali społecznościowych i funkcjonujących na tych portalach forach tworzonych przez osoby prywatne. Nie można wobec tego uznać, że kwestionowane udostępnienie danych osobowych skarżącej było niezbędne do zapewnienia innym współwłaścicielom prawa do współdziałania w zarządzie nieruchomością wspólną oraz do sprawowania kontroli działalności jej zarządcy.

Ponadto Prezes UODO nie stwierdził zaistnienia żadnej z przesłanek wymienionych w art. 6 ust. 1 RODO, w oparciu o którą wspólnota mogłaby w sposób zgodny z obowiązującymi przepisami udostępnić dane osobowe skarżącej w zakresie nazwiska oraz numeru lokalu, w sposób, w jaki to nastąpiło. Z uwagi na te okoliczności Prezes UODO udzielił wspólnocie upomnienia za stwierdzone naruszenie. W pozostałym zakresie Prezes UODO umorzył postępowanie ponieważ skarżąca kwestionowała również udostępnienie jej imienia, a przeprowadzone postępowanie wykazało, że nie doszło do kwestionowanego przetwarzania danych osobowych skarżącej w tym zakresie.

### Udostępnienie przez komornika na kopercie informacji o prowadzonym postępowaniu egzekucyjnym

Podmiotami skarżonymi w wielu sprawach zakończonych decyzjami wydanymi w 2025 r. byli **komornicy sądowi**[48]. W jednej z tego rodzaju spraw Prezes UODO udzielił upomnienia komornikowi sądowemu za naruszenie art. 6 ust. 1 RODO polegające na ujawnieniu danych osobowych w zakresie informacji o prowadzonym przeciwko skarżącej postępowaniu egzekucyjnym, poprzez umieszczenie na kopercie skrótów nazw pism zawartych w przesyłkach skierowanych przez komornika do tej osoby[49]. Komornik sądowy na kopertach przesyłek nadanych do skarżącej za pośrednictwem operatora pocztowego oprócz imienia, nazwiska, adresu skarżącej oraz sygnatury akt postępowania, zamieścił skróty nazw pism zawartych w korespondencji, tj. np.: „Rodzaj przesyłki: zaj. rach. bank., zaw. o wszcz., odpis tyt. wyk., wez. 801 K.p.c., formularz, Formularz skargi na czynności komornika, zaj. wierz. us.”.

W ocenie Prezesa UODO treść § 17 ust. 3 rozporządzenia Ministra Sprawiedliwości z dnia 18 grudnia 2018 r. w sprawie określania szczegółowych zasad

[48] DS.523.484.2023, DS.523.6853.2021, DS.523.2672.2021, DS.523.4071.2024, DS.523.4341.2024, DS.523.1459.2024, DS.523.2091.2021, DS.523.367.2025, DS.523.767.2020, DS.523.7986.2024, DS.523.329.2024, DS.523.1160.2024, DS.523.2743.2024.
[49] DS.523.8119.2021.

prowadzenia biurowości, rachunkowości i ewidencji operacji finansowych kancelarii komorniczych[50] wskazuje w sposób nie budzący wątpliwości, że w przypadku doręczenia przez komornika kilku pism jedną przesyłką, na zwrotnym potwierdzeniu odbioru (a nie na kopercie) należy zamieścić informacje pozwalające ustalić zawartość przesyłki. Analogiczne regulacje przewiduje rozporządzenie Ministra Sprawiedliwości z dnia 6 maja 2020 r. w sprawie szczegółowego trybu i sposobu doręczania pism sądowych w postępowaniu cywilnym[51]. Stosownie do § 1 ust. 2 ww. aktu przepisy rozporządzenia dotyczące sądu wysyłającego stosuje się odpowiednio do komornika. Z kolei § 2 ust. 1 zdanie 2 rozporządzenia stanowi wprost, że na stronie adresowej przesyłki, jako dodatkowy element umieszcza się jedynie napis: „Polecona – za potwierdzeniem odbioru". Prezes UODO uznał, że komornik zamieścił informacje dotyczące zawartości przesyłek kierowanych do skarżącej na kopertach niezgodnie z § 17 ust. 3 ww. rozporządzenia Ministra Sprawiedliwości.

Działanie to doprowadziło do sytuacji, w której, niezależnie od odebrania przez skarżącą korespondencji, informacja wskazująca na zawartość przesyłek była jawna już na etapie doręczania korespondencji, oraz że możliwe było zawarcie na zwrotnym potwierdzeniu odbioru (oraz kopercie) takich informacji, które będą jednoznacznie wskazywać na zawartość przesyłki, nie będą zaś informować o tym, jakiego rodzaju pismo komornik kieruje do skarżącej, np. indywidualny numer korespondencji. W tych okolicznościach umieszczenie na kopertach skrótów nazw pism kierowanych do skarżącej nie znajdowało oparcia w żadnej z przesłanek wskazanych w art. 6 ust. 1 RODO i stanowiło naruszenie tego przepisu.

**Udostępnienie przez Zakład Ubezpieczeń Społecznych danych osobowych osobie nieuprawnionej wskutek błędnego wpisu w systemie informatycznym**

Wiele decyzji wydanych w 2025 r. dotyczyło również **Zakładu Ubezpieczeń Społecznych**[52]. W jednej z nich Prezes UODO udzielił upomnienia Zakładowi Ubezpieczeń Społecznych za naruszenie art. 6 ust. 1 lit. c RODO polegające na udostępnieniu na rzecz osoby trzeciej danych osobowych zawartych w dokumencie PIT za rok 2024[53]. Dotyczyło ono skierowania przez Zakład Ubezpieczeń Społecznych korespondencji przeznaczonej dla skarżącej na adres osoby trzeciej, która na skutek błędu pracownika Zakładu Ubezpieczeń Społecznych, została zarejestrowana w systemie informatycznym jako pełnomocnik skarżącej. Prezes UODO uznał, że to udostępnienie nie znajdowało oparcia w żadnej spośród przesłanek określonych w art. 6 ust. 1 RODO, stanowiących o legalności przetwarzania (udostępnienia) danych osobowych i tym samym nastąpiło bez podstawy prawnej.

[50] Dz. U. z 2024 r. poz. 1256.
[51] Dz. U. z 2024 r. poz. 19.
[52] DS.523.3440.2024, DS.523.6500.2024, DS.523.232.2025, DS.523.1160.2023, DS.523.2228.2024, DS.523.7215.2024, DS.523.3775.2022, DS.523.5020.2022, DS.523.3287.2021, DS.523.208.2025, DS.523.107.2022, DS.523.233.2025, DS.523.6153.2022.
[53] DS.523.267.2025.

## 5.2. Sektor prywatny

### Przetwarzanie danych osobowych z wykorzystaniem monitoringu wizyjnego

W jednej ze spraw[54] Prezes UODO uznał, że stosowanie przez sąsiadów **wizjera cyfrowego z funkcją nagrywania i detekcji ruchu**, który obejmuje wspólną klatkę schodową, stanowi bezprawne przetwarzanie danych osobowych, ponieważ wykracza poza sferę czysto prywatną i narusza przepisy rozporządzenia 2016/679.

W toku postępowania ustalono, że monitoring ten nie opierał się na żadnej z dopuszczalnych podstaw prawnych, w tym na zgodzie sąsiadów ani na prawnie uzasadnionym interesie właścicieli urządzenia. Skarżeni nie zdołali udowodnić realnego zagrożenia swojego bezpieczeństwa, a ich hipotetyczna chęć ochrony mienia nie może przeważać nad prawem do prywatności osób trzecich, zwłaszcza że monitoring jest środkiem wyjątkowo inwazyjnym i powinien być stosowany dopiero po wyczerpaniu mniej dotkliwych metod zabezpieczeń.

W konsekwencji Prezes UODO stwierdził naruszenie art. 6 ust. 1 rozporządzenia 2016/679, podkreślając, że w przestrzeni wspólnej właściciel mieszkania ma obowiązek respektować wolności innych osób, a nieuzasadnione rejestrowanie ich wizerunku bez podstawy prawnej jest niedopuszczalne.

Prezes UODO nakazał skarżonym zaprzestanie przetwarzania danych osobowych skarżących, w zakresie ich wizerunku, za pomocą monitoringu wizyjnego (wizjera cyfrowego) obejmującego obszar wspólny nieruchomości oraz usunięcie ich danych osobowych z dotychczas utrwalonych nagrań.

Prywatny monitoring przestaje być sprawą wyłącznie osobistą w momencie, gdy obiektyw kamery „wychodzi” poza ogrodzenie posesji. W innej sprawie[55] Prezes UODO ustalił, że trzy kamery zainstalowane przez skarżoną rejestrowały nie tylko jej podwórko, ale również działkę sąsiadów oraz drogę publiczną. Takie szerokie pole widzenia sprawiło, że skarżona – nawet jeśli działała w dobrej wierze – stała się administratorem danych osobowych w rozumieniu rozporządzenia 2016/679 i zaczęła podlegać obostrzeniom tego rozporządzenia.

Organ odrzucił argumentację skarżonej o potrzebie zapewnienia bezpieczeństwa jako nadrzędną nad prywatnością sąsiadów. Uznał, że stała obserwacja osób postronnych na drodze dojazdowej i sąsiedniej posesji jest zbyt inwazyjna, a skarżona nie udowodniła, by na tym terenie dochodziło do realnych incydentów uzasadniających tak radykalne środki.

Skarżona otrzymała nakaz zaprzestania nagrywania obszarów poza swoją własnością oraz usunięcia danych osobowych zawartych w dotychczasowych nagraniach.

Zgodnie z wytycznymi Europejskiej Rady Ochrony Danych[56] monitoring wizyjny jest zgodny z prawem, o ile jest konieczny do osiągnięcia celu prawnie uzasadnionego interesu administratora danych lub strony trzeciej, chyba że interesy te są podrzędne

[54] DS.523.6032.2023.
[55] DS.523.6459.2023.
[56] Wytyczne EROD 3/2019.

w stosunku do interesów osób, których dane dotyczą, lub podstawowych praw i wolności (art. 6 ust. 1 lit. f).

W innej sprawie[57] Prezes UODO odmówił skarżącej uwzględnienia jej wniosku dotyczącego przetwarzania jej danych osobowych w postaci wizerunku bez podstawy prawnej za pośrednictwem monitoringu wizyjnego zainstalowanego przy użyciu bezprzewodowego dzwonka drzwiowego z wizjerem elektronicznym.

W przedmiotowej sprawie Prezes UODO uznał, że choć monitoring zainstalowany przez skarżonego wykracza poza granice jego prywatnej własności i obejmuje klatkę schodową, jest on wyjątkowo, w tej konkretnej sprawie, w pełni prawnie uzasadniony i zgodny z rozporządzeniem 2016/679. Decydującym czynnikiem był udokumentowany, intensywny konflikt sąsiedzki oraz fakt, że mąż skarżącej został już wcześniej skazany za konkretne akty agresji i nękania skierowane przeciwko skarżonemu (m.in. wulgarne gesty, zakłócanie ciszy nocnej czy próby uszkodzenia wizjera).

Interes bezpieczeństwa skarżonego był realny. Skarżony nie musiał ograniczać się tylko do progu własnych drzwi, ponieważ zagrożenie (zarówno w postaci agresji, jak i innych incydentów) ma miejsce bezpośrednio przed jego nieruchomością. Z kolei prywatność skarżącej nie była naruszona nadmiernie. Monitoring nie śledził jej stale, a jedynie rejestrował momenty, w których przebywa ona w bezpośrednim sąsiedztwie drzwi skarżonego.

Artykuł 6 ust. 1 lit. f rozporządzenia 2016/679 ma tu zastosowanie. Prawo skarżonego do ochrony zdrowia i bezpieczeństwa rodziny zostało uznane przez Prezesa UODO za nadrzędne wobec prawa skarżącej do prywatności na klatce schodowej.

### Przetwarzanie danych osobowych w celach marketingowych

W jednym z postępowań[58] spółka dopuściła się naruszenia przepisów rozporządzenia 2016/679 poprzez stosowanie wymuszonej zgody na **marketing bezpośredni.**

Zgoda na marketing bezpośredni ukryta w treści regulaminu serwisu traci przymiot dobrowolności, ponieważ klient zostaje postawiony w sytuacji bez wyjścia: musi ją zaakceptować, aby w ogóle skorzystać z usługi. Takie powiązanie zgody z głównym świadczeniem jest prawnie bezskuteczne na mocy art. 7 ust. 2 rozporządzenia 2016/679. W konsekwencji spółka *de facto* nigdy nie posiadała ważnej podstawy prawnej do wysyłki e-maili i SMS-ów do skarżącego.

Ostatecznie działanie to zostało uznane przez Prezesa UODO za niezgodne z prawem. Aktywne zachęcanie klientów do przejścia na e-fakturę poprzez wysyłanie im wiadomości elektronicznych nie znajduje uzasadnienia w obowiązujących przepisach prawa i stanowi w rzeczywistości niedozwolone działanie marketingowe. Informowanie o możliwości wyboru powyższego sposobu rozliczania się z umowy

[57] DWKSN.523.318.2025.
[58] DS.523.2180.2024.

powinno nastąpić w ramach zawartej umowy i dostępnych narzędzi, np. w portalu klienta.

Prezes UODO rozpatrywał w 2025 r. sprawę[59], w której spółka dokonała wysyłki wiadomości elektronicznej celem zachęcenia do aktywacji usługi e-faktury. Spółka tłumaczyła m.in., że faktura elektroniczna jest sposobem realizacji elementu umowy, jakim jest obsługa procesu płatności. Według spółki takie podejście ma uzasadnienie w przepisach prawa. Prezes UODO uznał powyższe działanie spółki za działanie marketingowe mające za zadanie wywołać reakcję skarżącego poprzez aktywację usługi e-faktury. Organ nadzorczy nie zgodził się ze spółką, że takie działanie ma swoją podstawę w przepisach. Klient powinien zostać poinformowany o tej metodzie rozliczania bezpośrednio w umowie oraz poprzez dostępne kanały komunikacji, takie jak portal klienta.

W tej sprawie Prezes UODO uznał za marketing bezpośredni również wiadomość e-mail spółki do skarżącego dotyczącą wyrażenia opinii na temat ostatniego rachunku za energię.

W tego typu sytuacjach Prezes UODO podziela stanowisko Wojewódzkiego Sądu Administracyjnego w Warszawie[60], który wskazał, że marketingiem bezpośrednim będzie skierowanie prośby do klienta spółki o ocenę jakości wykonanej usługi.

**Realizacja wniosku o usunięcie danych osobowych**

W jednej ze spraw[61] skarżący utracił dostęp do skrzynki pocztowej, która podana była przez niego przy aktywacji konta na **portalach przedsiębiorcy**, a także zapomniał hasła do tego konta. Przedsiębiorca odmówił skarżącemu uwzględnienia jego żądania dezaktywacji konta i usunięcia danych osobowych.

Przedsiębiorca jako administrator danych powinien wezwać o dane, które są niezbędne do identyfikacji osoby, której dane dotyczą, a także powinien ustalić taki sposób uwierzytelnienia osoby, której dane dotyczą, aby nie naruszyć żadnego przepisu rozporządzenia 2016/679.

Prezes UODO nie narzucając przedsiębiorcy konkretnej metody uwierzytelnienia skarżącego zwrócił uwagę, że pomimo braku dostępu do skrzynki pocztowej przez skarżącego, przedsiębiorca miał jednak możliwość uwierzytelnić skarżącego, chociażby poprzez zaproponowane przez niego, w prowadzonej korespondencji, okazanie wizerunku. Warto zaznaczyć, że przedsiębiorca i tak przetwarzał już imię, nazwisko, datę urodzenia oraz wizerunek użytkownika w celu prowadzenia jego konta, wykorzystanie tych informacji nie byłoby działaniem nadmiarowym ani nieadekwatnym. Przedsiębiorca – zdaniem Prezesa UODO – mógłby również dopytać skarżącego o informacje na temat jego konta, np. aktywności, o której tylko skarżący miałby wiedzę.

[59] DS.523.3715.2024.
[60] Wyrok WSA w Warszawie z 23 stycznia 2025 r. sygn. akt II SA/Wa 664/24, prawomocny.
[61] DS.523.3367.2023.

Prezes UODO w opisanej sprawie stwierdził, że brak dostępu do konta przez skarżącego w wyniku utraty danych uwierzytelniających nie może być przesłanką uniemożliwiającą usunięcie jego danych osobowych przetwarzanych przez przedsiębiorcę, jeżeli istnieje jakakolwiek inna możliwość jego identyfikacji. Prezes UODO nakazał zatem przedsiębiorcy podjęcie komunikacji ze skarżącym, poprzez zażądanie od niego dodatkowych informacji niezbędnych do potwierdzenia jego tożsamości.

**Udostępnienie danych osobowych**

Jedna ze spraw[62] dotyczyła spółki, która na prowadzonym przez siebie **serwisie internetowym** udostępniła dane osobowe skarżącego, w zakresie numeru księgi wieczystej dla działki ewidencyjnej, której skarżący był współwłaścicielem.

W tej sprawie Prezes UODO stwierdził, że numer księgi wieczystej stanowi dane osobowe w rozumieniu rozporządzenia 2016/679, co znajduje potwierdzenie w orzecznictwie sądów administracyjnych[63].

W regulaminie serwisu internetowego spółka została wskazana jako jego właściciel i administrator. Co więcej, źródłem zarobku spółki było udostępnianie numerów ksiąg wieczystych i pobieranie za ich udostępnianie opłaty. W związku z tym Prezes UODO uznał spółkę za administratora danych osobowych skarżącego.

Internetowa dostępność serwisu spółki sprawiała, że dane osobowe skarżącego były dostępne nieograniczonemu kręgowi odbiorców, zarówno z Polski, jak i z zagranicy.

W tej sprawie spółka udostępniła numer księgi wieczystej skarżącego na prowadzonej przez nią stronie internetowej, nie mając do tego podstawy prawnej. Z uwagi na to, że spółka nie wskazała żadnej podstawy prawnej do dalszego przetwarzania ww. danych osobowych skarżącego Prezes UDOO nakazał ich usunięcie.

W innym postępowaniu[64] skarżący wynajmował pokój w mieszkaniu należącym do skarżonej. Skarżona pozostawiła pismo dotyczące wypowiedzenia umowy najmu, zawierające imię, nazwisko i numer PESEL skarżącego, w kuchni, będącej pomieszczeniem ogólnodostępnym dla wszystkich lokatorów mieszkania. Skarżonej zależało, aby wypowiedzenie umowy najmu było skuteczne, więc zdecydowała się na pozostawienie pisma w miejscu ogólnodostępnym dla wszystkich lokatorów.

W ocenie Prezesa UODO poprzez działanie skarżonej umożliwiono dostęp do danych osobowych skarżącego przez osoby trzecie – pozostałych lokatorów mieszkania, do czego finalnie faktycznie doszło.

Według Prezesa UODO skuteczne wypowiedzenie umowy najmu powinno zawierać formę pisemną oraz zostać doręczone drugiej stronie tak, by tylko ona mogła zapoznać się z jego treścią. W konsekwencji skarżona mogła, np. wysłać je listem

[62] DS.523.4213.2022.
[63] Wyrok WSA z 5 maja 2021 r. sygn. akt II SA/Wa 2222/20 oraz wyrok NSA z 28 stycznia 2025 r. sygn. akt III OSK 6508/21.
[64] DS.523.401.2025.

poleconym ze zwrotnym potwierdzeniem odbioru na ostatni znany adres skarżącego lub osobiście wręczyć dokument w obecności świadka, który potwierdziłby fakt jego doręczenia.

Prezes UODO uznał, że działanie skarżonej nie miało podstawy prawnej w przepisach rozporządzenia 2016/679.

W innej sprawie[65] skarżony udostępnił dane skarżącej zawarte w treści pisma oraz wyroku dyrektorowi szkoły, kuratorowi oraz staroście. Przekazanie danych skarżącej wynikało wyłącznie z potrzeby zgłoszenia zastrzeżeń co do jej etyki zawodowej jako nauczyciela. Działanie to, wynikające z prawa do składania skarg, nie podlegało pod przepisy rozporządzenia 2016/679, gdyż miało charakter osobisty i prywatny, a nie zawodowy czy handlowy. Udostępnienie danych skarżącej ograniczyło się bowiem tylko do podmiotów kontrolujących pracę skarżącej jako nauczyciela. Należy również uwzględnić, że tłem sprawy był trwający konflikt rodzinno-sąsiedzki między stronami.

Prawo do ochrony danych osobowych nie ma charakteru bezwzględnego i nie może blokować obywatelowi możliwości dochodzenia praw przed właściwymi organami. W związku z tym, na podstawie art. 2 ust. 2 lit. c rozporządzenia 2016/679, przepisy tego rozporządzenia nie miały w tej sprawie zastosowania. Skutkowało to brakiem kompetencji Prezesa UODO do rozstrzygnięcia w drodze decyzji i umorzeniem postępowania.

**Prawo dostępu do danych przysługujące osobie, której dane dotyczą**

W ramach jednej ze spraw[66] skarżący, działając na podstawie art. 15 ust. 1 i 3 rozporządzenia 2016/679, zwrócił się do spółki (będącej administratorem danych przetwarzanych za pomocą monitoringu na lotnisku) z wnioskiem o udostępnienie mu nagrań z monitoringu, zawierających dane osobowe jego oraz jego małoletnich dzieci. Spółka w odpowiedzi na wniosek skarżącego wskazała, że ma uzasadnione wątpliwości w stosunku do jego tożsamości oraz jego występowania w imieniu jego małoletnich dzieci. Skarżący przesłał spółce dokumenty rozwiewające ww. wątpliwości. Wskazał również prawdopodobne daty przebywania jego małoletnich dzieci na lotnisku. Według spółki brak wystąpienia czynników wyróżniających przebywanie wskazanych osób przez skarżącego na terenie lotniska, w stosunku do pozostałych pasażerów, udostępnienie nagrań mogłoby stanowić pogwałcenie praw osób trzecich, których dane dotyczą, a których wizerunek został utrwalony. Skarżący w innym piśmie zwrócił się do spółki o przesłanie pisemnych stenogramów z zapisów, na których widnieją jego małoletnie dzieci. Spółka odpowiedziała skarżącemu, że nie jest w stanie zidentyfikować osób, których dane dotyczą. Spółka nie posiadała technicznych możliwości uzyskania informacji dotyczących lokalizacji wspomnianych przez skarżącego osób.

W ocenie Prezesa UODO zachodziło w tej sprawie wyłączenie zastosowania art. 15 ust. 1 i 3 rozporządzenia 2016/679, ponieważ zgodnie z art. 11 ust. 2

[65] DS.523.7146.2021.
[66] DS.523.4775.2023.

rozporządzenia 2016/679, administrator może wykazać, że nie jest w stanie zidentyfikować osób, których dane dotyczą, o czym spółka poinformowała skarżącego. Spółka przywołała w tej sytuacji jako podstawę odmowy okoliczność braku wystąpienia czynników wyróżniających przebywanie na jej terenie wskazanych we wniosku osób (tzn. brak możliwości ich identyfikacji na posiadanych nagraniach). Skarżący nie dostarczył spółce dodatkowych informacji, które mogłyby pomóc w zidentyfikowaniu wskazanych przez niego osób. Dodatkowo spółka prawidłowo wskazała na zbyt szeroki zakres żądań skarżącego obejmujący pełne daty dzienne, bez doprecyzowania konkretnego przedziału godzinowego, brak możliwości wyodrębnienia na zarejestrowanych nagraniach z posiadanych kilkudziesięciu kamer, obejmujących łącznie kilka tysięcy godzin nagrań, fragmentów zawierających wizerunek dzieci wnioskodawcy, przy zmasowanym ruchu osobowym, gdzie wymagałoby to ręcznego poklatkowego przeglądania zapisów wideo i prób identyfikacji, w oparciu o przesłane nie najwyższej jakości zdjęcia paszportowe dzieci. Jednocześnie spółka poinformowała skarżącego o powyższych powodach odmowy.

**Publikacja danych osobowych na portalu społecznościowym**

W jednej ze spraw[67] pomiędzy stronami zaistniał spór związany z prawidłowym wykonaniem usługi. Skarżący odmówił skarżonej zapłacenia za wykonaną przez nią usługę. W rezultacie skarżona opublikowała dane osobowe skarżącego na portalu społecznościowym, aby ostrzec inne osoby, wykonujące zawód skarżonej przed sytuacją, która ją spotkała. Jej zdaniem zachodziła realna obawa o bezpieczeństwo innych osób wykonujących jej zawód. Jako podstawę prawną udostępnienia danych skarżącego podała art. 6 ust. 1 lit. d, e, f rozporządzenia 2016/679. Prezes UODO nie mógł zgodzić się z taką argumentacją. W niniejszej sprawie, wbrew twierdzeniom skarżonej, nie znalazła zastosowania przesłanka legalizująca proces przetwarzania danych określona w art. 6 ust. 1 lit. d rozporządzenia 2016/679, ponieważ udostępnienie to nie było niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. Przesłanka ta dotyczy ochrony żywotnego interesu osoby, której dane dotyczą, tj. w tym przypadku skarżącego. Skarżona nie mogła powoływać się na tę przesłankę w odniesieniu do „żywotnych interesów" osób, którym dane skarżącego zostały udostępnione. Prezes UODO wskazał w wydanej decyzji, że jeżeli udostępnienie danych skarżącego przez skarżoną było formą jego negatywnej oceny to logicznym jest, że ten nie wyraziłby zgody na takie udostępnienie jego danych.

Prezes UODO odnosząc się do powoływanej przez skarżoną podstawy prawnej do udostępnienia danych osobowych skarżącego, mającej oparcie w art. 6 ust. 1 lit. e rozporządzenia 2016/679, stwierdził, że skarżona nie wskazała konkretnego przepisu prawa, który obligowałby ją do udostępnienia danych osobowych skarżącego w ramach zadania realizowanego w interesie publicznym, czy w ramach sprawowania władzy publicznej. Organ zwrócił uwagę, że samo stwierdzenie, że „porządek publiczny oraz ochrona osób przed aktami wszelkiej przemocy stoi bez wątpliwości

[67] DS.523.6668.2024.

zarówno w interesie poszczególnych osób, jak i w interesie publicznym" jest niewystarczające.

Skarżona wskazała również, że przetwarzała dane osobowe skarżącego na podstawie prawnie uzasadnionego interesu, jakim była obawa o bezpieczeństwo innych osób wykonujących jej zawód. Skarżona w żaden sposób nie wykazała jednak, że powyższe wchodzi w zakres prowadzonej przez nią działalności. Skarżona nie wykazała także, że wskazany przez nią interes miał charakter nadrzędny wobec interesów lub podstawowych praw i wolności skarżącego, np. poprzez przedstawienie wyników testu równowagi, o ile taki został przeprowadzony. W związku z tym udostępnienie danych osobowych skarżącego przez skarżoną nie mogło odbywać się również na podstawie przesłanki wskazanej w art. 6 ust. 1 lit. f rozporządzenia 2016/679.

Konflikt zaistniały pomiędzy skarżoną a skarżącym nie upoważniał jej do udostępnienia jego danych osobowych, a co za tym idzie stygmatyzacji wobec innych podmiotów, z którymi skarżący może współpracować. Prezes UODO wskazał, że kwestia zapewnienia bezpieczeństwa (w tym przypadku innym osobom wykonującym zawód skarżonej) nie leży w gestii skarżonej i zadanie to nie może być wykonywane przez nią za pomocą udostępniania danych osobowych innych osób. W ocenie Prezesa UODO skarżona wykonując swój zawód nie była uprawniona do zastępowania w tej kwestii właściwych organów państwowych. Prezes UODO zwrócił uwagę, że jeżeli zdaniem skarżonej w zaistniałej sytuacji doszło do wyczerpania znamion przestępstwa, skarżona zgodnie z literą prawa powinna zgłosić tę sytuację do właściwych organów ściągania, czego skarżona w tej sprawie nie uczyniła.

W konsekwencji Prezes UODO uznał, że skarżona nie legitymowała się żadną z przesłanek z art. 6 ust. 1 rozporządzenia 2016/679, pozwalającą na udostępnienie danych osobowych skarżącego na jednym z portali społecznościowych, jak również że kwestionowane przez skarżącego udostępnienie jego danych osobowych nastąpiło bez podstawy prawnej.

### Administrator strony internetowej jako administrator danych osobowych publikowanych przez użytkowników w komentarzach

W tej sprawie[68] spółka zaprzeczyła, aby była administratorem danych osobowych znajdujących się w treściach opinii dodawanych przez użytkowników w komentarzach na administrowanej przez nią stronie internetowej.

W ocenie Prezesa UODO spółka bezsprzecznie pełniła rolę administratora danych osobowych skarżących, przetwarzanych za pośrednictwem administrowanej przez nią strony internetowej. Jako podmiot prowadzący serwis internetowy, spółka określa cele przetwarzania danych oraz decyduje o sposobach ich przetwarzania, w tym również w sekcji przeznaczonej do publikowania opinii przez użytkowników portalu. Tym samym spółka pozostaje administratorem danych osobowych

[68] DS.523.4620.2022.

przetwarzanych w ramach funkcjonowania platformy internetowej, na której publikowane są treści zamieszczane przez osoby trzecie na forum serwisu.

Prezes UODO wskazał, że na podstawie art. 14 ust. 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[69], nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych. W nawiązaniu do powyższego organ nadzorczy stwierdził, że przepis ten nie stanowi o wyłączeniu odpowiedzialności spółki jako administratora danych osobowych, a jedynie o wyłączeniu odpowiedzialności administratora portalu internetowego z uwagi na jego nieświadomość w publikowaniu treści o bezprawnym charakterze. Prezes UODO zwrócił uwagę, że administrator portalu, który umożliwia wymianę poglądów użytkowników, zamieszczając jednocześnie ostrzeżenie o moderacji i usuwaniu wpisów niespełniających określonych reguł powinien liczyć się z tym, że może odpowiadać za treść publikowanych komentarzy zwłaszcza, gdy posiada wiedzę o – zdaniem niektórych osób – ich bezprawnym charakterze, zaś administrator portalu sam, i w pierwszej kolejności, decyduje o ich usunięciu, bądź nie. Organ nadzorczy powołał się w tym zakresie na wyrok Sądu Apelacyjnego w Lublinie z 18 stycznia 2011 r.[70], w którym sąd stwierdził, że usługodawca nie ma obowiązku monitorowania sieci, co więcej nie ma też obowiązku podejmowania kroków w celu wdrożenia oprogramowania monitorującego. Jedyną sytuacją prowadząca bez wątpienia do odpowiedzialności usługodawcy jest istnienie po jego stronie stanu wiedzy o fakcie naruszenia, czy też bezprawnym charakterze naruszenia.

W tej sprawie skarżący zwrócili się do spółki o usunięcie ich danych osobowych. Spółka nie odpowiedziała na ich żądanie. Dopiero po interwencji Prezesa UODO spółka zaprzestała przetwarzania danych osobowych skarżących w kwestionowany przez nich sposób, blokując również możliwość dodawania komentarzy na przedmiotowych stronach internetowych. W związku z powyższym brak było podstaw do wydania decyzji jakiej domagali się skarżący. Prezes UODO umorzył zatem postępowanie w powyższym zakresie. Spółka została jednak upomniana przez Prezesa UODO w zakresie braku terminowej odpowiedzi na wniosek skarżących.

### 5.3. Sektor finansów, ubezpieczeń i telekomunikacji

W 2025 roku Prezes Urzędu Ochrony Danych Osobowych, podobnie do lat poprzednich, rozpatrywał liczne skargi dotyczące działalności podmiotów sektora finansowego, takich jak banki, instytucje pożyczkowe, spółdzielcze kasy oszczędnościowo-kredytowe, instytucje utworzone na podstawie art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[71], związane z przetwarzaniem danych

[69] Dz. U. 2024 r. poz. 1513 ze zm.
[70] Sygn. akt I ACa 544/10.
[71] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2026 r. poz. 38), dalej: Prawo bankowe.

osobowych w związku z dokonywaniem oceny zdolności kredytowej i analizy ryzyka kredytowego.

**Przetwarzanie danych osobowych klienta banku po wygaśnięciu zobowiązania umownego**

Liczne decyzje wydane przez Prezesa UODO dotyczyły możliwości przetwarzania danych osobowych byłych klientów banków bez ich zgody w celu oceny zdolności kredytowej i analizy ryzyka kredytowego po wygaśnięciu zobowiązania. Taką możliwość przewiduje art. 105a ust. 3 Prawa bankowego. Podmioty wskazane w tym przepisie mogą przetwarzać informacje stanowiące tajemnicę bankową i informacje udostępnione przez instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy o kredycie konsumenckim[72], dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem, inną instytucją ustawowo upoważnioną do udzielania kredytów, instytucją pożyczkową lub podmiotem, o którym mowa w art. 59d ustawy o kredycie konsumenckim, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z ww. podmiotami, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby o zamiarze przetwarzania dotyczących jej informacji, bez jej zgody. Przepis zawiera zatem wskazanie konkretnych przesłanek, które bank musi spełnić, aby mógł przetwarzać dane byłych klientów na podstawie ww. przepisu.

Prezes UODO w swoich decyzjach wskazywał, że sam fakt, że były klient nie wykonał zobowiązania lub spóźnił się z jego wykonaniem co najmniej 60 dni, nie upoważnia podmiotu do przetwarzania jego danych na warunkach określonych w art. 105a ust. 3 Prawa bankowego. Istotne jest również spełnienie obowiązku informacyjnego wskazanego w ww. przepisie w zakresie poinformowania podmiotu danych o zamiarze przetwarzania jego danych na podstawie ww. przepisu. W konsekwencji podmiot, mając zamiar przetwarzać dane na ww. podstawie prawnej, musi wykazać, że klient został poinformowany o zamiarze przetwarzania jego danych bez jego zgody. W przypadku braku wykazania ww. dowodu Prezes UODO stwierdzał, że ww. przetwarzanie odbywa się bez podstawy prawnej, gdyż nie zostały spełnione wymogi wskazane ww. przepisie[73].

W roku 2025 r. Prezes UODO rozpatrywał także skargę dotyczącą przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego. Po przeprowadzeniu czynności wyjaśniających bank wskazał, że obowiązek poinformowania, o którym mowa w ww. przepisie, spełnił poprzez skierowanie do osoby skarżącej wiadomości e-mailowej z wypowiedzeniem umowy, zawierającej informację o przetwarzaniu danych osobowych bez jej zgody w trybie art. 105a ust. 3 Prawa bankowego, która została wysłana na podany przez osobę skarżącą w umowie adres e-mail. Dodatkowo w treści umowy zawartej z osobą skarżącą strony umówiły

[72] Ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim (Dz. U. z 2025 r. poz. 1362), dalej: ustawa o kredycie konsumenckim.
[73] DS.523.3292.2020.

się na prowadzenie działań monitorująco – upominawczych w postaci między innymi wysłanych wiadomości głosowych/sms/e-mail na podane w umowie numery telefonów oraz adresy e-mail. W celu udowodnienia odebrania wiadomości przez osobę skarżącą, bank przedłożył wydruk z systemu bankowego, z którego wynika, że wiadomość e-mailowa banku została przesłana na adres poczty elektronicznej – wydruk zawierał adres poczty elektronicznej odbiorcy, datę wysłania i odebrania wiadomości. Wobec spełnienia wymogu z art. 105a ust. 3 Prawa bankowego Prezes UODO uznał, że w sprawie nie doszło do nieprawidłowości[74].

W innej z rozpatrywanych spraw bank wskazał, że obowiązek poinformowania, o którym mowa w ww. przepisie, spełnił poprzez skierowanie do osoby skarżącej wiadomości e-mail z oświadczeniem o wypowiedzeniu umowy, zawierającej informację o przetwarzaniu danych osobowych bez jej zgody w trybie art. 105a ust. 3 Prawa bankowego, która została nadana i doręczona na adres e-mail podany przez osobę skarżącą w innej umowie. Podobnie jak w poprzednim przypadku na podstawie przedstawionego wydruku można było ustalić datę wysłania i doręczenia ww. wiadomości. Również w tym przypadku w umowie bank pozyskał ponadto zgodę osoby skarżącej na prowadzenie działań monitorująco – upominawczych między innymi wysłanych wiadomości głosowych/sms/e-mail na podane w umowie numery telefonów oraz adresy e-mail. Jednakże adres e-mail, na który wysłano ww. wiadomość, nie był podanym w umowie przez osobę skarżącą adresem do kontaktu. W umowie nie wskazała ona żadnego adresu e-mail do kontaktu z bankiem. W związku z powyższym, wobec wysłania oświadczenia o wypowiedzeniu przedmiotowej umowy wraz z informacją o zamiarze przetwarzania danych ww. osoby na podstawie art. 105a ust. 3 Prawa bankowego pocztą elektroniczną na adres podany w innej umowie, nie można uznać, że doszło do skutecznego doręczenia tej osobie ww. informacji[75].

Przy ocenie realizacji ww. obowiązku informacyjnego przez administratora Prezes UODO uwzględniał również zachowanie należytej staranności przy próbie poinformowania podmiotu danych o zamiarze przetwarzania jego danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego.

W jednej z rozpatrywanych spraw bank wyjaśnił, że jest uprawniony do przetwarzania danych na ww. podstawie prawnej pomimo braku odbioru przez podmiot danych przesyłki zawierającej informacje, o której mowa w przedmiotowym przepisie. Prezes UODO stwierdził, rozpatrując tą sprawę, że zobowiązanie osoby skarżącej, wynikające z umowy zawartej z bankiem wygasło, a ww. osoba dopuściła się trwającej dłużej niż 60 dni zwłoki w spłacie ww. zobowiązania. Kluczową w tej sprawie okolicznością był fakt, że bank dopełnił wszelkiej staranności, by spełnić wobec ww. osoby obowiązek wynikający z art. 105a ust. 3 Prawa bankowego, tj. podjął wszelkie możliwe działania, by poinformować podmiot danych o zamiarze przetwarzania dotyczących go informacji stanowiących tajemnicę bankową, bez jego zgody po wygaśnięciu zobowiązania wynikającego z przedmiotowej umowy i przedłożył dowody na powyższe. Powiadomienie o zamiarze przetwarzania danych w celu oceny

[74] DS.523.2497.2023.
[75] DS.523.2996.2024.

zdolności kredytowej i analizy ryzyka kredytowego, o którym mowa w art. 105a ust 3 Prawa bankowego, musi być doręczone osobie zainteresowanej w taki sposób, by mogła zapoznać się z jego treścią.

Wezwanie do zapłaty przeterminowanego zadłużenia, wraz z informacją o konsekwencjach dalszego uchylania się od spłaty, zostało przez bank wysłane do dłużnika na adres wskazany w zawartej pomiędzy ww. stronami umowie. Bank zaznaczył, że przesyłka nie została podjęta przez podmiot danych z placówki pocztowej w terminie, pomimo podwójnego awizowania, a następnie została zwrócona do banku. Bank rozpoczął przetwarzanie danych skarżącego w odniesieniu do ww. umowy w oparciu o art. 105a ust. 3 Prawa bankowego z upływem okresu 30 dni od przyjęcia fikcji poinformowania osoby skarżącej o zamiarze przetwarzania informacji jej dotyczących bez jej zgody. Pismo, w którym bank spełnił obowiązek informacyjny wynikający z art. 105a ust. 3 Prawa bankowego, musi być doręczone osobie zainteresowanej w taki sposób, by mogła zapoznać się z jego treścią. Wyżej wymienione zawiadomienie bank nadał listem poleconym za zwrotnym potwierdzeniem odbioru na adres wskazany przez podmiot danych. Korespondencja nie została odebrana. Bank przedstawił dowód w postaci kopii koperty, na której widnieją daty podwójnego awizowania przesyłki.

Wobec powyższego Prezes UODO uznał, że bank spełnił wymogi określone w wyżej wymienionym przepisie Prawa bankowego, które upoważniały go do rozpoczęcia przetwarzania danych osobowych osoby skarżącej w oparciu o ww. przepis po wygaśnięciu zobowiązania. W ocenie Prezesa UODO w przedmiotowej sprawie zaistniała określona w art. 6 ust. 1 lit. f RODO przesłanka legalizująca proces przetwarzania danych osobowych osoby skarżącej przez bank w bazie instytucji utworzonej na podstawie art. 105 ust. 4 Prawa bankowego, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego przez okres 5 lat od daty wygaśnięcia zobowiązania. W ocenie Prezesa UODO przetwarzanie to następuje w tym przypadku w celach wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, a interesy podmiotu danych nie mają nadrzędnego charakteru[76].

Prezes UODO rozstrzygał również sprawy, w których oceniał możliwość przetwarzania danych na podstawie art. 105a ust. 1 Prawa bankowego, który uprawnia do przetwarzania danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego w trakcie istnienia zobowiązania przed jego wygaśnięciem[77]. Prezes UODO podkreślał w tego typu sprawach, że przetwarzanie danych osobowych na podstawie art. 105a ust. 1 Prawa bankowego nie wymaga zgody podmiotu danych[78].

Zgodnie natomiast z przesłanką wskazaną w art. 105a ust. 4 Prawa bankowego, stanowiące tajemnicę bankową informacje dotyczące osoby fizycznej mogą być przetwarzane po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją ustawowo upoważnioną do udzielania kredytów bez

[76] DS.523.8168.2021.
[77] DS.523.2079.2021.
[78] DS.523.2178.2022.

zgody osoby, której informacje dotyczą, do celów stosowania metod wewnętrznych oraz innych metod i modeli, o których mowa w części trzeciej rozporządzenia CRR[79]. Prezes UODO orzekał o dopuszczalności przetwarzania danych osobowych po wygaśnięciu umowy na podstawie ww. przepisu[80].

Prezes UODO rozpatrywał także skargę w której podmiot danych kwestionował możliwość przetwarzania na podstawie art. 105a Prawa bankowego danych poręczycieli weksla. W sprawie tej ustalono, że odpowiedzialność osoby skarżącej była ograniczona do określonej kwoty. Prezes UODO przywołując przepisy Prawa bankowego (w szczególności art. 105 ust. 1 i 4 Prawa bankowego), a także przepisy art. 31 zd. 1 oraz art. 32 zd. 1 Prawa wekslowego[81], stanął na stanowisku, że art. 105a Prawa bankowego ma również zastosowanie do przetwarzania danych poręczycieli wekslowych[82].

### Zapytania kredytowe

Podobnie jak w latach poprzednich, Prezes UODO rozpoznawał skargi wniesione na przetwarzanie danych osobowych w zakresie wynikającym z **zapytań kredytowych** niezakończonych zawarciem umowy. Zapytania kredytowe składane są przez kredytodawców do instytucji utworzonej na podstawie art. 105 ust. 4 Prawa bankowego, zwanej również „biurem informacji kredytowej". Co do zasady podstawą prawną przetwarzania danych osobowych klientów w bazie ww. instytucji może być obecnie art. 6 ust. 1 lit. f RODO, gdy przetwarzanie to jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Skarżone podmioty (kredytodawcy oraz biuro informacji kredytowej) wskazywały liczne cele i podstawy prawne, które w ich ocenie legalizowały proces przetwarzania danych osobowych wynikających z zapytań kredytowych, które nie zakończyły się zawarciem umowy kredytu, takie jak:

- art. 105a ust. 1 Prawa bankowego,
- art. 105a ust. 4 Prawa bankowego,
- art. 70 ust. 1 Prawa bankowego,
- przepisy rozporządzenia CRR (takie jak: art. 144 ust. 1 lit. d, art. 145 ust. 1, art. 147 ust. 5 lit. b art. 171 ust. 2 CRR),
- rekomendacje Komisji Nadzoru Finansowego,
- art. 106d Prawa bankowego,
- przepisy ustawy AML[83],
- ustalenie, dochodzenie lub obrona ewentualnych roszczeń,
- rozpatrywanie ewentualnych reklamacji,

[79] Rozporządzenie Parlamentu Europejskiego i Rady nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz. Urz. UE L 2013 Nr 176, str. 1), dalej także: CRR.
[80] DS.523.2079.2021.
[81] Ustawa z dnia 28 kwietnia 1936 r. Prawo wekslowe (Dz. U. z 2022 r. poz. 282).
[82] DS.523.2079.2021.
[83] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644), zwana dalej także: AML.

- art. 70a Prawa bankowego w brzmieniu sprzed nowelizacji z 29 września 2023 r.

Odnosząc się do ww. podstaw i celów przetwarzania, Prezes UODO nie podzielał stanowiska kredytodawców i biur informacji kredytowej, że wskazane wyżej podstawy prawne i cele mogą przesądzać o legalności procesu przetwarzania danych osobowych wynikających z zapytań kredytowych, które nie skutkowały zawarciem umowy kredytu.

W ocenie Prezesa UODO przetwarzanie danych osobowych, wynikających z takich zapytań znajdowało oparcie w art. 106d Prawa bankowego w celu wykonywania obowiązków w zakresie określonym w przepisach AML w przypadku, gdy w związku z zapytaniami doszło do nawiązania stosunków gospodarczych z klientem[84]. W jednej ze spraw Prezes UODO uznał także, że podstawą prawną, legalizującą proces przetwarzania danych osobowych w zakresie wynikającym z zapytania kredytowego zakończonego zawarciem umowy kredytu, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, jest art. 105a ust. 1 Prawa bankowego z uwagi na powstałe i istniejące zobowiązanie, co warunkuje możliwość oparcia procesu przetwarzania danych stanowiących tajemnicę bankową o ww. przepis[85].

W zakresie procesu przetwarzania danych osobowych prowadzonego na podstawie art. 70a Prawa bankowego, Prezes UODO ustalał datę pozyskania danych osobowych wynikających z zapytania kredytowego. W przypadku, gdy dla danego zapytania kredytowego znajdował zastosowanie art. 70a Prawa bankowego w poprzednim brzmieniu, który nie przewidywał żadnego terminu na złożenie wniosku o udzielenie informacji dotyczących odmowy udzielenia kredytu, Prezes UODO w decyzjach podkreślał, że brak wskazania ww. terminu nie oznacza, że dane osobowe można przetwarzać bezterminowo, gdyż byłoby to sprzeczne z zasadą ograniczenia przechowywania, określoną w art. 5 ust. 1 lit. e RODO. Obecnie, po nowelizacji ustawy Prawo bankowe, taki termin na złożenie wniosku został przewidziany[86].

Pozytywnie należy ocenić również działanie instytucji utworzonej na podstawie art. 105 ust. 4 Prawa bankowego, która zaczęła zwracać się do podmiotów dokonujących zapytań kredytowych do jej bazy z pytaniem, czy zapytania te zakończyły się zawarciem umowy kredytu, czy też nie. W przypadku uzyskania odpowiedzi przeczącej, ww. instytucja usuwała samodzielnie dane osobowe w zakresie zapytania kredytowego[87].

**Przetwarzanie danych osobowych w związku ze współpracą banków z zakładami ubezpieczeń w formie „bancassurance"**

W jednej z rozpatrywanej spraw Prezes UODO stwierdził nieprawidłowości w procesie przetwarzania danych klientów banku w związku ze współpracą banku

[84] DS.523.1483.2022.
[85] DS.523.6941.2021.
[86] DS.523.6007.2023.
[87] DS.440.137.2019.

z zakładem ubezpieczeniowym w formie hybrydowego typu świadczeń banków, tzw. **„bancassurance”.** Bank może wstępować jako ubezpieczający, który zawiera umowę ubezpieczenia na rachunek swoich klientów jako ubezpieczonych lub też jest pośrednikiem ubezpieczeniowym na podstawie umowy agencyjnej między bankiem a ubezpieczycielem. Pojęcie „bancassurance” nie ma definicji ustawowej. W ramach ww. współpracy udział brał podmiot trzeci, który na rzecz banku świadczył usługi w zakresie prowadzenia call center.

Prezes UODO zauważył, że katalog czynności bankowych został wskazany w art. 5 Prawa bankowego, jednakże zgodnie z art. 6 tego aktu, banki uprawnione są również do podejmowania innej działalności, w tym mogą świadczyć inne usługi finansowe (art. 6 ust. 1 pkt 7) lub też wykonywać inne czynności, jeżeli przepisy odrębnych ustaw uprawniają je do tego (art. 6 ust. 1 pkt 8). W kontekście powyższego Prezes UODO zauważył, że zgodnie z definicją ustawową zawartą w art. 3 ust. 1 pkt 2 ustawy o dystrybucji ubezpieczeń[88] poprzez „agenta ubezpieczeniowego” należy rozumieć przedsiębiorcę innego niż agent oferujący ubezpieczenia uzupełniające, wykonującego działalność agencyjną na podstawie umowy agencyjnej zawartej z zakładem ubezpieczeń i wpisanego do rejestru agentów. Jak stanowi art. 21 ust. 1 d.u. zakład ubezpieczeń udziela agentowi ubezpieczeniowemu oraz agentowi oferującemu ubezpieczenia uzupełniające upoważnionym do zawierania w jego imieniu umów ubezpieczenia lub umów gwarancji ubezpieczeniowych, w formie pisemnej, pod rygorem nieważności, pełnomocnictw do dokonywania czynności agencyjnych w imieniu tego zakładu. W toku postępowania bank wykazał, że zostało mu udzielone przez zakład ubezpieczeniowy pełnomocnictwo w formie pisemnej, uprawniające do wykonywania w imieniu i na rzecz zakładu ubezpieczeniowego czynności pośrednictwa ubezpieczeniowego w zakresie ryzyk ubezpieczeniowych określonych w grupach 1-5 działu I załącznika do u.d.u.r.[89] polegających na m.in. wykonywaniu czynności przygotowawczych zmierzających do zawierania oferowanych przez zakład umów ubezpieczenia. Bank jest również wpisany do rejestru agentów.

Bank oraz zakład ubezpieczeń zawarły również umowę o współpracy, której przedmiotem była współpraca stron w zakresie administrowania umowami grupowego ubezpieczenia na życie. W powyższej umowie zakład ubezpieczeń zobowiązał się zapewnić na własny koszt wyspecjalizowane zasoby w zakresie outsourcingu call center/contact center. Wyniku powyższego bank, towarzystwo oraz trzeci podmiot zawarły następnie umowę o świadczenie usług, na mocy której ww. trzeci podmiot zobowiązał się do świadczenia na rzecz banku usług polegających na sprzedaży ubezpieczeń, których celem było przedstawienie klientom banku informacji o warunkach ubezpieczenia związanego z zabezpieczeniem ryzyka banku wynikającego z oferowanych przez bank usług klientom banku wspólnie z zakładem

[88] Ustawa z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń (Dz. U. z 2026 r. poz. 12), zwana dalej także: d.u.

[89] Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2025 r. poz. 1526), zwana także: u.d.u.r.

ubezpieczeń. Zgodnie z ww. umową usługi w tym zakresie świadczone były wyłącznie na rzecz banku na podstawie danych przekazanych przez bank.

Prezes UODO uznał w tej sprawie, że ww. dane osoby skarżącej, którymi posłużył się bank, działając jako agent ubezpieczeniowy, pozyskane zostały w związku z zawartymi przez bank z ww. osobą umowami o produkty bankowe i stanowiły tajemnicę bankową, do ujawnienia której bank nie posiadał upoważnienia skarżącego spełniającego wymogi z art. 104 ust. 3 Prawa bankowego. W konsekwencji powyższych ustaleń Prezes UODO uznał, że proces przetwarzania polegający na udostępnieniu przez bank danych osobowych skarżącego na rzecz towarzystwa nie znajdował oparcia w żadnej z przesłanek z art. 6 ust. 1 RODO i udzielił bankowi upomnienia[90].

### Przekazanie danych osobowych przez bank na rzecz podmiotu przetwarzającego w ramach outscourcingu bankowego dotyczącego czynności faktycznych zabezpieczenia kredytów

W jednej ze spraw Prezes UODO ocenił przekazanie danych przez bank celem dokonywania **monitoringu ubezpieczeń** stanowiących zabezpieczenie spłat kredytów i pożyczek. Prezes UODO zauważył, że umowa ubezpieczenia stanowi jedną z form zabezpieczenia kredytu, w której zakład ubezpieczeń zobowiązuje się do zapłacenia bankowi określonego w umowie odszkodowania za szkody poniesione przez bank spowodowane niespłaceniem kredytu. Prezes UODO ustalił, że powyższe nastąpiło na podstawie umowy powierzenia, o której mowa w art. 28 ust. 3 RODO. Jednocześnie Prezes UODO przywołał przepisy Prawa bankowego, które regulują outsourcing bankowy. Zgodnie bowiem z art. 6a ust. 1 pkt 1 i 2 Prawa bankowego, bank może, w drodze umowy zawartej na piśmie, powierzyć przedsiębiorcy lub przedsiębiorcy zagranicznemu, z zastrzeżeniem art. 6d, wykonywanie w imieniu i na rzecz banku pośrednictwa w zakresie określonych czynności wymienionych w art. 5 i 6 oraz czynności faktycznych związanych z działalnością banku. Natomiast jak stanowi art. 104 ust. 2 lit. a Prawa bankowego obowiązek przestrzegania tajemnicy bankowej, o którym mowa w art. 104 ust. 1, nie dotyczy przypadków, w których następuje ujawnienie informacji objętych tajemnicą bankową przedsiębiorcom lub przedsiębiorcom zagranicznym przez bank, gdy zgodnie z art. 6a ust. 1 powierzył on im wykonywanie, stale lub okresowo, czynności związanych z działalnością bankową. W świetle art. 6a ust. 1 pkt 1 lit. m Prawa bankowego należy wskazać, że outsourcing bankowy w zakresie czynności faktycznych związanych z działalnością banku nie wymaga zezwolenia Komisji Nadzoru Finansowego. Prezes UODO stanął na stanowisku, że bank mógł powierzyć innemu podmiotowi dane w celach realizacji ww. czynności faktycznych związanych z zabezpieczeniem kredytu[91].

### Przekazywanie kopii danych zawartych w nagraniu rozmowy telefonicznej przez banki w ramach realizacji prawa dostępu

[90] ZSPR.440.1500.2018.
[91] DS.523.934.2020.

Podobnie jak latach poprzednich również w aktualnym roku sprawozdawczym Prezes UODO rozpatrywał skargi wniesione na odmowę banku wydania na podstawie art. 15 ust. 3 RODO kopii danych osobowych zawartych w nagraniu rozmowy telefonicznej.

W jednej z rozpatrywanych spraw bank zamiast przekazać kopię danych poinformował wnioskującego o możliwości odsłuchania rozmowy w placówce banku. Prezes UODO przede wszystkim wskazał, że administrator realizując obowiązek wynikający z art. 15 ust. 3 RODO może poprzestać na wskazaniu treści danych dotyczących osoby, z wyłączeniem pozostałych utrwalonych informacji. Wykonanie obowiązku określonego w art. 15 ust. 3 RODO może być realizowane zarówno poprzez sporządzenie kopii lub odpisu nośnika (dokumentu lub nagrania) zawierającego dane osobowe oraz inne dane, jak i poprzez podanie uprawnionemu treści jego danych osobowych, z pominięciem informacji znajdujących się w nośniku, które nie są danymi osobowymi w rozumieniu art. 4 pkt 1 RODO. W przypadku zwrócenia się do administratora o kopię przetwarzanych danych osobowych, administrator każdorazowo podejmuje decyzję, w jaki sposób zrealizuje to uprawnienie. W przypadku danych osobowych utrwalonych na nagraniu, administrator może dokonać wyboru, czy udostępni kopię nagrania, czy też udostępni kopię danych zawartych w tym nagraniu. Przy realizacji obowiązku wynikającego z art. 15 ust. 3 RODO administrator musi również mieć na uwadze dodatkowo kontrolę nad zakresem przekazywanych kopii danych osobowych, co zostało wyrażone w treści motywu 63 RODO oraz art. 15 ust. 4 RODO.

Materiał dowodowy potwierdził w tej sprawie fakt zwrócenia się do banku przez osobę skarżącą z wnioskiem o udostępnienie jej kopii jej danych osobowych zawartych w nagraniu rozmowy telefonicznej. Bank nie zrealizował wniosku osoby skarżącej, tylko wskazał na możliwość odsłuchu nagrania w jego placówce. Prezes UODO podkreślił, że umożliwienie odsłuchania nagrania nie jest równoznaczne z wykonaniem ciążącego na administratorze obowiązku dostarczeniem osobie, której dane dotyczą kopii jej danych osobowych, a zatem z realizacją jej prawa z art. 15 ust. 3 RODO.

Prezes UODO podkreślił, że niewdrożenie przez bank odpowiednich środków technicznych, zapewniających ochronę praw i wolności, czy też danych osobowych innych osób, utrwalonych na nagraniach rozmowy telefonicznej nie stanowi podstawy do odmowy realizacji prawa skarżącej wskazanego w art. 15 ust. 3 RODO. W konsekwencji Prezes UODO nakazał bankowi spełnienie żądania osoby skarżącej[92].

### Udostępnienie przez ubezpieczyciela nagrania z monitoringu dokumentującego wypadek

W jednej ze spraw prowadzonych przez Prezesa UODO osoba, której dane dotyczą, powołując się na art. 15 ust. 3 RODO domagała się od ubezpieczyciela udostępnienia nagrania z **monitoringu** dokumentującego jej wypadek. Mimo wielokrotnych wniosków i powołania się na prawo dostępu do danych, skarżona spółka

[92] DS.523.7588.2024.

kilkakrotnie jednak odmówiła wydania nagrania z uwagi na wizerunek osób trzecich oraz brak zgody na ich przekazywanie. Ostatecznie spółka udostępniła sporną część akt szkodowych skarżącej. W decyzji Prezes UODO wskazał, że uprawnienie uczestnika postępowania ubezpieczeniowego do akt sprawy regulują przepisy ustawy o działalności ubezpieczeniowej i reasekuracyjnej[93]. Zgodnie z art. 29 ust. 6 u.d.u.r. zakład ubezpieczeń udostępnia ubezpieczającemu, ubezpieczonemu, osobie występującej z roszczeniem lub uprawnionemu z umowy ubezpieczenia informacje i dokumenty gromadzone w celu ustalenia odpowiedzialności zakładu ubezpieczeń lub wysokości odszkodowania lub świadczenia. Osoby te mogą żądać pisemnego potwierdzenia przez zakład ubezpieczeń udostępnionych informacji, a także sporządzenia na swój koszt kserokopii dokumentów i potwierdzenia ich zgodności z oryginałem przez zakład ubezpieczeń. Tym samym Prezes UODO uznał, że nie posiada kompetencji do orzekania w sprawach dotyczących postępowań odszkodowawczych. W ocenie Prezesa UODO wniosek dotyczył wyłącznie dostępu do akt szkodowych osoby skarżącej jako uczestnika postępowania szkodowego i tego typu żądanie nie może zostać ocenione jako żądanie z art. 15 ust. 3 RODO[94]. Niemniej jednak w treści wniosku osoba skarżąca jako podstawę swojego żądania wskazała art. 15 ust. 3 RODO. Wobec tego spółka, jako administrator danych, odmawiając jego realizacji, obowiązana była poinformować podmiot danych o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem, stosownie do przepisu art. 12 ust. 4 RODO w terminie miesiąca od dnia otrzymania tego wniosku. Spółka zaniechała jednak udzielenia jakiejkolwiek odpowiedzi na powyższy wniosek, dlatego Prezes UODO udzielił jej upomnienia.

**Ujawnienie danych o stanie zdrowia w tytule przelewu bankowego**

Kolejnym zagadnieniem w praktyce orzeczniczej Prezesa UODO była kwestia przestrzegania zasady minimalizacji danych przy dokonywaniu operacji bankowych. W badanej sprawie Prezes UODO stwierdził naruszenie przepisów przez ubezpieczyciela, który w tytule przelewu świadczenia skierowanego do skarżącego zawarł szczegółową diagnozę medyczną o treści: „Nowotwór złośliwy”. Prezes UODO uznał, że takie działanie doprowadziło do udostępnienia danych szczególnych kategorii osobom nieuprawnionym (pracownikom banku) bez właściwej podstawy prawnej. W toku postępowania Prezes UODO wykluczył zaistnienie którejkolwiek z przesłanek legalizujących proces przetwarzanie tego rodzaju danych osobowych zawartych w art. 9 ust. 2 RODO i uznał, że przetwarzanie danych o zdrowiu w tytule płatności nie było niezbędne do dochodzenia roszczeń ani nie opierało się na zgodzie klienta. Za nietrafną uznano argumentację spółki o konieczności rozróżniania ryzyk ubezpieczeniowych w systemie, podnosząc, że tytuł przelewu ma służyć jedynie identyfikacji wpłaty, a nie powielać treść merytorycznej decyzji, którą skarżący

[93] Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2025 r. poz.1526), dalej także: u.d.u.r.
[94] DS.523.6457.2023.

otrzymał osobnym kanałem komunikacji. W tej sprawie doszło do złamania zasady minimalizacji z art. 5 ust. 1 lit. c RODO, co potwierdziła również autorefleksja administratora, który zadeklarował usunięcie nazw ryzyk z systemów informatycznych[95].

**Bezprawne przetwarzanie danych po ustaniu celu i nadmiarowa retencja danych wynikających z dokumentów tożsamości**

W postępowaniach dotyczących sektora telekomunikacyjnego Prezes UODO poddawał ocenie m.in. legalność długotrwałego przetwarzania szerokiego katalogu danych abonentów (w tym numeru PESEL, danych lokalizacyjnych oraz skanów dokumentów tożsamości) po rozwiązaniu umowy. W jednej ze spraw skarżona spółka wywodziła uprawnienie do retencji danych, powołując się na realizację obowiązków podatkowych (art. 6 ust. 1 lit. c RODO) oraz dochodzenie roszczeń (art. 6 ust. 1 lit. f RODO). Organ nadzorczy, weryfikując te twierdzenia, ustalił jednak istotne sprzeczności w wyjaśnieniach administratora. Choć spółka wskazywała na operację finansową z 2019 r., jako moment rozpoczęcia biegu przedawnienia podatkowego, nie potrafiła wyjaśnić jej charakteru, podczas gdy pełna spłata zadłużenia w toku egzekucji komorniczej nastąpiła już 15 września 2016 r. W konsekwencji Prezes UODO uznał, że okres przedawnienia zobowiązań podatkowych wynikający z art. 70 § 1 Ordynacji podatkowej[96] upłynął z końcem 2021 r., co czyniło dalsze przetwarzanie danych bezprawnym.

Organ nadzorczy zakwestionował możliwość opierania procesu przetwarzania na przepisach Prawa telekomunikacyjnego[97] (m.in. art. 60b i art. 180a), które weszły w życie w 2008 r. już po rozwiązaniu umowy z osobą, której dane dotyczą, ponieważ przepisy te nie mogły stanowić podstawy prawnej działań administratora. Odrzucił również argumentację dotyczącą przetwarzania danych w celu obrony przed ewentualnymi roszczeniami na podstawie art. 6 ust. 1 lit. f RODO. Przywołując orzecznictwo Naczelnego Sądu Administracyjnego[98], Prezes UODO podkreślił, że niedopuszczalne jest gromadzenie danych „na zapas" w oczekiwaniu na niepewne roszczenia przyszłe. Przyjęcie odmiennej interpretacji prowadziłoby do permanentnego i nieograniczonego czasowo przetrzymywania danych osobowych, co naruszałoby istotę ochrony gwarantowanej przez RODO.

Osobną kategorię naruszeń stanowiło przechowywanie przez spółkę kserokopii dowodu osobistego oraz paszportu skarżącej. Prezes UODO stwierdził, że żadna z przywołanych przez administratora podstaw prawnych (w tym art. 118 K.c. czy przepisy podatkowe) nie przewidywała obowiązku ani nawet dopuszczalności wykonywania kopii dokumentów tożsamości w analizowanym celu. Działanie to uznano za naruszające zasadę minimalizacji oraz brak wykazania niezbędności takiego procesu, co w połączeniu z przekroczeniem terminów retencji skutkowało

[95] DS.523.6437.2024.
[96] Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz. U. z 2025 r. poz. 111).
[97] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34).
[98] Naczelny Sąd Administracyjny w wyroku z 6 marca 2019 r. sygn. akt I OSK 994/17.

stwierdzeniem naruszenia przepisów o ochronie danych osobowych do momentu faktycznego usunięcia danych z systemów skarżonej spółki[99].

### Udostępnienie danych osobowych wskutek błędnego adresowania korespondencji tradycyjnej

W praktyce orzeczniczej Prezesa UODO istotne miejsce zajmują sprawy dotyczące naruszenia poufności danych wynikające z błędów organizacyjnych przy **wysyłce korespondencji.** W jednej ze spraw organ nadzorczy stwierdził, że skarżona spółka wielokrotnie kierowała pisma do osoby skarżącej na nieprawidłowe adresy, co było skutkiem omyłek pisarskich pracowników oraz bezkrytycznego korzystania z nieaktualnych danych w systemach informatycznych. Prezes UODO uznał, że administrator ustalił adres osoby skarżącej w sposób dowolny, ignorując fakt, że komunikacja ze strony poszkodowanego odbywała się wyłącznie drogą elektroniczną. W ocenie organu, skarżona spółka naruszyła obowiązki wynikające z art. 24 ust. 1 RODO, nie wdrażając odpowiednich środków technicznych i organizacyjnych, które zapewniłyby weryfikację prawidłowości danych adresowych przed wysyłką. Takie zaniedbanie doprowadziło do udostępnienia danych osobowych osoby skarżącej (imienia i nazwiska na kopertach) osobom nieuprawnionym bez jakiejkolwiek przesłanki legalizującej z art. 6 ust. 1 RODO. W konsekwencji, na podstawie art. 58 ust. 2 lit. b RODO, Prezes UODO zastosował wobec skarżonego podmiotu upomnienie[100].

### Legalność dalszego przetwarzania danych osobowych po wygaśnięciu umowy ubezpieczenia OC

W ramach zakresu spraw dotyczących sektora ubezpieczeniowego, Prezes UODO rozstrzygał kwestię dopuszczalności dalszego przetwarzania danych osobowych przez zakład ubezpieczeń w sytuacji, gdy umowa ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych uległa już rozwiązaniu. W badanej sprawie skarżący domagał się usunięcia swoich danych na podstawie art. 17 ust. 1 RODO argumentując, że ochrona ubezpieczeniowa wygasła 14 czerwca 2023 r. Towarzystwo odmówiło realizacji żądania, wskazując na konieczność zabezpieczenia dokumentacji na wypadek ujawnienia się szkód z czynów niedozwolonych, które mogą zostać zgłoszone po zakończeniu okresu ochrony. Organ nadzorczy, analizując zasadność odmowy, przywołał przepisy szczególne zawarte przepisach u.d.u.r. Zgodnie z art. 29 ust. 6 i 10 tej ustawy, zakład ubezpieczeń jest ustawowo zobowiązany do przechowywania informacji i dokumentów gromadzonych w celu ustalenia odpowiedzialności oraz wysokości odszkodowania do czasu upływu terminu przedawnienia roszczeń. Prezes UODO wskazał, że terminy te wynikają z Kodeksu cywilnego i wynoszą standardowo trzy lata od dnia dowiedzenia się o szkodzie (art. $442^1$ § 1 K.c.), dziesięć lat od zdarzenia, a w przypadku, gdy szkoda wynikła z przestępstwa – dwadzieścia lat od dnia jego popełnienia (art. $442^2$ § 1 K.c.).

[99] DS.523.1588.2021.
[100] DS.523.4170.2020.

W świetle powyższych ustaleń organ uznał, że przetwarzanie danych skarżącego jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, co stanowi przesłankę legalizującą z art. 6 ust. 1 lit. c RODO. Jednocześnie podkreślono, że w ustalonym stanie faktycznym znajduje zastosowanie wyłączenie z art. 17 ust. 3 lit. b RODO, które wprost wskazuje, że prawo do usunięcia danych nie przysługuje, gdy przetwarzanie jest niezbędne do wywiązania się z obowiązku prawnego nałożonego na administratora przez prawo państwa członkowskiego. Prezes UODO stwierdził, że zakład ubezpieczeniowy postąpił więc prawidłowo, odmawiając usunięcia danych, gdyż ich retencja w celu zapewnienia realizacji przyszłych roszczeń i ochrony tajemnicy ubezpieczeniowej jest wymogiem ustawowym[101].

**Niewłaściwa weryfikacja tożsamości jako przyczyna odmowy realizacji prawa do bycia zapomnianym przez podmioty sektora ubezpieczeniowego i telekomunikacyjnego**

W obszarze orzeczniczym Prezesa UODO istotnym zagadnieniem pozostaje usuwanie barier proceduralnych utrudniających osobom fizycznym wykonywanie ich praw na podstawie RODO. W analizowanej sprawie organ nadzorczy oceniał działania spółki (działającej jako dostawca usług telekomunikacyjnych), która odmówiła realizacji telefonicznego żądania skarżącej o usunięcie numeru kontaktowego, powołując się na brak możliwości skutecznej weryfikacji jej tożsamości. Prezes UODO uznał taką argumentację za bezzasadną, podkreślając, że przepisy RODO nie wykluczają zgłaszania żądań drogą telefoniczną, a administrator ma obowiązek wdrożenia procedur ułatwiających realizację uprawnień osób, których dane dotyczą, wynikających z RODO. Organ ustalił, że w trakcie spornej rozmowy pracownik spółki nie podjął próby pozyskania dodatkowych informacji niezbędnych do potwierdzenia tożsamości, mimo że administrator dysponował pełnym zestawem danych klientki zawartych w umowie. Co więcej, niespójność postawy spółki potwierdził fakt, że podczas kolejnej rozmowy w marcu 2024 r. to samo żądanie zostało przyjęte bez żadnych zastrzeżeń co do tożsamości dzwoniącej. Prezes UODO wskazał, że skoro spółka wielokrotnie kontaktowała się ze skarżącą na ten konkretny numer przypisany do jej konta abonenckiego, nie sposób uznać, że istniały obiektywne i uzasadnione wątpliwości uniemożliwiające identyfikację rozmówcy już przy pierwszym zgłoszeniu. W konsekwencji organ stwierdził, że choć spółka ostatecznie usunęła numer telefonu w kwietniu 2024 r., uczyniła to z naruszeniem art. 17 ust. 1 w zw. z art. 12 ust. 3 RODO. Administrator uchybił obowiązkowi niezwłocznego usunięcia danych oraz zachowania miesięcznego terminu na poinformowanie osoby o podjętych działaniach. Prezes UODO podkreślił, że brak pewności co do tożsamości może uzasadniać prośbę o podanie dodatkowych informacji, ale nie może stanowić automatycznej bariery dla realizacji praw podmiotu danych, zwłaszcza gdy administrator posiada środki pozwalające na natychmiastową weryfikację klienta w toku interakcji telefonicznej[102].

[101] DS.523.4233.2023.
[102] DS.523.2360.2024.

W innej sprawie rozpatrywanej w 2025 r. stan faktyczny wykazał, że osoba skarżąca w październiku 2022 r. zwróciła się do administratora o podanie szczegółowych informacji o celach, zakresie, źródle oraz odbiorcach swoich danych. Spółka w pierwszej kolejności odmówiła realizacji wniosku, twierdząc, że podane przez ww. osobę imię, nazwisko oraz adres są niewystarczające do jednoznacznej identyfikacji osoby w jej systemach. Organ nadzorczy uznał powyższą odmowę za bezpodstawną i stanowiącą nieuzasadnione utrudnianie realizacji praw podmiotu danych. Przywołując art. 12 ust. 3 RODO, Prezes UODO podkreślił, że ewentualne wątpliwości administratora co do tożsamości wnioskodawcy muszą mieć charakter uzasadniony. W sytuacji, gdy wnioskujący podał komplet podstawowych danych identyfikacyjnych, a spółka dysponowała w swojej bazie m.in. jego numerem telefonu powiązanym z konkretnym adresem IP, odmowa udzielenia informacji na tym etapie była działaniem nieprawidłowym. Dalsza analiza wykazała, że udzielona po interwencji wnioskującego odpowiedź z grudnia 2022 r. była niepełna. Spółka ograniczyła się wówczas do wskazania jedynie danych kontaktowych, pomijając fakt przetwarzania informacji o modelach samochodów wykorzystywanych w kalkulacjach ubezpieczeniowych. Dopiero w styczniu 2023 r., po kolejnym wezwaniu ze strony skarżącego, administrator uzupełnił informację o wykaz przeprowadzonych kalkulacji oraz zakres danych im towarzyszących. Prezes UODO odniósł się również do twierdzenia spółki, jakoby dane o pojeździe stawały się danymi osobowymi dopiero po zawarciu polisy. Prezes UODO wskazał, że w kontekście korzystania z kalkulatora, dane te są ściśle powiązane z numerem telefonu i adresem IP użytkownika, co pozwala na jego identyfikację. W konsekwencji uznano, że spółka naruszyła przepisy o ochronie danych osobowych poprzez nieterminowe i etapowe udzielanie informacji, które powinny zostać przekazane w sposób pełny i przejrzysty już w odpowiedzi na pierwsze żądanie. Ostateczna realizacja wniosku nastąpiła z blisko trzymiesięcznym opóźnieniem, co wykracza poza ramy czasowe określone w art. 12 ust. 3 RODO[103].

**Status prawny adresu IP oraz terminowość realizacji prawa dostępu do danych przez operatora telekomunikacyjnego**

W jednym z przeprowadzonych postępowań z sektora telekomunikacyjnego Prezes UODO poddał analizie kwestię, czy dynamiczny numer IP stanowi dane osobowe, a w konsekwencji – czy użytkownik końcowy może skutecznie żądać wydania jego kopii na podstawie art. 15 ust. 3 RODO. W badanej sprawie spółka początkowo odmówiła skarżącym udostępnienia tych danych, argumentując, że adresy dynamiczne mają charakter tymczasowy, nie są archiwizowane, a operator nie ma prawnego obowiązku ich gromadzenia. Organ nadzorczy, odwołując się do definicji zawartej w art. 4 pkt 1 RODO oraz bogatego dorobku orzeczniczego Trybunału Sprawiedliwości Unii Europejskiej (m.in. sprawy C-582/14 i C-70/10) oraz Naczelnego Sądu Administracyjnego, jednoznacznie uznał to stanowisko za błędne.

[103] DS.523.6617.2022.

Prezes Urzędu podkreślił, że adres IP – nawet dynamiczny – stanowi dane osobowe, gdyż pozwala na pośrednią identyfikację osoby fizycznej, zwłaszcza z punktu widzenia dostawcy usług internetowych, który dysponuje narzędziami pozwalającymi powiązać numer IP z konkretną stroną umowy. Organ wskazał, że wbrew twierdzeniom spółki, obowiązek retencji takich danych przez okres 12 miesięcy wynikał wprost z przepisów art. 180a i 180c ustawy Prawo telekomunikacyjne oraz przepisów wykonawczych, które nakazują gromadzenie danych niezbędnych do ustalenia zakończenia sieci i użytkownika inicjującego połączenie, w tym właśnie adresów IP przypisanych do danej sesji.

Ujawniono, że skarżona spółka nie tylko bezzasadnie odmówiła realizacji wniosku, ale również wprowadziła skarżących w błąd, twierdząc, że danych tych nie przetwarza, by następnie – po wpłynięciu skargi do organu nadzorczego – ostatecznie je udostępnić. Prezes UODO stwierdził naruszenie art. 12 ust. 3 RODO, wskazując na brak zachowania miesięcznego terminu realizacji żądania oraz zaniechanie poinformowania strony o ewentualnym przedłużeniu terminu z uwagi na skomplikowany charakter sprawy. Organ zaznaczył, że administrator ma obowiązek wdrożenia takich rozwiązań technicznych, które umożliwią terminową realizację praw osób, których dane dotyczą, a trudności operacyjne czy konieczność przygotowania narzędzi informatycznych nie zwalniają z odpowiedzialności za terminową i rzetelną komunikację z wnioskodawcą[104].

**Relacja między przepisami Prawa telekomunikacyjnego a prawem dostępu do danych na podstawie RODO**

W jednym z postępowań Prezes UODO rozstrzygał kwestię zbiegu uprawnień abonenta wynikających z przepisów sektorowych oraz ogólnego rozporządzenia o ochronie danych. Skarżący zwrócił się do operatora o udostępnienie szczegółowego rejestru transferu danych (wielkość przesyłu w kB z dokładnością co do sekundy) w celu przeprowadzenia reklamacji. Wniosek został skierowany bezpośrednio do Inspektora Ochrony Danych (IOD) skarżonej spółki i zatytułowany jako żądanie udostępnienia danych osobowych. Spółka stanęła na stanowisku, że żądanie to nie stanowi wniosku opartego na RODO, lecz jest reklamacją rozpatrywaną wyłącznie na podstawie art. 80 ust. 1 ustawy Prawo telekomunikacyjne, który obliguje dostawcę do wydania szczegółowego wykazu wykonanych usług. Organ nadzorczy zakwestionował interpretację spółki, wskazując, że brzmienie przepisów Prawa telekomunikacyjnego w żaden sposób nie wyklucza możliwości skorzystania przez osobę, której dane dotyczą, z uprawnień przewidzianych w art. 15 ust. 3 RODO. Dane zawarte w bilingach i wykazach połączeń internetowych, jako informacje o aktywności konkretnego użytkownika, stanowią dane osobowe. Tym samym, jeśli osoba fizyczna wyraźnie formułuje żądanie jako „wniosek o udostępnienie danych osobowych” i kieruje go do IOD, administrator ma obowiązek rozpatrzyć go w trybie i na zasadach określonych w RODO. Pomimo błędnej kwalifikacji charakteru wniosku przez spółkę, Prezes UODO odmówił w tej sprawie uwzględnienia skargi. Ustalono bowiem, że choć

[104] DS.523.5899.2020.

skarżona spółka procedowała wniosek w trybie reklamacyjnym, to w odpowiedzi przekazała wnioskującemu pełen zakres żądanych informacji, którymi dysponowała (godziny połączeń wraz z ilością danych w kB)[105].

### Niedopuszczalność przetwarzania danych w celach marketingowych po wniesieniu sprzeciwu

W toku postępowań dotyczących **sektora ubezpieczeniowego** Prezes UODO rozstrzygał sprawę naruszenia przepisów RODO polegającego na kontynuowaniu działań marketingowych wobec klienta, który uprzednio skutecznie wniósł sprzeciw wobec takiego przetwarzania. Stan faktyczny wykazał, że mimo odnotowania w systemach spółki sprzeciwu z maja 2021 r., na polisie doręczonej skarżącemu w maju 2024 r. zamieszczono treści zachęcające do skorzystania z rabatów na inne produkty ubezpieczeniowe (m.in. ubezpieczenia turystyczne). Spółka argumentowała, że był to nadruk informacyjny, jednak organ nadzorczy odrzucił tę interpretację. Przyjmując linię orzeczniczą Naczelnego Sądu Administracyjnego[106] Prezes UODO wskazał, że za marketing należy uznać każdą informację o produktach, która podkreśla ich atrakcyjność i ma na celu nakłonienie odbiorcy do określonego działania lub wywołanie pozytywnych emocji wobec oferty. Zamieszczenie propozycji zniżek i zachęty do kontaktu z agentem w celu uzyskania kodu rabatowego wypełnia znamiona marketingu bezpośredniego, a nie czystej informacji technicznej związanej z obsługą zawartej już umowy. W konsekwencji organ uznał, że działanie spółki było niedopuszczalne i nie znajdowało oparcia w żadnej z przesłanek legalizujących z art. 6 ust. 1 RODO[107].

### Naruszenie zasady minimalizacji danych przy zawieraniu umów o świadczenie usług komunikacji elektronicznej

Prezes UODO poddał analizie legalność pozyskiwania i przechowywania serii oraz numeru dowodu osobistego abonenta. Spółka wywodziła, że gromadzenie tych danych jest niezbędne do weryfikacji tożsamości klienta, zawarcia umowy oraz późniejszego dochodzenia ewentualnych roszczeń. Administrator powoływał się przy tym na ogólne przesłanki z art. 6 ust. 1 RODO oraz przepisy sektorowe. Prezes UODO ustalił, że zarówno dawne przepisy Prawa telekomunikacyjnego (art. 60b), jak i obecnie obowiązujące Prawo komunikacji elektronicznej (art. 296 ust. 1), obligują abonenta będącego osobą fizyczną jedynie do podania imienia, nazwiska oraz numeru PESEL (a w przypadku jego braku, do podania serii i numeru dokumentu). W analizowanym stanie faktycznym umowa została doręczona przez kuriera, który dokonał fizycznej weryfikacji tożsamości osoby skarżącej na podstawie okazanego dokumentu. Zdaniem organu samo potwierdzenie tożsamości przez upoważnionego przedstawiciela skarżonej spółki jest wystarczające do skutecznego zawarcia

[105] DS.523.5494.2020.
[106] Naczelny Sąd Administracyjny w wyroku z 5 grudnia 2018 r. o sygn. akt I OSK 53/17.
[107] DS.523.3778.2024.

kontraktu i nie generuje po stronie administratora uprawnienia do trwałego zapisywania i przechowywania serii oraz numeru dowodu w systemach.

Prezes UODO odrzucił argumentację skarżonej spółki, jakoby terminy przedawnienia roszczeń automatycznie legitymowały administratora do przetwarzania dowolnego zakresu danych przez cały okres ich biegu. Podkreślono, że przetwarzanie serii i numeru dowodu osobistego „na zapas" stoi w sprzeczności z obowiązkiem ograniczania zbieranych informacji do minimum. W konsekwencji organ uznał, że spółka nie wykazała niezbędności tych danych do realizacji prawnie uzasadnionych interesów, co skutkowało stwierdzeniem naruszenia art. 5 ust. 1 lit. c RODO oraz brakiem podstaw legalizujących w art. 6 ust. 1 RODO. Rozstrzygnięcie to potwierdza, że administratorzy nie mogą gromadzić danych z dokumentów tożsamości w sposób szerszy, niż wymagają tego konkretne przepisy prawa lub obiektywna konieczność techniczna[108].

### 5.4. Sektor zdrowia, zatrudnienia i szkolnictwa

#### Uzyskiwanie przez lekarzy nieuprawnionego dostępu do danych osobowych przetwarzanych na PUE ZUS

Podobnie jak w latach ubiegłych, Prezes UODO rozpatrywał w 2025 r. liczne skargi na nieuprawnione przetwarzanie zgromadzonych na **Platformie Usług Elektronicznych Zakładu Ubezpieczeń Społecznych**[109] danych osobowych przez lekarzy. Dostęp lekarzy do PUE ZUS polega na tym, że lekarz logując się do PUE ZUS pacjenta celem wystawienia zwolnienia lekarskiego wprowadza w wyszukiwarkę numer PESEL. Następnie system prezentuje osobie mającej dostęp do systemu dane osobowe ubezpieczonego. Możliwość przeglądania danych osobowych osób objętych ubezpieczeniem społecznym przez lekarzy może prowadzić do nadużyć, ponieważ znacząca liczba lekarzy, na których wnoszone są skargi, zdaje się działać w błędnym przeświadczeniu, jakoby samo posiadanie uprawnień do uzyskania dostępu do danych osób znajdujących się na PUE ZUS wystarczyło dla prawidłowego uzasadnienia korzystania z tego dostępu w celach innych niż wystawienie zwolnienia lekarskiego.

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 przepisów RODO.

Z praktyki orzeczniczej Prezesa UODO wynika, że często lekarze korzystają zbyt swobodnie z posiadanych uprawnień dostępu do danych znajdujących się na PUE ZUS, realizując w ten sposób własne cele niemające związku z wykonywaniem działalności leczniczej. Lekarze często pozyskują w ten sposób 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.

[108] DS.523.2656.2021.
[109] Platforma Usług Elektronicznych Zakładu Ubezpieczeń Społecznych, dalej także: PUE ZUS.

W sprawach dotyczących ww. kwestii lekarze często uzasadniali nieuprawniony dostępu do danych znajdujących się na PUE ZUS pomyłką[110], chęcią sprawdzenia, z ciekawości, miejsca zatrudnienia skarżącej[111], sprawdzeniem zwolnienia L4 w związku z kontrolą zasadności zwolnienia przez ZUS (lekarz pełnił obowiązki Kierownika Medycznego w podmiocie, gdzie odbywała się kontrola)[112], sprawdzeniem czy skarżąca jest ubezpieczona[113], sprawdzeniem długości wystawionego skarżącej zwolnienia L4 (skarżąca była jedyną pielęgniarką w podmiocie, w którym pracował lekarz)[114]. Prezes UODO zajmował się również sprawami, w których jako powód dostępu do danych znajdujących się na PUE ZUS wskazywany był konflikt rodzinny z lekarzem[115].

W jednej z prowadzonych spraw[116] Prezes UODO ustalił, że uzyskanie dostępu do danych znajdujących się na PUE ZUS wynikało z potrzeby ustalenia aktualnego adresu zamieszkania skarżącej z uwagi na fakt, że skarżąca wystawiła lekarzowi negatywną opinię na portalu Znany Lekarz oraz wystosowała żądania związane z udzielaniem jej świadczeń zdrowotnych przez lekarza.

**Udostępnienie przez szpital nagrania z przebiegu operacji pacjentki na potrzeby programu telewizyjnego**

Prezes UODO zajmował się także skargą na działanie szpitala i nadawcy telewizyjnego[117]. W sprawie ustalono, że szpital dopuścił ekipę telewizyjną do nagrania fragmentu przebiegu operacji pacjentki pod narkozą na potrzeby programu telewizyjnego. Pacjentka przed operacją wyraziła sprzeciw co do udziału operatorów telewizji podczas jej zabiegu chirurgicznego. Szpital zignorował prawo pacjentki i udostępnił ekipie telewizyjnej szczegóły zabiegu i umożliwił sfilmowanie przebiegu świadczenia medycznego. Nadawca telewizyjny następnie wyemitował fragment ukazujący górną część twarzy i sylwetkę pacjentki oraz opis przypadku medycznego w treści serialu telewizyjnego. Prezes UODO ocenił, że udostępnienie danych dotyczących przypadku medycznego pacjentki na rzecz ekipy telewizyjnej oraz dopuszczenie operatorów do przebywania podczas zabiegu medycznego stanowiło naruszenie danych dotyczących zdrowia pacjentki i udzielił szpitalowi upomnienia. Przetwarzany przez nadawcę telewizyjnego fragment zabiegu medycznego stanowił materiał prasowy i w oparciu o wyłączenie stosowania przepisów RODO do działalności dziennikarskiej organ nadzorczy nie ma kompetencji do oceny legalności przetwarzania danych przez nadawcę telewizyjnego. Organ umorzył zatem

[110] DS.523.4252.2024, DS.523.4724.2024, DS.523.6148.2024, DS.523.298.2025, DWKSN.523.983.2025, DS.523.7970.2024, DWKSN.523.1056.2025, DWKSN.523.1873.2025; DS.523.7026.2023; DS.523.3814.2023; DS.523.4205.2023; DS.523.797.2023; DS.523.2388.2023; DS.523.2406.2024; DS.523.1908.2023; DS.523.1342.2023 ; DS.523.813.2024; DS.523.4089.2022; DS.523.2828.2024.
[111] DS.523.5071.2024.
[112] DS.523.7166.2024.
[113] DS.523.5075.2024.
[114] DS.523.728.2025.
[115] DS.523.3658.2023, DS.523.3403.2024, DWKSN.523.1549.2025.
[116] DS.523.1431.2023.
[117] DS.523.5082.2024.

postępowanie w zakresie przetwarzania danych pacjentki przez nadawcę telewizyjnego.

### Odpowiedzialność szpitala za udostępnienie wizerunku dziecka

W jednej ze spraw[118] skargę do Prezesa UODO złożyła osoba, która przeglądając media społecznościowe znalazła na profilu szpitala zdjęcie położnej trzymającej na rękach małoletniego syna skarżącej, który urodził się przedwcześnie w szpitalu, w którym był objęty wielomiesięczną hospitalizacją. Zdjęcie ukazywało wizerunek dziecka z charakterystycznymi oznakami przebytej operacji. Zdjęcie było dodane do wpisu zachęcającego do głosowania na położną, jako pracownika szpitala w konkursie dla medyków.

Szpital argumentował, że nie ponosi odpowiedzialności za naruszenie, ponieważ położna wykonała zdjęcie poza zakresem swoich obowiązków pracowniczych, zaś wizerunek dziecka nie był możliwy do rozpoznania dla nikogo poza osobami najbliższymi. Prezes UODO uznał, że fakt przekroczenia uprawnień przez pracownika szpitala, jako administratora danych osobowych, nie zwalnia szpitala z odpowiedzialności, gdyż to na administratorze spoczywa obowiązek takiego przygotowania i zorganizowania procesu przetwarzania danych, aby nie doszło do naruszenia przepisów RODO i naruszenia bezpieczeństwa danych osobowych, naruszenie miało miejsce w bezpośrednim związku z zatrudnieniem położnej, a szpital wiedział o zdjęciu i sam je udostępniał w mediach społecznościowych.

Prezes UODO stwierdził, że zdjęcie wizerunku jest identyfikatorem pozwalającym na identyfikację bezpośrednią, nie ma też znaczenia, że na zdjęciu widoczny jest wizerunek małoletniego dziecka, którego twarz ulega szybkim zmianom wyglądu. Wiek dziecka i tempo zmian fizycznych dziecka nie wpływają na ochronę jego prywatności, nie ograniczają prawa do ochrony danych osobowych. Wręcz przeciwnie – pozwalają one na przypisanie konkretnej osobie charakterystycznych dla niej w danym wieku i etapie rozwoju cech fizycznych. Ponadto zestawienie ze sobą wszystkich identyfikatorów wskazujących na problemy zdrowotne dziecka, przebywanie przez nie pod opieką położnej, zatrudnienie położnej w szpitalu, pozwala na identyfikację pośrednią dziecka, i to nie tylko dokonaną przez osoby najbliższe, lecz również pracowników szpitala, którzy ze względu na długi okres przebywania tam dziecka i jego charakterystyczne problemy zdrowotne, mogli go zidentyfikować. Prezes UODO udzielił wobec tego szpitalowi upomnienia za utrwalenie i udostępnienie wizerunku dziecka.

### Publikacja przez pracodawcę w BIP informacji o zwolnieniu lekarskim

W innej rozpatrywanej sprawie[119] skarżąca zarzuciła, że jej pracodawca – **Gminny Ośrodek Kultury** – opublikował na stronie internetowej BIP zarządzenie dyrektora, w którym zawarte zostały informacje dotyczące przebywania przez nią na zwolnieniu lekarskim. Skarżony podmiot nie wykazał, by kwestionowane

[118] DWKSN.523.148.2025.
[119] DS.523.1341.2024.

udostępnienie danych osobowych było niezbędne do realizacji jego celów. Z zebranego w sprawie materiału dowodowego wynikało, że udostępnienie danych osobowych skarżącej, które miało miejsce w przedmiotowej sprawie nie znajdowało oparcia w żadnej z przesłanek wymienionych w art. 9 ust. 1 RODO. Ustalono również, że zarówno artykuł dotyczący kwestionowanego zarządzenia, jak i sam dokument PDF został trwale usunięty z serwera i nie jest już dostępny w Internecie. Wobec powyższego Prezes UODO zdecydował o zastosowaniu wobec skarżonego podmiotu upomnienia za naruszenie art. 5 ust. 1 lit. a oraz 9 ust. 1 RODO polegające na udostępnieniu do publicznej wiadomości danych osobowych skarżącej dotyczących zdrowia bez podstawy prawnej.

**Przetwarzanie danych przez pracodawcę przy użyciu monitoringu wizyjnego**

Prezes UODO zajmował się również skargą na bezprawne przetwarzanie danych osobowych skarżącego przez pracodawcę za pośrednictwem systemu **monitoringu wizyjnego**[120].

W treści skargi skarżący wskazał, że spółka od 11 maja 2023 r. stosuje monitoring, którym obejmuje nowo utworzone pomieszczenia szatni, stołówki, łazienki i toalety, a pomimo tego nie oznacza tych miejsc, ani nie wypełnia wobec pracowników obowiązków informacyjnych. Skarżący wskazał również, że pomimo objęcia monitoringiem w szatni przestrzeni z umywalkami i pisuarami nie zastosowano technik uniemożliwiających identyfikację osób przebywających w tych pomieszczeniach. Skarżący zaznaczył, że pracodawca poinformował go pisemnie o stosowaniu monitoringu w dacie zatrudnienia, ale wówczas monitoring nie obejmował szatni, łazienek i toalet. Ponadto pracownicy obsługujący system monitoringu prawdopodobnie logują się do niego z urządzeń mobilnych typu smartfon i przeglądają zapis monitoringu, co w jego ocenie, daje możliwość zapisania obrazu na urządzeniu lub udostępnienia go osobom nieuprawnionym.

Prezes UODO wydał w tej sprawie decyzję nakazującą zaprzestania przetwarzania danych osobowych skarżącego za pośrednictwem kamer zainstalowanych w nowo utworzonych pomieszczeniach szatni i jadalni oraz odmówił uwzględnienia wniosku w pozostałym zakresie. Prezes UODO uznał, że w toku postępowania spółka nie wykazała, że zainstalowane w szatni i jadalni atrapy/kamery, które zdaniem spółki miały pełnić formę prewencyjną, nie są podłączone lub są atrapami.

W pozostałym zakresie, co do innych monitorowanych przestrzeni i celu monitorowania, tj. zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić spółkę na szkodę oraz realizacji obowiązków informacyjnych i innych obowiązków Prezes UODO nie stwierdził nieprawidłowości.

**Udostępnienie przez szkołę danych osobowych dziecka i jego rodzica na rzecz rodziców innych dzieci**

[120] DS.523.5413.2023.

Jedna z rozpatrzonych w roku 2025 spraw[121] dotyczyła przetwarzania danych osobowych skarżącej oraz jej małoletniej córki przez szkołę. Przetwarzanie polegało na udostępnieniu danych w zakresie treści prowadzonej korespondencji, nieobecności córki w szkole, uwag dotyczących nieprawidłowego informowania o przyczynach nieobecności córki, uwag dotyczących braku współpracy ze szkołą i uczestniczenia w zebraniach szkolnych oraz w zakończeniu roku szkolnego poprzez ich ujawnienie w komunikatorze internetowym na rzecz rodziców innych uczniów.

Skarżąca wskazała, że pracownik szkoły, do której uczęszcza jej córka, ujawnił treść prywatnej korespondencji prowadzonej między nią a szkołą na grupowym komunikatorze internetowym, do którego dostęp mają rodzice uczniów. Prywatne wiadomości zawierały dane osobowe jej oraz jej małoletniej córki, w tym m.in. wymienione wyżej informacje o nieobecnościach córki w szkole, uwagi dotyczące nieprawidłowego informowania o przyczynach nieobecności córki, uwagi dotyczące braku współpracy ze szkołą i uczestniczenia w zebraniach szkolnych oraz w zakończeniu roku szkolnego.

Szkoła wyjaśniła, że przesłanie wiadomości na komunikatorze internetowym nie stanowiło udostępniania ani przetwarzania danych osobowych skarżącej ani jej córki. Szkoła podała również, że udostępnienie przedmiotowych informacji nie stanowi naruszenia przepisów ani nie wykracza poza zgodę wyrażoną przez skarżącą. Szkoła wskazała, że usunęła wiadomość z komunikatora WhatsApp.

W ocenie Prezesa UODO szkoła nie miała podstawy prawnej ani celu, aby ujawniać dane osobowe, znajdujące się w treści prywatnej korespondencji skarżącej oraz jej małoletniej córki poprzez rozesłanie tych wiadomości do rodziców innych dzieci. Szkoła powinna była zachować poufność tych informacji i zapewnić prawo do prywatności rodzica oraz ucznia. Organ nadzorczy nie uznał, że ujawnienie tych wiadomości miało na celu realizację umowy o świadczenie usług edukacyjnych. Udostępnienie innym rodzicom pełnej treści korespondencji w żaden sposób nie realizowało tego celu. Włączanie innych rodziców do wewnętrznej dyskusji pomiędzy szkołą a skarżącą w sposób oczywisty naruszało prywatność tej korespondencji. Skarżąca w żaden sposób nie wyrażała zgody na ujawnienie treści prywatnej korespondencji. Wskazany przez szkołę rzekomy cel, jakim była konieczność ustalenia ilości uczestników wycieczki, nie uzasadnia dlaczego szkoła ujawniła innym rodzicom pełną treść korespondencji, która zawierała szereg innych informacji. Na podstawie art. 6 ust. 1 w zw. z art. 5 ust. 1 lit. a oraz art. 58 ust. 2 Prezes UODO udzielił szkole upomnienia stwierdzone naruszenie przepisów RODO.

### 5.5. Skargi na przewlekłość w sprawach skargowych

W 2025 roku skierowano łącznie **74 skargi** na przewlekłość oraz bezczynność organu nadzorczego w postępowaniach administracyjnych prowadzonych w Departamencie Skarg. Skargi te wraz z odpowiedzią Prezesa UODO przekazane zostały do rozpatrzenia przez Wojewódzki Sąd Administracyjny w Warszawie.

[121] DS.523.4958.2023**.**

W analizowanym roku do Prezesa Urzędu Ochrony Danych Osobowych wpłynęło **48 wyroków Wojewódzkiego Sądu Administracyjnego w Warszawie**, stwierdzających bezczynność lub przewlekłość organu w prowadzonych w Departamencie Skarg postępowaniach.

W tym samym okresie do organu wpłynęło **12 wyroków Naczelnego Sądu Administracyjnego w Warszawie** stwierdzających bezczynność lub przewlekłość w prowadzonych w Departamencie Skarg postępowaniach, co w świetle ogólnej liczby 7 831 zakończonych postępowań skargowych, stanowi zaledwie 0,15 %. Natomiast w odniesieniu do liczby 2020 decyzji skargowych wydanych w 2025 r. procent ten wynosi 0,6.

## 6. Naruszenia ochrony danych osobowych

Zgłaszanie Prezesowi UODO naruszeń ochrony danych osobowych przez administratorów jest skutecznym narzędziem przyczyniającym się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych. W toku prowadzonych czynności dokonywana jest kompleksowa analiza stanu faktycznego i prawnego, weryfikowana jest adekwatność reakcji na incydent w kontekście poziomu ryzyka dla praw lub wolności osób fizycznych. Dodatkowo prowadzone są działania informacyjne i edukacyjne skierowane do administratorów, ukierunkowane na podnoszenie poziomu zgodności z przepisami o ochronie danych osobowych. Obejmują one przekazywanie wyjaśnień, wskazywanie właściwych praktyk postępowania oraz rekomendowanie rozwiązań organizacyjnych lub technicznych służących zapobieganiu incydentom bezpieczeństwa danych osobowych.

Zgłaszając naruszenie organowi nadzorczemu administratorzy informują Prezesa UODO, czy – w ich ocenie – wystąpiło wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, oraz – jeśli takie ryzyko wystąpiło – to czy niezwłocznie przekazali stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. W uzasadnionych przypadkach mogą również przekazać informację, że zawiadomienie – 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 negatywnymi skutkami. Administrator ma obowiązek podjęcia skutecznych działań zapewniających ochronę danych osobowych, 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.

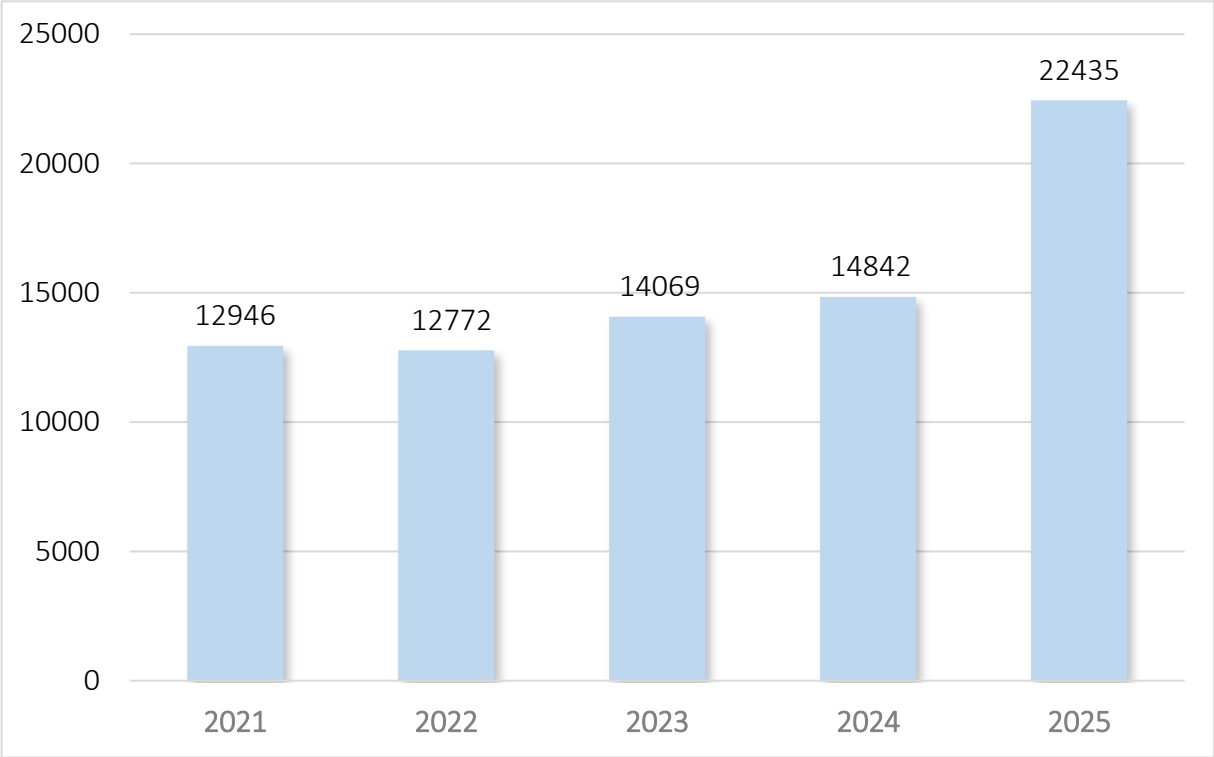
### 6.1. Wstępna kontrola naruszeń ochrony danych osobowych

W 2025 r. do Urzędu Ochrony Danych Osobowych wpłynęło **22 435 zgłoszeń naruszeń ochrony danych osobowych.** Dla porównania w 2024 r. zgłoszone zostały 14 842 naruszenia. Porównanie danych za analizowane lata wskazuje na bardzo znaczny, bo **51 % wzrost liczby notyfikowanych w 2025 r. naruszeń** ochrony danych osobowych.

Tendencja ta wynikała w szczególności z następujących czynników:

- **Zintensyfikowana działalność cyberprzestępcza** – odnotowano zwiększoną liczbę ataków ukierunkowanych na dane osobowe obywateli, obejmujących m.in. ataki ransomware, włamania do systemów informatycznych, przejęcia obszernych zbiorów danych do logowania, działania o charakterze phishingowym. Ataki te cechują się rosnącym stopniem automatyzacji i wyrafinowania technicznego.
- **Czynniki geopolityczne** – nasilające się napięcia geopolityczne sprzyjają zwiększonej liczbie incydentów bezpieczeństwa, w tym ukierunkowanych na podmioty posiadające status administratorów.
- **Podniesienie poziomu świadomości prawnej administratorów** – organizacje w coraz większym stopniu realizują obowiązki wynikające z rozporządzenia 2026/679, co przekłada się na częstsze i bardziej terminowe zgłaszanie naruszeń ochrony danych osobowych. Działania te są motywowane zarówno dążeniem do zapewnienia zgodności z przepisami, jak i minimalizacją ryzyka wszczęcia przez organ nadzorczy postępowań administracyjnych oraz nałożenia administracyjnych kar pieniężnych.

Podsumowując, do Prezesa UODO notyfikowana jest coraz większa liczba naruszeń ochrony danych osobowych, ponieważ incydentów jest więcej, a organizacje częściej potrafią je wykryć i lepiej znają swoje obowiązki.




**Wykres 4:** Liczba naruszeń ochrony danych osobowych, które wpłynęły do Prezesa UODO w latach 2021–2025.

### 6.2. Najczęściej zgłaszane naruszenia ochrony danych osobowych

Podobnie jak w latach ubiegłych, do najczęściej zgłaszanych przez administratorów 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, najczęściej wskutek błędu pracownika zatrudnionego przez administratora, zaś 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 też 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, dokumentacji medycznej, 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 przeznaczone do zamieszczenia w Internecie. Aby zminimalizować negatywne skutki takich naruszeń oraz zapobiec powtórzeniu się podobnych 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. Chociaż często udostępniane one były w dobrej wierze przez różnego rodzaju podmioty, np. gminne ośrodki, ich konsekwencją było zagrożenie bezpieczeństwa czy, co najmniej, 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 po stwierdzeniu naruszenia ochrony danych, w ramach działań zapobiegających wystąpieniu podobnych incydentów w przyszłości, składali reklamację do operatora pocztowego, dokonywali aktualizacji instrukcji kancelaryjnej oraz zmieniali postanowienia umów zawartych z operatorem pocztowym.

**5. nieuprawniony dostęp do baz danych**

Tego typu naruszenia były spowodowane najczęściej błędami oprogramowania ujawniającymi się po przeprowadzeniu aktualizacji programu,

brakiem regularnych, wewnętrznych testów bezpieczeństwa w kierunku wykrycia podatności systemu, a także nieprawidłowościami na etapie nadawania uprawnień w systemach informatycznych. 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 lokalizacji dokumentacji papierowej**

Tego rodzaju naruszenia ochrony danych miały charakter jednorazowych incydentów w danej organizacji i były często konsekwencją niefrasobliwości pracowników. W celu zmniejszenia prawdopodobieństwa wystąpienia takich naruszeń w przyszłości administratorzy 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**

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

### 6.3. Wstępna weryfikacja zgłoszonego naruszenia ochrony danych osobowych

W ramach wstępnej analizy zgłoszonego naruszenia ochrony danych osobowych organ nadzorczy w pierwszej kolejności weryfikował poniższe kwestie:

- rodzaj zgłoszenia – czy jest to zgłoszenie: kompletne / jednorazowe, wstępne, uzupełniające;
- właściwość podmiotu dokonującego zgłoszenia – czy zgłoszenie zostało złożone przez administratora lub inny właściwy podmiot zobowiązany;
- terminowość zgłoszenia – weryfikacja, czy zgłoszenia dokonano w terminie 24 lub 72h, stosownie do właściwych przepisów;
- uzasadnienie ewentualnego opóźnienia w powiadomieniu organu nadzorczego – organ oceniał podane powody przekroczenia terminu oraz czy są one racjonalnie uzasadnione;
- rodzaj naruszenia – klasyfikacja, czy naruszenie dotyczyło poufności, integralności lub dostępności danych;
- opis charakteru naruszenia – w tym sposób ujawnienia naruszenia, zakres

i przebieg zdarzenia;

- kategorie danych i kategorie osób objętych naruszeniem – kategorie osób dotkniętych naruszeniem, kategorie danych oraz ich wrażliwość (w tym ewentualne dane szczególnej kategorii, czy dane, o których mowa w art. 10 rozporządzenia 2016/679);
- ocena ryzyka naruszenia praw lub wolności osób fizycznych – w tym ustalenie, czy wystąpiło wysokie ryzyko, które obligowało administratora do zawiadomienia osób, których dane dotyczą, o naruszeniu;
- podjęte środki zaradcze – ocena, czy wdrożono działania zmniejszające ryzyko ponownego wystąpienia incydentu oraz minimalizujące jego skutki;
- zawiadomienie osób, których dane dotyczą – weryfikacja: czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu, w jakiej dacie, jakim kanałem komunikacji oraz czy treść przekazanych osobom zawiadomień spełniała wymogi wynikające z art. 34 ust. 2 w zw. z art. 33 ust. 3 rozporządzenia 2016/679.

W wyniku dokonanej wstępnej analizy zgłoszenia naruszenia ochrony danych osobowych, organ nadzorczy oceniał m.in. charakter i wagę zdarzenia, zakres zagrożeń dla praw lub wolności osób fizycznych oraz adekwatność podjętych działań zaradczych. W zależności od podjętych ustaleń i oceny zaistniałego ryzyka, zgłoszenie mogło zostać pozostawione bez podejmowania dalszych czynności związanych z jego zaistnieniem na etapie wstępnej weryfikacji lub mogło wymagać podjęcia działań wyjaśniających i dalszego procedowania przez Departament Kontroli i Naruszeń.

### 6.4. Współpraca z administratorami w związku z naruszeniami

Mając na względzie konieczność zapewnienia szybkiej i sprawnej obsługi znacznej liczby zgłoszonych w 2025 r. naruszeń ochrony danych osobowych Prezes UODO, w przypadku potrzeby uzyskania dodatkowych informacji w związku z dokonanym zgłoszeniem, kontaktował się z administratorami w pierwszej kolejności mailowo lub telefonicznie, zwracając się z prośbą o pisemne ich przesłanie. Pierwszą linię kontaktu stanowili inspektorzy ochrony danych lub inne punkty kontaktowe, które dane administrator wskazał w treści zgłoszenia. W zdecydowanej większości przypadków inspektorzy ochrony danych lub inne punkty kontaktowe szybko i sprawnie przekazywali potrzebne informacje. Najczęściej organ nadzorczy zwracał się do administratorów o wskazanie:

- przybliżonej daty uzupełnienia zgłoszenia, w przypadku braku tej informacji we wstępnym zgłoszeniu naruszenia,
- powodów opóźnienia w powiadomieniu Prezesa UODO o naruszeniu,
- daty zawiadomienia osób o naruszeniu (w przypadku braku jej wskazania w zgłoszeniu lub wskazania daty planowanego zawiadomienia),
- liczby zawiadomionych osób,
- środków komunikacji wykorzystanych do zawiadomienia osób, a także
- o przesłanie zanonimizowanej treści zawiadomienia skierowanego do osób, których danych dotyczy naruszenie.

Przedmiotem zainteresowania organu nadzorczego były również środki bezpieczeństwa zastosowane lub proponowane przez administratorów w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia oraz minimalizujące jego skutki.

Nie zawsze informacje udzielone mailowo lub telefonicznie mogły zostać uznane za wystarczające lub nie istniała możliwość ich uzyskania tymi kanałami komunikacji (np. brak wyznaczonego inspektora ochrony danych, brak określenia innego punktu kontaktowego, brak możliwości ustalenia danych kontaktowych administratora, brak reakcji administratora na tę formę kontaktu ze strony organu nadzorczego, brak przekazania adekwatnych informacji). Wówczas Prezes UODO korzystał z zasadniczego uprawnienia organu nadzorczego, niezbędnego do prawidłowego prowadzenia czynności w następstwie dokonanego zgłoszenia naruszenia ochrony danych osobowych, tj. uprawnienia do nakazania dostarczenia informacji przez zgłaszającego. Prawodawca wyposażył organ nadzorczy w te uprawnienia w art. 58 ust. 1 lit. a oraz lit. e rozporządzenia 2016/679.

Korzystając z uprawnień określonych w ww. przepisie, polegających na nakazaniu administratorom, podmiotom przetwarzającym oraz ich przedstawicielom, zapewnienia dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji jego zadań, DWKSN wystosował do administratorów dokonujących zgłoszeń naruszeń **63 pisemne wezwania do złożenia wyjaśnień.** W większości przypadków dotyczyły one wyżej wskazanych kwestii, a ponadto: konieczności przesłania uzupełniającego zgłoszenia naruszenia ochrony danych osobowych, przekazania brakujących informacji objętych formularzem zgłoszenia naruszenia, w sytuacjach gdy zgłoszenia nie zostały złożone z użyciem dedykowanego w tym celu formularza.

### 6.5. Statystyka naruszeń ochrony danych osobowych

Jak już o tym wspomniano, w analizowanym 2025 roku do Urzędu Ochrony Danych Osobowych wpłynęło **ogółem 22435 zgłoszeń naruszeń ochrony danych osobowych.** Po wstępnej kontroli w zakresie braków formalnych, do Departamentu Kontroli i Naruszeń zostało przekazanych **4282 zgłoszeń naruszeń ochrony danych osobowych**, w których niezbędne było podjęcie przez Prezesa UODO działań na mocy przysługujących mu kompetencji.

Korzystając z uprawnień określonych w art. 58 ust. 1 lit. a oraz lit. e rozporządzenia 2016/679, 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 dokonujących zgłoszeń naruszeń ochrony danych osobowych **971 pisemnych wezwań do złożenia wyjaśnień.**

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;
- środki bezpieczeństwa dotychczas stosowane w organizacji administratora;
- nieprawidłowe oszacowania poziomu ryzyka naruszenia praw lub wolności osób fizycznych;
- nieprawidłowe wskazania 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 zgłoszeń naruszeń ochrony danych osobowych wynika, że realizacja kompetencji Prezesa UODO w trybie art. 58 ust. 1 lit. a oraz lit. e rozporządzenia 2016/679 pozytywnie wpływała na ochronę danych osobowych. Znacznie bowiem skracała proces przywracania stanu zgodnego z prawem, pozwalając organowi nadzorczemu na natychmiastowe działanie.

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 2025 roku Prezes UODO skierował **596 wystąpień** 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 o których mowa w art. 34 ust. 2 rozporządzenia 2016/679.

Wystąpienia te 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. Administratorzy, do których Prezes UODO skierował wystąpienia, podejmowali działania zmierzające do wykonania obowiązków wynikających z przepisów o ochronie danych osobowych w odpowiednim zakresie i czasie. W większości przypadków przekazywali oni informacje potwierdzające dokonanie prawidłowego zawiadomienia osoby, której dane dotyczą oraz sposobu realizacji tego obowiązku. Na podstawie przeprowadzonych analiz należy ocenić pozytywnie skuteczność kierowanych przez Prezesa UODO wystąpień.

## 7. Postępowania administracyjne w sprawie naruszeń

Impulsem do wszczęcia postępowania administracyjnego są przede wszystkim ustalenia dokonane w toku przeprowadzonych kontroli, jak i czynności wyjaśniających podejmowanych w związku z dokonywanymi przez administratorów zgłoszeniami naruszenia ochrony danych osobowych, wskazujące na naruszenie przez administratorów i podmioty przetwarzające spoczywających na nich obowiązków wynikających z rozporządzenia 2016/679, dotyczących zapewnienia zgodnego z przepisami tego aktu prawnego realizowania procesów przetwarzania danych osobowych. Podkreślić należy, że przysługujące Prezesowi UODO uprawnienia naprawcze, o których mowa w art. 58 ust. 2 rozporządzenia 2016/679, stosowane są w przypadku stwierdzonych w toku prowadzonych postępowań naruszeń przepisów rozporządzenia 2016/679, a nie np. w związku z wystąpieniem naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 tego rozporządzenia.

W 2025 r. Prezes UODO **wszczął z urzędu 22 postępowań administracyjnych** w sprawie naruszenia przepisów o ochronie danych osobowych.

### 7.1. Decyzje administracyjne

W wyniku prowadzonych przez Prezesa UODO postępowań administracyjnych, które zostały zakończone w 2025 r., **wydano 31 decyzji administracyjnych w związku ze stwierdzeniem naruszenia przepisów o ochronie danych osobowych.**

W przypadku **15 decyzji administracyjnych w związku ze stwierdzeniem naruszenia przepisów o ochronie danych osobowych** Prezes UODO, po przeprowadzeniu postępowań administracyjnych, zdecydował się nałożyć na administratorów danych lub podmioty przetwarzające **administracyjne kary pieniężne**, w tym w **4 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, a w **3 przypadkach** udzielono dodatkowo upomnienia. W **2 przypadkach** postępowanie zostało umorzone w całości. W **14 przypadkach** udzielono upomnienia lub sformułowano nakazy dostosowania operacji przetwarzania do przepisów rozporządzenia 2016/679.

### 7.2. Administracyjne kary pieniężne w związku z naruszeniem

Jedno z postępowań administracyjnych, prowadzone wobec jednostki z **sektora medycznego**, zakończone zostało wydaniem decyzji[122] nakładającej na placówkę medyczną dwóch kar pieniężnych. Jedna z kar została nałożona za naruszenie art. 5 ust. 1 lit. a (zasada zgodności z prawem, rzetelności i przejrzystości), art. 5 ust. 2 (zasady rozliczalności), art. 6 ust. 1 i art. 9 ust. 1 oraz art. 13 ust. 1 i 2 rozporządzenia

[122] DKN.5131.4.2024.

2016/679. Drugą zaś karę Prezes UODO nałożył za naruszenie art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. Postępowanie dotyczyło kwestii dopuszczalności przetwarzania danych osobowych w związku ze stosowaniem urządzeń rejestrujących obraz na salach oddziału szpitalnego, a także bezpieczeństwa przetwarzanych w ten sposób danych. W toku postępowania ustalono, że monitoring wprowadzony był niezgodnie z obowiązującymi przepisami prawa (23a ust. 1 pkt 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[123]), dodatkowo zaś administrator nie spełnił obowiązku informacyjnego w stosunku do osób objętych monitoringiem wizyjnym (brak precyzyjnego oznaczenia obszaru objętego monitoringiem oraz brak wyszczególnienia w klauzuli informacyjnej poszczególnych pomieszczeń objętych rejestracją obrazu). Badany proces przetwarzania danych realizowany był – w ocenie organu nadzorczego – bez podstawy prawnej i w warunkach celowego jego nieujawniania podmiotom danych (osoby objęte monitoringiem nie były świadome stosowania tego rozwiązania). Placówka wdrażając monitoring na ww. obszarze nie zastosowała się również do własnych procedur związanych z technicznym zabezpieczeniem urządzeń rejestrujących. Analiza ryzyka związana z przetwarzaniem danych osobowych przy użyciu nośników danych została przeprowadzona w sposób nieprawidłowy, gdyż nie uwzględniała ona szczegółowo wyodrębnionych podatności, a zagrożenia związane z przetwarzaniem danych osobowych w związku z prowadzonym monitoringiem wizyjnym nie zostały prawidłowo i wyczerpująco zidentyfikowane. W konsekwencji ww. analiza ryzyka nie określała środków bezpieczeństwa, mających na celu zmitygowanie ryzyk związanych z prowadzonym przez placówkę monitoringiem wizyjnym. Zaistniałe w przedmiotowej sprawie naruszenie ochrony danych osobowych (w rozumieniu art. 4 pkt 12 rozporządzenia 2016/679), związane z utratą w niewyjaśnionych okolicznościach nośników danych zgormadzonych poprzez urządzenia monitorujące, stanowiło swoiste potwierdzenie nieprawidłowości w obszarze zabezpieczenia przetwarzanych danych, zaistniałych po stronie administratora.

Decyzja w ww. sprawie została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie, który utrzymał ją w mocy. Od ww. wyroku administrator złożył skargę kasacyjną do Naczelnego Sądu Administracyjnego (sprawa oczekuje na rozstrzygnięcie).

Kolejna sprawa z **sektora medycznego** dotyczyła podmiotu będącego Samodzielnym Publicznym Zakładem Opieki Zdrowotnej[124]. Administracyjna kara pieniężna nałożona została za naruszenie przepisów art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. Ponadto Prezes UODO w decyzji nakazał dostosowanie operacji przetwarzania do przepisów tego rozporządzenia w terminie 60 dni od dnia doręczenia decyzji. Impulsem do przyjrzenia się, jak w ww. podmiocie zorganizowany został system ochrony danych osobowych oraz w jaki sposób zapewniane jest bezpieczeństwo przetwarzanych

[123] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2026 r. poz. 156).
[124] DKN.5131.48.2022.

danych osobowych (a w konsekwencji do wszczęcia z urzędu postępowania w tej sprawie) było zgłoszenie naruszenia ochrony danych osobowych polegającego na przełamaniu zabezpieczeń infrastruktury informatycznej administratora i zainfekowaniu jej złośliwym oprogramowaniem ransomware. Cyberatak skutkował naruszeniem poufności i dostępności danych osobowych ok. 2 000 pracowników. Administrator nie zdołał w pełni odtworzyć utraconych danych. W toku postępowania Prezes UODO stwierdził, że szpital nie przeprowadził prawidłowej analizy ryzyka dla operacji przetwarzania danych osobowych, stanowiącej fundament doboru odpowiednich środków technicznych i organizacyjnych na gruncie rozporządzenia 2016/679. Przedłożona dokumentacja analizy ryzyka opierała się na wadliwej procedurze, koncentrującej się na skutkach dla szpitala jako organizacji, a nie na ryzyku dla praw lub wolności osób, których dane dotyczą. Ponadto administrator nie powiązał logicznie zidentyfikowanych zagrożeń z podatnościami systemów informatycznych ani z konkretnymi środkami zaradczymi, co stało w sprzeczności z wymogami rozporządzenia 2016/679. Prezes UODO ustalił również, że szpital nie wdrożył odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności zabezpieczeń przetwarzanych danych osobowych. Administrator twierdził, że takie testy przeprowadzał, jednak nie był w stanie tego wykazać. Audyt cyberbezpieczeństwa przeprowadzony po incydencie przez zewnętrzną firmę ujawnił poważne zaniedbania w zakresie bezpieczeństwa teleinformatycznego.

Decyzja w ww. sprawie jest prawomocna. Administracyjna kara pieniężna została zapłacona.

Kolejna decyzja wydana przez Prezesa UODO w stosunku do podmiotu **sektora medycznego** adresowana była do Niepublicznego Zakładu Opieki Zdrowotnej[125]. Postępowanie administracyjne z urzędu zostało w tym przypadku wszczęte w następstwie przeprowadzonych czynności wyjaśniających mających na celu ustalenie, jak w ww. podmiocie zorganizowany został system ochrony danych osobowych oraz w jaki sposób zapewniane jest bezpieczeństwo przetwarzanych danych osobowych, po zgłoszeniu przez administratora incydentu polegającego na kradzieży prywatnego samochodu pracownika, w którym znajdowała się papierowa dokumentacja medyczna zawierająca szeroki zakres danych osobowych ośmiu pacjentów, w tym noworodków. Prezes UODO w toku postępowania ustalił, że administrator dopuścił się naruszenia art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679, co w konsekwencji doprowadziło do złamania zasad integralności, poufności oraz rozliczalności określonych w art. 5 rozporządzenia 2016/679. Kluczowym uchybieniem administratora było nieprzeprowadzenie rzetelnej analizy ryzyka dla operacji przetwarzania danych związanych z realizacją świadczeń opieki zdrowotnej w formie wizyt domowych. Choć administrator posiadał ogólną politykę bezpieczeństwa, nie odnosiła się ona w żaden sposób do zasad transportu dokumentów zawierających dane osobowe pacjentów prywatnymi autami pracowników, a rekomendacje z audytów przeprowadzonych jeszcze w 2017 i 2018

[125] DKN.5131.17.2022.

roku, wskazujące na konieczność niezwłocznego zwrotu kartotek do przychodni (po wykorzystaniu ich na potrzeby odbywanych wizyt domowych), nigdy (przed wystąpieniem naruszenia ochrony danych osobowych) nie przybrały formy wiążących procedur. W związku ze stwierdzonymi uchybieniami Prezes UODO nałożył na administratora karę pieniężną. Decyzja w tej sprawie stanowi jasne przypomnienie, że analiza ryzyka musi mieć charakter ciągły i uwzględniać realne operacje składające się na proces przetwarzania danych (takie jak – w badanym przypadku – wizyty domowe), a brak realizacji zaleceń audytowych, czy brak formalnego odzwierciedlenia określonych rozwiązań w procedurach, stanowi rażące naruszenie obowiązków w zakresie zapewnienia bezpieczeństwa danych, a zarazem naruszenie obowiązków wynikających z zasady rozliczalności.

Decyzja jest prawomocna, a nałożona przez Prezesa UODO administracyjna kara pieniężna została zapłacona przez administratora.

Kolejna decyzja[126] dotycząca podmiotu z **sektora medycznego** związana była z naruszeniem ochrony danych polegającym na nieuprawnionym ujawnieniu przez pracownika administratora, na rzecz osoby nieuprawnionej (niewłaściwej pacjentki), danych osobowych pacjentki oraz jej męża utrwalonych w dokumencie potwierdzenia przelewu (dokument ten wskazywał na zwrot należności uregulowanej za określoną procedurę medyczną). W przedmiotowej sprawie bezpośrednio po wystąpieniu incydentu przeprowadzona została analiza ryzyka, która nie wykazała, aby zdarzenie wiązało się z możliwością naruszenia praw lub wolności osób fizycznych – w związku z czym administrator odstąpił od zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu. Błędnie przeprowadzona analiza ryzyka związanego z naruszeniem ochrony danych osobowych skutkowała bezpodstawnym zaniechaniem realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu wynikającego z art. 33 ust. 1 rozporządzenia 2016/679, a także niezwłocznego zawiadomienia o incydencie podmiotów danych, o którym mowa w art. 34 ust. 1 rozporządzenia 2016/679. Za naruszenie art. 33 ust. 1 rozporządzenia 2016/679 Prezes UODO nałożył na administratora karę pieniężną. Ponadto udzielił mu upomnienia za naruszenie art. 34 ust. 1 rozporządzenia 2016/679. Prezes UODO odstępując od wymierzenia administracyjnej kary pieniężnej za naruszenie ww. przepisu uwzględnił fakt, że administrator finalnie (po uprzednim wystąpieniu Prezesa UODO) zawiadomił podmiot danych o naruszeniu ochrony danych osobowych.

Administrator złożył do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na przedmiotową decyzję Prezesa UODO.

W związku ze stwierdzonymi nieprawidłowościami w procesie przetwarzania danych osobowych podczas organizacji tzw. **„wyborów kopertowych”** wydana została decyzja[127], mocą której Prezes UODO nałożył administracyjne kary pieniężne na **Ministra Cyfryzacji** oraz na **Pocztę Polską S.A.** W przedmiotowej sprawie Prezes UODO stwierdził naruszenie przez Ministra Cyfryzacji art. 6 ust. 1

[126] DKN.5131.3.2025.
[127] DKN.5131.1.2025.

rozporządzenia 2016/679, polegające na niezgodnym z prawem przetwarzaniu danych osobowych zgromadzonych w rejestrze PESEL, poprzez ich udostępnienie 22 kwietnia 2020 r. bez podstawy prawnej w zakresie: numeru PESEL, imion, nazwisk, ostatniego aktualnego adresu zameldowania na pobyt stały (a gdy go brak: ostatniego nieaktualnego), adresu zameldowania na pobyt czasowy (wraz z deklarowanym terminem tego pobytu), a także aktualnie zarejestrowanego wyjazdu czasowego poza granice kraju, wszystkich osób pełnoletnich 10 maja 2020 r., które w dniu wygenerowania danych posiadały w ww. rejestrze zarejestrowane obywatelstwo polskie, figurowały jako osoby żyjące i dla których wskazanym krajem zamieszkania była Polska, na rzecz Poczty Polskiej S.A., co skutkowało naruszeniem zasady zgodności przetwarzania z prawem określonej w art. 5 ust. 1 lit. a rozporządzenia 2016/679. W tej samej sprawie Prezes UODO stwierdził naruszenie przez Pocztę Polską S.A. art. 6 ust. 1 rozporządzenia 2016/679, polegające na przetwarzaniu bez podstawy prawnej udostępnionych tej spółce 22 kwietnia 2020 r. przez Ministra Cyfryzacji ww. danych osobowych, co skutkowało naruszeniem zasady zgodności przetwarzania z prawem określonej w art. 5 ust. 1 lit. a rozporządzenia 2016/679.

Organizacja tzw. „**wyborów kopertowych”** stała się przedmiotem wielu dyskusji m.in. w mediach i wzbudziła liczne kontrowersje oraz niepokój części opinii publicznej. W toku postępowania prowadzonego przez Prezesa UODO ustalono, że analizowany proces przetwarzania danych osobowych przez Ministra i ww. spółkę był realizowany pomimo braku podstawy prawnej z art. 6 ust. 1 rozporządzenia 2016/679, co wiązało się ze stwierdzeniem, że wskazani administratorzy naruszyli swoim działaniem także art. 5 ust. 1 lit. a ww. aktu prawnego – łamiąc wyrażoną w nim zasadę zgodności z prawem, rzetelności i przejrzystości.

Poczta Polska S.A. złożyła skargę na wydaną decyzję w części jej dotyczącej, zaś Minister Cyfryzacji jej nie zakwestionował i zapłacił nałożoną na niego administracyjną karę pieniężną w całości.

W 2025 r. Prezes UODO wydał również decyzję[128] stanowiącą jedno z najbardziej kompleksowych rozstrzygnięć w polskiej praktyce nadzorczej, analizujących wielopoziomowe zaniedbania w procesie przetwarzania danych osobowych i ich powierzenia oraz techniczne aspekty bezpieczeństwa systemów teleinformatycznych. Postępowanie, które zakończyło się nałożeniem na podmioty **sektora prywatnego** kar finansowych, zostało zainicjowane ustaleniami dokonanymi w następstwie zgłoszenia naruszenia ochrony danych przez administratora, który stwierdził, że dane jego pracowników oraz pracowników jego franczyzobiorców były publicznie dostępne w sieci Internet. Zakres ujawnionych informacji był niezwykle szeroki i obejmował imiona, nazwiska, numery PESEL, numery paszportów, a także szczegółowe dane dotyczące czasu pracy, stanowisk i identyfikatorów systemowych, co w ocenie organu generowało wysokie ryzyko kradzieży tożsamości lub nadużyć finansowych dla osób dotkniętych incydentem.

[128] DKN.5130.4179.2020.

Analiza odpowiedzialności podmiotu przetwarzającego wykazała szereg rażących naruszeń przepisów rozporządzenia 2016/679, w tym przede wszystkim art. 32 ust. 1 i 2, dotyczącego bezpieczeństwa przetwarzania. Równie surowo oceniono działania i zaniechania administratora, który mimo powierzenia operacji na danych podmiotowi zewnętrznemu, pozostał odpowiedzialny za ich bezpieczeństwo i zgodność z ogólnymi zasadami przetwarzania. Pierwszym kluczowym uchybieniem była wadliwa weryfikacja podmiotu przetwarzającego przed zawarciem umowy powierzenia, gdzie administrator oparł swój wybór na wieloletniej współpracy w obszarze usług public relations oraz referencjach marketingowych, zamiast rzetelnie ocenić gwarancje techniczne i organizacyjne procesora w zakresie ochrony danych. Ponadto administrator naruszył zasadę minimalizacji danych oraz zasadę ochrony danych w fazie projektowania, wykorzystując numer PESEL jako identyfikator pracownika w bazie danych, mimo że cel ten można było osiągnąć za pomocą mniej inwazyjnych środków, co zresztą wdrożono natychmiast po ujawnieniu naruszenia poufności danych. Organ wskazał również na brak realnego nadzoru nad procesorem – administrator nie korzystał z przysługujących mu uprawnień audytowych i nie weryfikował skuteczności zabezpieczeń stosowanych przez procesora, poprzestając na ogólnej wymianie korespondencji e-mail, która w oczywisty sposób nie mogła zostać uznana za równoważną rzetelnemu testowaniu systemów.

Kolejnym istotnym aspektem decyzji była ocena sposobu powiadomienia osób, których dane dotyczą, o wystąpieniu naruszenia. O ile administrator indywidualnie zawiadomił obecnych pracowników, o tyle w przypadku byłych zatrudnionych zdecydował się na publiczne ogłoszenia w prasie, argumentując to niewspółmiernie dużym wysiłkiem potrzebnym do dotarcia do każdej osoby z osobna. Prezes UODO odrzucił tę argumentację, wskazując, że administrator jako pracodawca ma prawny obowiązek przechowywania akt osobowych zawierających adresy korespondencyjne przez wiele lat, a zatem posiadał wszelkie dane niezbędne do bezpośredniego kontaktu. Decyzja rozstrzygnęła również kwestię statusu administratora w odniesieniu do pracowników franczyzobiorców, uznając, że spółka, jako właściciel i projektant modułu grafików decydujący o celach i sposobach przetwarzania (m.in. poprzez narzucenie zakresu zbieranych danych), pełniła rolę administratora również wobec tej grupy osób.

W przedmiotowej sprawie zostały nałożone administracyjne kary pieniężne zarówno na administratora, jak i podmiot przetwarzający. Podmiot przetwarzający zapłacił nałożone na niego kary, zaś administrator złożył do Wojewódzkiego Sądu Administracyjnego skargę na wydaną przez Prezesa UODO decyzję.

Kolejna zakończona wydaniem decyzji[129] sprawa dotycząca podmiotu **sektora prywatnego** zainicjowana została przekazaniem przez Prokuraturę Rejonową w Puławach informacji z prawomocnie zakończonego postępowania przygotowawczego prowadzonego w związku z zagubieniem przez zakład pogrzebowy na poboczu drogi pudeł z dokumentami zawierającymi m.in. dane

[129] DKN.5131.10.2023.

osobowe. Niezabezpieczone do transportu pudła spadły z samochodu, czego pracownik je przewożący nie zauważył. W związku z tym zdarzeniem administrator nie dokonał zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych zgodnie z art. 33 ust. 1 rozporządzenia 2016/679. W toku postępowania Prezes UODO ustalił m.in., że w ramach obowiązującej polityki bezpieczeństwa administrator nie przewidywał w ogóle możliwości transportu takiej dokumentacji do innego miejsca wykonywania działalności gospodarczej. Ustalone przez Prezesa UODO naruszenie przepisów art. 24 ust. 1, art. 25 ust. 1 i art. 32 ust. 1 i 2 rozporządzenia 2016/679 było wynikiem niezidentyfikowania zagrożeń związanych z realizowanymi przez administratora procesami przetwarzania, w szczególności związanych z transportem dokumentów z siedziby Administratora do innego miejsca prowadzenia działalności.

W konsekwencji stwierdzonych uchybień, Prezes UODO wydał decyzję administracyjną i nałożył w przedmiotowej sprawie dwie administracyjne kary pieniężne za niewdrożenie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa oraz za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych zgodnie z art. 33 ust. 1 rozporządzenia 2016/679. Ponadto w przedmiotowej sprawie nałożono na administratora nakaz wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zminimalizowania ryzyka wiążącego się z przetwarzaniem danych osobowych w dokumentacji administratora, a także nakaz wdrożenia odpowiednich rozwiązań w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności przyjętych środków służących bezpieczeństwu danych.

Administrator zaskarżył ww. decyzję do Wojewódzkiego Sądu Administracyjnego. W zapadłym 4 grudnia 2025 r. nieprawomocnym wyroku Wojewódzki Sąd Administracyjny w Warszawie całkowicie podzielił argumentację zaprezentowaną przez Prezesa UODO w omówionej decyzji, oddalając skargę na decyzję.

Kolejna sprawa dotyczyła naruszenia przez jeden z podmiotów **sektora prywatnego** przepisów 5 ust. 1 lit. a, lit. b i lit. c oraz art. 6 ust. 1 rozporządzenia 2016/679, polegającego na przetwarzaniu bez podstawy prawnej danych osobowych pozyskiwanych poprzez dokonywanie kopii (skanów) dokumentów tożsamości klientów i potencjalnych klientów bez odpowiedniej weryfikacji, czy w danym przypadku działania takie są uzasadnione wymogiem stosowania przez ten podmiot środków bezpieczeństwa finansowego na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[130] (w związku ze stosowaniem których instytucje obowiązane mogą korzystać z uprawnienia z art. 34 ust. 4 tej ustawy). W decyzji tej Prezes UODO wskazał m.in., że sporządzanie kopii (skanów) dowodów tożsamości przez instytucje obowiązane jest legalne jedynie wtedy, gdy wiąże się z koniecznym z punktu widzenia ww. ustawy zastosowaniem

[130] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644), zwana także: AML.

środków bezpieczeństwa finansowego mających na celu przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu. Zadaniem instytucji obowiązanej jest przeprowadzenie indywidualnej oceny ryzyka prania pieniędzy i finansowania terroryzmu i zaprojektowanie środków bezpieczeństwa odpowiednich do jej wyniku (podejście oparte na ryzyku). Jeśli instytucja obowiązana wykaże, że w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu konieczne jest stosowanie środków bezpieczeństwa finansowego wiążące się z przetwarzaniem informacji zawartych w dokumentach tożsamości oraz sporządzaniem ich kopii (skanów), wtedy ma prawo żądać ich wykonania. Skutkiem stwierdzonych naruszeń było wydanie decyzji[131] nakładającej na administratora przez Prezesa UODO administracyjnej kary pieniężnej.

Decyzja ta została zaskarżona przez administratora do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Postępowanie administracyjne, w którym wydana została kolejna decyzja[132] zostało wszczęte po uprzednim przeprowadzeniu przez Prezesa UODO kontroli w siedzibie podmiotu **sektora prywatnego** (przedsiębiorcy). Inspiracją do dokonania oceny realizacji przez administratora spoczywających na nim obowiązków regulowanych przepisami o ochronie danych osobowych dotyczących zwłaszcza zapewnienia bezpieczeństwa danych i organizacji systemu ochrony danych osobowych były w tym przypadku informacje uzyskane przez organ nadzorczy w związku ze zgłoszonym mu naruszeniem ochrony danych osobowych. W toku kontroli Prezes UODO ustalił, że przedsiębiorca nie dokonał analizy ryzyka dla operacji przetwarzania danych, co z kolei uniemożliwiło mu miarodajną ocenę wdrażanych środków służących bezpieczeństwu przetwarzania. Z zebranego materiału dowodowego w sprawie wynikało również, że przedsiębiorca nie zapewnił, aby osoby dopuszczone przez niego do przetwarzania danych czyniły to z jego upoważnienia i wyłącznie na jego polecenie. W toku postępowania przedsiębiorca nie przedstawił dowodów na to, że np. udzielił swoim pracownikom upoważnień do przetwarzania danych albo w inny sposób zapewnił, aby przetwarzali oni dane wyłącznie na jego polecenie. Kolejnym zarzutem postawionym przedsiębiorcy w toku postępowania był ten wskazujący na zaniechanie przez niego prowadzenia rejestru czynności przetwarzania, do czego był zobowiązany. Brak ww. rejestru uniemożliwiał mu przejrzyste skatalogowanie czynności przetwarzania w sposób umożliwiający przeprowadzenie w należyty sposób analizy ryzyk związanych z przetwarzaniem danych oraz dobranie adekwatnych środków zapewniających bezpieczeństwo przetwarzania danych osobowych.

W przedmiotowej sprawie administracyjne kary pieniężne nałożone zostały za naruszenie art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 32 ust. 1 i 2 oraz art. 29 i art. 32 ust. 4, jak również art. 30 ust. 1 i 3 rozporządzenia 2016/679. Przedstawiona decyzja jest prawomocna. Administracyjna kara pieniężna została zapłacona.

[131] DKN.5112.6.2020.
[132] DKN.5112.27.2022.

Nieprawidłowości związane z pełnieniem funkcji inspektora ochrony danych były podstawą do wydania kolejnej decyzji[133] Prezesa UODO nakładającej administracyjną karę pieniężną na podmiot **sektora prywatnego**. W toku postępowania ustalono, że funkcję inspektora ochrony danych (dalej jako IOD) w organizacji administratora pełniła osoba zajmująca równolegle (ze sprawowaniem funkcji IOD) stanowisko prezesa zarządu, co implikowało ocenę, że administrator naruszył spoczywający na nim obowiązek zapewnienia, by wykonywane przez IOD inne zadania i obowiązki nie powodowały konfliktu interesów (jak wymaga tego art. 38 ust. 6 rozporządzenia 2016/679).

W tym kontekście podkreślić należy, że Prezes UODO w swoich wystąpieniach wielokrotnie odnosił się do kwestii konfliktu interesów wśród osób pełniących funkcję IOD oraz dopuszczalności łączenia funkcji IOD z innymi stanowiskami – przy czym organ nadzorczy wyraźnie zaznaczał, że cyt.: „Niedopuszczalne jest powołanie na IOD osoby będącej kierownikiem (zarządzającym) podmiotem posiadającym status administratora lub podmiotu przetwarzającego, takich jak np. członka zarządu stowarzyszenia, dyrektora szkoły, wójta, członka zarządu spółki. Przyjęcie odmiennego stanowiska prowadziłoby do sytuacji, w których IOD w zakresie przestrzegania przepisów o ochronie danych osobowych – oceniałby i monitorował samego siebie". Ww. decyzja stanowiła zatem oczywiste potwierdzenie prezentowanego konsekwentnie stanowiska.

W przedmiotowej sprawie administracyjna kara pieniężna nałożona została za naruszenie przepisu art. 38 ust. 6 rozporządzenia 2016/679. Decyzja jest prawomocna, a nałożona przez Prezesa UODO administracyjna kara pieniężna została zapłacona przez administratora.

Inspiracją dla kolejnego postępowania administracyjnego z urzędu, zakończonego decyzją[134] nakładającą administracyjną karę pieniężną stały się ustalenia wskazujące na naruszenie przepisów rozporządzenia 2016/679, dokonane w wyniku czynności wyjaśniających podjętych w następstwie naruszenia ochrony danych osobowych notyfikowanego organowi nadzorczemu przez podmiot **sektora publicznego** i polegającego na zagubieniu przez byłego pracownika administratora prywatnego zewnętrznego nośnika danych (pendrive), na którym przetwarzane były dane osobowe wiążące się z funkcjonowaniem administratora (wypełnianiem jego zadań).

Przeprowadzone postępowanie wyjaśniające i administracyjne wykazało, że administrator w sposób nieprawidłowy przeprowadził analizę ryzyka związanego z realizowanymi procesami przetwarzania danych, tj. nie przewidział w niej zdarzenia będącego przyczyną wystąpienia przedmiotowego naruszenia (skopiowanie danych na prywatny nośnik, który następnie został zagubiony). Jednocześnie, z przekazanych przez administratora dokumentów wynikało, że obszar dotyczący możliwości przetwarzania danych przez pracowników na ich prywatnych nośnikach nie był w żaden sposób kontrolowany.

[133] DKN.5131.7.2025.
[134] DKN.5131.3.2024.

Wieńczącą postępowanie decyzją nałożono na administratora karę pieniężną za naruszenie przepisów art. 5 ust. 1 lit. f, art. 5 ust. 2, art. 25 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. Administrator w całości zaskarżył decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Również podmiotu **sektora publicznego** dotyczyła kolejna sprawa, w której Prezes UODO wydał decyzję[135] nakładającą administracyjne kary pieniężne zarówno na administratora, jak i na podmiot przetwarzający. Sprawa zainicjowana została uzyskaniem informacji wskazujących na naruszenie przepisów o ochronie danych osobowych dotyczących zapewnienia bezpieczeństwa dla przetwarzanych danych. Czynności w tym zakresie podjęte zostały w następstwie zgłoszenia naruszenia ochrony danych osobowych, do którego doszło w podmiocie przetwarzającym. Naruszenie ochrony danych osobowych było następstwem ataku ransomware, w wyniku którego zostały zaszyfrowane dane osobowe administratora. Co istotne, w przedmiotowej sprawie naruszenie zgłosił podmiot przetwarzający. Administrator także zgłosił to naruszenie ochrony danych osobowych, ale zrealizował swój obowiązek dopiero w toku postępowania administracyjnego prowadzonego przez Prezesa UODO niemal półtora roku od wystąpienia zdarzenia powodującego obowiązek zgłoszenia. W postępowaniu ustalono, że przed wystąpieniem naruszenia ochrony danych osobowych administrator oraz podmiot przetwarzający przeprowadzili analizę ryzyka. Podmiot przetwarzający nie uwzględnił jednak ryzyka zaszyfrowania danych w swojej analizie. Konsekwencją powyższego był brak wdrożenia adekwatnych środków bezpieczeństwa. Analiza ryzyka przeprowadzona przez samego administratora uwzględniała natomiast ryzyko związane z zaszyfrowaniem danych, ale działania kontrolne administratora względem podmiotu przetwarzającego w ww. obszarze, w związku z powierzeniem mu przetwarzania danych okazały się nieskuteczne.

Administracyjna kara pieniężna została nałożona na podmiot przetwarzający za naruszenie art. 32 ust. 1 i 2 w związku z art. 28 ust. 3 lit. c i lit. f rozporządzenia 2016/679, a na administratora za naruszenie art. 25 ust. 1, art. 28 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. Ponadto w tej sprawie Prezes UODO udzielił administratorowi upomnienia za naruszenie art. 33 ust. 1 rozporządzenia 2016/679, polegające na niezgłoszeniu Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Administrator oraz podmiot przetwarzający w całości zaskarżyli decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie.

Kolejna decyzja[136] wydana została po przeprowadzonej przez Prezesa UODO **kontroli w podmiocie publicznym**. W przedmiotowej sprawie, w związku ze stwierdzeniem naruszenia art. 32 ust. 1 i ust. 2 rozporządzenia 2016/679, Prezes UODO nałożył administracyjną karę pieniężną, a ponadto wydał nakaz dostosowanie operacji przetwarzania do przepisów rozporządzenia 2016/679. Administracyjna kara pieniężna została nałożona za brak zapewnienia odpowiedniego poziomu

[135] DKN.5131.30.2022.
[136] DKN.5112.10.2024.

bezpieczeństwa danych, które oparte powinno być na analizie ryzyka wiążącego się z ich przetwarzaniem oraz za niedostateczną kontrolę skuteczności zabezpieczeń. Stosowane przez administratora środki techniczne i organizacyjne były niewystarczające, a ich skuteczność nie była oceniana. Stwierdzone naruszenie przepisów rozporządzenia 2016/679 polegało m.in. na nieprzeprowadzeniu analizy ryzyka dla operacji przetwarzania danych osobowych w związku z prowadzeniem działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych. W toku kontroli ustalono również, że administrator nie stosował się do postanowień własnych regulacji dotyczących obszaru przetwarzania danych osobowych, czego wyrazem był m.in. brak analizy ryzyka dla procesów przetwarzania danych oraz brak szyfrowania nośników wykorzystywanych do przetwarzania danych.

Administrator złożył do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na przedmiotową decyzję Prezesa UODO.

W związku z niezgłoszeniem do organu nadzorczego naruszenia ochrony danych osobowych bez zbędnej zwłoki oraz za niezawiadomienie o tym osoby, której dane dotyczyły, Prezes UODO wydał decyzję[137] nakładającą administracyjną karę pieniężną na **komornika sądowego**.

Naruszenie polegało na omyłkowym wysłaniu pisma o zajęciu wynagrodzenia niewłaściwej osobie. Prezes UODO dowiedział się o tym w wyniku zawiadomienia osoby, która była nieuprawnionym odbiorcą tej korespondencji. Osoba ta zawiadomiła także komornika i wskazała, że obawia się, że także jej dane mogły być udostępnione niewłaściwemu adresatowi – jeśli ktoś przez pomyłkę pozamieniał koperty. W wyniku przeprowadzonego postępowania ustalono, że komornik nie powiadomił o incydencie ani Prezesa UODO, ani osoby, której dane dotyczyły. Administrator uznał, że zachodzi „małe prawdopodobieństwo", że zdarzenie to może doprowadzić do naruszenia praw lub wolności osoby, której dane dotyczą. Postępowanie Prezesa UODO wykazało, że nie miał podstaw do takiej oceny sytuacji, skoro w ogóle nie została wykonana analiza ryzyka naruszenia praw lub wolności osoby objętej naruszeniem.

Dopiero w korespondencji z Prezesem UODO administrator wyjaśnił, że nie zgłosił naruszenia organowi nadzorczemu i nie powiadomił o nim osoby, której dane dotyczą (nie zrealizował obowiązków wynikających z art. 33 i 34 rozporządzenia 2016/679), gdyż pomyłka była jednostkowym przypadkiem wśród tysięcy wysyłanych listów, a skoro omyłkowy odbiorca przesyłki z powagą podszedł do kwestii ochrony danych osobowych, to jest mało prawdopodobne, by zdarzenie to skutkowało ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą.

Decyzja została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie.

W kolejnej sprawie Prezes UODO wydał decyzję[138] nakładającą na **Komendanta Miejskiego Policji** dwie administracyjne kary pieniężne oraz

[137] DKN.5131.17.2024.
[138] DKN.5131.5.2024.

nakazującą dostosowanie operacji przetwarzania w ramach działalności prasowo-informacyjnej do przepisów rozporządzenia 2016/679.

Sprawa dotyczyła opublikowania na stronie internetowej komendy komunikatu prasowego, przygotowanego w odpowiedzi na reportaż telewizyjny o jednej z interwencji Policji. W treści komunikatu zamieszczono dane osobowe uczestniczki interwencji, w tym m.in. dane dotyczące stanu zdrowia. Dane te, wśród których znajdowały się szczególne kategorie danych osobowych w rozumieniu art. 9 ust. 1 rozporządzenia 2016/679, pozyskano z Systemu Wspomagania Dowodzenia Policji i wykorzystano w celu odmiennym od tego, w którym pierwotnie je zgromadzono. Prezes UODO stwierdził dwa odrębne naruszenia przepisów rozporządzenia 2016/679. Pierwsze polegało na niezgodnym z prawem przetwarzaniu danych osobowych, w tym szczególnych kategorii danych, poprzez ich opublikowanie na stronie internetowej bez jakiejkolwiek podstawy prawnej określonej w art. 6 ust. 1 oraz art. 9 ust. 1 rozporządzenia 2016/679, co skutkowało naruszeniem zasady zgodności z prawem (art. 5 ust. 1 lit. a) i zasady rozliczalności (art. 5 ust. 2). Drugie naruszenie polegało na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zaprojektowanych w celu skutecznej realizacji zasad ochrony danych (art. 25 ust. 1 i 2 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679), skutkującym naruszeniem zasady integralności i poufności (art. 5 ust. 1 lit. f) oraz zasady rozliczalności (art. 5 ust. 2). Komendant nie przeprowadził analizy ryzyka w obszarze publikacji komunikatów prasowych i nie testował skuteczności stosowanych zabezpieczeń.

Decyzja została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie.

### 7.3. Decyzje wydane w związku z kampanią wyborczą

W 2025 r. Prezes UODO udzielił upomnienia trzem komitetom wyborczym, których działania związane z prowadzeniem prezydenckiej kampanii wyborczej doprowadziły do naruszenia przepisów rozporządzenia 2016/679. W dwóch spośród wydanych decyzji[139] Prezes UODO stwierdził naruszenia obowiązków wynikających z art. 5 ust. 1 lit. a oraz art. 6 ust. 1 rozporządzenia 2016/679, natomiast w trzeciej decyzji[140] stwierdzono naruszenie z art. 5 ust. 1 lit. a, art. 6 ust. 1 oraz art. 9 ust. 1 rozporządzenia 2016/679.

Naruszenia przepisów rozporządzenia 2016/679 wynikały z ujawnienia przez komitety wyborcze, w trakcie prezydenckiej kampanii wyborczej, danych osobowych osób niepełniących funkcji publicznych, bez podstawy prawnej. Ww. decyzje stanowią istotny sygnał wskazujący, że doniosłe cele realizowane przez określonych administratorów (w tym przypadku związane z prowadzeniem kampanii wyborczej), nie usprawiedliwiają takich ich działań, które wiążą się z bezprawną ingerencją w podstawowe prawa podmiotowe. Prezes UODO zauważył, że publikowanie ściśle prywatnych informacji dotyczących życia osoby, której dane dotyczą, nie może być uzasadniane prawem do obrony, a zdecydowanie nie może być traktowane jako

[139] DKN.5131.9.2025, DKN.5131.11.2025.
[140] DKN.5131.10.2025.

ochrona żywotnych interesów tej osoby. Prezes UODO wskazał ponadto, że działanie administratora, polegające na ujawnieniu danych osobowych znajdujących się na listach poparcia kandydata nie stanowi realizacji celu bezpośrednio wskazanego przepisami Kodeksu Wyborczego. Prezes UODO podkreślił, że przyjęcie interesów komitetu wyborczego nie może nastąpić bez uwzględnienia możliwych konsekwencji dla osób, których dane dotyczą.

## 8. Sygnaliści

25 grudnia 2024 r. weszła w życie ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów[141] w części dotyczącej jej rozdziału 4, czyli zgłoszeń zewnętrznych. Zgodnie z art. 30 tej ustawy organy publiczne są zobowiązane do przyjmowania zgłoszeń zewnętrznych sygnalistów.

Prezes UODO zapewnił następujące kanały przyjmowania zgłoszeń zewnętrznych sygnalistów:

1) poczta tradycyjna (wymagane dopisanie na kopercie informacji o zgłoszeniu),
2) formularz na stronie internetowej urzędu,
3) kontakt telefoniczny.

W razie wskazania przez sygnalistę adresu poczty elektronicznej do kontaktu, korespondencja nadawana jest z dedykowanej skrzynki pocztowej, do której dostęp mają jedynie upoważnieni pracownicy.

Powyższe kanały komunikacji są niezależne od kanałów komunikacji wykorzystywanych w ramach zwykłej działalności organu, zapewniają kompletność, poufność i integralność danych, w tym ich zabezpieczenie przed dostępem osób nieupoważnionych. Pozwalają zarazem na przechowywanie informacji w sposób trwały w celu umożliwienia prowadzenia dalszego postępowania wyjaśniającego.

Zgłoszenia dotyczą zarówno naruszeń w sprawach indywidualnych, jak i naruszeń ochrony danych osobowych wielu osób. Dlatego do **obsługi zgłoszeń skierowano zarówno osoby mające wiedzę o postępowaniach w sprawach skarg osób, których dane dotyczą, jak i osoby z doświadczeniem w rozpatrywaniu zgłaszanych przez administratorów naruszeń.**

Każde zgłoszenie jest analizowane zgodnie z wymogami u.o.s. Prezes UODO dokonuje najpierw wstępnej weryfikacji zgłoszenia zewnętrznego. Polega ona na ustaleniu, czy zgłoszenie dotyczy informacji o naruszeniu prawa z dziedzin określonych u.o.s., a następnie, czy zgłoszenie dotyczy naruszeń prawa w dziedzinie należącej do zakresu działania Prezesa UODO, a jeżeli nie należy – na ustaleniu organu publicznego właściwego do podjęcia działań następczych. W takiej sytuacji zgłoszenie przekazywane jest do organu właściwego na wskazane przez niego kanały komunikacji dedykowane sygnalistom zewnętrznym. Jeżeli właściwy w sprawie jest

[141] Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. z 2024 r. poz. 928 ze zm.), zwana dalej: u.o.s.

Prezes UODO – zanonimizowane zgłoszenie przekazywane jest do komórki właściwej do podjęcia działań następczych. Jeśli działania takie nie mogą być podjęte bez ujawnienia tożsamości sygnalisty – organ występuje o zgodę na takie ujawnienie.

W 2025 r. do Urzędu Ochrony Danych Osobowych wpłynęło **299 zgłoszeń rozpatrywanych w ramach ustawy o ochronie sygnalistów.** Blisko 15 % stanowiły skargi indywidualne, których rozpatrzenie wymaga, po zawiadomieniu sygnalisty, ujawnienia jego danych osobowych[142]. Pozostałe zgłaszane były w interesie publicznym. Duża część zgłoszeń (ponad 10%) dotyczyła szeroko pojętego monitoringu w miejscu pracy. Powtarzalne były także zgłoszenia dotyczące nieodebrania uprawnień pracownikowi, który zakończył stosunek pracy, czy niewłaściwe zabezpieczenie i udostępnienie osobom nieuprawnionym danych osobowych.

Wejście w życie ustawy o ochronie sygnalistów implementującej dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1937 nadało Prezesowi UODO istotną funkcję systemową polegającą na wzmacnianiu bezpieczeństwa przetwarzania danych osobowych w skali całej administracji publicznej oraz sektora prywatnego. Zgłoszenia nieprawidłowości przez sygnalistów są wykorzystywane przez Prezesa UODO jako źródło dodatkowej informacji o stanie zabezpieczeń organizacyjnych i technicznych stosowanych przez administratorów. W związku z wpływem zgłoszeń dotyczących naruszeń przepisów Departament Kontroli i Naruszeń UODO dokonuje ich analizy pod kątem ryzyka systemowego. Oznacza to, że:

- identyfikowane są powtarzalne schematy nieprawidłowości w zakresie ochrony danych osobowych, np. niewłaściwe upoważnienia, nadmierne uprawnienia pracowników lub brak kontroli dostępów do danych osobowych,
- ustalane są przyczyny źródłowych naruszeń przepisów o ochronie danych osobowych, m.in. brak procedur, audytów, nieaktualne zabezpieczenia systemów teleinformatycznych,
- ocenie podlega charakter naruszenia – jednostkowy lub strukturalny w organizacji.

Zgłoszenia sygnalistów pozwalają Prezesowi UODO dodatkowo identyfikować zagrożenia prowadzące do masowych wycieków danych. W roku sprawozdawczym 2025 do Departamentu Kontroli i Naruszeń zostało przekazanych **41 zgłoszeń sygnalistów**. Na podstawie pozyskanych informacji Prezes UODO podejmował czynności wyjaśniające, a sygnały płynące od osób fizycznych pozwoliły m.in. zaplanować kontrole sektorowe.

Analizując zgłoszenia Prezes UODO wskazuje dobre praktyki dotyczące minimalizacji zakresu przetwarzania danych, zarządzania dostępami do systemów, rejestrowania operacji przetwarzania danych (logowanie zdarzeń), a także retencji i usuwania danych. Zgłoszenia sygnalistów obok zgłoszeń naruszeń ochrony danych ujawniają sposoby funkcjonowania organizacji. Reakcje Prezesa UODO na ww.

[142] Na zasadach określonych w art. 8 ust. 1-3 ustawy o ochronie sygnalistów.

zdarzenia podnoszą poziom bezpieczeństwa ochrony danych osobowych oraz cyberbezpieczeństwa. Podczas badania zgłoszeń Prezes UODO weryfikuje m.in. skuteczność wdrożonych zabezpieczeń. Obejmuje to w szczególności:

- ocenę funkcjonowania kontroli dostępu,
- analizę procedur reagowania na incydenty,
- ocenę bezpieczeństwa systemów teleinformatycznych,
- sprawdzenie zarządzania uprawnieniami.

Analiza zgłoszeń pozwala identyfikować strukturalne słabości w sposobie przetwarzania danych osobowych. Mechanizm sygnalizowania naruszeń jest narzędziem wzmacniającym stabilność i bezpieczeństwo całego systemu ochrony danych osobowych.

## 9. Współpraca z innymi organami w zakresie reagowania na incydenty bezpieczeństwa i naruszenia

Prezes UODO, wykonując zadania organu nadzorczego w rozumieniu art. 51-59 rozporządzenia 2016/679, prowadzi stałą współpracę z właściwymi organami krajowymi i zagranicznymi, których kompetencje pozostają w związku z zapewnieniem bezpieczeństwa informacji, cyberbezpieczeństwa oraz ochrony praw osób fizycznych. Współpraca ma charakter systemowy i wynika to z faktu, że naruszenia ochrony danych osobowych mogą stanowić jednocześnie zdarzenia o charakterze prawnym, technicznym, gospodarczym i społecznym. W związku z powyższym działania podejmowane są w koordynacji z innymi podmiotowo organami.

Prezes UODO współpracuje m.in. z:

1. podmiotami krajowego systemu cyberbezpieczeństwa, w tym zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);
2. organami ścigania i ochrony państwa;
3. organami regulacyjnymi i nadzorczymi właściwym sektorowo (Komisja Nadzoru Finansowego, Rzecznik Praw Obywatelskich, Rzecznik Praw Dziecka);
4. organami nadzorczymi państw członkowskich Unii Europejskiej.

Współpraca pozwala na pełną koordynację podejmowanych działań w związku z np. incydentami bezpieczeństwa teleinformatycznego. Zdarzenia tego rodzaju, w szczególności cyberataki, obejmują równocześnie kilka obszarów odpowiedzialności instytucjonalnej. Jedno zdarzenie może jednocześnie stanowić incydent w rozumieniu przepisów o krajowym systemie cyberbezpieczeństwa, prowadzić do naruszenia praw lub wolności osób fizycznych, wyczerpać znamiona czynu zabronionego oraz oddziaływać na stabilność sektora finansowego lub rynku usług. Przyjęty model współdziałania instytucyjnego obejmuje w szczególności wymianę informacji o incydentach i naruszeniach ochrony danych osobowych,

koordynację działań nadzorczych i kontrolnych, wzajemne wsparcie eksperckie oraz udział w postępowaniach transgranicznych.

Dzięki współpracy wzmacniany jest krajowy system reagowania na incydenty bezpieczeństwa poprzez skrócenie czasu identyfikacji naruszenia, zwiększenie skuteczności informowania podmiotów danych, umożliwienie równoległego prowadzenia działań technicznych i prawnych oraz ograniczenie skutków naruszeń, w tym kradzieży tożsamości, oszustw finansowych oraz nadużyć informacyjnych. Koordynacja podejmowanych działań zapewnia większą ochronę praw osób fizycznych.

## 10. 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 w rozdziale 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa UODO planem kontroli oraz zatwierdzanymi planami miesięcznymi.

Prezes UODO przeprowadził w 2025 r. czynności kontrolne w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych **w 76 podmiotach** (tj. o 52 % więcej niż w 2024 r., w którym przeprowadzono 50 kontroli). Wymienione działania były realizowane w wykonaniu uprawnień przysługujących organowi nadzorczemu na podstawie art. 58 rozporządzenia 2016/679. Na podstawie przyjętego na 2025 r. planu kontroli sektorowych przeprowadzono **41 kontroli. Pięć (5)** kontroli przeprowadzonych zostało w związku ze zgłoszonymi Prezesowi UODO przez administratorów **naruszeniami ochrony danych osobowych**. Przeprowadzono również **pięć (5)** kontroli przetwarzania danych osobowych **w Wielkoskalowych Systemach Unii Europejskiej**, w tym na podstawie art. 34 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym. Pozostałe **kontrole (25)** zostały podjęte w rezultacie uzyskania przez Prezesa UODO informacji o występujących nieprawidłowościach w związku z przetwarzaniem danych osobowych. Prezes UODO ponadto przeprowadził **dwadzieścia (20) sprawdzeń stosowania art. 11 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości**[143].

Zgodnie z planem kontroli sektorowych czynnościami kontrolnymi zostały objęte następujące zagadnienia: 1) przetwarzanie danych obejmujących wizerunki dzieci, gdy wymagana jest zgoda wyrażona przez rodziców lub opiekunów prawnych (12 kontroli), 2) realizacja obowiązku wynikającego z art. 33 ust. 5 rozporządzenia 2016/679, polegającego na dokumentowaniu wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte

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

działania zaradcze (17 kontroli), 3) sposób zapewnienia bezpieczeństwa danych osobowych pacjentów (7 kontroli), 3) przetwarzanie danych osobowych w Wielkoskalowych Systemach Unii Europejskiej (5 kontroli).

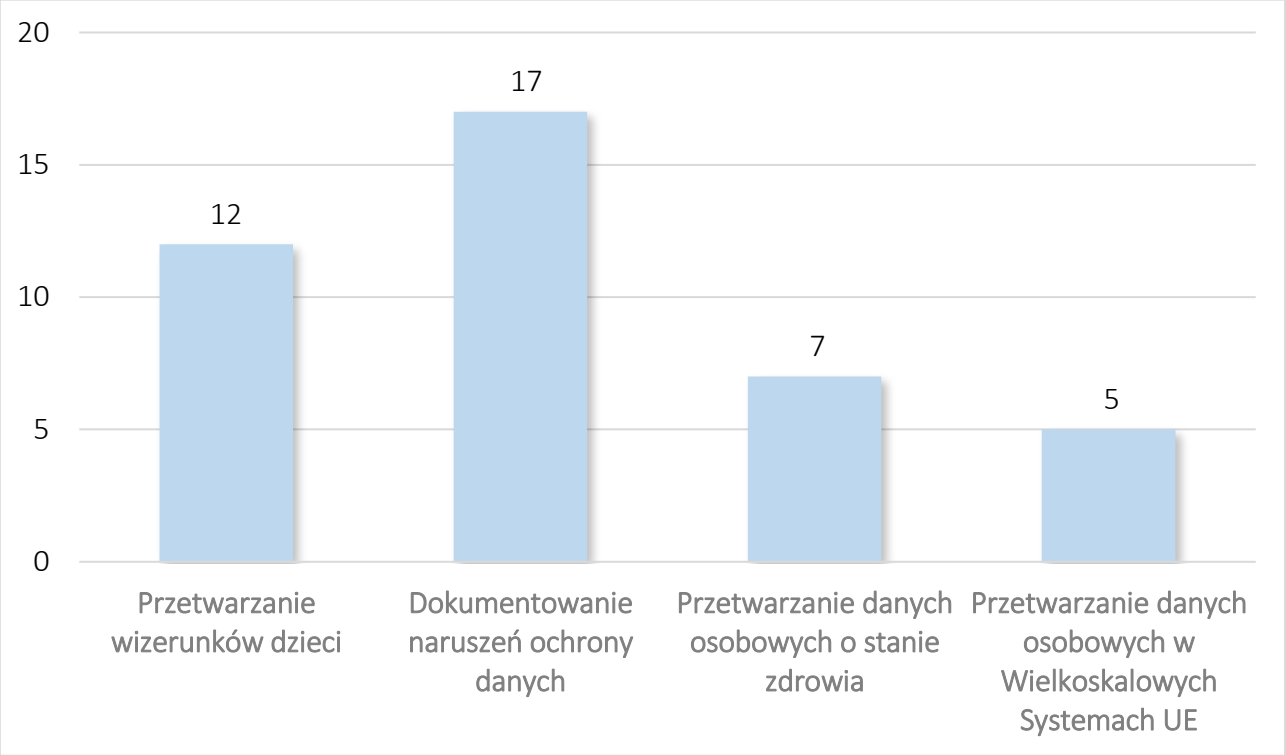
**Zgodnie z planem kontroli sektorowych UODO na 2025 r. czynnościami kontrolnymi zostały objęte:**

− szkoły i przedszkola – w zakresie prawidłowości przetwarzania wizerunków dzieci, gdy wymagana jest zgoda wyrażona przez rodziców lub opiekunów prawnych **(12 kontroli)**,

− podmioty przetwarzające dane osobowe – w zakresie realizacji obowiązku wynikającego z art. 33 ust. 5 rozporządzenia 2016/679, polegającego na dokumentowaniu wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze **(17 kontroli),**

- podmioty przetwarzające dane o stanie zdrowia – w zakresie sposobu zapewnienia bezpieczeństwa danych osobowych pacjentów **(7 kontroli),**

− organy przetwarzające dane osobowe w Wielkoskalowych Systemach Unii Europejskiej **(5 kontroli).**




**Wykres 5:** Liczba i zakres przeprowadzonych czynności kontrolnych, podjętych na podstawie planu kontroli sektorowych Prezesa UODO na 2025 r.

### 10.1. Przetwarzanie wizerunków dzieci

W ramach tego sektora przeprowadzono kontrole w placówkach edukacyjnych obejmujących szkoły (9), przedszkola (2) oraz placówkę opiekuńczo – wychowawczą socjalizacyjną (1).

Kontrolami objęto przetwarzanie danych osobowych w postaci wizerunku dzieci, gdy wymagana jest zgoda wyrażona przez rodziców lub opiekunów prawnych, w zakresie: celu przetwarzania danych osobowych, sposobu wyrażania zgody. Badając warunki wyrażenia zgody sprawdzano, w jaki sposób jest wyrażana oraz odwoływana, a w szczególności, czy klauzula o wyrażeniu zgody była przekazywana w łatwo dostępnej formie, jasnym i prostym językiem oraz czy miała miejsce rzeczywista dobrowolność wyrażenia zgody, która w praktyce oznacza, że można było ją wyrazić z osobna na różne operacje przetwarzania danych osobowych, wycofać lub odmówić jej udzielenia bez niekorzystnych konsekwencji.

W ramach przeprowadzonych kontroli ustalono, że dane w postaci wizerunku dzieci przetwarzane były w oparciu o zgodę przez placówki edukacyjne w celach ich promocji (udzielanie informacji o procesie edukacji oraz uzyskanych przez uczniów osiągnięciach w procesie edukacji i organizowanych konkursach). Przetwarzanie polegało na udostępnianiu wizerunku m.in. na stronie internetowej placówki edukacyjnej, profilu placówki na platformie Meta (Facebook) oraz YouTube. Podczas kontroli pojawiły się wątpliwości, czy stosowane przez placówki oświatowe zgody powinny być pozyskiwane odrębnie dla każdego miejsca publikacji danych dziecka (np. Facebook, You Tube) z uwagi na to, że dochodziło do przetwarzania danych przez różnych administratorów, czy też mogą być wyrażane łącznie dla wszystkich. W większości przypadków przedmiotowa zgoda pozyskiwana była w treści jednego oświadczenia, bez możliwości dokonania wyboru dla poszczególnych miejsc publikacji wizerunku.

Kolejną kwestią badaną w czasie kontroli był okres obowiązywania takiej zgody, a w związku z tym retencji danych, tj. wizerunku dziecka przetwarzanego na jej podstawie. Na podstawie analizy pozyskanych w toku kontroli materiałów dowodowych wynikało, że w większości placówek okres obowiązywania zgody nie był wskazany, natomiast w nielicznych przypadkach obejmował on okres edukacji dziecka w placówce.

Stwierdzono również przypadek udzielenia zgody na przetwarzanie wizerunku dziecka, o której mowa w art. 81 ust. 1 ustawy o prawie autorskim i prawach pokrewnych, bez udzielenia odrębnej zgody na podstawie rozporządzenia 2016/679.

### 10.2. Dokumentowanie naruszeń ochrony danych osobowych

W ramach tego sektora przeprowadzono **17 kontroli,** którymi objęto zarówno podmioty publiczne, jak i podmioty z sektora prywatnego. Przedmiot kontroli dotyczył realizacji obowiązku wynikającego z art. 33 ust. 5 rozporządzenia 2016/679. Obowiązek ten polega na dokumentowaniu wszelkich naruszeń ochrony danych osobowych w zakresie opracowania i wdrożenia procedur dotyczących realizacji obowiązku, o którym mowa w powołanym wyżej przepisie, zakresu i dokładności

gromadzenia dokumentacji dotyczącej wszelkich naruszeń ochrony danych osobowych, w tym dokumentowania okoliczności naruszenia ochrony danych osobowych, skutków naruszenia oraz podjętych działań zaradczych. Czynności kontrolne obejmowały również ustalenie, kto jest odpowiedzialny za prowadzenie takiej dokumentacji, w tym jej aktualizację.

Podsumowując ustalenia z kontroli sektorowych w zakresie realizacji ww. obowiązku wskazać należy, że w kontrolowanych podmiotach opracowane zostały i wdrożone procedury w przedmiocie dokumentowania naruszeń. Naruszenia ochrony danych osobowych dokumentowane były w rejestrze naruszeń, który zazwyczaj prowadzony był w formie elektronicznej, w tabeli w pliku EXCEL. W tabelach umieszczane były zwykle szczegółowe informacje dotyczące konkretnego naruszenia, w tym m.in. okoliczności wystąpienia naruszenia, jego skutki, podjęte działania zaradcze, informacje o zawiadomieniu, bądź niezawiadomieniu Prezesa Urzędu Ochrony Danych Osobowych. Co do zasady, dla każdego naruszenia zidentyfikowanego i ujawnionego w rejestrze naruszeń prowadzona była dokumentacja uzupełniająca, zawierająca m.in. korespondencję wewnętrzną dotyczącą konkretnego naruszenia.

W toku przeprowadzonych czynności kontrolnych ustalono, że zarządzanie naruszeniami ochrony danych osobowych oraz zarządzanie incydentami bezpieczeństwa informacji określają szczegółowe procedury. W szczególności rejestracji podlegają: okoliczności naruszenia, analiza ryzyka dla podmiotu danych, realizacja obowiązków z art. 33 oraz 34 rozporządzenia 2016/679 oraz podejmowane środki zaradcze i naprawcze.

Większość odnotowanych naruszeń wynikała z błędu ludzkiego, np. przekazania danych osobie nieuprawnionej, wysłania dokumentów osobie trzeciej, zagubienia przesyłki przez operatora pocztowego lub dostarczenia przesyłki niewłaściwemu adresatowi.

Zgłoszenia naruszeń najczęściej były dokonywane za pośrednictwem poczty elektronicznej (email), podczas rozmowy telefonicznej lub osobiście. W ramach procedowania naruszeń ochrony danych osobowych podmioty gromadziły dowody w formie m.in. zrzutów ekranu, logów systemowych, komunikatów, dokumentów papierowych, zdjęć pomieszczeń lub sprzętu związanego z danym incydentem. Informacje o wszystkich incydentach na bieżąco odnotowywane były w prowadzonym przez większość podmiotów rejestrach incydentów. Niektóre podmioty z każdego incydentu naruszenia danych osobowych sporządzały raport naruszenia bezpieczeństwa danych osobowych. Na podstawie zgromadzonego materiału dotyczącego incydentu administrator podejmował decyzję o zgłoszeniu lub niezgłoszeniu do organu nadzorczego danego naruszenia oraz zakres ewentualnych działań zaradczych.

Największe wątpliwości ujawnione w toku kontroli dotyczyły roli inspektora ochrony danych w procesie dokumentowania naruszeń. W kilku podmiotach czynności dotyczące dokumentowania naruszeń były realizowane przez inspektora ochrony danych, jego zastępcę bądź też zespół inspektora ochrony danych, który bezpośrednio mu podlegał. W omawianych podmiotach zmiana w tym zakresie nie była poprzedzona

utrwaloną na piśmie analizą konfliktu interesów. Podmioty te wskazywały, że w ich ocenie taki konflikt interesów nie zachodzi.

### 10.3. Bezpieczeństwo danych osobowych pacjentów

Zakresem kontroli objęto sposób zapewnienia bezpieczeństwa danych osobowych pacjentów przetwarzanych przez jednostki medyczne: szpitale, jednostki naukowo-badawcze i przychodnie. Kontrolą objęto **7 podmiotów**.

Kontroli poddano m.in. następujące zagadnienia: ustalenie czy są prowadzone szkolenia, sposób zarządzania nadawaniem uprawnień do systemu informatycznego, w którym przetwarzane są dane osobowe pacjentów oraz sposób prowadzenia polityki tworzenia i utrzymywania kopii zapasowych tych systemów, wdrożenie odpowiednich środków technicznych i organizacyjnych ochrony danych, wprowadzenie odpowiednich procedur i polityk bezpieczeństwa danych.

**Nieprawidłowości w procesie przetwarzania przez poddanych kontroli administratorów danych osobowych dotyczyły następujących kwestii:**

1. Niezapewnienia szkoleń uzupełniających z zakresu ochrony danych osobowych dla pracowników oraz szkoleń specjalistycznych dla personelu IT.

Ustalono, że prowadzone były szkolenia z zakresu ochrony danych osobowych jedynie dla osób nowo zatrudnionych. Natomiast administrator nie zapewniał dla swoich pracowników żadnych dodatkowych szkoleń uzupełniających z zakresu ochrony danych osobowych, jak i szkoleń specjalistycznych dla personelu IT. Ogranicza to zdolność administratora do właściwego zarządzania ryzykiem związanym z przetwarzaniem danych osobowych, albowiem nieprzeszkoleni pracownicy mogą nie posiadać wystarczającej wiedzy i świadomości ewentualnych zagrożeń ani też wystarczających umiejętności w zakresie reagowania i zapobiegania incydentom. Brak szkoleń specjalizacyjnych może przyczyniać się do wzrostu ryzyka błędów technicznych i konfiguracyjnych, które prowadzą do naruszenia poufności, dostępności lub integralności danych. Stanowi to naruszenie obowiązku, o którym mowa w art. 24 ust. 1, art. 32 ust. 1 lit. b rozporządzenia 2016/679, a także naruszenie zasady integralności i poufności określonej w art. 5 ust. 1 lit. f rozporządzenia 2016/679.

2. Niewdrożenia przez administratora opracowanych procedur dotyczących ochrony danych osobowych.

Z przeprowadzonych kontroli wynikało, że w niektórych podmiotach nie były stosowane m.in. zasady dotyczące nadawania i odbierania uprawnień do systemów informatycznych, które wynikały z przedłożonych w toku kontroli procedur. Niewdrożenie przez administratora tych procedur naruszało art. 5 ust. 2 i art. 24 ust. 1 w związku z art. 32 ust. 1 rozporządzenia 2016/679.

3.Niezapewnienia rozliczalności użytkowników systemów informatycznych użytkowanych przez administratora (brak rejestrów logowania, pobierania plików, zmian w plikach).

Stwierdzono w niektórych podmiotach, że systemy informatyczne służące do przetwarzania danych osobowych uniemożliwiały prowadzenie rozliczalności użytkowników systemów (brak było rejestrów logowania, pobierania plików, zmian w plikach). Ponadto brak było zarządzania uprawnieniami i kontrolą dostępu do danych osobowych, gdyż nie było ewidencjonowane zarówno nadawanie, jak i odbieranie uprawnień do systemów informatycznych. Brak było też dowodów potwierdzających dostępy administracyjne do systemów, nie były też prowadzone wykazy osób i podmiotów mających zdalny dostęp do systemów informatycznych. W pewnych podmiotach nie wykazano, czy stosowany jest Active Directory lub inna technologia w celu centralnego zarządzania całym zbiorem użytkowników w sieci oraz wskazaniem uprawnień użytkowników do zasobów sieciowych.

Brak rozliczalności w zakresie zarządzania uprawnieniami i kontrolą dostępu do danych osobowych przetwarzanych w systemach informatycznych naruszały obowiązek zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzania danych osobowych, o którym mowa w art. 32 ust. 2 lit. c rozporządzenia 2016/679, a także zasadę rozliczalności, o której mowa w art. 5 ust. 2 tego aktu.

4. Przechowywania kopii zapasowych systemu operacyjnego w tym samym miejscu co baza danych.

Ustalenia kontroli wykazały, że niektórzy administratorzy danych przechowywali kopie zapasowe w tym samym miejscu, w którym zlokalizowana była cała baza danych. Taka sytuacja niesie za sobą zagrożenia dotyczące utraty dostępności danych osobowych lub utraty danych osobowych, albowiem w przypadku zdarzeń losowych takich jak np. pożar, zalanie, awaria zasilania, lub celowego działania osób trzecich (np. ataku ransomware), zarówno dane produkcyjne, jak i ich kopie mogą zostać jednocześnie zniszczone lub zaszyfrowane. Taki stan rzeczy był również niezgodny z podstawowymi zasadami bezpieczeństwa informacji określonymi m.in. w normie ISO/IEC 27001, która zaleca fizyczne i logiczne rozdzielenie środowisk produkcyjnych i backupowych. Brak takiego rozdzielenia znacząco obniżało odporność administratora danych na incydenty i uniemożliwiało skuteczne odtworzenie danych po awarii.

W takich przypadkach należy uznać, że administrator danych nie zapewniał zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, co narusza art. 32 ust. 1 lit. c rozporządzenia 2016/679 oraz zasadę integralności i poufności określoną w art. 5 ust. 1 lit. f rozporządzenia 2016/679.

6. Niedokonywaniu przez administratora testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych oraz niewykonywaniu testów przywracania systemu z kopii.

Stwierdzono, że zdarzały się przypadki niedokonywania przez administratorów testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych. Ponadto nie były wykonywane testy przywracania systemu z kopii.

Brak testowania przywracania danych z kopii zapasowych oznacza, że administrator nie spełniał wymogu weryfikacji skuteczności środka technicznego mającego na celu zapewnienie dostępności i integralności danych osobowych w razie incydentu fizycznego lub technicznego. Środek ten stawał się w praktyce niezweryfikowany, co prowadziło do naruszenia obowiązku określonego w art. 32 ust. 1 lit. d rozporządzenia 2016/679 i było sprzeczne z zasadą integralności i poufności określoną w art. 5 ust. 1 lit. f rozporządzenia 2016/679 oraz zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO.

7. Braku rozliczalności w zakresie fizycznego dostępu do serwerowni.

W jednym z kontrolowanych podmiotów klucze do serwerowni przechowywane były w pomieszczeniu portierni, natomiast drugi komplet kluczy do serwerowni przechowywany był w pokoju informatyków. Fakt pobrania i zdania kluczy nie był w żaden sposób ewidencjonowany ani rozliczany. Administrator nie dysponował zatem dowodami pozwalającymi jednoznacznie ustalić, kto i na jakiej podstawie uzyskał dostęp do infrastruktury, w której przetwarzane były dane osobowe. Brak rozliczalności w tym zakresie uniemożliwiał także ustalenie, czy dostęp do serwerowni posiadały wyłącznie osoby upoważnione. Skutkiem tego mógł być brak możliwości ewentualnej identyfikacji potencjalnych incydentów naruszenia poufności.

Brak rozliczalności w opisanej sytuacji naruszał obowiązek zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzania danych osobowych, o którym mowa w art. 32 ust. 2 lit. c rozporządzenia 2016/679 i tym samym naruszał zasadę integralności i poufności, o której mowa art. 5 ust. 1 lit. f rozporządzenia 2016/679.

### 10.4. Przetwarzanie danych osobowych w Wielkoskalowych Systemach UE

W ramach tego sektora przeprowadzono kontrole w Ministerstwie Rozwoju i Technologii, Ministerstwie Spraw Zagranicznych oraz Urzędzie do Spraw Cudzoziemców. Ponadto skierowano do inspektorów ochrony danych powołanych przez Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Żandarmerii Wojskowej, Służby Ochrony Państwa i Krajowej Administracji Skarbowej wnioski o przeprowadzenie sprawdzeń w trybie ustawy grudniowej w zakresie dokonania kontroli logów SIS.

#### 10.4.1. Wizowy System Informacyjny (VIS)

Wizowy System Informacyjny (VIS) służy wymianie danych wizowych między Państwami Członkowskimi, który umożliwia upoważnionym do tego celu władzom krajowym wprowadzanie i uaktualnianie danych wizowych oraz elektroniczną konsultację tych danych. VIS zawiera dane na temat wniosków wizowych, decyzji wizowych, wydanych, cofniętych i unieważnionych wiz Schengen. W Polsce węzłem krajowym jest Centralny Organ Techniczny Krajowego Systemu Informatycznego, którym jest Komendant Główny Policji. Wszystkie instytucje krajowe (Ministerstwo Spraw Zagranicznych, Urząd do Spraw Cudzoziemców, Straż Graniczna, i inne wymienione w ustawie o udziale Rzeczypospolitej Polskiej w SIS i VIS) komunikują się z centralnym VIS poprzez Krajowy System Informatyczny. Zgodnie z art. 41 ust. 3

rozporządzenia 767/2008 w sprawie VIS, organ nadzorczy, o którym mowa w art. 51 ust. 1 rozporządzenia (UE) 2016/679, zapewnia przeprowadzenie co najmniej raz na cztery lata kontroli – zgodnie z odpowiednimi międzynarodowymi standardami przeprowadzania kontroli – operacji przetwarzania danych przez odpowiedzialne organy krajowe. Wyniki tej kontroli mogą być uwzględniane w ocenach przeprowadzanych w ramach mechanizmu ustanowionego rozporządzeniem Rady (UE) nr 1053/2013. Ostatnia kontrola w rozumieniu art. 41 ust. 3 rozporządzenia 767/2008 miała miejsce w październiku 2021 r. w Centralnym Organie Technicznym Krajowego Systemu Informacyjnego, którym jest Komendant Główny Policji. Kontrola w Ministerstwie Spraw Zagranicznych została prowadzona w oparciu o Wspólne Ramy Inspekcji, opracowane przez Grupę ds. Koordynacji Nadzoru nad VIS, zwracając szczególną uwagę na kwestie wynikające z zaleceń Ewaluacji Schengen w 2024 r.

### 10.4.2. Kontrola w Ministerstwie Rozwoju i Technologii w zakresie IMI

Kontrola w Ministerstwie Rozwoju i Technologii w zakresie nadawania uprawnień w IMI, wynikała z przyjętego skoordynowanego zadania Komitetu Skoordynowanego Nadzoru (CSC). W trakcie kontroli skupiono się w szczególności na procedurach nadzoru na poziomie krajowym nad nadawaniem uprawnień do systemu, określeniu roli danego podmiotu – Komisji Europejskiej i organu państwa członkowskiego zarządzającego IMI, prawidłowości sporządzenia klauzuli informacyjnej przez Ministerstwo w zakresie wskazania administratora oraz podmiotu przetwarzającego dane w systemie na zlecenie administratora.

### 10.4.3. Kontrola w Urzędzie do Spraw Cudzoziemców

W 2025 r. Prezes UODO przeprowadził kontrolę w Urzędzie do Spraw Cudzoziemców w zakresie realizacji prawa dostępu do danych w systemie EURODAC. Zgodnie z art. 29 ust. 4 i 5 rozporządzenia nr 603/2013, cudzoziemiec ma prawo do uzyskania informacji o danych, które go dotyczą, zapisanych w systemie Eurodac oraz o państwie członkowskim, które przesłało je do tego systemu. Cudzoziemiec, którego dane daktyloskopijne zostały przesłane do systemu Eurodac, jest uprawniony do złożenia ustnie do protokołu lub pisemnie wniosku o sprawdzenie swoich danych w systemie Eurodac. Cudzoziemiec powinien złożyć wniosek do Szefa Urzędu do Spraw Cudzoziemców. Sposób składania tego rodzaju wniosków określają przepisy ogólne, tj. Kodeks postępowania administracyjnego. Nie przewidziano szczególnego wzoru formularza. Każdy zainteresowany może wystąpić z wnioskiem na piśmie, ustnie do protokołu, a także za pomocą e-PUAP lub usługi e-doręczenia. W toku kontroli badany był proces procedowania takiego wniosku przez Szefa Urzędu do Spraw Cudzoziemców.

### 10.4.4. Wydział Konsularny i Polonii Ambasady RP w Rabacie

Zakresem kontroli zostało objęte przetwarzane przez Konsulat RP danych osobowych w związku z dostępem do Krajowego Systemu Informatycznego, w celu dokonywania wpisów danych VIS oraz wglądu do danych VIS i danych SIS.

W toku prowadzonych czynności kontrolnych odebrano od Konsula RP ustne wyjaśnienia na okoliczność m.in. zapewnienia bezpieczeństwa, zgodności i aktualności przetwarzanych danych, spełnienia obowiązków informacyjnych oraz dokonano oględzin serwerowni oraz budynku i pomieszczeń, w których wykonywane były czynności związane z procesem wydawania wiz. W procesie wydawania wiz zachowana była retencja danych, przetwarzanie danych w VIS i SIS odbywało się na podstawie stosownych upoważnień przez stałych pracowników przeszkolonych z zakresu bezpieczeństwa informacji.

### 10.4.5. Kontrola u Komendanta Głównego Straży Granicznej

Kontrolę przeprowadzono u Komendanta Głównego Straży Granicznej pełniącego funkcję Centralnego Organu Technicznego Krajowego Systemu Informatycznego EES oraz Krajowej Jednostki do spraw EES, który na mocy ustawy z dnia 18 października 2024 r. o udziale Rzeczypospolitej Polskiej w Systemie Wjazdu/Wyjazdu[144] oraz dyspozycji określonej w art. 15 ust. 1 tejże ustawy, wniósł o przeprowadzenie kontroli w zakresie spełnienia przez KSI EES wymogów określonych w przepisach o ochronie danych osobowych. Jak ustalono, Komendant Główny Straży Granicznej zawarł z organami uprawnionymi do dostępu bezpośredniego/pośredniego do KSI EES, porozumienia w sprawie dostępu do KSI EES, w których określił m.in. wymagania dla osób, które będą miały dostęp oraz kwestie zgłaszania incydentów.

System KSI EES w obszarze bezpieczeństwa podlegał wymogom funkcjonującego w SG Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), z uwzględnieniem odrębności wynikających z przepisów prawa (np. dodatkowe szkolenia). Ponadto działał w odseparowanym środowisku informatycznym (sieć i systemy) bez dostępu do globalnego Internetu. Wdrożone też zostały techniczne systemy zabezpieczeń, takie jak system antywirusowy z aktualną bazą sygnatur wirusów; system IDS/IPS (system wykrywania i zapobiegania włamaniom); system wykrywania i reagowania na zagrożenia urządzeń końcowych EDR. Spełnianie wymogów rozporządzenia 2016/679 jest w trakcie analizy.

## 10.5. Kontrole w wyniku zgłoszonego naruszenia

1) Do najistotniejszych kontroli przeprowadzonych w związku ze zgłoszonym naruszeniem należała kontrola u Głównego Geodety Kraju (Główny Urząd Geodezji i Kartografii), Prezydenta Miasta Bytom oraz w podmiocie świadczącym usługi informatyczne na rzecz organów samorządu terytorialnego.

Kontrolą u **Głównego Geodetę Kraju (GGK)** objęto przetwarzanie danych osobowych przy wykorzystaniu funkcjonalności usługi weryfikacji danych osobowych w rejestrze PESEL za pomocą Zintegrowanego Systemu Informacji o Nieruchomościach.

[144] Dz. U z 2024 r. poz. 1688.

Podstawę prawną do stworzenia i utrzymywania Zintegrowanego Systemu Informacji o Nieruchomościach (ZSIN) stanowią przepisy ustawy z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne[145]. Decyzją z 28 stycznia 2016[146] oraz decyzją z 1 lutego 2016 r.[147] Minister Cyfryzacji wyraził zgodę na udostępnienie Głównemu Geodecie Kraju danych z rejestru PESEL za pomocą urządzeń teletransmisji danych. Kwestię komunikacji ZSIN z rejestrem PESEL reguluje rozporządzenie Rady Ministrów z dnia 14 października 2022 r. w sprawie zintegrowanego systemu informacji o nieruchomościach[148]. Z kolei wewnętrznym zarządzeniem określono zasady zdalnego dostępu do zasobów teleinformatycznych i wniosku o przyznanie/odebranie uprawnień dostępu do ZSIN.

W systemie ZSIN została zaimplementowana integracja z następującymi rejestrami publicznymi: EGiB (Ewidencja Gruntów i Budynków); KSEP; Księgi Wieczyste; REGON; TERYT; PESEL; PRG; EPN. Podstawową funkcją ZSIN było prowadzenie centralnego repozytorium kopii zbiorów danych EGiB zgromadzonych w powiatowych bazach danych (tzw. Centralne Repozytorium ZSIN), a także wymiana i weryfikacja danych pomiędzy EGiB a innymi rejestrami publicznymi. Jednym z komponentów systemu ZSIN była szyna usług ZSIN, która udostępniała publiczne usługi systemu ZSIN (dostępne dla systemów/użytkowników zewnętrznych), a także stanowiła punkt dostępowy dla systemu ZSIN do usług zewnętrznych (w tym rejestru PESEL). Szyna usług zapewniała separację systemu ZSIN od sieci publicznych i innych sieci dostępowych. Główny Urząd Geodezji i Kartografi (GUGiK) pełnił funkcję punktu dostępowego zapewniającego przepływ informacji m.in. pomiędzy EGiB a rejestrem PESEL oraz umożliwiał – poprzez mechanizmy logów – pełną rozliczalność wykonywanych zapytań do rejestru PESEL. Nie były natomiast odkładane informacje zawierające odpowiedzi z rejestru PESEL.

W toku kontroli ustalono również, że doszło do zdarzenia polegającego na nieskutecznym (pomimo złożonego wniosku) cofnięciu uprawnień dostępu do portalu ZSIN dla byłego pracownika Urzędu Miasta Bytomia. Jak ustalono, było to spowodowane nieodebraniem ról podczas blokowania konta. Od czasu ujawnienia zdarzenia wprowadzony został obowiązek sprawdzania, czy proces blokowania przebiega prawidłowo oraz czy w systemie zapisało się działanie odebrania ról i zablokowania konta.

W związku z tym, że zdarzenie opisane powyżej było związane również z jednostką terenową GUGiK, kontrolą objęto również przetwarzanie przez **Urząd Miejski w Bytomiu** danych osobowych w identycznym zakresie.

W toku kontroli ustalono, że w Urzędzie Miejskim w Bytomiu wykorzystywany był system Geo-Info opracowany przez prywatny podmiot, służący do prowadzenia geodezyjnych baz danych, w szczególności ewidencji gruntów i budynków; geodezyjnej ewidencji sieci uzbrojenia terenu (GESUT); bazy danych obiektów topograficznych (BDOT500); rejestru cen nieruchomości (RCN); bazy danych

[145] Dz. U z 2024 r. poz. 1151 ze zm.
[146] znak: DEP-WUD-6173-2-23/16.
[147] znak: DEP-WUD-6173-9-8/16.
[148] Dz. U. poz. 2469 ze zm.

szczegółowych osnów geodezyjnych (BDSOG). Zapytania do rejestru PESEL w ramach okresowej weryfikacji danych w zakresie zgodności danych z bazą EGiB były realizowane wyłącznie w ramach działania dedykowanego narzędzia zaimplementowanego w 2022 r. w systemie do prowadzenia geodezyjnych baz danych Geo-Info. Narzędzie to automatycznie i cyklicznie weryfikowało dane osób fizycznych poprzez porównanie danych zgromadzonych w powiatowej bazie EGiB z rejestrem PESEL. Odbywało się to po godzinach pracy urzędu, aby nie zakłócać bieżącej pracy w systemie. Mogło to odbywać się podczas nieobecności osoby, której konto było wykorzystywane do sprawdzania danych, ponieważ działanie było całkowicie automatyczne, wykonywane według harmonogramu i nie wymagało działania operatora. Mechanizm ten musiał być powiązany z indywidualnym kontem użytkownika. Wynikiem działania była informacja zwrotna: zgodne/niezgodne. Mechanizm nie pobierał, nie zapisywał i nie aktualizuował żadnych danych w bazie danych EGiB na podstawie rejestru PESEL. Ponadto, jak zostało to już opisane powyżej, skierowano do Głównego Geodety Kraju wniosek o cofnięcie byłemu pracownikowi Urzędu Miasta Bytom wszystkich uprawnień wynikających z dostępu do kont zarządzanych przez Główny Urząd Geodezji i Kartografii. Jednakże z uwagi na to, że konto to było powiązane z procesem automatycznej weryfikacji danych z ewidencji gruntów i budynków z rejestrem PESEL oraz, że w tym zakresie nie zostało wyłączone, nadal automatyczna weryfikacja była realizowana. Urząd Miejski w Bytomiu nie miał zatem świadomości, że pomimo złożenia ww. wniosku narzędzie cyklicznej weryfikacji w dalszym ciągu operowało na wskazanym koncie.

Wstępna analiza zebranego materiału wskazywała na konieczność zbadania rozwiązań dotyczących automatycznej weryfikacji danych z rejestrem PESEL pod kątem rozliczalności tej usługi. Natomiast w odniesieniu do zdarzenia polegającego na nieskutecznym cofnięciu uprawnień, z ustaleń kontroli wynikało, że było to zdarzenie incydentalne, błąd pracownika, który w przedmiotowej sprawie nie skutkował ryzykiem naruszenia praw i wolności osób, których dane były weryfikowane w rejestrze PESEL.

2) W związku z innym zgłoszonym naruszeniem przeprowadzono kontrolę w podmiocie zajmującym się **budowaniem (produkowaniem) baz danych telefonicznych** w oparciu o wyrażoną zgodę na przetwarzanie numeru telefonu. Celem tworzenia baz danych było udzielenie czasowej licencji na korzystanie z bazy danych przez kontrahenta podmiotu (licencjobiorcę) w celu m.in. prowadzenia przez niego telemarketingu usług własnych. Umowa licencyjna obejmowała m.in. oświadczenia podmiotu jako licencjodawcy o posiadaniu zgód na przetwarzanie danych oraz oświadczenie o spełnieniu względem osób, których dane dotyczą, obowiązków wynikających z rozporządzenia 2016/679, a także postanowienie o uregulowaniu w załączniku treści zgód jakie będą pozyskiwane. Treści cyfrowe służące budowaniu bazy danych były prezentowane za pośrednictwem strony www.mojakolorowanka.pl, gdzie można było pobrać kolorowankę po udostępnieniu numeru telefonu i potwierdzeniu udostępnienia za pomocą kodu przesłanego SMS-em. Potwierdzenie kodem było wymagane ze względu na zapewnienie

bezpieczeństwa przed wykorzystaniem numeru telefonu przez osobę/osoby niebędące ich prawnym użytkownikiem/właścicielem, jak również uniknięcia stosowania mechanizmu „botów". Po potwierdzeniu kodem możliwe było udzielenie podmiotowi zgody na korzystanie z udostępnionego numeru telefonu dla celów prowadzonej działalności oraz zapoznanie się z obowiązkiem informacyjnym. Obowiązek informacyjny był realizowany za pośrednictwem strony internetowej www.mojakolorowanka.pl pod treścią formularza zgód, gdzie zawarta była aktywna zakładka „Klauzula informacyjna" oraz aktywna zakładka „Zrezygnuj" umożliwiająca nawiązanie kontaktu z podmiotem i przesłanie wiadomości, m.in. wniosku o wycofanie zgody/zgód. W zakresie objętym przedmiotową kontrolą, po dokonaniu analizy zebranego materiału dowodowego, nie stwierdzono naruszenia przepisów o ochronie danych osobowych w związku z przetwarzaniem przez spółkę danych w postaci numeru telefonu. Wyrażone przez podmiot danych zgody spełniały kryteria określone w art. 4 pkt 11 rozporządzenia 2016/679. Sposób wyrażenia zgody (zaznaczenie pustego okienka) wskazywało na wyraźne i świadome działanie osoby, której dane dotyczą, jednocześnie zapewniając, aby zgoda była wyrażona w sposób dobrowolny, konkretny i świadomy. Pozostają również w zgodzie z wymogami art. 7 rozporządzenia 2016/679, ponieważ zostały zredagowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, nie były powiązane z innymi kwestiami. Nadto usługi oferowane przez spółkę nie były uzależnione od wyrażenia zgody.

### 10.6. Wystąpienia o przeprowadzenie sprawdzeń

W analizowanym roku sprawozdawczym skierowano do inspektorów ochrony danych u **Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Żandarmerii Wojskowej, Służby Ochrony Państwa i Krajowej Administracji Skarbowej/Mazowieckiego Urzędu Celno-Skarbowego w Warszawie** wystąpienia o przeprowadzenie sprawdzeń zapisów w rejestrze N.SIS, o którym mowa w art. 12 w związku z art. 10, art. 13 i art. 66 ust. 2 rozporządzenia 2018/1862 oraz art. 31 ust. 1 pkt 2 i pkt 6 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Sprawdzenie miało objąć zapisy pierwszej i ostatniej (w danym dniu) operacji przetwarzania danych do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych, ścigania ich lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom odnotowanych 3 czerwca 2025 r., 17 lipca 2025 r., 21 sierpnia 2025 r. – w zakresie ustalenia w stosunku do każdego z ww. zapisów:

1. Czy operacje przetwarzania wykonywali użytkownicy posiadający ważne upoważnienia?
2. Czy dostęp do danych nie wykraczał poza zakres obowiązków służbowych użytkownika?
3. Czy wystąpiły przypadki aktywności użytkownika w czasie, w którym nie powinien wykonywać czynności służbowych?

W razie braku zapisów w powyższych dniach IOD miał przeanalizować najbliższy kolejny dzień, w którym odnotowano operacje przetwarzania, przedstawiając dowody na brak operacji we wskazanych terminach.

Ponadto zobowiązano do wskazania, czy w ciągu ostatnich 6 miesięcy występowały nietypowe zdarzenia w rejestrze N.SIS, na przykład: nagły wzrost liczby operacji przetwarzania przez danego użytkownika w krótkim odstępie czasu, wielokrotne nieudane próby logowania, logowania z nietypowych lokalizacji lub inne odstępstwa od standardowych wzorców aktywności.

Skierowano również do inspektorów ochrony danych w: **Komendach Powiatowych Policji**, **Komendzie Miejskiej Policji** oraz w **Oddziałach Straży Granicznej** łącznie 15 wystąpień o dokonanie sprawdzenia w przedmiocie ustalenia, czy w okresie od 1 stycznia do 30 sierpnia 2025 r. realizowano obowiązek, o którym mowa w art. 23 ust. 3 ustawy z dnia 14 grudnia 2018 r., to jest czy informowano osobę, której dane dotyczą, o przyczynach odmowy lub ograniczenia dostępu oraz o możliwości wniesienia do Prezesa Urzędu skargi w przypadku naruszenia praw osoby w wyniku przetwarzania jej danych osobowych w celach określonych w art. 1 ust. 1 pkt 1 ww. ustawy, w odniesieniu do zbiorów danych osobowych utworzonych przez administratora w celu realizacji swoich ustawowych zadań. Jeżeli nastąpiła odmowa lub ograniczenie dostępu, należało ustalić przyczynę i zasadność takiej decyzji. Łącznie przeprowadzono 20 sprawdzeń.

## 11. Zawiadomienia o podejrzeniu popełnienia przestępstwa

W analizowanym 2025 roku Prezes UODO złożył **8 zawiadomień o podejrzeniu popełnienia przestępstwa.**

Pierwsze zawiadomienie[149] dotyczyło wygenerowania przez uczniów z podwarszawskiej szkoły podstawowej zdjęć nagiej koleżanki, którzy zachęcali jednocześnie innych do wykorzystywania jej wizerunku stworzonego w aplikacji. Osoba, której wizerunek został zmodyfikowany przy użyciu aplikacji wykorzystującej sztuczną inteligencję, była osobą małoletnią poniżej 15. roku życia i istniało wysokie prawdopodobieństwo jej identyfikacji. Postępowanie kolegów nie tylko naruszyło drastycznie prywatność dziewczyny, ale zagroziło naruszeniem jej elementarnych interesów życiowych w przyszłości. W związku z powzięciem informacji o tym zdarzeniu Prezes UODO złożył zawiadomienie o możliwości popełnienia przestępstwa na podstawie art. 107 ust. 1 ustawy o ochronie danych osobowych oraz art. 202 § 3 Kodeksu karnego. Organy ścigania nie podzieliły jednak stanowiska organu nadzorczego i zadecydowały o prawomocnym zakończeniu przedmiotowego postępowania. Mając na uwadze powyższe, Prezes UODO skierował wniosek w trybie art. 327 § 1 Kodeksu postępowania karnego do Prokuratora Generalnego o polecenie podjęcia na nowo prawomocnie zakończonego postępowania przygotowawczego. W wyniku podjętych przez

[149] DKN.5101.131.2025.

Prezesa UODO działań prokuratura rejonowa podjęła na nowo postępowanie przygotowawcze i wszczęła śledztwo, które następnie ponownie zostało umorzone wobec uznania tym razem, że czyn nie wypełnił ustawowych znamion czynu zabronionego. Prezes UODO odwołał się od powyższego postanowienia i wniósł zażalenie do sądu, które nie zostało jeszcze rozpoznane.

Kolejne zawiadomienie[150] dotyczyło pozyskania informacji wskazującej na stosowanie monitoringu wizyjnego w sali reanimacyjnej szpitalnego oddziału ratunkowego, w sposób niewidoczny dla pracowników i pacjentów. Zgodnie z wyjaśnieniami administratora monitoring został zainstalowany przez pracownika w związku ze zgłaszanymi przez personel sygnałami dotyczącymi podejrzenia działania niektórych pracowników na szkodę majątkową szpitala jako zakładu pracy i skierowany był wyłącznie na miejsce przechowywania leków. W związku powyższym, Prezes UODO skierował do prokuratury rejonowej dwa zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa na podstawie art. 304 § 2 Kodeksu postępowania karnego w związku z przetwarzaniem danych osobowych pacjentów oraz pracowników szpitala polegającym na prowadzeniu ukrytego monitoringu wizyjnego w sali reanimacyjnej Szpitalnego Oddziału Ratunkowego bez podstawy prawnej, tj. przestępstwa określonego w art. 107 ust. 1 ustawy o ochronie danych osobowych.

Prokuratura rejonowa umorzyła dochodzenie w sprawie ww. zawiadomień. Prezes UODO złożył zażalenie na ww. postanowienie do sądu rejonowego wskazując, że kwestionowane postanowienie oparte zostało na błędnej ocenie prawnej okoliczności, a umorzenie dochodzenia w niniejszej sprawie było wynikiem niewłaściwej interpretacji oraz częściowego pominięcia materiału dowodowego zgromadzonego na etapie prowadzonych czynności wyjaśniających przez organ nadzorczy. Sąd rejonowy utrzymał w mocy zaskarżone postanowienie podnosząc, że zostało ono wydane po przeprowadzeniu pełnego i wyczerpującego postępowania przygotowawczego, w toku którego zgromadzono kompletny materiał dowodowy pozwalający na dokonanie jednoznacznych i prawidłowych ustaleń faktycznych.

Kolejne zawiadomienie o popełnieniu przestępstwa[151] zostało złożone w związku z zamieszczeniem w serwisie internetowym X przez posła na Sejm RP, będącego użytkownikiem tego serwisu, zdjęcia osoby prywatnej o kolorze skóry wskazującym na odmienne niż europejskie pochodzenie – tj. przestępstwa określonego w art. 107 ust. 1 ustawy o ochronie danych osobowych. Do publikacji wizerunku ww. osoby doszło wraz z wpisem, w którym poseł zapowiedział, że będzie publikował zdjęcia i wpisy, które przysyłają mu zaniepokojeni mieszkańcy. Zdjęcie to zostało ww. posłowi przekazane przez niezidentyfikowaną osobę, której wiadomość również zamieszczono w ww. wpisie (cyt.): „Panie Pośle, już są w Szczecinie, proszę zwrócić uwagę na bliznę na policzku, dziś w autobusie trasa

[150] DKN.5101.448.2024.
[151] DKN.5101.59.2025.

Załom-Podjuchy”. W sprawie wydane zostało postanowienie o odmowie wszczęcia dochodzenia wobec stwierdzenia przez prokuraturę, że społeczna szkodliwość czynu jest znikoma. Po wniesieniu zażalenia na ww. postanowienie przez Prezesa UODO, sąd rejonowy wydał postanowienie o uchyleniu zaskarżonego postanowienia, po którym prokuratura wydała ponownie postanowienie o odmowie wszczęcia dochodzenia – tym razem wobec stwierdzenia, że czyn nie zawiera znamion czynu zabronionego. Na postanowienie to Prezes UODO złożył kolejne zażalenie.

Również kolejne zawiadomienie o popełnieniu przestępstwa[152] określonego w art. 107 ust. 1 ustawy o ochronie danych osobowych dotyczyło zamieszczenia w serwisie internetowym X przez posła na Sejm RP, będącego użytkownikiem tego serwisu posługującym się nazwą, wizerunków wraz z danymi osobowymi trzech obywateli Erytrei. Do publikacji wizerunków oraz danych ww. osób doszło wraz z wpisem, w którym Poseł przytoczył opis informatora: „sytuacja na przejściu granicznym w Lubieszynie. Spotkałem tam trzech migrantów z Erytrei. Posiadali oni białe kartki – dokumenty wydane w języku arabskim, które, jak się okazało po przetłumaczeniu, były decyzjami o wydaleniu ich z terytorium Niemiec. Na miejsce została wezwana Straż Graniczna oraz policja. Funkcjonariusze spisali dane mężczyzn, jednak ostatecznie pozostali oni na wolności, ponieważ posiadali tymczasowe karty pobytu. Nie mam informacji, co stało się z nimi dalej. PS. Oni zawsze są urodzeni 1.01”. Do swojego wpisu poseł załączył cztery zdjęcia: trzy z nich przedstawiały dokumenty zawierające dane osobowe (imiona, nazwisko, imiona rodziców, datę urodzenia, miejsce i kraj urodzenia, a także obywatelstwo) wraz ze zdjęciami i podpisami trzech osób – obywateli Erytrei. Czwarte zdjęcie przedstawiało najprawdopodobniej jeden z wyżej wspomnianych dokumentów w języku arabskim, który to dokument zawierał dane osobowe jednej z tych trzech osób. Czynności organów ścigania są w toku.

W wyniku zamieszczenia przez użytkowników serwisu społecznościowego X dokumentów głównie w postaci dawnych kwestionariuszy paszportowych, zawierających szczegółowe dane osobowe osób pełniących funkcje publiczne lub działających w przestrzeni publicznej, Prezes UODO złożył zawiadomienie o popełnieniu przestępstwa[153] określonego w art. 107 ust. 1 ustawy o ochronie danych osobowych. W związku z zawiadomieniem prowadzone było przez prokuraturę dochodzenie, które w przypadku części zdarzeń zostało umorzone w związku z przedawnieniem karalności tych czynów, co nie było kwestionowane przez Prezesa UODO. W zakresie pozostałych czynów objętych tym postępowaniem, tj. czynów polegających na ponownym udostępnieniu w latach 2021 i 2022 udostępnionych już w roku 2018 zdjęć, prokuratura dokonała niewłaściwej oceny zdarzenia i uznała że ich ponowne opublikowanie stanowiło

[152] DKN.5101.192.2025.
[153] DKN.5101.61.2025.

czyn o znikomej społecznej szkodliwości. Prezes UODO nie zgodził się z taką oceną i złożył zażalenie w tym zakresie, które nie zostało jeszcze rozpoznane.

Prezes UODO złożył zawiadomienie o popełnieniu przestępstwa[154] dotyczące nielegalnego przewarzania danych osobowych w związku z zamieszczeniem w serwisie internetowym o charakterze pornograficznym, znajdującym się pod adresami zbiornik.com oraz zbiornik.tv, wizerunków osób bez ich wiedzy i zgody. Prezes UODO powziął informacje, że w ramach ww. serwisu udostępniane są zdjęcia lub nagrania osób, które mogą być nieświadome nie tylko tego, że udostępniono ich wizerunek innym osobom korzystającym z ww. serwisu o charakterze pornograficznym, ale że w ogóle zrobiono im zdjęcia lub nagrano je np. w intymnej sytuacji. W takich przypadkach oczywistym jest, że podmiot, który przetwarza dane osobowe osoby nieświadomej utrwalenia jej wizerunku lub celu jego wykorzystania, nie czyni tego za zgodą tej osoby, ani na żadnej innej podstawie wskazanej w art. 6 ust. 1 lub 9 ust. 2 rozporządzenia 2016/679. Czynności organów ścigania są w dalszym ciągu prowadzone.

W ramach kontynuacji podjętych czynności w związku z zawiadomieniem[155] o popełnieniu przestępstwa z 2024 r. Prezes UODO złożył zażalenie na postanowienie o umorzeniu dochodzenia. Sprawa dotyczyła tworzenia map z danymi osobowymi osób, których dane wyciekły z chińskiej platformy zakupowej. Sąd w wyniku złożonego przez Prezesa UODO zażalenia przekazał sprawę do prokuratury rejonowej celem przeprowadzenia stosownego postępowania. W treści ww. postanowienia sąd wskazał, że przedstawione przez Prezesa UODO okoliczności świadczą o uzasadnionym przypuszczeniu popełniania przestępstwa z art. 107 ust. 1 ustawy o ochronie danych osobowych, zaś przekazane informacje zostały przy tym potwierdzone w toku czynności policyjnych. Prokuratura rejonowa ponownie jednak umorzyła dochodzenie, wskazując na brak dostatecznych danych uzasadniających podejrzenie popełnienia przestępstwa. Prezes UODO następnie złożył zażalenie na ww. postanowienie. Zdaniem Prezesa UODO, organy ścigania nie podjęły działań mających na celu wyjaśnienie przedstawionej przez organ nadzorczy sprawy, pozostawiając sprawcę lub sprawców udostępnienia danych osobowych wielu osób w Internecie bezkarnych. Zażalenie Prezesa UODO na postanowienie o umorzeniu dochodzenia aktualnie oczekuje na rozpatrzenie go przez prokuraturę nadrzędną.

## 12. Orzecznictwo sądów administracyjnych

### 12.1. Orzecznictwo sądów administracyjnych dotyczące postanowień wydanych na etapie wstępnej kontroli skarg

W 2025 r. część postanowień wydanych przez Prezesa UODO była przedmiotem skarg kierowanych do Wojewódzkiego Sądu Administracyjnego w Warszawie.

[154] DKN.5101.334.2025.
[155] DKN.5101.151.2024.

W zdecydowanej większości przypadków, tj. 8 z 10 wydanych orzeczeń, WSA podzielił stanowisko Prezesa UODO sformułowane w postanowieniach. W jednym przypadku WSA zadecydował o odrzuceniu skargi na postanowienie, natomiast tylko w jednym – o uchyleniu postanowienia. Powyższe świadczy o wysokiej trafności oraz zasadności wydawanych przez Prezesa UODO postanowień oraz o spójności interpretacji przyjmowanej zarówno przez organ nadzorczy, jak i WSA. Poniżej przedstawiono przykładowe orzecznictwo dotyczące postanowień Prezesa UODO.

**Wyrok w sprawie nadużycia prawa do ochrony danych osobowych w celu uzyskania korzyści majątkowej**

W jednej ze spraw[156] WSA oddalił skargę na postanowienie Prezesa UODO o odmowie wszczęcia postępowania w sprawie skargi na bezprawne przetwarzanie danych osobowych oraz niewypełnienie obowiązków informacyjnych[157]. Sąd podzielił stanowisko organu, który stwierdził, że działania skarżącego polegające na uzależnieniu wycofania swoich roszczeń od zapłaty sumy pieniężnej stanowi nadużycie prawa przez skarżącego, ponieważ celem wniesionej skargi w istocie nie była ochrona jego danych osobowych. WSA podniósł również, że nadużywanie prawa do ochrony danych osobowych powoduje ograniczenie innym podmiotom dostępu do skutecznego realizowania tego prawa przed organem nadzorczym, poprzez zakłócenie sprawnego funkcjonowania urzędu obsługującego ten organ, i dotyczy to także sytuacji, w których skarga ma na celu udręczenie podmiotu rozpatrującego.

**Wyrok w sprawie dotyczącej domniemania przetwarzania danych osobowych poprzez urządzenia obsługujące przesyłki kurierskie**

Wyrokiem z 29 października 2025 r.[158] WSA oddalił skargę na postanowienie Prezesa UODO o odmowie wszczęcia postępowania w sprawie dotyczącej zarzutu przetwarzania danych osobowych, w tym wizerunku, za pomocą monitoringu zainstalowanego w urządzeniach obsługujących przesyłki kurierskie[159]. Sąd podzielił stanowisko organu, który stwierdził, że skoro skarżąca wskazała, że nie korzystała z tych urządzeń ani się do nich nie zbliżała, to nawet jeśli jej wizerunek został zarejestrowany, był on nieczytelny, a tym samym nie pozwalał na jej identyfikację, więc nie stanowił danych osobowych. W ocenie sądu, administrator nie pozyskał danych osobowych skarżącej, a zatem ich nie przetwarzał, co stanowiło uzasadnioną przyczynę uniemożliwiającą wszczęcie postępowania w tej sprawie. Opisany wyrok jest prawomocny.

[156] Sygn. akt II SA/Wa 1464/25.
[157] DWKSN.523.4100.2025.
[158] Sygn. akt II SA/Wa 1119/25.
[159] DS.523.4772.2024.

**Wyrok w sprawie dotyczącej żądania administratora udostępnienia skanu dokumentu tożsamości**

Wyrokiem z 23 września 2025 r.[160] WSA oddalił skargę na postanowienie Prezesa UODO o odmowie wszczęcia postępowania w sprawie procedury weryfikacji konta użytkownika, polegającej na żądaniu udostępnienia skanu dokumentu tożsamości[161]. Skoro skarżący wskazał, że nie udostępnił swoich danych osobowych w ramach ww. procedury, to nie doszło do ich przetwarzania, a więc organ nie był uprawniony do wszczęcia postępowania ze skargi indywidualnej, ponieważ brak jest przedmiotu, który mógłby zostać oceniony. WSA podzielił stanowisko Prezesa UODO wskazując, że w chwili żądania podania danych osobowych ich przetwarzanie jeszcze się nie rozpoczyna. W ocenie sądu w takich okolicznościach nie wystąpiły przesłanki do prowadzenia postępowania na wniosek, a ewentualna kontrola ogólnych praktyk administratora mogłaby zostać przeprowadzona przez organ nadzorczy z urzędu. Opisany wyrok jest prawomocny.

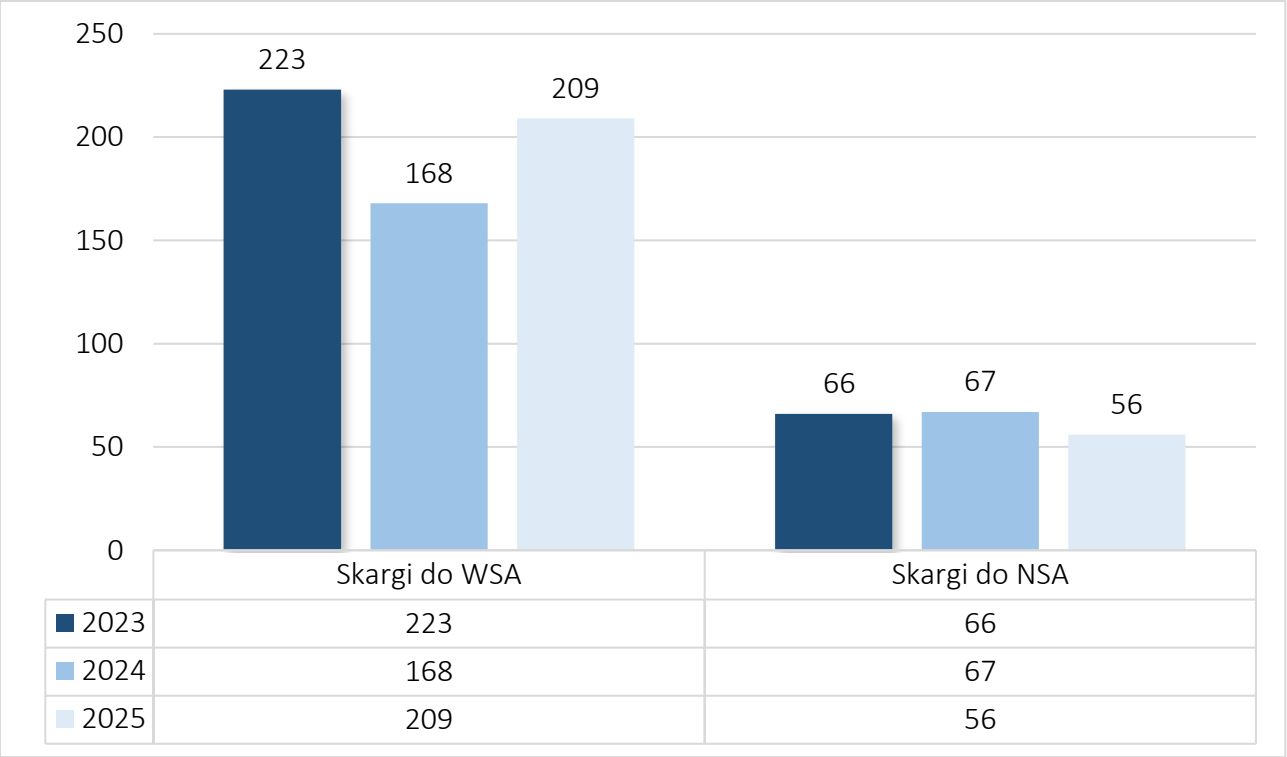
## 12.2. Orzecznictwo sądów administracyjnych w sprawach skargowych

Przegląd przykładowego orzecznictwa dotyczącego decyzji Prezesa UODO wydanych w sprawach skargowych należy rozpocząć od wskazania, że w roku 2025 odnotowano wzrost liczby skarg wniesionych na decyzje organu do Wojewódzkiego Sądu Administracyjnego w Warszawie, która wyniosła **209.** W roku 2024 skarga taka została wniesiona w 168 przypadkach, zaś w roku 2023 r. odnotowano 223 skargi. Na wzrost liczby skarg na decyzje w stosunku do roku 2024 r. wpływ miał przede wszystkim wzrost liczby decyzji administracyjnych wydanych przez Prezesa UODO w 2025 r.

Spadła natomiast zaskarżalność wyroków wydanych przez Wojewódzki Sąd Administracyjny w Warszawie w sprawach decyzji Prezesa Urzędu Ochrony danych Osobowych wydanych w sprawach skargowych. Takich skarg do Naczelnego Sądu Administracyjnego w roku 2025 wniesiono **56,** w roku 2024 – 67, podczas gdy w roku 2023 wniesiono ich 66.

[160] Sygn. akt II SA/Wa 930/25.

[161] DS.523.5769.2024.




**Wykres 6:** Decyzje wydane w postępowaniach skargowych, zaskarżone do WSA i skargi do NSA w sprawach wyroków WSA dotyczących decyzji wydanych przez Prezesa UODO w latach 2023-2025.

**Wyrok w sprawie umieszczenia danych osobowych w zakresie imienia, nazwiska i adresu w postanowieniu wysłanym do wszystkich stron postępowania administracyjnego**

Naczelny Sąd Administracyjny[162] uznał, że zarówno skarga kasacyjna Prezesa UODO, jak i Wojewódzkiego Inspektora Nadzoru Budowlanego zasługują na uwzględnienie i wydał wyrok, w którym uchylił wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie uchylający decyzję Prezesa UODO w przedmiocie przetwarzania danych osobowych[163] oraz oddalił skargę na decyzję Prezesa UODO dotyczącą udostępnienia przez Wojewódzkiego Inspektora Nadzoru Budowlanego danych osobowych skarżących w zakresie imion, nazwiska i adresu w postanowieniu na rzecz wszystkich stron postępowania.

Uwzględniając skargę na decyzję Prezesa UODO Wojewódzki Sąd Administracyjny w Warszawie wskazał, że Prezes UODO w swoich rozważaniach pominął kwestię adekwatności zamieszczenia, a co za tym idzie udostępnienia, w badanym postanowieniu danych osobowych skarżących w zakresie ich adresu, uznając, że udostępnienie tych danych miało swoje oparcie w art. 6 ust. 1 lit. c, RODO

[162] Wyrok NSA z 22 stycznia 2025 r. sygn. akt III OSK 6043/21.
[163] Wyrok WSA z 16 kwietnia 2021 r. sygn. akt II SA/Wa 1715/20.

w zw. z art. 124 § 1 i art. 40 § 1 K.p.a., gdy zdaniem sądu przepis art. 124 § 1 K.p.a. nie nakłada na organ bezwzględnego obowiązku wskazania w postanowieniu administracyjnym miejsca zamieszkania osoby fizycznej.

Naczelny Sąd Administracyjny stanął jednak na stanowisku, że użyte w przepisie art. 124 § 1 K.p.a. wyrażenia językowe nakazujące „oznaczenie strony lub stron postępowania" zobowiązują organ orzekający w sprawie administracyjnej do jednoznacznego, a zatem pełnego zidentyfikowania osób biorących udział w sprawie, co w odniesieniu do osób fizycznych następuje przez podanie ich danych personalnych w postaci imienia i nazwiska oraz wskazanie ich adresu zamieszkania. Naczelny Sąd Administracyjny uznał, że należy zgodzić się, że przetwarzanie w toku postępowania danych osobowych strony lub stron postępowania w zakresie ich imion, nazwisk i adresów zamieszkania znajduje podstawę prawną w normie zawartej w art. 6 ust. 1 lit. c RODO, a organ, przetwarzając te dane, działa realizując obowiązek prawny wynikający z przepisu art. 124 § 1 K.p.a., nakazujący mu „oznaczenie strony lub stron postępowania". Sąd uznał, że są to dane osobowe adekwatne, stosowne i ograniczone do tego co jest niezbędne z punktu widzenia indywidualno-konkretnego charakteru prawnego postanowienia (decyzji końcowej), jego samoistnej roli pełnionej w obrocie prawnym, tj. możliwości ustalenia stanu prawnego i zindywidualizowanych osób, do których się on odnosi, bez konieczności sięgania do akt administracyjnych sprawy, w której dany akt administracyjny został wydany. Przetwarzanie danych osobowych w tym zakresie wypełnia zatem obowiązek minimalizacji danych, o którym mowa w art. 5 ust. 1 lit. c RODO.

### Wyrok w sprawie przetwarzania danych osobowych w Krajowym Systemie Informacyjnym Policji (KSIP)

Naczelny Sąd Administracyjny[164] oddalił skargę kasacyjną Komendanta Głównego Policji od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie[165] oddalającego skargę Komendanta Głównego Policji na decyzję Prezesa Urzędu Ochrony Danych Osobowych w przedmiocie przetwarzania danych osobowych.

W toku prowadzonego postępowania Prezes UODO ustalił, że postępowanie karne w sprawie popełnionego przez skarżącego czynu wypełniającego znamiona przestępstwa zostało przez sąd warunkowo umorzone z okresem próby 1 roku od dnia uprawomocnienia się orzeczenia. Prezes UODO, oceniając stan sprawy zbadał, czy kwestionowane przetwarzanie danych osobowych znajdowało oparcie choć w jednej z przesłanek legalizujących przetwarzanie danych osobowych wskazanych w art. 13 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, zgodnie z którym właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa oraz –- w przypadku przetwarzania danych wrażliwych –- w przesłankach legalizujących przetwarzanie określonych w art. 14 ust. 2 ustawy o ochronie danych osobowych przetwarzanych

[164] Wyrok NSA z 17 października 2025 r. sygn. akt III OSK 2223/22.
[165] Wyrok WSA z 28 kwietnia 2022 r. sygn. akt II SA/Wa 3288/21.

w związku z zapobieganiem i zwalczaniem przestępczości. Po przeprowadzonym postępowaniu Prezes UODO stwierdził, że nie istnieje obecnie potrzeba przetwarzania w KSIP danych osobowych skarżącego, a zatem uznał, że przetwarzanie przez Komendanta Głównego Policji danych osobowych skarżącego odbywa się z naruszeniem art. 13 oraz art. 31 ust. 1 pkt 5 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości i niezbędne jest nakazanie przywrócenia stanu zgodnego z prawem z tym zakresie. Dlatego też Prezes UODO, działając na podstawie art. 8 ust. 1 pkt 5 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nakazał Komendantowi Głównemu Policji wyeliminowanie nieprawidłowości w procesie przetwarzania danych osobowych skarżącego, poprzez usunięcie jego danych osobowych z KSIP.

Wojewódzki Sąd Administracyjny uznał, że Prezes UODO zasadnie przyjął, że cel przetwarzania przez Komendanta Głównego Policji danych osobowych skarżącego w KSIP został zrealizowany i dlatego też dalsze przetwarzanie jego danych osobowych odbywa się z naruszeniem art. 13 oraz art. 31 ust. 1 pkt 5 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, co wymagało nakazania przywrócenia stanu zgodnego z prawem w tym zakresie.

Naczelny Sąd Administracyjny stwierdził, że trafne jest stanowisko sądu I instancji, że do kompetencji Prezesa UODO należy ocena prawidłowości dalszego przetwarzania danych osobowych przez ich administratora, tj. Komendanta Głównego Policji. Zgodnie z art. 5 ust. 1 pkt 1 i 6 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości do zadań Prezesa UODO należy monitorowanie i egzekwowanie stosowania przepisów ww. ustawy oraz wydanych na jej podstawie aktów wykonawczych oraz rozpatrywanie skarg osób, których dane osobowe są przetwarzane niezgodnie z prawem, i prowadzenie postępowań w tym zakresie. Naczelny Sąd Administracyjny uznał również, że sąd I instancji stanął na trafnym stanowisku, że dla oceny zgodności z prawem przetwarzania danych w KSIP konieczne jest systemowe uwzględnianie zarówno przepisów ustawy o Policji, jak i przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości i doszedł do trafnego wniosku, że przepisy ustawy o Policji są na tyle ogólne, że biorąc tylko je pod uwagę możliwym byłoby zakwalifikowanie wszystkich zebranych przez policję danych osobowych, w oparciu o art. 16 ww. ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości periodycznie co 10 lat, jako niezbędnych dla realizacji jej zadań, co umożliwia bezterminowe przechowywanie danych pomimo osiągnięcia celu, w którym zostały zebrane, oraz że ustawa o Policji nie wykluczyła obowiązku administratora danych wynikającego z art. 31 ust. 1 pkt 5 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, tj. obowiązku zapewnienia, aby dane osobowe były przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania.

Naczelny Sąd Administracyjny wskazał na ogólnikowość argumentacji Komendanta Głównego Policji. Ocena okoliczności faktycznych niniejszej sprawy (która nie została skutecznie podważona w ramach zarzutów naruszenia przepisów postępowania) doprowadziła sąd I instancji do prawidłowej konstatacji. Sąd uznał, że Komendant Główny Policji nie uzasadnił, jaki konkretnie cel determinuje dalsze przetwarzanie danych osobowych skarżącego w KSIP w związku z prowadzonym przeciwko niemu postępowaniem karnym i nie wykazał, w jaki sposób przetwarzanie jego danych osobowych przyczynia się do realizacji któregokolwiek z zadań określonych w art. 1 ust. 2 ustawy o Policji. Stanowisko Komendanta Głównego Policji, że przetwarzanie danych uczestnika postępowania w KSIP jest niezbędne w celu prowadzenia „dalszych prognoz kryminologicznych" pozostaje w kolizji z wydanym w sprawie karnej rozstrzygnięciem sądu, który jako organ do tego właściwy takiej oceny w istocie uprzednio dokonał warunkowo, umarzając wobec niego postępowanie karne i przesądzając tym samym, że stopień winy i społecznej szkodliwości czynu przestępczego, stosunek psychiczny sprawcy do popełnionego czynu, a także dotychczasowy tryb życia sprawcy, sposób popełnienia czynu i zachowanie się po czynie, uzasadnia skorzystanie z instytucji określonej w art. 66 § 1 Kodeksu karnego, tj. instytucji warunkowego umorzenia postępowania karnego. Skoro od czasu pozyskania i wprowadzenia danych osobowych do zbioru KSIP w związku z prowadzonym postępowaniem karnym nie doszło do postawienia skarżącemu innego zarzutu o charakterze prawnokarnym i nie toczy się przeciwko niemu żadne postępowanie karne, to cel przetwarzania przez Komendanta Głównego Policji danych osobowych skarżącego w KSIP został zrealizowany i dlatego też dalsze przetwarzanie jego danych osobowych odbywa się z naruszeniem art. 13 oraz art. 31 ust. 1 pkt 5 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, a w konsekwencji konieczne było nakazanie przez Prezesa UODO przywrócenia stanu zgodnego z prawem w tym zakresie poprzez nakazanie usunięcia z KSIP danych osobowych skarżącego.

**Wyrok w sprawie decyzji dotyczącej udostępnienia danych osobowych mocodawcy w zawiadomieniu o możliwości naruszenia etyki zawodowej przez profesjonalnego pełnomocnika**

Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę skarżącej na decyzję Prezesa UODO[166], mocą której organ stwierdził, że Urząd Celno-Skarbowy bezpodstawnie udostępnił jej dane osobowe w zakresie imienia, nazwiska, numeru PESEL oraz informacji o prowadzonej przeciwko niej kontroli celno-skarbowej na rzecz Okręgowej Izby Adwokackiej w związku z zawiadomieniem o możliwości naruszenia etyki adwokackiej przez pełnomocnika skarżącej.

Prezes UODO, korzystając z przysługujących mu uprawnień naprawczych, udzielił upomnienia za stwierdzone naruszenie RODO, natomiast skarżąca domagała się nałożenia na administratora kary administracyjnej w wysokości 1.000.000 zł (jeden

[166] Wyrok WSA z 19 marca 2025 r. w sprawie o sygn. akt II SA/Wa 1173/23.

milion złotych). Wojewódzki Sąd Administracyjny w Warszawie wskazał, że Prezes UODO zastosował – w stanie faktycznym tej sprawy – adekwatny środek prawny. Sąd podkreślił ponadto, że decyzja o nałożeniu administracyjnej kary pieniężnej należy w pełni do organu nadzorczego, który w żaden sposób nie jest związany kierowanym do niego wnioskiem.

### Wyrok w sprawie publikacji danych osobowych na zamkniętych portalach społecznościowych

Naczelny Sąd Administracyjny uznał[167], że publikacja danych osobowych na zamkniętych portalach społecznościowych nie jest przetwarzaniem danych osobowych przez osobę fizyczną o czysto osobistym lub domowym charakterze w rozumieniu art. 2 ust. 2 lit. c rozporządzenia 2016/679, jeśli osoba fizyczna publikująca dane osobowe nie jest administratorem danej społeczności, nie dobiera sobie osobiście jej uczestników, a tylko do niej przystępuje, a pozostali członkowie grupy nie dysponują uprawnieniem do złożenia wiążącego sprzeciwu w stosunku do jej wniosku o przystąpienie do danej wspólnoty.

W przedmiotowej sprawie skarżąca wyraziła zgodę, aby na blogu zamieszczono zdjęcie jej certyfikatu szczepienia, jednakże bez jakichkolwiek danych osobowych jako przykładowy certyfikat. Skarżony wykorzystał zdjęcie certyfikatu szczepienia skarżącej w ten sposób, że korzystając z aplikacji mobilnej pozyskał dane osobowe skarżącej w zakresie imienia i nazwiska, a następnie zamieścił przekreślone zdjęcie certyfikatu wraz z podaniem imienia i nazwiska skarżącej na jednym z portali społecznościowych. Prezes UODO udzielił skarżonemu upomnienia za przetwarzanie danych osobowych skarżącej w zakresie imienia i nazwiska udostępnionych we wpisie na grupie na portalu społecznościowym bez podstawy prawnej.

Sąd wskazał, że ze względu na dość znaczną liczbę uczestników grupy, a także na to, że skarżony nie był administratorem tej grupy i nie dobierał sobie osobiście jej uczestników, a jedynie do niej przystąpił, a zatem nie pozostawał w żadnych innych relacjach z tymi osobami poza przynależnością do grupy, nie sposób uznać, aby miało miejsce przetwarzanie danych o charakterze osobistym lub domowym, o którym mowa w art. 2 ust. 2 rozporządzenia 2016/679.

### Wyrok w sprawie publikacji danych osobowych w artykule prasowym

W innej sprawie[168] Naczelny Sąd Administracyjny stwierdził, że działalność prasowa została zasadniczo wyłączona spod reżimu regulacji administracyjnoprawnej regulującej ochronę danych osobowych, a Prezes UODO nie dysponuje kompetencjami administracyjnymi do zapewnienia ochrony procesów przetwarzania danych osobowych w tej sferze przetwarzania danych osobowych. W tym zakresie – zdaniem NSA – nie może dojść do powstania sprawy administracyjnej w sensie materialnym, a to oznacza, że nigdy nie może dojść do wszczęcia postępowania w zakresie wyłączonym spod regulacji administracyjnoprawnej. Jeśli jednak mimo to

[167] Wyrok NSA z 20 maja 2025 r. w sprawie o sygn. akt III OSK 1101/24.
[168] Wyrok NSA z 18 września 2025 r. w sprawie o sygn. akt III OSK 1501/22.

zainteresowana osoba będzie domagać się wszczęcia postępowania, obowiązkiem organu – zdaniem NSA – jest skorzystanie z instytucji odmowy wszczęcia postępowania administracyjnego.

Powyższe stanowisko NSA zostało przedstawione w związku z wydanym przez Prezesa UODO postanowieniem, na podstawie którego odmówił skarżącemu wszczęcia postępowania w sprawie dotyczącej przetwarzania jego danych osobowych w zakresie imienia, nazwiska, wizerunku, informacji o prowadzonym postępowaniu dyscyplinarnym, a także o przedstawionych zarzutach dyscyplinarnych, ich liczbie i przedmiocie przez spółkę, poprzez opublikowanie ich w artykule prasowym, w tym na stronie internetowej.

Prezes UODO w uzasadnieniu swojego rozstrzygnięcia wskazał, że przedmiotowy artykuł odpowiada definicji prasy zgodnie z art. 7 ust. 2 pkt 1 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe[169] i stanowi przejaw dziennikarskiej działalności prasowej. Zdaniem Prezesa UODO w tej sprawie nie można było dokonać oceny legalności przetwarzania danych w oparciu o przesłanki określone w art. 6 ust. 1 rozporządzenia 2016/679 ze względu na wyłączenie stosowania tego przepisu do działalności dziennikarskiej. Z uwagi na brak możliwości dokonania w oparciu o obowiązujące przepisy o ochronie danych osobowych merytorycznej oceny udostępnienia danych osobowych skarżącego na łamach opublikowanego artykułu, w tym w artykule prasowym umieszczonym na wskazanej przez skarżącego stronie internetowej, niemożliwym było wykorzystanie uprawnień pozwalających na przywrócenie stanu zgodnego z prawem. NSA w pełni podzielił argumentację organu zawartą w uzasadnieniu wydanego w niniejszej sprawie postanowienia[170].

**Wyrok w sprawie postanowienia o odmowie wszczęcia postępowania z uwagi na nadmierny charakter żądania**

Wojewódzki Sąd Administracyjny w Warszawie, w wyroku[171] potwierdził słuszność postanowienia Prezesa UODO, w którym odmówił on podjęcia działań ze względu na nadmierny charakter żądania strony skarżącej. Organ nadzorczy uznał, że o ww. nadmierności nie decyduje jedynie znaczna liczba skarg wnoszonych przez nią, lecz przede wszystkim sposób, w jaki kieruje ona swoje żądania względem organu i działania podejmowane przez nią w toku rozpatrywania tych skarg. Działania ww. osoby w ocenie sądu świadczyły o nieadekwatnym wykorzystaniu prawa, o którym mowa w art. 77 ust. 1 RODO, prowadzącym do utrudniania, zakłócania, czy wręcz uniemożliwiania realizacji ustawowych zadań organu ochrony danych osobowych w sprawach innych podmiotów.

Działania strony – polegające na wielości i rozbudowanym sposobie formułowania zarzutów, ciągłym ich modyfikowaniu, rozszerzaniu żądań oraz zasypywaniu organu licznymi wnioskami dowodowymi – stanowiły nieproporcjonalne obciążenie i miały na celu sztuczne skomplikowanie oraz wydłużenie postępowań.

[169] Dz. U. z 2018 r. poz. 1914.
[170] Wyrok NSA z 26 marca 2025 r. w sprawie o sygn. akt III OSK 2713/23.
[171] Wyrok WSA z 17 września 2025 r. w sprawie o sygn. II SA/Wa 1087/25.

Kluczowym argumentem przemawiającym za słusznością podjętego przez organ nadzorczy rozstrzygnięcia było w ocenie sądu to, że intencją skarżącego nie była realna ochrona danych osobowych, lecz instrumentalne wykorzystanie procedury administracyjnej i próba sparaliżowania pracy urzędu. W ocenie sądu wykorzystywanie procedur prawnych jako narzędzia nacisku, a nie w celu ochrony własnych interesów, w pełni uzasadnia uznanie żądania za nadmierne i odmowę wszczęcia postępowania.

**Wyroki dotyczące przetwarzania danych osobowych „na zapas" przez podmioty finansowe**

W 2025 r. Naczelny Sąd Administracyjny potwierdził stanowisko Prezesa UODO odnośnie do niedopuszczalności przetwarzania danych osobowych „na zapas" przez okres przedawnienia roszczeń wynikający z przepisów prawa cywilnego. Powyższy cel przetwarzania administratorzy uzasadniali na podstawie art. 6 ust. 1 lit. f RODO. Naczelny Sąd Administracyjny uznał[172] za prawidłowe stanowisko Prezesa UODO i sądu pierwszej instancji, że niedopuszczalne jest przetwarzanie danych osobowych niejako „na zapas" z założeniem, że mogą być one ewentualnie przydatne w przyszłości oraz z odwołaniem się do przepisów dotyczących przedawnienia roszczeń cywilnoprawnych.

Niedopuszczalność przetwarzania „na zapas" przez okres przedawnień ewentualnych roszczeń została potwierdzona przez Naczelny Sąd Administracyjny także w innym wyroku[173], w którym sąd wskazał, że akceptacja przetwarzania danych osobowych „na zapas", z uwagi na niepewne przyszłe zdarzenie jakim jest ewentualne zgłoszenie roszczeń w przyszłości, doprowadziłoby do sytuacji, w której podmioty finansowe mogłyby przetwarzać dane osobowe swoich klientów, bez konieczności ich usunięcia, nawet jeśli łączyłaby ich wcześniej jedynie krótkotrwale trwająca relacja umowna, czy też zobowiązaniowa. Naczelny Sąd Administracyjny podkreślił, że taka interpretacja art. 6 ust. 1 lit. f RODO jest nieprawidłowa. Wskazał również, że przesłanka określona w art. 6 ust. 1 lit. f RODO nie jest ukierunkowana na pełną ochronę interesów sektora gospodarczego (finansowego), ale uzależniona jest od tego, czy przetwarzanie to 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. Regulacja ta nie odnosi się zatem do ochrony wszelkich interesów sektora gospodarczego (finansowego). Przede wszystkim ma za zadanie chronić osoby, których proces ten dotyczy przed nieuprawnionym przetwarzaniem ich danych osobowych. Nie można twierdzić, że przetwarzanie danych osobowych „na wszelki wypadek", czy „na zapas" lub w odniesieniu do „ewentualnych i potencjalnych roszczeń" stanowi „uzasadniony interes" banku. Każdej osobie przysługuje własne indywidualne prawo do prywatności, chroniące prywatną sferę tej osoby i uprawniające ją do samodzielnego decydowania o ujawnieniu informacji pochodzących z tej sfery. Niedopuszczalność takiego

[172] Wyrok NSA z 8 stycznia 2025 r. sygn. akt III OSK 4868/21.
[173] Wyrok NSA z 10 lipca 2025 r. sygn. akt III OSK 1594/22.

przetwarzania Naczelny Sąd Administracyjny potwierdził także w innych wyrokach zapadłych w 2025 roku[174].

**Wyroki w sprawie przetwarzania danych osobowych w zakresie wynikającym z zapytań kredytowych, które nie zakończyły się zawarciem umowy kredytu**

Naczelny Sąd Administracyjny potwierdził słuszność stanowiska Prezesa UODO w zakresie przetwarzania danych osobowych przez banki i instytucje wskazane w art. 105 ust. 4 Prawa bankowego w zakresie zapytań kredytowych, które nie zakończyły się zawarciem umowy kredytu[175]. Naczelny Sąd Administracyjny w jednym z wyroków[176] wskazał, że skoro nie doszło do zawarcia umowy kredytowej nie może być wątpliwości, że ocena zdolności kredytowej i analiza ryzyka kredytowego zostały dokonane (zrealizowane). Cel przetwarzania danych, dla którego zostały one zgromadzone w zapytaniach kredytowych, został tym samym osiągnięty. Odpadła przesłanka legalizująca dalsze przetwarzanie danych osobowych wnioskodawcy przez bank oraz instytucje, o której mowa w art. 105 ust. 4 Prawa bankowego, które to przetwarzanie miało na celu ocenę zdolności kredytowej i analizę ryzyka kredytowego (przed zawarciem umowy). Pomiędzy bankiem a wnioskodawcą nie nawiązał się bowiem żaden stosunek zobowiązaniowy, który stosownie do art. 105a ust. 1-5 Prawa bankowego dawałby podstawę do dalszego przetwarzania jego danych osobowych zarówno przez bank, jak i instytucje.

**Wyroki w sprawie przetwarzania danych osobowych w oparciu o art. 105a ust. 3 Prawa bankowego**

Podobnie jak w latach poprzednich, również w 2025 roku 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[177] Naczelny Sąd Administracyjny potwierdzając prawidłowość wykładni organu nadzorczego dotyczącą art. 105a ust. 3 Prawa bankowego podkreślił, że w związku z konstrukcją tego przepisu to rolą banku jest wykazanie w postępowaniu przed Prezesem UODO daty, w której doszło do poinformowania osoby, której dane dotyczą, o zamiarze przetwarzania jej danych osobowych po wygaśnięciu zobowiązania bez jej zgody, nie zaś daty, w której hipotetycznie osoba ta mogła zapoznać się z powyższą informacją.

Ponadto w innym wyroku[178] Naczelny Sąd Administracyjny wypowiedział się co do spornej kwestii, czy obowiązki wskazane w ww. przepisie dotyczą wyłącznie osób

[174] Wyrok NSA z 1 października 2025 r. sygn. III OSK 872/22, wyrok NSA z 19 listopada 2025 r. sygn. III OSK 2472/22.
[175] W wyrokach NSA z 13 lutego 2025 r. sygn. III OSK 6563/21, wyrok NSA z 29 maja 2025 r. sygn. III OSK 984/22, wyrok NSA z 10 lipca 2025 r. sygn. III OSK 165/22, wyrok NSA z 1 października 2025 r. sygn. III OSK 1877/22, wyrok NSA z 1 października 2025 r. sygn. III OSK 1552/22, wyrok NSA z 13 listopada 2025 r. sygn. III OSK 2513/22, wyrok NSA z 13 listopada 2025 r. sygn. III OSK 2636/22, wyrok NSA z 14 listopada 2026 r. sygn. akt III OSK 183/23.
[176] Wyrok NSA z 13 lutego 2025 r. sygn. III OSK 6563/21.
[177] Wyrok NSA z 10 października 2025 r. sygn. III OSK 1937/22.
[178] Wyrok NSA z 25 kwietnia 2025 r. sygn. III OSK 7370/21.

fizycznych nieprowadzących działalności gospodarczej. Prezes UODO stanął na stanowisku, że przepis ten znajduje zastosowanie do wszystkich osób fizycznych bez względu na to, czy prowadzą działalność gospodarczą. Wykładnia ta była negowana przez banki, które nie stosowały wymogów wskazanych w art. 105a ust. 3 Prawa bankowego do przetwarzania w celu oceny zdolności kredytowej i analizy ryzyka kredytowego danych osobowych osób fizycznych prowadzących działalność gospodarczą. Naczelny Sąd Administracyjny wskazał, że literalne brzmienie art. 105a ust. 3 Prawa bankowego nie pozostawia wątpliwości co do tego, że hipoteza (zakres podmiotowy) statuowanej nim normy obejmuje wszystkie osoby fizyczne. Odnośny przepis nie wprowadza wyraźnie ani też w sposób możliwy do zidentyfikowania nie nawiązuje do rozróżnienia osób fizycznych na te, które prowadzą działalność gospodarczą, i te, które takiej działalności nie prowadzą (przedsiębiorców i konsumentów).

### Wyrok w sprawie przetwarzania danych osobowych w oparciu o art. 105a ust. 1 Prawa bankowego w związku z zobowiązaniem, które uległo przedawnieniu

Naczelny Sąd Administracyjny wydał w 2025 r. wyrok[179], w którym potwierdził prawidłowość dokonanej przez Prezesa UODO wykładni art. 105a ust. 1 Prawa bankowego, zgodnie z którą bank jest uprawniony do przetwarzania danych osobowych w celach oceny zdolności kredytowej i analizy ryzyka kredytowego w zakresie zobowiązań, które uległy przedawnieniu, w tym w bazie instytucji, o której mowa w art. 105 ust. 4 Prawa bankowego. W ocenie organu nadzorczego ww. przetwarzanie jest legalne. Innego zdania był były dłużnik wskazując, że przetwarzanie w bazie ww. instytucji przez bank danych o zobowiązaniach przedawnionych stanowi niedopuszczalną formę nacisku uregulowania należności. Naczelny Sąd Administracyjny podkreślił, że przedawnienie zobowiązania kredytowego nie oznaczało jego wygaśnięcia i bank był uprawniony utrzymywać rachunek kredytowy jako aktywny. Naczelny Sąd Administracyjny wskazał, że dane osobowe klienta banku odnoszące się do etapu realizacji zawartej umowy kredytowej stanowią informacje będące tajemnicę bankową, które bank ma prawo przetwarzać i przekazać do systemu instytucji utworzonej na podstawie art. 105 ust. 4 Prawa bankowego na podstawie art. 105 ust. 1 pkt 1c i ust. 4 w zw. z art. 105a ust. 1 Prawa bankowego. System bankowy został w ocenie Sądu ukształtowany w taki sposób, aby wszystkie instytucje udzielające kredytów, czy pożyczek mogły pozyskać informacje o klientach, którzy w przeszłości nie spłacili swoich zobowiązań w ogóle, albo pozostają w tym zakresie w zwłoce.

### Wyrok w sprawie stosowania przepisów RODO do ochrony danych osobowych podmiotów innych niż osoby prywatne

W 2025 r. Naczelny Sąd Administracyjny wydał wyrok[180], w którym uchylił zaskarżony kasacyjnie przez Prezesa Urzędu Ochrony Danych Osobowych wyrok

[179] Wyrok NSA z 9 września 2025 r. sygn. III OSK 1640/22.
[180] Wyrok NSA z 20 maja 2025 r. sygn. III OSK 622/22.

Wojewódzkiego Sądu Administracyjnego w Warszawie i podzielił stanowisko organu nadzorczego, który odmówił uwzględnienia wniosku z uwagi na to, że skarżący w chwili złożenia do dyrektora szkoły wniosku o udostępnienie sprawozdań, planów pracy i analiz egzaminów pełnił funkcję przewodniczącego rady rodziców i wystąpił z tym wnioskiem, nie jako osoba fizyczna, lecz jako przewodniczący rady rodziców.

Naczelny Sąd Administracyjny wskazał, że w takiej sytuacji nie może dojść do naruszenia przepisów o ochronie danych osobowych, gdyż zgodnie z art. 1 ust. 2 RODO rozporządzenie to chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. Naczelny Sąd Administracyjny podkreślił, że prawo do ochrony danych osobowych jako prawo wolnościowe gwarantowane jest osobie prywatnej. W rozpoznawanej sprawie skarżący nie występował do dyrektora szkoły jako osoba prywatna, lecz jako przewodniczący organu administrującego, odwołując się w swoim wniosku do kompetencji ustawowych tego organu jako uzasadnienia dla jego wniosku. Działał zatem na podstawie kompetencji ustawowej jako organ. Organy nie korzystają z praw wolnościowych. Tym samym skarżący kierując jako przewodniczący organu administrującego wniosek i dalsze pisma z nim powiązane nie może korzystać z ochrony swojej prywatności, w tym z ochrony danych osobowych.

**Wyrok w sprawie informacji dotyczących podmiotu prowadzącego działalność gospodarczą**

W jednym z wydanych wyroków[181] Naczelny Sąd Administracyjny oceniał czy znajdujące się na portalu internetowym informacje o praktyce lekarza w zakresie (prywatny gabinet stomatologiczny, adres prowadzenia działalności oraz numer telefonu) stanowią dane osobowe. Naczelny Sąd Administracyjny stwierdził, że dane w postaci nazwy, adresu prowadzonej działalności oraz numeru telefonu, pod którym można się kontaktować, same w sobie nie stanowią danych osobowych, które pozwalają bezpośrednio ustalić dane osobowe podmiotu, który pod tym adresem prowadzi dany rodzaj działalności, a zatem informacje te nie stanowią danych o zidentyfikowanej osobie fizycznej. Nie ma w nich bowiem ani imienia, ani nazwiska takiej osoby. Naczelny Sąd Administracyjny wskazał również, że w sytuacji, gdy dane dotyczą tylko nazwy podmiotu prowadzącego działalność gospodarczą, jego adresu i numeru telefonu bez dodatkowych informacji, to nie można uznać, że dotyczą one danych osobowych konkretnej osoby fizycznej, ponieważ dla jej zidentyfikowania koniecznym jest posiadanie szeregu innych informacji związanych z tą określoną działalnością gospodarczą. Sąd nie dopatrzył się, aby w spornym przypadku identyfikacja ta była możliwa przy niewielkim nakładzie środków.

[181] Wyrok NSA z 15 października 2025 r. sygn. III OSK 2357/22.

**Wyrok w sprawie upoważnienia do przetwarzania danych osobowych wydanego w formie ustnej**

W innym wyroku[182] Naczelny Sąd Administracyjny zaakceptował stanowisko Prezesa UODO stwierdzając, że upoważnienie do przetwarzania danych może być wydane w formie ustnej, a takiego udzielił administrator swojej pracownicy. Administrator polecił pracownicy przygotowanie żądanej informacji publicznej i co jest oczywiste upoważnił ją do przetwarzania danych osobowych wnioskodawcy. Irrelewantną okolicznością dla tej kwestii jest to, czy pracownica sądu ma pisemne upoważnienie do przetwarzania danych osobowych, na które dodatkowo powoływał się administrator. Ponadto, wbrew stanowisku skarżącego, trudno sobie wyobrazić, polecenie przygotowania żądanej informacji publicznej i ewentualnego projektu odpowiedzi na wniosek, bez przekazania pracownicy danych wnioskodawcy zawartych we wniosku. Dla prawidłowego upoważnienia wystarczające jest polecenie, z którego wynika uprawnienie do przetwarzania danych osobowych. Sąd stwierdził również, że przepisy dotyczące obowiązku informacyjnego nie narzucają administratorowi konkretnego sposobu jego realizacji. Istotne jest by właściwa informacja dotarła do podmiotu danych i aby administrator był w stanie wykazać zrealizowanie tego obowiązku wobec konkretnego podmiotu danych.

**Wyrok rozstrzygający czy postępowanie prowadzone przez Prezesa UODO służy ujawnieniu sprawcy kradzieży danych osobowych**

W zapadłym w 2025 r. wyroku[183] Naczelny Sąd Administracyjny rozstrzygnął że postępowanie prowadzone przez Prezesa UODO nie służy ujawnieniu sprawcy kradzieży danych osobowych (tym powinny zająć się organy ścigania), lecz zapobieżeniu przetwarzania danych osobowych w sposób niezgodny z prawem, kontroli czy są one zabezpieczone przez stosowne procedury przed ich nieuprawnionym pozyskaniem przez osoby trzecie, a także jest ukierunkowane na wydanie decyzji przywracającej stan zgodny z prawem w tym zakresie. Sąd, podtrzymując w tej sprawie decyzję Prezesa UODO, stwierdził, że dopiero ustalenie osoby podszywającej się pod skarżącą umożliwiłoby ustalenie, czy dane osobowe skarżącej zostały pozyskane z zasobów byłego pracodawcy oraz pozwoliłoby ocenić prawidłowość zabezpieczenia dostępu do tych danych w świetle przepisów dotyczących ochrony danych osobowych.

**Wyrok w sprawie dostępu lekarza do danych pacjenta poprzez PUE ZUS**

Naczelny Sąd Administracyjny poparł w jednym z wydanych wyroków[184] stanowisko Prezesa UODO i podkreślił rolę lekarza jako administratora odpowiedzialnego za przetwarzanie danych osobowych, do których ma dostęp poprzez PUE ZUS (w toku postępowania przed organem lekarka tłumaczyła się m.in. tym, że ktoś inny w przychodni mógł skorzystać z jej konta). Naczelny Sąd

[182] Wyrok NSA z 28 stycznia 2025 r. sygn. III OSK 6061/21.
[183] Wyrok NSA z 10 października 2025 r. sygn. III OSK 1854/22.
[184] Wyrok NSA z 23 października 2025 r. sygn. III OSK 2471/22.

Administracyjny wskazał, że uprawnienia do wystawiania zaświadczeń lekarskich, w tym do związanego z tym przetwarzania danych osobowych osób ubezpieczonych, przysługują lekarzom, a nie zatrudniającym ich placówkom. W sytuacji, kiedy to lekarz uzyskuje dostęp do indywidualnego konta przydzielanego przez ZUS (bez udziału przychodni) to lekarz ten, a nie zatrudniający go podmiot, ustala cele i sposoby przetwarzania danych osobowych. Sąd ten podkreślił, że dostęp do konta lekarza w PUE ZUS powinien mieć wyłącznie ten lekarz. W rezultacie w związku ze wskazaniem, że ktoś inny w przychodni mógł skorzystać z konta lekarza, sąd uznał że lekarz jako administrator nie zapewnił przetwarzania danych w sposób gwarantujący odpowiednie bezpieczeństwo danych osobowych zawartych w systemie PUE ZUS.

### 12.3. Przykłady innych wyroków utrzymujących w mocy decyzje Prezesa UODO

Wyrokiem z 11 czerwca 2025 r.[185], wydanym w następstwie rozpatrzenia skargi administratora na adresowaną do niego decyzję[186] Prezesa UODO, Wojewódzki Sąd Administracyjny w Warszawie **utrzymał w mocy ww. decyzję organu nadzorczego**.

W sprawie, w której finalnie zapadł ww. wyrok, postępowanie administracyjne zainicjowane zostało wskutek otrzymania przez organ nadzorczy informacji o braku wyznaczenia przez administratora inspektora ochrony danych. Administrator tymczasem, jako organ publiczny – w rozumieniu art. 37 ust. 1 rozporządzenia 2016/679 i art. 9 ustawy o ochronie danych osobowych w związku z art. 9 pkt 1-14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[187] – zobowiązany był do wyznaczenia inspektora z mocy prawa. Naturalną konsekwencją braku dopełnienia ww. obowiązku był brak publikacji danych kontaktowych inspektora ochrony danych oraz zawiadomienia o nich 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 pełnienia roli IOD w swojej organizacji jednego z pracowników działu kadr. Swoje stanowisko uzasadniał argumentując, że pracownik ten przeszedł szkolenie z zakresu ochrony danych osobowych, zaś jego dane osobowe, jako osoby pełniącej funkcję inspektora, umieszczone zostały w klauzuli informacyjnej dotyczącej przetwarzania danych, skierowanej do osób zatrudnionych w strukturze administratora. W ocenie organu nadzorczego środki dowodowe dostarczone przez administratora były niewystarczające by wykazać, że należycie wypełnił on obowiązki wynikające z art. 37 ust. 1 lit. a oraz art. 37 ust. 7 rozporządzenia 2016/679.

Wobec powyższego, organ nadzorczy nałożył 25 tys. zł administracyjnej kary pieniężnej na administratora za niewyznaczenie inspektora ochrony danych (administrator dokonał skutecznego wyznaczenia IOD dopiero po wszczęciu postępowania administracyjnego w przedmiotowej sprawie), a w konsekwencji brak

[185] Sygn. akt II SA/Wa 2065/24.
[186] DKN.5112.35.2021.
[187] Dz. U. z 2023 r. poz. 1270.

publikacji jego danych kontaktowych i brak zawiadomienia o tych danych organu nadzorczego.

W przedmiotowej sprawie Prezes UODO zaznaczył, że kierując się potrzebą wykazania przed organem nadzorczym prawidłowej realizacji obowiązków związanych z wyznaczeniem inspektora ochrony danych, administrator powinien dążyć, by akt (np. wewnętrzne zarządzenie, uchwała, powierzenie obowiązków) bądź umowa z osobą, która ma sprawować funkcję IOD, w sposób nie budzący wątpliwości wskazywały na wyznaczenie do pełnienia funkcji inspektora ochrony danych konkretnej osoby. Dla celów dowodowych istotne jest pisemne udokumentowanie powyższego. Konieczne jest też precyzyjne przypisanie ww. osobie określonego zakresu obowiązków zgodnie z przepisami art. 38 i art. 39 rozporządzenia 2016/679. Co istotne, skuteczne wyznaczenie i publikacja danych IOD stanowią 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 zadań. W ocenie organu nadzorczego stwierdzonym w niniejszej sprawie naruszeniom art. 37 ust. 1 lit. a oraz art. 37 ust. 7 rozporządzenia 2016/679 należało zatem przypisywać znaczenie szersze niż to wynika z ich formalnego charakteru. Prezes UODO stanął na stanowisku, że niewyznaczenie IOD przez administratora może niejednokrotnie utrudniać lub wręcz uniemożliwiać realizację praw osobom fizycznym, co nakazuje traktować stwierdzone w toku postępowania 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 prawodawcy – IOD).

W korzystnym z perspektywy organu nadzorczego wyroku WSA podkreślił spoczywające na administratorze obowiązki w zakresie należytego wykazania (za pomocą odpowiednich środków dowodowych) okoliczności wyznaczenia IOD. **Wyrok jest prawomocny.**

Wyrokiem z 12 czerwca 2025 r.[188] Naczelny Sąd Administracyjny oddalił skargę kasacyjną Krajowej Szkoły Sądownictwa i Prokuratury (KSSiP) od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 26 stycznia 2022 r.[189] i utrzymał w mocy decyzję[190] Prezesa UODO nakładającą na ww. administratora karę pieniężną.

W wyroku dotyczącym przedmiotowej sprawy NSA podkreślił, że odpowiedzialność administratora za naruszenie ochrony danych osobowych, jakkolwiek nie ma charakteru odpowiedzialności absolutnej, to jest odpowiedzialnością obiektywną. NSA wskazał, że z orzecznictwa Trybunału Konstytucyjnego wynika, że administracyjna kara pieniężna „nie jest konsekwencją dopuszczenia się czynu zabronionego, lecz skutkiem zaistnienia stanu niezgodnego z prawem, co sprawia, że ocena stosunku sprawcy do czynu nie

[188] Sygn. akt III OSK 1394/22.
[189] Sygn. akt II SA/Wa 1384/2.
[190] DKN.5130.2024.2020.

mieści się w reżimie odpowiedzialności obiektywnej". Tym samym administrator ponosi odpowiedzialność także za działanie osób i podmiotów od siebie zależnych, przy pomocy których przetwarza dane osobowe.

Sądy obydwu instancji, podzielając argumentację Prezesa UODO, dopatrzyły się też braków kompleksowych postanowień w umowie powierzenia przetwarzania danych, której treść w sposób niewystarczający określała zakres powierzanych danych, w tym ich kategorii. Ponadto administrator nie zawarł w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora.

NSA zważył, że administrator nie podjął starań zabezpieczenia całego procesu migracji danych, ani nie informował podmiotu przetwarzającego o oczekiwaniach dotyczących tej operacji. Sąd II instancji podtrzymał zatem, że administrator jest inicjatorem działań jako podmiot decydujący o celach oraz sposobach przetwarzania. W konsekwencji fakt, czy do wycieku doszło w efekcie błędu pracownika firmy zewnętrznej, czy z innych przyczyn, nie ma znaczenia dla odpowiedzialności administratora wynikającej z art. 32 rozporządzenia 2016/679. W ocenie NSA, to na administratorze spoczywa odpowiedzialność także za działanie osób i podmiotów od siebie zależnych, przy pomocy których przetwarza dane osobowe. Zawarcie umowy powierzenia przetwarzania danych osobowych nie oznacza więc „transferu ryzyka" z administratora na podmiot przetwarzający – nie dochodzi więc w takiej sytuacji do wyłączenia jego odpowiedzialności na gruncie wspomnianego przepisu. **Wyrok jest prawomocny**.

Wyrokiem z 1 października 2025 r.[191] Naczelny Sąd Administracyjny **uchylił zaskarżony** przez Prezesa UODO wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 19 kwietnia 2022 r.[192], uchylający decyzję[193] Prezesa UODO nakładającą administracyjną karę pieniężną i przekazał sprawę WSA do ponownego rozpoznania.

W przedmiotowej sprawie administracyjna kara pieniężna była konsekwencją braku zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych oraz braku zawiadomienia o naruszeniu osoby, której dane dotyczą, tj. naruszenia obowiązków administratora statuowanych odpowiednio w art. 33 i art. 34 rozporządzenia 2016/679. Stwierdzenie uchybienia drugiemu z ww. obowiązków wiązało się również ze sformułowanym w ww. decyzji wobec administratora nakazem zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dane dotyczą.

**Wyrok jest prawomocny.** Pismem z 12 listopada 2025 r. administrator wycofał skargę na decyzję i złożył wniosek o umorzenie postępowania przed WSA. W związku z powyższym decyzja Prezesa UODO stała się prawomocna.

[191] Sygn. akt III OSK 1830/22.
[192] Sygn. akt II SA/Wa 3024/21.
[193] DKN.5131.3.2021.

Kolejna sprawa zakończyła się wyrokiem z 20 marca 2025 r.[194] w którym Naczelny Sąd Administracyjny **oddalił skargę kasacyjną** złożoną przez Śląski Uniwersytet Medyczny w Katowicach od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 22 września 2021 r. oddalającego skargę tego podmiotu na decyzję[195] wydaną przez Prezesa UODO.

W przedmiotowej sprawie administracyjna kara pieniężna nałożona została przez organ nadzorczy na administratora za brak zgłoszenia naruszenia ochrony danych osobowych oraz zawiadomienia o naruszeniu osób, których dane dotyczą, tj. naruszenie art. 33 i art. 34 rozporządzenia 2016/679. Prezes UODO nakazał równocześnie administratorowi realizację obowiązku informacyjnego z art. 34 rozporządzenia 2016/679 – tj. zawiadomienie o naruszeniu ochrony danych osobowych osób, których dane dotyczą.

W analizowanej sprawie doszło do niezamierzonej publikacji nagrań z egzaminów, do których przystępowali studenci legitymujący się widocznymi w niektórych przypadkach na nagraniu legitymacjami studenckimi lub dowodami osobistymi. Niektóre dane uwiecznione na tych dokumentach były na nagraniach czytelne, a inne dla zwiększenia czytelności wymagałyby „wyostrzenia", co w ocenie Prezesa UODO było technicznie możliwe. Prezes UODO nie skorzystał dla potwierdzenia tej możliwości z opinii biegłego (opierając się na ocenie dokonanej we własnym zakresie), co było przedmiotem zarzutów podnoszonych przez ukarany podmiot. Istotnym jest, że w uzasadnieniu ww. wyroku NSA wskazano m.in., że „Prezesa UODO należy zaliczyć do grona organów administracji specjalnej, co oznacza, że dysponuje on zasobami kadrowymi wyspecjalizowanymi w zakresie powierzonych mu zadań i kompetencji. Te okoliczności, które dla zwykłego obywatela stanowią zakres wiedzy specjalistycznej, z punktu widzenia organu załatwiane są jednak bez konieczności sięgania do pomocy biegłych z danej dziedziny, gdyż zatrudnia on urzędników mogących na podstawie własnej wiedzy specjalistycznej ocenić je w ramach urzędu. Materialny zakres zastosowania rozporządzenia 2016/679 wynikający z art. 2 ust. 1 wyraźnie wskazuje, że jego przepisy dotyczą przetwarzania danych osobowych w sposób zautomatyzowany. Jest zatem oczywistym, że organ zatrudnia specjalistów z zakresu informatyki i dziedzin wiedzy z nią powiązanych. Kwestia ustalenia tego, czy jest możliwe odczytanie niewyraźnych danych została rozstrzygnięta wewnątrz urzędu przez fachowców z tych dziedzin wiedzy". **Wyrok jest prawomocny.**

Wyrokiem z 3 grudnia 2025 r.[196] Naczelny Sąd Administracyjny **oddalił skargę kasacyjną** złożoną przez Bank Millennium S.A. z siedzibą w Warszawie od wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 1 lipca 2022 r., oddalającego skargę tego podmiotu na decyzję[197] wydaną przez Prezesa UODO.

[194] Sygn. akt III OSK 210/22.
[195] DKN.5131.6.2020.
[196] Sygn. akt III OSK 2416/22.
[197] DKN.5131.16.2021.

W przedmiotowej sprawie administracyjna kara pieniężna nałożona została przez organ nadzorczy na administratora za brak zgłoszenia naruszenia ochrony danych osobowych oraz zawiadomienia o tym naruszeniu osób, których dane dotyczą, tj. naruszenie art. 33 ust. 1 i art. 34 ust. 1 rozporządzenia 2016/679. Prezes UODO nakazał równocześnie administratorowi realizację obowiązku z art. 34 rozporządzenia 2016/679 – tj. zawiadomienie o naruszeniu ochrony danych osobowych osób, których dane dotyczą.

W sprawie będącej przedmiotem postępowania doszło do zagubienia przez operatora pocztowego przesyłki z dokumentacją bankową zawierającą dane osobowe klientów banku w postaci: numeru PESEL wraz z imieniem i nazwiskiem, adresem zameldowania, numerem rachunków bankowych, numerem CIF (numer identyfikacyjny nadawany klientom banku). W sprawie tej jednym z kluczowych argumentów strony przeciwnej było to, że bank w chwili zagubienia przesyłki zawierającej dokumentację nie był jej administratorem w rozumieniu art. 4 pkt 7 rozporządzenia 2016/679, lecz była to firma kurierska, która sprawowała nad nią władztwo i pełną kontrolę, wykonując własne, ustawowe obowiązki operatora pocztowego.

W uzasadnieniu ww. wyroku NSA wskazał m.in., że „prawidłowa jest ocena organu i sądu I instancji, w myśl której naruszenie danych osobowych polegające na zagubieniu dokumentacji bankowej (…) i zawierającej dane osobowe klientów banku (…) może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Na aprobatę zasługuje przy tym argumentacja organu i sądu I instancji dotycząca znaczenia numeru PESEL, którego pozyskanie przez osoby trzecie – zwłaszcza razem z innymi danymi – ułatwia kradzież lub sfałszowanie tożsamości”. W dalszej części wyroku NSA podkreślił, że „W ocenie Naczelnego Sądu Administracyjnego, sąd I instancji prawidłowo przyjął, że administratorem danych zawartych w dokumentacji bankowej, znajdującej się w zagubionej przesyłce, pozostaje bank, gdyż to on określił cele i sposoby ich przetwarzania. Operator pocztowy (firma kurierska), który nie ma wiedzy ani dostępu do zawartości przesyłki, może mieć status administratora wyłącznie w odniesieniu do danych osobowych nadawcy i odbiorcy. Operator pocztowy, w ramach podejmowanych przezeń czynności (abstrahując od sytuacji atypowych), nie określa celów ani sposobów przetwarzania danych zawartych w dokumentacji bankowej”. **Wyrok jest prawomocny.**

## 13. 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[198], jest wierzycielem i organem egzekucyjnym w odniesieniu do egzekucji obowiązków o charakterze niepieniężnym z zakresu ochrony danych

[198] Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2026 r. poz. 268), zwana dalej także: „u.p.e.a”.

osobowych. Dzięki temu Prezes UODO może prowadzić czynności mające na celu zapewnienie wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych. Ponadto Prezes UODO jest wierzycielem w zakresie egzekucji należności pieniężnych (w szczególności administracyjnych kar pieniężnych, grzywien, kosztów upomnienia, kosztów egzekucyjnych, grzywien w celu przymuszenia, opłat za certyfikację oraz naliczonych od tych należności odsetek za zwłokę). Organem egzekucyjnym w zakresie egzekucji pieniężnych jest naczelnik właściwego urzędu skarbowego.

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

a) **ostateczne decyzje** nakładające na administratora lub podmiot przetwarzający (zobowiązanego) **obowiązki 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)[199]. 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[200]. Prezes UODO ma prawo nałożyć na podmiot z sektora prywatnego 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[201]. 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[202].

[199] Art. 61 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2026 r. poz. 143 ze zm.).
[200] Art. 74 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
[201] Art. 83 ust. 4-6 RODO.
[202] Art. 102 ust. 1-3 u.o.d.o.

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

Pierwszym etapem postępowania prowadzonego w UODO, wspólnym dla postępowań dotyczących decyzji nakładających oba rodzaje obowiązków, jest **postępowanie sprawdzające wykonanie przez zobowiązanego decyzji** (dające zobowiązanemu możliwość dobrowolnego jej wykonania jeszcze na tym etapie sprawy). W przypadku, gdy postępowanie to nie wykaże, że decyzja została wykonana, do zobowiązanego kierowane jest upomnienie[203] 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**[204]. Jak wskazano wyżej, w postępowaniu tym Prezes UODO występuje jednocześnie w roli wierzyciela i organu egzekucyjnego.

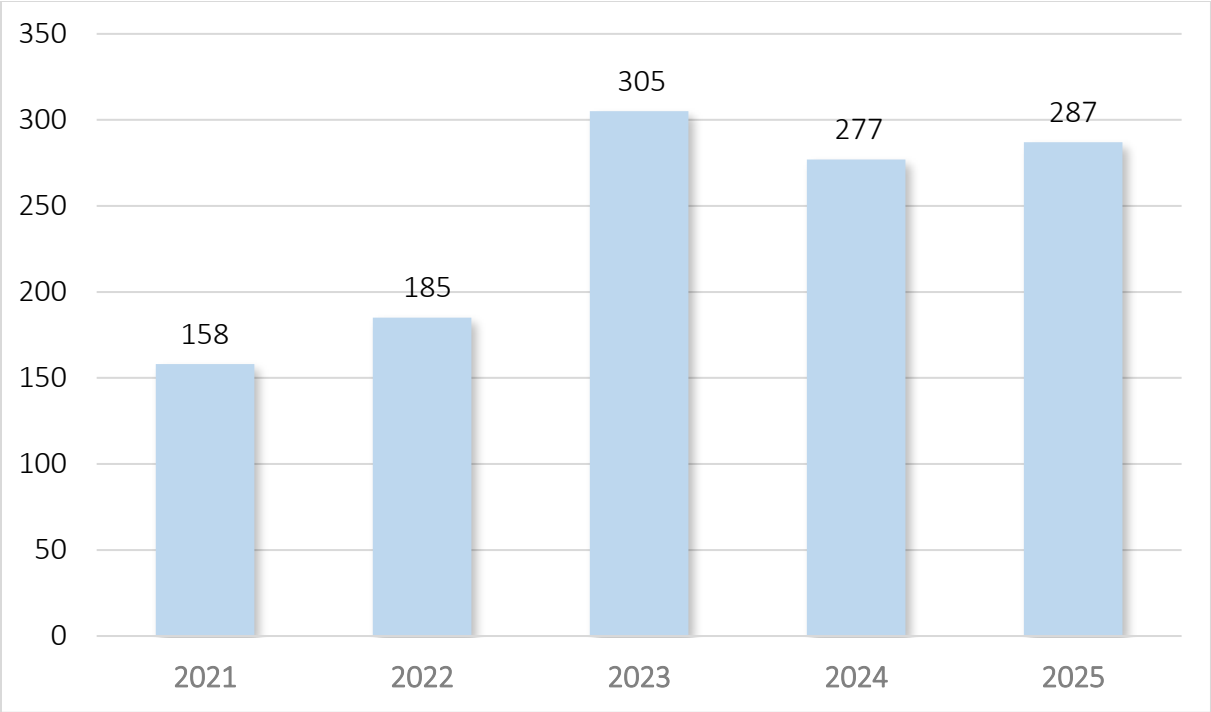
Brak zapłaty przez zobowiązanego orzeczonej na poprzednim etapie postępowania grzywny w celu przymuszenia powoduje konieczność wszczęcia wobec niego **egzekucji należności pieniężnych**. Takie też postępowanie wszczynane jest w przypadku stwierdzenia w postępowaniu sprawdzającym braku dobrowolnej zapłaty 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.

### 13.1. Postępowania w zakresie egzekucji decyzji Prezesa UODO

W 2025 r. wszczętych zostało **287 postępowań sprawdzających wykonanie decyzji Prezesa UODO** (4 postępowania dotyczyły sprawdzenia wykonania decyzji nakładających administracyjne kary pieniężne, 278 postępowań – decyzji zawierających nakaz, tj. obowiązek o charakterze niepieniężnym, zaś pozostałe 5 – decyzji nakładających oba ww. obowiązki łącznie).

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

Powyższe dane wskazują na **wzrost tego rodzaju postępowań o 4 % w stosunku do roku 2024**, w którym wszczęto 277 postępowań sprawdzających. Jednocześnie jednak liczba postępowań zainicjowanych w ostatnich dwóch okresach sprawozdawczych pozostaje niższa od liczby tego rodzaju postępowań wszczętych w roku 2023, co ilustruje poniższy wykres.




**Wykres 7:** Zestawienie liczby decyzji i postanowień Prezesa UODO przekazanych do sprawdzenia wykonania i ewentualnej egzekucji administracyjnej w latach 2021–2025.

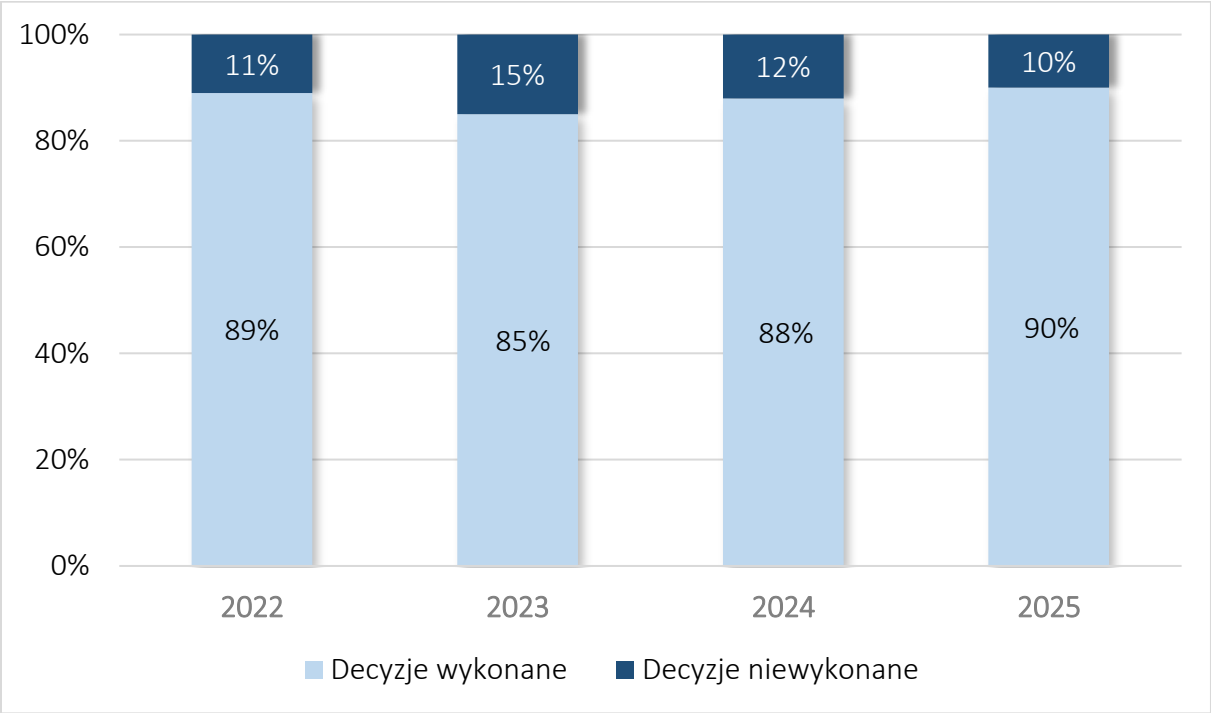
Efektywność prowadzonych przez Prezesa UODO działań, mających na celu sprawdzenie i doprowadzenie do wykonania przez zobowiązanych obowiązków nałożonych na nich decyzjami administracyjnymi Prezesa UODO, przedstawia się następująco:

- spośród 287 decyzji, w odniesieniu do których wszczęte zostały postępowania w 2025 r., **zakończonych zostało 257,**
- pozostałe 30 decyzje nadal objęte są działaniami Prezesa UODO.

W 3 przypadkach wszczęta została egzekucja obowiązku o charakterze niepieniężnym, w ramach których na zobowiązanych nałożone zostały grzywny w celu przymuszenia. W stosunku do 3 zobowiązanych Prezes UODO wszczął – już po zakończeniu omawianego okresu sprawozdawczego, a przed dniem sporządzenia niniejszego sprawozdania – postępowanie administracyjne w przedmiocie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy.

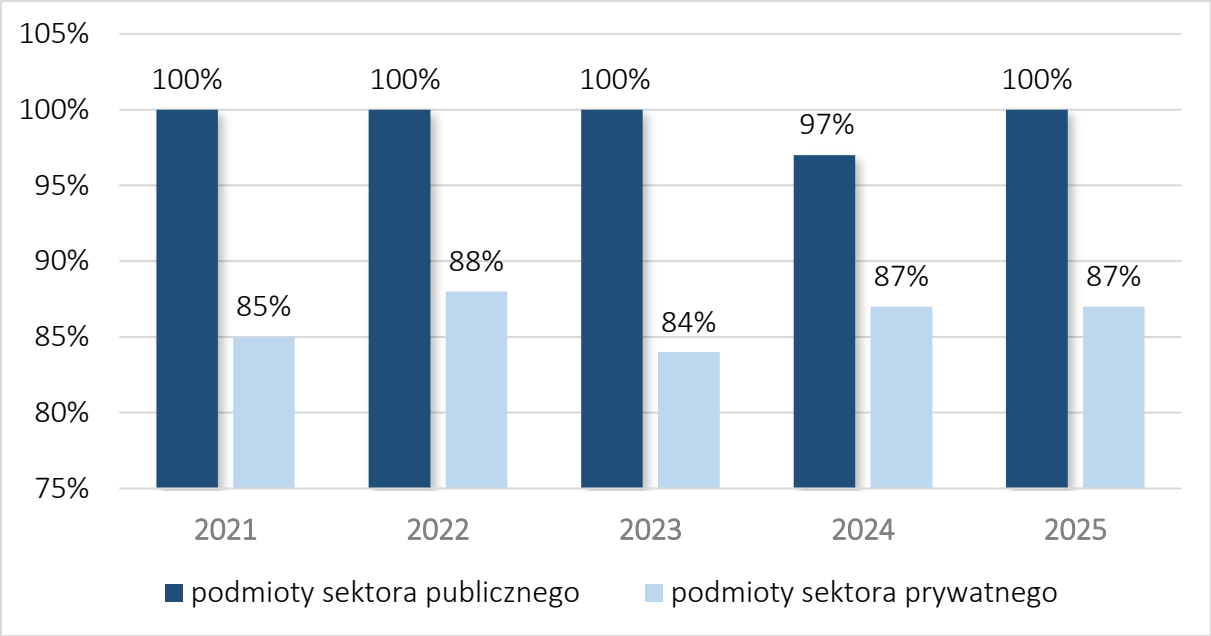
W odniesieniu do pozostałych 24 decyzji prowadzone są w dalszym ciągu działania mające na celu sprawdzenie ich wykonania lub spowodowanie ich dobrowolnego wykonania przez zobowiązanych.

Procentowy wskaźnik efektywności działań w odniesieniu do wszystkich decyzji administracyjnych Prezesa UODO, co do których wszczęte zostały w roku 2025 postępowania sprawdzające, wyniósł **90 %**. Porównanie wskaźnika efektywności w latach 2022–2025 obrazuje Wykres 8.




**Wykres 8:** Procentowe zestawienie efektywności działań egzekucyjnych Prezesa UODO w latach 2022–2025.

Podjęte w 2025 r. działania w zakresie sprawdzenia wykonania i egzekucji decyzji administracyjnych Prezesa UODO dotyczyły w 13 % przypadków podmiotów z sektora publicznego (37 postępowań), a w pozostałych 87 % przypadków – podmiotów prywatnych (250 postępowań). W analizowany okresie sprawozdawczym, podobnie jak w latach 2021-2023, wskaźnik wykonalności decyzji Prezesa UODO skierowanych do podmiotów publicznych wyniósł 100 % (wyjątek od czego stanowił rok 2024 z wynikiem na poziomie 97 %). Adresatami wszystkich niewykonanych decyzji, objętych działaniami Prezesa UODO w 2025 r. były natomiast podmioty z sektora prywatnego. Przy czym 3 spośród nich nie posiadały jednostek organizacyjnych na terenie Europejskiego Obszaru Gospodarczego, co istotnie utrudniało Prezesowi UODO podjęcie wobec nich skutecznych działań egzekucyjnych.




**Wykres 9:** Zestawienie efektywności działań egzekucyjnych prowadzonych w latach 2021–2025 w odniesieniu do podmiotów sektora publicznego i sektora prywatnego.

### 13.2. Egzekucja obowiązków o charakterze niepieniężnym

Wobec stwierdzenia niewykonania przez zobowiązanych nakazów decyzji Prezesa UODO (w tym wynikających z rozstrzygnięć wydanych w poprzednich okresach sprawozdawczych) w 2025 r. wszczętych zostało **7 egzekucji obowiązków o charakterze niepieniężnym**. Wystawione w tym okresie tytuły wykonawcze objęły nakazy orzeczone 7 decyzjami administracyjnymi, a łączna kwota grzywien w celu przymuszenia zastosowanych wobec zobowiązanych przez Prezesa UODO w tych postępowaniach wyniosła **60 000 zł**. Spośród 7 wszczętych w 2025 r. egzekucji obowiązków o charakterze niepieniężnym:

a) 3 egzekucje doprowadziły do ustalenia, że zobowiązani wykonali adresowane do nich nakazy decyzji Prezesa UODO – przy tym w jednym przypadku nałożona na zobowiązanego grzywna w celu przymuszenia w kwocie 15 000 zł została uprzednio uiszczona w całości, zaś w dwóch pozostałych sprawach grzywny w łącznej kwocie 10 000 zł umorzono[205],
b) 2 egzekucje okazały się bezskutecznymi na tym etapie sprawy, w związku z czym wobec zobowiązanych wszczęto egzekucje należności pieniężnych mające na celu wyegzekwowanie grzywien w celu przymuszenia nałożonych na nich w łącznej kwocie 15 000 zł – postępowania te nie doprowadziły jak dotąd do ustalenia wykonania nakazu decyzji,
c) w toku pozostają 2 egzekucje, w których na zobowiązanych nałożono grzywny w celu przymuszenia w łącznej kwocie 20 000 zł.

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

### 13.3. Egzekucja należności pieniężnych

W 2025 r. Prezes UODO doprowadził do wszczęcia **12 egzekucji należności pieniężnych,** których łączna wysokość wyniosła **307 826 zł**). Porównując liczbę tego rodzaju spraw z rokiem poprzednim, należy wskazać na 60 % ich spadek ilościowy – w roku 2025 wszczęto bowiem 30 takich postępowań. Mimo wyraźnej tendencji zniżkowej należy jednak odnotować nieznaczny, bo zaledwie 11 %, spadek poziomu, na jakim kształtowała się suma należności podlegających egzekucji pieniężnej – w 2024 r. wyniosła ona bowiem 346 945 zł. W omawianym okresie sprawozdawczym egzekucje należności pieniężnych dotyczyły trzech rodzajów należności: nałożonych przez Prezesa UODO administracyjnych kar pieniężnych, grzywien w celu przymuszenia orzeczonych przez Prezesa UODO jako środki egzekucyjne w egzekucjach obowiązków o charakterze niepieniężnym oraz kosztów skierowanych do zobowiązanym pisemnych upomnień[206]. W ujęciu liczbowym postępowania te i ich efekty przedstawiają się następująco:

1) Prezes UODO w bieżącym okresie sprawozdawczym doprowadził do wszczęcia **3 egzekucji**, których przedmiotem były **administracyjne kary pieniężne** w łącznej wysokości **253 762 zł**. Wszystkie egzekwowane w tych postępowaniach kary pieniężne nałożone zostały na podmioty prywatne – 1 spółkę prawa handlowego oraz 2 osoby fizyczne prowadzące indywidualną działalność gospodarczą. W przypadku jednego spośród ww. postępowań, egzekwowana w nim **administracyjna kara pieniężna w wysokości 18 941 zł została skutecznie wyegzekwowana**. W przypadku kolejnego postępowania, w którym egzekwowana była kara w kwocie 209 566 zł, organ egzekucyjny (właściwy naczelnik urzędu skarbowego) umorzył je ze względu na brak majątku lub źródła dochodu, z których możliwa byłaby egzekucja należności. W ostatnim zaś przypadku właściwy organ egzekucyjny podejmuje w dalszym ciągu działania, zmierzające do wyegzekwowania należności Prezesa UODO w kwocie 25 255 zł.
2) Przedmiotem **7 wszczętych przez Prezesa UODO egzekucji** należności pieniężnych były **grzywny w celu przymuszenia** (w łącznej kwocie **54 000 zł**). Wszystkie tego rodzaju środki egzekucyjne orzeczone zostały wobec podmiotów prywatnych – 3 spółek prawa handlowego, 2 osób fizycznych prowadzących indywidualną działalność gospodarczą oraz 2 osób fizycznych nieprowadzących takiej działalności. W przypadku **3 tytułów wykonawczych** wystawionych przez Prezesa UODO (na łączną kwotę **16 500 zł**) właściwi naczelnicy urzędów skarbowych **wyegzekwowali w całości objęte nimi należności**. W przypadku **2 postępowań**, w których egzekwowane były grzywny w celu przymuszenia w łącznej wysokości **17 500 zł**, Prezes UODO – w związku z ustaleniem, że zobowiązani wykonali adresowane do nich obowiązki o charakterze

[206] Art. 15 § 1 „u.p.e.a" w zw. z § 1 rozporządzenia Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 5 stycznia 2021 r. w sprawie wysokości kosztów upomnienia doręczanego zobowiązanemu przed wszczęciem egzekucji administracyjnej (Dz. U. z 2021 r. poz. 67).

niepieniężnym – wydał postanowienia o **umorzeniu lub zwrocie**[207] **egzekwowanych należności**. Pozostałe egzekucje (dotyczące **2 tytułów wykonawczych** na łączną kwotę **20 000 zł**) nadal są prowadzone przez właściwe organy egzekucyjne.

3) W omawianym okresie sprawozdawczym Prezes UODO wszczął **2 egzekucje**, których przedmiotem były **nieuiszczone koszty** wynikające ze skierowanych do zobowiązanych **pisemnych upomnień** (w łącznej wysokości 64 zł). W przypadku 1 spośród tych postępowań właściwy organ egzekucyjny wyegzekwował objętą nim należność w kwocie 16 zł. Drugie postępowanie egzekucyjne (dotyczące tytułu wykonawczego wystawionego na kwotę 48 zł) umorzono wobec ustalenia, że zobowiązany utracił byt prawny[208].

## 14. 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. 445 Prawa komunikacji elektronicznej[209], 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 jednak z tego uprawnienia.

W 2025 r. Prezes UODO skorzystał z uprawnienia do zastosowania administracyjnej kary pieniężnej w przypadkach naruszenia przepisów RODO w 20 sprawach, nakładając na **23 podmioty** łącznie 32 administracyjne kary pieniężne w całkowitej kwocie **64 436 940,25 zł**. W porównaniu z rokiem poprzednim oznacza to **wzrost liczby nałożonych kar o 18,5 %,** przy jednoczesnym **wzroście ich łącznej wysokości o 363 %** (w 2024 r. orzeczonych zostało 27 administracyjnych kar pieniężnych na łączną kwotę 13 907 740,96 zł). Najwyższa kara orzeczona przez Prezesa UODO w analizowanym okresie sprawozdawczym – kara nałożona na Pocztę Polską S.A.[210] – wyniosła 27 124 816 zł (co stanowiło 42 % wartości wszystkich administracyjnych kar pieniężnych wymierzonych w 2025 r. oraz 195 % wartości wszystkich kar orzeczonych w 2024 r.). Z kolei najniższa kara została orzeczona – wobec osoby fizycznej prowadzącej jednoosobową działalność gospodarczą – w kwocie 3 157 zł (stanowiącej 0,005 % wartości wszystkich kar). Istotne zwiększenie wysokości kar nakładanych przez Prezesa UODO – w porównaniu do lat poprzednich, co zostało zobrazowane na poniższym wykresie – świadczy o rosnącej roli tego rodzaju sankcji, jako kluczowego środka służącego egzekwowaniu przepisów o ochronie danych osobowych. Zwiększenie wysokości administracyjnych kar pieniężnych jest również konsekwencją postępującej harmonizacji działań

[207] Art. 126 u.p.e.a.
[208] Art. 59 § 1 pkt 1 w zw. z art. 59 § 4 u.p.e.a.
[209] Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 ze zm.).
[210] DKN.5131.1.2025.

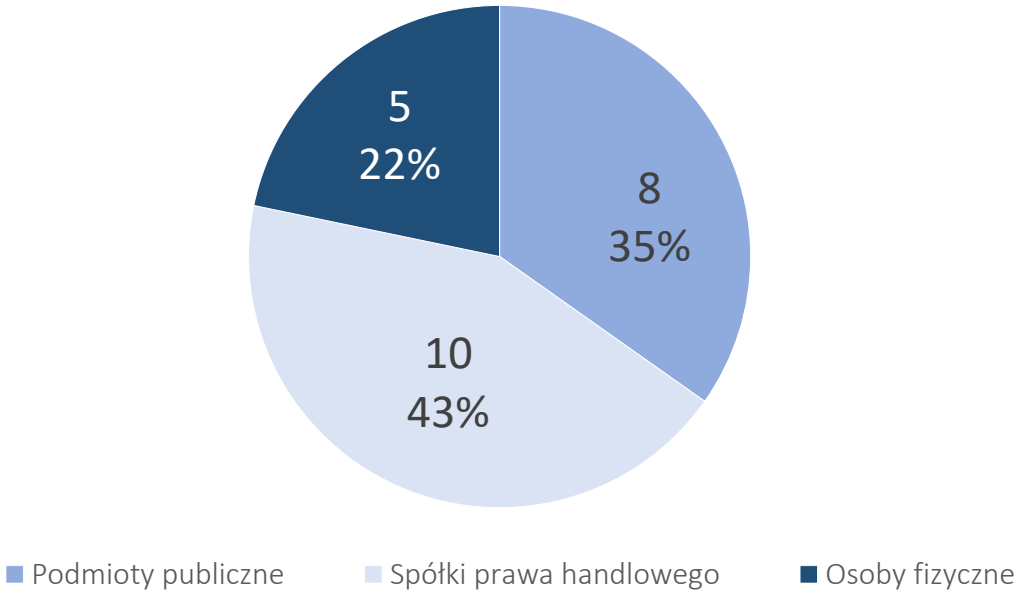
europejskich organów ochrony danych osobowych, wynikającej z przyjęcia i stosowania Wytycznych EROD 04/2022 dotyczących obliczania administracyjnych kar pieniężnych na podstawie RODO[211].




**Wykres 10:** Zestawienie liczby i łącznej wysokości administracyjnych kar pieniężnych orzeczonych przez Prezesa UODO w latach 2021-2025.

Spośród 23 ukaranych podmiotów 8 należało do sektora finansów publicznych Suma nałożonych na nie kar wyniosła 375 400 zł. Wśród pozostałych 15 ukaranych podmiotów prywatnych: 10 to spółki prawa handlowego (przy czym całkowita wysokość nałożonych na nie kar wyniosła 63 959 973,25 zł), zaś 5 ukaranych to osoby fizyczne prowadzące działalność gospodarczą (z sumą kar wynoszącą 101 567 zł).

[211] Wytyczne EROD 04/2022 dotyczące obliczania administracyjnych kar pieniężnych na podstawie RODO, wersja 2.1. przyjęte 24 maja 2023 r. zob.: https://edpb.europa.eu/system/files/2024-01/edpb_guidelines_042022_calculationofadministrativefines_pl_0.pdf.




**Wykres 11:** Zestawienie podmiotów podlegających w 2025 r. ukaraniu administracyjną karą pieniężną, z podziałem na ich status i formę prawną.

Przedstawiając w ujęciu statystycznym z jednej strony działania podmiotów ukaranych, a z drugiej – Prezesa UODO, w odniesieniu do orzeczonych w 2025 r. administracyjnych kar pieniężnych, wskazać należy, że:

1) **prawomocnych** na dzień 31 grudnia 2025 r. ze względu na ich niezaskarżenie do Wojewódzkiego Sądu Administracyjnego w Warszawie było – w całości lub w części, w sytuacji, gdy ukaraniu w jednej decyzji podlegało kilka podmiotów – 7 decyzji nakładających w sumie **9 administracyjnych kar pieniężnych** w łącznej kwocie **438 751 zł**. Spośród tych kar:
   a) 7 kar zapłaconych zostało dobrowolnie przez ukarane podmioty[212],
   b) wobec 1 ukaranego podmiotu wszczęta została egzekucja należności pieniężnych, w wyniku której nałożona kara została wyegzekwowana[213],
   c) wobec 1 ukaranego podmiotu wszczęta została egzekucja należności pieniężnych, która pozostaje w toku[214];
2) **nieprawomocnych** na dzień 31 grudnia 2025 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 **16 administracyjnych kar pieniężnych** w łącznej wysokości **63 881 675,25 zł**, z czego:

[212] DKN.5130.4179.2020 (sześć kar orzeczonych jedną decyzją, przy czym trzy nie podlegały zaskarżeniu), DKN.5131.17.2022, DKN.5131.48.2022, DKN.5131.1.2025 (dwie kary orzeczone jedną decyzją, przy czym jedna nie podlegała zaskarżeniu), DKN.5131.7.2025.
[213] DKE.561.1.2025.
[214] DOKE.561.2.2024.

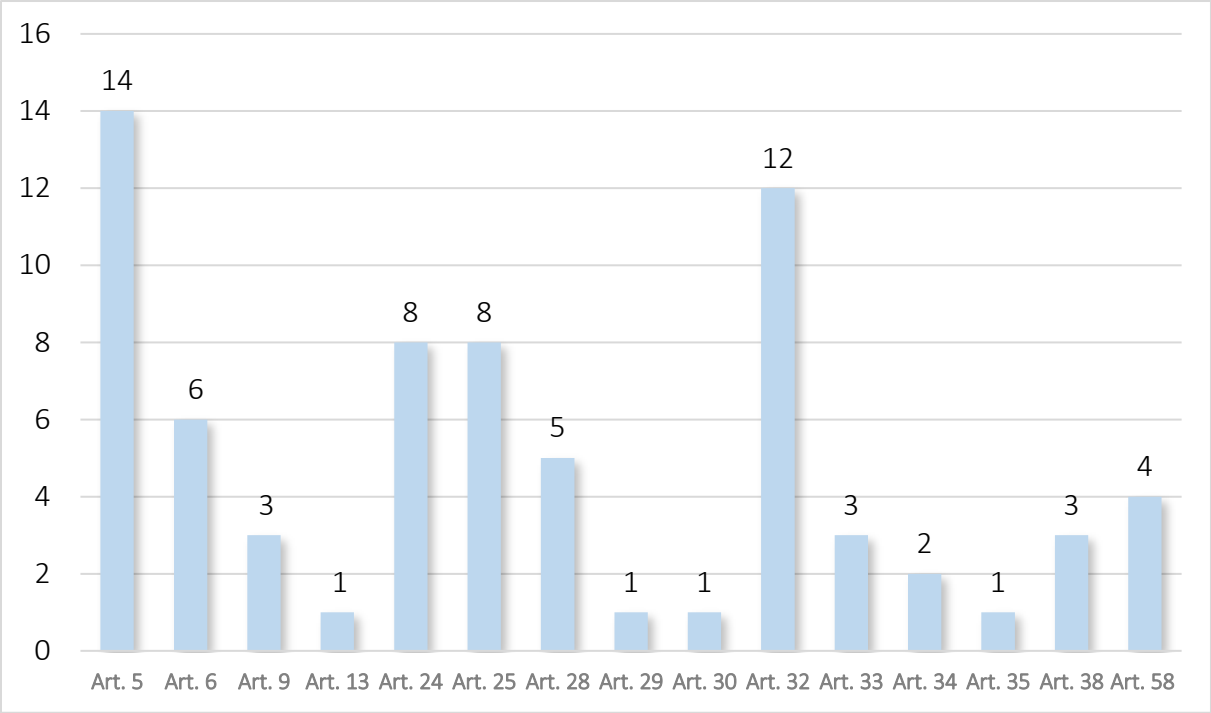
a) 4 administracyjne kary pieniężne zostały utrzymane w mocy przez Wojewódzki Sąd Administracyjny, przy czym zapadłe w tym przedmiocie rozstrzygnięcia na koniec okresu sprawozdawczego nie były prawomocne (w przypadku dwóch kar ukarany skierował do Naczelnego Sądu Administracyjnego skargę kasacyjną, a w odniesieniu do dwóch kar nie upłynął termin na wniesienie przez ukaranego skargi kasacyjnej)[215],
b) w odniesieniu do 12 administracyjnych kar pieniężnych postępowania przed Wojewódzkim Sądem Administracyjnym nadal trwały[216],

3) **nieprawomocnych** na dzień 31 grudnia 2025 r. i **niezaskarżonych** do sądu administracyjnego, było 5 decyzji nakładających **7 administracyjnych kar pieniężnych** w łącznej wysokości **116 514 zł**, przy czym oczekiwały one na wpływ skargi[217] lub uprawomocnienie się[218].

Na poniższym wykresie przedstawiono z kolei informację o rodzajach naruszeń podlegających ukaraniu administracyjnymi karami pieniężnymi, tj. o przepisach RODO, których naruszenie stwierdzone zostało przez Prezesa UODO w decyzjach nakładających na administratorów lub podmioty przetwarzające administracyjne kary pieniężne w 2025 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.

[215] DKN.5131.10.2023 (dwie kary orzeczone jedną decyzją), DKN.5131.4.2024 (dwie kary orzeczone jedną decyzją).
[216] DKN.5112.6.2020, DKN.5130.4179.2020 (sześć kar orzeczonych jedną decyzją, przy czym trzy podlegały zaskarżeniu), DKN.5131.30.2022 (dwie kary orzeczone jedną decyzją), DS.523.4750.2023, DKN.5112.10.2024, DKN.5131.3.2024, DKN.5131.17.2024 (dwie kary orzeczone jedną decyzją), DKN.5131.1.2025 (dwie kary orzeczone jedną decyzją, przy czym jedna podlegała zaskarżeniu), DKN.5131.3.2025.
[217] DOKE.561.6.2023, DKN.5131.3.2024, DKN.5131.5.2024 (dwie kary orzeczone jedną decyzją).
[218] DKN.5112.27.2022 (dwie kary orzeczone jedną decyzją), DOKE.561.11.2024.



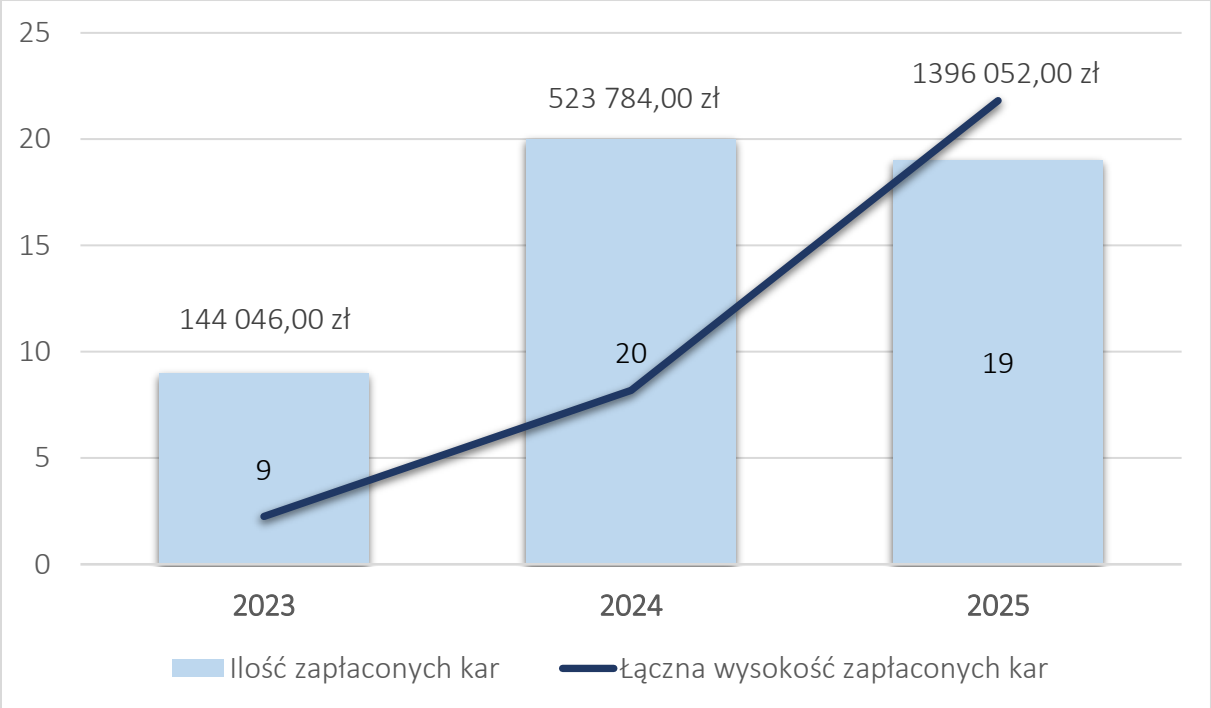

**Wykres 12:** Zestawienie naruszeń poszczególnych przepisów RODO podlegających ukaraniu administracyjnymi karami pieniężnym w 2025 r.

W analizowanym okresie sprawozdawczym **zostało zapłaconych,** to jest uiszczonych dobrowolnie lub ściągniętych w trybie egzekucji administracyjnej, **19 administracyjnych kar pieniężnych** nałożonych w drodze decyzji Prezesa UODO, w tym:

1) **8 kar** w łącznej kwocie 413 496 zł **orzeczonych w 2025 r.** – zapłaconych bez zaskarżenia do sądów administracyjnych;
2) **11 kar** w łącznej kwocie 982 555,60 zł **orzeczonych w poprzednich latach**, z których:
   a) 2 kary w łącznej kwocie 29 547,60 zł zapłacone lub wyegzekwowane zostały bez kontroli sądowej (bez zaskarżenia do sądów administracyjnych),
   b) 1 kara w kwocie 25 000 zł zapłacona została po prawomocnym wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie oddalającym skargę podmiotu ukaranego,
   c) 1 kara w kwocie 159 176 zł zapłacona została po wyroku Naczelnego Sądu Administracyjnego i cofnięciu przez stronę skargi do Wojewódzkiego Sądu Administracyjnego,
   d) 7 kar w łącznej kwocie 768 832 zł zapłaconych zostało po wyrokach Naczelnego Sądu Administracyjnego oddalających skargi kasacyjne podmiotów ukaranych na wyroki Wojewódzkiego Sądu Administracyjnego oddalające ich skargi na decyzje Prezesa UODO.

Liczba 19 zapłaconych kar pieniężnych oznacza nieznaczny – **o 5 %** – **spadek ilościowy takich kar w stosunku do roku 2024**, w którym uiszczonych dobrowolnie

lub wyegzekwowanych kar było 20. Jednocześnie oznacza to **wzrost o 111 % w porównaniu z rokiem 2023**, w którym zapłaconych zostało 9 kar. Wyraźna tendencja zwyżkowa dotyczy natomiast sumy wysokości zapłaconych administracyjnych kar pieniężnych, która w 2025 r. wyniosła **1 396 052 zł**. Oznacza to **wzrost kwotowy o 167 % w stosunku do roku 2024**, w którym łączna wysokość uiszczonych kar wyniosła 523 783,82 zł oraz **wzrost o 869 % w porównaniu do roku 2023**, w którym suma ta wyniosła 144 046,28 zł. Wyżej omówione tendencje skuteczności egzekwowania administracyjnych kar pieniężnych orzekanych przez Prezesa UODO ilustruje poniższy **Wykres 13**. Zauważyć należy, że wzrost wysokości zapłaconych kar związany był w dużym stopniu z wyczerpaniem przez strony środków zaskarżenia w postępowaniu sądowo-administracyjnym. W omawianym okresie sprawozdawczym 7 kar (orzeczonych w latach 2020-2023) zapłaconych zostało po wyrokach Naczelnego Sądu Administracyjnego utrzymujących prawomocnie w mocy decyzje Prezesa UODO, podczas gdy w poprzednich latach – od daty rozpoczęcia stosowania RODO do końca roku 2024 – takich sytuacji było jedynie dwie.




**Wykres 13:** Zestawienie liczby i łącznej wysokości administracyjnych kar pieniężnych zapłaconych w latach 2023–2025.

W ramach kompetencji do orzekania o sankcjach finansowych, Prezesowi Urzędu Ochrony Danych Osobowych przysługuje **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 –

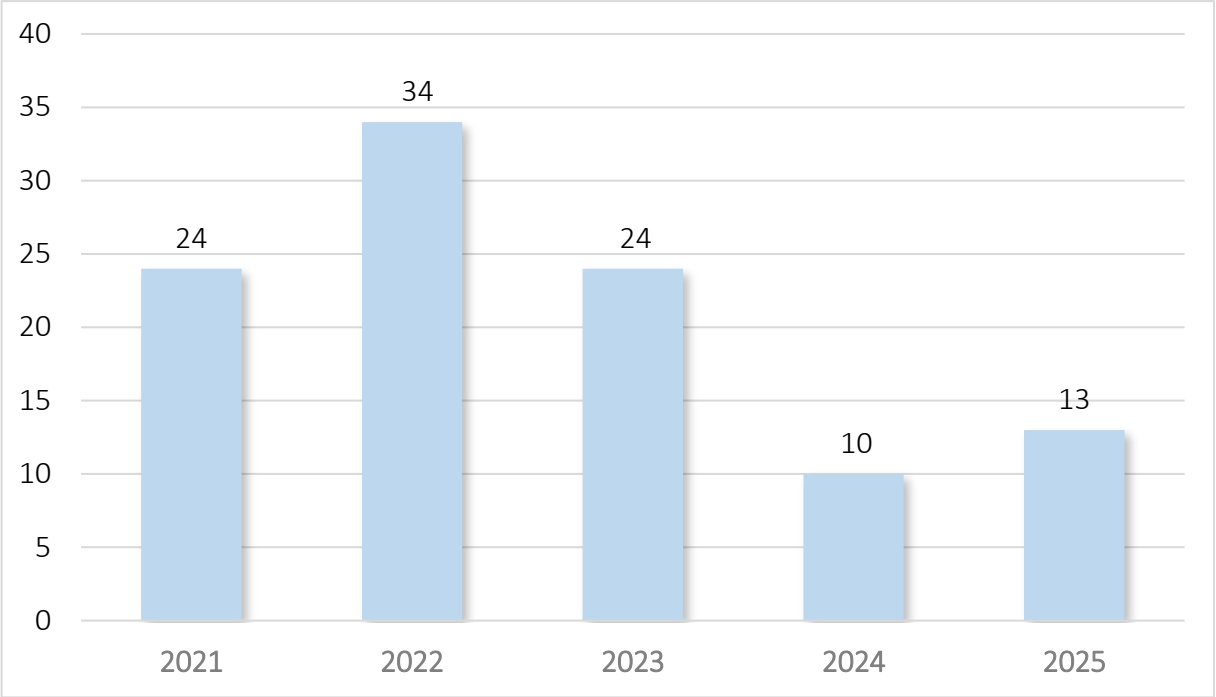
**do wykonywania obowiązków nałożonych na te podmioty decyzjami Prezesa UODO**. Funkcja drugiego rodzaju z tych kar jest alternatywną lub uzupełniającą wobec narzędzi, którymi dysponuje Prezes UODO – w celu wyegzekwowania orzeczonych przez siebie obowiązków niepieniężnych – w oparciu o przepisy ustawy o postępowaniu egzekucyjnym w administracji.

### 14.1. 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, na udzielaniu informacji niepełnych lub przez osoby do tego nieupoważnione, co nie pozwalało na rozstrzygnięcie sprawy lub wydłużało w sposób nieuzasadniony czas trwania postępowań.

W celu zdyscyplinowania stron postępowań do prawidłowego wypełniania obowiązków procesowych, Prezes UODO wszczął w 2025 r. z urzędu **13 postępowań** w przedmiocie nałożenia administracyjnej kary pieniężnej za tego rodzaju naruszenia. Oznacza to wzrost liczby tego rodzaju postępowań o 30 % w stosunku do poprzedniego okresu sprawozdawczego, w którym wszczęto 10 rodzaju postępowań. Dane dotyczące liczby analogicznych postępowań zainicjowanych w poprzednich okresach sprawozdawczych – w porównaniu z rokiem 2025 – przedstawia poniższy wykres.




**Wykres 14:** Zestawienie liczby wszczętych w latach 2021–2025 postępowań w przedmiocie nałożenia kary za brak współpracy z Prezesem UODO i za niezapewnienie organowi 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**[219].

**Decyzjami nakładającymi administracyjne kary pieniężne** zakończyły się **2 postępowania**; wysokość nałożonych tymi decyzjami kar wyniosła łącznie **35 745 zł,** przy czym w przypadku jednej z ww. kar została ona wyegzekwowana w całości w drodze egzekucji należności pieniężnych[220], druga zaś oczekuje na uprawomocnienie się[221].

Pozostałych **7 postępowań** w przedmiocie nałożenia kary za brak współpracy z organem oraz niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań wszczętych w 2025 r. **nie zostało zakończonych** do dnia sporządzenia niniejszego sprawozdania.

[219] DKE.561.2.2025, DKE.561.3.2025, DKE.561.5.2025, DKE.561.7.2025.
[220] DKE.561.1.2025.
[221] DKE.561.9.2025.

### 14.2. 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 2025 Prezes UODO **nie wszczął żadnego postępowania** w przedmiocie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazu, orzeczonego przez siebie w decyzji administracyjnej. Wydał natomiast w tym okresie **jedną decyzję nakładającą administracyjną karę pieniężną w kwocie 25 255 zł** (w postępowaniu wszczętym jeszcze w 2024 roku)[222].

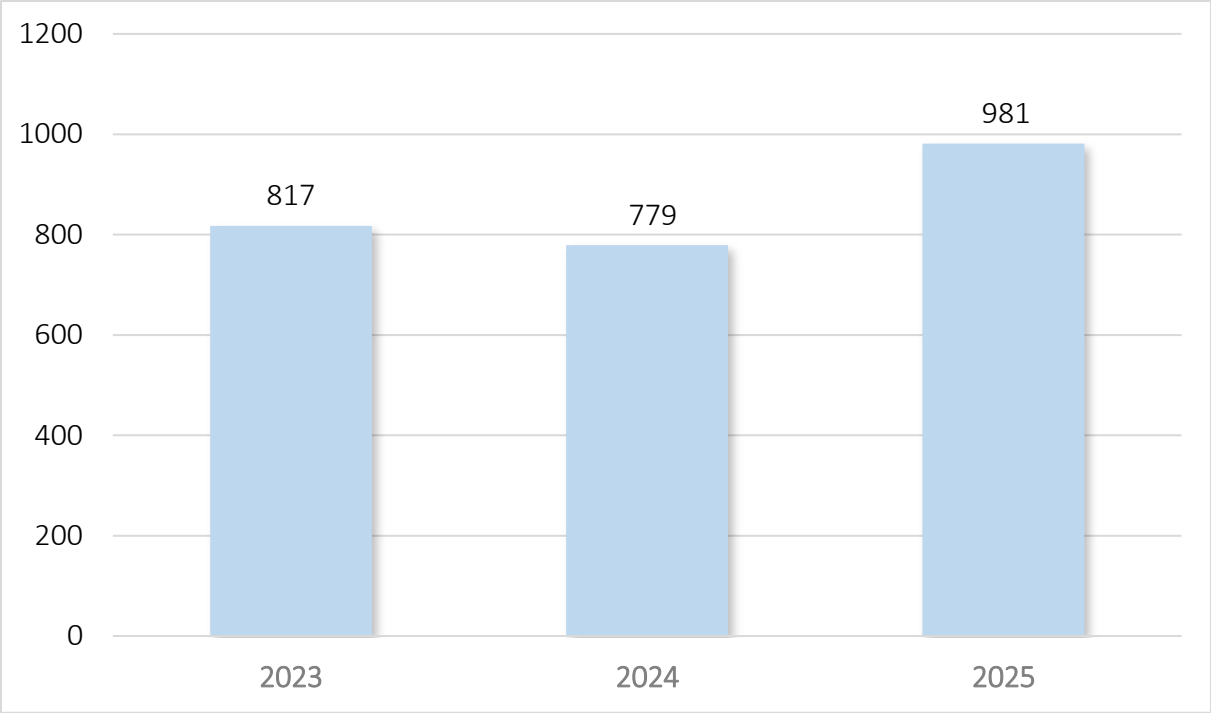
## 15. Opiniowanie projektów aktów prawnych dotyczących ochrony danych osobowych

Zgodnie z art. 57 ust. 1 lit. c RODO rolą organu nadzorczego jest doradzanie parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych. Jednym z kluczowych zadań realizowanych przez Prezesa UODO jest zatem opiniowanie projektów aktów prawnych pod względem ich zgodności z normami dotyczącymi ochrony danych osobowych.

W roku 2025 do Prezesa Urzędu Ochrony Danych Osobowych **wpłynęły 623 projekty aktów prawnych** (rządowych, poselskich, obywatelskich i innych), w tym ustaw, rozporządzeń oraz innych aktów krajowych i międzynarodowych. Łącznie w ubiegłym roku **zaopiniowano 981 projektów**.

To zdecydowanie więcej niż w roku poprzednim, w którym wpłynęło 570 projektów aktów prawnych, a łącznie zaopiniowano ich 779.

[222] DOKE.561.2.2024.




**Wykres 15:** Liczba zaopiniowanych projektów aktów prawnych, które wpłynęły do Urzędu Ochrony Danych Osobowych w latach 2023–2025.

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 RODO.

Na podstawie analizy opinii legislacyjnych Prezesa UODO wyróżnić można kwestie, które budzą problemy, a także wskazać powtarzające się uchybienia. Wiele z nich stanowi powielenie tendencji zauważonych w latach ubiegłych. W roku 2025 z jeszcze większą siłą uwidoczniły się jednak liczne trudności związane głównie z wdrażaniem nowych technologii, a także stałą rozbudową systemów cyfrowych oraz operacji przetwarzania opartych o rozbudowane rejestry państwowe.

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

1) uwzględnienie ochrony danych osobowych w fazie projektowania;
2) implementacja testu prywatności jako elementu oceny skutków przyjmowanych regulacji;
3) stosowanie zasady praworządności, przyjęcie właściwej konstrukcji podstawy prawnej przetwarzania danych osobowych, zachowanie zasad hierarchii źródeł prawa, odpowiedniej rangi aktu prawnego regulującego prawa i obowiązki w przedmiocie przetwarzania danych osobowych;

4) 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;
5) rozgraniczenie ról podmiotów biorących udział w procesach przetwarzania danych – normy kierowane do wykonawców regulacji: administratorów, podmiotów działających w ich imieniu czy na ich rzecz;
6) stosowanie zasad przetwarzania danych osobowych, zwłaszcza zgodności z prawem, rzetelności i przejrzystości oraz rozliczalności, w tym dla przetwarzania danych szczególnych kategorii oraz identyfikatora PESEL;
7) przetwarzanie danych w kontekście procesów cyfryzacji państwa i stosowania nowych technologii;
8) kształtowanie zakresu i modelu nowych kompetencji Prezesa Urzędu Ochrony Danych Osobowych wynikających z aktów unijnych oraz przepisów krajowych implementujących czy służących stosowaniu prawa unijnego;
9) przetwarzanie danych osobowych w kontekście nowych projektów informatycznych, w szczególności w zakresie testu prywatności, zasad: zgodności z prawem, rzetelności i przejrzystości oraz rozliczalności.

## 15.1. Uwzględnienie ochrony danych osobowych na etapie prac legislacyjnych

Uprawnienie przyznane organowi nadzorczemu w art. 57 ust. 1 lit. c RODO pozwala na eliminowanie nieprawidłowości dotyczących procesów przetwarzania danych osobowych już na etapie tworzenia prawa. Stosownie do treści tego przepisu 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. Państwa członkowskie, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli dotyczy on przetwarzania danych osobowych – zgodnie z art. 36 ust. 4 RODO konsultują się z organem nadzorczym. Przedstawianie do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych projektów aktów prawnych dotyczących przetwarzania danych osobowych jest obowiązkiem wynikającym zarówno z art. 51 ustawy o ochronie danych osobowych, jak i z § 38 ust. 1 pkt 3 Regulaminu pracy Rady Ministrów[223].

Pomimo ciążącego obowiązku kierowania do organu nadzorczego projektów aktów odnoszących się do problematyki ochrony danych osobowych, część z nich nie jest przedstawiana jego ocenie. Zjawisko to odnotować należy w 2025 r. tak, jak miało to miejsce w poprzednich latach. Prezes UODO nierzadko angażowany jest dopiero na późniejszym etapie prac legislacyjnych. Ma to miejsce za sprawą np. zaproszenia od Rządowego Centrum Legislacji do udziału w komisji prawniczej, a także na etapie opiniowania w parlamentarnym procesie legislacyjnym. Opiniowanie ma także miejsce

[223] Uchwała nr 190 z 29 października 2013 r.

w odniesieniu do poselskich i senackich projektów, w czasie sejmowych i senackich prac nad regulacjami. Jednak przyjmowanie i wdrażanie eksperckich wskazówek organu na tak późnym etapie prac rządowych czy bez konsultacji na etapie rządowym może powodować duże utrudnienia dla projektodawcy we wdrażaniu regulacji odpowiadających standardom ochrony danych osobowych, m.in. ze względu na stopień zaawansowania tych prac i poczynionych ustaleń na etapie uzgodnień i konstatacji z innymi resortami. Wypracowywanie przepisów prawa wymaga tymczasem uwzględnienia ochrony danych osobowych na jak najwcześniejszym etapie planowania czy podejmowania decyzji o przetwarzaniu, na etapie poprzedzającym opiniowanie aktu prawnego zgodnie z zapewnieniem ochrony danych w fazie projektowania oraz domyślną ochroną danych (art. 25 ust. 1 RODO[224]). Ma to coraz większe znaczenie również w świetle innych aktów związanych z ochroną danych osobowych, takich jak akt w sprawie sztucznej inteligencji[225], rozporządzenie eIDAS2[226], dyrektywa 2016/680[227], dyrektywa NIS2[228], EHDS[229]. Pomijanie tak ważnego elementu w procesie tworzenia prawa, jak konsultowanie projektów aktów prawa dotyczących przetwarzania danych osobowych, niesie za sobą ryzyka. Przyjmowane są regulacje niekompletne, wadliwe czy niewystarczające – szkodliwe dla systemu prawa krajowego i europejskiego, dla wykonawców norm (administratorów), niezapewniające pełnych gwarancji dla podmiotów danych, niekiedy ograniczające w ustawodawstwie krajowym prawo europejskie. Jest to wskazywane w opiniach organu nadzorczego. W 2025 r. organ opiniował także niektóre projekty z własnej inicjatywy, z urzędu.

---

[224] Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

[225] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmian rozporządzonych (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).

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej, dalej: eIDAS2.

[227] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, dalej: dyrektywa 2016/680.

[228] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwo na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

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

Wynikiem własnej inicjatywy organu była opinia do **projektu ustawy o zmianie ustawy o działalności leczniczej oraz niektórych innych ustaw**[230]. Nie był on bowiem przekazany do zaopiniowania w trybie uzgodnień wbrew obowiązkowi prawnemu i pomimo, że rozwiązania zawarte w projekcie ściśle wiązały się z przetwarzaniem danych osobowych w elektronicznej dokumentacji medycznej. Organ zwrócił szczególną uwagę na zakres danych osobowych przetwarzanych w tej dokumentacji, w tym numer PESEL identyfikujący osobę trzecią, tj. wystawcę tej dokumentacji, jako nieadekwatny, zważywszy na inne identyfikujące go dane oraz możliwość wykorzystania identyfikatora zawodowego. Zakwestionowana została również niezbędność i zasadność przekazywania pełnej (całej) dokumentacji medycznej służbom statystyki publicznej. Zwrócono uwagę na konieczność poszanowania zasad i gwarancji wynikających z przepisów RODO oraz na pozyskiwanie przez organ publiczny danych z innych rejestrów, które nie powinno prowadzić do łączenia całych zasobów znajdujących się w systemach publicznych. Tworzenie przepisów regulujących tego rodzaju rozwiązania powinno być poprzedzone pogłębioną analizą, tak by zakres pozyskiwanych danych osobowych nie miał charakteru nadmiarowego i nieadekwatnego do zadań realizowanych przez podmioty publiczne. Proces legislacyjny nie został zakończony.

W tym trybie przedstawiono również opinię do **projektu ustawy o zmianie ustawy o działalności pożytku publicznego i o wolontariacie oraz ustawy o grach hazardowych**[231]. Prezes Urzędu, w myśl konstytucyjnej zasady legalizmu, działając z urzędu, zwrócił uwagę na istotne kwestie regulowane tym aktem, w tym na: konieczność zrezygnowania z identyfikacji osoby, której dane dotyczą, za pomocą danych osób trzecich, jawny model przetwarzania danych, a także na nieprawidłowo wyznaczoną rolę administratora. Eksperckie wsparcie organu nadzorczego przyniosło skutek i zakończyło się sukcesem legislacyjnym – w toku prac nad ustawą uwzględnione zostały uwagi Prezesa UODO wniesione z urzędu, co niewątpliwie przyczyni się do uchwalenia regulacji uwzględniającej standardy przetwarzania i ochrony danych osobowych. Ustawa została uchwalona i podpisana przez Prezydenta [232].

**Projekt ustawy o zmianie ustawy o systemie ubezpieczeń społecznych**[233], mimo że dotyczył niezwykle istotnych kwestii w kontekście ochrony danych i prywatności, trafił do organu dopiero na etapie sejmowego procesu legislacyjnego. Przewidywał **przekazywanie przez Zakład Ubezpieczeń Społecznych danych osobowych zgromadzonych na koncie płatnika składek podmiotom prywatnym**, tj. bankom, instytucjom finansowym, instytucjom kredytowym oraz instytucjom pożyczkowym. Na jego podstawie podmioty prywatne mają zyskać uprawnienie do pozyskiwania danych dotyczących znacznej liczby osób fizycznych będących płatnikami składek, a obejmujących m.in. informacje o stanie rozliczeń należnych

[230] DPNT.401.413.2025.
[231] DPNT.401.348.2025.
[232] Dz. U. z 2026 r. poz. 1040.
[233] DPNT.401.193.2025.

składek, do poboru których uprawniony jest ZUS. Prezes UODO odniósł się nie tylko do szczegółowych rozwiązań przewidzianych w projekcie, lecz podał w wątpliwość zasadność samego przekazywania podmiotom prywatnym tego rodzaju danych, tj. czy jest ono rzeczywiście niezbędne do realizacji zakładanego celu, jakim jest „ograniczenie biurokracji, przyspieszenie procesów decyzyjnych i zwiększenie efektywności gospodarki" (uzasadnienie projektu ustawy). Niestety, pomimo doniosłości projektowanej regulacji, projektodawca w żaden sposób nie odniósł się do uwag Prezesa UODO i nie zostały one uwzględnione. Proces legislacyjny nie został zakończony.

Do zaopiniowania nie przekazano organowi również **projektu ustawy o zmianie ustawy o podatku od towarów i usług oraz ustawy o zasadach ewidencji i identyfikacji podatników i płatników**[234]. Przewidywał on obowiązek prowadzenia przez podatnika ewidencji m.in. kontrahentów, a uwagi Prezesa UODO dotyczyły zakresu danych osobowych w niej zawartych oraz okresu ich przechowywania. Projektodawca zapowiedział uwzględnienie uwag. Proces legislacyjny nie został zakończony.

Prezes Urzędu w swoich opiniach legislacyjnych zwraca również uwagę na konieczność dostosowania projektowanych regulacji do dyrektywy 2016/680. Takiej ocenie poddano **projekt ustawy o koordynacji działań antykorupcyjnych oraz likwidacji Centralnego Biura Antykorupcyjnego**[235]. Zauważono, że charakter proponowanych zmian wymagał przeprowadzenia oceny skutków dla ochrony danych. Konsekwencją przeprowadzenia takiej analizy ryzyka powinno być odzwierciedlenie projektowanych zmian w obowiązującym porządku prawnym z uwzględnieniem zasad przetwarzana danych osobowych i obowiązków administratora danych wynikających z rozporządzenia 2016/679 oraz dyrektywy 2016/680. Proces legislacyjny nie został zakończony.

Kwestię konieczności dostosowania projektowanych przepisów do dyrektywy 2016/680 Prezes UODO podniósł także w opinii do **projektu ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw**[236]. Zwrócił uwagę, że projektowane rozwiązania odnoszące się do przetwarzania danych osobowych, w tym o szczególnym charakterze, wymagają doprecyzowania. Ponadto powinny one zyskać taki kształt, by zagwarantować danym poufność i integralność. Uwagi Prezesa UODO nie zostały uwzględnione. Ustawa została uchwalona i podpisana przez Prezydenta RP[237].

Kolejnym przykładem oceny dokonanej z perspektywy zarówno zgodności z RODO, jak i z dyrektywą 2016/680 jest **projekt ustawy o zmianie ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych oraz niektórych innych ustaw**[238]. W swojej opinii Prezes UODO zwrócił uwagę m.in. na

[234] DPNT.401.436.2025.
[235] DPNT.401.458.2025.
[236] DPNT.401.2.2025.
[237] Dz. U. z 2026. poz. 1178.
[238] DPNT.401.367.2025.

prowadzenie kontroli przez wyznaczony do tego organ w niezidentyfikowanych ustawowo podmiotach, co w świetle zasad ochrony danych osobowych, jak i konstytucyjnej zasady legalizmu budziło wątpliwości. Uwagę organu uwzględniono, wykreślając z kręgu podmiotów podlegających kontroli nieokreślone w przepisach jednostki. Proces legislacyjny nie został zakończony.

## 15.2. Ocena skutków dla ochrony danych osobowych w procesie legislacyjnym

W toku opiniowania projektów aktów prawnych w roku 2025 r. Prezes UODO zwrócił uwagę na brak wykonywania przez projektodawcę testu prywatności wraz z oceną skutków dla ochrony danych.

Przeprowadzanie takiej oceny, zwanej także roboczo testem prywatności, wywodzić należy z art. 35 ust. 10 RODO w zw. z art. 25 ust. 1 RODO. Ocena skutków regulacji dla ochrony danych osobowych wykonywana powinna być dla projektów wymagających szczególnej uwagi pod kątem ryzyk dla ochrony danych. Pozwala ona m.in. zbadać, czy projektowane przepisy, zgodnie z art. 6 ust. 3 RODO, są proporcjonalne i stanowią gwarancje odpowiednie do *ratio legis*, tj. do wyznaczonego, prawnie uzasadnionego celu przetwarzania danych osobowych, a także wypracować – już na etapie projektowania aktu prawnego – rozwiązania gwarancyjne dla podmiotów danych.

Prezes UODO w celu usunięcia dostrzeżonych luk w procesie stanowienia rozwiązań prawnych związanych z przetwarzaniem danych osobowych skierował wystąpienie do Przewodniczącego Komitetu Stałego Rady Ministrów z wnioskiem o podjęcie działań legislacyjnych mających na celu uzupełnienie Regulaminu pracy Rady Ministrów w zakresie obowiązku sporządzenia OSR prywatności do projektowanych aktów normatywnych, celem zapewnienia dostosowania ich do przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[239]. Odpowiedź na wystąpienie organu nadzorczego miała zasadniczo wymiar pozytywny. Przewodniczący Komitetu Stałego Rady Ministrów w piśmie z 31 marca 2025 roku z jednej strony podkreślił znaczenie obowiązku przedstawiania projektowanych regulacji dotyczących danych osobowych do zaopiniowania organowi do spraw ochrony danych osobowych[240]. Wskazał również, że ocena skutków społeczno-gospodarczych

[239] Wystąpienie Prezesa Urzędu Danych Osobowych do Przewodniczącego Komitetu Stałego Rady Ministrów z 14 lutego 2025 r. (znak: DOL.413.15.2024) z wnioskiem o podjęcie działań legislacyjnych mających na celu uzupełnienie Regulaminu pracy Rady Ministrów w zakresie obowiązku sporządzenia OSR prywatności do projektowanych aktów normatywnych, celem zapewnienia dostosowania ich do przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

[240] Pismo Ministra M. Berka, Przewodniczącego Komitetu Stałego Rady Ministrów z 31 marca 2025 r. znak: DPPR.WPPR.0635.1.2025. W niniejszym piśmie Pan Minister wskazał m.in., że „drugim narzędziem, ustanowionym w przepisach prawa, które ma na celu zagwarantowanie odpowiedniego standardu ochrony danych osobowych w projektowanych regulacjach, jest wyrażony w art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych obowiązek przekazywania założeń i projektów aktów prawnych dotyczących danych osobowych do zaopiniowania Prezesowi Urzędu Ochrony Danych Osobowych. Dodatkowo kompetencje do opiniowania projektów przekazanych przez Prezesa Urzędu Ochrony Danych Osobowych posiada również Rada do Spraw Ochrony Danych Osobowych. Te

w zakresie ochrony danych osobowych powinna być dokonywana przez organ wnioskujący już na etapie poprzedzającym opracowanie projektu legislacyjnego[241]. Prezes UODO swoje stanowisko dotyczące konieczności wykonywania testu prywatności zgłaszał również podczas opiniowania projektów informatycznych[242].

Niezależnie od powyższego przeprowadzenie przez projektodawcę oceny skutków dla ochrony danych na etapie prac legislacyjnych wciąż pozostaje niezwykle istotnym postulatem stale przewijającym się w opiniach legislacyjnych Prezesa UODO. Zgodnie z art. 35 ust. 1 RODO 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. Pomimo istotności tego zagadnienia, wciąż powtarzającym się zjawiskiem jest ignorowanie przez projektodawców przeprowadzenia oceny skutków dla ochrony danych jako elementu procesu legislacyjnego, co nie sprzyja zapewnieniu odpowiedniego poziomu ochrony danych w projektowanych regulacjach. Z drugiej strony należy odnotować, że w porównaniu z rokiem 2024 r. sytuacja uległa pewnej poprawie. Projektodawcy w przedstawianych do zaopiniowania projektach aktów prawnych zaczęli bowiem uwzględniać przeprowadzenie ocena skutków dla ochrony danych, jednak bywa ona niewystarczająca, tzn. nie wykazuje ona dostatecznie niezbędności przetwarzania określonych danych osobowych ani potencjalnych ryzyk związanych z ich przetwarzaniem.

Za przykład takiej sprawy może służyć **projekt ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych**

---

ustawowe gwarancje znajdują swoje odzwierciedlenie w przepisach Regulaminu pracy RM. Zgodnie bowiem z § 38 ust. 1 pkt 3 Regulaminu pracy RM każdy projekt dokumentu rządowego, który dotyczy danych osobowych, powinien zostać skierowany do zaopiniowania przez Prezesa Urzędu Ochrony Danych Osobowych. Gwarancję realizacji tego obowiązku stanowi natomiast regulacja § 21a Regulaminu pracy RM, która zobowiązuje Rządowe Centrum Legislacji do weryfikowania wykonania przez organ wnioskujący obowiązków związanych z przekazaniem projektu do zaopiniowania".

[241] Jak wskazał Minister M. Berek, Przewodniczący Komitetu Stałego Rady Ministrów w piśmie z 31 marca 2025 r. znak: DPPR.WPPR.0635.1.2025: „Jeżeli projektowane rozwiązania dotyczą danych osobowych to ocena skutków społeczno-gospodarczych w zakresie ochrony danych osobowych powinna być dokonywana przez organ wnioskujący już na etapie poprzedzającym opracowanie projektu. Formularz OSR przedstawia natomiast zbiorcze, zagregowane podsumowanie wyników oceny skutków regulacji, zaś katalog elementów, który należy uwzględnić podsumowując dokonywaną ocenę wpływu, określony w § 28 ust. 2 Regulaminu pracy Rady Ministrów, ma charakter otwarty. Należy odnotować, że obowiązujący wzór formularza OSR zawiera pkt 10 „Wpływ na pozostałe obszary", w którym jest możliwe odniesienie się do wpływu projektowanej regulacji na ochronę danych osobowych. W praktyce ocena skutków w zakresie danych osobowych jest przedstawiana w OSR (w sposób syntetyczny) lub w uzasadnieniu projektu.".

[242] Więcej na ten temat w dalszej części niniejszego sprawozdania dotyczącej opiniowania projektów informatycznych.

**i niektórych innych ustaw**[243]. Zakładał on prowadzenie centralnej elektronicznej rejestracji, obejmującej m.in. dane dotyczące usługobiorców, o których mowa w ustawie o systemie informacji w ochronie zdrowia. Miały być w niej przetwarzane za pomocą systemu informatycznego w szerokim zakresie dane osobowe osób fizycznych, w tym dane, które mogą być przetwarzane biometrycznie (pozyskiwane, w tym nagrywane, z wykorzystaniem asystenta głosowego) i dane dotyczące zdrowia. Projektodawca dokonał wprawdzie analizy skutków regulacji dla ochrony danych, co ocenić należy pozytywnie, niemniej wzbudziła on zastrzeżenia organu nadzorczego. Projekt przewidywał bowiem przetwarzanie szerokiego zakresu danych, w tym danych szczególnych kategorii, za pomocą zautomatyzowanych systemów. Z dużym prawdopodobieństwem takie przetwarzanie powodować może wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Z analizy dołączonej do projektu wynikało tymczasem, że ryzyko przetwarzania projektodawca oszacował jako niskie i nie przewidział żadnych gwarancji ochrony danych osobowych. W opinii organu nadzorczego przeprowadzenie oceny skutków regulacji dla ochrony danych na etapie projektowania regulacji powinno prowadzić do wykazania niezbędności przetwarzania danych osobowych, w określony sposób, we wskazanym konkretnie celu i zakresie oraz do właściwej oceny ryzyka, jakie projektowane rozwiązania powodują w zakresie przetwarzania danych osobowych, a w konsekwencji jak wpływają na prywatność osób fizycznych. Projektodawca nie wykazał, aby konieczne było przetwarzanie wszystkich wskazanych w projekcie kategorii danych. W szczególności nie wyjaśnił kwestii przetwarzania danych biometrycznych wszystkich usługobiorców w celu, jakim ma być łatwiejszy dostęp do informacji o dostępności terminów u wszystkich świadczeniodawców. Ustawa została uchwalona i podpisana przez Prezydenta RP[244].

Podobnie było w przypadku **projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw**[245]. Choć projektodawca dokonał analizy skutków regulacji dla ochrony danych, to Prezes UODO zwrócił uwagę, że powinna ona uwzględniać gwarancje ochrony danych osobowych. Gwarancje takie powinny wynikać wprost z projektowanych regulacji. Wątpliwości budziło zatem to, że określeniu przez projektodawcę „środków mających na celu zmniejszenie ryzyka", odnoszących się do technicznych i organizacyjnych kwestii, nie towarzyszyło wprowadzenie w regulacji gwarancji praw pacjentów określonych w projektowanych normach prawnych odpowiednio do ryzyk przewidywanego przetwarzania szczególnych kategorii danych w sposób głęboko ingerujący w prawa i wolności podmiotów danych. Proces legislacyjny nie został zakończony.

Ocena skutków wykonywanych operacji dla praw i wolności osób fizycznych stała się obowiązkiem nie tylko z punktu widzenia przetwarzania danych osobowych, lecz także stosowania systemów sztucznej inteligencji. Niektóre projekty ze względu na doniosłość przetwarzania wynikającą z charakteru operacji wykonywanych na danych

[243] DPNT.401.101.2025.
[244] Dz. U. z 2025 r. poz. 1537.
[245] DPNT.401.224.2025.

wymagała dokonania właśnie takiej oceny. W tym kontekście istotny jest **projekt ustawy o kredycie konsumenckim**[246], implementujący do krajowego porządku prawnego dyrektywy unijne. Ich cel to zwiększenie poziomu ochrony interesów konsumentów, którym oferowane są kredyty konsumenckie lub usługi finansowe zawierane na odległość oraz ułatwienie rozwoju działalności transgranicznej, w tym za pośrednictwem narzędzi cyfrowych, a także uproszczenie i unowocześnienie rozwiązań funkcjonujących na rynku wewnętrznym kredytów konsumenckich. Wprowadzenie proponowanej regulacji miało prowadzić do przetwarzania – co istotne, także przy użyciu nowych technologii – znacznej ilości i na dużą skalę danych osób fizycznych, w tym danych szczególnych kategorii (w rozumieniu w art. 9 ust. 1 RODO, m.in. danych dotyczących zdrowia), podlegających wzmocnionej ochronie prawnej. Na podstawie projektowanych przepisów przetwarzane miały też być informacje objęte tajemnicą prawnie chronioną. Projektowane przepisy zakładały także zautomatyzowane przetwarzanie danych osobowych, w tym profilowanie. Zachodziło zatem prawdopodobieństwo, że w związku z oceną zdolności kredytowej mogą być wykorzystywane przez kredytodawców systemy sztucznej inteligencji. W związku z tym w ocenie organu nadzorczego projektodawca powinien wziąć pod uwagę nie tylko przepisy RODO, ale także akt w sprawie sztucznej inteligencji (AI Act), z którego wynika (art. 27) odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (FRIA). W motywie 96 AI Act prawodawca podkreślił, że FRIA ma na celu uzupełnienie oceny ochrony danych, a nie jej zastąpienie. Jeżeli wykonywanie projektowanych norm będzie wiązało się z wykorzystaniem systemów sztucznej inteligencji, to projektodawca powinien również uwzględnić dokonanie takiej oceny. Co więcej, systemy AI powinny być transparentne – wykonawcy norm (kredytobiorcy) powinni być świadomi, że dana interakcja odbywa się ze sztuczną inteligencją, a regulacja o odpowiedniej randze (ustawa) powinna określać cele, których realizacji służy, jakim podmiotom przypisany zostanie status administratora danych, jak również jakie gwarancje ochrony praw i wolności osób zostaną określonej jej przepisami. Zgodnie z AI Act, usługi finansowe związane z udzielaniem pożyczek stanowią systemy AI wysokiego ryzyka, w związku z czym przepisy ww. rozporządzenia również wymagają uwzględnienia przez projektodawcę oceny, o której mowa w art. 27 AI Act. Systemy sztucznej inteligencji, które stwarzają wysokie ryzyko dla zdrowia i bezpieczeństwa lub praw podstawowych osób fizycznych, mogą być dopuszczone do obrotu wyłącznie pod warunkiem spełnienia określonych wymogów i przeprowadzenia oceny zgodności (zaznaczyć należy, że uznanie systemu sztucznej inteligencji za system wysokiego ryzyka nie opiera się wyłącznie na analizie funkcji pełnionej przez system sztucznej inteligencji, ale przede wszystkim na ocenie celu i sposobu jego wykorzystania (motyw 28 i art. 6 AI Act). Proces legislacyjny nie został zakończony.

Zdarza się również, że projektodawca odnosi się do skutków projektowanej regulacji dla ochrony danych na skutek uwag Prezesa UODO. Przykładem takiej sprawy jest **projekt ustawy o ochronie małoletnich przed dostępem do treści**

[246] DPNT.401.262.2025.

**pornograficznych w internecie**[247]. Podstawowym założeniem projektu jest stworzenie systemu służącego skutecznej weryfikacji wieku (potwierdzeniu pełnoletności) użytkownika uzyskującego dostęp do treści pornograficznych, co potencjalnie wiąże się z poważną ingerencją w prywatność osoby, której wiek będzie weryfikowany. Ma to tym większe znaczenie, że z pierwszej wersji projektu przedstawionej do zaopiniowania nie wynikało w żaden sposób, na czym ta weryfikacja ma polegać ani jakie kryteria spełniać. Nie było zatem jasne, jakie dane osobowe będą przetwarzane w celu takiej weryfikacji i w jaki sposób. Jednocześnie projektodawca nie przedstawił oceny skutków projektowanych rozwiązań dla ochrony danych, na co Prezes UODO zwrócił uwagę w swojej opinii. Z zadowoleniem należy odnotować, że w kolejnej wersji projektu ustawy taka ocena skutków regulacji została dokonana. Proces legislacyjny dotyczący projektu nie został zakończony[248].

Innym przykładem sprawy, w której projektodawca przeprowadził test prywatności wskutek wniesienia uwag przez organ nadzorczy, jest **projekt ustawy o zabezpieczeniu socjalnym osób wykonujących zawód artystyczny**[249]. Przeprowadzenie tej oceny ułatwiło projektodawcy określenie zarówno kryteriów zgodności z przepisami ogólnego rozporządzenia o ochronie danych, jak również proporcjonalności planowanych środków przetwarzania do wyznaczonego, prawnie uzasadnionego celu. Ponadto, dzięki przeprowadzeniu oceny skutków, projektodawca zidentyfikował zagrożenia powodujące wysokie ryzyko naruszenia praw podmiotów danych oraz zaplanował konkretne rozwiązania prawne oraz środki techniczne i organizacyjne łagodzące ryzyko oraz pozwalające na stosowne zabezpieczenie owych praw i wolności w planowanych procesach przetwarzania, z korzyścią dla przyszłych wykonawców norm – administratorów, a także dla podmiotów danych. Celem regulacji miało być zagwarantowanie prawidłowego włączenia osób wykonujących zawód artystyczny do systemu ubezpieczeń społecznych i zdrowotnych. Projekt zakładał rozwiązania oparte na podejmowaniu rozstrzygnięć w sprawach o dopłatę dla artysty zawodowego w oparciu o zautomatyzowane przetwarzanie danych osobowych – w tym potencjalnie także danych szczególnych kategorii. Organ nadzorczy zwrócił uwagę, że tego rodzaju przetwarzanie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym m.in.: prawidłowe informowanie osoby, której dane dotyczą, realizację prawa do uzyskania interwencji człowieka, prawa do wyrażenia własnego stanowiska, prawa do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawa do zakwestionowania takiej decyzji, stosowanie odpowiednich matematycznych lub statystycznych procedur profilowania, środków zapewniających korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów i ryzyka dyskryminacji. Uwzględniając uwagi organu nadzorczego, projektodawca zdecydował

[247] DPNT.401.59.2025.
[248] Więcej szczegółów nt. opinii Prezesa UODO ws. projektu ustawy o ochronie małoletnich przed dostępem do treści pornograficznych w internecie dostępnych jest na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3729.
[249] DPNT.401.155.2025.

się uzupełnić projekt o ocenę skutków dla ochrony danych. Proces legislacyjny nie został zakończony.

### 15.3. Zasada zgodności z prawem (praworządności, legalności)

Wszelkie prawa i obowiązki powinny – zgodnie z Konstytucją RP (art. 31 art. 87 ust. 1) – wynikać z aktu prawnego rangi ustawy. Tym samym nie powinny być regulowane przepisami rozporządzenia wykonawczego czy, tym bardziej, aktu wewnętrznie obowiązującego, np. zarządzenia, porozumienia, wytycznych. Zatem prawodawca, określając prawa i obowiązki, z realizacją których związane jest przetwarzanie danych osobowych, powinien odpowiednie elementy wprowadzić w przepisach ustawowych. Wynika to jednoznacznie także z art. 51 Konstytucji RP. Chodzi o:

- odpowiednio skonstruowaną podstawę prawną dla określenia obowiązku przetwarzania danych,
- określenie celu/celów i zakresu, a także rodzaju przetwarzanych danych niezbędnych dla wykonywania tego celu/celów,
- określenie sposobów przetwarzania danych adekwatnie do celów przetwarzania i przyporządkowanie wykonywania operacji na danych osobowych ściśle określonym organom/lub podmiotom, zgodnie z ich kompetencjami wynikającymi z powszechnie obowiązujących przepisów prawa,
- określenie okresów retencji danych,
- określenie innych aspektów niezbędnych dla kompleksowego uregulowania przetwarzania danych dla osiągnięcia *ratio legis*, z uwzględnieniem elementów z art. 6 ust. 3 RODO.

Na brak właściwej regulacji ustawowej zwrócono uwagę w opinii do **projektu ustawy o ochronie małoletnich przed dostępem do treści pornograficznych w internecie**[250]. Pierwsza wersja projektu przedstawiona do zaopiniowania przewidywała, że warunki systemów weryfikacji wieku użytkownika, uzyskującego dostęp do treści pornograficznych, będą określone w zaleceniach. Miałyby one być wydane przez ministra właściwego ds. informatyzacji, w porozumieniu z Prezesem Urzędu Komunikacji Elektronicznej i po zaopiniowaniu przez Prezesa UODO. Z uwzględnieniem: potrzeby zapewnienia skutecznej ochrony małoletnich przed dostępem do treści szkodliwych; możliwości technicznych usługodawców oraz zapewnienia ochrony danych osobowych. Takie rozwiązanie nie mogło zyskać akceptacji, jako że zalecenia nie mieszczą się w hierarchii źródeł prawa, nie stanowią źródła powszechnie obowiązującego prawa (sprzeczność z przepisami RODO oraz konstytucyjnymi zasadami systemu prawa). Mocą zaleceń nie można kształtować żadnych praw ani obowiązków podmiotów prawa. Warunki, jakie ma spełniać weryfikacja wieku, powinny być określone w ustawie. Projektodawca uwzględnił uwagi organu nadzorczego w tym zakresie – zrezygnował z przedmiotowych zaleceń

[250] DPNT.401.59.2025.

i w kolejnej wersji projektu ustawy określił ogólne warunki, jakie powinna spełniać weryfikacja wieku, co stanowi kolejny sukces legislacyjny organu nadzorczego.

Podobna opinia została wyrażona do **projektu rozporządzenia Ministra Edukacji zmieniającego rozporządzenie w sprawie świadectw, dyplomów państwowych i innych druków**[251]. Projekt przewidywał rozszerzenie funkcji legitymacji szkolnej i przedszkolnej – dopuszczenie ich używania do potwierdzania oraz obsługi elektronicznych systemów i usług (szkolnych oraz transportowych). Mankamentem były istotne rozszerzenia zakresu i celów przetwarzania danych osobowych osób małoletnich. Z dokumentu służącego dotychczas głównie do potwierdzania statusu ucznia/dziecka oraz prawa do uzyskiwania ulg ustawowych, legitymacja miała stać się narzędziem identyfikacji elektronicznej. Przewidywano, że poprzez zakodowanie w warstwie elektronicznej legitymacji nowych funkcji w postaci możliwości dostępu do usług czy obsługi elektronicznych systemów wprowadzona zostanie możliwość automatycznej identyfikacji i weryfikacji statusu dziecka - ucznia w wielu niezależnych systemach. W swojej opinii Prezes UODO podniósł, że regulacja dotycząca dokumentu, jakim ma być legitymacja szkolna z różnymi funkcjonalnościami, musi być oparta na jasnych przepisach ustawowych ustalających prawa i obowiązki organów/podmiotów odpowiedzialnych za wydawanie legitymacji szkolnej czy mLegitymacji, w tym w zakresie przetwarzania danych osobowych. Także status legitymacji jako dokumentu, w którego treści mają być przetwarzane dane osobowe, powinien być określony mocą przepisów ustawy, a nie w sposób nieograniczony, określany i rozszerzany jedynie aktem wykonawczym. Jednocześnie obowiązujące aktualnie blankietowe regulacje ustawowe nie pozwalają na uznanie legitymacji szkolnej za dokument potwierdzający tożsamość. Prawodawca powinien określić na poziomie ustawy, jaki jest co do zasady status legitymacji szkolnej, jak również dokumentu elektronicznego odpowiadającego usłudze związanej z mLegitymacją szkolną i odpowiednio do celów przetwarzania ukształtować w nich adekwatne katalogi danych[252]. Rozporządzenie zostało podpisane i ogłoszone[253].

Problem ten nie pojawił się po raz pierwszy w 2025 r. Na przestrzeni lat organ do spraw ochrony danych osobowych kilkukrotnie już krytycznie odnosił się do umieszczania numeru PESEL ucznia na nowych wzorach legitymacji szkolnych[254]. Jest to problem aktualny tym bardziej, że w ustawie – Prawo oświatowe brak, jak wyżej

[251] DPNT.401.533.2025.
[252] Opinia Prezesa UODO z 13 października 2023 r. do projektu rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie świadectw, dyplomów państwowych i innych druków (DOL.401.495.2023 – opinia dotycząca mLegitymacji); opinia Prezesa UODO z 22 czerwca 2022 r. do projektu ustawy o aplikacji mObywatel. (DOL.401.276.2022).
[253] Dz. U. z 2026 r. poz. 439.
[254] Wystąpienie GIODO z 2 marca 2015 r. (DOLiS – 035 – 711/15) skierowane do resortu edukacji w sprawie rozważenia wprowadzenia do rozporządzenia Ministra Edukacji Narodowej z dnia 28 maja 2010 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych zmian dotyczących zakresu danych umieszczanych na legitymacji szkolnej; opinia Prezesa UODO z 9 kwietnia 2021 r. do projektu rozporządzenia Ministra Edukacji i Nauki zmieniającego rozporządzenie w sprawie świadectw, dyplomów państwowych i innych druków (DOL.401.132.2021); opinia Prezesa UODO z 9 lipca 2019 r. do projektu rozporządzenia Ministra Edukacji Narodowej w sprawie świadectw, dyplomów państwowych i innych druków (https://legislacja.rcl.gov.pl/projekt/12321987/katalog/12600180#12600180).

wskazano, nadania legitymacji statusu prawnego dokumentu potwierdzającego tożsamość. Organ nadzorczy przedstawił te zagadnienia jako postulat o charakterze *de lege ferenda* – wymagający dalszej analizy po stronie projektodawcy. Proces legislacyjny nie zakończył się.

Z kolei rozwiązania zawarte w **projekcie rozporządzenia Rady Ministrów w sprawie wzoru kwestionariusza szacowania ryzyka zagrożenia dla życia lub zdrowia dziecka służącego stwierdzeniu zasadności zapewnienia dziecku ochrony w związku z przemocą domową**[255] dotyczyły przetwarzania szczególnych kategorii danych (art. 9 i 10 RODO). Materia ta, zwłaszcza zakres danych osobowych, które miałyby być pozyskiwane przy użyciu kwestionariusza, powinna być jasno i wyczerpująco uregulowana przepisami rangi ustawowej, co Prezes UODO podkreślił w swojej opinii. Za konieczne uznał również przeprowadzenie przez projektodawcę oceny skutków dla ochrony danych ze względu na fakt, że rozporządzenie określało szczegółowy tryb działania odpowiednich służb realizujących procedury odebrania dziecka z rodziny. Uwagi organu nadzorczego dotyczyły również tego, jaki podmiot będzie administratorem zawartych w kwestionariuszu danych, i co za tym idzie, kto będzie odpowiadał za jakość i prawidłowość informacji w nim zawartych. Odnosiły się również do sformułowań zawartych w kwestionariuszu, które w kontekście braku kompleksowego uregulowania zakresu danych i trybu odbierania dziecka z rodziny na poziomie ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy domowej, mogą powodować niejasności interpretacyjne przy wypełnianiu kwestionariusza. Projektodawca nie odniósł się do uwag organu nadzorczego. Rozporządzenie zostało podpisane i ogłoszone[256].

Na to, że ograniczenie wynikających z RODO praw może odbywać się wyłącznie zgodnie z przepisami i warunkami określonymi w art. 23 tego aktu prawnego, organ nadzorczy zwrócił uwagę m.in. w toku opiniowania **komisyjnego projektu ustawy o zmianie ustawy o radcach prawnych**[257]. Zawierał on przepisy częściowo ograniczające prawo do uzyskania informacji o źródle pozyskanych danych (art. 15 ust. 1 lit. g RODO) oraz prawo do ograniczenia przetwarzania (art. 18 ust. 1 RODO) w związku z przetwarzaniem danych osobowych przez Krajową Izbę Radców Prawnych i okręgowe izby radców prawnych w toku realizacji swoich zadań. Organ nadzorczy zwrócił uwagę, że regulacje wprowadzające ograniczenia praw podmiotów powinny zostać poprzedzone gruntowną analizą mającą na celu wykazanie rzeczywistej niezbędności dla prawnie uzasadnionych celów i w sposób wyczerpujący uzasadnione. Mając na względzie warunki określone w art. 23 ust. 1 RODO, projektodawca może wprowadzić jedynie regulację proporcjonalną – ograniczyć prawo podmiotowe, ale nie zupełnie to prawo wyłączyć. Przepis ustawy ograniczający prawa osób, których dane dotyczą, powinien przewidywać środki gwarancyjne i łagodzące

[255] DPNT.401.40.2025.
[256] Rozporządzenie Rady Ministrów z dnia 19 lutego 2025 r. w sprawie wzoru kwestionariusza szacowania ryzyka zagrożenia dla życia lub zdrowia dziecka służącego stwierdzeniu zasadności zapewnienia dziecku ochrony w związku z przemocą domową (Dz. U. poz. 213).
[257] DPNT.401.433.2025.

ryzyko naruszenia tych praw, w tym szczegółowe granice zakresu wprowadzonych ograniczeń, środki prawne zapobiegające nadużyciom i zapewniające, że instytucja odmowy udzielenia informacji lub ograniczenia przetwarzania stosowana jest tylko w sytuacjach wyjątkowych i realnie uzasadnionych. W sprawie tej projektodawca przychylił się do stanowiska wyrażonego w opinii Prezesa Urzędu i odstąpił od zakwestionowanych regulacji, wprowadzając jednocześnie inne rozwiązania korzystne z punktu widzenia ochrony danych osobowych, tym samym współpraca obu podmiotów przyniosła pożądane rezultaty. Ustawa w takim kształcie została przyjęta przez parlament i podpisana przez Prezydenta RP[258].

Projekt **ustawy o zmianie niektórych ustaw w związku z poprawą bezpieczeństwa ruchu drogowego**[259] zakładał nałożenie na osobę przystępującą do egzaminu państwowego na prawo jazdy obowiązku składania pod rygorem odpowiedzialności karnej oświadczenia, że nie toczy się wobec niej postępowanie karne o przestępstwo pozostające w związku z bezpieczeństwem ruchu drogowego. Tymczasem przepisy prawa materialnego nie przewidują takiego wymagania (ustawa o kierujących pojazdami zakazuje jedynie przystępowania do egzaminu państwowego na prawo jazdy osobie, która ma „aktywny" zakaz prowadzenia pojazdów). Projektodawca – na skutek uwag organu nadzorczego – usunął z projektu wadliwe unormowanie. Ustawa została uchwalona i podpisana przez Prezydenta RP[260].

### 15.4. Rejestry publiczne i systemy teleinformatyczne

Rejestry publiczne wciąż pozostają bardzo ważnym i stale pojawiającym się wątkiem w projektach aktów prawnych przedstawianych Prezesowi UODO do zaopiniowania. Rejestry te służą bardzo różnym, często doniosłym celom i – co oczywiste – ich utworzenie bezpośrednio wiąże się z przetwarzaniem danych osób fizycznych, często na szeroką skalę. Organ nadzorczy, nie kwestionując przeważnie samej potrzeby i zasadności prowadzenia określonego rejestru dla realizacji celów państwa, w swoich opiniach nieustannie zwraca jednak uwagę na konieczność zapewnienia właściwego poziomu ochrony danych osobowych w przepisach stanowiących podstawę prawną ich funkcjonowania. Podkreśla, że powinny one określać w szczególności precyzyjnie: zakres danych przetwarzanych w rejestrze i kategorie osób, których dane dotyczą; podmiot odpowiedzialny za prowadzenie i utrzymanie rejestru; cel (cele) jego prowadzenia; zasady udostępniania danych z rejestru czy okres retencji danych. W przypadku tworzenia rejestru, zmiany czy rozszerzenia celów przetwarzania danych w rejestrze istotne jest również przeprowadzenie oceny skutków dla ochrony danych w związku z planowanymi operacjami przetwarzania danych osobowych. Kompleksowo przeprowadzony test prywatności pozwala na mitygację ryzyk związanych z przetwarzaniem. Niedostateczne uwzględnienie powyższych elementów w projektach aktów prawnych statuujących rejestry czy systemy informatyczne wciąż pozostaje, niestety, stale

[258] Dz. U. z 2026 r. poz 731.
[259] DPNT.401.33.2025.
[260] Dz. U. z 2025 r. poz. 1872.

pojawiającym się mankamentem tych dokumentów i Prezes UODO nieustannie zwraca uwagę na powyższe kwestie w swoich opiniach legislacyjnych.

Przykładowo **poselski projekt ustawy o zmianie ustawy o ochotniczych strażach pożarnych**[261] zakładał powstanie nowego rejestru legitymacji strażaków ratowników OSP i osób uprawnionych do świadczenia ratowniczego. Ani z projektu ustawy, ani z uzasadnienia nie wynikało wprost, czy jest to nowy rejestr publiczny. Zakres danych przetwarzanych w ww. rejestrze miał być szerszy niż wynika z obecnie obowiązujących przepisów w przedmiotowym zakresie. Projektodawca nie wykazał konieczności tworzenia rejestru ani niezbędności przetwarzania określonych danych (m.in. numeru PESEL, drugiego imienia) dla realizacji zakładanego celu (tj. identyfikacji i korzystania z dodatkowych świadczeń). Jednocześnie regulował go w sposób nazbyt ogólny – nie odniósł się do sposobu jego funkcjonowania pod kątem zapewnienia poszanowania zasad ochrony danych osobowych, a w konsekwencji nie uwzględniał ich na każdym etapie jego tworzenia i projektowania (w tym zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych). Z projektu nie wynikały także role podmiotów biorących udział w procesie przetwarzania danych w rejestrze ani sposoby, warunki i tryb (wnioskowy czy bezwnioskowy) udostępniania danych. Prezes UODO wskazał na: konieczność zmiany przepisów ustawy o aplikacji mObywatel[262] tak, aby dostosować ją do projektowanych regulacji dotyczących legitymacji strażaka w postaci dokumentu mobilnego w aplikacji mObywatel; zasadność przeprowadzenia przez projektodawcę oceny skutków dla ochrony danych, zwłaszcza w celu wykazania niezbędności przetwarzania danych osobowych we wskazanym konkretnie celu (celach) i zakresie, oraz na niedopuszczalność regulowania zadań podmiotów publicznych (w tym przetwarzania danych osobowych) w drodze porozumień zawieranych między tymi podmiotami – kwestie te powinny wynikać bezpośrednio z przepisów prawa. Ustawa została uchwalona i podpisana przez Prezydenta RP[263].

Z kolei w **projekcie ustawy zmieniającej ustawę o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw oraz ustawę o finansach publicznych**[264] projektodawca nie wykazał przesłanki niezbędności przetwarzania danych osobowych w sposób umożliwiający ich ujawnienie w centralnym rejestrze umów (CRU) do celu związanego z wykonaniem zadania realizowanego w interesie publicznym. W CRU mają być bowiem gromadzone i publikowane dane osobowe oraz dane finansowe szerokiego kręgu podmiotów, w tym osób fizycznych, będących stronami umów z jednostkami sektora finansów publicznych. Udostępnienie danych osobowych za pomocą narzędzia umożliwiającego przeszukiwanie i publiczne udostępnienie informacji wiąże się z ryzykiem dowolnego i dalszego ich przetwarzania w celach niezwiązanych z jawnością wydatków publicznych. Ryzyko dotyczy też łączenia danych, profilowania osób fizycznych, wnioskowania o ich sytuacji życiowej. Prezes

[261] DPNT.401.108.2025.
[262] Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275 ze zm.).
[263] Dz.U. 2025 poz. 900.
[264] DPNT.401.97.2025.

UODO zwrócił uwagę na te ryzyka w kontekście orzecznictwa trybunałów europejskich[265]. W ocenie organu nadzorczego, skoro rejestr nie jest jedynym sposobem udostępnienia informacji o gospodarowaniu środkami publicznymi (gdyż informacje te mogą zostać udostępnione na wniosek w trybie ustawy o dostępie do informacji publicznej) i ma funkcjonować obok istniejących i funkcjonujących już rejestrów (np. rejestru umów cywilno-prawnych), to wątpliwości budzi konieczność wprowadzenia narzędzia, które stanowi tak istotną ingerencję w odniesieniu do praw: do prywatności i ochrony danych osobowych osób fizycznych, których dane – zarówno osobowe, jak i finansowe – mają być przetwarzane na szeroką skalę w powszechnym rejestrze. Ustawa została uchwalona i podpisana przez Prezydenta RP[266].

W opinii legislacyjnej do **projektu ustawy o zmianie ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich oraz ustawy o Krajowym Rejestrze Karnym**[267] Prezes UODO wskazał, że aktualne rozwiązania prawne dotyczące gromadzenia danych osobowych w rejestrze sprawców przestępstw na tle seksualnym, w odniesieniu do osób nieletnich, mogą stanowić nieproporcjonalne ograniczenie ich prawa do ochrony danych osobowych oraz prawa do prywatności. Dostęp do danych zawartych w Rejestrze z dostępem ograniczonym jest aktualnie znacznie ułatwiony i wykorzystywany szeroko w działalności koncentrującej się na różnych formach opieki nad dziećmi. Przetwarzany jest szeroki zakres danych osobowych nieletniego, co wiąże się z wysokim ryzykiem naruszenia praw osób nieletnich związanym z wtórnym wykorzystaniem tych danych do celów innych niż związane z pierwotnym celem ich przetwarzania, w tym z ryzykiem związanym z łączeniem z innymi danymi, profilowaniem osób fizycznych, wnioskowaniem o ich sytuacji życiowej. Ponadto usuwanie danych osób nieletnich z rejestru następuje co do zasady 10 lat po ukończeniu przez nieletniego osiemnastego roku życia, co oznacza, że dane nieletnich mogą być przechowywane w rejestrze znacząco dłużej niż dane sprawców pełnoletnich, powodując tym samym zaostrzenie represji wobec nieletnich i rezygnację z oddziaływania wychowawczego. W świetle wymogów art. 10 w zw. z art. 6 RODO Prezes UODO wyraził wątpliwości co do zapewnienia odpowiednich gwarancji bezpieczeństwa danych osób nieletnich przetwarzanych w rejestrze publicznym, w tym co do zagwarantowania odpowiedniego nadzoru władz publicznych nad dostępem do rejestru (art. 10 zd. 2 RODO), a także na ryzyka związane z wykorzystaniem danych przetwarzanych w rejestrze w celach innych niż pierwotnie określone. Proces legislacyjny nie został zakończony.

[265] Trybunał Sprawiedliwości UE oraz Europejski Trybunał Praw Człowieka wskazują, że jeżeli chodzi o dane osób fizycznych w przeszukiwalnym i dostępnym publicznie rejestrze, to – z uwagi na możliwość powtórnego wykorzystania tych danych w innych celach – jest on niezgodny z prawem Unii Europejskiej (zob. np. wyrok TSUE z 9 listopada 2010 r., Volker und Markus Schecke i Eifert, w sprawach połączonych C-92/09 i C-93/09 oraz wyrok TSUE z 2 listopada 2022 r. w połączonych sprawach C-37/20 i C-601/20).
[266] Dz.U. 2025 poz. 1844.
[267] DPNT.401.322.2025.

Zagrożeń związanych z dostępem do danych zgromadzonych w wielu rejestrach publicznych dotyczyła opinia Prezesa UODO do **poselskiego projektu ustawy o Karcie Rodziny Mundurowej**[268]. Przewidywał on przetwarzanie danych osobowych na szeroką skalę, w tym również dotyczących zdrowia, za pomocą infrastruktury informatycznej. Projektowane rozwiązania wiązały się z dostępem do wielu rejestrów publicznych i innych niezidentyfikowanych w ustawie zasobów. Dostęp do bliżej nieokreślonych rejestrów publicznych, realizowany przez podmioty publiczne, w tym w sposób automatyczny drogą elektroniczną budził zastrzeżenia organu zarówno z perspektywy norm konstytucyjnych, jak i zasad przetwarzania danych osobowych. Organ zwrócił uwagę, że blankietowy charakter regulacji dotyczących weryfikacji danych o przyznanie Karty stanowi istotną przeszkodę dla wykonawców norm w ustaleniu zasobów informacji, z jakich mogą korzystać. Automatyczne pozyskiwanie danych z rejestrów zasadniczo uniemożliwia administratorowi sprawowanie kontroli nad przetwarzaniem danych, w tym nad zakresem pozyskiwanych danych, gdyż to nie systemy odpowiadają za procesy przetwarzania danych osobowych, ale administratorzy udostępniający i pozyskujący te dane za pomocą tych systemów. Proces legislacyjny nie został zakończony.

Na liczne mankamenty w regulacjach dotyczących funkcjonowania rejestru publicznego wskazano też w opinii do **projektu ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu**[269]. Zawierał on istotne zmiany dotyczące funkcjonowania Centralnego Rejestru Beneficjentów Rzeczywistych (CRBR). Zakładał odejście od pełnej jawności rejestru na skutek wyroku TSUE (sprawy połączone C-37/20 i C-601/20), który uznał pełną jawność CRBR jako nieproporcjonalną ingerencję w prywatność osób fizycznych. W swojej opinii Prezes UODO wskazał, że projektowane przepisy nie określają trybu udostępniania danych oraz ról podmiotów/organów biorących udział w procesach przetwarzania danych osobowych zawartych w CRBR – w odniesieniu do celów przetwarzania. Także cel udostępnienia jest określony w projektowanym przepisie w sposób bardzo ogólny (realizacja ustawowych zadań). Organ nadzorczy zwrócił też uwagę na przetwarzanie numeru PESEL w sytuacjach zawodowych – numer ten nie powinien identyfikować osób w relacjach zawodowych (służbowych) na zasadzie prawnego obowiązku (osoby te mają inne identyfikatory, na podstawie których można je zweryfikować, np. numer wpisu na listę prowadzoną przez organy samorządu zawodowego). Z projektu wynikało również udostępnianie podmiotom i instytucjom obowiązanym informacji z Rejestru, obejmujących numer PESEL albo datę urodzenia. Mając na uwadze zasadę minimalizacji danych, nieuzasadnione jest przetwarzanie numeru PESEL, jeśli wystarczające jest przetwarzanie w tym celu daty urodzenia oraz jeśli identyfikacja jest w pełni możliwa w oparciu o pozostałe dane przetwarzane w Rejestrze. Wątpliwości organu wzbudziły także przepisy dotyczące ewidencji podmiotów, którym organ prowadzący CRBR udostępnił informacje z Rejestru. W projektowanych przepisach nie zostały dookreślone szczegóły prowadzenia tej

[268] DPNT.401.439.2025.
[269] DPNT.401.120.2025.

ewidencji (cel, forma, zasady korzystania z ewidencji przez inne podmioty/organy), co organ nadzorczy uznał za wymagające ponownej analizy i doprecyzowania. Prowadzona ewidencja związana jest z przetwarzaniem danych osobowych, a zatem w ocenie organu ta materia powinna być przejrzyście uregulowana w przepisach prawa, z uwzględnieniem zasad określonych w art. 5 ogólnego rozporządzenia o ochronie danych. Projektowane przepisy powinny wskazywać formę prowadzenia ewidencji, tryb ewentualnego przekazywania/udostępniania danych z ewidencji czy okres przechowywania w niej danych osobowych. Proces legislacyjny nie został zakończony.

**Projekt rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie systemów teleinformatycznych stosowanych w publicznych służbach zatrudnienia**[270] został skierowany do zaopiniowania przez organ nadzorczy na etapie Komitetu do spraw Cyfryzacji. Organ nadzorczy wskazał na konieczność przeprowadzenia przez projektodawcę oceny skutków dla ochrony danych. Rekomendował przyjęcie takich rozwiązań, które nie będą powodowały konieczności przekazywania danych osobowych pomiędzy ministrem właściwym do spraw pracy a producentem. Rozporządzenie zostało podpisane i opublikowane[271].

Głównym celem **projektu ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw**[272] było rozszerzenie możliwości doręczania pism procesowych w postępowaniach karnych i wykroczeniowych za pośrednictwem portalu informacyjnego. Prezes UODO zwrócił uwagę na konieczność dostosowania przepisów nowelizowanych aktów prawnych do dyrektywy 2016/680 – poprzez nowelizację ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jak i wprowadzenie w Kodeksie postępowania karnego, ustawie Prawo o prokuraturze oraz Kodeksie postępowania w sprawach o wykroczenia – rozwiązań uszczegóławiających procesy przetwarzania danych osobowych, a także gwarantujących poufność i integralność tym danym, w tym także dla wykonywania procedury zamieszczania pism procesowych na portalu informacyjnym. Uwagi organu nadzorczego nie zostały uwzględnione. Ustawa została uchwalona i podpisana przez Prezydenta RP[273].

**Projekt ustawy o zmianie ustawy o podatku od towarów i usług oraz zmieniającej ustawę o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw**[274] dotyczył m.in. zmiany modelu przetwarzania danych osób fizycznych – nabywców towarów i usług (będących konsumentami), których dane zawarte w fakturach mają być pozyskiwane do Krajowego Systemu e-Faktur (dalej: KSeF). Organ nadzorczy wskazał na: potrzebę objęcia projektu testem prywatności; ryzyka wykorzystywania zamieszczonych w fakturach informacji stanowiących dane osobowe do profilowania. Zakwestionował także przepisy dotyczące przekazywania

[270] DPNT.401.527.2025.
[271] Dz.U. z 2026 r. poz. 842.
[272] DPNT.401.2.2025.
[273] Dz.U. z 2025 r. poz. 1178.
[274] DPNT.401.178.2025.

faktur z danymi osobowymi konsumentów do Krajowego Systemie e-Faktur, wskazując, że projektowane rozwiązania pomijają obowiązek zapewnienia stosowania w regulacji krajowej przestrzegania i gwarancji ochrony praw i wolności osób, których dane dotyczą. Poza realizacją celów fiskalnych nie uzasadniono w projekcie, dlaczego pozyskanie przez organy państwa ogromnej ilości danych osób fizycznych jest niezbędne i proporcjonalne. Projektowane rozwiązanie nie odpowiadały w pełni wynikającym z RODO zasadom: zgodności z prawem, rzetelności i przejrzystości, minimalizacji danych, ograniczenia celu, a w konsekwencji zasadzie rozliczalności. Projektowana ustawa weszła w życie[275]. Projektodawca nie uwzględnił uwag Prezesa UODO. Ustawa została uchwalona i podpisana przez Prezydenta[276].

Projekt **ustawy o zmianie niektórych ustaw w związku z poprawą bezpieczeństwa ruchu drogowego**[277] wprowadzał zmianę w publicznym rejestrze administracyjnym – centralnej ewidencji pojazdów (CEP) – prowadzonym w systemie teleinformatycznym polegającą – w ocenie Prezesa UODO – na: a) nieuzasadnionej zmianie celu prowadzenia tego rejestru; b) niezasadnym rozszerzeniu zakresu danych gromadzonych w „zreformowanym" CEP (zamieszczanie w CEP informacji o wykorzystaniu pojazdu do popełnienia przestępstwa), a dokonany w nim wpis miał być skuteczny wobec każdoczesnego posiadacza takiego pojazdu i nie miał być usuwany, nawet po zatarciu skazania albo ukarania. Projekt nakładał na osobę przystępującą do egzaminu państwowego na prawo jazdy obowiązek składania oświadczenia pod rygorem odpowiedzialności karnej, że nie toczy się wobec niej postępowanie karne o przestępstwo pozostające w związku z bezpieczeństwem ruchu drogowego, przy braku przepisu prawa materialnego przewidującego wymaganie, by wobec osoby przystępującej do egzaminu państwowego na prawo jazdy nie toczyło się postępowanie karne o przestępstwo pozostające w związku z bezpieczeństwem ruchu drogowego (ustawa o kierujących pojazdami zakazuje jedynie przystępowania do egzaminu państwowego na prawo jazdy osobie, która ma „aktywny" zakaz prowadzenia pojazdów). W sprawie tej Prezes UODO odniósł sukces legislacyjny – projektodawca usunął z projektu ww. wadliwe unormowania. Ustawa została uchwalona i podpisana przez Prezydenta RP[278].

Opiniując **projekt ustawy o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw**[279] Prezes UODO zanegował nową procedurę udostępniania podmiotom publicznym oraz podmiotom niebędącym podmiotami publicznymi, ale realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji, informacji z Krajowego Rejestru Sądowego za pośrednictwem usług sieciowych. Wskazał, że w świetle projektowanych przepisów Minister Sprawiedliwości jedynie może, a nie jest prawnie zobligowany, by żądać od ww. podmiotów szczegółowego

[275] https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=1407.
[276] Dz.U. z 2025 r. poz. 1203.
[277] DPNT.401.33.2025.
[278] Dz.U. z 2025 r. poz. 1872.
[279] DPNT.401.373.2025.

wykazania, że spełniają one – określone w nowelizowanej ustawie o KRS – przesłanki udostępnienia im danych z tego rejestru za pośrednictwem usług sieciowych. Rodziło to zasadnicze pytanie, na czym (na jakich i jak pozyskanych ustaleniach faktycznych) Minister Sprawiedliwości (administrator) zamierza oprzeć wydawaną decyzję administracyjną o zgodzie na udostępnianie danych z Krajowego Rejestru Sądowego za pośrednictwem usług sieciowych. Uwagi Prezesa UODO nie zostały jednak uwzględnione – ustawa z dnia 26 września 2025 r. o zmianie ustawy o Krajowym Rejestrze Sądowym oraz niektórych innych ustaw[280] została uchwalona w niezmienionym kształcie i podpisana przez Prezydenta RP[281].

### 15.5. Role podmiotów w procesach przetwarzania danych osobowych

W wielu opiniach legislacyjnych organ nadzorczy zwracał uwagę na kwestię prawidłowego określenia ról podmiotów biorących udział w procesach przetwarzania danych osobowych, w szczególności na rolę administratora[282]. Nadal zauważalną tendencją jest jej wyznaczanie poprzez samo wskazanie w regulacji określonego podmiotu jako administratora, co nie jest wystarczające i może stanowić jedynie wskazówkę. Rola ta przede wszystkim powinna wynikać z charakteru kompetencji lub zakresu zadań, jakie normy prawne mu przypisują. W przypadku tworzenia regulacji prawnych formułujących podstawy procesów przetwarzania najważniejsze jest precyzyjne określenie zakresu kompetencji oraz ról poszczególnych podmiotów, zwłaszcza gdy w procesach przetwarzania uczestniczy wielu współadministratorów lub podmiotów przetwarzających. Punktem wyjścia dla prawidłowego określenia ról podmiotów uczestniczących w procesach przetwarzania danych osobowych jest również odniesienie do szczegółowo określonych celów przetwarzania, operacji (zestawów operacji) przetwarzania danych osobowych. Rola administratora ma kluczowe znaczenie dla rozstrzygnięcia, który podmiot stanie się odpowiedzialny zarówno za realizację zasad ochrony danych osobowych, zwłaszcza zasady rozliczalności, jak i za wykonywanie praw osób, których dane dotyczą, czy też zgłaszanie naruszeń.

**Projekt ustawy o koordynacji działań antykorupcyjnych oraz likwidacji Centralnego Biura Antykorupcyjnego**[283] zakładał przede wszystkim usprawnienie i wzmocnienie koordynacji działań antykorupcyjnych prowadzonych obecnie przez różne służby państwowe. Projektodawca nie zapewnił jednak w projektowanych regulacjach wystarczającej przejrzystości przetwarzania danych osobowych przez podmiot wykonujący obowiązki administratora w odniesieniu do przetwarzanych informacji. W tym konkretnym przypadku organ nadzorczy poddał pod rozwagę określenie wprost w przepisach prawa roli pełnionej przez nowo powstały organ jako administratora. Takie jednoznaczne przesądzenie jego statusu zapewniłoby zgodność projektu z przyjętymi w dyrektywie 2016/680 oraz rozporządzeniu 2016/679 zasadami

[280] Dz. U. poz. 1556.
[281] Dz.U. z 2025 r. poz. 1556.
[282] Wytyczne Europejskiej Rady Ochrony Danych nr 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO.
[283] DPNT.401.458.2025.

przetwarzania danych osobowych oraz mogłoby zapobiec przyszłym praktycznym trudnościom w stosowaniu przepisów zmienianej ustawy o Policji. Przejrzyste określenie roli nowo powstałego organu Policji w procesie przetwarzania danych i związanej z tym odpowiedzialności za przetwarzanie danych osobowych jest niezwykle ważne z perspektywy zapewnienia osobom, których dane dotyczą, jak najwyższych gwarancji ochrony tych danych. Organ zalecił też przeprowadzenie oceny skutków dla ochrony danych, by projektowane zmiany w obowiązującym porządku prawnym nastąpiły z uwzględnieniem zasad przetwarzania danych osobowych i obowiązków administratora danych wynikających z rozporządzenia 2016/679 oraz dyrektywy 2016/680. Proces legislacyjny nie został zakończony.

Organ nadzorczy w opinii dotyczącej **projektu ustawy o zmianie ustawy o finansach publicznych oraz niektórych innych ustaw**[284] zwrócił uwagę na zbędne bezpośrednie wskazywanie administratora, a jednocześnie czynienie tego w sposób niewyczerpujący, bez dokonania analizy ról poszczególnych organów/podmiotów w procesach przetwarzania danych – w celu ustalenia czy minister finansów będzie jedynym administratorem czy zadania innych organów związane z przetwarzaniem danych będą determinować ich status jako kolejnych administratorów/ współadministratorów, co powinno znaleźć swoje odzwierciedlenie także w ocenie skutków projektowanej ustawy dla ochrony danych. Wskazał również, że role i obowiązki podmiotów biorących udział w procesach przetwarzania danych powinny być precyzyjnie określone w projektowanych przepisach, także do szczegółowo określanych celów przetwarzania, operacji przetwarzania podmiotów pozyskujących dane z systemu teleinformatycznego oraz zasilających system danymi osobowymi. Zwrócił przy tym uwagę na wyrok TSUE z 11 stycznia 2024 r. w sprawie C-231/22 Etat belge, w którym uznano, że podmiot publiczny publikujący dokumenty urzędowe ponosi odpowiedzialność również za treść publikowanych danych (a nie tylko za udostępnienie narzędzia teleinformatycznego i odpowiada za publikowane treści). Ustawa została uchwalona i podpisana przez Prezydenta RP[285].

Podobne zastrzeżenia dotyczyły **poselskiego projektu ustawy o zmianie ustawy o ochotniczych strażach pożarnych**[286]. Prezes UODO zwrócił uwagę na nieprecyzyjne przepisy dotyczące „powierzenia funkcji administratora", która wynika z charakteru, kompetencji lub też zakresu zadań publicznych, jakie przepisy te mu przypisują. Ustawa została uchwalona i podpisana przez Prezydenta RP[287].

**Poselski projekt ustawy o asystencji osobistej osób z niepełnosprawnościami**[288] przewidywał stworzenie systemowych ram dla asystencji osobistej osób z niepełnosprawnościami. Działania służące: ustaleniu prawa do asystencji osobistej oraz jej realizacja miały odbywać się drogą elektroniczną w systemach teleinformatycznych utworzonych przez Zakład Ubezpieczeń

[284] DPNT.401.149.2025.
[285] Dz.U. z 2026 r. poz. 635.
[286] DPNT.401.108.2025.
[287] Dz.U. z 2025 r. poz. 900.
[288] DPNT.401.441.2025.

Społecznych (ZUS) do obsługi realizacji prawa do asystencji osobistej oraz przez ministra właściwego do spraw zabezpieczenia społecznego do ustalania prawa do asystencji osobistej. W ramach pierwszego z tych systemów w szczególności prowadzone miały być Rejestr realizatorów [asystencji osobistej] i Rejestr asystentów. Projekt ustawy wskazywał wojewodę jako administratora danych osobowych objętych rejestrem w systemie prowadzonym przez ZUS. Organ zwrócił uwagę, że takie wskazanie administratora jest niezrozumiałe, ponieważ faktyczna realizacja tych zadań leży po stronie ZUS jako podmiotu tworzącego i rozbudowującego system teleinformatyczny. Brak jasno określonych ról ww. podmiotów w przetwarzaniu danych prowadzi do nieokreślonego zakresu ich odpowiedzialności za naruszenie ochrony danych osobowych. Sejmowy proces legislacyjny trwa.

Opiniując **projekt rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy**[289], organ nadzorczy zaproponował utworzenie nowej grupy zawodów o nazwie „Specjaliści do spraw danych" oraz przeniesienie do niej **zawodu „inspektor ochrony danych"** oraz usunięcie go z dotychczasowych grup. Aktualne regulacje (rozporządzenie 2016/679 oraz dyrektywa 2016/680) wprowadziły istotne zmiany w zakresie statusu i zadań inspektora ochrony danych w porównaniu z administratorem bezpieczeństwa informacji[290]. Przepisy te statuują inspektora jako niezależnego specjalistę z dziedziny ochrony danych osobowych stojącego na straży przestrzegania przepisów z tego zakresu oraz praw i wolności jednostki w związku z przetwarzaniem jej danych osobowych. Do zadań inspektorów należy wspieranie podmiotów publicznych i prywatnych poprzez monitorowanie ich działalności pod względem zgodności z prawem oraz fachowe doradzanie tym podmiotom w zakresie prawa i praktyk w dziedzinie ochrony danych. Do zadań inspektora ochrony danych – z uwagi na jego niezależność – nie mogą należeć natomiast działania (dotychczasowej grupy) o charakterze zarządczym (tj. związane z decydowaniem o celach i sposobach przetwarzania danych osobowych) oraz polegające na wykonywaniu jakichkolwiek obowiązków organizacji wchodzących z zakres oceny (monitorowania) przez inspektora. Uwagi organu zostały uwzględnione, rozporządzenie w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy weszło w życie[291].

### 15.6. Zasady przetwarzania danych osobowych, dane szczególnych kategorii, PESEL

Problemem stale pojawiającym się przy opiniowaniu przez Prezesa UODO projektów aktów prawnych było nieuwzględnianie przez projektodawcę krajowego zasad wyrażonych w art. 5 RODO, a stanowiących ogólne ramy zgodnego z prawem przetwarzania danych osobowych. Tymczasem ich respektowanie już na etapie prac nad projektem aktu normatywnego sprzyja zapewnieniu odpowiedniego, zgodnego ze

[289] DPNT.401.275.2025.
[290] Funkcja pełniona na gruncie ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (nieobowiązująca).
[291] (Dz. U. poz. 1534).

standardami RODO, poziomu przetwarzania danych osobowych przez podmioty stosujące przyjęte przepisy. Jest to szczególnie istotne w przypadku przetwarzania danych szczególnych kategorii, o których mowa w art. 9 ust. 1 RODO. Prawodawca unijny uznał je za szczególnie wrażliwe w świetle podstawowych praw i wolności, czyli wymagające szczególnej ochrony (zob. motyw 51 RODO). Odpowiednie wdrożenie tych zasad przez prawodawcę pomaga wykonawcom norm w zapewnieniu odpowiedniego poziomu ochrony danych osobowych.

Niestety wciąż utrzymującą się tendencją jest niedostateczne uwzględnienie przez projektodawców zasad przetwarzania z art. 5 RODO. Przejawia się to na przykład poprzez ustanawianie w projektowanych przepisach otwartych katalogów przetwarzanych danych osobowych, co jest rozwiązaniem niedopuszczalnym z punktu widzenia zasady minimalizacji (art. 5 ust. 1 lit. c RODO), a także poprzez nieprecyzyjne określenie celu (celów) przetwarzania, co jest problematyczne ze względu na zasadę ograniczenia celu (art. 5 ust. 1 lit. b RODO), ale i – w odniesieniu do podmiotów publicznych, które muszą działać na podstawie i w granicach prawa – konstytucyjną zasadę praworządności.

Właściwe wdrożenie w projektowanych przepisach zasad przetwarzania danych osobowych z art. 5 RODO było tym bardziej istotne w przypadku regulacji odnoszących się do przetwarzania danych osobowych małoletnich oraz seniorów. Kwestia ochrony ich praw jest szczególnie bliska Prezesowi UODO, który w swojej działalności wielokrotnie podnosił kwestie dotyczące zabezpieczenia praw tych grup, nie tylko w kontekście prawa do ochrony danych osobowych.

Częstym problemem było również ustanawianie w projektowanych regulacjach obowiązku przetwarzania numeru PESEL, również wtedy, gdy jego przetwarzanie nie wydaje się niezbędne do osiągnięcia zamierzonego celu. Ma to znaczenie nie tylko z punktu widzenia zasad z art. 5 (w szczególności zasady minimalizacji) ale też innej regulacji RODO, tj. art. 87, zgodnie z którym krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym (w Polsce jest nim numer PESEL) używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą.

Dla zilustrowania opisywanych problemów wskazać można opinie Prezesa UODO wyrażone w poniższych sprawach.

Wkład do **projektu stanowiska RP dotyczącego projektu rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego wspólny system powrotów obywateli państw trzecich nielegalnie przebywających w Unii oraz uchylającego dyrektywę Parlamentu Europejskiego i Rady 2008/115/WE, dyrektywę Rady 2001/40/WE i decyzję Rady 2004/191/WE COM(2025) 101**[292] dotyczył realizacji – na podstawie prawa UE – wymiany informacji, w tym wymiany danych dotyczących tożsamości, obywatelstwa obywateli państw trzecich, dokumentów podróży, przetwarzania danych szczególnej kategorii, w tym danych biometrycznych oraz wyroków skazujących. Jednym z założeń projektu było ujednolicenie krajowych systemów i praktyk, w obszarze systematycznego, ustrukturyzowanego procesu

[292] DPNT.401.148.2025.

identyfikacji i przyspieszenia powrotu obywateli państw trzecich stwarzających zagrożenie dla bezpieczeństwa. Prezes UODO zgłaszał uwagi co do braku zapewnienia w projekcie gwarancji ochrony praw podstawowych, w tym w zakresie ciążącego na administratorze obowiązku informacyjnego na gruncie art. 13 i 14 RODO w związku z przetwarzaniem danych oraz praw przysługujących osobie, której dane dotyczą: dostępu do danych, sprostowania danych (art. 16), usunięcia danych (art. 17) oraz prawa do ograniczenia przetwarzania (art. 18 RODO). Projekt został zatwierdzony przez Parlament Europejski, jednak unijny proces legislacyjny nie został zakończony.

**Projekt ustawy o zmianie ustawy o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych oraz niektórych innych ustaw**[293] zawierał rozwiązania wiążące się z przetwarzaniem szczególnych kategorii danych dotyczących zdrowia oraz danych poddanych pseudonimizacji, a w przypadku gdy nie jest to możliwe przetwarzanie identyfikatora usługobiorcy (numer PESEL) w systemie, a także przetwarzanie danych w sposób umożliwiający łączenie informacji z różnych bliżej nieokreślonych systemów w trybie bezwnioskowym. Pozyskiwanie przez organ publiczny danych z innych zbiorów danych powinno odbywać się z poszanowaniem zasad i gwarancji wynikających z ogólnego rozporządzenia o ochronie danych. Łączenie informacji i danych z różnych systemów nie powinno prowadzić do łączenia całych zasobów znajdujących się w systemach publicznych. Wdrażanie tego rodzaju rozwiązań powinno szczegółowo określać: procedurę, formę, zakres i tryb dostępu do danych osobowych. Organ nadzorczy pozytywnie natomiast przyjął uchylenie w ustawie przepisu dającego podstawę identyfikacji osoby odbierającej wyrób medyczny za pomocą numeru PESEL, a w przypadku jego braku, za pomocą serii i numeru paszportu albo numeru innego dokumentu stwierdzającego tożsamość. Proces legislacyjny dotyczący projektu nie został zakończony[294].

**Poselski projekt ustawy o klubach seniora**[295] zakładał powstanie nowego, co do zasady jawnego rejestru tj. Krajowego Rejestru Klubów Seniora. Wątpliwości Prezesa UODO wzbudziły: przepisy dotyczące jawności i powszechnej dostępności do danych z rejestru; nieprecyzyjne określenie katalogu przetwarzanych danych; brak wskazania formy rejestru – w szczególności, czy będzie on prowadzony w systemie teleinformatycznym. Za konieczne uznał również określenie celów przetwarzania danych osobowych oraz okresu przechowywania danych w Rejestrze. Zwracając uwagę na powyższe wymagające dopracowania elementy regulacji, organ nadzorczy z uznaniem przyjął ją jako kierunkowo zbieżną z jego aktywnością w zakresie wspierania seniorów w realizacji przysługujących im praw. Proces legislacyjny nie został zakończony.

[293] DPNT.401.181.2025.
[294] https://legislacja.gov.pl/projekt/12398102.
[295] DPNT.401.480.2025.

Prezes UODO przedstawił również uwagi do **projektu ustawy o zmianie ustawy o Krajowej Sieci Onkologicznej oraz niektórych innych ustaw**[296], który przewidywał zmiany w zakresie dostępu do danych osobowych lub jednostkowych danych medycznych usługobiorców, przetwarzanych w systemie teleinformatycznym usługodawcy lub w Systemie Informacji Medycznej (zawierających karty diagnostyki i leczenia onkologicznego w postaci elektronicznej). Wątpliwości Prezesa UODO wzbudziło udostępnianie przetwarzanych w systemach danych szerokiemu kręgowi osób, w tym spoza personelu medycznego, a także przetwarzanie danych w nieokreślonych, ogólnych celach. Zwrócił więc uwagę, że wprowadzanie szerokiego dostępu do danych wiąże się z ryzykami, które powinny być zidentyfikowane i zminimalizowane mocą regulacji. Ograniczeniu tych ryzyk służy zapewnienie rozliczalności dostępu do systemu oraz dodatkowe mechanizmy kontroli celów pozyskiwania danych. Projekt przewidywał także monitorowanie przez Narodowy Fundusz Zdrowia jakości opieki onkologicznej w ramach Krajowej Sieci Onkologicznej. Przyznanie nowych uprawnień Narodowemu Funduszowi Zdrowia w postaci „monitorowania jakości opieki onkologicznej" i ich realizacja powiązana bezpośrednio z przetwarzaniem danych osobowych – w postaci „nieprzetworzonych danych osobowych" – budziło wątpliwości, gdyż godziło w zasady dotyczące przetwarzania danych osobowych: zasadę zgodności z prawem, ograniczonego celu i minimalizacji danych, a także konstytucyjną zasadę proporcjonalności. Ustawa została uchwalona i podpisana przez Prezydenta RP[297].

Celem **projektu ustawy o zmianie ustawy – Ordynacja podatkowa oraz niektórych innych ustaw**[298] była poprawa relacji między podatnikami i organami podatkowymi, a także zwiększenie efektywności działania organów podatkowych. Organ nadzorczy wskazał na potrzebę objęcia projektu testem prywatności. Zakwestionował rozwiązania dotyczące przetwarzania danych osobowych w informacjach o schematach podatkowych. Akceptacji zyskać nie mogły: brak szczegółowych rozwiązań w zakresie technicznych i organizacyjnych aspektów przechowywania, przekazywania do organów podatkowych oraz usuwania przez promotorów danych osobowych osób fizycznych, które są ujawniane w schematach podatkowych. Kolejnym kwestionowanym rozwiązaniem były nie w pełni odpowiadające zasadom przetwarzania danych osobowych przepisy dotyczące przesłuchania strony lub świadka przez organ podatkowy na odległość z wykorzystaniem urządzeń technicznych rejestrujących dźwięk albo obraz. Poważne zastrzeżenia organ nadzorczy zgłaszał także do planowanego w projekcie rozszerzenia dostępu do danych osobowych przetwarzanych przez organy skarbowe, w tym danych objętych tajemnicą skarbową. Projektowane w tym zakresie przepisy wiązały się bowiem ze zmianą celów dotychczasowego przetwarzania danych osobowych. Organ nadzorczy zauważył, że nie wszystkie rozwiązania dotyczące udostępniania danych osobowych podatników spełniały kryteria gwarancji

[296] DPNT.401.443.2025.
[297] Dz.U. z 2026 r. poz. 1007.
[298] DPNT.401.110.2025.

niezbędności i proporcjonalności co do zmiany pierwotnego celu przetwarzania. Projektodawca uwzględnił część uwag Prezesa UODO. Ustawa została uchwalona i podpisana przez Prezydenta RP[299].

Rządowe prace legislacyjne nad **projektem ustawy o zmianie ustawy o sporcie oraz niektórych innych ustaw**[300] – których celem było rozszerzenie zakresu pozyskiwania, przekazywania, gromadzenia, jak również pośrednio udostępniania danych zawartych w ewidencji „Sportowe talenty" o dane uczniów objętych edukacją wczesnoszkolną – stanowiły dobrą okazję do przedstawienia projektodawcy licznych wątpliwości organu nadzorczego w zakresie proporcjonalności i celowości obowiązujących rozwiązań dotyczących gromadzenia i udostępniania danych zawartych w tej ewidencji z perspektywy konstytucyjnych i unijnych standardów ochrony danych osobowych.

Zidentyfikowane braki projektu to: nieokreślony, niekonkretny, nieprzejrzysty i prawnie nieuzasadniony cel przetwarzania danych osobowych (imię, nazwisko, numer PESEL) w ewidencji; brak podstaw dla obowiązku przetwarzania w ewidencji danych szczególnej kategorii, tj. informacji o masie i wzroście ucznia, powiązanych z informacją o uzyskanych przez niego wynikach z testów sprawnościowych. W ocenie Prezesa UODO nie było uzasadnienia, by przetwarzane (obowiązkowo) przez państwo dane uczniów mogły służyć podmiotom spoza systemu oświaty (klubom, związkom sportowym), tzn. aby były im przekazywane informacje o uczniu zgromadzone w publicznej bazie danych. Zwrócono również uwagę na nadmierny planowany okres retencji danych gromadzonych w ewidencji – powinien zostać skrócony, maksymalnie do dnia zakończenia przez ucznia nauki w szkole, w której uzyskał wynik z testów sprawnościowych. Projektodawca, tworząc ewidencję „Sportowe talenty", nie zdecydował się na przeprowadzenie testu prywatności. Pozytywną konsekwencją przedstawionych uwag organu nadzorczego było zrezygnowanie projektodawcy z wprowadzenia w ustawie o sporcie planowanych zmian – zadeklarował on weryfikację obowiązujących przepisów w zakresie prowadzenia ewidencji „Sportowe talenty" tak, by określone nimi przetwarzanie danych osobowych zostało zaprojektowane na podstawie przeprowadzonego testu prywatności, co stanowi sukces legislacyjny. Ustawa została uchwalona i podpisana przez Prezydenta RP[301].

**Obywatelski projekt ustawy o ochronie małoletnich przed treściami pornograficznymi w Internecie oraz o zmianie ustawy – Prawo telekomunikacyjne**[302] w założeniu dotyczy tożsamej materii i ma rozwiązywać ten sam problem, co wyżej wspomniany rządowy projekt ustawy o ochronie małoletnich przed treściami pornograficznymi w internecie. Zgodnie z projektem dostawcy tego typu treści mieliby obowiązek stosowania skutecznej weryfikacji wieku użytkownika, aby uniemożliwić dostęp do nich osobom niepełnoletnim. Prezes UODO dostrzega

[299] Dz.U. z 2026 r. poz. 846.
[300] DPNT.401.425.2025; omówienie i opinia dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3948.
[301] Dz.U. z 2026 r. poz. 615.
[302] DPNT.401.13.2025.

konieczność rozwiązania problemu przedstawionego przez autorów projektu i uznał kierunek proponowanych regulacji za jednoznacznie słuszny. Jednocześnie wskazał jednak, że aby projektowane przepisy skutecznie spełniały założony przez projektodawcę cel, jakim jest ochrona dobrostanu małoletnich, regulacje te powinny być przejrzyste oraz w sposób jasny i precyzyjny określać obowiązki określonych podmiotów związane z weryfikacją wieku (w tym również w zakresie przetwarzania przez te podmioty danych osobowych). Projekt ustawy nie określał bowiem, na czym ma polegać weryfikacja wieku ani jakie kryteria ma ona spełniać. Prezes UODO zwrócił uwagę na konieczność przejrzystego i rzetelnego oraz wyczerpującego uregulowania w projekcie aspektów przetwarzania danych osobowych, w tym w systemach weryfikacji wieku, w celu zabezpieczenia praw i wolności osób, których dane dotyczą. Powyższe pozwoli zapewnić zgodność projektu z zasadami wyrażonymi w art. 5 RODO, zwłaszcza z zasadami zgodności z prawem, rzetelności i przejrzystości oraz zasadą rozliczalności, zapewniając realizację celu projektu. Projekt został odrzucony w całości na komisji sejmowej.

**Projekt ustawy o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz niektórych innych ustaw**[303] zawierał przepisy dotyczące m.in. zmiany zakresu przetwarzanych danych osobowych obywateli Ukrainy, a także przekazywania ich innym organom do celów innych niż te, w których pierwotnie je zebrano, oraz usuwania tych danych. Statuował także nowe uprawnienia organów publicznych do pozyskiwania danych osobowych osób fizycznych, w tym danych dotyczących stanu zdrowa i danych biometrycznych. Organ nadzorczy wskazał na potrzebę objęcia projektu testem prywatności oraz zmiany projektowanych przepisów w zakresie stanowienia mechanizmów identyfikacji biometrycznej w obszarze wizerunku osoby poprzez dodanie rozwiązań uściślających procedurę udostępniania między organami fotografii twarzy obywateli Ukrainy. Organ nadzorczy postulował także rozbudowanie projektowanych przepisów o odpowiednie do regulacji gwarancje, określające sposób przetwarzania danych osobowych przez wojewodę dla realizacji procedury wykwaterowania obywateli Ukrainy, a także zakres danych osobowych przetwarzanych w tej procedurze. W związku z likwidacją portalu „Praca w Polsce" organ nadzorczy wniósł także o to, by przepisy wprost określały retencję/usuwanie danych osobowych zgromadzonych w likwidowanym portalu. Projektodawca częściowo uwzględnił uwagi Prezesa UODO. Ustawa została zawetowana przez Prezydenta RP.

Stale powracającym tematem w projektach aktów prawnych opiniowanych przez Prezesa UODO jest statystyka publiczna. Projekt **rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie programu badań statystycznych statystyki publicznej na rok 2025**[304] oraz **projekt rozporządzenia Rady Ministrów w sprawie programu badań statystycznych statystyki publicznej na rok 2026**[305] przewidywały, by na potrzeby badania statystycznego dotyczącego zgonów jako

[303] DPNT.401.234.2025.
[304] DPNT.401.92.2025.
[305] DPNT.401.135.2025.

źródło danych wykorzystać system informacyjny Ministerstwa Cyfryzacji będący obszernym zbiorem danych osobowych osób żyjących. Zaproponowane przez GUS rozwiązanie budziło wątpliwości z punktu widzenia zasad: legalizmu, rzetelności i przejrzystości oraz minimalizacji danych. Organ nadzorczy wskazywał też, że skoro GUS na potrzeby badania dotyczącego zgonów może pozyskać interesujące go dane z innego systemu informacyjnego Ministerstwa Cyfryzacji, to nie zachodzi niezbędność pozyskiwania ich z bazy osób żyjących. W sprawie tej Prezes UODO odnotował sukces legislacyjny – Główny Urząd Statystyczny odstąpił od wykorzystywania danych osób żyjących na potrzeby badania statystycznego odnoszącego się do osób zmarłych i wprowadził stosowne zmiany w obu ww. projektach. Oba rozporządzenia zostały podpisane i obowiązują[306].

### 15.7. Postęp technologiczny a ochrona danych

Dynamiczny rozwój technologii cyfrowych, w tym sztucznej inteligencji i automatyzacji procesów, stwarza wiele szans dla zrównoważonego rozwoju państwa i jego obywateli, ale wiąże się także z istotnymi zagrożeniami dla praw jednostki, w tym prawa do prywatności i autonomii informacyjnej. Wprowadzane rozwiązania prawne związane z nowymi technologiami powinny więc być konstruowane tak, aby zapewniać poszanowanie praw podstawowych jednostki. Na te aspekty Prezes UODO zwracał uwagę w wielu opiniach legislacyjnych.

Jednym z przykładów jest **Memorandum z 18 marca 2025 r. przygotowane przez podsekcję Grupy Roboczej ds. Sztucznej Inteligencji (GRAI) przy Ministrze Cyfryzacji**[307], którego przedmiotem jest „przedstawienie ram i warunków prawnych, jakie powinny być spełnione, aby ograniczyć stosowanie RODO". Organ nadzorczy zwrócił uwagę, że tak sformułowany cel dokumentu wskazuje, że założeniem była „liberalizacja" stosowania RODO w zakresie właściwości poszczególnych, wskazanych w dokumencie sektorów. Tymczasem nie ma możliwości „ograniczenia stosowania RODO". Możliwe jest ograniczenie zakresu obowiązków i praw pod ściśle określonymi warunkami, o których mowa w art. 23 RODO. Ewentualne ograniczenia stosowania RODO – ale nie jego wyłączenie – mogą następować w dość szerokim, ale nie w pełnym zakresie oraz tylko wtedy, gdy spełnione zostaną cele oraz warunki sprecyzowane w art. 23 RODO.

Omówienie wymagań z art. 23 RODO w dokumencie nie zostało dokonane przez pryzmat równolegle obowiązującego aktu w sprawie sztucznej inteligencji – nie została dokonana analiza dopuszczalności ewentualnego ograniczenia praw osób, których dane dotyczą, oraz obowiązków administratorów w oparciu o prawa i obowiązki wynikające z tego rozporządzenia, zwłaszcza jeśli chodzi o kwestie przejrzystości systemów sztucznej inteligencji wysokiego ryzyka.

Odnosząc się do zmian sektorowych zaproponowanych w Memorandum, organ nadzorczy zaznaczył, że – ze względu na stosowanie technologii, sposób, zakres

[306] Dz.U. 2025 poz. 1842 oraz Dz.U. 2026 poz. 54.
[307] DPNT.401.305.2025.

i charakter przetwarzanych danych – niezwykle istotne jest, aby projektodawca wziął pod uwagę, że projektowane przepisy powinny przewidywać rozwiązania adekwatne do celów, konieczne i jedynie niezbędne dla realizacji *ratio legis*, a także zapewniać właściwe gwarancje ochrony danych osobowych dla podmiotów danych. Realizacja celów Memorandum, ale i zapewnienia stosowania aktu w sprawie sztucznej inteligencji wymaga przeglądu obowiązującego stanu prawnego – prawodawstwa krajowego pod kątem zapewnienia stosowania AI Act.

Organ nadzorczy przedstawił wątpliwości w odniesieniu do zaproponowanych zmian w Prawie o szkolnictwie wyższym i nauce, tj. odnośnie do wyraźnego dopuszczenia przetwarzania danych osobowych w ramach projektów badawczych AI prowadzonych przez uczelnie i instytuty, poprzez zakwalifikowanie ich jako przetwarzanie w ważnym interesie publicznym. O tym, czy przetwarzanie było realizowane w ważnym interesie publicznym powinny decydować przesłanki wskazujące i uzasadniające ważny interes publiczny, a nie sam fakt chęci użycia AI do rozwiązania określonego problemu.

Zalecono przegląd regulacji dotyczących przetwarzania danych osobowych (w tym szczególnej kategorii) do celów badań naukowych w obowiązujących regulacjach, np. w ww. ustawie o szkolnictwie wyższym i nauce czy ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta.

Szereg wątpliwości wzbudziła również propozycja zmian Prawa bankowego polegająca na umożliwieniu testowania algorytmów AI na prawdziwych danych klientów w ramach piaskownicy lub programu pilotażowego, za zgodą regulatora i przy anonimizacji wyników.

W uwagach do **projektu uchwały Rady Ministrów w sprawie przyjęcia strategii dotyczącej informatyzacji państwa zwanej „Strategią Cyfryzacji Państwa do 2035 r.”**[308] Prezes UODO podkreślił potrzebę pogłębionej refleksji nad uwzględnieniem ochrony praw podstawowych w projektowanym procesie rozwoju cyfrowego Polski. Zarówno horyzontalny proces transformacji cyfrowej, jak i planowany rozwój cyfrowy w trzech obszarach (państwo, ludzie oraz gospodarka i technologie) wymagają zaprojektowania rozwiązań gwarantujących ochronę danych osobowych.

Dla realizacji poszczególnych działań strategii informatyzacji państwa niezbędne było dokonanie przeglądu i zidentyfikowanie obszarów wymagających zmian legislacyjnych, a także określenie podstaw prawnych. Jest to szczególnie istotne w odniesieniu do: planowanego rozwoju cyfrowych usług publicznych, centralizacji usług administracyjnych, zwiększenia interoperacyjności publicznych systemów teleinformatycznych i rejestrów publicznych czy wdrożenia sztucznej inteligencji oraz automatyzacji procesów przy realizacji e-usług publicznych.

Istotne było również zagwarantowanie w projektowanych aktach prawnych oraz tworzonych rozwiązaniach dla wszystkich nowych i rozwijanych usług cyfrowych standardów przetwarzania i ochrony danych osobowych służących ochronie praw

[308] DPNT.401.462.2025.

i wolności osób, których dane osobowe będą przetwarzane, w oparciu o przeprowadzoną w ramach oceny skutków regulacji ocenę skutków dla ochrony danych zgodnie z art. 35 RODO.

Projektodawca odniósł się do uwag organu ochrony danych. Poinformował, że szczegółowe aspekty związane z wdrożeniem strategii informatyzacji państwa zostaną ujęte w planie operacyjnym lub bezpośrednio w nowelizowanych aktach prawnych. Zadeklarował, że tworzenie spójnych ram prawnych w zakresie ochrony prywatności będzie stanowić przedmiot dalszej współpracy z Prezesem UODO w ramach wdrażania celów projektowanej strategii. Strategia została przyjęta przez Radę Ministrów[309].

Organ nadzorczy zwraca i będzie zwracał szczególną uwagę na poszczególne projekty przepisów służących wykonaniu tej strategii państwa.

W odniesieniu do projektu dokumentu pt. „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029", stanowiącego załącznik do projektu **uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029** (ID131)[310], Prezes UODO przedstawił odmienną od projektodawcy (Ministerstwa Cyfryzacji) koncepcję ww. dokumentu. Wskazał też na potrzebę przyjęcia szczegółowych rozwiązań, w tym dokonania zmian w przepisach prawa w zakresie wskazanym w projekcie strategii, argumentując, że rozwiązania mające zapewnić cyberbezpieczeństwo mogą być wprowadzane jedynie w oparciu o wyraźną podstawę prawną. Zasygnalizował również potrzebę dokonania przeglądu dotychczasowego modelu funkcjonowania rejestrów publicznych i wypracowania jednolitych standardów ich tworzenia. A także zaapelował o uwzględnienie w strategii: a) zagadnienia przetwarzania danych biometrycznych, b) zapewnienia bezpieczeństwa usługi przetwarzania w Publicznej Chmurze Obliczeniowej, c) ryzyk związanych z użyciem sztucznej inteligencji. Ujęcie tych kwestii w strategii (choćby w sposób syntetyczny) będzie mogło mieć bardzo pozytywny wpływ na jakość projektowanych w przyszłości rozwiązań prawnych odnoszących się do problematyki cyberbezpieczeństwa.

Projektodawca nie podzielił stanowiska Prezesa UODO podnosząc, że dokument pt. „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029" ma charakter jedynie kierunkowy, wskazujący na zamierzenia organów państwa w zakresie zapewnienia cyberbezpieczeństwa. Nie może zatem zawierać wnioskowanych przez organ nadzorczy rozwiązań szczegółowych. Strategia została przyjęta przez Radę Ministrów[311].

Na zagrożenia towarzyszące rozwojowi elektronicznych usług publicznych oraz wykorzystywaniu sztucznej inteligencji w procesach administracyjnych zwrócono

[309] https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-panstwa--kompleksowy-plan-transformacji-cyfrowej-polski.
[310] DPNT.401.18.2025.
[311] Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. 2026 poz. 309).

uwagę w opinii **do projektu ustawy o zmianie ustawy o aplikacji mObywatel**[312]. Założenia projektu powielały wadliwe rozwiązania przyjęte w dotychczas obowiązującej ustawie, a krytykowane w poprzednich opiniach organu nadzorczego do pierwotnego projektu ustawy o aplikacji mObywatel. Uwagi te odnosiły się m.in. do zawierania między ministrem ds. informatyzacji a podmiotami prowadzącymi rejestry lub systemy teleinformatyczne „porozumień", skutkujących regulowaniem procesów przetwarzania danych osobowych na podstawie instrumentu prawnego pozbawionego waloru powszechnie obowiązującego prawa. Bardzo ogólnie sformułowane przepisy przewidywały niedookreślony i niezwykle szeroki dostęp przez ministra właściwego do spraw informatyzacji do przetwarzania danych pochodzących z otwartego katalogu rejestrów publicznych, niepublicznych lub systemów teleinformatycznych podmiotów publicznych lub podmiotów niepublicznych, nie wprowadzając jednocześnie żadnych mechanizmów zapewniających zgodność z prawem, rzetelność, przejrzystość, ograniczenie celu, minimalizację przetwarzania, ani środków weryfikacji i kontroli. Zdecydowanemu rozszerzeniu zakresu usług, jakie mogą być oferowane za pośrednictwem aplikacji mObywatel poprzez otwarcie dotychczas zamkniętego katalogu usług, towarzyszyły wskazania podmiotów, na których spoczywać ma odpowiedzialność za zapewnienie warunków bezpieczeństwa.

Jednym z najważniejszych założeń projektu było wprowadzenie do aplikacji mObywatel funkcjonalności wirtualnego asystenta opartego o model sztucznej inteligencji ogólnego przeznaczenia. Regulacja w tym zakresie była bardzo szczątkowa – ograniczała się jedynie do jednego, ogólnie sformułowanego przepisu. Nie wynikało z niej zwłaszcza, na czym polegać ma planowana usługa ani do realizacji jakich czynności ma być wykorzystywana. W żaden sposób nie określono: warunków, celów czy zasad, na jakich „wirtualny asystent" miałby funkcjonować, ani do jakich zasobów system SI będzie miał dostęp, jakie dane będzie pozyskiwał. Nie wskazano, w jaki sposób i według jakich kryteriów przeprowadzany jest proces uczenia maszynowego, w jaki sposób chronione są informacje przekazywane przez użytkownika lub inne informacje, do których system SI będzie miał dostęp, czy system SI gromadzi informacje pozyskiwane od użytkowników, a jeżeli tak, to na jakich zasadach są one pozyskiwane i dalej wykorzystywane. Ponadto nie uwzględniono aspektów bezpieczeństwa danych, cyberbezpieczeństwa, odporności systemu na wpływ osób trzecich, w tym na ataki hybrydowe, a także środków ograniczających ryzyka związane z błędnymi lub stronniczymi wynikami czy wykorzystaniem systemu SI do ataków dezinformacyjnych. Nie podjęto się wprowadzenia proponowanych przez organ nadzorczy mechanizmów akredytacji, certyfikacji i kontroli podmiotów-dostawców oraz samego systemu SI. Co niemniej istotne – także zapewnienia dobrowolności stosowania takiej technologii i przejrzystego informowania o zakresie jej oddziaływania, kryteriów monitorowania, skutecznego nadzoru ze strony człowieka. Uwagi organu nadzorczego nie zostały uwzględnione, a ustawa weszła w życie[313].

[312] DPNT.401.126.2025.
[313] Dz.U. 2025 r. poz. 1019

W 2025 r. Prezes UODO przedstawił też uwagi do **projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych i niektórych innych ustaw**[314]. Odnosiły się one do prowadzenia centralnej elektronicznej rejestracji, w szczególności przetwarzania w szerokim zakresie danych osobowych, w tym danych biometrycznych i dotyczących zdrowia. Wątpliwości organu nadzorczego budziła usługa tzw. asystenta głosowego (voicebota) – automatyzacja połączeń telefonicznych, rejestracji w centralnej elektronicznej rejestracji przy zastosowaniu technologii wykorzystującej automatyczne przetwarzanie danych osobowych – czy będzie dochodziło do przetwarzania danych biometrycznych w związku z nagrywaniem rozmów telefonicznych. Zdaniem organu takie rozwiązania należy rozważyć nie tylko z punktu widzenia RODO – w tym w zakresie potencjalnego zautomatyzowanego podejmowania decyzji i profilowania (art. 22), ale także aktu w sprawie sztucznej inteligencji – w tym oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (art. 27 aktu). Prezes UODO zauważył, że projektowane przepisy nie zawierały: rozwiązań dotyczących sposobów i procedur przetwarzania danych osobowych, w tym danych dotyczących zdrowia; regulacji w zakresie zabezpieczeń, w tym co sposobu dokonywania identyfikacji świadczeniobiorcy; regulacji dotyczących realizacji praw osób fizycznych, takich jak prawa do sprostowania danych, dostępu do danych, usunięcia danych oraz innych instrumentów ochrony praw osób fizycznych, takich jak prawa do interwencji ludzkiej, kontroli przez człowieka. Zwrócił również uwagę, że w przypadku nieskutecznego dialogu z asystentem głosowym projektodawca powinien przewidzieć instrumenty zapewniające właściwe środki ochrony tych praw, w tym prawa do interwencji ludzkiej – konieczny jest dostęp do usługi nie tylko przez tzw. bot, czyli asystenta głosowego, ale przez połączenie z infolinią obsługiwaną przez człowieka (usługa „chcę rozmawiać z człowiekiem”).

W czasie prac nad projektem – stosownie do uwag Prezesa UODO – projektodawca doprecyzował przepis dotyczący wykorzystywania asystenta głosowego do prowadzenia centralnej elektronicznej rejestracji. Określił cel przetwarzania danych i ich zakres. Wskazał, że przetwarzanie danych osobowych o cechach biometrycznych w związku z nagrywaniem rozmów pacjentów prowadzonych z asystentem głosowym nie może być wykorzystywane w celach służących do identyfikacji i weryfikacji osób fizycznych, zapewniając w tym zakresie właściwe gwarancje ochrony danych osobowych. Jednak nie wszystkie uwagi organu nadzorczego zostały uwzględnione, czego przykładem jest niezapewnienie prawa do interwencji ludzkiej (kontroli przez człowieka). Ustawa obowiązuje[315].

Postulaty organu nadzorczego zawarte w korespondencji z resortem cyfryzacji dotyczące **projektu ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw**[316] – mimo zapewnień projektodawcy o ich uwzględnieniu w nowelizacji ustawy – nie zostały niestety odzwierciedlone

[314] DPNT.401.101.2025.
[315] Dz. U. z 2026 r. poz. 1537
[316] DPNT.401.325.2025.

w projektowanych przepisach. Prezes UODO nie uzyskał odpowiedzi resortu, czy prowadzone są prace nad zmianą modelu dostępu do danych osobowych w związku z realizacją usługi e-doręczeń, celem dostosowania do zasad ochrony danych osobowych, w tym zmiany minimalizujące ryzyka dla osób, których dane dotyczą. Projektodawca nie odniósł się w projektowanych przepisach (nie uwzględnił uwag organu nadzorczego zgłaszanych w wystąpieniu w tej sprawie[317]) m.in. do kwestii związanej z wykorzystywaniem numeru PESEL oraz prywatnego profilu mObywatela, profilu zaufanego oraz osobistej bankowości elektronicznej pracownika do celów służbowych, który jest wymagany w związku z utworzeniem adresu do doręczeń elektronicznych (ADE) i wskazywaniem tych osób jako administratora/ów oraz użytkowników skrzynki doręczeń, o których mowa w ustawie o doręczeniach elektronicznych. Uwagi organu nadzorczego zawarte w wystąpieniu związane z modelem dostępu do danych osobowych w związku z realizacją usługi oraz inne wątpliwości Prezesa UODO nieuwzględnione w projektowanych przepisach pozostały aktualne i ponownie resortowi wskazane. W 2026 r. przedstawiono organowi nadzorczemu do zaopiniowania kolejną wersję projektu, która nie uwzględnia kompleksowo postulatów zgłoszonych zarówno w wystąpieniu dotyczącym e-doręczeń, jak i opinii z 22 września 2025 r. Proces legislacyjny nie został zakończony.

**Projekt ustawy o usłudze e-Płatności**[318] zakładał stworzenie „usługi online umożliwiającej realizację elektronicznych transakcji płatniczych dotyczących należności pobieranych przez podmioty publiczne", dostępnej za pośrednictwem Platformy e-Płatności. Przewidywał m.in. możliwość integracji systemów teleinformatycznych podmiotów publicznych, Banku Gospodarstwa Krajowego oraz usług płatniczych dostawców usług płatniczych z Platformą ePłatności. Co więcej, zgodnie z projektem podmioty publiczne miały przekazywać ministrowi właściwemu do spraw informatyzacji dane niezbędne do świadczenia usługi ePłatności, w tym dane osobowe użytkownika usługi ePłatności oraz dane dotyczące należności. Prezes UODO zwrócił uwagę, że podstawa prawna przetwarzania danych osobowych przez podmiot publiczny, w tym do przekazania danych, powinna przede wszystkim dotyczyć określonego podmiotu. Nie powinna w sposób generalny zobowiązywać wszystkich podmiotów publicznych do udostępniania danych osobowych, i to na podstawie wadliwie skonstruowanych przepisów (definicji). W zakresie integracji systemów niejasne były role w procesach przetwarzania danych osobowych w ww. usłudze ani to, jakie zadania związane z przetwarzaniem danych miały realizować poszczególne podmioty. Problematyczne było również potencjalne łączenie systemów teleinformatycznych podmiotów publicznych z Platformą ePłatności (por. motyw 31 RODO). Projektodawca na skutek uwag Prezesa UODO – w toku spotkania konsultacyjnego – zapowiedział bardziej precyzyjne ustalenie sposobu prowadzenia systemu płatności i samej platformy im służącej, która ma być zintegrowana z aplikacją mObywatel. Proces legislacyjny nie został zakończony.

[317] DOL.413.7.2024; opisane w części „Wystąpienia Prezesa UODO".
[318] DPNT.401.365.2025.

Rozwiązania zawarte w **poselskim projekcie ustawy o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw**[319] dotyczyły automatyzacji i nowych rozwiązań technologicznych zastosowanych w pojazdach zautomatyzowanych, które wiązały się z przetwarzaniem danych osobowych, w tym danych szczególnych kategorii, bo dotyczących zdrowia. Wątpliwości organu nadzorczego wzbudziła celowość prowadzenia rejestru zdarzeń (wypadków) z udziałem pojazdów zautomatyzowanych oraz na zakres danych przekazywanych w kopii zapisów zdarzeń zarejestrowanych przez elektroniczne rejestratory zamontowane w badanych pojazdach. W swojej opinii podniósł, że wdrażanie innowacyjnych rozwiązań technologicznych związanych z wprowadzaniem do porządku prawnego praw i obowiązków dotyczących zarówno podmiotów danych, jak i administratorów powinno poprzedzone powinno być testem prywatności, pożądanym zawsze, gdy istnieje wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ustawa obowiązuje[320].

Prace nad **projektem ustawy o bonie senioralnym**[321] zainicjowane w 2024 r. kontynuowano w 2025 roku. Kolejna wersja projektu ustawy zawierała nowe rozwiązania, w tym przewidujące przeprowadzanie oceny poziomu niezaspokojonych potrzeb w zakresie podstawowych czynności życia codziennego seniora w sposób zautomatyzowany. Organ nadzorczy zwrócił uwagę, że przetwarzanie danych osobowych, w tym szczególnych kategorii (dotyczących zdrowia), w sposób zautomatyzowany obarczone jest wieloma ryzykami dla praw i wolności osób fizycznych, o ile miałoby następować bez wprowadzenia zabezpieczeń odpowiednich do planowanych rozwiązań. Zauważył też, że taki sposób przetwarzania może wiązać się z wykorzystaniem algorytmów sztucznej inteligencji, co wymagało oceny nie tylko pod kątem przepisów o ochronie danych osobowych, ale również oceny przez pryzmat aktu w sprawie sztucznej inteligencji (AI Act). Organ nadzorczy ponownie zwrócił uwagę na potrzebę objęcia projektu testem prywatności, w tym oceną skutków dla ochrony danych osobowych, a także uzupełnienie jej oceną skutków systemów AI wysokiego ryzyka dla praw podstawowych jako odrębnego obowiązku wynikającego z aktu w sprawie sztucznej inteligencji. Regulacja obowiązuje. Przyjęła ostateczny kształt jako ustawa z dnia 11 czerwca 2026 r. o osobach starszych i koordynacji opieki długoterminowej[322].

Istotne działania Prezesa UODO mające wpływ na kształtowanie prawidłowych rozwiązań systemowych związanych z przetwarzaniem danych osobowych w procesie informatyzacji państwa wiążą się z niezależnym udziałem (z głosem doradczym) w pracach **Komitetu Rady Ministrów do spraw Cyfryzacji (KRMdsC)** i powołanego

[319] DPNT.401.477.2025.
[320] Dz. U. 2025 r. poz. 1843.
[321] DPNT.401.354.2025.
[322] Dz. U. z 2026 poz. 986.

w jego miejsce (w lipcu 2025 r.) **Komitetu do spraw Cyfryzacji**[323] **(KdsC).** Podczas prac obu tych podmiotów organ nadzorczy zgłaszał swoje liczne uwagi do procedowanych dokumentów i projektów. Przedstawiał także uwagi do kolejnych wersji projektu Regulaminu Komitetu do spraw Cyfryzacji[324].

Ważnym zagadnieniem, sygnalizowanym w 2025 r. zarówno przy opiniowaniu regulaminu KdsC, jak i w toku współpracy z KRMdsC, była potrzeba zmiany procedur i dobrych praktyk przy tworzeniu projektów informatycznych. Chodzi o to, by w czasie prac nad nowymi rozwiązaniami w zakresie tworzenia systemów teleinformatycznych oraz rejestrów publicznych na kolejnych etapach prac były wykonywane testy prywatności (obejmujące m.in. ocenę skutków dla ochrony danych)[325].

W związku ze stanowiskiem Prezesa UODO, na początku 2025 r. sekretarz KRMdsC zadeklarował rozszerzenie zakresu informacji przedkładanych Komitetowi odnośnie do przetwarzanych w ramach projektów informatycznych danych osobowych, w tym zmianę wzoru opisu założeń projektów informatycznych (OZPI)[326]. Monitorowanie i opiniowanie projektów informatycznych w zakresie założeń postępów i efektów realizacji takich przedsięwzięć w ramach prac KdsC było istotnym mechanizmem mającym zagwarantować właściwy proces transformacji cyfrowej państwa, zwłaszcza administracji publicznej. Z tego powodu proces transformacji państwa powinien następować w zgodzie z przepisami o ochronie danych osobowych. Niepoprawnie skonstruowane rozwiązania informatyczne mogą bowiem generować wiele ryzyk, także dla prawidłowego przetwarzania danych osobowych i prywatności.

Pominięcie aspektu ochrony danych osobowych w czasie projektowania systemów informatycznych czy rejestrów publicznych może na dalszych etapach prac skutkować stworzeniem narzędzia technologicznego niezgodnego z obowiązującym w tym zakresie prawem, nie tylko z przepisami RODO, ale także m.in. Aktu w sprawie zarządzania danymi, Aktu w sprawie sztucznej inteligencji, Aktu o usługach cyfrowych, Aktu w sprawie danych, rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia, rozporządzenia w sprawie zmiany rozporządzenia (UE) nr

---

[323] Zgodnie z art. 17 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 ze zm.) „Do zadań Rady należy: 1) proponowanie i opiniowanie na zlecenie ministra właściwego do spraw informatyzacji projektów stanowisk Rady Ministrów w sprawie dokumentów Komisji Europejskiej i Parlamentu Europejskiego dotyczących informatyzacji; 1a) opiniowanie projektu strategii oraz innych dokumentów rządowych, w tym projektów strategii rozwoju i projektów programów, w rozumieniu przepisów ustawy z 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju, dotyczących informatyzacji państwa; 2) opiniowanie projektów przepisów wydawanych na podstawie art. 18; 3) opiniowanie innych projektów aktów prawnych i innych dokumentów dotyczących informatyzacji państwa przekazanych przez ministra właściwego do spraw informatyzacji; 4) opiniowanie na zlecenie ministra właściwego do spraw informatyzacji raportów i innych opracowań dotyczących: a) potrzeb i postulatów dotyczących rozwoju społeczeństwa informacyjnego, b) zasad funkcjonowania rejestrów publicznych, c) zasad wdrażania systemów teleinformatycznych w administracji publicznej oraz stanu ich realizacji, d) aktualnych rozwiązań technicznych mających zastosowanie w informatyzacji administracji, rozwoju sieci i usług szerokopasmowych, e) terminologii polskiej z zakresu informatyki.”.

[324] Opinia Prezesa Urzędu Ochrony Danych Osobowych do projektu Regulaminu Komitetu do spraw Cyfryzacji. Pisma: z 3 października 2025 r.; 15 listopada 2025 r.; 1 grudnia 2025 r. (znak: DPNT.060.70.2025).

[325] Pismo Prezesa Urzędu Ochrony Danych Osobowych z 13 stycznia 2025 r. (DPNT.071.42.2024).

[326] Pismo Sekretarza Komitetu Rady Ministrów do spraw Cyfryzacji z 31 stycznia 2025 r. (znak: DPiS.WWKS.501.1.1.2025).

910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej[327] czy dyrektywy 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[328], jak i dyrektywy NIS2.

Jednocześnie obecna sytuacja międzynarodowa nakazuje na nowo spojrzeć na bezpieczeństwo danych osobowych. Zwłaszcza tych, które mają być przetwarzane na podstawie projektowanych rozwiązań informatycznych. Istotny jest pryzmat sytuacji zagrożenia państwa i bezpieczeństwa narodowego w wielu jego aspektach oraz potraktowanie ich kompleksowo.

Wypracowanie rozwiązań, które będą gwarantowały ochronę danych osobowych, było więc podyktowane nie tylko zagrożeniami dla prywatności jednostki, ale także istotnymi ryzykami w sferze obronności Polski i Unii Europejskiej. Ryzyka te nie ograniczają się do cyberzagrożeń. Wiążą się z całym spektrum działań związanych z nielegalnym przetwarzaniem danych osobowych.

Na aspekty te Prezes UODO zwracał szczególną uwagę w swoich stanowiskach do poszczególnych projektów informatycznych procedowanych w ramach prac KdsC.

**Do najczęściej zgłaszanych uwag należały te odnoszące się do:**

1. konieczności przeprowadzenia testu prywatności dla projektu;
2. konieczności dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych określonej w art. 27 Aktu w sprawie sztucznej inteligencji;
3. dokonania realnej oceny otoczenia prawnego projektu i uwzględnienia zmian w ramach planowanych zmian legislacyjnych;
4. ryzyk związanych z integralnością i poufnością danych osobowych w związku z wykorzystaniem infrastruktury chmurowej w ramach projektu, a także wykorzystywania rozwiązań open-source;
5. przeprowadzenia analiz związanych z podatnością systemów na potencjalne cyberataki i działania hybrydowe;
6. ryzyk związanych ze zmianą pierwotnych celów przetwarzania danych osobowych oraz łączenia baz danych;
7. konieczności uwzględnienia gwarancji dla podmiotów danych zwłaszcza w przypadku przetwarzania danych osobowych objętych wzmocnioną ochroną (danych szczególnych kategorii określonych w art. 9 ust. 1 RODO, danych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa objętych ochroną z art. 10 RODO, numerów PESEL, a także danych objętych tajemnicą prawnie chronioną);

[327] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 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 r. poz. 1183 ze zm.), dalej: rozporządzenie w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej.
[328] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE. L 2016/1148 z 19.07.2016), dalej: Dyrektywa 2016/1148.

8. skali i zakresu procedowanych projektów informatycznych. Uwagi w tym zakresie obrazują szczególne znaczenie procedur związanych z ich opiniowaniem na prawidłowy proces transformacji cyfrowej organów publicznych. Prezes UODO wspiera eksperckimi opiniami Komitet do spraw Cyfryzacji oraz wnioskodawców tych projektów. Biorąc pod uwagę, że obszary objęte realizacją projektów informatycznych, takie jak np. zdrowie publiczne, sądownictwo, zamówienia publiczne, transport, system podatkowy mają kluczowe znaczenie dla funkcjonowania państwa, zdiagnozowanie ewentualnych ryzyk także dla prawidłowego przetwarzania w nich danych osobowych ma istotną rolę w zapewnieniu ich bezpieczeństwa, a także zagwarantowania praw osób, których dane dotyczą;
9. ryzyk związanych z wykorzystaniem przez wnioskodawcę inwazyjnych metod przetwarzania danych osobowych (np. profilowanie, wykorzystanie AI, transmisja i nagrywanie).

Wśród istotnych przedstawionych przez organ nadzorczy opinii dla takich projektów należy wskazać m.in. **projekt informatyczny „e-Zdrowie KPO”**[329]**.** Miał on na celu dostarczenie nowoczesnych narzędzi wspierających analizę stanu zdrowia pacjentów oraz cyfryzację dokumentacji medycznej z wykorzystaniem zaawansowanych technologii, takich jak sztuczna inteligencja (AI) oraz uczenie maszynowe (ML). Efektami projektu miały być: poprawa jakości opieki zdrowotnej, optymalizacja procesów diagnostycznych oraz zwiększenie dostępności usług medycznych dla pacjentów, a także dostęp do narzędzi analitycznych dla lekarzy. Projekt zakładał szeroką integrację systemów i stworzenie megabazy w postaci centralnego repozytorium danych medycznych. Miała dotyczyć aż 56 takich systemów, w tym m.in. Systemu Gromadzenia Danych Medycznych (SGP); Krajowej Sieci Onkologicznej (KSO); Elektronicznej Dokumentacji Medycznej (EDM); Systemu Domowej Opieki Medycznej (DOM); e-Proflu Pacjenta (ePP) czy Kompleksowego Systemu Informatycznego ZUS (KSI ZUS). Rozwiązania projektu przewidywały, że dane osobowe podlegające szczególnej ochronie prawnej[330] mają być przetwarzane w projektowanym systemie informatycznym za pomocą nowych technologii, przy użyciu metod wykorzystujących sztuczną inteligencję (AI) oraz uczenie maszynowe (ML), a także zakładały możliwość profilowania osób fizycznych oraz automatycznego przetwarzania ich danych.

Organ nadzorczy, opiniując projekt, zarekomendował przyspieszenie wykonania planowanego przez projektodawcę testu prywatności, by na jak najwcześniejszym etapie zdiagnozować ryzyka w sferze ochrony danych osobowych. Zalecił rozważenie dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych na podstawie art. 27 Aktu w sprawie sztucznej inteligencji. Wskazał na zmianę pierwotnych celów przetwarzania danych osobowych – to poważne ryzyko związane z

[329] DPNT.060.20.2025.

[330] Dane dotyczące stanu zdrowia, dane genetyczne, dane biometryczne, a także inne dane szczególnych kategorii wskazane w art. 9 RODO, numery PESEL, zawarte w dokumentacji medycznej, tajemnice prawnie chronione, a także potencjalnie dane dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa z art. 10 RODO.

planowaną integracją systemów w jednej magabazie. Za wysoce pożądane i zasadne uznał dokonanie przez wnioskodawcę projektu informatycznego pogłębionej analizy otoczenia prawnego projektu w celu zweryfikowania przepisów, aby dane osobowe w projektowanym systemie były przetwarzane w sposób legalny.

Przeprowadzenie testu prywatności rekomendowano również w opinii do **projektu informatycznego „Wdrożenie Zapasowego Centrum Przetwarzania Danych SPOE KAS”**[331]. Projekt miał na celu wdrożenie zapasowego Centrum Przetwarzania Danych (Zapasowe CPD) w celu zapewnienia ciągłości działania Systemu Poboru Opłaty Elektronicznej Krajowej Administracji Skarbowej (SPOE KAS). Projektowane rozwiązanie miało: zapewnić ciągłość działania systemu, zwiększyć bezpieczeństwo poboru opłaty elektronicznej i stabilne zasilanie Krajowego Funduszu Drogowego opłatami elektronicznymi. Projekt informatyczny miał być realizowany z wykorzystaniem szeregu systemów teleinformatycznych, w tym m.in.: Systemu Poboru Opłaty Elektronicznej KAS, e-Urzędu Skarbowego, Węzła Krajowego, Systemu Informatycznego CEPiK 2.0, Centralnej Hurtowni Danych w Resorcie Finansów (CHD RF). Zakładał przetwarzanie danych na szeroką skalę, w tym danych osób fizycznych, pojazdów, praw jazdy, dokumentów pojazdu, danych kart płatniczych czy nr PESEL. Projektowany system miał korzystać z danych z Centralnego Rejestru Podmiotów – Krajowej Ewidencji Podatników (CRP KEP), w którym to rejestrze publicznym przetwarzane są m.in. dane ewidencyjne z rejestru PESEL dotyczące osób fizycznych objętych tym rejestrem. Dla realizacji projektu miało być też wykorzystane środowisko chmurowe.

Biorąc pod uwagę, że realizacja projektu informatycznego miała się wiązać z przetwarzaniem w znacznej ilości i na dużą skalę danych osób fizycznych objętych tajemnicą prawnie chronioną (tajemnica skarbowa), numeru PESEL, a potencjalnie także danych szczególnych kategorii (danych o stanie zdrowia kierowców), organ nadzorczy zalecił wykonanie dla projektu informatycznego testu prywatności. Zwrócił także uwagę, że przetwarzanie danych osobowych w środowisku chmurowym może generować ryzyka dla integralności i poufności tych danych – co wnioskodawca powinien uwzględnić, realizując projekt.

Podobne stanowisko wyrażono do **projektu informatycznego „Automatyzacja i optymalizacja procesu egzekucji administracyjnej w KAS - wytworzenie w ramach JSP Modułu Egzekucji (JSP Egzekucja)”**[332]. Projekt zakładał udostępnienie nowego systemu JSP Egzekucja, a także aplikacji do prowadzenia licytacji elektronicznych. Jak wskazywano w jego założeniach, za pomocą tej aplikacji każdy obywatel każdego państwa członkowskiego UE będzie mógł brać udział w licytacjach elektronicznych prowadzonych przez organy egzekucyjne KAS. W ramach projektu informatycznego miała zostać też uruchomiona Aplikacja Mobilny Poborca II, która m.in. miała wesprzeć pracowników w terenie, dostarczać aktualną informację o stanie należności zobowiązanych, pozwolić na odnotowanie pobrania gotówki lub dokonanie

[331] DPNT.060.24.2025.
[332] DPNT.060.25.2025.

płatności bezgotówkowej. Informacje o czynnościach dokonanych w terenie miały być odnotowywane w Jednolitym Systemie Podatkowym.

Realizacja projektu będzie się wiązać z przetwarzaniem w znacznej ilości i na dużą skalę danych osób fizycznych, w tym danych szczególnych kategorii (np. związanych ze stanem zdrowia dłużników), danych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa objętych ochroną z art. 10 RODO, numeru PESEL, a także danych objętych tajemnicą prawnie chronioną (tajemnica skarbowa). Prezes UODO zalecił zatem wykonanie dla projektu informatycznego testu prywatności oraz analizy otoczenia prawnego w związku z ryzykiem łączenia baz danych (motyw 31 rozporządzenia 2016/679[333]).

Pozytywnie oceniono deklarację projektodawcy wykonania testu prywatności dla **projektu informatycznego „Cyfrowy Sąd”**[334]. Organ nadzorczy podkreślił, że projektowane rozwiązania (uruchomienie jednego ogólnokrajowego systemu dedykowanego sądom powszechnym w oparciu o nowoczesne rozwiązania techniczno-systemowe) w przypadku ich wejścia w życie będą miały poważny wpływ na przetwarzanie danych osobowych w związku ze sprawowaniem wymiaru sprawiedliwości w Polsce. W tworzonym na podstawie projektu systemie informatycznym będą bowiem przetwarzane dane, w tym dane osobowe, na wielką skalę związane ze sprawowaniem wymiaru sprawiedliwości, w szczególności dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa objęte dodatkową ochroną z art. 10 RODO, znajdujące się w aktach postępowań różnego charakteru dane szczególnych kategorii. W systemie tym będą także przetwarzane numery PESEL oraz dane objęte tajemnicą prawnie chronioną zawarte w aktach spraw postępowań. Dodatkowo zauważono, że jeżeli w projektowanym systemie mają być wykorzystywane systemy sztucznej inteligencji, to wnioskodawca powinien wziąć pod uwagę nie tylko przepisy RODO, ale także akt w sprawie sztucznej inteligencji, w tym jego art. 27, z którego wynika odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych.

Poważne wątpliwości Prezesa UODO wzbudziło natomiast to, że wnioskodawca nie przewidywał w związku z realizacją projektu zmiany obowiązujących aktów prawnych. Jednocześnie wśród ryzyk o niskim prawdopodobieństwie wystąpienia, ale o dużej sile odziaływania wskazał brak zapewnienia zgodności przetwarzania danych

---

[333] Zgodnie z motywem 31 rozporządzenia 2016/679 organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

[334] DPNT.060.28.2025.

osobowych z obowiązującymi regulacjami. W tym zakresie organ nadzorczy przedstawił odmienne stanowisko i zaznaczył, że w jego opinii istotna zmiana przepisów prawa regulujących model przetwarzania danych osobowych w ramach prowadzenia postępowań karnych, obejmująca również przetwarzanie tych danych w systemach teleinformatycznych, jest konieczna.

Podobne stanowisko Prezes UODO wyraził w odniesieniu do **projektu informatycznego „Platforma e-Zamówienia”**[335], który zakładał jako cel dostarczenie uczestnikom rynku zamówień publicznych narzędzi elektronicznych wspierających proces udzielenia zamówienia publicznego we wszystkich procedurach wskazanych w ustawie Prawo zamówień publicznych[336] oraz w ustawie o umowie koncesji na roboty budowlane lub usługi[337]. Jednocześnie projektowany system informatyczny miał przetwarzać zawartość rejestrów publicznych i systemów teleinformatycznych, takich jak m.in.: e-Doręczenia, Platforma Aukcji Elektronicznych, Platforma e-Zamówienia, EZD RP, REGON, TERYT, a także wykorzystywać Węzeł Krajowy oraz technologie sztucznej inteligencji.

Prezes UODO podkreślił, że przewidywane rozwiązania w przypadku ich wejścia w życie będą miały ogromny wpływ na model przetwarzania danych osobowych w ramach zamówień publicznych w Polsce – w tym przy użyciu nowych technologii. Wskazał, że na podstawie projektowanych rozwiązań będą przetwarzane na wielką skalę dane osobowe znajdujące się w aktach postępowań o zamówienia publiczne, w tym dotyczące m.in. wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa objętych ochroną z art. 10 RODO, a w części przypadków znajdujące się w aktach tych postępowań różnego charakteru dane szczególnych kategorii. W systemie tym byłyby także przetwarzane numery PESEL.

Z tego powodu organ nadzorczy pozytywnie ocenił deklarację projektodawcy wykonania testu prywatności dla projektu. Dodatkowo jednak wskazał na potrzebę dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych określoną w art. 27 Aktu w sprawie sztucznej inteligencji. Jednocześnie zgłaszał wątpliwości do stanowiska wnioskodawcy, który w dokumentacji nie przewidywał potrzeby zmiany aktów prawnych w związku z realizacją projektu. Ponadto zasygnalizował, że wykorzystanie infrastruktury chmurowej dla projektu, w ramach którego ma być przetwarzana ogromna ilość danych osobowych o charakterze sensytywnym, może rodzić ryzyka w sferze cyberbezpieczeństwa, zwłaszcza gdy wnioskodawca nie wyklucza wykorzystania w tym celu domeny prywatnej, a także rozwiązań open-source.

W **projekcie informatycznym „Wsparcie usprawniania usług publicznych poprzez udostępnienie narzędzi cyfryzacji procesów back-office i rozwój systemu EZD RP w podmiotach realizujących zadania publiczne wraz**

[335] DPNT.060.31.2025.
[336] Ustawa z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320).
[337] Ustawa z dnia 21 października 2016 r. o umowie koncesji na roboty budowlane lub usługi (Dz. U. z 2023 r. poz. 140).

**z zapewnieniem wsparcia wdrożeniowego”**[338] wnioskodawca założył niezwykle poważne cele: 1) usprawnienie funkcjonowania administracji publicznej poprzez budowę, rozwój i udostępnienie nowoczesnych narzędzi cyfryzujących procesy back-office w ramach ekosystemu EZD RP; 2) likwidację bariery technologicznej podmiotów publicznych w postaci ograniczonej zdolności do wdrożenia systemu EZD we własnym środowisku (model on-premise) poprzez udostępnienie możliwości korzystania z aplikacji EZD RP w środowisku chmurowym zgodnie z potrzebami kolejnych podmiotów realizujących zadania publiczne; 3) maksymalizację skali wykorzystania systemów klasy EZD w administracji publicznej poprzez zapewnienie wsparcia w procesie wdrożenia systemu do elektronicznego zarządzania dokumentacją (EZD RP) udostępnianego nieodpłatnie przez NASK-PIB podmiotom realizującym zadania publiczne; 4) wprowadzenie usługi umożliwiającej zautomatyzowaną wymianę danych między zgrupowanymi instytucjami posiadającymi EZD RP.

Organ nadzorczy, analizując zawarte w projekcie informatycznym rozwiązania, zwrócił uwagę, że ich wejście w życie będzie miało istotny wpływ na model przetwarzania danych osobowych w związku z realizacją zadań podmiotów publicznych z wykorzystaniem systemu EZD RP w skali całego kraju. W modyfikowanym systemie informatycznym będą bowiem przetwarzane przez podmioty publiczne dane, w tym dane osobowe, na wielką skalę związane m.in. ze stanem zdrowia, a także inne dane szczególnych kategorii oraz numery PESEL, dane dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa objęte dodatkową ochroną z art. 10 RODO oraz dane objęte tajemnicą prawnie chronioną zawarte w dokumentacji podmiotów publicznych. W związku z powyższym organ nadzorczy rekomendował przeprowadzenie dla projektu informatycznego testu prywatności, a w przypadku zastosowania w projekcie rozwiązań z wykorzystaniem systemów AI wysokiego ryzyka dla praw podstawowych – przeprowadzenie także oceny skutków określonej w art. 27 Aktu w sprawie sztucznej inteligencji. Biorąc pod uwagę kwestię cyberbezpieczeństwa danych osobowych przetwarzanych w EZD RP, Prezes UODO podkreślił, że planowane wykorzystanie **infrastruktury chmurowej** wymaga szczególnie wnikliwej analizy wszystkich ryzyk z tym związanych.

Uwzględniając z kolei szeroki zakres zmian przepisów prawa, jakie będą musiały towarzyszyć wdrożeniu projektowanego rozwiązania, wskazywał na potrzebę szczególnie wnikliwej analizy otoczenia prawnego projektu. Zwrócił także uwagę na ryzyka związane ze zmianą pierwotnych celów przetwarzania danych osobowych w ramach projektu informatycznego, która może zachodzić jedynie w sytuacjach ściśle określonych w RODO.

Realizacja **projektu informatycznego „Transformacja Cyfrowa Kolejowych Ośrodków Dokumentacji Geodezyjnej i Kartograficznej”**[339] miała wiązać się z przetwarzaniem danych osobowych w szerokim zakresie, gdyż przewidywał on wykorzystywanie systemów, w których miały być gromadzone dane osobowe (m.in.

[338] DPNT.060.57.2025.
[339] DPNT.060.38.2025.

osób prywatnych posiadających nieruchomości graniczące z terenami kolejowymi, stron umów najmu i dzierżawy zamkniętych terenów kolejowych, pracowników beneficjenta, czyli PKP S.A.).

Z tego powodu organ nadzorczy pozytywnie ocenił deklarację projektodawcy wykonania testu prywatności dla projektu. Dodatkowo Prezes UODO podkreślił, że jeżeli w projektowanym systemie mają być wykorzystywane systemy sztucznej inteligencji, wnioskodawca powinien wziąć pod uwagę nie tylko przepisy RODO, ale także Aktu w sprawie sztucznej inteligencji, w tym jego art. 27, z którego wynika odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych. W ocenie organu nadzorczego ponownej oceny wnioskodawcy wymagało otoczenie prawne projektu[340]. Prezes UODO zwrócił także uwagę, że ze względu na charakter przetwarzania danych i wiążące się z nim ryzyko naruszenia praw i wolności osób fizycznych, poszerzonej analizy wymagają także procedowane w ramach projektu rozwiązania związane z podatnością systemu na potencjalne cyberataki i działania hybrydowe.

Jak wskazywał wnioskodawca projektu **informatycznego „Udzielenie wsparcia finansowego na realizację działań związanych z informatyzacją szpitali w systemie podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej (PSZ)”**[341], szpitale coraz częściej są celem cyberataków, a więc istnieje pilna potrzeba wzmocnienia bezpieczeństwa przetwarzania danych osobowych w elektronicznej dokumentacji medycznej (dalej: EDM) w tych podmiotach. Wśród celów projektu wskazano „integrację z narzędziami i funkcjonalnościami wytworzonymi przez CeZ”, digitalizację dokumentacji medycznej oraz zwiększenie poziomu cyberbezpieczeństwa szpitali. Projekt zakładał również wdrożenie rozwiązań AI i podłączenie do centralnego repozytorium danych medycznych.

Opiniując ten projekt informatyczny, organ nadzorczy zarekomendował wykonanie testu prywatności. Zalecił także rozważenie dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych na podstawie art. 27 Aktu w sprawie sztucznej inteligencji. Wskazał również na potrzebę podjęcia działań legislacyjnych mających na celu określenie właściwej podstawy prawnej dla funkcjonowania projektowanego systemu informatycznego, uczulając przy tym na ryzyka związane z łączeniem zbiorów danych osobowych. Zwrócił również uwagę na potrzebę uwzględnienia przepisów Rozporządzenia o europejskiej przestrzeni danych dotyczących zdrowia (ang. EHDS), które weszło w życie 26 marca 2025 r i odnosi się m.in. do pierwotnego i wtórnego wykorzystywania danych.

**Celem projektu informatycznego „SDD 1.0. – system do prowadzenia postępowań dyscyplinarnych w samorządzie komorniczym”**[342] miało być

[340] W związku z tym, że omawiany projekt informatyczny miał ścisły związek ze Strategią Cyfryzacji Polski, organ nadzorczy opiniując go, przypomniał swoje stanowisko w sprawie projektu „Strategii Cyfryzacji Polski do 2035 roku”, w którym zwrócił uwagę, że wdrożeniu rozwiązań technologicznych powinny towarzyszyć stosowne rozwiązania prawne gwarantujące wymagany poziom poszanowania praw podstawowych, w tym konstytucyjnego prawa do prywatności oraz ochrony danych osobowych.
[341] DPNT.060.65.2025.
[342] DPNT.060.33.2025.

stworzenie systemu teleinformatycznego umożliwiającego przede wszystkim dostęp do materiałów postępowań dyscyplinarnych przez ich strony oraz wymiany dokumentów i korespondencji między komisją dyscyplinarną, stronami i sądami. Za pośrednictwem systemu przetwarzane miały być dane osobowe uczestników postępowań (stron, pełnomocników, świadków, biegłych), w tym również dane sensytywne (art. 9 ust. 1 RODO) czy identyfikatory PESEL (art. 87 RODO). Ze względu na przedmiot prowadzonych postępowań oraz ich poufny charakter, informacje dotyczące osób fizycznych zawarte w dokumentacji miały mieć charakter wysoce osobisty lub wrażliwy. Ponadto system zapewniać miał funkcjonalność polegającą na przesłuchiwaniu stron, świadków, biegłych w formie wideokonferencji. Wdrożenie SDD wiązać się miało ponadto z przetwarzaniem danych osobowych w oparciu o infrastrukturę wykorzystującą chmurę podmiotu prywatnego.

W przedstawionej opinii organ nadzorczy pozytywnie ocenił implementację testów prywatności na różnych etapach wdrażania systemu, jak też założenia ogólne dotyczące bezpieczeństwa, przewidujące trójwarstwowy model ochrony informacji, oparty o jasne określenie ról i odpowiedzialności w tym zakresie. Natomiast jednym z jego postulatów było poszerzenie analizy o kryteria związane z podatnością systemu na potencjalne cyberataki i działania hybrydowe. Prezes UODO zwrócił także uwagę na zagrożenia związane z opieraniem infrastruktury o rozwiązania chmurowe od prywatnych dostawców – zarówno pod względem zapewniania ciągłości działania systemu, jak i poufności danych. Wskazał przy tym, że taki model przetwarzania poparty powinien być w każdym przypadku konkretnymi i skutecznymi środkami weryfikacji i kontroli podmiotów zapewniających usługę chmurową.

Warto podkreślić, że opiniując projekty dotyczące rozwiązań cyfrowych, organ nadzorczy przywiązywał szczególną wagę do aspektów związanych z ochroną danych w wymiarze obejmującym bezpieczeństwo narodowe, wskazując na potrzebę zapewnienia wzmożonego reżimu odporności systemów o znaczeniu istotnym dla funkcjonowania państwa.

### 15.8. Nowe kompetencje Prezesa UODO

W 2025 roku Prezes UODO, podobnie jak w roku 2024, prowadził z właściwymi resortami, a głównie resortem cyfryzacji, ustalenia związane z zakresem jego nowych kompetencji wynikających z prawa unijnego i ich odpowiedniego wdrożenia w krajowym porządku prawnym poprzez projekty ustaw. Uwagi zgłaszane przez Prezesa UODO dotyczyły przede wszystkim właściwego określenia ram współpracy Prezesa UODO z innymi organami tak, aby zapewnić możliwie jak najpełniejsze wykonywanie zadań przewidzianych przez prawodawcę unijnego.

W 2025 r. Prezes UODO prowadził korespondencję z resortem cyfryzacji ws. **projektu ustawy o systemach sztucznej inteligencji**[343]. Ustawa ta ma stanowić „rozwiązania instytucjonalne” dla zapewnienia stosowania AI Act, który wchodzi życie etapami. 2 sierpnia 2025 r. weszły w życie przepisy AI Act dotyczące m.in. nadzoru nad rynkiem oraz kar dla podmiotów, które będą korzystać ze sztucznej inteligencji

[343] DOL.401.354.2024.

w sposób sprzeczny z prawem. Prawodawstwo krajowe powinno już być dostosowane do powyższych regulacji. Ustawa obowiązuje[344].

Ustawa ta wprowadza przepisy proceduralne pozwalające na stosowanie w polskim porządku prawnym aktu w sprawie sztucznej inteligencji (AI Act), w tym powołania oraz funkcjonowania nowego organu nadzoru rynku – Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji. Komisja, będzie organem kolegialnym, przewodniczący będzie powoływany przez Sejm za zgodą Senatu na 5-letnią kadencję, w pracach komisji będą uczestniczyć z głosem doradczym również przedstawiciele innych instytucji oraz zaproszeni eksperci. Komisja ma sprawować nadzór nad przestrzeganiem przepisów europejskiego rozporządzenia w sprawie sztucznej inteligencji, będzie m.in. wydawać opinie indywidualne i wyjaśnienia, tworzyć i prowadzić piaskownice regulacyjne, rozpatrywać skargi osób, których prawa mogły zostać naruszone przez niezgodne z prawem systemy sztucznej inteligencji, oraz będzie realizować zadania w zakresie pojedynczego punktu kontaktowego, także dla europejskich piaskownic regulacyjnych.

Komisja będzie współpracować z Prezesem UODO, kluczowe regulacje odnoszą się do:

- materii piaskownic regulacyjnych (art. 57 aktu w sprawie sztucznej inteligencji), w zakresie określonym rozporządzeniem 2024/1689 i ustawą Komisja ma współpracować z Prezesem Urzędu Ochrony Danych Osobowych – w zakresie spraw, o których mowa w art. 57 ust. 10 rozporządzenia 2024/1689 i ustawie (art. 20 ust. 1 pkt 3 ustawy);
- wyłaniania kandydatów na zastępców Przewodniczącego Komisji - przedstawiciel wyznaczony przez Prezesa UODO ma wchodzić w skład zespołu powołanego przez Przewodniczącego Komisji wyłaniającego ww. osobę (art. 32 ust. 2 pkt 3 ustawy);
- opinii dotyczących oczekiwań regulacyjnych w odniesieniu do przetwarzania danych osobowych w piaskownicy regulacyjnej - Prezes UODO będzie przedstawiał Komisji lub podmiotom uczestniczącym w piaskownicy regulacyjnej takie opinie, bez uszczerbku dla swoich uprawnień nadzorczych określonych w rozporządzeniu 2016/679, z uwzględnieniem art. 57 ust. 12 rozporządzenia 2024/1689 (art. 92 ustawy).

Mocą ustawy o systemach sztucznej inteligencji do przepisów ustawy o ochronie danych osobowych dodany został art. 59a stanowiący o współpracy Prezes UODO współpracuje z Komisją (Art. 123 ustawy).

27 lipca 2026 r. wszedł w życie Digital Omnibus on AI – rozporządzenie zmieniające AI Act. Istotna dla organu nadzorczego jest m.in. zmiana terminu rozpoczęcia stosowania pełnych wymogów i obowiązków w zakresie samodzielnych systemów sztucznej inteligencji wysokiego ryzyka (z Załącznika III do AI Act) – nowy termin to 2 grudnia 2027 r.

[344] Dz. U. z 2026 poz. 1003.

Do zadań Prezesa UODO w związku z nowymi obowiązkami nałożonymi rozporządzeniem (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiającym europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) oraz **projektem ustawy o udziale Rzeczypospolitej Polskiej w europejskim systemie informacji o podróży oraz zezwoleń na podróż (ETIAS)**[345] należy przeprowadzenie kontroli zarówno przed uruchomieniem systemu na wniosek Komendanta Głównego Straży Granicznej, jak i przynajmniej raz na trzy lata kontroli (audytu) operacji przetwarzania danych w krajowej infrastrukturze granicznej, zgodnie z odpowiednimi międzynarodowymi standardami przeprowadzania kontroli (w tym kontrole na miejscu, delegacje krajowe i zagraniczne). Co więcej organ nadzorczy zobowiązany jest również do prowadzenia postępowań związanych z kontrolą naruszeń, jak i monitorowania, czy przetwarzanie danych osobowych w KSI ETIAS odbywa się zgodnie z prawem. Działania te prowadzone są w ramach postępowania skargowego, pośredniego dostępu, przyjmowania dokumentacji dotyczącej decyzji o sprostowaniu lub usunięciu danych, kontroli przekazywania danych do państw trzecich, nadzoru nad profilami dostępu (w celu zapewnienia, by wszystkie uprawnione organy utworzyły i udostępniły organom nadzorczym właściwym w sprawach ochrony danych osobowych profile określające funkcje i obowiązki osób uprawnionych do operacji na danych), udzielania wsparcia w przypadku sporów dotyczących decyzji administracyjnych związanych z ETIAS, pomocy osobom, których dane dotyczą (udzielanie pomocy i porad w zakresie wykonywania prawa do sprostowania, uzupełnienia, usunięcia lub ograniczenia przetwarzania danych, zapewnienie dostępności pomocy przez cały czas trwania postępowania w sprawie ochrony praw), współpracy transgranicznej (między organami właściwymi w sprawie ochrony danych osobowych, tj. państwa przekazującego dane i państwa rozpatrującego wniosek osoby), monitorowania legalności przetwarzania danych w ETIAS, w tym przesyłania danych do i z systemu, dostępu do informacji i infrastruktury (otrzymywanie żądanych informacji o działaniach organów dostępowych, dostęp do rejestrów operacji oraz do wszystkich pomieszczeń związanych z systemem.

W kontekście tych nowych zadań, w toku opiniowania projektu ustawy Prezes UODO zwrócił uwagę na kolizję kompetencji Prezesa UODO do sprawowania funkcji organu nadzorczego w odniesieniu do przetwarzania danych osobowych w ramach systemu ETIAS z kompetencjami organów wskazanych w art. 191a Prawa o prokuraturze[346]. W toku uzgodnień ustalono, że przepis projektu ustawy ustanawiający tę kompetencję Prezesa UODO stanowi *lex specialis* względem ww. regulacji Prawa o prokuraturze.

Prezes UODO, zgłaszając uwagi do **projektu ustawy o sprawiedliwym dostępie do danych**[347], służącej stosowaniu przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854, tj. Aktu w sprawie danych, podkreślił, że ukształtowanie mocą tworzonych przepisów krajowego nadzoru instytucjonalnego

[345] DPNT.401.292.2025.
[346] Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (Dz. U. z 2024 r. poz. 390 ze zm.).
[347] DPNT.401.467.2025.

wymaga uwzględnienia kompetencji nadzorczych przyznanych organom ochrony danych przez sam Akt w sprawie danych, który wprost powierza organowi ochrony danych osobowych realne kompetencje służące monitorowaniu stosowania tego aktu w zakresie ochrony danych osobowych. Projektowane rozwiązania wymagają zatem ustawowego doprecyzowania podziału kompetencji między organem właściwym, tj. Prezesem Urzędu Komunikacji Elektronicznej a Prezesem UODO, oraz wprowadzenia wiążących mechanizmów współpracy pomiędzy równoległymi organami nadzorczymi. Proces legislacyjny nie został zakończony – prace w tym zakresie trwają w 2026 r. i angażowany jest w nie Prezes UODO.

W 2025 r. trwały prace legislacyjne nad **projektem ustawy o zarządzaniu danymi**, które zakończyły się w 2026 r. Przyjęcie ustawy o zarządzaniu danymi miało na celu zapewnienie pełnego stosowania w Polsce rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi (Akt w sprawie zarządzania danymi)[348]. Akt w sprawie zarządzania danymi służy zwiększeniu zaufania do dzielenia się danymi poprzez ustanowienie odpowiednich mechanizmów kontroli sprawowanej przez osoby, których dane dotyczą, i posiadaczy danych nad danymi, które ich dotyczą, oraz usunięciu innych barier dla dobrze funkcjonującej i konkurencyjnej gospodarki opartej na danych (Motyw 5 DGA).

DGA wprowadza szereg mechanizmów mających zapewnić bezpieczny i przejrzysty przepływ danych, w szczególności poprzez:

- uregulowanie zasad ponownego wykorzystywania określonych kategorii danych pozostających w posiadaniu podmiotów sektora publicznego, które podlegają ochronie praw osób trzecich (tzw. dane chronione);
- ustanowienie ram prawnych dla działalności dostawców usług pośrednictwa w zakresie danych w celu zwiększenia zaufania między podmiotami udostępniającymi i korzystającymi z danych;
- zachęcanie do udostępniania danych w interesie publicznym (altruizm danych);
- ustanowienie Europejskiej Rady ds. Innowacji w zakresie Danych, której zadaniem jest wspieranie spójnego stosowania przepisów i wymiany dobrych praktyk między państwami członkowskimi.

Przygotowany przez Ministra Cyfryzacji w 2024 r. projekt ustawy o zarządzaniu danymi (projekt UC67) przyznał Prezesowi UODO kompetencje organu właściwego zarówno do spraw usług pośrednictwa danych, jak i rejestracji organizacji altruizmu danych. Projekt ustawy nadał także Prezesowi UODO kompetencję w zakresie prowadzenia postępowań dotyczących naruszeń zasad przekazywania danych nieosobowych do państw trzecich.

Rada Ministrów przyjęła projekt tej ustawy 21 października 2025 r.[349] Ostatecznie ustawa została uchwalona 27 marca 2026 r. [350] i weszła w życie 23 lipca 2026 r.

[348] Dz. Urz. UE L 152 z 3.6.2022, s. 1–44), dalej jako: „DGA”.
[349] https://legislacja.rcl.gov.pl/projekt/12389302.
[350] Dz. U. z 2026 r. poz. 548.

## 15.9. Deregulacja

W 2025 r. Prezes UODO odnosił się również do projektów przepisów deregulacyjnych, których celem była poprawa warunków prowadzenia działalności gospodarczej i upraszczanie relacji obywatel – państwo.

Jednym z takich rozwiązań była zmiana **ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, ustawy z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi oraz ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów**[351]. W projektowanych przepisach zaproponowano rezygnację z pisemnej formy upoważnień do przetwarzania danych osobowych w: art. $22^{1b}$ § 3 Kodeksu pracy[352], art. 36 ust. 4 ustawy o badaniach klinicznych produktów leczniczych stosowanych u ludzi[353] oraz art. 27 ust. 2 ustawy o ochronie sygnalistów[354]. Organ nadzorczy zwrócił uwagę, że obowiązkiem każdego administratora jest zapewnienie, aby osoba fizyczna, która działa z upoważnienia administratora (oraz podmiotu przetwarzającego), mająca dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego (art. 32 ust. 4 RODO). To administrator określa krąg osób, które mają dostęp do danych i dalszych form ich przetwarzania. Artykuł 29 RODO nie wymaga sformalizowanej konstrukcji pisemnych upoważnień wydawanych przez administratorów jako warunku dopuszczenia danej osoby do przetwarzania danych osobowych. Prawodawca wymaga faktycznego, a nie jedynie formalnego podniesienia standardu ochrony danych i prawa osób fizycznych – ochrona powinna być rzeczywista i skuteczna. Zatem pisemne upoważnienie jest środkiem niewymaganym przez rozporządzenie 2016/679. Na aspekt ten, w uzasadnionych przypadkach, Prezes UODO wielokrotnie zwracał uwagę w swoich opiniach legislacyjnych. Podkreślał, że rolą administratora jest wyznaczenie poleceniem ram, w jakich mogą się poruszać osoby, którym nadano dostęp do danych osobowych, a sama forma wyznaczenia przez administratora dostępu do danych czy systemów, w których są one przetwarzane, nie została precyzyjnie określona w przepisach rozporządzenia 2016/679[355].

---

[351] DPNT.401.329.2025.

[352] „Do przetwarzania danych osobowych, o których mowa w § 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy."

[353] „Sponsor dopuszcza do przetwarzania danych osobowych wyłącznie osoby posiadające pisemne upoważnienie wydane przez administratora danych. Osoby upoważnione do przetwarzania danych osobowych zobowiązują się na piśmie do zachowania ich w tajemnicy."

[354] „Do przyjmowania i weryfikacji zgłoszeń wewnętrznych, podejmowania działań następczych oraz przetwarzania danych osobowych osób, o których mowa w ust. 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie podmiotu prawnego. Osoby upoważnione są obowiązane do zachowania tajemnicy w zakresie informacji i danych osobowych, które uzyskały w ramach przyjmowania i weryfikacji zgłoszeń wewnętrznych, oraz podejmowania działań następczych, także po ustaniu stosunku pracy lub innego stosunku prawnego, w ramach którego wykonywały tę pracę."

[355] Opinia w tej sprawie została omówiona i zamieszczona na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3876.

Opisywany projekt zmian przedstawiono jako część inicjatywy „SprawdzaMY – deregulacja dla Polski". Dotychczas przepisy w ww. zakresie nie zmieniły się – pisemne upoważnienia nadal obowiązują w przedmiotowych ustawach.

Odnosząc się do **zmiany przepisów w ramach tzw. deregulacji, tj. zmian ustawy z dnia 30 maja 2014 r. o prawach konsumenta** (Dz. U. z 2024 r. poz. 1796) **oraz ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców** (Dz. U z 2024 r. poz. 236 ze zm.)[356], zakładającej uchylenie art. 4a ustawy o prawach konsumenta oraz dodanie nowego przepisu w ustawie Prawo przedsiębiorców, organ nadzorczy wskazał, że możliwość ograniczenia realizacji przez administratora obowiązków informacyjnych określonych w art. 13 i 14 RODO uwarunkowana jest koniecznością spełnienia warunków wskazanych w art. 23 RODO. Podkreślił również, że przepis ten nie dopuszcza wyłączenia realizacji wymienionych obowiązków informacyjnych, a stanowi jedynie o możliwym ich ograniczeniu.

Ustawa deregulacyjna, tj. ustawa z 21 maja 2025 r. o zmianie niektórych ustaw w celu deregulacji prawa gospodarczego i administracyjnego oraz doskonalenia zasad opracowywania prawa gospodarczego, która weszła w życie 13 lipca 2025 r., nie zawiera zmian dotyczących ograniczeń obowiązków informacyjnych.

**Propozycja deregulacyjna dotycząca stworzenia cyfrowej bazy danych do weryfikacji dokumentów przez przedsiębiorców i zmiany ustawy – Prawo przedsiębiorców**[357] zakładała stworzenie zdigitalizowanej bazy danych, w tym danych osobowych, obejmującej takie dokumenty, jak: prawa jazdy, dowody osobiste, dyplomy ukończenia studiów, zaświadczenia czy pozwolenia, „umożliwiającej przedsiębiorcom szybki dostęp do weryfikacji dokumentów (…) przy zachowaniu odpowiednich zabezpieczeń dostępu (np. zgoda osoby, której dane dotyczą, przez profil zaufany lub aplikację mObywatel)", w celu ułatwienia procesu zatrudnienia. Projektowano zgromadzenie dużej ilości danych osobowych, odnoszących się do wielu rodzajów dokumentów, zebranych dotąd w różnych i odrębnych rejestrach czy zasobach prowadzonych przez organy/podmioty publiczne. Samo w sobie powoduje to poważne potencjalne ryzyko dla bezpieczeństwa tych danych oraz informacji, w tym ryzyko wykorzystywania przez podmioty komercyjne danych osobowych do innych celów niż te, których realizacji służyłaby baza danych. Prezes UODO w swojej opinii podniósł także, że ustawa wdrażająca proponowane rozwiązanie powinna kompleksowo regulować wszystkie aspekty przetwarzania danych osobowych w ww. bazie danych, zwłaszcza: podmiot (podmioty) odpowiedzialny za prowadzenie bazy danych; zamknięty katalog przetwarzanych danych osobowych i określenie kategorii podmiotów tych danych (osób, których dane dotyczą); cel (cele) przetwarzania danych osobowych; katalog podmiotów, które miałyby mieć dostęp do danych zebranych w bazie oraz zasady uzyskiwania tego dostępu; okres (okresy) przechowywania danych osobowych; tryb aktualizacji i prostowania danych osobowych zebranych w bazie. Nie jest dopuszczalne rozwiązanie, w myśl którego przedsiębiorca miałby nieograniczony i bezwarunkowy dostęp do informacji o każdej osobie fizycznej, której

[356] DPNT.401.140.2025.
[357] DPNT.401.168.2025.

dane osobowe byłyby przetwarzane w projektowanej bazie danych w powiązaniu z informacjami o posiadanych przez tę osobę dokumentach potwierdzających tożsamość, uprawnienia, poziom i kierunek wykształcenia itp. Ponadto dostęp danego podmiotu do zebranych przez organy / podmioty publiczne informacji o konkretnej osobie fizycznej następować powinien po wykazaniu interesu prawnego danego podmiotu do uzyskania takich danych, w trybie wnioskowym.

Prezes UODO nie zakwestionował zmian mających na celu poprawę warunków prowadzenia działalności gospodarczej przez przedsiębiorców proponowanych w **projekcie ustawy o zmianie ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy oraz ustawy o podatku od towarów i usług**[358]. Wskazał natomiast, że doprecyzowania wymagają zasady dostępu do systemu teleinformatycznego i zakres informacji przekazywanej za jego pomocą. Uwagi dotyczyły dostępu do danych w Punkcie Informacji dla Przedsiębiorcy, w tym ich publikacji, a także przekazywania tych danych/wymiany informacji pomiędzy systemami PIP i KAS w zakresie informacji zawartych w wykazie podatników VAT[359]. Ustawa została uchwalona – ustawa z dnia 17 października 2025 r. o zmianie ustawy o CEIDG i PIP oraz ustawy o podatku od towarów i usług. Ustawa została uchwalona i podpisana przez Prezydenta RP[360].

**Projekt ustawy o zmianie ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych oraz ustawy o ewidencji ludności**[361] przewidywał przyznanie uprawnienia weryfikacji zastrzeżenia numeru PESEL przez zakłady ubezpieczeń w zakresie umów ubezpieczenia OC posiadaczy pojazdów mechanicznych, za pośrednictwem systemu teleinformatycznego UFG, który stanowi węzeł informacyjny dla zakładów ubezpieczeń pośredniczący w komunikacji z różnymi rejestrami publicznymi, bez określenia celu dostępu do rejestru i do danych osobowych. Organ nadzorczy wskazywał na niedookreślenie w ustawie o ewidencji ludności szczegółowej regulacji dotyczącej zakresu przetwarzania, w związku z ustawowymi zadaniami i obowiązkami podmiotu żądającego. Związek ten ma wynikać z niezbędności posiadania danych osobowych dla osiągnięcia celu wyznaczonego treścią obowiązku. Projektodawca odsyła wyłącznie do sposobu weryfikacji zastrzeżonego numeru PESEL w sposób ogólny, tymczasem niezbędne wydaje się rozgraniczenie pozycji UFG oraz zakładów ubezpieczeń w procesie dostępu do rejestru zastrzeżeń numerów PESEL. Dodatkowo nie jest jasne, w jaki sposób działa „pośrednictwo systemu obsługującego UFG, który stanowi węzeł informacyjny dla zakładów ubezpieczeń pośredniczący w komunikacji z różnymi rejestrami publicznymi” w kontekście relacji

[358] DPNT.401.210.2025.
[359] Więcej informacji i tekst opinii dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3797.
[360] Dz. U. z 2025 r. poz. 1541.
[361] DPNT.401.165.2025.

tego systemu z rejestrem zastrzeżeń numerów PESEL. Ustawa została uchwalona i podpisana przez Prezydenta RP[362].

### 15.10. Podsumowanie

Przedstawiony powyżej udział organu nadzorczego w procesie stanowienia prawa nie wyczerpuje pełnego katalogu zagadnień legislacyjnych, którymi w 2025 r. zajmował się Urząd Ochrony Danych Osobowych, natomiast wskazuje na wybrane kwestie o charakterze przykładowym, które w ocenie Prezesa UODO mają szczególne znaczenie.

Podejmowane działania dowodzą rosnącego znaczenia i zakresu zaangażowania organu nadzorczego w procesie legislacyjnym, który niekiedy z własnej inicjatywy opiniował nie tylko projekty aktów prawnych *sensu stricto*, lecz także inne dokumenty o istotnym znaczeniu dla funkcjonowania państwa i życia społecznego oraz horyzontalnym wpływie na system regulacyjny, w tym także prawa i wolności osób fizycznych.

Analiza spraw legislacyjnych prowadzonych w 2025 r. pokazuje, że podejmowane działania organu nadzorczego w procesie stanowienia prawa przynoszą pozytywne efekty i stale podnoszą świadomość i odpowiedzialność projektodawców za jakość tworzonego prawa i jego zgodność ze standardami ochrony danych osobowych. Wzrasta także gotowość projektodawców do podejmowania współpracy celem wypracowania rozwiązań zapewniających odpowiedni poziom ochrony danych osobowych.

Z drugiej strony wciąż istotnym problemem pozostaje brak kompleksowego przeglądu obowiązujących regulacji pod kątem ich pełnej zgodności z wymogami zarówno przepisów z zakresu ochrony danych osobowych, jak i nowych unijnych regulacji. Kwestia ta nabiera szczególnego znaczenia w kontekście rosnącej liczby wchodzących w życie cyfrowych aktów unijnych. Złożoność regulacji unijnych, wprowadzających nowe sposoby i cele przetwarzania danych osobowych, wzmaga potrzebę przeglądu regulacji krajowych i podjęcia odpowiednich działań legislacyjnych zmierzających do ustanowienia podstaw prawnych oraz warunków przetwarzania danych osobowych z wykorzystaniem nowych technologii.

Mimo istniejących problemów związanych z zagwarantowaniem ochrony danych osobowych w procesie stanowienia prawa, Prezes UODO – dostrzegając pozytywne zmiany – wyraża nadzieję, że w kolejnych latach nastąpi dalszy wzrost zaangażowania projektodawców w uwzględnienie aspektów związanych z ochroną danych osobowych w procesie legislacyjnym, by poprzez dialog i współpracę móc sprostać postępującej transformacji cyfrowej i jednocześnie zapewnić pełną realizację konstytucyjnych praw jednostki do prywatności.

[362] Dz. U. z 2025 r. poz. 1176.

## 16. Uprzednie konsultacje

Do zadań organu nadzorczego realizowanych przez Wydział Współpracy z Inspektorami Ochrony Danych UODO 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. Efektem takich konsultacji jest udzielenie administratorowi pisemnego zalecenia. Ponadto organ nadzorczy może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58 RODO, tj. np. wydać ostrzeżenie (art. 36 ust. 2 RODO).

Jednocześnie warto podkreślić, że wniosek o przeprowadzenie uprzednich konsultacji powinien spełniać wymogi formalne określone w art. 63 ustawy – Kodeks postępowania administracyjnego (dalej również jako K.p.a.), a także zawierać informacje, o których mowa w art. 36 ust. 3 RODO. Jeśli wniosek nie spełnia ww. wymogów, Prezes UODO informuje wnioskodawcę o nieudzieleniu konsultacji, wskazując przyczyny ich nieudzielenia (art. 57 ust. 3 ustawy o ochronie danych osobowych).

W omawianym okresie sprawozdawczym do Prezesa UODO wpłynęły **4 wnioski o przeprowadzenie uprzednich konsultacji.** W poprzednim roku wpłynęło ich 2, w 2023 – 3, w 2022 – 7, w 2021 i 2020 r. – po 3, w 2019 r. – 5, a w 2018 r. – 2.

W 2025 r. – podobnie jak w poprzednich latach – administratorzy w niewielkim zakresie korzystali z tego uprawnienia. Dodatkowo należy zauważyć, że żadne z postępowań nie zakończyło się udzieleniem zaleceń. Wynikało to przede wszystkim z tego, że administratorzy przed złożeniem takiego wniosku nie dokonali wnikliwej analizy całego planowanego procesu przetwarzania. Zanim bowiem administrator przystąpi do oceny ryzyka, a następnie oceny skutków dla ochrony danych, powinien w pierwszej kolejności prawidłowo ustalić i ocenić zagadnienia o podstawowym znaczeniu dla zgodności przetwarzania danych osobowych z prawem. Są to zwłaszcza: status wnioskodawcy w procesie przetwarzania, kwalifikacja informacji jako danych osobowych oraz istnienie podstawy prawnej do prowadzenia określonych operacji przetwarzania danych osobowych.

Kwestie te mają podstawowe znaczenie i wymagają uprzedniej prawidłowej oceny. Szczególnie ważne jest wcześniejsze przeprowadzenie przez administratorów analizy w zakresie istnienia podstaw prawnych do realizacji planowanego przez nich

procesu przetwarzania danych osobowych. Ich brak 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.

Wniesione w 2025 r. wnioski o uprzednie konsultacje obarczone były brakami, w szczególności nie zawierały wszelkich niezbędnych informacji. W efekcie nie mogły one zainicjować postępowania i udzielenia zaleceń.

Przykładowo jeden z wniosków[363] nie zawierał oceny skutków dla ochrony danych, która jest podstawowym i obowiązkowym elementem wniosku o udzielenie uprzednich konsultacji (art. 36 ust. 3 lit. e RODO).

W innym przypadku przesłany przez szkołę publiczną wniosek o uprzednie konsultacje dotyczący planowanego wdrożenia monitoringu wizyjnego w szatni szkolnej[364] nie zawierał wszystkich informacji, o których mowa w art. 36 ust. 3 lit. d i e RODO. Brak było też – mimo takich zapowiedzi – danych kontaktowych wyznaczonego IOD. Ponadto przedłożona przez administratora ocena skutków dla ochrony danych nie zawierała wszystkich niezbędnych informacji, o których mowa w art. 35 RODO. Przede wszystkim nie został przedstawiony regulamin monitoringu przestrzeni szatni szkolnej, który określałby np.: liczbę i sposób usytuowania kamer, funkcjonowanie samego sytemu (wyłącznie podgląd w czasie rzeczywistym czy rejestracja zapisu), sposób zabezpieczenia danych, zasady ich udostępniania, a także okres przechowywania danych. W ocenie skutków dla ochrony danych nie wykazano też, jak administrator zamierza osiągnąć cel monitoringu, jakim zgodnie z przepisami Prawa oświatowego może być zapewnienie bezpieczeństwa uczniom i pracownikom lub ochrona mienia, w sytuacji kiedy system monitoringu uniemożliwia rozpoznawanie twarzy. Nie zostały przedstawione argumenty świadczące o tym, że zastosowanie monitoringu w szatni jest środkiem niezbędnym dla zapewnienia bezpieczeństwa uczniom w szatni szkolnej, przeciwdziałania zachowaniom agresywnym czy też kradzieży odzieży i obuwia, skoro zastosowana technika uniemożliwia rozpoznanie twarzy. Tym samym nie było jasne, w jaki sposób monitoring w szatni miałby przyczynić się do ograniczenia czy wyeliminowania wymienionych zjawisk i zapewnienia bezpieczeństwa. Administrator nie wykazał również, że wprowadzenie monitoringu w szatni uzgodnił z organem prowadzącym szkołę, nie wskazał też czy przeprowadzono konsultacje z radą pedagogiczną, radą rodziców i samorządem uczniowskim. A zatem, czy spełnione zostały wymogi, przewidziane w przepisach prawa dla prowadzenia planowanych operacji przetwarzania.

Kolejny wniosek o uprzednie konsultacje[365] również obarczony był brakami, które uniemożliwiły dalsze jego procedowanie. Dotyczył on planowanego wprowadzenia nowej usługi – aplikacji umożliwiającej przechowywanie, przeglądanie i udostępnianie zdjęć. W tym przypadku braki polegały na niespełnieniu wymogów określonych w przepisach prawa, zwłaszcza w art. 36 ust. 3 oraz w art. 63 § 1 K.p.a. Odnosząc się

[363] DPNT.5100.1.2025.
[364] DPNT.5100.2.2025.
[365] DPNT.5100.4.2025.

do wymogów określonych w K.p.a., organ nadzorczy poinformował, że wniosek o uprzednie konsultacje należy złożyć za pośrednictwem Elektronicznej Skrzynki Podawczej UODO[366]. Adres poczty email: kancelaria@uodo.gov.pl nie służy do składania podań (w tym wniosków o uprzednie konsultacje) w rozumieniu przepisów K.p.a. Wniosek nie został podpisany przez wszystkich wspólników spółki cywilnej jako administratorów planowanego procesu przetwarzania danych osobowych. Dodatkowo powyższy wniosek o przeprowadzenie uprzednich konsultacji nie zawierał wszystkich informacji, o których mowa w art. 36 ust. 3 RODO. Przede wszystkim administrator nie określił dokładnie obowiązków poszczególnych podmiotów uczestniczących w planowanym procesie przetwarzania danych. Z przedstawionego wniosku nie wynikało, jak w planowanym procesie przetwarzania kształtują się obowiązki poszczególnych administratorów i podmiotów przetwarzających, a także czy administrator przeprowadził analizę pod kątem zapewnienia przez podmioty uczestniczące w planowanym procesie przetwarzania danych wystarczających gwarancji ochrony dla podmiotów danych, a także czy administrator właściwie ocenił spełnienie przez niego warunków legalności przekazywania danych do państw trzecich. Kolejną przeszkodą do udzielenia konsultacji było to, że nieprawidłowo przeprowadzona została również ocena skutków dla ochrony danych. Przede wszystkim nie został dokładnie określony opis operacji przetwarzania, nie wskazano precyzyjnie podstawy przetwarzania danych szczególnej kategorii, niejasny był sposób szacowania ryzyka dla praw i wolności osób fizycznych, nie zawarto środków planowanych w celu zaradzenia ryzyku, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych, administrator nie zasięgnął opinii osób, których dane dotyczą, w sprawie zamierzonego przetwarzania.

Inny z wniosków złożonych w trybie uprzednich konsultacji dotyczył wątpliwości odnoszących się do zakresu danych, jakie powinny zostać udostępnione przez organ publiczny w postępowaniu wszczętym na skutek wniosku złożonego w trybie ustawy o dostępie do informacji publicznej[367]. W odpowiedzi na ten wniosek organ nadzorczy poinformował, że tego rodzaju wątpliwości powinny być rozstrzygane na podstawie właściwych przepisów regulujących tego typu kwestie, nie zaś w trybie uruchamianym na podstawie art. 36 RODO. Przede wszystkim należy mieć na uwadze, że o udostępnieniu informacji lub o odmowie ich udostępnienia na podstawie wniosku o dostęp do informacji publicznej każdorazowo, w określonym stanie faktycznym i prawnym, rozstrzyga podmiot zobowiązany do udostępnienia informacji publicznej. W razie odmowy udostępnienia informacji wnioskodawca może się zwrócić ze skargą do sądu administracyjnego (art. 21 ustawy o dostępie do informacji publicznej). Organ nadzorczy wskazał ponadto, że procedura uprzednich konsultacji została ustanowiona w innym celu niż rozstrzyganie wątpliwości co do istnienia podstaw prawnych przetwarzania, w tym udostępnienia danych osobowych. Procedura ta ma bowiem zastosowanie wówczas, gdy planowana operacja przetwarzania danych, tj. planowany proces, w którym przetwarzane są dane osobowe (np. wprowadzenie w organizacji

[366] Informacje w tym zakresie dostępne są pod linkiem: https://www.uodo.gov.pl/pl/p/kontakt.
[367] DPNT.5100.3.2025.

nowej technologii, wprowadzenie nowej usługi), budzi wątpliwości administratora w zakresie środków, jakie powinien zastosować w celu zminimalizowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, jakie może mieć miejsce podczas takiego przetwarzania.

**Podsumowując część sprawozdania dotyczącą wniosków o uprzednie konsultacje** zauważyć można, że mimo upływu kilku lat od wprowadzenia tej procedury niewiele podmiotów z niej korzysta. Dodatkowo można też wywnioskować, że w wielu przypadkach podmioty te nie do końca są świadome, w jakich przypadkach należy z niej skorzystać. Dlatego powołując się na art. 36 RODO, przesyłają pytania dotyczące możliwości udostępnienia danych osobowych albo też przedkładają projekty, z realizacją których związane jest przetwarzanie danych osobowych. Natomiast nie analizują wcześniej, na jakiej podstawie prawnej dane te będą przetwarzane lub nie przeprowadzają oceny skutków dla ochrony danych, która powinna być dokonana przed rozpoczęciem procedury uprzednich konsultacji.

Odpowiadając na takie wnioski, organ nadzorczy informuje o nieudzieleniu uprzednich konsultacji oraz o powodach ich nieudzielenia. Dzięki wskazywaniu powodów nieudzielenia konsultacji, w tym tego, jakie działania należy podjąć przed złożeniem takiego wniosku, administratorzy mogą ponownie przyjrzeć się planowanemu przedsięwzięciu i dokonać jego analizy pod kątem ochrony danych osobowych, w tym wskazać postawę prawną czy też prawidłowo przeprowadzić ocenę skutków dla ochrony danych.

## 17. Kodeksy postępowania i monitorowanie ich przestrzegania

Na mocy art. 40 RODO wprowadzony został instrument prawny w postaci kodeksu postępowania. Jest to dobrowolne narzędzie, dzięki któremu administratorzy lub podmioty przetwarzające mogą wykazać zgodność (rozliczalność)[368]. **Kodeks postępowania ma pomóc we właściwym stosowaniu RODO – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw**[369].

Jak przewidziano w niewyczerpującym wykazie zawartym w art. 40 ust. 2 RODO, kodeksy postępowania mogą obejmować w szczególności takie zagadnienia, jak:

- rzetelne i przejrzyste przetwarzanie;
- prawnie uzasadnione interesy realizowane przez administratorów w określonych kontekstach;
- zbieranie danych osobowych;
- pseudonimizacja danych osobowych;
- informowanie osób fizycznych i wykonywanie przysługujących tym osobom praw;

[368] Por.: art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. e RODO.
[369] Art. 40 ust. 1 RODO.

- informowanie i ochrona dzieci (w tym sposoby pozyskiwania zgody rodziców);
- środki techniczne i organizacyjne, w tym ochrona danych już w fazie projektowania i domyślna ochrona danych, a także środki bezpieczeństwa;
- zgłaszanie naruszeń;
- przekazywanie danych poza UE, lub
- tryby rozstrzygania sporów[370].

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[371] w tym zakresie.

**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**[372] oraz **kryteria dopuszczalności**, o których mowa w Wytycznych EROD 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679[373]. Na tym etapie Prezes UODO ocenia m.in. następujące kwestie: czy wniosek o zatwierdzenie kodeksu złożył podmiot do tego uprawniony, czy z treści kodeksu jasno wynika, do jakich administratorów lub podmiotów przetwarzających skierowany jest kodeks i jakich czynności przetwarzania dotyczy, czy kodeks zawiera propozycje mechanizmów umożliwiających monitorowanie przestrzegania jego przepisów przez administratorów lub podmioty przetwarzające, którzy będą go stosować, a w przypadku kodeksu skierowanego do podmiotów prywatnych – czy został wskazany w kodeksie podmiot monitorujący. Organ nadzorczy weryfikuje również, czy zostały przeprowadzone, i w odpowiednim zakresie, konsultacje publiczne projektu kodeksu[374], a dowodem na ich przeprowadzenie może być złożony przez wnioskodawcę np. raport, zawierający opis ich przebiegu i odpowiednie podsumowanie. Po zakończeniu tego etapu oceny, jeśli wniosek lub projekt kodeksu wymaga uzupełnień, organ nadzorczy kieruje do wnioskodawcy pismo, wskazując braki i 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**[375]. Etap ten służy wyjaśnieniu treści projektu z wnioskodawcą,

---

[370] Pkt 8 Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.
[371] Por. art. 7 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
[372] Art. 40 RODO, art. 27 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, art. 63 i nast. Kodeksu postępowania administracyjnego (Dz.U. z 2025 r. poz. 1691).
[373] Dalej: Wytyczne EROD 1/2019, zob. Pkt 19-31 Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.
[374] Por.: motyw 99 RODO, art. 27 ust. 2-4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
[375] Pkt 32-41 Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.

umożliwiając mu wprowadzenie ewentualnych modyfikacji. Prezes UODO ocenia, w jaki sposób kodeks przyczyni się do właściwego stosowania RODO, tzn. czy: zaspokaja określoną potrzebę danego sektora dokonującego przetwarzania lub danej czynności przetwarzania, ułatwia stosowanie RODO, doprecyzowuje stosowanie RODO, zapewnia wystarczające zabezpieczenia oraz zapewnia skuteczne mechanizmy monitorowania przestrzegania kodeksu[376]. Ten etap kończy się wydaniem przez organ nadzorczy **opinii o zgodności przedłożonego projektu z przepisami RODO**, albo o braku takiej zgodności. W przypadku projektu kodeksu postępowania skierowanego do podmiotów prywatnych wydanie przez organ nadzorczy pozytywnej opinii o zgodności jego treści z RODO, albo czas tuż przed wydaniem takiej opinii, **to właściwy moment na złożenie wniosku o akredytację przez podmiot monitorujący**[377], który ma prowadzić monitorowanie przestrzegania postanowień kodeksu przez jego przyszłych członków.

Ostatni etap postępowania ws. zatwierdzenia kodeksu postępowania obejmuje **zatwierdzenie kodeksu postępowania w formie decyzji administracyjnej**, o ile organ nadzorczy uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO. Odmowa zatwierdzenia kodeksu również następuje w tej samej formie.

Zatwierdzone kodeksy postępowania są następnie rejestrowane przez Prezesa UODO i EROD. Tę samą, opisaną powyżej procedurę zatwierdzenia projektu kodeksu, stosuje się do zmiany zatwierdzonego kodeksu postępowania lub jego rozszerzenia.

### 17.1. Kodeksy postępowania zatwierdzone przez organ nadzorczy

24 listopada 2025 r. Prezes UODO zatwierdził „**Kodeks postępowania dotyczący przetwarzania danych osobowych przez prywatne agencje badawcze”**[378]. Twórcą kodeksu jest Związek Pracodawców Organizacja Firm Badania Opinii i Rynku (OFBOR) – jedyne w Polsce stowarzyszenie pracodawców skupiające prywatne agencje badawcze. Tego samego dnia Prezes UODO udzielił akredytacji Omni Modo sp. z o.o., która jest podmiotem monitorującym stosowanie tego kodeksu. Następnego dnia odbyło się uroczyste wręczenie decyzji ws. zatwierdzenia kodeksu postępowania oraz certyfikatu akredytacyjnego dla podmiotu monitorującego. Relacja z tego wydarzenia oraz treść kodeksu dostępna są na stronie internetowej Urzędu Ochrony Danych Osobowych w zakładce Aktualności[379] oraz w zakładce Zatwierdzone kodeksy postępowania[380].

Zagadnieniom uregulowanym w ww. kodeksie zostały poświęcone dwa artykuły zamieszczone w kolejnych wydaniach **Biuletynu UODO**[381]: „**Lista Robinsona” –**

[376] Pkt 32 Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.
[377] Por.: art. 41 RODO, art. 29 i nast. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
[378] DOL.4421.2.2020.
[379] https://uodo.gov.pl/pl/138/3979.
[380] https://uodo.gov.pl/pl/426/1110.
[381] Biuletyny dostępne na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

**narzędzie z kodeksu postępowania dla prywatnych agencji badania opinii i rynku”** (Biuletyn UODO nr 1/26) oraz **„Sygnatariusze kodeksu postępowania dla prywatnych agencji badania opinii i rynku muszą powołać IOD”** (Biuletyn UODO nr 2/26).

**Warto wspomnieć, że od chwili rozpoczęcia stosowania RODO Prezes UODO zatwierdził 3 kodeksy postępowania**[382]. To tyle samo, co organy nadzorcze w Niemczech i Hiszpanii, a więcej niż np. we Francji[383]. Oprócz wspomnianego powyżej kodeksu dla prywatnych agencji badania opinii i rynku, decyzją polskiego organu nadzorczego w poprzednich latach zostały zatwierdzone:

- w 2022 r. **„Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych”** – twórca kodeksu: Porozumienie Zielonogórskie; akredytowany podmiot monitorujący: RS Jamano spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie,
- w 2023 r. „**Kodeks postępowania dla sektora ochrony zdrowia”** – twórca kodeksu: Polska Federacja Szpitali; akredytowany podmiot monitorujący: KPMG Advisory spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie.

### 17.2. Nowe wnioski o ztwierdzenie lub zmianę kodeksów postępowania

W sierpniu 2025 r. Krajowy Cech Fotografów z siedzibą w Katowicach złożył do Prezesa UODO wniosek o zatwierdzenie **„Kodeksu postępowania RODO dla Fotografów”**[384]. Organ nadzorczy przeprowadził ocenę formalną, w tym w zakresie spełnienia kryteriów dopuszczalności wniosku i projektu kodeksu postępowania.

W październiku 2025 r. wpłynął do Prezesa UODO wniosek Federacji Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie" **w sprawie zmian w zatwierdzonym w 2022 r. „Kodeksie postępowania dotyczącym ochrony danych osobowych przetwarzanych w małych placówkach medycznych”**[385]. Wniosek poprzedziły spotkania pracowników UODO z przedstawicielami wnioskodawcy, w czasie których przedyskutowano zakres projektowanych zmian w kodeksie i omówiono procedurę związaną ze zmianą kodeksu postępowania.

### 17.3. Postępowania prowadzone w 2025 r. w sprawie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone we wcześniejszych latach

W okresie sprawozdawczym 2025 r. kontynuowane były postępowania w sprawie zatwierdzenia „**Kodeksu postępowania Krajowej Izby Doradców Podatkowych**

[382] https://uodo.gov.pl/pl/426/1110.
[383] Por. rejestr EROD https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_pl, dostęp 13 marca 2026 r.
[384] DPNT.4421.1.2025.
[385] DPNT.4421.2.2025.

**w sprawie ochrony danych osobowych”**[386]. Podmiot ten w 2025 r. przedstawił nową wersję kodeksu postępowania, uwzględniającą uwagi organu nadzorczego zgłoszone w 2024 r. W celu jej omówienia w październiku 2025 r. odbyło się spotkanie z przedstawicielami twórcy kodeksu. W czasie spotkania pracownicy UODO przedstawili uwagi do nowych postanowień projektu kodeksu oraz wskazali kierunki dalszych, niezbędnych zmian. Poprawiona wersja kodeksu oczekiwana jest w 2026 r.

W 2025 r. trwała również ocena merytoryczna (kryteria zatwierdzenia kodeksu) projektu **„Kodeksu postępowania dla sektora handlu wydanego zgodnie z art. 40 RODO dotyczącego podmiotów prowadzących centra handlowe”**[387] – wnioskodawcą w sprawie jest Polska Rada Centrów Handlowych.

Na etapie oceny merytorycznej jest również projekt **„Kodeksu postępowania i dobrych praktyk w sprawie danych osobowych w branży hotelarskiej”,** którego twórcą jest Izba Gospodarcza Hotelarstwa Polskiego[388].

W 2025 roku została zakończona ocena formalna projektu **„Kodeksu postępowania i dobrych praktyk w zakresie przetwarzania danych osobowych w branży reklamy internetowej”**[389], którego twórcą jest Związek Pracodawców Branży Internetowej Interactive Advertising Bureau Polska. Wniosek o zatwierdzenie tego kodeksu wpłynął do Prezesa UODO pod koniec 2024 r. W 2025 r. organ nadzorczy rozpoczął ocenę projektu tego kodeksu pod kątem spełnienia kryteriów zatwierdzenia kodeksu.

Informacje na temat wszystkich trwających postępowań w sprawie zatwierdzenia kodeksów postępowania dostępne są na stronie internetowej UODO[390].

### 17.4. Wspieranie branż w pracy nad kodeksami postępowania

Prezes UODO informuje również za pośrednictwem strony internetowej UODO[391] o zgłoszonych mu inicjatywach pracujących nad kodeksami postępowania:

- **Kodeks postępowania z danymi osobowymi w jednostkach samorządu terytorialnego** (Związek Województw RP i Instytut Szkoleniowo – Doradczy z Łodzi)[392]. Warto przypomnieć, że w 2024 r. w UODO odbyły się liczne spotkania z organizacjami reprezentującymi poszczególne jednostki samorządu terytorialnego, w tym z przedstawicielami Związku Województw RP, o czym więcej w Biuletynie UODO Wydanie podwójne (grudzień - styczeń 2024/2025)[393], w artykule „UODO zachęca jednostki samorządu terytorialnego do opracowania kodeksu postępowania”;

[386] DOL.4421.1.2020.
[387] DOL.4421.3.2020.
[388] DOL.4421.1.2023.
[389] DOL.4421.2.2024 .
[390] https://uodo.gov.pl/pl/426/1109.
[391] https://uodo.gov.pl/pl/426/2790.
[392] DOL.4420.1.2024.
[393] https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

- **Kodeks postępowania w sądach powszechnych, obejmujący czynności niewchodzące w zakres wymiaru sprawiedliwości** (grupa inspektorów ochrony danych z sądów apelacyjnych i okręgowych)[394]. Warto w tym miejscu wspomnieć o Zarządzeniu Ministra Sprawiedliwości z 23 grudnia 2024 r. w sprawie powołania stałego Zespołu do spraw ochrony danych osobowych w sądach powszechnych[395]. Jednym z celów prac tego zespołu jest podjęcie działań zmierzających do opracowania projektu kodeksu postępowania (w ozumieniu art. 40 RODO) dla sądów powszechnych;
- **Kodeks postępowania dla branży badań medycznych** (INFARMA Związek Pracodawców Innowacyjnych Firm Farmaceutycznych)[396]. Prezes UODO za pośrednictwem strony internetowej (https://uodo.gov.pl/pl/138/3722) informował o rozpoczęciu procesu konsultacji publicznych projektu tego kodeksu;
- **Kodeks postępowania dotyczący ochrony danych osobowych w sektorze organizacji pozarządowych** (grupa organizacji pozarządowych pod przewodnictwem Fundacji Onkologicznej ALIVIA)[397]. Prezes UODO za pośrednictwem strony internetowej (https://uodo.gov.pl/pl/138/3612) informował o spotkaniu organizacji pozarządowych ws. utworzenia kodeksu postępowania RODO dla trzeciego sektora.

### 17.5. Wspieranie branż planujących pracę nad kodeksami postępowania

W 2025 r. w UODO odbyło się spotkanie z inicjatywą planującą prace nad kodeksem postępowania dla portów lotniczych - **Polskimi Portami Lotniczymi i Związkiem Regionalnych Portów Lotniczych**[398]. Przyszli twórcy kodeksu wskazali konkretne zagadnienia, które planują uregulować w kodeksie, omówiono szereg zagadnień praktycznych. Informacja w tym zakresie dostępna jest na stronie internetowej UODO[399]. Należy wspomnieć, że w lutym 2026 r. ww. podmioty podpisały list intencyjny w sprawie opracowania branżowego Kodeksu postępowania w zakresie ochrony danych osobowych dla podmiotów zarządzających infrastrukturą lotniskową[400].

W 2025 r. pracownicy UODO spotkali się także z **przedstawicielami branży wyrobów medycznych** (Organizacją Pracodawców Przemysłu Medycznego TECHNOMED; Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych; Polskim Centrum Badań i Certyfikacji)[401]. Uczestnicy spotkania dyskutowali nad koniecznością zapewnienia zgodności z przepisami ochrony danych osobowych certyfikowanych wyrobów medycznych, za pomocą

[394] DOL.4420.1.2022.
[395] Dz.Urz.MS z 2024 r. poz. 292.
[396] DOL.4420.1.2021.
[397] DOL.4420.3.2024.
[398] DPNT.4420.1.2025.
[399] https://uodo.gov.pl/pl/138/3502.
[400] https://www.polish-airports.com/pl/aktualnosci/0/562/szczegoly.html.
[401] https://uodo.gov.pl/pl/138/3799.

których będą przetwarzane dane osobowe. Omówiono problemy z tym związane, rozważano możliwość wykorzystania w tym celu narzędzi zgodności określonych w RODO, przede wszystkim kodeksów postępowania. Ustalono, że konieczne jest dalsze kontytuowanie wspólnych spotkań[402].

### 17.6. Działania zachęcające do pracy nad kodeksami postępowania

W 2025 roku Prezes UODO podejmował liczne działania zachęcające do opracowywania kodeksów postępowania:

- przedstawiciele UODO uczestniczyli w spotkaniu **„Cyberbezpieczeństwo danych osobowych”**, którego organizatorem było **Ministerstwo Spraw Wewnętrznych i Administracji**[403]. Tematem wydarzenia były zagadnienia odnoszące się do cyberbezpieczeństwa i działań podejmowanych dla urealniania ochrony danych osobowych zakładów opieki zdrowotnej MSWiA, jak również omówienie potencjału, jaki wniósłby dla nich dedykowany ich działalności kodeks postępowania;
- Prezes UODO zwrócił się do Ministra Zdrowia o rozważenie możliwości dokonania zmian legislacyjnych, w wyniku których podmioty medyczne stosujące kodeksy postępowania albo posiadające certyfikaty w rozumieniu RODO mogłyby uzyskać **dodatkowe punkty przy kontraktowaniu usług z NFZ**[404];
- w ramach konferencji szkoleniowo-metodycznej pt. „Bezpieczne dane dzieci i młodzieży oraz nowe kierunki rozwoju w obszarze kultury fizycznej. Jak sprostać współczesnym wyzwaniom?”, która była częścią obchodów 60-lecia Krakowskiego Szkolnego Ośrodka Sportowego im. Szarych Szeregów, przedstawiciel UODO omówił temat **„Kodeks dobrych praktyk czy Kodeks postępowania? Korzyści kodeksu postępowania w rozumieniu RODO”**[405];
- w Olsztynie, w ramach ogólnopolskiej inicjatywy „UODO rusza w kraj”, której celem jest wzmacnianie świadomości społecznej w zakresie ochrony danych osobowych i odpowiedzialnego korzystania z nowych technologii, zostało zaprezentowane m.in. zagadnienie **„Kodeks postępowania dla podmiotów publicznych i zapewnienie realizacji obowiązków w zakresie ochrony danych osobowych w ramach kontroli zarządczej w jednostkach sektora finansów publicznych**”[406];
- w 2025 r. została przygotowana **ulotka promująca kodeksy postępowania**, która zawiera najważniejsze informacje na temat tego narzędzia zgodności z RODO. Skondensowana treść tego materiału ma wyjaśnić administratorom i podmiotom przetwarzającym, czym jest kodeks postępowania i jakie korzyści

[402] DPNT.4420.2.2025.
[403] https://uodo.gov.pl/pl/138/3800.
[404] DPNT.413.22.2025; informacja w tej sprawie oraz treść pisma dostępne na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/138/3823.
[405] Informacje na ten temat dostępne pod linkami: https://uodo.gov.pl/pl/531/3896; https://uodo.gov.pl/pl/531/3922.
[406] Więcej w informacji dostępnej pod linkiem https://uodo.gov.pl/pl/601/3928.

wynikają z formalnego stosowania kodeksu, a tym samym zachęcać sektory do prac nad kodeksami i przystępowania do kodeksów;

- prowadzenie na stronie internetowej UODO **zakładki Kodeksy postępowania**[407], która dotyczy następujących zagadnień: Podstawowe informacje; Procedura zatwierdzania kodeksu krajowego; Procedura zatwierdzania kodeksu europejskiego; Kodeks jako narzędzie międzynarodowych transferów danych; Mechanizmy monitorowania kodeksów; Wymogi akredytacji podmiotów monitorujących kodeksy; Błędy najczęściej popełniane podczas przygotowania kodeksu; Organizacje pracujące nad kodeksami; Wnioski o zatwierdzenie kodeksów; Zatwierdzone kodeksy postępowania; Wykaz podmiotów akredytowanych.

Warto odnotować, że złożone do organu nadzorczego wnioski o zatwierdzenie projektów kodeksów postępowania, ale też sygnały od inicjatyw, które rozpoczynają prace związane z opracowaniem kodeksu, wskazują, że wciąż jest dostrzegana potrzeba i zalety korzystania z tego typu narzędzia, które pozwala wykazać rozliczalność, o której mowa w art. 5 ust. 2 RODO. Zaletą odpowiednio przygotowanego kodeksu jest nie tylko gwarancja pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy, ale także nadzór nad procesami przetwarzania danych osobowych realizowanymi przez administratorów lub podmioty przetwarzające z sektora prywatnego (do których ma zastosowanie zatwierdzony kodeks) przez akredytowany przez Prezesa UODO podmiot monitorujący.

Należy także zauważyć, że w 2025 r. na żadnego z członków zatwierdzonego kodeksu postępowania nie wpłynęła skarga do Prezesa UODO. Ponadto warto zwrócić uwagę na decyzję Prezesa UODO, w której organ nadzorczy uznał przystąpienie przez administratora, u którego doszło do naruszenia ochrony danych osobowych, do kodeksu postępowania za „inny czynnik łagodzący” (art. 83 ust. 2 lit. k RODO), dzięki któremu obniżono administracyjną karę pieniężną[408].

### 17.7. 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

[407] https://uodo.gov.pl/pl/426.
[408] Prezes UODO uznał tak, mimo że przystąpienie do kodeksu miało miejsce już po ustaniu stanu naruszenia i w czasie trwania postępowania prowadzonego przez Prezesa UODO; patrz decyzja Prezesa UODO z 4 lipca 2025 r. (DKN.5131.17.2022) dostępna pod linkiem https://orzeczenia.uodo.gov.pl/document/urn:ndoc:gov:pl:uodo:2022:dkn_5131_17/content?query=.

opisane w „**Wymogach akredytacji podmiotów monitorujących kodeksy postępowania”**[409] (dalej jako: Wymogi akredytacji).

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[410].

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

### 17.7.1. Wnioski o udzielenie akredytacji do monitorowania kodeksów postępowania. Akredytacje udzielone przez organ nadzorczy

W 2025 r. do organu nadzorczego wpłynął wniosek **Omni Modo Sp. z o.o. z siedzibą w Warszawie** o udzielenie akredytacji do monitorowania przestrzegania „Kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencje badawcze” (OFBOR)[411]. Po przeprowadzonej przez Prezesa UODO ocenie formalnej i merytorycznej wniosku 24 listopada 2025 r. polski organ nadzorczy udzielił akredytacji ww. podmiotowi i wpisał go do wykazu[412] prowadzonego na podstawie art. 33 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Informacja dotycząca uroczystego wręczenia certyfikatu akredytacyjnego[413] dla Omni Modo Sp. z o.o. i decyzji w przedmiocie zatwierdzenia kodeksu dla OFBOR dostępna jest na stronie internetowej UODO[414]. Podczas tego spotkania przedstawiciele obu ww. podmiotów podzielili się swoimi doświadczeniami nt. przebiegu prac związanych z opracowywaniem treści kodeksu i procedur, na podstawie których będzie działał podmiot go monitorujący.

---

[409] 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.

[410] Pkt 88 Wytycznych EROD 1/2019 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_pl.

[411] DPNT.420.1.2025.

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

[413] Zob. art. 31 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

[414] https://uodo.gov.pl/pl/138/3979.

### 17.7.2. Współpraca z podmiotami monitorującymi akredytowanymi w 2022 i 2023

Zasady komunikacji akredytowanego podmiotu monitorującego z Prezesem UODO wynikają z § 3 pkt 6 wspomnianych Wymogów akredytacji. Akredytowany podmiot monitorujący składa roczne sprawozdanie do organu nadzorczego o wszelkich działaniach prowadzonych przez niego w odniesieniu do kodeksu postępowania.

Na początku 2025 r., zgodnie z obowiązującymi je terminami, akredytowane w latach 2022 i 2023 przez Prezesa UODO podmioty monitorujące złożyły sprawozdania ze swojej działalności w 2024 r.:

- RS Jamano spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie – dla „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych" (Porozumienie Zielonogórskie)[415];
- KPMG Advisory spółka z ograniczoną odpowiedzialnością spółka komandytowa z siedzibą w Warszawie – dla „Kodeksu postępowania dla sektora ochrony zdrowia" (Polska Federacja Szpitali)[416].

## 17.8. Podsumowanie

**Wszystkie podmioty, które chciałyby opracować kodeks postępowania powinny dobrze zaplanować działania w tym zakresie** – przede wszystkim ważne jest ustalenie, jakie są oczekiwania administratorów lub podmiotów przetwarzających co do zagadnień, które mogłyby zostać uregulowane w takim kodeksie. Zgodnie ze stanowiskiem EROD cyt.: „Twórcy kodeksów muszą wykazać, że istnieje potrzeba ustanowienia kodeksu. Kodeks jako taki musi odnosić się do problemów z ochroną danych, które pojawiają się w danym sektorze lub w przypadku określonej czynności przetwarzania"[417].

Kodeks postępowania musi więc obejmować konkretne rozwiązania w zakresie przetwarzania danych osobowych oparte na przepisach RODO i mających zastosowanie przepisach branżowych (art. 40 ust. 2 RODO), ale także mechanizm monitorowania przestrzegania kodeksu przez jego członków, w tym określenie podmiotu monitorującego (podmiotów monitorujących) w przypadku gdy będą mogły do niego przystąpić podmioty z sektora prywatnego (art. 40 ust. 4 RODO).

Pomimo że to od decyzji danego sektora (branży) zależy treść kodeksu postępowania, opracowując jego projekt, twórcy takiego dokumentu muszą mieć na uwadze kryteria dopuszczalności i kryteria zatwierdzenia, o których mowa w Wytycznych 1/2019 EROD. Istotne jest, aby kodeksy postępowania ułatwiały stosowanie RODO i go doprecyzowywały, tzn. przewidywały konkretne rozwiązania w zakresie obowiązków administratorów lub podmiotów przetwarzających (np. opisywały

[415] DPNT.423.1.2025.
[416] DPNT.423.2.2025.
[417] Pkt 33 Wytycznych EROD 1/2019.

sposób weryfikacji osób, których dane dotyczą, w ramach procedury realizacji praw osób; określały okres retencji danych osobowych albo wskazywały warunki jego określenia; wskazywały zasady weryfikacji podmiotów przetwarzających) czy wzory niezbędnych dokumentów (np. klauzul informacyjnych, formularzy zgód na przetwarzanie danych osobowych, wzory umów powierzenia), a nie były tylko kopią przepisów RODO.

Projektując mechanizm monitorowania twórcy kodeksu powinni poszukiwać wskazówek w Wytycznych EROD 1/2019, ale także w zatwierdzonych przez Prezesa UODO Wymogach akredytacji[418]. Wymogi akredytacji formułują warunki, których spełnienie przez podmiot monitorujący oceniane jest dopiero w postępowaniu akredytacyjnym, ale znajomość treści wymogów pozwoli we właściwy sposób określić mechanizm monitorowania w kodeksie postępowania.

Twórcy kodeksów postępowania powinni mieć też na uwadze pozostałe wytyczne EROD[419], a z doświadczenia polskiego organu nadzorczego wynika, że nie jest to zasadą. Tak jak już zostało to wskazane powyżej punktem wyjściowym są Wytyczne EROD 1/2019[420], które zawierają ramy opracowywania kodeksów postępowania, ale nie można również zapominać o wytycznych EROD odnoszących się do realizacji konkretnych obowiązków administratorów lub podmiotów przetwarzających wynikających z RODO, np. wytycznych dotyczących pojęć administratora i podmiotu przetwarzającego[421], wytycznych dotyczących prawa dostępu[422] czy wytycznych dotyczących zgłaszania naruszeń ochrony danych[423]. Należy mieć również na uwadze ciągle obowiązujące wytyczne Grupy Roboczej Art. 29, w szczególności te dotyczące przejrzystości[424]. **Istotne jest zatem, aby kodeksy we właściwy sposób uwzględniały odpowiednie opinie i stanowiska opublikowane lub zatwierdzone przez EROD**.

Kodeksy postępowania muszą również uwzględniać orzecznictwo krajowe i europejskie, jeśli wiąże się ono z przetwarzaniem danych osobowych w danym sektorze, i którego będzie dotyczył kodeks postępowania.

Mając na uwadze dotychczasowe doświadczenia ze współpracy ze środowiskami pracującymi nad kodeksami postępowania, a także z prowadzonych postępowań ws. zatwierdzenia kodeksów postępowania, Prezes UODO dostrzega potrzebę podejmowania stale działań informacyjno-edukacyjnych w celu zachęcania do opracowywania kolejnych kodeksów postępowania. Warto podkreślić, że kodeksy postępowania mogą obejmować m.in. zagadnienia dotyczące środków i procedur,

---

418 https://uodo.gov.pl/pl/426/2788.
419 https://www.edpb.europa.eu/our-work-tools/documents/our-documents_pl?f%5B0%5D=all_publication_type%3A64.
420 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_pl.
421 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_pl.
422 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_pl.
423 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_pl.
424 https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_pl.pdf.

o których mowa w art. 24 i 25 RODO, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32 RODO, co jest niezwykle istotne w związku z coraz popularniejszym zastosowaniem sztucznej inteligencji oraz innych nowych technologii. Nie można bowiem zapominać, że kodeksy postępowania mają pomóc we właściwym stosowaniu RODO z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania. W ocenie EROD i EIOD cyt.: „bezpieczeństwo na mocy RODO wiąże się z ryzykiem dla podstawowych praw i wolności osób fizycznych. Chociaż definicja prawna cyberbezpieczeństwa w prawie Unii zasadniczo obejmuje ochronę użytkowników i innych osób, zakres środków w zakresie cyberbezpieczeństwa zazwyczaj obejmuje wszelkiego rodzaju ryzyko dla danej organizacji. Nadal istnieje możliwość ustanowienia synergii, tak aby ocena ryzyka mogła uwzględniać ochronę praw i wolności osób fizycznych”[425].

## 18. Pytania dotyczące wykładni prawa, wnioski o dostęp do informacji

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.

### 18.1. Pytania dotyczące wykładni prawa

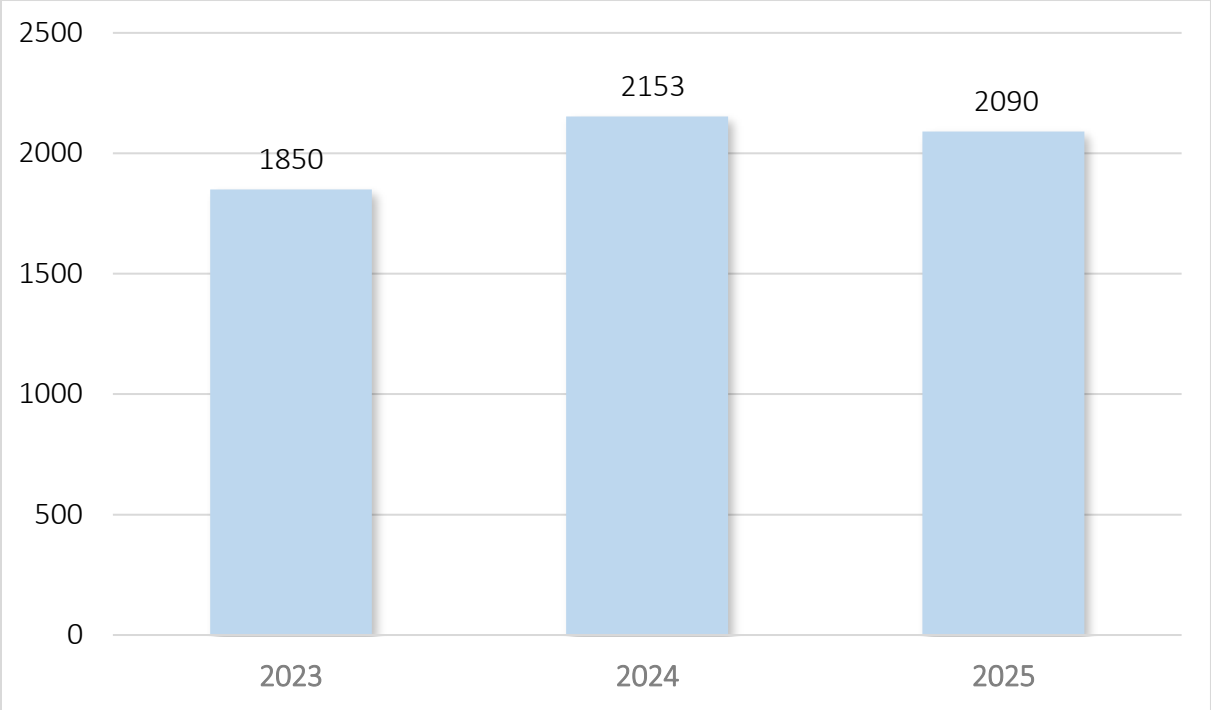
W związku z wpływającymi do Prezesa UODO pytaniami organ nadzorczy informuje osoby, których dane dotyczą, o prawach przysługujących im na mocy RODO, zaś administratorom i podmiotom przetwarzającym udziela kierunkowych wskazówek, co do ich obowiązków w zakresie ochrony danych osobowych. W wyjaśnieniach 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 2025 **administratorzy oraz osoby fizyczne** skierowali do Urzędu Ochrony Danych Osobowych **1815** pism z **pytaniami prawnymi**, zaś **218** pism wpłynęły od **inspektorów ochrony danych**. Ponadto w 2025 r. do Prezesa UODO

[425] Pkt 36 Wspólnej opinia EROD i EIOD 4/2026 w sprawie wniosku dotyczącego ustawy o cyberbezpieczeństwie 2 i wniosku dotyczącego zmian w dyrektywie NIS 2 (tłumaczenie maszynowe) https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-42026-proposal_en.

wpłynęło **57** zapytań **organów nadzorczych z innych państw**[426]. Zatem **w sumie** w 2025 r. do Prezesa UODO wpłynęło **2090 pytań prawnych**.




**Wykres 16:** Liczba pytań dotyczących wykładni prawa, które wpłynęły do Prezesa UODO w latach 2023–2025.

Nieznaczne zmniejszenie liczby wpływających pytań może być spowodowane tym, że wiele kwestii zostało już przez organ nadzorczy wyjaśnionych, np. w komunikatach zamieszczonych na stronie internetowej Urzędu czy w „Biuletynie UODO". Część zainteresowanych korzysta też z pomocy Infolinii UODO czy punktów konsultacyjnych uruchamianych przez organ m.in. podczas uczestnictwa w różnego rodzaju przedsięwzięciach organizowanych w całej Polsce.

Zauważyć też można, że mniej jest ogólnych pytań o interpretację RODO, a rośnie liczba tych, które wymagają **analizy ustaw sektorowych** w kontekście zgodności z unijnymi standardami ochrony danych osobowych.

Podkreślić również należy, że kierowane do Prezesa UODO pytania bywają coraz bardziej złożone, zwłaszcza gdy **odnoszą się kwestii związanych z przetwarzaniem danych osobowych przy użyciu nowoczesnych rozwiązań informatycznych**.

W roku 2025 rozpatrzonych zostało **1846 pism z pytaniami od administratorów oraz osób fizycznych.**

Osobną grupę spraw stanowiły pytania od inspektorów ochrony danych (IOD), do których organ nadzorczy – biorąc pod uwagę niezwykle ważną rolę, jaką osoby wykonujące tę funkcję mają pełnić w systemie ochrony danych osobowych – podchodzi ze szczególną uwagą. W 2025 r. do Prezesa UODO wpłynęło **218 pytań**

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

od inspektorów ochrony danych (IOD). Odpowiedzi udzielono na 236 pytań od IOD. W poprzednich latach takich pytań wpłynęło: w 2024 r – 233, a w 2023 r. – 253.

### 18.1.1. Pytania od administratorów i osób fizycznych

Zakres tematyczny zagadnień poruszanych w pytaniach prawnych od administratorów i osób fizycznych dotyczył różnych aspektów przetwarzania danych osobowych oraz stosowania nie tylko RODO, ale także innych, szczególnych przepisów prawa. Zarówno podmioty z sektora publicznego, jak i prywatnego oraz osoby fizyczne zgłaszały wątpliwości dotyczące takich kwestii, jak:

1. przetwarzanie danych przez pracodawców i związki zawodowe,
2. stosowanie monitoringu wizyjnego i nagrywanie rozmów,
3. przetwarzanie danych biometrycznych,
4. udostępniania i pozyskiwania danych zawartych w dokumentacji medycznej,
5. przetwarzanie danych w związku ze świadczeniem pomocy społecznej,
6. ochrona danych osobowych w sektorze administracji publicznej,
7. przetwarzanie danych osobowych dzieci i małoletnich,
8. obowiązki związane z wyznaczeniem i zapewnieniem niezależności inspektora ochrony danych,
9. inne.

**Ad 1. Przetwarzanie danych przez pracodawców i związki zawodowe**

Przetwarzanie **danych osobowych w stosunkach pracy i przez związki zawodowe** to zagadnienia, które co roku podnoszone są w pytaniach kierowanych do Prezesa UODO.

1) **Delegowanie kierowców**

Jedno z nich dotyczyło np. stosowania art. 12 ust. 5 ustawy z dnia 28 lipca 2023 r. o delegowaniu kierowców w transporcie drogowym i związanego z nim **obowiązku przetwarzania danych zawartych w zgłoszeniu delegowania kierowcy w sposób niezautomatyzowany**[427]. Pytano, czy możliwe byłoby zastosowanie elektronicznego oprogramowania służącego do obsługi tego typu zgłoszeń. W odpowiedzi organ nadzorczy wskazał, że powołany przepis nie dopuszcza możliwości przetwarzania zgłoszeń delegowania kierowcy na terytorium Rzeczypospolitej Polskiej z państwa trzeciego w sposób, który można by uznać za zautomatyzowany. Zaznaczył, że wprowadzenie jakiekolwiek formy zautomatyzowanego przetwarzania tych danych (niezależnie czy całkowicie, czy częściowo), w tym elektronicznego oprogramowania służącego do takiej obsługi wpływających zgłoszeń delegowania kierowców, musiałoby zostać poprzedzone odpowiednią nowelizacją ustawy o delegowaniu kierowców w transporcie drogowym.

2) **Udostępnianie danych osobowych**

Inne z pytań dotyczyło możliwości **udostępnienia przez pracodawcę informacji o wysokości wynagrodzeń na poszczególnych stanowiskach**

[427] DPNT.023.542.2025.

**organizacji związkowej działającej przy pracodawcy**[428]. W odpowiedzi organ nadzorczy wskazał, że każdy wniosek o udostępnienie danych osobowych powinien być należycie uzasadniony, tak aby administrator nie miał wątpliwości, o jakie dane chodzi i w jakim celu będą one wykorzystane. Organizacja związkowa, zwracając się o udostępnienie na jej rzecz danych dotyczących jej członków, powinna powołać się na ustawę o związkach zawodowych[429], a nie na ustawę o dostępie do informacji publicznej[430], i wskazać na cele wynikające z przepisów regulujących jej działalność. Zaniechanie takiego trybu może czynić niemożliwą ze strony pracodawcy (administratora) ocenę takiego wniosku o dane osobowe. Zgodnie zatem z art. 28 ust. 1 pkt 1-4 ustawy o związkach zawodowych pracodawca jest obowiązany udzielić na wniosek zakładowej organizacji związkowej informacji niezbędnych do prowadzenia działalności związkowej, w szczególności informacji dotyczących: warunków pracy i zasad wynagradzania; działalności i sytuacji ekonomicznej pracodawcy związanych z zatrudnieniem oraz przewidywanych w tym zakresie zmian; stanu, struktury i przewidywanych zmian zatrudnienia oraz działań mających na celu utrzymanie poziomu zatrudnienia; działań, które mogą powodować istotne zmiany w organizacji pracy lub podstawach zatrudnienia. Jeśli chodzi o ocenę tego, jakie informacje mogą mieścić się w zasadach wynagradzania, to cenną wskazówkę interpretacyjną może stanowić wyrok Sądu Apelacyjnego w Białymstoku z 25 czerwca 2014 r.[431], w którym sąd ten orzekł, że przez pojęcie „informacji o zasadach wynagradzania" nie można rozumieć tylko informacji o przepisach regulujących kształtowanie wynagrodzeń, które przecież ze swej istoty są jawne i powszechnie dostępne. Informacja o zasadach wynagradzania obejmuje dane o konkretnie występujących w zakładzie pracy zjawiskach gospodarczych, o jego sytuacji finansowej, określonych funduszach, w tym zwłaszcza funduszu płac, czy nawet informacje o wysokości wynagrodzeń określonej grupy zawodowej lub o kształtowaniu się wynagrodzeń na określonych rodzajach stanowisk. Informacja „o zasadach wynagradzania" z natury rzeczy musi zawierać pewien stopień ogólności, jest więc czymś innym niż informacja o wysokości wynagrodzenia indywidualnego pracownika. Dla realizacji ustawowych i statutowych zadań związku zawodowego co do zasady wystarczające jest pozyskanie informacji przetworzonych w postaci danych statystycznych dotyczących zasad wynagradzania poszczególnych grup pracowników.

W 2025 r. Prezes UODO proszony był też o **ocenę odmowy udostępnienia organizacji związkowej danych osobowych pracowników w celu przeprowadzenia wyborów społecznego inspektora pracy**[432]. W udzielonych wyjaśnieniach wskazał, że obowiązki pracodawcy w zakresie współpracy ze związkami zawodowymi regulują przepisy ustawy o związkach zawodowych. Zgodnie z jej art. 28 ust. 1 pracodawca jest obowiązany udzielić na wniosek zakładowej

[428] DPNT.023.663.2025.
[429] Ustawa z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2025 r. poz. 440).
[430] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).
[431] Sygn. akt III AUa 2078/13.
[432] DPNT.023.868.2025.

organizacji związkowej informacji niezbędnych do prowadzenia działalności związkowej, w szczególności informacji dotyczących: 1) warunków pracy i zasad wynagradzania, 2) działalności i sytuacji ekonomicznej pracodawcy związanych z zatrudnieniem oraz przewidywanych w tym zakresie zmian, 3) stanu, struktury i przewidywanych zmian zatrudnienia oraz działań mających na celu utrzymanie poziomu zatrudnienia, 4) działań, które mogą powodować istotne zmiany w organizacji pracy lub podstawach zatrudnienia. Pracodawca udziela zakładowej organizacji związkowej powyższych informacji w terminie 30 dni od dnia otrzymania wniosku (art. 28 ust. 2). W świetle zaś art. 6 ust. 6 ustawy o społecznej inspekcji pracy[433] wybory społecznego inspektora pracy przeprowadza zakładowa organizacja związkowa na podstawie uchwalonego przez siebie regulaminu. Jeśli zatem dane osobowe pracowników są niezbędne organizacji związkowej do prowadzenia działalności związkowej i związanego z nią wyboru społecznego inspektora pracy, to pracodawca ma obowiązek przekazać żądane informacje. Takie działanie powinno jednocześnie znaleźć oparcie w przesłance przetwarzania danych z art. 6 ust. 1 RODO. To podmiot występujący o dane osobowe ma obowiązek uzasadnić niezbędność pozyskania danych osobowych w określonym celu, a także wskazać podstawę prawną, aby administrator mógł ocenić, czy takie udostępnienie danych nie naruszy praw i wolności osób, których te dane dotyczą.

Kolejne z pytań dotyczyło **legalności udostępniania danych pracowników tymczasowych na rzecz pracodawcy**[434]. W związku z nim Prezes UODO wyjaśnił, że dla oceny legalności udostępniania danych pracowników tymczasowych na rzecz pracodawcy użytkownika podstawowe znaczenie mają przepisy: ustawy o zatrudnianiu pracowników tymczasowych[435], ustawy o warunkach dopuszczalności powierzania pracy cudzoziemcom na terytorium Rzeczypospolitej Polskiej[436], Kodeksu pracy[437] w powiązaniu z zasadami przetwarzania danych osobowych określonymi w RODO.

Stosownie do art. 17 ust. 1 pkt 10 ustawy o warunkach dopuszczalności powierzania pracy cudzoziemcom na terytorium Rzeczypospolitej Polskiej agencja pracy tymczasowej (jako podmiot powierzający pracę cudzoziemcowi) na wniosek pracodawcy użytkownika przekazuje mu kopię zezwolenia na pracę dotyczącego pracownika tymczasowego. Ponadto, zgodnie z art. 32 ust. 2 tej ustawy, w zezwoleniu na pracę cudzoziemca w charakterze pracownika tymczasowego jest określany pracodawca użytkownik. Jednocześnie pracodawca użytkownik nie jest uznawany za pracodawcę w rozumieniu Kodeksu pracy (art. 2 pkt 1 ustawy o zatrudnianiu pracowników tymczasowych), a przepisy ustawy o zatrudnianiu pracowników tymczasowych wskazują wprost, że pracodawcą dla pracowników tymczasowych są

[433] Ustawa z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy (Dz. U. z 2015, poz. 567 ze zm.).
[434] DPNT.023.1122.2025.
[435] Ustawa z dnia 9 lipca 2003 r. o zatrudnianiu pracowników tymczasowych (Dz. U. z 2025 r. poz. 236 ze zm.).
[436] Ustawa z dnia 20 marca 2025 r. o warunkach dopuszczalności powierzania pracy cudzoziemcom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 621), dalej cytowana jako „ustawa o warunkach dopuszczalności".
[437] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2025 r. poz. 277 ze zm.).

agencje pracy. To także te przepisy określają zakres obowiązków, zarówno pracodawcy, czyli agencji pracy tymczasowej, jak i pracodawcy użytkownika. Te uprawnienia nie są tożsame, ale skoro są ustalone ustawowo, to pozyskiwanie zgody pracownika czy opieranie się na przesłance uzasadnionego interesu dla legalności pozyskania danych osobowych pracowników tymczasowych przez pracodawcę użytkownika może stanowić próbę obejścia przepisów prawa. Należy zatem pamiętać, że ostatecznie to administrator odpowiada za zachowanie zasad ochrony danych osobowych, m.in. legalizmu, i wykazanie ich przestrzegania (art. 5 ust. 2 RODO). Zgodnie jednak z Wytycznymi EROD 1/2024[438] art. 6 ust. 1 lit. f RODO nie powinien być również postrzegany przez administratorów jako preferowany wariant, a jego stosowanie nie powinno być nadmiernie rozszerzane w celu obejścia szczególnych wymogów prawnych ponieważ byłoby uznawane za mniej restrykcyjne niż inne podstawy prawne określone w art. 6 ust. 1 RODO.

W kontekście opisanych w piśmie sytuacji należy zauważyć, że zasady przetwarzania danych odnoszą się do wszystkich danych osobowych, niezależnie od formy, w jakiej są przechowywane. Dlatego w sytuacji kopiowania określonego dokumentu zawierającego dane osobowe należy sprawdzić, czy nie dochodzi do pozyskania danych osobowych w zakresie szerszym niż dopuszczalny w świetle przepisów prawa[439].

Jeden z przewoźników kolejowych zwrócił się z prośbą o wskazanie, czy dopuszczalna jest **wymiana informacji o czasie pracy maszynisty między przewoźnikami**[440]. Takie działanie umożliwiłoby pracodawcom lub zleceniodawcom kontrolowanie łącznego czasu pracy maszynisty, aby uniknąć przekroczenia dopuszczalnych norm.

W odpowiedzi organ nadzorczy wskazał, że związku z sygnalizowanymi mu problemami w stosowaniu przepisów ustawy o transporcie kolejowym[441] w zakresie kontroli łącznego czasu pracy maszynistów sprawowanej przez przewoźników kolejowych wystąpił[442] do Ministra Infrastruktury z wnioskiem o podjęcie działań legislacyjnych prowadzących do zmiany ww. przepisów celem dostosowania ich do zasad ochrony danych osobowych określonych w art. 5 RODO[443]. W swoim piśmie podniósł, że przepisy ustawy o transporcie kolejowym w sposób jednoznaczny

[438] Zob. Wytyczne 1/2024 Europejskiej Rady Ochrony Danych w sprawie przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. f https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en

[439] Tak NSA w wyrokach z 13 czerwca 2019 r. (sygn. akt I OSK 1715/17) czy z 20 kwietnia 2021 r. (sygn. akt III OSK 161/21). Warto też wskazać stanowisko sądu z uzasadnienia prawomocnego wyroku WSA w Warszawie z 24 maja 2024 r. (sygn. akt II SA/Wa 1788/23): „utrwalenie danych osobowych poprzez wykonanie skanu dowodu tożsamości jest legalne wyłącznie wtedy, gdy taki obowiązek nakłada na bank przepis rangi ustawy".

[440] DPNT.023.1287.2025.

[441] Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234 ze zm.).

[442] Zgodnie z art. 52 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych może występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

[443] DPNT.413.36.2025.

i konkretny określają, komu i w jaki sposób (kiedy i przez podanie jakich danych) maszynista składa oświadczenia związane z jego czasem pracy (art. 22ca) i wyraźnie określają, komu to oświadczenie może być przekazane przez przewoźnika (art. 22ca ust. 4). W związku z takim ukształtowaniem normatywnym, jedynie maszynista został zobowiązany do niezwłocznego poinformowania przewoźnika kolejowego lub zarządcy, na rzecz których świadczy pracę lub usługi, w drodze pisemnego oświadczenia, informacji o swoim czasie pracy. Przepisy wskazują następnie na przekazywanie tych oświadczeń Prezesowi UTK przez przewoźnika kolejowego lub zarządcę. Nie przewidują one natomiast przekazywania przez przewoźnika informacji o czasie pracy maszynisty do innych przewoźników. Podkreślić zatem należy, że tego rodzaju przetwarzanie, w tym udostępnianie danych o czasie pracy maszynistów pomiędzy różnymi przewoźnikami zatrudniającymi tę samą osobę możliwe byłoby jedynie, gdyby istniała ku temu podstawa prawna w postaci przepisów prawa, do których nie zaliczają się akty takie jak np. rekomendacje. Obecnie Prezes UODO oczekuje na podjęcie przez ministerstwo stosownych działań[444], co nie wyłącza zasadności sygnalizowania resortowi także przez stosujących wskazane przepisy potrzeby ich zmian. Organ ochrony danych osobowych nie posiada bowiem inicjatywy legislacyjnej.

3) **Postępowanie z dokumentacją pracowniczą**

Państwowa Inspekcja Pracy zwróciła się z prośbą o wskazanie sposobu postępowania z nadesłaną do niej dokumentacją pracowniczą nieistniejącego już podmiotu (wykreślony z KRS) w związku m.in. z nieskuteczną próbą zdania dokumentów do archiwum państwowego[445]. Organ nadzorczy w odpowiedzi wskazał, że nie ma kompetencji do oceny, czy Naczelny Dyrektor Archiwów Państwowych prawidłowo ocenił przesłanki określone w art. 51z ust. 1 ustawy z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[446], który stanowi, że Naczelny Dyrektor Archiwów Państwowych może wydać decyzję nakazującą złożenie dokumentacji, która należała do pracodawcy wykreślonego z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, na odpłatne przechowywanie we wskazanym archiwum państwowym, jeżeli istnieje zagrożenie jej zniszczenia, w szczególności na skutek oddziaływania czynników atmosferycznych lub bezprawnego działania osób trzecich, a brak jest podstaw prawnych do jej przekazania innemu podmiotowi do dalszego przechowywania.

Zaznaczył jednak, że mając na uwadze okoliczności przedstawionej sprawy, pewne wskazówki interpretacyjne płyną z orzecznictwa sądów administracyjnych. Np. w wyroku WSA w Warszawie z 12 listopada 2020 r.[447] analizowana była sprawa porzuconej dokumentacji pracowniczej (osobowej i płacowej), w której posiadanie wszedł Zakład Ubezpieczeń Społecznych. Dokumentacja należała do zlikwidowanej

[444] W odpowiedzi na wystąpienie przekazane 8.10.2025 r. Ministerstwo Infrastruktury zadeklarowało, że „Departament Kolejnictwa przeanalizuje zakres wymaganej prawnie interwencji legislacyjnej i podejmie stosowne działania".
[445] DPNT.023.1062.2025.
[446] Dz. U. z 2020 r. poz. 164.
[447] Sygn. akt II SA/Wa 365/20, LEX nr 3100711.

Fotograficznej Spółdzielni Pracy. ZUS wystąpił do Naczelnego Dyrektora Archiwów Państwowych o wszczęcie z urzędu postępowania administracyjnego w przedmiocie nakazania złożenia dokumentacji w postaci akt osobowych pracowników, kart wynagrodzeń oraz list płac pozostałych po zlikwidowanej FSP w trybie art. 51z ust. 1 ustawy o narodowym zasobie archiwalnym i archiwach. Dyrektor początkowo wydał postanowienie o braku przesłanek wszczęcia postępowania na podstawie art. 61a K.p.a., które to postanowienie zostało uchylone przez sąd administracyjny, a następnie wydał decyzję w której odmówił złożenia dokumentacji osobowej i płacowej Fotograficznej Spółdzielni Pracy na odpłatne przechowywanie w archiwum państwowym. ZUS zaskarżył decyzję organu do sądu administracyjnego, zarzucając m.in. naruszenie art. 51z ust. 1 ustawy o narodowym zasobie archiwalnym i archiwach, poprzez jego niezastosowanie w sprawie w wyniku błędnego ustalenia, że nie została spełniona przesłanka wykreślenia Fotograficznej Spółdzielni Pracy "(...)" z Krajowego Rejestru Sądowego. ZUS nie posiadał interesu prawnego, lecz wyłącznie interes faktyczny w złożeniu dokumentacji pracowniczej do archiwum. Ponadto do wykreślenia pracodawcy z rejestru doszło również z mocy prawa, gdyż nie było prowadzone postępowanie likwidacyjne, przez co w jego imieniu nie działał organ reprezentujący (likwidator, zarząd). W uzasadnieniu wyroku uchylającego decyzję odmowną Dyrektora sąd administracyjny wskazał, że przepis art. 51z ust. 1 ustawy o narodowym zasobie archiwalnym i archiwach reguluje sytuację, w której pracodawca wytworzył podlegającą przechowywaniu przez określony czas dokumentację pracowniczą, a przed upływem tego czasu został wykreślony z rejestru lub ewidencji i nie wywiązał się z obowiązku zapewnienia przechowywania tej dokumentacji do końca przewidzianego przez prawo okresu jej przechowywania. Tym samym regulacja ta odnosi się do wyjątkowej sytuacji, w której pracodawca przed wykreśleniem z rejestru lub ewidencji, a więc w czasie kiedy funkcjonował jeszcze jako podmiot prawa, nie zapewnił dalszego przechowywania wytworzonych dokumentów pracowniczych. W takiej sytuacji przepis ten przewiduje uprawnienie Naczelnego Dyrektora Archiwów Państwowych do wydania – w ramach uznania administracyjnego – decyzji nakazującej złożenie dokumentacji wytworzonej przez takiego pracodawcę na odpłatne przechowywanie we wskazanym archiwum państwowym.

### Ad. 2. Stosowanie monitoringu wizyjnego i nagrywanie rozmów

Sporo wpływających pytań odnosiło się do legalności stosowania kamer w różnych instytucjach (szkołach, szpitalach) oraz w przestrzeni miejskiej, a także nagrywania rozmów telefonicznych (m.in. przez straż miejską czy urzędy gmin.)

#### 1) Kamery w podmiotach leczniczych

Odpowiadając na pytanie zespołu opieki zdrowotnej o **legalność stosowania monitoringu wizyjnego w podmiotach leczniczych**[448] Prezes UODO poinformował, że problematyka ta była w ostatnim czasie przedmiotem wystąpienia do Ministra

[448] DPNT.023.265.2025.

Zdrowia[449], w którym organ nadzorczy wyraził wątpliwości co do zgodności aktualnych regulacji dotyczących stosowania monitoringu wizyjnego, przewidzianych w ustawie o działalności leczniczej, z przepisami RODO i wniósł o rozważenie podjęcia działań w celu doprecyzowania tych przepisów.

Jednocześnie zwrócił uwagę pytającego, że analizę legalności przetwarzania danych osobowych w przypadku stosowania monitoringu wizyjnego każdorazowo powinien w pierwszej kolejności przeprowadzić inspektor ochrony danych (IOD), którego powołanie w podmiotach publicznych zgodnie z art. 37 ust. 1 lit. a RODO jest obligatoryjne. Administrator ma zarówno obowiązek zorganizowania bezpieczeństwa procesu przetwarzania danych osobowych, w sposób odpowiadający przepisom obowiązującym w zakresie przetwarzania danych osobowych, jak i prawo dokonania tego w taki sposób, który będzie odpowiadał zagrożeniom oraz kategoriom przetwarzanych danych. Tak więc to on decyduje i odpowiada za powyższe i za przetwarzanie danych zgodnie z prawem. Co ważne, administrator ma obowiązek przeprowadzić analizę ryzyka dla wprowadzenia technologii monitoringu, która wiąże się ze szczególną ingerencją w sferę praw jednostki, jak również wykazać, że wprowadzane regulacje pozostają w zgodzie z przepisami prawa pracy.

**2) Udostępnianie obrazu z kamer monitoringu w trybie bieżącego podglądu**

Część pytań związana była z możliwością udostępnienia przez podmiot prowadzący monitoring obrazu z kamer w trybie podglądu w czasie rzeczywistym innym podmiotom.

Przykładowo prezydent jednego z miast pytał, czy możliwe jest udostępnienie **obrazu z kamer miejskiego monitoringu wizyjnego placówce Żandarmerii Wojskowej w trybie bieżącego podglądu** i czy Żandarmeria Wojskowa może występować w takim przypadku w roli podmiotu przetwarzającego[450]. W odpowiedzi Prezes UODO wskazał, że organy administracji publicznej są zobowiązane działać w granicach i na podstawie obowiązujących przepisów prawa regulujących ich działalność. Zgodnie z zasadą rozliczalności, wyrażoną w art. 5 ust. 2 RODO, administrator jest zobowiązany wykazać, że przetwarzanie danych jest zgodne z przepisami RODO i odbywa się z poszanowaniem zasad wyrażonych w jego art. 5 ust. 1. Zgodnie zaś z art. 6 ust. 1 RODO przetwarzanie jest zgodne z prawem m.in. wtedy, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (lit. c) lub gdy jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (lit. e). Jednocześnie zaznaczył, że umowa powierzenia, o której mowa w RODO, nie może przyznawać nowych uprawnień organom, których kompetencje i zakres działania zostały określone w ustawach. W związku z powyższym kwestię udostępnienia przez prezydenta miasta (jako administratora) obrazu z kamer miejskiego monitoringu wizyjnego placówce Żandarmerii Wojskowej

[449] DOL.413.13.2024; opisane i zamieszczone na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/file/5192.
[450] DPNT.023.1172.2025.

w trybie bieżącego podglądu należy rozpatrywać w kontekście zadań administratorów określonych w przepisach ustawowych. Podstawa prawna do przetwarzania danych osobowych za pomocą monitoringu prowadzonego w miejscach publicznych na terenie gminy wynika z ustawy o samorządzie gminnym[451], w tym jej art. 9a. Z kolei ustawa o Żandarmerii Wojskowej i wojskowych organach podatkowych[452] określa zakres działania i organizację Żandarmerii Wojskowej oraz uprawnienia i obowiązki jej żołnierzy. Jako zadania Żandarmerii Wojskowej (art. 4) wymienia m.in.: zapewnianie przestrzegania dyscypliny wojskowej; ochranianie porządku publicznego na terenach i obiektach jednostek wojskowych oraz w miejscach publicznych; ochranianie życia i zdrowia ludzi oraz mienia wojskowego przed zamachami naruszającymi te dobra. Stanowi ponadto, że Żandarmeria Wojskowa wykonuje zadania należące do jej zakresu działania w Siłach Zbrojnych oraz w stosunku do określonych osób, m.in. żołnierzy pełniących czynną służbę wojskową; żołnierzy niebędących w czynnej służbie wojskowej w czasie noszenia przez nich mundurów oraz odznak i oznak wojskowych; żołnierzy w aktywnej rezerwie podczas pełnienia przez nich służby; osób niebędących żołnierzami, jeżeli współdziałają z osobami, o których mowa w pkt. 1-5, w popełnieniu czynu zabronionego przez ustawę pod groźbą kary albo też jeżeli dokonują czynów zagrażających dyscyplinie wojskowej albo czynów przeciwko życiu lub zdrowiu żołnierza albo mieniu wojskowemu (art. 3 ust. 1 w zw. z ust. 2). Żandarmeria Wojskowa nie jest zatem właściwa do kontrolowania osób cywilnych, których dotyczy monitoring prowadzony przez gminę w celu poprawy ich bezpieczeństwa i bezpieczeństwa publicznego.

Z podobnymi wątpliwościami, bo dotyczącymi **możliwości przyznania dostępu do monitoringu miejskiego w drodze teletransmisji jednostkom policji,** zwracali się przedstawiciele innych jednostek samorządu terytorialnego[453]. Prezes UODO, po przeanalizowaniu przepisów sektorowych wskazał m.in., że gmina mogłaby udostępnić dane z monitoringu jedynie wówczas, gdyby taką sytuację przewidywał (zezwalał na to) przepis prawa o randze ustawowej. Tymczasem brak jest jakiejkolwiek normy prawnej, która przewidywałaby możliwość stałego udostępniania przez jednostki samorządu terytorialnego monitoringu miejskiego organom ścigania. Także przepisy ustawy z dnia 6 kwietnia 1990 r. o Policji nie dają podstaw do prowadzenia przez organy ścigania stałego, systematycznego nadzoru – w ramach współprowadzenia monitoringu miejskiego (gminnego). Nie uprawniają też policji do stosowania monitoringu stałego o charakterze i zakresie analogicznym do monitoringu gminnego. Zaznaczył, że analogiczne uwagi odnoszą się do sytuacji, gdy monitorowania przestrzeni publicznej dokonuje straż gminna na podstawie art. 11 ust. 2 ustawy z 29 sierpnia 1997 r. o strażach gminnych[454].

[451] Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153 ze zm.).
[452] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach podatkowych (Dz. U. z 2025 r. poz. 12 ze zm.).
[453] DPNT.023.645.2025; DPNT.023.655.2025.
[454] Sprawa ta została szczegółowo opisana w Biuletynie UODO nr 09/09/25.

### 3) Nagrywanie rozmów telefonicznych

Kolejna grupa spraw analizowanych w 2025 r. związana była z możliwością nagrywania rozmów.

O dopuszczalność takiego działania w kontaktach **z dzwoniącymi interesantami** pytał np. pewien urząd gminy[455]. W odpowiedzi Prezes UODO wskazał, że należy odróżnić dwa rodzaje sytuacji – taką, w której organ działa w toku postępowania administracyjnego (np. podatkowego), realizując przysługujące mu władztwo administracyjne, np. zbierając materiał dowodowy w sposób dopuszczony przepisami prawa i pozostałe sytuacje, gdy takich czynności nie prowadzi. W odniesieniu do przetwarzania danych osobowych za pomocą telefonu (czy innych podobnych urządzeń) w toku prowadzonych postępowań zauważyć należy, że RODO jest aktem o charakterze ogólnym, zatem wszędzie tam, gdzie obowiązują przepisy szczegółowe przewidujące przetwarzanie danych w ten sposób, będą one miały zastosowanie. Zaznaczył, że w kontekście treści pytania należy wziąć pod uwagę art. 6 ust. 1 lit. c oraz lit. e RODO, zgodnie z którym przetwarzanie danych jest dopuszczalne, jeśli jest to niezbędne dla wypełnienia obowiązku prawnego ciążącego na administratorze. Jednocześnie podkreślił, że podstawa przetwarzania danych przez organy władzy publicznej powinna być określona w prawie UE lub w prawie polskim, stosownie do wymagań art. 6 ust. 3 RODO. Odesłał też do zamieszczonego w Biuletynie UODO Nr 11/11/2023 materiału dotyczącego nagrywania rozmów telefonicznych z interesantami.

Do stanowiska tego odwoływała się również odpowiedź na pytanie dotyczące kwestii **utrwalania rozmów w ramach Krajowego Systemu Zarządzania Ruchem Drogowym**[456]. Prezes UODO przypomniał, że nagrywanie przez administratora z sektora publicznego rozmów telefonicznych z interesantami, w czasie których dochodzi do przetwarzania danych osobowych, powinno odbywać się na podstawie przepisów prawa. Administratorzy tacy, podejmując działania w celu realizacji przypisanych im kompetencji, przetwarzając dane w jakikolwiek sposób, powinni działać z zachowaniem przesłanek określonych w art. 6 ust. 1 lit. c lub e RODO. Art. 6 ust. 3 RODO uściśla, że wskazana podstawa przetwarzania powinna być niezbędna i określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator oraz precyzyjnie regulować różne aspekty takiego przetwarzania (np. okresy przechowywania danych). Organ nadzorczy zaznaczył, że ustawa o drogach publicznych[457] nie zawiera regulacji uprawniających administratora danych w ramach funkcjonowania Punktu Informacji Drogowej (dalej „PID") do rejestrowania rozmów telefonicznych i określających cel takiego przetwarzania. Zasady funkcjonowania PID ustalone zostały w „Regulaminie Organizacyjnym PID" stanowiącym załącznik do zarządzenia Nr 4 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 11 lutego 2019 r. w sprawie organizacji Punktu Informacji Drogowej oraz zasad gromadzenia i przekazywania informacji o warunkach ruchu na drogach krajowych (§ 4 ust. 1

[455] DPNT.023.421.2025.
[456] DPNT.023.679.2025.
[457] Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889).

zarządzenia). Z powyższego wynika, że regulacje dotyczące PID nie opierają się na przepisach ustawy o drogach publicznych, lecz wyłącznie na aktach prawnych administracyjnych o charakterze wewnętrznym, które nie są uznawane za źródło prawa z punktu widzenia podstaw prawnych działania administratora realizującego zadania publiczne. Trybunał Sprawiedliwości Unii Europejskiej w wielu wyrokach zajął stanowisko, zgodnie z którym wszelkie ograniczenia w korzystaniu przez jednostkę z praw podstawowych, w tym gwarantowanych w art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej praw do poszanowania życia prywatnego i ochrony danych osobowych, muszą być zgodnie z art. 52 ust. 1 Karty, być przewidziane ustawą i szanować zasadę proporcjonalności. Jednocześnie uregulowania prawne dotyczące tych ograniczeń powinny zawierać jasne i precyzyjne zasady normujące zakres i stosowanie tych ograniczeń[458]. W odniesieniu natomiast do pytania o dopuszczalność nagrywania rozmów telefonicznych z uwagi na weryfikację zachowania operatora podczas rozmowy, zwłaszcza w kontekście oceny tego zachowania w związku z wniesioną skargą, należy mieć na uwadze przede wszystkim przepisy z zakresu prawa pracy. Monitorowanie pracowników powinno odbywać się zgodnie z art. 22[3] § 4 Kodeksu pracy, jeżeli zastosowanie tej formy monitoringu jest konieczne do realizacji celów w postaci: niezbędności zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy, w sposób nienaruszający dóbr osobistych pracownika. Przepis ten nie przewiduje natomiast przesłanek w postaci kontroli zachowania operatora w kontakcie z rozmówcą, sprawdzenia jakości udzielonej przez niego odpowiedzi czy też gromadzenia materiału w perspektywie udzielenia odpowiedzi na przyszłą ewentualną skargę.

Odnośnie zaś do przesłanki zgody podmiotu danych (osoby dokonującej zgłoszenia) na nagrywanie rozmów telefonicznych i przetwarzanie jej danych zauważyć należy, że warunkiem skuteczności takiej zgody jest istnienie równowagi między osobą, której dane dotyczą, a administratorem (motyw 43 RODO). Zgodnie bowiem z tym rozporządzeniem zgoda powinna być dobrowolna, świadoma i osoba, której dane dotyczą, ma prawo ją odwołać bez negatywnych konsekwencji (motyw 42 oraz art. 4 pkt 11 i art. 7 RODO). W kontekście administratora z sektora publicznego wykazanie spełnienia takich warunków zgody wymagałoby szczegółowego uzasadnienia i dodatkowych analiz.

Prezes UODO pytany też był o **dopuszczalność rejestrowania przez straż miejską rozmów telefonicznych z osobami dokonującymi zgłoszeń**[459]. Wskazał, że organy publiczne co do zasady nie powinny powoływać się na zgodę jako podstawę przetwarzania danych ze względu na wyraźny brak równowagi w stosunkach między administratorem będącym organem wykonującym władzą publiczną a osobą, której dane dotyczą. Prawnie uzasadniony interes administratora, o którym mowa w art. 6 ust. 1 lit. f RODO, nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań,

[458] Wyrok z 22 czerwca 2021 r., Latvijas Republikas Saeima, sygn. akt C- 439/19 (pkt 105); wyrok z 16 lipca 2020 r., Facebook Ireland i Schrems, sygn. akt C-311/18 (pkt. 172–176).
[459] DPNT.023.620.2025.

bowiem podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca. Komendant straży miejskiej (gminnej) niewątpliwie jest organem publicznym, a straż samorządowa umundurowaną formacją tworzoną przez radę gminy. W obowiązującym prawie brak jest przepisów zezwalających na rejestrację rozmów telefonicznych przez staż gminną (miejską). Jednocześnie telefon alarmowy straży gminnej (miejskiej) to 986 i nie jest on objęty regulacjami ustawy o systemie powiadamiania ratunkowego[460]. System powiadamiania ratunkowego składa się z centrów powiadamiania ratunkowego tworzących jednolity system do obsługi zgłoszeń alarmowych, kierowanych do numerów alarmowych 112, 997 i 998, umożliwiający przekazanie zgłoszenia alarmowego w celu zaangażowania właściwych zasobów ratowniczych (art. 3 ust. 2 ustawy). W ramach systemu mogą być obsługiwane numery 991, 992, 993, 994 i 987 oraz inne niż wymienione w ust. 2 numery alarmowe podmiotów, do których zadań należy ochrona życia, zdrowia, bezpieczeństwa i porządku publicznego, mienia lub środowiska (art. 3 ust. 3 ustawy). Jak wskazuje z kolei art. 8 ust. 1 pkt 2 ustawy o systemie powiadamiania ratunkowego, do zadań centrum należy wprowadzanie do systemu teleinformatycznego i ewidencjonowanie w tym systemie danych dotyczących treści zgłoszeń alarmowych, w tym nagrań rozmów telefonicznych obejmujących całość zgłoszenia alarmowego, danych osób zgłaszających i innych osób wskazanych w trakcie przyjmowania zgłoszenia, pozycji geograficznych, informacji o miejscu zdarzenia i jego rodzaju oraz skróconego opisu zdarzenia. Polskie przepisy prawa nie przewidują natomiast możliwości rejestrowania zgłoszeń alarmowych poza systemem centrum powiadamiania ratunkowego, a ewentualne dokonywanie takowej rejestracji powinno wynikać z uprawnień ustawowych.

**Ad 3. Przetwarzanie danych biometrycznych**

RODO co do zasady zabrania przetwarzania danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej. Zaliczając je do szczególnych kategorii danych osobowych, ich pozyskiwanie i wykorzystywanie dopuszcza pod warunkami określonymi w art. 9 ust. 2. O konsultacje, kiedy można je uznać za spełnione, Prezes UODO proszony był m.in. w opisanych niżej przypadkach.

**1) Wyrażanie zgody na przetwarzanie danych biometrycznych w związku z zawieraniem umów przez konsumentów**

W związku z prowadzonym postępowaniem wyjaśniającym w stosunku do jednego z przedsiębiorstw Urząd Ochrony Konkurencji i Konsumentów skierował do Prezesa UODO pytanie o dopuszczalność wyrażania zgody na wykorzystanie danych biometrycznych przez konsumentów, którzy zawierają z firmą umowy, składając podpis na tablecie[461].

W kierunkowych wyjaśnieniach Prezes UODO zwrócił uwagę, że zgodnie z art. 4 pkt 14 RODO dane biometryczne oznaczają dane osobowe, które wynikają ze

[460] Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz. U. z 2025 r. poz. 1354).
[461] DPNT.023.72.2025.

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. Zostały one zakwalifikowane przez prawodawcę unijnego do szczególnej kategorii danych osobowych, których przetwarzanie jest możliwe po spełnieniu określonych w RODO warunków. Wyodrębnienie tej kategorii danych osobowych podyktowane jest potrzebą zapewnienia im dodatkowych środków ochrony, ponieważ przetwarzanie informacji odnoszących się do cech biologicznych konkretnych osób, na podstawie których możliwe jest niemal bezbłędne ustalenie ich tożsamości, może powodować znacznie większe zagrożenia niż przetwarzanie danych zwykłych. Z tych przyczyn przetwarzanie danych biometrycznych jest co do zasady zakazane. Zakaz ten został ujęty zarówno w art. 9 ust. 1 RODO, art. 10 dyrektywy 2016/680[462], jak i w art. 10 ust. 1 rozporządzenia 2018/1725[463], przy czym nie ma on charakteru bezwzględnego. Dopuszczalność przetwarzania tej szczególnej kategorii danych osobowych zależy od spełnienia warunków określonych w przepisach.

Europejska Rada Ochrony Danych (EROD) w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo (Wersja 2.0 przyjęta 29 stycznia 2020 r.), wskazała, że aby dane były uznane za biometryczne należy wziąć pod uwagę łącznie trzy elementy: 1) charakter danych – dane dotyczą cech fizycznych, fizjologicznych lub behawioralnych danej osoby fizycznej, 2) środki i sposób przetwarzania wynikać muszą z użycia odpowiedniej technologii oraz 3) dane są przetwarzane w celu jednoznacznej identyfikacji osoby fizycznej.

W świetle RODO zasadą jest zakaz przetwarzania danych biometrycznych (art. 9 ust. 1 RODO), a odstępstwo od niego powinno mieć wyraźne oparcie w jednym z wyjątków wymienionych w ust. 2 tego przepisu. W kontekście przedstawionej sprawy należy mieć na uwadze przesłankę dotyczącą zgody osoby, której dane są przetwarzane, która ma być świadoma. Żeby można było mówić o wyrażeniu przez podmiot zgody wyraźnej, konieczne jest poinformowanie osoby przez administratora o ryzykach związanych z przetwarzaniem takich danych, zasadach ich przetwarzania, stosowanych zabezpieczeniach i przysługujących mu uprawnieniach. Zgoda powinna także wyraźnie precyzować cel przetwarzania w momencie jej odbierania. Zastosowanie przesłanki legalizującej przetwarzanie danych w postaci zgody podmiotu danych wymaga spełnienia warunków określonych w art. 4 pkt 11 i art. 7 RODO. Z przepisów tych wynika, że musi być to zgoda konkretna, świadoma, jednoznaczna i dobrowolna (art. 4 pkt 11 RODO). Istotne jest, aby konsument, udzielając zgody, znał zakres i cel udzielanej zgody i wiedział, na czym konkretnie

[462] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

[463] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 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.

przetwarzanie jego danych będzie polegało. Zgoda powinna zostać zarejestrowana w systemie. Konsument powinien zostać powiadomiony o możliwości wycofania zgody w każdym czasie oraz o tym, że działanie to nie wpływa na zgodność z prawem wcześniejszych działań wykonanych na jej podstawie (art. 7 ust. 3 RODO). Europejska Rada Ochrony Danych w wytycznych dotyczących zgody wskazuje, że do uzyskania świadomej zgody wymagane jest udzielenie przez administratora co najmniej informacji dotyczących: tożsamości administratora, jego danych kontaktowych, celów przetwarzania, zakresu przetwarzanych danych (jakie dane czy rodzaj danych będą gromadzone i wykorzystywane), istnienia prawa do wycofania zgody, zautomatyzowanego podejmowania decyzji (zgodnie z art. 22 ust. 2 lit. c RODO), w tym profilowania, ryzyk związanych z transferami danych do państw trzecich w związku z brakiem decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń zgodnie z art. 46 RODO. Powinna istnieć również alternatywna metoda, z której podmiot danych mógłby skorzystać w przypadku braku zgody – tak, aby nie zostać pozbawionym możliwości skorzystania z konkretnej usługi.

Odnosząc powyższe do analizowanego przypadku organ nadzorczy wskazał, że w tej sprawie kluczowe znaczenie ma nie tylko treść zgody, ale i jej odbieranie w sytuacji, gdy nie jest to działanie proporcjonalne do realizowanego przez administratora celu. Należy bowiem zauważyć, że aby zawrzeć umowę dotyczącą realizacji usług świadczonych przez podmiot, wobec którego jest prowadzone postępowanie wyjaśniające, przepisy prawa nie przewidują składania podpisu biometrycznego. Zgoda natomiast, aby mogła być uznana za skuteczną przesłankę powinna być dobrowolna – należy więc rozważyć, czy konsument ma możliwość zawarcia umowy także składając inny niż biometryczny rodzaj podpisu. Jest to istotne także z punktu widzenia adekwatności / proporcjonalności – dlaczego akurat takie a nie inne rozwiązanie zostało przyjęte i uznane za konieczne oraz z jakich względów cel może być osiągnięty tylko w ten sposób. Jeśli osiągnięcie celu możliwe jest również w inny sposób, wyjaśnienia wymaga, z jakich względów przyjęto akurat taki model identyfikacji. Sprecyzowania wymaga także, czy celem jest identyfikacja, czy uwierzytelnienie konsumenta. Wskazać ponadto należy, kto i na jakiej podstawie prawnej będzie miał dostęp do danych. W orzecznictwie zarówno sądów krajowych, jak i TSUE zaleca się, aby ze względu na szczególnie wysokie ryzyko naruszenia prawa do prywatności w przypadku przetwarzania danych biometrycznych ograniczyć to przetwarzanie do sytuacji, gdy można mówić o zachowaniu proporcji, równowagi między interesem (celem) realizowanym przez administratora a sytuacją dotyczącą podmiotu danych. Wskazać również należy na konieczność uwzględnienia oceny skutków dla ochrony danych (art. 35 ust. 1 RODO, który reguluje obowiązek dokonania – przed rozpoczęciem przetwarzania albo w związku z tworzeniem przepisów regulujących operację lub zestaw operacji przetwarzania – oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych). Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędności przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych.

### 2) Przetwarzanie wizerunku biometrycznego na potrzeby przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu

Prezes UODO przedstawił obszerne stanowisko w odpowiedzi na pytanie Ministerstwa Finansów dotyczące dopuszczalności przetwarzania wizerunku biometrycznego osoby na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[464]. Organ nadzorczy wskazał, że dane biometryczne są danymi o wyjątkowo sensytywnym charakterze i aby zobowiązywać osobę do podania takich danych i móc je dalej przetwarzać, muszą istnieć szczególne rozwiązania gwarancyjne, o których stanowi art. 9 ust. 2-4 RODO.

Podstawą prawną do przetwarzania tych danych nie może być art. 9 ust. 2 lit. g RODO, w związku z art. 34 ust. 1 i ust. 4 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Art. 9 ust. 2 lit. g RODO stanowi, że przetwarzanie jest dopuszczalne, jeżeli jest niezbędne 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. W omawianym przypadku celem pozyskania danych biometrycznych miałoby być zapobieganie przypadkom prania pieniędzy i finansowania terroryzmu, które jedynie pośrednio wiązać można z działaniem mieszczącym się w pojęciu interesu publicznego, a nie interesu instytucji finansowej. Ponadto aktualne brzmienie przepisów ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu nie pozwala na wniosek, że spełniony jest przy przetwarzaniu danych biometrycznych warunek dotyczący istnienia odpowiednich i konkretnych środków ochrony praw podstawowych i interesów osoby, której dane dotyczą. W szczególności środki takie nie wynikają z wskazanego art. 34 ust. 1 i ust. 4. Przepis ten stanowi bowiem jedynie o identyfikacji klienta i sprawdzeniu jego tożsamości, jak też przetwarzaniu danych zawartych w dokumencie tożsamości (również w formie kopii) w kontekście podejmowania środków bezpieczeństwa finansowego. Nie ma natomiast w tym przepisie mowy o środkach gwarancyjnych dla prawa do prywatności klienta instytucji.

## Ad 4. Udostępnianie i pozyskiwanie danych zawartych w dokumentacji medycznej

Istotną grupę pytań stanowiły te od podmiotów z szeroko rozumianego sektora medycznego, które dotyczyły m.in. o **wtórnego wykorzystania** danych medycznych oraz udostępniania danych zawartych w dokumentacji medycznej.

[464] DPNT.023.179.2025.

### 1) Udostępnianie dokumentacji medycznej do wykorzystania w celach naukowych

W odpowiedzi na pytanie Agencji Badań Medycznych[465] dotyczące wykładni art. 26 ust. 4 ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[466] w kontekście udostępniania dokumentacji medycznej do wykorzystania w celach naukowych Prezes UODO poinformował, że powołany przepis przewiduje możliwość udostępnienia dokumentacji medycznej szkole wyższej lub instytutowi badawczemu w celach naukowych „bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy". Za niewłaściwe rozwiązanie organ nadzorczy uznał przedstawioną przez Agencję Badań Medycznych propozycję pseudonimizacji dokumentacji medycznej przed jej udostępnieniem. Powołany przepis wprost odnosi się do obowiązku anonimizacji danych osobowych w udostępnianej dokumentacji medycznej.

Przyjęta i konsekwentnie prezentowana przez Prezesa UODO interpretacja tej regulacji jest również zgodna z wykładnią definicji danych osobowych przyjmowaną w Wytycznych Grupy Roboczej Art. 29 oraz EROD. Dane medyczne mają być przekazane bez ujawniania danych identyfikujących osobę, której dotyczą, a wzgląd na konieczność szanowania zasady minimalizacji danych z art. 5 ust. 1 lit. c RODO wymaga, by dane osobowe zawarte w dokumentacji medycznej, zgodnie z art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, były udostępniane po usunięciu elementów identyfikujących osoby, których dotyczą.

Jednocześnie, w ocenie Prezesa UODO, należy podjąć właściwe działania legislacyjne w kierunku określenia właściwej podstawy prawnej dla udostępnienia danych w formacie spsedonimizowanym. Taka podstawa prawna powinna jednocześnie stworzyć właściwe gwarancje dla ochrony danych osobowych, jak tego wymagają regulacje RODO (art. 9 ust. 2 lit. j w zw. z art. 89 ust. 1 RODO) oraz EHDS[467] dotyczące wtórnego wykorzystywania danych dotyczących zdrowia. Realizacja zasady zgodności z prawem, rzetelności i przejrzystości wynikająca z art. 5 ust. 1 lit. a RODO w zw. z jego art. 6 ust. 3 oraz art. 9 ust. 2 lit. j w zw. z art. 89 ust. 1, wymaga bowiem od prawodawcy krajowego właściwego wdrożenia unijnych przepisów dotyczących wtórnego wykorzystywania danych dotyczących zdrowia poprzez stworzenie adekwatnych rozwiązań prawnych, które w sposób jasny i precyzyjny będą wskazywały na właściwe gwarancje ochrony danych osobowych dotyczących zdrowia. Rozwiązania te powinny zostać osadzone w polskim porządku konstytucyjnym, który przewiduje wysoki standard ochrony danych osobowych i prawa do prywatności, wskazując na konieczność wprowadzenia ograniczeń tych praw w formie ustawowej (art. 47 oraz art. 51 w zw. z art. 31 ust. 3 Konstytucji RP)[468].

---

[465] DPNT.023.713.2025.

[466] Dz. U. z 2024 r. poz. 581.

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

[468] Prezes UODO skierował w tej sprawie wystąpienie do Ministra Zdrowia, o którym więcej piszemy w części dotyczącej Wystąpień.

### 2) Udostępnianie danych medycznych zaspołom interdyscyplinarnym (przemoc domowa)

W odpowiedzi na pytanie administratora – dyrektora samodzielnego publicznego zakładu opieki zdrowotnej dotyczące legalności udostępniania danych o charakterze medycznym zespołowi interdyscyplinarnemu oraz grupie diagnostyczno-pomocowej w celu realizacji zadań ustawowych w zakresie przeciwdziałania przemocy domowej[469] Prezes UODO wskazał, że podstawa przetwarzania danych osobowych powinna być określona – w sposób jasny i precyzyjny – w przepisach prawa. To przepisy ustawy powinny zatem precyzować zasady przetwarzania danych osobowych, nie zaś porozumienie, które nie stanowi źródła prawa powszechnie obowiązującego. Ani z przepisów ustawy o przeciwdziałaniu przemocy domowej, ani z przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta nie wynika podstawa prawna do udostępnienia dokumentacji medycznej czy informacji o stanie zdrowia pacjenta w związku z realizacją zadań przez zespół interdyscyplinarny. Tym samym podstawa udostępnienia danych osobowych w opisanej sytuacji, tj. na podstawie porozumienia o współpracy w zespole interdyscyplinarnym, budzi wątpliwości.

### 3) Udostępnianie danych medycznych służbom prowadzącym postępowanie sprawdzające

W odpowiedzi na pytanie Ośrodka Terapii Uzależnienia i Współuzależnienia dotyczące dopuszczalności udostępnienia kopii dokumentacji medycznej pacjenta na wniosek Agencji Bezpieczeństwa Wewnętrznego prowadzącej postępowanie sprawdzające[470] Prezes UODO wskazał, że w tej sytuacji pod uwagę wziąć należy przepisy ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego[471] (art. 50 ust. 1 i ust. 2 pkt 4), ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[472] (art. 24 ust. 3 pkt 2 i 3) oraz ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[473] regulujące kwestie udostępniania dokumentacji medycznej, a także zasady przetwarzania danych określone w art. 5 RODO, w tym zwłaszcza zasadę ograniczenia celu (art. 5 ust. 1 lit. b) oraz zasadę minimalizacji danych (art. 5 ust. 1 lit. c). Z art. 50 ust. 2 pkt 4 o ochronie zdrowia psychicznego w związku z art. 24 ust. 3 pkt. 2 i 3 ustawy o ochronie informacji niejawnych wynika, że uprawniony w nich podmiot ma prawo do żądania informacji na temat stanu zdrowia psychicznego danej osoby w zakresie niezbędnym do przeprowadzenia dotyczącego jej postępowania sprawdzającego. Oznacza to, że administrator ma prawo do udostępnienia danych zawartych w prowadzonej dokumentacji ww. służbom, ale jedynie w zakresie niezbędnym do prowadzenia postępowania sprawdzającego.

[469] DOL.023.985.2024.
[470] DPNT.023.174.2025.
[471] Dz. U. z 2024 r. poz. 917.
[472] Dz. U. z 2025 poz. 1209.
[473] Dz. U. z 2024 r. poz. 581.

**Ad 5. Przetwarzanie danych osobowych w związku ze świadczeniem pomocy społecznej**

Także sektor pomocy społecznej, przetwarzający wiele danych osobowych, często o bardzo szczególnym charakterze, zwraca się do Prezesa UODO z różnymi pytaniami.

Do Prezesa Urzędu zwrócił się ośrodek pomocy społecznej o interpretację odnośnie do stosowania art. 105 ustawy o pomocy społecznej, jako podstawy prawnej **udostępniania przez podmioty lecznicze danych osobowych na rzecz ośrodków pomocy społecznej**[474]. Organ nadzorczy wskazał, że zgodnie z ustawą o prawach pacjenta, pacjent ma prawo do zachowania w tajemnicy informacji z nim związanych w związku z udzielanym świadczeniem medycznym. Przepisów tych nie stosuje się jeśli przepisy odrębne tak stanowią – podmiot występujący o udostępnienie danych powinien w sposób prawidłowy wskazać podstawę prawną uprawniającą go do uzyskania określonych i niezbędnych danych.

**Kwestia upoważnienia pracownika sekretariatu do przetwarzania danych osobowych w zakresie odbierania i wysyłania korespondencji elektronicznej i papierowej dotyczącej procedury „Niebieskie Karty”**[475]. Zgodnie z art. 29 rozporządzenia 2016/679, podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Powyższy przepis należy rozumieć w ten sposób, że podmiot przetwarzający oraz osoba działająca z upoważnienia administratora nie powinna przetwarzać danych z wyjątkiem przetwarzania zgodnie z instrukcjami administratora, chyba że wymagają tego [przetwarzania] przepisy prawa UE lub prawa państwa członkowskiego. Zgodnie z art. 9c ust. 6 ustawy o przeciwdziałaniu przemocy domowej[476], administratorem danych przetwarzanych na podstawie przepisów niniejszego artykułu jest ośrodek pomocy społecznej, a w przypadku przekształcenia ośrodka pomocy społecznej w centrum usług społecznych na podstawie przepisów ustawy z dnia 19 lipca 2019 r. o realizowaniu usług społecznych przez centrum usług społecznych - centrum usług społecznych, zapewniające obsługę organizacyjno-techniczną i finansową zespołu interdyscyplinarnego. Natomiast zgodnie z art. 9c ust. 7 UPPD, zabezpieczenia stosowane przez administratora danych w celu ochrony danych osobowych polegają co najmniej na dopuszczeniu do przetwarzania danych osobowych wyłącznie osób posiadających pisemne upoważnienie wydane przez administratora danych, pisemnym zobowiązaniu osób upoważnionych do przetwarzania danych osobowych do zachowania ich w tajemnicy. Przepisy stanowią zatem o warunkach dopuszczenia do przetwarzania danych osób realizujących zadania, o których mowa w tych przepisach. Przetwarzanie, w stanie faktycznym opisanym w piśmie przywołanym na

[474] DPNT.023.1159.2025.
[475] DPNT.023.780.2025.
[476] Ustawa z dnia 29 lipca 2005 roku o przeciwdziałaniu przemocy domowej (Dz. U. z 2024 r. poz. 1673).

wstępie, musi ponadto odbywać się w taki sposób, aby spełnione zostały przesłanki z art. 5 ust. 1 rozporządzenia 2016/679, w szczególności zaś – w okolicznościach przedmiotowej sprawy – chodzi o art. 5 ust. 1 lit. f rozporządzenia 2016/679, zgodnie z którym dane osobowe przetwarzane są w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"). Zgodnie zaś z art. 5 ust. 2 rozporządzenia 2016/679 administrator jest odpowiedzialny za przestrzeganie wszystkich warunków przetwarzania danych osobowych, o których mowa w art. 5 ust. 1 rozporządzenia 2016/679, i musi być w stanie wykazać ich przestrzeganie (zasada rozliczalności). Podsumowując zatem – Miejski Ośrodek Pomocy Społecznej, jako administrator danych, powinien dokonać analizy ryzyka, skonsultować procesy związane z bezpieczeństwem danych z inspektorem ochrony danych osobowych i podjąć działania pozwalające wykazać mu spełnienie zasady rozliczalności, o której mowa w art. 5 ust. 2 rozporządzenia 2016/679.

### Ad 6. Ochrona danych osobowych w sektorze publicznym

Podobnie jak w latach ubiegłych wiele pytań pochodziło od podmiotów z sektora publicznego. Ich wątpliwości dotyczy wielu aspektów przetwarzania danych osobowych, w tym podstaw prawnych, statusu podmiotów w procesie przetwarzania danych osobowych, upubliczniania danych osobowych czy kwestii pogodzenia prawa do ochrony danych osobowych i prywatności z prawem dostępu do informacji publicznej. Wzrosła jednak liczba pytań związanych z postępującą **cyfryzacją administracji i rozwojem e-usług**.

#### 1) Postać wniosku o udostępnienie danych

Jedno z pytań dotyczyło warunków formalnych, jakie powinien spełniać kierowany do administratora wniosek o udostępnienie danych[477]. W odpowiedzi organ nadzorczy informacyjnie wskazał, że ani RODO, ani przepisy krajowe nie określają ogólnej formy, w jakiej ma zostać złożony wniosek o udostępnienie danych. Kwestia tego, jak oceniać każdy taki wniosek należy do administratora, który powinien posiadać odpowiednie wewnętrzne uregulowania dotyczące tej materii.

#### 2) Status podmiotów w procesie przetwarzania danych osobowych

Do Prezesa UODO wciąż wpływają pytania związane z określeniem ról podmiotów uczestniczących w procesie przetwarzania danych osobowych. Mimo prezentowanych zarówno przez EROD, jak i przez UODO wskazówek w zakresie określania statusu administratora oraz podmiotu przetwarzającego, zagadnienie to w dalszym ciągu budzi liczne wątpliwości. Powodem tego może być sposób ujęcia terminu „administrator" w przepisach o ochronie danych osobowych. Choć odwołanie się w definicji administratora do kryterium decydowania o celach i sposobach

[477] DPNT.023.429.2025.

przetwarzania danych osobowych uznać należy za racjonalne i uzasadnione, to jednak zastosowanie tego kryterium w praktyce rodzi wątpliwości, powodując konieczność dokonywania szczegółowej analizy konkretnych sytuacji.

Przykładowo pewien burmistrz zwrócił się do Prezesa UODO z pytaniem, czy jednostka samorządu terytorialnego lub inny **podmiot publiczny prowadzący fanpage na Facebooku faktycznie pełni funkcję współadministratora danych osobowych użytkowników** wraz z META Platforms”[478]. Organ nadzorczy wskazał, że ustalając kwestię podmiotu, któremu w procesie przetwarzania danych osobowych będzie przysługiwał status administratora, przede wszystkim należy kierować się definicją tego pojęcia. Zgodnie z art. 4 pkt 7 RODO „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. To, jaki podmiot pełni funkcję administratora, w każdym przypadku będzie wynikało z okoliczności faktycznych. Administratorem jest więc ten podmiot, który poprzez wzgląd na zakres przysługujących mu kompetencji i zadań bierze udział w procesach przetwarzania, wykonuje operacje na danych osobowych, decydując o ich celach i sposobach. Natomiast zastosowanie instytucji współadministrowania w rozumieniu art. 26 RODO możliwe jest, jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania. Przepis ten stanowi, że współadministratorzy, w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

Organ nadzorczy wskazał, że w tym aspekcie warto sięgnąć po wyrok z 11 stycznia 2024 r. C-231/22 Etat belge, w którym Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że „biorąc pod uwagę brzmienie art. 4 pkt 7 RODO, interpretowanego w świetle tego celu [tj. zapewnienia, poprzez szeroką definicję pojęcia „administratora”, skutecznej i pełnej ochrony osobom, których dane dotyczą], okazuje się, że aby ustalić, czy daną osobę lub podmiot należy uznać za „administratora” w rozumieniu tego przepisu, należy zbadać, czy ta osoba lub ten podmiot samodzielnie lub wspólnie z innymi ustalają cele i sposoby przetwarzania, czy też są one określone w prawie krajowym”. Zagadnienie to jest szerzej omówione w przyjętych przez Europejską Radę Ochrony Danych 7 lipca 2021 r. Wytycznych 7/2020 w sprawie pojęć administratora, współadministratora i podmiotu przetwarzającego na gruncie RODO. W kontekście publikacji danych osobowych na portalach

[478] DPNT.023.1056.2025.

społecznościowych, warto również przypomnieć Decyzję Prezesa UODO z 2019 r. podtrzymaną przez NSA wyrokiem z 28 lutego 2024 r. w sprawie o sygn. akt. II OSK 3839/213.

W podsumowaniu tych wyjaśnień Prezes UODO podkreślił, że administrator decyduje i ponosi pełną odpowiedzialność za cały proces przetwarzania danych osobowych dokonywany w związku z realizacją nałożonych na niego zadań, który musi być zgodny z przepisami o ochronie danych osobowych.

### 3) Pozyskiwanie, udostępnianie i upublicznianie danych osobowych

Do Prezesa UODO niezmiennie wpływają też pytania dotyczące pozyskiwania lub udostępniania danych osobowych, a także ich upubliczniania.

Dla przykładu pewien audytor (z powiatu) zwrócił się z pytaniem o **możliwość przekazania jednostkom organizacyjnym powiatu informacji** (pozyskanych z innych audytowanych jednostek) o zawyżaniu cen usług przez niektórych wykonawców, w tym ich danych osobowych i kontaktowych, tak by jednostki mogły samodzielnie i świadomie podejmować decyzje związane z wyborem profesjonalnego, rzetelnego i niedrogiego wykonawcy[479]. Odnosząc się do tego pytania, Prezes UODO poinformował, że audyt zazwyczaj przeprowadzany jest wewnętrznie w danym podmiocie w celu usprawnienia jego działalności w określonym zakresie. Przetwarzanie danych osobowych musi być adekwatne i związane z celem takiego audytu. Audytor wewnętrzny po uzgodnieniu wstępnych wyników audytu sporządza sprawozdanie, które następnie przekazywane jest audytowanemu i kierownikowi jednostki. Zgodnie z § 5 ust. 4 rozporządzenia Ministra Finansów w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu[480] – dokumentacja dotycząca audytu wewnętrznego stanowi własność jednostki.

Inne z pytań dotyczyło **dopuszczalności pozyskiwania przez gminę danych osobowych od MOPS na potrzeby przydziału lokali mieszkalnych oraz oceny wniosków o najem lokali z zasobu mieszkaniowego gminy przez komisję mieszkaniową**[481]. Udzielając ogólnych wskazówek, Prezes UODO zwrócił uwagę na art. 6 ust. 1 lit. c RODO, zgodnie z którym przetwarzanie danych jest dopuszczalne, jeśli jest to niezbędne dla wypełnienia obowiązku prawnego ciążącego na administratorze – przy czym podstawa przetwarzania danych powinna być określona w prawie UE lub w prawie polskim zgodnie z art. 6 ust. 3 RODO. Oznacza to, że dane osobowe mogą być przetwarzane przez dany podmiot, jeśli przewidują to przepisy prawa. Podmioty publiczne zgodnie z konstytucyjną zasadą działają na podstawie i w granicach prawa. Organ nie może domniemywać swoich kompetencji, jeśli nie wynikają one wprost z przepisu prawa. Stąd pozyskanie danych osobowych przez podmiot realizujący zadania publiczne powinno wynikać z przepisów prawa odnoszących się do zadań tego podmiotu. Gmina, zgodnie z art. 4 ust. 2 ustawy

[479] DPNT.023.424.2025.
[480] Rozporządzenie Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz. U. z 2018 r. poz. 506).
[481] DPNT.023.1049.2025.

o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego[482], zapewnia lokale socjalne i zamienne, a także zaspokaja potrzeby mieszkaniowe gospodarstw domowych o niskich dochodach. Rada gminy uchwala zasady wynajmowania lokali wchodzących w skład mieszkaniowego zasobu gminy, w tym zasady i kryteria wynajmowania lokali, jeżeli w mieszkaniowym zasobie gminy wydzielono lokale przeznaczone na ten cel, w tym na potrzeby beneficjentów ustawy o pomocy społecznej oraz ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej[483] (art. 21 ust. 3 pkt 6b ustawy o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego). Osoba ubiegająca się o lokal socjalny składa w tym celu deklarację wraz z oświadczeniem o wysokości dochodów i stanie majątkowym członków rodziny będących członkami gospodarstwa domowego. W razie wątpliwości co do zawartych w deklaracji informacji i danych, gmina może wezwać osobę do udostępnienia dokumentów potwierdzających wykazane informacje.

W art. 21b ust. 1b ustawy o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego wskazane zostało, że w celu zweryfikowania informacji i danych zawartych w deklaracji, gmina może przetwarzać dane osobowe i informacje dotyczące osoby ubiegającej się o zawarcie umowy najmu albo podnajmu lokalu albo najmu socjalnego lokalu wchodzącego w skład mieszkaniowego zasobu gminy, pozyskane w toku innych postępowań prowadzonych przez gminę lub jej jednostki organizacyjne. Powyższy przepis nie precyzuje jednak formy, trybu, zakresu pozyskiwanych danych osobowych oraz co najważniejsze – nie wskazuje, że źródła mają być zewnętrzne. Mając zatem powyższe na uwadze administrator, przed podjęciem decyzji o pozyskaniu przez gminę lub udostępnieniu gminie określonych danych osobowych, powinien przeprowadzić wnikliwą ocenę, czy przekazanie (udostępnienie) danych będzie zgodne z zasadami RODO, zwłaszcza zasadą zgodności z prawem, rzetelności i przejrzystości o której mowa w art. 5 ust. 1 lit. a RODO. Należy zatem dokonać analizy przepisów prawa regulujących przetwarzanie danych osobowych przez określone podmioty, zwłaszcza że posiadane przez nich informacje mogą być objęte tajemnicami prawnie chronionymi, np. tajemnicą pomocy społecznej, która nie powinna być osłabiana. Pozyskując dane od takich jednostek organizacyjnych gminy, należy mieć na uwadze, że powinny być to sytuacje wyjątkowe, kiedy nie jest możliwa weryfikacja informacji na podstawie innych źródeł. Legalność żądania przez komisję pozyskania danych osobowych od ośrodka pomocy społecznej powinna być oceniona także przez pryzmat art. 100 ust. 7 ustawy o pomocy społecznej[484], który ustanawia tajemnicę służbową i wskazuje, że podmioty i osoby realizujące zadania w zakresie pomocy społecznej określone w niniejszej ustawie obowiązane są do zachowania w tajemnicy wszelkich informacji i danych, które uzyskały przy wykonywaniu tych zadań. Administrator powinien również zadbać, by

[482] Ustawa z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego (Dz. U. z 2023 r. poz. 725).
[483] Dz. U. z 2025 r. poz. 49.
[484] Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2025 r. poz. 1214 ze zm.).

nie przetwarzać (w tym nie udostępniać) danych nadmiarowych, a jedynie te, które są niezbędne do wykonania ustawowego zadania, np. na potrzeby prowadzonego już postępowania weryfikacyjnego, czyli w konkretnym celu i zakresie, zgodnie z zasadą ograniczenia celu wskazaną w art. 5 ust. 1 lit. b przy zachowaniu zasady minimalizacji danych określonej w art. 5 ust. 1 lit. c RODO. Podsumowując organ nadzorczy zaznaczył, że to administrator decyduje i ponosi pełną odpowiedzialność za cały proces przetwarzania danych osobowych w związku z realizacją nałożonych na niego zadań.

Urząd Komunikacji Elektronicznej pytał natomiast o **dopuszczalność publikacji w rejestrze przedsiębiorców telekomunikacyjnych (rejestr PT) oraz rejestrze jednostek samorządu terytorialnego prowadzących działalność w zakresie telekomunikacji** (rejestr JST), o których mowa w art. 9 i 10 ustawy Prawo komunikacji elektronicznej[485] **informacji w zakresie dotyczącym osoby wyznaczonej do kontaktu z Prezesem UKE na stronie BIP tego urzędu**[486].W odpowiedzi Prezes UODO zaznaczył, że zgodnie z RODO przetwarzanie (w tym udostępnianie) danych osobowych tzw. zwykłych (jak np. imię i nazwisko, adres, dane kontaktowe, numer PESEL) jest uzależnione od spełnienia jednej z przesłanek legalności wymienionych w art. 6 ust. 1 RODO. Jedną z nich jest sytuacja, gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c). Z przepisów Prawa komunikacji elektronicznej wynika, że do rejestru przedsiębiorców telekomunikacyjnych (rejestr PT) oraz rejestru jednostek samorządu terytorialnego prowadzących działalność w zakresie telekomunikacji (rejestr JST) wpisuje się imię, nazwisko, adres do korespondencji, adres poczty elektronicznej i numer telefonu osoby wyznaczonej do kontaktu z Prezesem UKE (art. 6 ust. 1 pkt 4 w zw. z art. 9 i art. 7 ust. 1 pkt 8 w zw. z art. 10). Zgodnie zaś z art. 5 ust. 5 ww. ustawy rejestr PT i rejestr JST są jawne i udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa UKE. Co istotne, ww. dane zawarte są także we wniosku o wpis do wymienionych rejestrów (art. 6 ust. 1 i art. 7 ust. 10). Oznacza to, że w razie konieczności kontaktu Prezesa UKE z przedsiębiorcą telekomunikacyjnym lub jednostką samorządu terytorialnego prowadzącą działalność w zakresie telekomunikacji posiada on wiedzę o osobie wyznaczonej do kontaktu w imieniu takiego przedsiębiorcy czy takiej jednostki samorządowej. Pomimo zatem, że przepisy Prawa komunikacji elektronicznej zobowiązują Prezesa UKE do pozyskania i następnie publikacji w Biuletynie Informacji Publicznej danych osoby wyznaczonej do kontaktu z Prezesem UKE w zakresie wskazanym w tych przepisach, to jednak nie wskazują wyraźnie celu ich publikacji. Należy zatem mieć na względzie, że przepisy RODO wymagają, aby dane osobowe były przetwarzane nie tylko zgodnie z zasadą legalności (art. 5 ust. 1 lit. a w zw. z art. 6 ust. 1 RODO), ale także zgodnie z zasadą ograniczenia celu (art. 5 ust. 1 lit. b). Oznacza to, że administrator powinien zbierać dane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzać ich dalej w sposób niezgodny z tymi celami. Skoro zatem celem zbierania danych

[485] Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 ze zm.).
[486] DPNT.023.455.2025.

osobowych pracownika przedsiębiorcy telekomunikacyjnego i pracownika jednostki samorządu terytorialnego we wnioskach o wpis do rejestrów PT i JST jest kontakt z Prezesem UKE, to powstaje pytanie, czy bez ich publikacji w BIP cel ten zostanie osiągnięty. Jeśli tak, to nie mamy spełnionej przesłanki niezbędności takiej publikacji, co jednocześnie stoi w sprzeczności z zasadą celowości przetwarzania danych z art. 5 ust. 1 lit b RODO. W przypadku publikacji danych osobowych w BIP należy mieć na względzie określenie okresu retencji tak ujawnianych danych. W sytuacjach, w których prawo nie reguluje okresu retencji danych w Biuletynie Informacji Publicznej, po przeprowadzeniu analiz, należy określić ten okres tak, aby przetwarzanie danych było zgodne z celami, z tórymi je pozyskano. Stanowisko takie zaprezentowane zostało także w uzasadnieniu wyroku Wojewódzkiego Sądu Administracyjnego w Lublinie z 1 marca 2016 r.[487]

### 4) Przetwarzanie danych osobowych podczas posiedzeń rad i transmisja ich obrad

Zapewnianie transparentności życia publicznego z poszanowaniem prawa do prywatności i ochrony danych osobowych to kolejne z zagadnień, które przysparza administracji publicznej wielu problemów. Stąd prośby o wyjaśnienia i wskazówki w tym zakresie.

Odnosząc się do pytania dotyczącego **transmisji obrad i udostępniania nagrań z posiedzeń kolegialnych organów jednostek samorządu terytorialnego**[488], Prezes UODO wskazał, że realizacja tego zadania powinna odbywać się z poszanowaniem określonych w RODO zasad. Obowiązkiem administratora jest zapewnienie właściwego (uwzględniającego ochronę danych osobowych) sposobu transmisji, utrwalania i udostępniania w Internecie nagrań z posiedzeń. Jednocześnie podkreślił, że obowiązek upublicznienia nagrań w BIP i na stronach internetowych nie oznacza prawa do ujawnienia wszystkich danych osobowych przetwarzanych na posiedzeniu kolegialnych organów. Również podczas transmisji obrad na żywo organy jednostek samorządu terytorialnego zobowiązane są do zadbania o ochronę danych osobowych osób biorących w udział posiedzeniach, w szczególności osób prywatnych. Co ważne, orzecznictwo sądów administracyjnych potwierdza, że publikacja informacji publicznej w BIP powinna wiązać się z usunięciem danych osobowych osób prywatnych lub ich zanonimizowaniem[489].

Podobnych wyjaśnień Prezes UODO udzielił w związku z pytaniem dotyczącym **transmisji obrad sesji rady dzielnicy**[490].

Przedmiotem analiz była też kwestia tego, czy **odczytanie danych osobowych przedstawicieli organizacji związkowej podczas posiedzenia komisji rady gminy** jest naruszeniem przepisów o ochronie danych osobowych[491]. W odpowiedzi Prezes

[487] Sygn. akt II SA/Lu 876/15.
[488] DPNT.023.21.2025.
[489] Zob. wyrok NSA z 14 marca 2013 r., sygn. akt I OSK 620/12; wyrok WSA w Warszawie z 18 listopada 2008 r., sygn. akt II SA/Wa 1177/08; decyzja Prezesa UODO, sygn. ZSPU.421.3.2019.
[490] DPNT.023.263.2025.
[491] DPNT.023.1153.2025.

UODO wskazał, że art. 18 ust. 2 ustawy o dostępie do informacji publicznej[492] stanowi, że posiedzenia kolegialnych organów pomocniczych (np. komisji rad gminy), o których mowa w ust. 1, są jawne i dostępne, o ile stanowią tak przepisy ustaw albo akty wydane na ich podstawie lub gdy organ pomocniczy tak postanowi. Zgodnie z art. 19 tej ustawy zarówno kolegialne organy władzy publicznej, jak i kolegialne organy pomocnicze sporządzają i udostępniają protokoły lub stenogramy swoich obrad, chyba że sporządzą i udostępnią materiały audiowizualne lub teleinformatyczne rejestrujące w pełni te obrady. Natomiast prawo dostępu do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej. 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 (art. 5 ust. 2 tej ustawy). Art. 11 b ustawy o samorządzie gminnym wskazuje, że jawność działania organów gminy obejmuje w szczególności prawo obywateli do uzyskiwania informacji, wstępu na sesje rady gminy i posiedzenia jej komisji, a także dostępu do dokumentów wynikających z wykonywania zadań publicznych, w tym protokołów posiedzeń organów gminy i komisji rady gminy. Upublicznienie danych osobowych jest jedną z możliwych operacji przetwarzania danych osobowych, które jest dopuszczalne po spełnieniu jednej z przesłanek wymienionych w art. 6 RODO, który wskazuje, że dane osobowe mogą być przetwarzane m.in., jeśli osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych (art. 6 ust. 1 lit. a RODO), przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO). Jeśli administrator nie dysponuje przesłanką uprawniającą go do przetwarzania (upublicznienia) danych osobowych, ujawnienie ich stanowiłoby naruszenie w myśl przepisów o ochronie danych osobowych.

W 2025 r. Prezes UODO pytany był również o to, czy **adres zamieszkania sołtysa** podlega ochronie wynikającej z art. 5 ust. 2 ustawy o dostępie do informacji publicznej[493]. W odpowiedzi organ nadzorczy powołał przepisy ustawy o dostępie do informacji publicznej oraz wyrok Wojewódzkiego Sądu Administracyjnego w Opolu z 9 stycznia 2025 r.[494] dotyczący przekazywania przez burmistrza dokumentów związanych z aktywnością sołtysa, a także wskazał na dotychczasowe stanowiska UODO odnoszące się do tego zagadnienia.

Poinformował, że w numerze specjalnym Biuletynu UODO został opublikowany materiał „Czy prywatny numer telefonu sołtysa stanowi informację publiczną?", w którym wskazano m.in., że „dane osobowe sołtysa, o ile ściśle wiążą się z pełnioną przez sołtysa rolą publiczną i nie wkraczają w jego prywatność, podlegają ograniczonej ochronie prawnej. Nie budzi zatem wątpliwości ujawnianie przez urząd gminy takich danych sołtysa, jak jego imię i nazwisko, adres, pod którym urzęduje, czy też służbowy numer telefonu i służbowy adres poczty elektronicznej"[495].

[492] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).
[493] DPNT.023.558.2025.
[494] Sygn. akt I SAB/Op 110/24.
[495] Biuletyn UODO numer specjalny, s. 90; dostępny na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/490/4077.

Zaznaczył jednak, że ocena spełnienia przesłanki ograniczenia ze względu na prywatność osoby fizycznej dostępu do informacji publicznej, także w kontekście udostępnienia danych osobowych sołtysa, należy do organu rozpatrującego wniosek o udostępnienie informacji publicznej.

### Ad 7. Przetwarzanie danych osobowych dzieci i małoletnich

Ważną grupę pytań stanowiły te dotyczące przetwarzania danych osobowych dzieci i małoletnich. Są one istotne m.in. dlatego, że RODO nakazuje podchodzić do tej grupy osób ze szczególną troską, wskazując że dzieci mogą być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.

Kierowane do Prezesa UODO pytania dotyczyły przetwarzania danych osobowych najmłodszych w bardzo różnych sytuacjach.

Jedno z nich dotyczyło dopuszczalności **udostępnienia rodzicom adopcyjnym danych osobowych dziecka zawartych w dokumentacji jego pobytu w placówce sprawującej pieczę zastępczą**[496]. W udzielonych wyjaśnieniach Prezes UODO zaznaczył, że przetwarzanie danych osobowych powinno odbywać się zgodnie z zasadami przewidzianymi w art. 5 ust. 1 RODO, w tym zgodnie z zasadą legalności (art. 5 ust. 1 lit. a), a także warunkami określonymi w art. 6 i art. 9 RODO.

W kontekście przesłanek legalności przetwarzania danych osobowych Prezes UODO wskazał, że przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej[497] zawierają regulacje odnoszące się do udostępnienia dokumentacji dotyczącej dziecka. Regulacje te wskazują na podmioty zobowiązane do udostępnienia dokumentacji oraz zakres udostępnianych informacji, z tym że w doktrynie przyjmuje się, że katalog gromadzonych informacji i dokumentów, o których mowa w ustawie, nie ma charakteru zamkniętego, a zatem jest to tylko przykładowe ich wymienienie. Prezes zauważył jednak, że przepisy tej ustawy nie regulują kwestii dostępu do dokumentacji rodziców adopcyjnych, którzy wnioskują o dane dziecka z pobytu w ramach pieczy zastępczej, np. w celu wykorzystania ich dla konsultacji z psychologiem, czy też dorosłych adoptowanych, co budzi zastrzeżenia z punktu widzenia art. 5 ust. 1 lit. a w zw. z art. 6 ust. 1 w zw. z art. 6 ust. 3 oraz w zw. z art. 15 RODO.

Jednocześnie zwrócił uwagę na prawo dostępu do danych, wynikające z art. 15 RODO i zagwarantowane również w art. 8 ust. 2 Karty Praw Podstawowych UE, oraz 51 ust. 3 Konstytucji RP, a także na istotne orzecznictwo Trybunału Sprawiedliwości UE w tym obszarze[498].

---

[496] DPNT.023.8.2025.

[497] Ustawa z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej (Dz. U. z 2025 r. poz.49).

[498] M.in. wyrok z 20 grudnia 2017 r. Nowak przeciwko Data Protection Commissioner, C-434/16; wyrok z 17 lipca 2014 r. w sprawie Ys. I M. i S. przeciwko Minister voor Immigratie, Integratie en Asiel, C-141/12; wyrok z 27 maja 2024 r. w sprawie Addiko Bank p-ko Agencija za zaštitu osobnih podataka, C-312/23.

Prezes UODO podkreślił, że każdorazowo ocena udostępnienia dokumentacji 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 niezbędnym zakresie, a także w środowisku bezpiecznym dla danych, tak aby ograniczyć ryzyko udostępnienia informacji podmiotom/osobom nieuprawnionym, w nadmiarowym zakresie, czy ryzyko zaginięcia lub uszkodzenia stosowanie do zasady ograniczonego celu i minimalizacji danych oraz zasady integralności i poufności .Przede wszystkim należy zadbać o to, aby wtedy, kiedy jest to konieczne, dokonać anonimizacji danych. Zgodnie z zasadą rozliczalności, administrator wykazuje, że zastosował rozwiązania adekwatne do stwierdzonych ryzyk. Wspierać go w tym procesie może inspektor ochrony danych.

W 2025 r. rodzinny dom dziecka zwrócił się do Urzędu z pytaniem, **jakie dokumenty i dane osobowe dzieci przebywających w pieczy zastępczej należy przekazywać do organizatora pieczy zastępczej**[499]. Odpowiadając na nie organ nadzorczy wskazał, że prowadzenie rodzinnych domów dziecka regulują przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej. Zgodnie z jej art. 39 ust. 1 pkt 2, formą rodzinnej pieczy zastępczej jest rodzinny dom dziecka. Organizatorem rodzinnej pieczy zastępczej jest jednostka organizacyjna powiatu lub podmiot, któremu powiat zlecił realizację tego zadania na podstawie art. 190 tej ustawy. Do zadań organizatora rodzinnej pieczy zastępczej należy m.in. dokonywanie okresowej oceny sytuacji dzieci przebywających w rodzinnej pieczy zastępczej (art. 76 ust. 2 pkt 11). Kontrolę nad pieczą zastępczą sprawuje natomiast zarząd powiatu, który zgodnie z art. 38b ust. 8 ustawy w związku z przeprowadzanym postępowaniem kontrolnym ma prawo żądania informacji, dokumentów i danych, niezbędnych do sprawowania kontroli. Zgodnie z ogólnym rozporządzeniem o ochronie danych podmiot może przetwarzać (w tym pozyskiwać) dane osobowe wyłącznie wtedy, gdy istnieje podstawa prawna przetwarzania danych. Przepisem uprawniającym administratorów danych do przetwarzania zwykłych danych osób fizycznych jest art. 6 ust. 1 RODO, zgodnie z którym, przetwarzanie danych jest dopuszczalne tylko wtedy, gdy spełniona jest jedna z przesłanek wskazanych w tym przepisie. Natomiast dla legalności przetwarzania danych szczególnych kategorii w rozumieniu art. 9 ust. 1 RODO, m.in. dotyczących zdrowia, którym przepisy RODO nadają szczególne znaczenie i reżim wykonywania na nich operacji przetwarzania, niezbędne jest spełnienie jednego z warunków wskazanych w art. 9 ust. 2 RODO. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że przesłanki te co do zasady są równoprawne, a wobec tego spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych. Ponadto należy zauważyć, że – zgodnie z zasadami rzetelności, ograniczenia celu i minimalizacji danych – każdy administrator musi dbać o to, aby dane osobowe były przetwarzane (w tym pozyskiwane) zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą, zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób

[499] DPNT.023.976.2025.

niezgodny z tymi celami oraz aby dane osobowe były adekwatne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane – art. 5 ust. 1 lit, a, b, c RODO. Podmiot chcący pozyskać dane osobowe powinien wskazać jasno określone kryteria, na podstawie których żądane dane osobowe powinny zostać udostępnione, powinien legitymować się co najmniej jedną z podstaw prawnych wynikających z art. 6 ust. 1 RODO (lub art. 9 ust. 2 RODO) oraz wskazać cel i uzasadnić potrzebę pozyskania danych.

Prezes UODO proszony był też o **interpretację przepisów dotyczących udostępniania materiałów z monitoringu wizyjnego w szkołach podstawowych, w szczególności w kontekście wniosków rodziców uczniów**[500]. W udzielonych wyjaśnieniach wskazał, że podstawy prawne funkcjonowania monitoringu wizyjnego w placówkach oświatowych reguluje art. 108a ustawy Prawo oświatowe[501]. Zgodnie z tym przepisem, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia, dyrektor szkoły lub placówki, w uzgodnieniu z organem prowadzącym szkołę lub placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring). Zgodnie z art. 108a ust. 4 nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, szkoła lub placówka przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nie dłuższy niż 3 miesiące od dnia nagrania. Dyrektor szkoły lub placówki informuje uczniów i pracowników szkoły lub placówki o wprowadzeniu monitoringu, w sposób przyjęty w danej szkole lub placówce, nie później niż 14 dni przed uruchomieniem monitoringu (art. 108a ust. 6). To także dyrektor szkoły lub placówki uzgadnia z organem prowadzącym szkołę lub placówkę odpowiednie środki techniczne i organizacyjne w celu ochrony przechowywanych nagrań obrazu oraz danych osobowych uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, uzyskanych w wyniku monitoringu (art. 108a ust. 9). Na podstawie ww. przepisów można uznać, że dyrektor szkoły lub placówki oświatowej jest organem odpowiedzialnym za prawidłowe funkcjonowanie monitoringu w szkole. W myśl zasady rozliczalności (art. 5 ust. 2 RODO) to na nim spoczywa obowiązek zapewnienia zgodności przetwarzania danych z prawem. To, jakie środki techniczne i organizacyjne powinny być brane pod uwagę w fazie planowania, oceny skutków i zapewnienia bezpieczeństwa w przypadku stosowania monitoringu wizyjnego oraz kto powinien mieć dostęp do nagrań z monitoringu i ile czasu dane mogą być przechowywane, zostało omówione podczas webinarium pt. „Monitoring wizyjny w szkole – aspekty prawne i techniczne. Niezależnie od powyższego, w kontekście wniosków składanych o udostępnienie danych osobowych utrwalonych w ramach monitoringu szkoły należy brać pod uwagę przepis art. 15 RODO. Na jego podstawie podmiot danych (czyli osoba, której dane osobowe są

[500] DPNT.023.688.2025.
[501] Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2024 r. poz. 737).

przetwarzane, jak też jej przedstawiciel ustawowy) ma prawo dostępu do danych oraz uzyskania ich kopii. Więcej informacji na ten temat można znaleźć w sprawozdaniu z działalności Prezesa UODO w roku 2020 (str. 77 i nast.) oraz we wskazanych w nim decyzjach[502].

Z kolei Rzeczniczka Praw Dziecka zwróciła się do Prezesa UODO o stanowisko ws. **stosowanej przez organy policji** praktyki **publikowania, w tym mediach społecznościowych, materiałów z akcji o charakterze edukacyjnym i profilaktycznym z udziałem dzieci** (np. ze spotkań dotyczących zasad bezpieczeństwa na drodze)[503]. W odpowiedzi organ nadzorczy zaznaczył, że wizerunek człowieka jest nie tylko dobrem osobistym i podlega ochronie na podstawie przepisów Kodeksu cywilnego, ale stanowi też informację o charakterze osobowym i jego przetwarzanie (np. udostępnianie) powinno odbywać się zgodnie z zasadami ochrony danych osobowych zawartymi w RODO. W ich świetle dzieci traktowane są w sposób szczególny, uwzględniający fakt, że mają słabszą pozycję prawną (jako podmioty pozbawione zdolności do czynności prawnych lub dysponujące nią w zakresie ograniczonym) i posiadające mniejszą świadomość przysługujących im praw. W motywie 38 RODO podkreślono, że szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich. Ponadto, zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć (motyw 58 RODO). W konsekwencji administratorzy przetwarzający dane osobowe dzieci, np. publikujący ich wizerunki, powinni działać zgodnie z zasadami określonymi w art. 5 RODO, w szczególności dysponować odpowiednią podstawą wynikającą z przepisów prawa. Stosownie do art. 5 ust. 1 lit. a RODO dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą („zgodność z prawem, rzetelność i przejrzystość").

Odnosząc się do opisanych działań organów policji, Prezes UODO zaznaczył, że w ustawie o Policji[504] przewidziano, że do podstawowych zadań Policji należy m.in. inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi (art. 1 ust. 2 pkt 3). Można zatem uznać, że organizowanie spotkań policji z dziećmi i młodzieżą w celu przekazania im wiedzy o swojej działalności, o zasadach ruchu drogowego i inne podobne inicjatywy mieszczą się w szeroko pojętej prewencji

[502] Np. decyzja z 30 listopada 2020 r. sygn. ZWOS.440.5216.2019.
[503] DPNT.051.17.2025.
[504] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636 ze zm.).

i budowania zaufania społecznego do organów policji. W konsekwencji uzasadniona jest ocena, że dane osobowe dzieci przetwarzane są w ramach takich działań na podstawie przepisu art. 6 ust. 1 lit. e RODO, dopuszczającego przetwarzanie niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Niemniej w ocenie Prezesa UODO brak jest podstaw do uznania, że publikowanie przez jednostki policji na ich oficjalnych stronach internetowych, w mediach społecznościowych oraz w innych publicznie dostępnych materiałach treści zawierających wizerunki dzieci uczestniczących w ww. spotkaniach jest konieczne i dopuszczalne w oparciu o ww. przesłankę. Należy wyraźnie rozróżnić dwie odrębne działalności: samo prowadzenie zajęć edukacyjnych przez funkcjonariuszy policji z udziałem dzieci oraz utrwalanie i następnie upublicznianie relacji z tych spotkań. Takie upublicznianie nie jest bowiem samo w sobie konieczne do realizacji celu edukacyjnego i zadań policji określonych w art. 1 ust. 2 pkt 3 ustawy o Policji.

Z przeglądu wybranych stron internetowych komend powiatowych policji w Polsce wynika, że praktyka publikacji zdjęć (nagrań) ze spotkań edukacyjnych z dziećmi jest różna. Niektóre jednostki publikują takie materiały w sposób uniemożliwiający rozpoznanie twarzy dzieci (są odwrócone tyłem lub bokiem, wizerunek jest rozmyty, itp.), co stanowi niewątpliwie dobrą praktykę, ale zdarzają się także sytuacje publikacji zdjęć z wyraźnymi wizerunkami. Taka publikacja pełnych wizerunków dzieci, umożliwiających ich identyfikację, budzi wątpliwości w świetle zasady minimalizacji danych przewidzianej w art. 5 ust. 1 lit. c RODO, który stanowi, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Prezes UODO zaznaczył, że wykorzystywanie wizerunków dzieci przez różne podmioty publiczne i organy władzy publicznej jest zjawiskiem niestety dość powszechnym i dotyczy nie tylko policji. Do Prezesa Urzędu Ochrony Danych Osobowych wpływają skargi dotyczące m.in. przedszkoli, szkół, placówek medycznych czy urzędów publicznych, które bez zgody rodziców (lub też po jej wycofaniu) przetwarzały (udostępniły) wizerunek dziecka, np. zdjęcia na stronie internetowej placówki bądź też na profilu w mediach społecznościowych.

Organ nadzorczy podkreślił, że samo korzystanie przez administratora, także z sektora publicznego, z internetowych serwisów społecznościowych powinno być poprzedzone uprzednią analizą ryzyka, ponieważ dostęp do informacji uzyskuje podmiot zarządzający takim serwisem, a więc inny administrator. W tym kontekście warto zwrócić uwagę na wyrok Naczelnego Sądu Administracyjnego z 28 lutego 2024 r.[505], w którym sąd 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 i ról podmiotów występujących w tych procesach. Analiza ryzyka może pozwolić administratorowi upewnić się, czy dane z tego serwisu można odzyskać, czy w każdej sytuacji istnieje możliwość zrealizowania prawa osób do

[505] Sygn. akt II OSK 3839/21.

dostępu do dotyczących ich danych, czy nie należy mieć stosownych kopii nagrań ze względów bezpieczeństwa, jak też powinien rozważyć w pewnych okolicznościach inne, odpowiednie środki ochrony danych, jak np. ich anonimizacja.

Prezes UODO zapewnił, że w sposób szczególny podchodzi do ochrony wizerunku dzieci, podejmując szereg inicjatyw edukacyjnych na rzecz uświadamiania społeczeństwa o wadze ochrony danych osobowych dzieci. Jednocześnie zadeklarował swoje i Urzędu Ochrony Danych Osobowych wsparcie w przypadku działań Rzecznika Praw Dziecka w tym obszarze.

W 2025 r. Prezes UODO udzielił odpowiedzi na pytanie posła RP dotyczące prawa **dostępu do dokumentacji uczennicy szkoły podstawowej w ramach interwencji poselskiej** mającej na celu wyjaśnienie kwestii przeniesienia jej do innej placówki[506]. Zaznaczył w niej, że uprawnienia parlamentarzystów do uzyskania informacji lub wyjaśnień oraz do podejmowania interwencji wynikają bezpośrednio z unormowań ustawy o wykonywaniu mandatu posła i senatora[507]. Niemniej, pomimo doniosłości tego prawa, podlega ono ograniczeniom. Ograniczenia takie dotyczą ochrony dóbr osobistych oraz tajemnic prawnie chronionych, o czym stanowi art. 19 ust. 1 powołanej ustawy. Przepis ten stanowi, że w wykonywaniu mandatu poseł lub senator ma prawo, jeżeli nie narusza dóbr osobistych innych osób, do uzyskiwania informacji i materiałów, wstępu do pomieszczeń, w których znajdują się te informacje i materiały oraz wglądu w działalność organów administracji rządowej i samorządu terytorialnego, a także spółek z udziałem Skarbu Państwa oraz zakładów i przedsiębiorstw państwowych i samorządowych, z zachowaniem przepisów o tajemnicy prawnie chronionej (ust. 1). Zasady i tryb udostępniania posłom i senatorom informacji niejawnych określają przepisy o ochronie informacji niejawnych (ust. 2). Jednocześnie zgodnie z art. 20 ust. 1 powyższej ustawy, poseł lub senator ma prawo podjąć – w wykonywaniu swoich obowiązków poselskich lub senatorskich – interwencję w organie administracji rządowej i samorządu terytorialnego, zakładzie lub przedsiębiorstwie państwowym oraz organizacji społecznej, a także w jednostkach gospodarki niepaństwowej dla załatwienia sprawy, którą wnosi we własnym imieniu albo w imieniu wyborcy lub wyborców, jak również zaznajamiać się z tokiem jej rozpatrywania. Zgodnie z ust. 2 ww. przepisu, organy i jednostki wymienione w ust. 1, wobec których poseł lub senator podjął interwencję, są obowiązane najpóźniej w ciągu czternastu dni powiadomić posła lub senatora o stanie rozpatrywania sprawy i w terminie uzgodnionym z posłem lub senatorem ostatecznie ją załatwić. Kierownicy organów i jednostek, o których mowa w ust. 1, są obowiązani niezwłocznie przyjąć posła lub senatora, który przybył w związku ze sprawą wynikającą z wykonywania jego mandatu, oraz udzielić informacji i wyjaśnień dotyczących sprawy (ust. 3).

W kontekście uzyskania dostępu do dokumentacji zawierającej informację o konkretnym uczniu, którego dane osobowe są przetwarzane przez publiczną szkołę należy podkreślić, że Prawo oświatowe w art. 30a wprowadza szczególne ograniczenia w zakresie przetwarzania danych osobowych, a także zachowania

[506] DPNT.023.758.2025.
[507] Ustawa z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora (Dz. U. z 2024 r. poz. 907).

poufności informacji dotyczących uczniów. Jak wynika bowiem z ust. 2 tego przepisu nauczyciele oraz inne osoby pełniące funkcje lub wykonujące pracę w szkole są obowiązani do zachowania w poufności informacji uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą, dotyczących zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, seksualności, orientacji seksualnej, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych uczniów. W istocie więc ustawodawca wprowadził do Prawa oświatowego tajemnicę prawnie chronioną obejmującą szereg informacji o uczniach. Zgodnie z art. 30a ust. 3 Prawa oświatowego tajemnica ta nie ma zastosowania w trzech przypadkach: 1) zagrożenia zdrowia ucznia; 2) jeżeli uczeń, a w przypadku ucznia niepełnoletniego jego rodzic, wyrazi zgodę na ujawnienie określonych informacji; 3) gdy przewidują to przepisy szczególne.

Podobne ograniczenia związane z dostępem do informacji na temat konkretnego ucznia omawianymi w ramach zebrań rady pedagogicznej, które są protokółowane, wynikają z art. 73 ust. 3 Prawa oświatowego. W przepisie tym określono, że osoby biorące udział w zebraniu rady pedagogicznej są obowiązane do nieujawniania spraw poruszanych na zebraniu rady pedagogicznej, które mogą naruszać dobra osobiste uczniów lub ich rodziców, a także nauczycieli i innych pracowników szkoły lub placówki.

Jednym z dóbr osobistych jest natomiast prawo do prywatności.

Jednocześnie Prezes UODO zaznaczył, że administratorem danych osobowych uczniów przetwarzanych przez szkołę jest jej dyrektor. W sytuacji, gdy wpływa do niego wniosek o dostęp do danych ucznia, powinien ocenić go, biorąc pod uwagę jego treść, oraz ustalić, czy udostępnienie to nie naruszy prawa do prywatności ucznia, czy nie jest potrzebna zgoda jego rodzica (przedstawiciela ustawowego, mając na względzie zakres tajemnicy wynikającej z Prawa oświatowego). W przypadku wniosku składanego przez posła pod uwagę wziąć należy przepisy ustawy o wykonywaniu mandatu posła i senatora. Ocena dopuszczalności udostępnienia danych, w świetle szczegółowych okoliczności konkretnej sprawy, należy do administratora. Powinien on udostępnić jedynie te informacje, które nie spełniają przesłanek ograniczenia informacji wskazanych w art. 19 ust. 1 ustawy o wykonywaniu mandatu posła i senatora.

### Ad. 8. Obowiązki związane z wyznaczeniem i zapewnieniem niezależności inspektora ochrony danych

W 2025 roku administratorzy skierowali do organu nadzorczego wiele pytań dotyczących istotnych kwestii związanych z pełnieniem funkcji przez inspektora ochrony danych. Dotyczyły one wyznaczania IOD, zawiadamiania Prezesa UODO o jego wyznaczeniu czy też zapewnienia inspektorowi właściwych warunków do pełnienia funkcji albo powierzenia mu dodatkowych zadań.

Odpowiadając na pytanie o **konieczność wyznaczenia IOD przez podmiot medyczny**[508] organ nadzorczy wskazał, że podmiot ten – niezależnie od tego, czy

[508] DPNT.5101.105.2025.

będzie korzystać z usług podmiotu przetwarzającego, który będzie przechowywać dane pacjenta w chmurze i który posiada własnego inspektora ochrony danych – zobowiązany jest samodzielnie ocenić, czy taki obowiązek istnieje w przypadku tego podmiotu medycznego jako administratora. Odwołując się do odpowiedzi na pytanie: Czy należy wyznaczyć IOD w niepublicznym zakładzie opieki zdrowotnej?[509], organ nadzorczy wskazał, że w przedstawionym przypadku administrator powinien dokonać oceny konieczności wyznaczenia IOD, analizując, czy spełnia którąś z przesłanek wskazanych w art. 37 ust. 1 lit. b i c RODO, tj.:

b) czy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) czy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 (np. dane dotyczące zdrowia), lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

Organ nadzorczy przypomniał ponadto, że pomocne w interpretacji terminów i kryteriów użytych w tych przesłankach, tj. „główna działalność", „regularne i systematyczne monitorowanie" oraz „na dużą skalę", są przede wszystkim Wytyczne dotyczące inspektorów ochrony danych[510], zawierające także wiele praktycznych, konkretnych przykładów sytuacji spełniających te kryteria (str. 8 i 9). Grupa Robocza Art. 29 w ww. Wytycznych wskazała, że „główna działalność" może być rozumiana jako fundamentalne operacje podejmowane w celu osiągnięcia celów administratora lub podmiotu przetwarzającego. Obejmuje ona również wszelkie działania, w których przetwarzanie danych stanowi nieodłączną część działalności administratora lub podmiotu przetwarzającego. Na przykład przetwarzanie danych dotyczących stanu zdrowia, takich jak dokumentacja zdrowotna pacjenta, powinno być uważane za jedno z głównych działań szpitala (czy też jak w omawianym przypadku placówki medycznej). Odnośnie zaś do „dużej skali" Grupa robocza Art. 29 zalecała natomiast rozważenie następujących czynników w celu określenia, czy przetwarzanie jest przeprowadzane na dużą skalę: liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa; zakres przetwarzanych danych osobowych; okres, przez jaki dane są przetwarzane; zakres geograficzny przetwarzania danych osobowych. Do przykładów „przetwarzania na dużą skalę" zalicza przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności. Jednocześnie jako przykład przetwarzania niemieszczącego się w definicji „dużej skali" Grupa robocza Art. 29 wskazuje przetwarzanie danych pacjentów dokonywane przez pojedynczego lekarza.

[509] Odpowiedź ta opublikowana jest na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/497/2366.

[510] Wytyczne dotyczące inspektorów ochrony danych dostępne są pod linkiem: https://uodo.gov.pl/data/filemanager_pl/15.pdf.

Organ nadzorczy zwrócił również uwagę, że Grupa robocza Art. 29 zaleca, aby przeprowadzenie oceny w zakresie istnienia obowiązku wyznaczenia inspektora udokumentować, a nawet powtarzać taką ocenę w razie potrzeby co jakiś czas. Sytuacja danego podmiotu może się bowiem zmieniać. Na przykład mała przychodnia może stopniowo rozszerzać swoją działalność o nowe usługi i świadczenia i po jakimś czasie stać się dużym podmiotem przetwarzającym dane wrażliwe na dużą skalę.

W odpowiedzi poinformowano także, że warto zapoznać się z treścią dwóch kodeksów postępowania dla podmiotów sektora medycznego, które zostały zatwierdzone przez Prezesa UODO. Administratorzy znajdą tam pomocne informacje dotyczące wyznaczenia IOD w placówkach medycznych[511].

Ciekawe zagadnienie dotyczące IOD pojawiło się w pytaniu od likwidatora spółki. Dotyczyło ono tego, **czy spółka w likwidacji może wyznaczyć inspektora ochrony danych**[512].

W odpowiedzi organ nadzorczy wskazał, że zgodnie z przepisami ustawy z 15 września 2000 r. – Kodeks spółek handlowych, likwidator działa w imieniu spółki w okresie likwidacji, reprezentując jej interesy i podejmując wszelkie niezbędne działania związane z procesem likwidacyjnym. Jest również uprawniony do podejmowania decyzji w imieniu spółki oraz do podejmowania wszelkich czynności prawnych, administracyjnych i finansowych koniecznych do zakończenia działalności spółki zgodnie z przepisami prawa. Mając zatem powyższe na uwadze, w okresie likwidacji, tj. do czasu wykreślenia spółki z Krajowego Rejestru Sądowego, likwidator, działając w imieniu likwidowanej spółki, może wyznaczyć inspektora ochrony danych i inspektor może pełnić swoją funkcję. Powołanie IOD na pewno zwiększy szanse na zapewnienie zgodności przetwarzania danych osobowych z przepisami o ochronie danych. Organ nadzorczy podkreślił jednak, że rola inspektora nie może polegać na „realizacji obowiązków administratora", bo byłoby to niezgodne z prawem. Rola IOD polega na staniu na straży właściwego przestrzegania przez administratora – w tym przypadku spółki w likwidacji – przepisów o ochronie danych. Wobec tego na inspektora nie mogą być nakładane zadania, które następnie – zgodnie z art. 39 ust. 1 lit. b RODO – miałby on poddawać swojej ocenie. Doprowadziłoby to do sytuacji, w której IOD sprawowałby *de facto* nadzór nad własną działalnością, a więc do konfliktu interesów, którego występowania zakazuje art. 38 ust. 6 RODO[513].

Odnosząc się natomiast do kwestii przetwarzania danych osobowych w przypadku likwidacji spółki, organ nadzorczy poinformował, że likwidator ma obowiązek zadbać o prawidłowe zabezpieczenie i uporządkowanie dokumentacji

---

[511] Informacje na temat tych kodeksów znaleźć można na stronie internetowej UODO w zakładce Kodeksy i certyfikacja pod linkiem: https://uodo.gov.pl/pl/426/1110.

[512] DPNT.5101.102.2025.

[513] Na niewłaściwą praktykę przerzucania obowiązków administratora na IOD organ nadzorczy zwracał uwagę m.in. w: odpowiedzi na pytanie „Czy administrator może przerzucać swoje obowiązki na IOD?", zamieszczonej w Biuletynie UODO - Wydanie specjalne, który dostępny jest pod linkiem: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod; sprawozdaniu krajowym polskiego organu nadzorczego opracowanego w ramach CEF DPO (str. 9 i 10) (https://uodo.gov.pl/pl/138/2960); prezentacji załączonej do materiału Niezależność IOD musi być standardem – podsumowanie efektów spotkania w UODO (https://uodo.gov.pl/pl/138/3118), w szczególności w panelach nr 1, 3 i 4.

spółki, w tym pracowniczej, a następnie przekazać ją do przechowywania właściwemu podmiotowi. Przepisy prawa nakładają obowiązki przechowywania dokumentacji, określając okresy jej przechowywania w sytuacji likwidacji podmiotu. Zgodnie z art. 288 § 3 ustawy – Kodeks spółek handlowych (rozdział 6 Rozwiązanie i likwidacja spółki) księgi i dokumenty rozwiązanej spółki powinny być oddane na przechowanie osobie wskazanej w umowie spółki lub w uchwale wspólników. W przypadku braku takiego wskazania, przechowawcę wyznacza sąd rejestrowy. Odnośnie zaś do przechowywania dokumentacji pracowniczej i płacowej w rozdziale 4b ustawy o narodowym zasobie archiwalnym i archiwach określono postępowanie z dokumentacją osobową i płacową w przypadku likwidacji lub upadłości pracodawcy. Przepisy tej ustawy określają również zasady udostępniania przejętej dokumentacji oraz wydawanie z niej odpisów i kopii na żądanie osoby, której dokumentacja dotyczy. Zadania takie nie mogą być wykonywane przez IOD.

Odpowiadając natomiast na pytanie, czy wskazane przez likwidatora informacje mogą zostać uwzględnione w rejestrze IOD, organ nadzorczy poinformował, że Urząd Ochrony Danych Osobowych nie prowadzi jawnego rejestru inspektorów ochrony danych (nie dokonuje rejestracji wyznaczonych IOD), niemniej w razie powołania IOD administrator zobowiązany jest poinformować o tym Prezesa UODO (art. 10 ustawy z 10 maja 2018 r. o ochronie danych osobowych). Zgodnie natomiast z art. 10 ust. 4 ustawy o ochronie danych osobowych podmiot, który wyznaczył IOD, ma obowiązek zawiadomienia Prezesa UODO o jego odwołaniu. A zatem przed formalnym wykreśleniem spółki w likwidacji z KRS osoba upoważniona do reprezentowania spółki w likwidacji – likwidator powinien powiadomić Prezesa UODO o odwołaniu IOD.

Wątpliwości innego z administratorów dotyczyły tego, jak IOD powinien być umiejscowiony w strukturze administratora, aby spełnić **warunek bezpośredniego podlegania najwyższemu kierownictwu**[514]. Organ nadzorczy wskazał, że jedną z gwarancji niezależności IOD, wskazanych w RODO, jest właśnie bezpośrednia podległość inspektora ochrony danych najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (art. 38 ust. 3). Celem tego przepisu jest zapobieganie sytuacji, w której pomiędzy inspektorem a najwyższym kierownictwem (np. ministrem, prezesem, itp.) istniałyby ogniwa pośredniczące (kolejni zwierzchnicy, np. dyrektor departamentu), ponieważ sytuacja taka może prowadzić do ograniczenia skuteczności działań inspektora ochrony danych.

Odwołując się również do doktryny, organ nadzorczy wskazał, że podleganie przez inspektora wyłącznie najwyższemu kierownictwu pozwala na efektywne i niezakłócone sprawowanie jego funkcji, polegającej przede wszystkim na staniu na straży przestrzegania prawa oraz poszanowania praw osób, których dane dotyczą. Takie ukształtowanie funkcji IOD służy również interesom administratora, który przecież ponosi bezpośrednią odpowiedzialność za zgodną z prawem działalność i prawidłowe przetwarzanie danych osobowych. Z jego perspektywy zapewnienie inspektorowi możliwości bezpośredniego kontaktu, bez pośrednictwa kierownictwa

[514] DPNT.5101.68.2025.

niższego szczebla, daje gwarancję najpełniejszej i najszybszej informacji w kwestii procesów przetwarzania i umożliwia szybką reakcję na zalecenie inspektora[515]. Z kolei podległość innym osobom niż podmioty wykonujące zadania administratora (lub podmiotu przetwarzającego) oznacza faktyczne ograniczenie w możliwości nadzorowania działań tych osób przez inspektora, co również stanowi istotną przyczynę przyjęcia konstrukcji nakazującej zapewnienie bezpośredniej podległości inspektora ochrony danych najwyższemu kierownictwu[516].

Z powyższych powodów – w ocenie organu nadzorczego – wszelkie rozwiązania, w których inspektor ochrony danych nie podlega bezpośrednio najwyższemu kierownictwu administratora należy uznać za niezgodne z art. 38 ust. 3 RODO.

Kolejne pytanie pochodzące od ww. administratora dotyczyło kwestii **możliwości powierzenia jednemu inspektorowi ochrony danych pełnienia funkcji IOD u kilku administratorów**. W odpowiedzi Prezes UODO wskazał, że taka sytuacja uregulowana jest w art. 37 ust. 3 RODO, zgodnie z którym jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć jednego inspektora ochrony danych, ale uwzględnić przy tym należy ich strukturę organizacyjną i wielkość.

Odwołując się do doktryny, organ nadzorczy podkreślił, że prawodawca unijny w ww. przepisie nie wprowadził obowiązku powołania dla kilku organów/podmiotów publicznych jednego inspektora ochrony danych. Powołanie jednego IOD traktuje natomiast jako uprawnienie uzasadnione ekonomicznie i racjonalne z punktu widzenia zapewnienia prawidłowego przetwarzania danych osobowych przez podmioty publiczne, jeżeli spełnione są warunki wskazane w przepisach rozporządzenia 2016/679[517]. Skorzystanie z takiego rozwiązania wymaga jednak dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora danych. Organ nadzorczy zwrócił także uwagę, że trzeba mieć przy tym świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył, oraz tzw. efektywnej dostępności inspektora dla osób z danej organizacji. Organ nadzorczy przypomniał również, że aby zapewnić IOD właściwe funkcjonowanie, w RODO wprowadzono odpowiednie przepisy gwarancyjne, zaś za ich przestrzeganie i odpowiednie wdrożenie odpowiada każdy z administratorów. Wśród tych gwarancji znajdują się m.in. bezpośrednia podległość IOD najwyższemu kierownictwu, wspieranie IOD w wypełnianiu jego zadań poprzez zapewnienie mu niezbędnych zasobów do realizacji zadań, a także do utrzymania jego

[515] E. Bielak-Jomaa [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. D. Lubasz, Warszawa 2018, art. 38.
[516] 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. 38.
[517] E. Bielak-Jomaa [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. D. Lubasz, Warszawa 2018, art. 37.

wiedzy fachowej, zakaz wydawania instrukcji IOD co do wykonywania przez niego zadań, unikanie konfliktu interesów oraz obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez IOD. Zatem to do administratorów należy przyjęcie takich rozwiązań organizacyjnych, które zagwarantują, że IOD będzie w stanie autentycznie wypełniać swoje obowiązki wobec każdej obsługiwanej przez niego organizacji i to w sposób w pełni odpowiadający przepisom prawa i potrzebom konkretnego administratora. Organ nadzorczy przypomniał również, że zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO, każdy administrator powinien umieć wykazać się szczegółowymi, dostosowanymi do swojej działalności, rozwiązaniami w zakresie poszczególnych obowiązków wynikających z przepisów o ochronie danych osobowych, w tym tych dotyczących IOD.

W odpowiedzi zwrócono również uwagę, że istotna w procesie przyjmowania rozwiązań dotyczących funkcjonowania inspektora jest również rola samego IOD jako fachowego doradcy i podmiotu monitorującego przestrzeganie przepisów o ochronie danych osobowych. Jak zostało wskazane w odpowiedzi na pytanie „Czy administrator jest zobowiązany na podstawie rozporządzenia 2016/679 do zapewnienia inspektorowi zespołu IOD?”[518], „administrator wyznaczając na inspektora daną osobę powinien wspólnie z nią określić zasady dotyczące zapewnienia takiemu inspektorowi wystarczającej ilości czasu na wypełnianie jego obowiązków, pomocy w stworzeniu planu jego pracy, a w razie potrzeby wsparcie jego funkcjonowania zespołem odpowiednich specjalistów”. Dodatkowo, wyznaczony przez administratora IOD może budować właściwą świadomość danej organizacji i doradzać jej w zakresie zapewnienia w powyższym obszarze należytych standardów, w tym np. identyfikować i sygnalizować administratorowi ryzyko wystąpienia konfliktu interesów i innych zagrożeń przy wykonywaniu jego zadań, by możliwe było odpowiednio wczesne zapobieganie takim sytuacjom.

Ponieważ z pisma administratora dotyczącego tej sprawy nie wynikało, czy konsultował projektowane rozwiązania z inspektorem ochrony danych, organ nadzorczy wskazał, że zapoznanie się z opinią IOD byłoby bardzo pomocne. Warto bowiem w takich sytuacjach poznać punkt widzenia osoby, której te zmiany miałyby bezpośrednio dotyczyć i do której zadań należy monitorowanie prawidłowości przyjmowanych przez administratora rozwiązań w zakresie ochrony danych.

Pytanie od innego administratora z sektora publicznego dotyczyło wątpliwości w zakresie **możliwości wyznaczenia przez administratora dwóch inspektorów ochrony danych**[519]. Organ nadzorczy przypomniał, że od początku stosowania rozporządzenia 2016/679 informował, że wyznaczenie więcej niż jednego IOD jest nieprawidłowe. Do tego zagadnienia odniósł się w szczególności w odpowiedzi na pytanie „Czy można powołać więcej niż jednego IOD?”[520]. Wskazał w niej, że przepisy

[518] Odpowiedź opublikowana została w Biuletynie UODO - Wydanie specjalne, dostępnym pod linkiem: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.
[519] DPNT.5101.94.2025.
[520] Treść odpowiedzi na pytanie „Czy można powołać więcej niż jednego IOD? opublikowana jest w Biuletynie UODO – Wydanie specjalne (str. 32), który dostępny jest na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

o ochronie danych osobowych nie przewidują możliwości wyznaczenia więcej niż jednego IOD. Prawodawca przyjął bowiem, że dla wszystkich – zarówno wewnątrz podmiotu będącego administratorem, jak i w relacjach zewnętrznych – musi być jasne, kto pełni tę funkcję. Dzięki temu zarówno pracownicy administratora, jak i osoby, których dane dotyczą, czy organ nadzorczy mogą w łatwy sposób skontaktować się z IOD, bez konieczności dokonywania dodatkowych analiz, który z inspektorów byłby właściwy w danej sprawie. Dla osób, których dane dotyczą, oraz dla organu nadzorczego IOD jest bowiem punktem kontaktowym (zgodnie z art. 38 ust. 4 i art. 39 ust. 1 lit. e RODO). Jednocześnie przepisy ustawy o ochronie danych osobowych doprecyzowują sposób realizacji obowiązku informowania o powołanym IOD i zobowiązują podmiot, który wyznaczył inspektora ochrony danych, by udostępnił imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora na swojej stronie internetowej (art. 11), a także przekazał te dane Prezesowi UODO (art. 10 tej ustawy).

Jednocześnie organ nadzorczy wskazał, że w ramach zapewnienia wsparcia IOD w wykonywaniu jego zadań w dużych podmiotach, takich jak np. ministerstwa, właściwym rozwiązaniem – oprócz powołania zespołu inspektora ochrony danych – może być wyznaczenie jego zastępcy, tj. osoby zastępującej inspektora w czasie jego nieobecności[521]. Podsumowując tę odpowiedź, organ nadzorczy podkreślił, że to do administratora należy przyjęcie takich rozwiązań organizacyjnych, które zapewnią wyznaczonemu przez niego inspektorowi ochrony danych realną możliwość prawidłowego wypełniania obowiązków. Wskazał ponadto, że ważne jest włączenie IOD do wspólnego określenia zasad dotyczących zapewnienia inspektorowi odpowiednich warunków do wykonywania jego funkcji.

Innym problemem, z którym zwrócił się administrator, były **wątpliwości co do powierzenia funkcji IOD sekretarzowi szkoły lub głównemu specjaliście ds. kadr i płac**[522]. Odnosząc się do tych wątpliwości, organ nadzorczy wskazał, że gdyby administrator chciał nałożyć na IOD dodatkowe zadania bądź wyznaczyć do pełnienia tej funkcji osobę, która dotychczas miała w zakresie swoich obowiązków inne zadania (w tym przypadku związane z obsługą obszaru kadr i płac bądź z pełnieniem funkcji sekretarza szkoły), powinien dokonać starannej analizy. Musi mieć bowiem pewność, że osoba wyznaczona do pełnienia funkcji IOD będzie miała zapewnione właściwe warunki dla zachowania niezależności i prawidłowego wykonywania zadań IOD. Administrator lub podmiot przetwarzający są bowiem – zgodnie z art. 38 ust. 6 RODO – zobowiązani zapewnić, by nakładanie na IOD innych zadań nie powodowało konfliktu interesów. Pomocne w dokonaniu oceny w tym zakresie może być zastosowanie trzech kryteriów: organizacyjnego, merytorycznego i czasowego[523].

---

[521] Więcej informacji w tym zakresie znaleźć można w materiale „IOD może mieć dwóch zastępców", który znajduje się w Biuletynie UODO – Wydanie specjalne (str. 12), dostępnym pod linkiem https://uodo.gov.pl/file/5579.

[522] DPNT.5101.56.2025.

[523] Zob. odpowiedź na pytanie „Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?", która dostępna jest pod linkiem https://uodo.gov.pl/pl/495/2372.

Biorąc pod uwagę kryterium organizacyjne wskazać należy, że IOD powinien podlegać bezpośrednio najwyższemu kierownictwu jednostki organizacyjnej. W przypadku jednoczesnego pełnienia funkcji IOD i wykonywania innych zadań wykluczone jest rozwiązanie, w którym osoba taka podlegałaby np. dyrektorowi departamentu, kierownikowi działu lub jakiejkolwiek innej osobie, która nie jest najwyższym kierownictwem w rozumieniu art. 38 ust. 3 RODO. To oznacza, że IOD nie może podlegać jakimkolwiek innym osobom niż najwyższe kierownictwo (art. 38 ust. 3 RODO). Ma mu to gwarantować niezależne, prawidłowe i skuteczne wykonywanie funkcji.

Z punktu widzenia kryterium merytorycznego istotne jest, aby inne obowiązki nie wpływały negatywnie na niezależne wykonywanie zadań IOD. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Konflikt interesów następuje, jeśli nie można pogodzić prawidłowego wykonywania zadań IOD z realizacją innych zadań. Wówczas pomiędzy zadaniami występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. Oznacza to m.in., że IOD nie może zajmować w organizacji stanowiska, na którym określa się sposoby i cele przetwarzania danych osobowych. W Wytycznych dotyczących IOD wskazane zostały przykłady takich stanowisk. Należą do nich: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli sprawujące je osoby biorą udział w określaniu celów i sposobów przetwarzania danych osobowych. Na te kwestie zwrócił uwagę również Trybunał Sprawiedliwości Unii Europejskiej w wyroku C-453/21 z 9 lutego 2023 r. w sprawie X-FAB Dresden GmbH & Co. KG. Trybunał stwierdził m.in., 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.

Odnosząc się do przedstawionej przez administratora sytuacji, organ nadzorczy wskazał, że wydaje się, że praca w dziale kadr i płac czy też wykonywanie zadań związanych z pełnieniem funkcji sekretarza szkoły może wiązać się z podejmowaniem decyzji lub współuczestniczeniem w podejmowaniu decyzji co do określania celów i sposobów przetwarzania danych osobowych. Co ważne, może to dotyczyć nie tylko osoby kierującej takim działem. Zakres zadań pracownika działu kadr i płac nie został ustawowo określony i może on obejmować różnego rodzaju zadania, np. przygotowanie procesu rekrutacji, prowadzenie akt osobowych pracownika. Formułowanie treści ogłoszeń o pracę może wiązać się koniecznością określenia kategorii danych osobowych, których podania wymaga pracodawca w związku z prowadzoną rekrutacją na dane stanowisko. Natomiast prowadzenie akt osobowych pracownika to niejednokrotnie podejmowanie decyzji, czy i jakie dokumenty należy przechowywać w aktach osobowych pracownika oraz jak długo. Z kolei sekretarz szkoły odpowiada za szeroko rozumianą obsługę administracyjną placówki. Do jego zadań należy m.in. prowadzenie dokumentacji uczniów. Dlatego konieczne jest przeprowadzenie przez administratora analizy, czy wskazane w jego piśmie osoby,

w zakresie powierzonych im zadań, podejmują decyzje co do kluczowych aspektów przetwarzania na gruncie przepisów RODO. Należy przy tym pamiętać, że realizacja zadań prowadzących do określania celów i sposobów przetwarzania danych nie może należeć do IOD.

Organ nadzorczy wskazał również, że Europejska Rada Ochrony Danych w **Wytycznych 07/2020 dotyczących pojęć administratora i podmiotu przetwarzającego zawartych w RODO**, 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 (pkt 40).

Zgodnie natomiast z trzecim kryterium, które należy brać pod uwagę przy ocenie możliwości wystąpienia konfliktu interesów, tj. kryterium czasowym, IOD powinien dysponować czasem wystarczającym do wykonywania swoich zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania. Konflikt interesów może być również 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.

W podsumowaniu organ nadzorczy wskazał, że administrator – przed powierzeniem funkcji IOD osobie, która wykonuje już inne zadania – powinien zatem dokonać analizy, czy IOD będzie w stanie wykonywać prawidłowo swoje obowiązki. Natomiast nieprzeprowadzenie przez administratora analizy w powyższym zakresie może w konsekwencji spowodować naruszenie przepisów o ochronie danych osobowych.

**Podsumowując pytania od administratorów dotyczące pełnienia funkcji IOD** warto wskazać, że Prezes UODO od początku stosowania RODO uświadamiał administratorów zarówno co do ich obowiązków związanych z przetwarzaniem danych osobowych, w tym z wyznaczeniem IOD, jak również co do korzyści płynących z posiadania wsparcia w postaci fachowego, dobrze znającego organizację i niezależnego inspektora ochrony danych. Niemniej powyższe przykłady pytań od administratorów, które dotyczą inspektorów ochrony danych, dowodzą, że nadal istnieje potrzeba upowszechniania informacji zarówno na temat przesłanek wpływających na powstanie obowiązku wyznaczenia IOD, jak i warunków, jakie należy zapewnić, aby IOD mógł prawidłowo realizować swoje zadania. Mając na uwadze, że kwestie te wciąż budzą wątpliwości, organ nadzorczy również w tym okresie sprawozdawczym podejmował działania mające na celu podnoszenie wiedzy i świadomości w zakresie zagadnień związanych z wyznaczaniem, zadaniami i statusem IOD. Ich przykładem może być przeprowadzanie szkoleń dla jednostek samorządu terytorialnego m.in. w ramach akcji „UODO rusza w kraj”.

### Ad. 9. Inne zagadnienia

W związku z tym, że dane osobowe przetwarzane są niemal w każdej dziedzinie życia, wpływające do Prezesa UODO pytania dotyczą bardzo różnych sektorów

i sytuacji. Wielu z nich 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.

W 2025 r. wpłynęło np. **pytanie od posła w sprawie funkcjonowania systemu ROBUS (Rejestru Osób Biorących Udział w Postępowaniach Sądowych)**[524], w tym tego, kto jest administratorem i jaka jest podstawa prawna przekazywania przez samorządy zawodowe danych osobowych swoich członków. W odpowiedzi Prezes UODO wskazał, że system ROBUS został wprowadzony rozporządzeniem Ministra Sprawiedliwości[525] wydanym na podstawie art. 53e § 2 ustawy – Prawo o ustroju sądów powszechnych[526], który został dodany w 2024 r. Z definicji legalnej dotyczącej tego systemu zawartej w ww. rozporządzeniu wynika, że przez ROBUS należy rozumieć Rejestr Osób Biorących Udział w Postępowaniach Sądowych, za pośrednictwem którego właściwe samorządy zawodowe lub inne podmioty zobowiązane udostępniają sądom właściwe listy, rejestry i wykazy profesjonalnych uczestników postępowań sądowych na podstawie obowiązujących przepisów prawa (§ 2 pkt 13). Przepisy rozporządzenia określają zasady zakładania kont w portalu informacyjnym, rozróżniając konta dla osoby fizycznej oraz konto instytucjonalne (dla podmiotu publicznego). Przepis § 4 rozporządzenia wskazuje, że konto dla osoby fizycznej zakłada się po złożeniu przez nią na formularzu w portalu informacyjnym wniosku zawierającego: imiona i nazwisko, numer PESEL, a w przypadku obcokrajowca nieposiadającego numeru PESEL – datę urodzenia, nazwę kraju oraz serię i/lub numer dokumentu stwierdzającego tożsamość i obywatelstwo; adres poczty elektronicznej; wybranie profilu użytkownika; adres zamieszkania; numer telefonu komórkowego; w przypadku pełnomocnika zawodowego – numer wpisu na właściwą listę prowadzoną przez samorząd zawodowy. Mimo że z definicji systemu wynika, że jest to system, na podstawie którego właściwe samorządy zawodowe lub inne podmioty zobowiązane udostępniają sądom właściwe listy, rejestry i wykazy profesjonalnych uczestników postępowań sądowych na podstawie obowiązujących przepisów prawa to, ani przepisy powołanego rozporządzenia, ani ustawy – Prawo o ustroju sądów powszechnych, nie określają zasad, na jakich ma się odbywać przekazywanie tych informacji.

Na konieczność uregulowania tych zasad Prezes UODO zwracał uwagę już na etapie prac legislacyjnych, nad projektem rozporządzenia Ministra Sprawiedliwości w sprawie warunków technicznych korzystania z portalu informacyjnego i jego funkcjonowania oraz trybu zakładania, udostępniania i likwidacji konta w portalu informacyjnym[527], którym wprowadzono system ROBUS. Organ nadzorczy negatywnie odniósł się do projektowanych przepisów wskazując, że system ROBUS nie został zdefiniowany w Prawie o ustroju sądów powszechnych ani innych przepisach rangi ustawowej (§ 2 pkt 13 projektu rozporządzenia nie zawierał żadnych

[524] DPNT.052.4.2025.
[525] Rozporządzenie Ministra Sprawiedliwości z dnia 12 marca 2024 r. (Dz. U. z 2024 r. poz. 366).
[526] Ustawa z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2024 r. poz. 334).
[527] DOL.401.556.2023.

odesłań w tym zakresie). Nie zostało także odpowiednio wyjaśnione, kto jest administratorem systemu ROBUS, które samorządy zawodowe będą przekazywać dane do tego rejestru, w jakim zakresie oraz w jaki sposób. Brak było również szeregu rozwiązań wymaganych w związku z funkcjonowaniem tego typu rejestrów, w tym chociażby dotyczących retencji danych oraz powiązania sytemu ROBUS z innymi rejestrami publicznymi. Organ nadzorczy zwrócił wówczas projektodawcom uwagę, że dla zachowania zgodności z zasadami określonymi w RODO, w tym zasadą zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a), zasadą ograniczenia celu (art. 5 ust. 1 lit. b), zasadą minimalizacji danych (art. 5 ust. 1 lit. c), zasadą ograniczenia przechowywania (art. 5 ust. 1 lit. e) oraz zasadą integralności i poufności (art. 5 ust. 1 lit. f) konieczne jest wprowadzenie wielu zmian. Po pierwsze – niezbędne jest uregulowanie funkcjonowania sytemu ROBUS i przetwarzania w nim danych osobowych w sposób kompleksowy. Po drugie – rozwiązania w takim zakresie, jako kształtujące prawa i obowiązki, w tym w odniesieniu do przetwarzania danych osobowych, powinny być regulowane na poziomie ustawowym. Jest to konieczne z uwagi na konstytucyjną zasadę praworządności (art. 7 Konstytucji RP) oraz postanowienia dotyczące ochrony danych osobowych (art. 51 w zw. z art. 31 ust. 3 Konstytucji RP), jak również ze względu na wymogi stawiane rejestrom publicznym wynikające z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[528] dotyczące chociażby wymogów wiążących podmioty prowadzące taki rejestr (art. 14) czy też zasad udostępniania z niego danych (art. 15). Pomimo uwag ze strony Prezesa UODO kwestionowane rozwiązania zostały przyjęte w wersji aktualnie obowiązującej.

Inne z pytań dotyczyło tego, czy **numer działki ewidencyjnej** wskazany w decyzji administracyjnej (np. decyzji środowiskowej, decyzji o pozwoleniu na budowę) **to dana osobowa**, a w konsekwencji **wymaga anonimizacji** przy udostępnianiu decyzji administracyjnych w trybie ustawy o dostępie do informacji publicznej lub przy ich publikacji w Biuletynie Informacji Publicznej[529]. W odpowiedzi organ nadzorczy wyjaśnił, że zgodnie z art. 4 pkt 1 RODO „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. W świetle przywołanej definicji legalnej rozstrzygające znaczenie ma okoliczność, czy osoba dysponująca daną informacją ma możliwość ustalenia, kogo konkretnie informacja ta dotyczy. Zwrócić uwagę należy na motyw 26 RODO: „Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do

[528] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 ze zm.).
[529] DPNT.023.1270.2025.

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

O tym, na ile poszczególne czynniki identyfikujące pozwalają na ostateczne ustalenie tożsamości osoby fizycznej, decydują szczególne okoliczności danej sytuacji. Orzecznictwo TSUE[530] wskazuje na szerokie rozumienie pojęcia danych osobowych. Np. w wyroku z 19 października 2016 r. w sprawie Breyer C-582/14 dotyczącym adresu IP jako danej osobowej TSUE stwierdził, że do tego, aby dane mogły zostać uznane za „osobowe" w rozumieniu art. 2 lit. a) dyrektywy 95/46, nie jest wymagane, aby wszystkie informacje umożliwiające identyfikację danej osoby znajdowały się w rękach tylko jednego podmiotu. Nie wydaje się zatem, by okoliczność, że dodatkowe informacje konieczne do identyfikacji użytkownika strony internetowej są w posiadaniu nie dostawcy usług medialnych online, lecz dostawcy dostępu do Internetu dla tego użytkownika, mogła wykluczać to, że dynamiczne adresy IP zarejestrowane przez dostawcę usług medialnych online stanowią dla niego dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46 (pkt 43, 44). W konsekwencji Trybunał orzekł, że dynamiczny adres IP zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46, w sytuacji gdy dysponuje on środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby (pkt 49; sentencja, pkt 1).

Prezes UODO zaznaczył, że rozwój technologii coraz bardziej ułatwia łączenie jednych danych z innymi, co umożliwia pozyskanie kolejnych danych pozwalających na identyfikację konkretnej osoby. Dane, które przy wstępnej analizie nie wydają się być danymi osobowymi, w rzeczywistości mogą stanowić swoisty kod wskazujący na konkretną osobę.

Jednocześnie zwrócił uwagę na wyrok WSA w Gorzowie Wielkopolskim z 26 czerwca 2024 r.[531], w którym zostało wskazane, że udostępnienie przez organ

[530] Wyroki TSUE dotyczące adresu IP: C-140/20, C-293/12 i C-594/12, C-461/10, C 793/19 i C 794/19.
[531] Sygn. akt II SAB/Go 52/24.

numerów geodezyjnych nieruchomości pozwala na ustalenie tożsamości właścicieli, a uzyskanie numerów działek w trybie ustawy o dostępie do informacji publicznej stanowiłoby obejście przepisów, które przewidują szczególny tryb dostępu i zasadę odpłatności. W analizowanej sprawie sąd wskazał, że udostępnienie informacji publicznej jest obowiązkiem podmiotów wykonujących zadania publiczne oraz prawem podmiotowym wynikającym z art. 61 ust. 1 Konstytucji RP. Niemniej każda osoba fizyczna ma prawo do ochrony jej danych osobowych, a udostępnienie informacji publicznej jest dopuszczalne z poszanowaniem prawa do prywatności. WSA zauważył, że zgodnie z art. 5 ust. 2 ustawy o dostępie do informacji publicznej, prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej. Natomiast dysponowanie numerem działki pozwala na ustalenie tożsamości właściciela nieruchomości. „W ocenie Sądu, numery geodezyjne działek gruntu, które bez nadzwyczajnego wysiłku dają się „powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, należą do kategorii danych osobowych. Podkreślenia przy tym wymaga, że przy obecnym stanie rozwoju techniki, w dobie istnienia rozmaitych sposobów uzyskiwania informacji, dysponowanie numerem działki pozwala na ustalenie tożsamości właściciela nieruchomości nawet laikowi przy dołożeniu minimum staranności i wykorzystaniu powszechnie dostępnych metod. To zaś może naruszać prywatność właścicieli działek gruntu. Potwierdzeniem powyższego jest również teza wyroku NSA z 16 października 2015 r.[532], według której „informacje o adresie nieruchomości dotyczą zidentyfikowanej bądź możliwej do zidentyfikowania osoby". Taką informację sąd uznał za informację dotyczącą prywatności osoby fizycznej, która podlega ochronie".

Wobec powyższego Prezes UODO uznał, że prawidłowym działaniem było przekazywanie przez organy władzy publicznej żądanych informacji zawierających numery działek ewidencyjnych dopiero po usunięciu danych chronionych (anonimizacji).

Podobnej kwestii dotyczyło pytanie pismo jednej z gmin z prośbą o zajęcie stanowiska w sprawie dopuszczalności **podania do publicznej wiadomości numerów ksiąg wieczystych** w wykazie nieruchomości przeznaczonych do sprzedaży sporządzonym zgodnie z art. 35 ust. 1 ustawy z 21 sierpnia 1997 r. o gospodarce nieruchomościami oraz w ogłoszeniach o przetargu[533]. Jak wskazała numery ksiąg wieczystych dotyczą nieruchomości, których gmina jest współwłaścicielem wraz z innymi współwłaścicielami i stanowią drogi wewnętrzne, przez które nieruchomość przeznaczona do sprzedaży ma zapewniony dostęp do drogi publicznej, a sprzedaż następuje wraz z udziałami w tych drogach. Odnosząc się do tej kwestii organ nadzorczy zaznaczył, przepisy ustawy o gospodarce nieruchomościami[534] w art. 35 ust. 2 w sposób wyczerpujący regulują zakres informacji (danych) zamieszczanych w wykazie nieruchomości stanowiących własność Skarbu

[532] I OSK 1986/14 (publ. orzeczenia.nsa.gov.pl., dalej: CBOSO).
[533] DPNT.023.831.2025.
[534] Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (Dz. U. z 2023 r. poz. 344 z późn. zm.).

Państwa lub jednostki samorządu terytorialnego przeznaczonych do zbycia lub oddania w użytkowanie, najem, dzierżawę lub użyczenie. Wśród elementów, które musi zawierać ów wykaz, ustawodawca wymienił m.in. „oznaczenie nieruchomości według księgi wieczystej oraz katastru nieruchomości" – art. 35 ust. 2 pkt 1 ustawy o gospodarce nieruchomościami. W myśl zaś art. 35 ust. 1 zdanie pierwsze i drugie oraz art. 38 ust. 2 tejże ustawy przedmiotowy wykaz jest upubliczniany poprzez wywieszenie na okres 21 dni w siedzibie właściwego urzędu, zamieszczenie na stronie internetowej tego urzędu, jak również podawany do publicznej wiadomości w ogłoszeniu o przetargu.

O ile jednak ustawa o gospodarce nieruchomościami w ramach realizacji zasady jawności w zakresie gospodarowania nieruchomościami stanowiącymi własność Skarbu Państwa lub jednostki samorządu terytorialnego wskazuje zawartość wykazu oraz okoliczności jego upublicznienia, to na administratorze danych osobowych (podmiocie sporządzającym wykaz) ciążą obowiązki dotyczące zapewnienia zgodnego z prawem i właściwego z punktu widzenia celu przetwarzania okresu udostępnienia tego wykazu – zasada zgodności z prawem (art. 5 ust. 1 lit. a RODO) i ograniczenia celu (art. 5 ust. 1 lit. b RODO).

Oznaczenie nieruchomości według księgi wieczystej oraz katastru nieruchomości dotyczy wskazania wprost numeru księgi wieczystej. Dla postępowania przetargowego jest to istotny element, gdyż zainteresowanym pozwala na potwierdzenie aktualnego stanu prawnego nieruchomości nie tylko w chwili przygotowania do opublikowania danego dokumentu, ale również w okresie jego wywieszenia. W ocenie organu nadzorczego ujawnienie numeru księgi wieczystej, a tym samym danych w niej zawartych odbywa się na podstawie art. 6 ust. 1 lit. c RODO. Zgodnie z powyższym artykułem przetwarzanie danych osobowych jest zgodne z prawem, jeżeli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (obowiązek wynikający z art. 35 ust. 1 ustawy o gospodarce nieruchomościami). Niezachowanie wymogu umieszczenia informacji w wykazie nieruchomości, o którym mowa w przepisach art. 35 ustawy o gospodarce nieruchomościami, prowadzi do nieważności umowy zawartej z pominięciem tego obowiązku[535].

Prezes UODO zaznaczył jednocześnie, że ze względu na konieczność zapewnienia bezpieczeństwa danych osobowych zgromadzonych w zbiorach ksiąg wieczystych oraz ryzyko niewłaściwego do nich dostępu, od lat wnioskuje do resortu sprawiedliwości o odpowiednie uregulowanie tej kwestii w sposób zapewniający poszanowanie zasad ochrony danych osobowych.

Inne z pytań dotyczyło **organizacji i sposobu przeprowadzania kwalifikacji wojskowej**[536]. W odpowiedzi Prezes UODO zaznaczył, że nie dysponuje ani wytycznymi, ani zaleceniami co do przeprowadzania kwalifikacji wojskowej. Podstawy prawne dotyczące kwalifikacji wojskowej zostały określone przepisami ustawy

[535] Por. wyrok SN z 11.05.2005 r. sygn. akt III CK 562/04, LEX nr 155352.
[536] DPNT.023.511.2025.

o obronie ojczyzny[537] i Rozporządzenia Ministra Obrony w sprawie orzekania o zdolności do służby wojskowej i trybu postępowania wojskowych komisji lekarskich w tych sprawach[538]. Powyższe regulacje nie zawierają przepisów dotyczących tego, jak w praktyce powinny być przeprowadzane wymagane badania przed wojskową komisją lekarską. Mając jednak na uwadze, że podczas przeprowadzanych badań dochodzi do przetwarzania danych osobowych, w tym danych dotyczących zdrowia osób stawających przed komisją, to takie przetwarzanie powinno realizować zasady określone w art. 5 RODO. Przede wszystkim dane takie powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"). Powszechnie przyjmuje się, że poufność danych to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom. Przetwarzanie danych osobowych zwykłych, a tym bardziej danych osobowych szczególnych kategorii, powinno odbywać się z poszanowaniem powyższej zasady, a administrator danych (podmiot przetwarzający) powinien zorganizować proces przetwarzania w taki sposób, by ten był zgodny z wymaganiami RODO.

Ponadto udzielane w 2025 r. **odpowiedzi dotyczyły wielu innych szczegółowych zagadnień**, w tym m.in.: brakowania/usuwania dokumentów przekazanych do podmiotów publicznych niezgodnie z właściwością[539], weryfikacji podmiotów przetwarzających w kontekście udzielania zamówień publicznych[540], zamieszczanie wizerunku osoby fizycznej w publikacji nt. działalności szkoły[541]; zakresu danych gromadzonych przez Koło Gospodyń Wiejskich[542] czy legalności udostępnienia danych osobowych zawartych w księgach wieczystych kancelarii prawnej, z którą została zawarta umowa na świadczenie usług prawnych[543].

### 18.2. Pytania od inspektorów ochrony danych

Zgodnie z założeniami prawodawcy unijnego inspektorzy ochrony danych, dysponujący odpowiednią wiedzą i umiejętnościami, a także mający odpowiednią pozycję w organizacji, w której funkcjonują, stanowią fundament skutecznego systemu ochrony danych osobowych. Dlatego przepisy RODO przewidują konkretne gwarancje, których celem jest umożliwienie IOD skutecznego i niezależnego wykonywania zadań.

Szczególna rola inspektorów ochrony danych przejawia się głównie w fachowym wspieraniu administratorów w obszarze zapewnienia zgodnego z prawem

[537] Ustawa z dnia 11 marca 2022 r. o obronie ojczyzny (Dz.U. z 2025 r. poz. 825).
[538] Rozporządzenie Ministra Obrony Narodowej z dnia 25 marca 2024 r. w sprawie orzekania o zdolności do służby wojskowej i trybu postępowania wojskowych komisji lekarskich w tych sprawach (Dz. U. poz. 466).
[539] DPNT.071.30.2025.
[540] DPNT.023.1142.2025.
[541] DPNT.023.449.2025.
[542] DPNT.023.411.2025.
[543] DPNT.023.656.2025.

przetwarzania danych osobowych. Wsparcie to polega przede wszystkim na staniu na straży (monitorowaniu) przestrzegania prawa w poszczególnych organizacjach, w jakich zostali oni wyznaczeni do pełnienia swojej funkcji, a także doradzaniu w zakresie obowiązków ciążących na administratorach i podmiotach przetwarzających. Niezwykle istotna jest również rola IOD jako punktu kontaktowego dla osób, których dane dotyczą, a także dla organu nadzorczego. Jednocześnie IOD ma prawo zwrócić się do organu nadzorczego o udzielenie mu konsultacji w kwestiach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem swojej funkcji, co również ma istotne znaczenie dla doskonalenia systemu ochrony danych osobowych.

Prezes UODO, doceniając rolę inspektorów ochrony danych w procesie zapewnienia prawidłowej ochrony danych osobowych, z uwagą podchodził i podchodzi do realizacji przez administratorów (w tym przez podmioty publiczne) ich obowiązków dotyczących funkcjonowania IOD i identyfikuje występujące w tym obszarze trudności i wątpliwości.

Z powyższych względów współpraca organu nadzorczego z inspektorami ochrony danych i udzielanie im wsparcia odbywa się w wielu formach. Bardzo cenne dla obu stron są działania umożliwiające wymianę poglądów i doświadczeń. Zaliczyć do nich można zarówno inicjatywy skierowane do całej społeczności IOD, jak również indywidualne konsultacje w sprawach przedstawianych przez poszczególnych inspektorów.

Pytania kierowane do organu nadzorczego w ramach tych indywidualnych konsultacji są dla organu nadzorczego ważnym źródłem wiedzy na temat problemów, z jakimi mierzą się oni w związku z pełnieniem swojej funkcji. Często dotyczą one kwestii związanych z nieprawidłowym rozumieniem funkcji IOD, ale też innych problemów zauważonych przez inspektorów, a wynikających np. z luk w przepisach prawa, nieodpowiedniej interpretacji przepisów czy też niewłaściwej praktyki. Odpowiadając na takie pytania, UODO w zależności od konkretnej sytuacji udziela wskazówek, które pozwalają ocenić, jak postąpić w przedstawionej sprawie czy też jak dokonać analizy w zakresie określania ról podmiotów, podstaw prawnych albo realizacji praw osób. Organ nadzorczy przedstawia również kierunek i zasady interpretacji przepisów pomocne przy rozstrzyganiu wątpliwości z zakresu ochrony danych osobowych.

Jednocześnie należy podkreślić, że sygnalizowane przez inspektorów problemy 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:

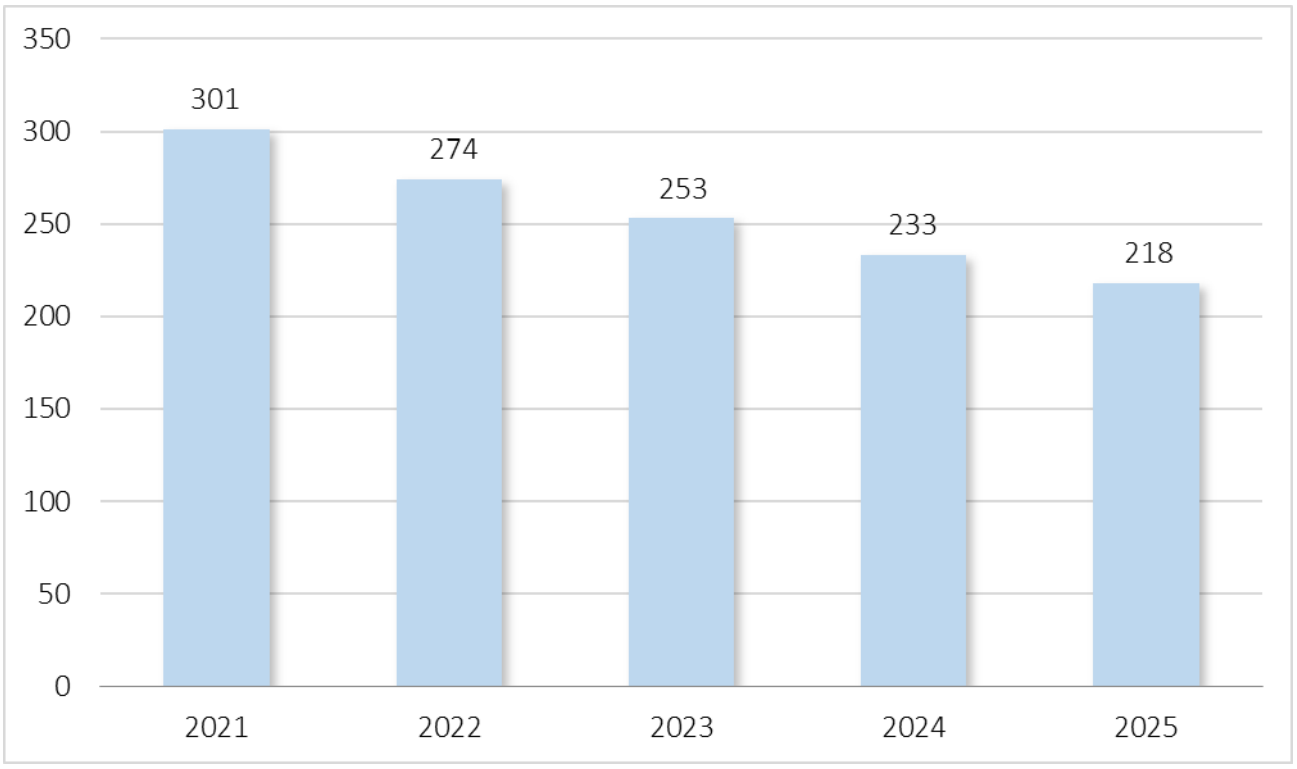
− udzielanie odpowiedzi na pytania IOD i przygotowywanie wyjaśnień publikowanych na stronie internetowej UODO lub Biuletynie UODO,

– poruszanie przedstawianych kwestii na szkoleniach czy konferencjach,

− sygnalizowanie właściwym podmiotom zaobserwowanych nieprawidłowości lub potrzeby zmian legislacyjnych.

W 2025 roku do Prezesa UODO wpłynęło **218 pytań od inspektorów ochrony danych.** Udzielono zaś 206 odpowiedzi na takie pytania.

Liczba pytań od IOD corocznie maleje (w 2021 r. było ich 301, a następnych latach liczba pytań sukcesywnie malała: w 2022 r. wpłynęły 274 pytania, w 2023 r. – 253 pytania, a w 2024 r. – 233).




**Wykres 17**: Liczba pytań od inspektorów ochrony danych, które wpłynęły do Prezesa UODO w latach 2021-2025.

Sytuacja ta może być efektem licznych działań edukacyjnych i informacyjnych prowadzonych przez organ nadzorczy. Ponadto wpływ na to może mieć fakt, że dzięki wspólnemu dorobkowi wypracowanemu z IOD w zakresie pytań i odpowiedzi 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 na stronie internetowej UODO czy w Biuletynie UODO[544].

Zagadnienia przedstawione przez IOD w pytaniach przesłanych w 2025 r. były bardzo zróżnicowane tematycznie. Dotyczyły zarówno pełnienia funkcji przez IOD, jak również problemów związanych z ochroną danych osobowych w różnych sektorach gospodarki, w tym w samorządzie terytorialnym, podmiotach leczniczych, organach ścigania czy sądach.

**Wśród pytań przesłanych w 2025 r. wyróżnić można w szczególności następujące grupy tematyczne:**

[544] https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

1) status i zadania inspektora ochrony danych,
2) łączenie funkcji IOD z innymi zadaniami,
3) pojęcie danych osobowych,
4) określenie statusu podmiotów w procesie przetwarzania danych osobowych,
5) realizacja obowiązków wynikających z RODO,
6) podstawa prawna do przetwarzania,
7) udostępnianie danych osobowych,
8) naruszenia ochrony danych osobowych,
9) przetwarzanie wizerunku,
10) działalność dziennikarska i radiowa,
11) stosowanie nowych regulacji prawnych.

W omawianym okresie sprawozdawczym szczególnie ważną część zagadnień, których dotyczyły pytania i sygnały od inspektorów ochrony danych, stanowiły kwestie wskazane w punktach 1-2, związane z prawidłowym pełnieniem funkcji przez IOD. Zauważyć należy, że przepisy rozporządzenia 2016/679 przewidują konkretne gwarancje, których celem jest umożliwienie IOD skutecznego i niezależnego wykonywania zadań. Zaliczyć do nich należy zwłaszcza: nałożenie na podmiot zobowiązany do wyznaczenia IOD obowiązku wyboru do pełnienia tej funkcji odpowiedniej osoby, bezpośrednią podległość IOD najwyższemu kierownictwu, wspieranie IOD w wypełnianiu jego zadań, zapewnienie udziału IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych, zakaz wydawania IOD instrukcji co do wykonywania przez niego zadań, unikanie konfliktu interesów, zakaz odwoływania i karania IOD, obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez IOD.

Podkreślenia wymaga, że przedstawione powyżej kwestie były już wielokrotnie przedmiotem różnych działań podejmowanych przez organ nadzorczy, w tym edukacyjnych, informacyjnych czy też kontrolnych i egzekucyjnych. Jednak fakt, że zagadnienia te nadal licznie pojawiają się w pytaniach zarówno od inspektorów, jak i od podmiotów zobowiązanych do wyznaczenia IOD pokazuje, że nadal istnieje potrzeba dalszego podnoszenia świadomości (w szczególności odnosi się to do administratorów) co do ich obowiązków związanych z wyznaczeniem IOD, a także co do roli IOD oraz korzyści płynących z posiadania inspektora dysponującego odpowiednią wiedzą i umiejętnościami, a także mającego odpowiednią pozycję w organizacji, który stanowi realne i fachowe wsparcie w zapewnieniu prawidłowego przetwarzania danych osobowych.

Poniżej przedstawione zostały odpowiedzi na pytania od inspektorów ochrony danych zgodnie z grupami tematycznymi wymienionymi we wcześniejszym punkcie.

### Ad 1. Status i zadania inspektora ochrony danych

Dla inspektorów ochrony danych kwestie ich niezależnej pozycji mają fundamentalne znaczenie, stanowią bowiem gwarancję prawidłowego wykonywania

ich funkcji. RODO zawiera wiele warunków i obowiązków odnoszących się do funkcjonowania IOD, które muszą być spełnione przez administratorów.

Przepisy ww. rozporządzenia określają w szczególności status i zadania IOD, a także warunki, jakie należy spełnić, aby możliwe było wyznaczenie IOD dla kilku podmiotów, w tym dla kilku podmiotów publicznych.

W odpowiedzi[545] na pytanie dotyczące możliwości skorzystania z modelu **jeden IOD dla kilku podmiotów publicznych**, o którym mowa w art. 37 ust. 3 RODO, organ nadzorczy wskazał, że przyjęcie takiego rozwiązania wymaga dokonania starannej analizy przez każdego z administratorów, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego z nich. Dokonując tej oceny, trzeba mieć świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. efektywnej dostępności inspektora dla osób z danej organizacji. Do zadań IOD należy np. bieżące monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa oraz udzielanie informacji i rad w zakresie obowiązków wynikających z tych przepisów. Trudno jest również wykonywać równolegle w wielu podmiotach zadania w zakresie punktu kontaktowego dla osób, których dane dotyczą, oraz punktu kontaktowego dla organu nadzorczego. Na mocy RODO bowiem 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.

Ponadto administrator zobowiązany jest do dokonania analizy, czy powierzone IOD zadania nie spowodują konfliktu interesów (art. 38 ust. 6 RODO). Warto przy tym pamiętać, że konflikt interesów może być również 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. W odpowiedziach, w których organ nadzorczy wskazuje na konieczność analizy, czy nie występuje konflikt interesów, zazwyczaj przypomina również kryteria, jakie administrator powinien uwzględnić przy dokonywaniu takiej analizy.

W tym przypadku Prezes UODO rekomendował spojrzenie na tę sytuację poprzez:

a) kryterium merytoryczne (inne obowiązki nie powinny negatywnie wpływać na niezależne wykonywanie zadań IOD),

b) kryterium czasowe (IOD powinien dysponować czasem wystarczającym do wykonywania swoich zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania).

[545] DPNT.502.116.2025.

W podsumowaniu tej odpowiedzi organ nadzorczy zwrócił uwagę, że z wyznaczeniem i pełnieniem funkcji IOD przez jedną osobę dla kilku podmiotów publicznych wiążą się bardzo konkretne wymagania prawne i wymagań tych każdy z administratorów będzie musiał przestrzegać.

W innej sprawie[546] inspektor ochrony danych zwróci się o wydanie opinii, czy prawidłowym działaniem jest **nakładanie na inspektora ochrony danych zadań polegających na koordynacji postępowania z naruszeniami ochrony danych osobowych** oraz **koordynacji rozpatrywania wniosków o realizację praw osób**, których dane dotyczą, o których mowa w art. 15-22 RODO.

Odnosząc się do tego pytania wskazano, że inspektor ochrony danych to funkcja szczególna, której cechą jest niezależność. Z tego powodu przepisy prawa zobowiązują administratora do zapewnienia inspektorowi możliwości niezależnego i skutecznego wykonywania zadań. RODO przewiduje w tym zakresie m.in. zakaz nakładania na IOD zadań, które powodować mogą konflikt interesów (art. 38 ust. 6 RODO). Do konfliktu interesów może dojść zwłaszcza wówczas, gdy:

1) na inspektora nakładane są obowiązki administratora (organizacji). W RODO role IOD oraz administratora zostały wyraźnie oddzielone. IOD z racji pełnienia swojej funkcji i przypisanych mu zadań nie może wykonywać obowiązków przypisanych administratorowi, ponieważ rolą inspektora jest ocena realizacji tych obowiązków pod kątem jej zgodności z przepisami powszechnie obowiązującymi oraz regulacjami wewnętrznymi. Na inspektora nie mogą być nakładane obowiązki/czynności/działania, które następnie zgodnie z art. 39 ust. 1 lit. b RODO miałby on poddawać swojej ocenie.

2) inspektorowi ochrony danych powierzane są zadania lub obowiązki, które prowadziłyby do określania przez niego celów i sposobów przetwarzania danych osobowych, ponieważ decyzje takie, a także związana z nimi odpowiedzialność należą do administratora (osób zarządzających/kierujących podmiotem będącym administratorem). IOD natomiast jest obowiązany w sposób niezależny doradzać kierownictwu i pracownikom oraz kontrolować, czy decyzje te odpowiadają wymogom prawa.

Wagę niezależności i wspominanego wymogu co do braku konfliktu interesów podkreśla się w orzecznictwie TSUE. W wyroku w sprawie C-453/21 X-FAB Dresden (m.in. punktach 41-45) TSUE wskazał, że w świetle znaczenia wyrażenia „konflikt interesów" w języku potocznym, należy uznać, że zgodnie z celem realizowanym przez art. 38 ust. 6 RODO nie można powierzyć osobie będącej IOD wykonywania zadań lub obowiązków, które mogłyby zaszkodzić pełnieniu funkcji, które wykonuje jako IOD, a tym samym negatywnie wpłynąć na zapewnienie skuteczności przepisów RODO.

Zgodnie z przepisami RODO (art. 39) zadania inspektora ochrony danych koncentrują się na monitorowaniu przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk danego administratora, doradzaniu i podnoszeniu świadomości kierownictwa i pracowników w tym zakresie, a także

[546] DPNT.502.107.2025.

pełnieniu roli punktu kontaktowego. W przedstawionym przez inspektora przypadku do zadań IOD miałaby należeć koordynacja postępowania z naruszeniami ochrony danych osobowych oraz koordynacja rozpatrywania wniosków o realizację praw osób.

W ocenie organu nadzorczego nakładanie na IOD takich zadań należałoby uznać za niezgodne z prawem. Ze względu na niezależność IOD nie mogą bowiem należeć do niego działania o charakterze zarządczym czy kierowniczym (tj. związane z decydowaniem o celach i sposobach przetwarzania danych osobowych), a do takich zapewne należałoby zaliczyć ww. zadania polegające na koordynowaniu działań różnych osób/komórek, w tym podejmowaniu decyzji co do konkretnych działań z naruszeniem czy wnioskiem o realizację praw osób, których dane dotyczą. Działania prowadzone przez IOD w związku z koordynacją ww. zadań nie mogłyby następnie podlegać ocenie (monitorowaniu) przez inspektora, gdyż byłaby to ocena nieobiektywna.

Powierzając inspektorowi zadanie należące do administratora (w tym przypadku koordynowanie postępowań z naruszeniami lub wnioskami dotyczącymi praw osób), eliminuje się cel, w jakim funkcja IOD została ustanowiona w RODO. Celem tym jest posiadanie przez administratora niezależnego fachowca oceniającego zgodność prowadzonego przez niego przetwarzania danych osobowych z przepisami o ochronie danych. Taka sytuacja tym samym negatywnie wpływa na zapewnienie skuteczności przepisów RODO.

Jednocześnie w odpowiedzi tej przypomniano, że do roli IOD w postępowaniu z naruszeniami oraz z wnioskami dot. praw osób Prezes UODO odnosił się już w materiałach publikowanych na stronie internetowej Urzędu[547]. Wskazano w nich m.in., że przepisy RODO – art. 15, art. 12, art. 33 i art. 34 – wymieniają administratora jako podmiot, który w określony sposób i w określonym terminie ma wykonywać zadania związane z naruszeniami czy realizować prawa osób, których dane dotyczą, a dodatkowo przewidzieć procedury postępowania z naruszeniami ochrony danych oraz realizowania praw i żądań osób, których dane są przetwarzane. Natomiast rola IOD powinna polegać na budowaniu świadomości administratora w zakresie tych obowiązków, a następnie monitorowaniu skuteczności przyjętych w tym zakresie przez administratora procedur i rozwiązań, a gdy to konieczne – rekomendowaniu ich modyfikacji.

Podobnego zagadnienia dotyczyło pytanie, **czy IOD powinien być włączany w proces wdrażania systemu Elektronicznego Zarządzania Dokumentacją**[548]. Odpowiadając na nie, organ nadzorczy wskazał, że inspektor ochrony danych powinien swoją wiedzą, doświadczeniem i umiejętnościami wspierać administratora w zapewnieniu zgodności przetwarzania danych z przepisami o ochronie danych. Aby IOD mógł efektywnie realizować ten cel, przepis art. 38 ust. 1 RODO nakłada na administratora obowiązek zapewnienia, by inspektor ochrony danych był właściwie

[547] M.in. w „Poradniku dotyczącym naruszeń ochrony danych osobowych” (https://uodo.gov.pl/pl/598/3563), a także w materiale pt. „Za realizację praw osób w zakresie dostępu do dotyczących ich danych odpowiada administrator” (Biuletyn UODO, Wydanie 1 (styczeń 2024); https://uodo.gov.pl/pl/438/1183).
[548] DPNT.502.40.2025.

i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Oznacza to, że IOD powinien:

- mieć możliwość „właściwego" włączenia w sprawę, a więc zapewniającego możliwie kompleksowe zapoznanie się IOD z okolicznościami przetwarzania danych osobowych – kontekstem, celami, zakresem, charakterem, uwarunkowaniami czasowymi, technicznymi, prawnymi;
- być włączany w sprawę niezwłocznie – a więc bez nieuzasadnionej zwłoki, możliwie szybko, na możliwie najwcześniejszym etapie – najlepiej – o ile to możliwe – zanim jeszcze zaczną być dokonywane operacje przewarzania;
- być włączany do wszystkich spraw dotyczących ochrony danych osobowych.

Należy go zatem informować i angażować we wszystkie sprawy z zakresu ochrony danych osobowych bez względu na to, jakich kategorii danych czy osób one dotyczą oraz czy stanowią istotę działalności administratora, czy też mają wyłącznie charakter akcesoryjny.

Jak wskazano w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243)[549] istotne jest włączanie IOD lub jego zespołu we wszystkie sprawy dotyczące ochrony danych osobowych na jak najwcześniejszym etapie. Zapewnienie informowania IOD i konsultowania się z nim od samego początku ułatwi przestrzeganie RODO, promowanie podejścia zakładającego uwzględnienie ochrony prywatności w fazie projektowania, a zatem powinno być standardową procedurą w ramach zarządzania organizacją. Ponadto ważne jest, aby IOD był postrzegany w organizacji jako partner w dyskusji i był włączany w prace grup roboczych wykonujących czynności przetwarzania danych w organizacji.

W związku z tym – jak wskazuje Grupa Robocza Art. 29 w ww. Wytycznych – organizacja powinna zapewnić m.in., aby:

- IOD był zapraszany do regularnego udziału w posiedzeniach kadry kierowniczej wyższego i średniego szczebla;
- uczestniczył w podejmowaniu decyzji mających wpływ na ochronę danych. Wszystkie niezbędne informacje należy udostępnić IOD odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska;
- opinia inspektora ochrony danych musi być zawsze należycie uwzględniana. W przypadku braku porozumienia Grupa Robocza Art. 29 zaleca, jako dobrą praktykę, dokumentowanie powodów niezastosowania się do porady inspektora ochrony danych;
- w przypadku stwierdzenia naruszenia ochrony danych lub innego incydentu należy niezwłocznie skonsultować się z IOD.

W opinii Prezesa UODO dobrą praktyką powinno być opracowanie przez administratora wewnętrznych wytycznych, w których określi, kiedy należy skonsultować się z IOD. Organ nadzorczy zwrócił też uwagę, że niedopełnienie lub nienależyte wypełnienie obowiązku włączania IOD we wszystkie sprawy dotyczące

[549] Dostępnych pod linkiem https://uodo.gov.pl/data/filemanager_pl/15.pdf.

ochrony danych osobowych może przybrać postać pomijania inspektora ochrony danych w sprawach związanych z przetwarzaniem i ochroną danych lub informowania go ze znacznym opóźnieniem, co może prowadzić do naruszenia przepisów o ochronie danych, a w konsekwencji również nałożenia na administratora administracyjnej kary pieniężnej[550].

Jednocześnie udzielając wskazówek organ nadzorczy zastrzegł, że ze względu na charakter zadań IOD skupiających się na doradzaniu oraz monitorowaniu działalności administratora pod kątem zgodności z przepisami o ochronie danych osobowych oraz wymóg sprawowania tej funkcji w sposób niezależny, włączanie IOD w sprawy dotyczące ochrony danych, np. w proces wdrażania systemu EZD, nie może oznaczać przerzucania na IOD zadań związanych z wdrożeniem takiego systemu. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za wykonanie określonego zadania administratora, np. wdrożenie systemu, a jednocześnie miałby monitorować zgodność wykonywania tego zadania z przepisami o ochronie danych osobowych, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów (o którym mowa w art. 38 ust. 6 RODO)[551].

Inną kwestią podnoszoną w odpowiedzi na pismo IOD było **udzielanie inspektorowi pełnomocnictwa do zawiadamiania Prezesa UODO** o wyznaczeniu IOD. W odpowiedzi organ nadzorczy przypomniał, że obowiązek zawiadomienia o wyznaczeniu IOD ciąży na administratorze, nie zaś na wyznaczonym przez niego inspektorze (art. 37 ust. 7 RODO w zw. z art. 10 ust. 1 ustawy o ochronie danych osobowych). Wobec powyższego to administrator, a nie IOD, powinien podpisać i przesłać takie zawiadomienie. Administrator może oczywiście ustanowić pełnomocnika do dokonania takiego zawiadomienia (art. 10 ust. 2 ustawy o ochronie danych osobowych), jednak na takiego pełnomocnika nie powinien wyznaczać inspektora ochrony danych. Udzielenie inspektorowi ochrony danych pełnomocnictwa do występowania w imieniu administratora (reprezentowania administratora) przed organem nadzorczym w sprawach z zakresu ochrony danych osobowych stoi w kolizji z nakazem nienakładania na IOD zadań powodujących konflikt interesów (art. 38 ust.

---

[550] Przykładami takich decyzji Prezesa UODO mogą być: decyzja z 21 sierpnia 2020 r. w sprawie ZSOŚS.421.25.2019 oraz decyzja z 23 czerwca 2025 r. w sprawie DKN.5130.4179.2020.

[551] Ze stanowiskiem Prezesa UODO dotyczącym konieczności rozdzielenia ról IOD i administratora zapoznać się można w decyzji Prezesa UODO z 22.09.2020 r. ZWAD.405.31.331.2019 (https://uodo.gov.pl/decyzje/ZWAD.405.31.331.2019) oraz w odpowiedziach na pytania od IOD: „Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?", „Jakie zadania ma IOD?", „Czy administrator może przerzucać swoje obowiązki na IOD?", „Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?", „Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD?", „Czy IOD może nadawać upoważnienia?", „Kto powinien opracować wewnętrzną politykę ochrony danych osobowych? Administrator czy IOD?", „Czy IOD może w imieniu administratora zawierać umowy powierzenia?". Odpowiedzi te opublikowane były na poprzedniej stronie internetowej UODO w zakładce IOD (https://archiwum.uodo.gov.pl/p/zadania-iod), a obecnie znaleźć je można w Biuletynie UODO - wydaniu specjalnym (https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod). Na problem nakładania na IOD obowiązków administratora UODO zwracał uwagę również: w sprawozdaniu EROD z działania CEF DPO (Sprawozdanie krajowe polskiego organu nadzorczego w ramach CEF DPO https://uodo.gov.pl/pl/138/2960), w podsumowaniu efektów spotkania pt. „Niezależność IOD musi być standardem" (https://uodo.gov.pl/pl/138/3118) oraz w ramach akcji 27 pytań (https://archiwum.uodo.gov.pl/pl/138/2336).

6 RODO) oraz zakazem udzielania inspektorowi instrukcji co do wykonywania zadań (art. 38 ust. 3 RODO). Zadaniem IOD jest informowanie administratora o obowiązkach spoczywających na nim na mocy RODO, doradzanie mu w tym zakresie oraz monitorowanie wykonania tych obowiązków (art. 39 ust. 1 lit. a i b RODO). Występowanie w roli pełnomocnika administratora w zakresie obowiązków nałożonych na administratora może istotnie utrudniać lub uniemożliwiać inspektorowi niezależną ocenę, czy obowiązki administratora są wykonywane i czy są wykonywane prawidłowo. Dlatego IOD nie powinien np. podpisywać zawiadomień o wyznaczeniu IOD czy też formularzy zgłoszenia naruszenia. Ze względu zaś na swoją rolę fachowego doradcy i podmiotu monitorującego w sposób niezależny przestrzeganie przepisów o ochronie danych osobowych również IOD powinien ze swej strony odpowiednio wcześnie identyfikować i sygnalizować administratorowi ryzyko wystąpienia takiego konfliktu, by możliwe było odpowiednio wczesne zapobieganie mu[552].

Odnosząc się z kolei do pytania dotyczącego nakładania na IOD zadania polegającego na **prowadzeniu rejestru czynności przetwarzania**[553], organ nadzorczy, powołując się na dotychczas prezentowane stanowiska, wskazał, że prowadzenie rejestru czynności przetwarzania/rejestru kategorii czynności przetwarzania to zadanie administratora/podmiotu przetwarzającego (zarówno na podstawie RODO, jak i przepisów wdrażających dyrektywę 2016/680), a IOD powinien jedynie monitorować wykonanie tego obowiązku. To te podmioty są odpowiedzialne za efektywne wykonanie ww. obowiązku i pozostawanie w gotowości do wykazania tego na żądanie organów ochrony danych. Natomiast inspektor ochrony danych jako fachowiec może wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez doradzanie mu w kwestiach związanych z wykonaniem tego obowiązku.

Motyw 82 RODO wskazuje na dwie podstawowe funkcje obowiązku prowadzenia przez administratora rejestru czynności przetwarzania. Po pierwsze, administrator powinien prowadzić rejestry czynności przetwarzania dla zachowania zgodności z rozporządzeniem, po drugie, każdy administrator ma obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać rejestr w celu umożliwienia organowi nadzorczemu monitorowania prowadzonych operacji przetwarzania.

W sytuacji zaś gdy administrator nakłada na IOD zadania, które mogą stać się następnie przedmiotem dokonywanych przez IOD czynności monitorowania, w szczególności chodzi o zadania należące do administratora (np. prowadzenie

---

[552] Informacje na temat sytuacji, w których może dochodzić do konfliktu interesów w związku z występowaniem przez IOD w roli pełnomocnika administratora, znaleźć można w szczególności w:
- materiale pt. „Za realizację praw osób w zakresie dostępu do dotyczących ich danych odpowiada administrator" zamieszczonym w Biuletynie UODO, Wydanie 1 ze stycznia 2024 r. zob. link: (https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod),
- sprawozdaniu krajowym polskiego organu nadzorczego w ramach CEF DPO (str. 9 i 10) (https://uodo.gov.pl/pl/138/2960),
- w prezentacji załączonej do materiału „Niezależność IOD musi być standardem – podsumowanie efektów spotkania w UODO" (https://uodo.gov.pl/pl/138/3118 ), zwłaszcza w panelach nr 1, 3 i 4,
- poradniku dotyczącym naruszeń ochrony danych osobowych (https://uodo.gov.pl/pl/598/3563).

[553] DPNT.502.63.2025.

rejestru czynności przetwarzania), IOD zmuszony jest oceniać wyniki swojej pracy, co z kolei wpływa na niezależność i obiektywizm tej oceny, a więc prowadzi do konfliktu interesów. Dlatego administrator nie może nakładać na inspektora obowiązków przypisanych w przepisach RODO administratorowi[554].

**Ad 2. Łączenie funkcji IOD z innymi zadaniami**

Jednym z istotnych zagadnień dotyczących statusu IOD pojawiających się w pismach od inspektorów w 2025 r. była możliwość **łączenia funkcji IOD z innymi zadaniami, w tym w szczególności z zadaniami: zastępcy głównego księgowego**[555], **kierownika ds. kontroli**[556], **pełnomocnika ds. sytemu zarządzania bezpieczeństwem informacji (SZBI)**[557], **radcy prawnego**[558].

Udzielając odpowiedzi na takie pytania, organ nadzorczy wskazywał, że administrator powinien dokonać starannej analizy za każdym razem, gdy chce nałożyć na IOD dodatkowe zadania bądź wyznaczyć do pełnienia tej funkcji osobę, która dotychczas miała w zakresie swoich obowiązków inne zadania. Musi mieć bowiem pewność, że osoba wyznaczona do pełnienia funkcji IOD będzie miała zapewnione właściwe warunki dla zachowania niezależności i prawidłowego wykonywania zadań IOD, w tym, by nakładanie na IOD innych zadań nie powodowało konfliktu interesów.

Przeprowadzona w tym zakresie ocena powinna uwzględniać kryteria: organizacyjne, merytoryczne, czasowe[559].

W odpowiedzi na pytanie IOD dotyczące powierzenia IOD dodatkowego zadania, jakim byłoby pełnienie funkcji kierownika do spraw kontroli, organ nadzorczy wskazał, że w jego opinii pełnienie tej dodatkowej funkcji może wiązać się z podejmowaniem decyzji lub współuczestniczeniem w podejmowaniu decyzji co do określania celów i sposobów przetwarzania danych osobowych (np. w odniesieniu do tego, czy i jakie dokumenty należy przechowywać oraz jak długo). Kierownik do spraw kontroli, zgodnie z ustawą z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[560], decyduje bowiem o zakresie kontroli (art. 14) obejmującym także pisemne wyjaśnienia jej dotyczące (art. 35) oraz ma prawo żądać przedstawienia dokumentów lub złożenia

---

[554] Więcej informacji dotyczących nieprawidłowej praktyki nakładania na IOD obowiązków administratora w zakresie prowadzenia rejestru czynności przetwarzania znajduje się: w odpowiedzi na pytanie Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD? (która opublikowana była na poprzedniej stronie internetowej UODO w zakładce IOD, a obecnie znaleźć ją można w Biuletynie UODO - wydaniu specjalnym: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod), w sprawozdaniu krajowym polskiego organu nadzorczego w ramach CEF DPO (https://uodo.gov.pl/pl/138/2960) oraz w prezentacji załączonej do materiału „Niezależność IOD musi być standardem – podsumowanie efektów spotkania w UODO", w szczególności w panelach nr 1 i 3 (https://uodo.gov.pl/pl/138/3118).

[555] DPNT.502.26.2025.

[556] DPNT.502.91.2025.

[557] DPNT.502.83.2025.

[558] DOL.502.159.2025.

[559] Więcej informacji na temat tych kryteriów znaleźć można w odpowiedzi Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?, która opublikowana była na poprzedniej stronie internetowej UODO w zakładce IOD, a obecnie znaleźć ją można w Biuletynie UODO - wydaniu specjalnym: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

[560] Dz. U. z 2026 r. poz. 158.

pisemnych wyjaśnień przez pracowników jednostki kontrolowanej (art. 44). Warto też dodać, że osoba ta podejmuję również decyzje o wyłączeniu z udziału w kontroli (art. 19 ust. 5), podpisuje projekt wystąpienia pokontrolnego (art. 37), rozpatruje zastrzeżenia do projektu wystąpienia pokontrolnego (art. 42, 44 i 45). Wskazane wyżej kompetencje kierownika do spraw kontroli mogą powodować, że osoba taka w związku z wykonywaniem innych zadań niż IOD, podejmuje decyzje (współuczestniczy w podejmowaniu decyzji) o sposobach i celach przetwarzania danych, a z drugiej strony – jako IOD bada zgodność przetwarzania danych z przepisami o ochronie danych osobowych. Może to tym samym powodować, że kontroluje procesy przetwarzania danych, o których będzie jednocześnie decydować.

Dlatego w ocenie organu nadzorczego konieczne jest przeprowadzenie przez administratora analizy, czy kierownik komórki do spraw kontroli, w zakresie powierzonych mu zadań, podejmuje decyzje co do kluczowych aspektów przetwarzania na gruncie przepisów RODO, mając na uwadze, że realizacja zadań prowadzących do określania celów i sposobów przetwarzania danych nie może należeć do IOD.

Podobnie do kwestii określania celów i sposobów organ nadzorczy odniósł się w przypadku zadań pełnomocnika ds. sytemu zarządzania bezpieczeństwem informacji (SZBI). W odpowiedzi wskazał, że mimo że przepisy prawa nie określają, jaki jest zakres zadań pełnomocnika ds. SZBI, to z międzynarodowych standardów dotyczących systemów zarządzania bezpieczeństwem informacji, np. normy I PN-EN ISO/IEC 27001, wynika, że pełnienie tej funkcji wiąże się z wykonywaniem zadań związanych z zapewnieniem odpowiedniej ochrony i bezpieczeństwa informacji, w tym z wdrożeniem i właściwym funkcjonowaniem systemu zarządzania bezpieczeństwem informacji. Zadania te mogą polegać m.in. na opracowaniu odpowiedniej dokumentacji (np. polityki bezpieczeństwa informacji), procedur, a także na monitorowaniu ich stosowania i aktualizacji. Ponadto pełnomocnikowi mogą być powierzone zadania związane z szacowaniem ryzyka naruszenia poufności, integralności, dostępności informacji. Pełnomocnik np. opracowuje i aktualizuje polityki bezpieczeństwa informacji oraz stale monitoruje ryzyka naruszenia bezpieczeństwa informacji, co oznacza, że może podejmować decyzje, jakie środki techniczne i organizacyjne powinny być wprowadzone, aby właściwe zarządzać bezpieczeństwem informacji, w tym bezpieczeństwem danych osobowych. Tym samym istnieją podstawy do przyjęcia, że pełnomocnik ds. SZBI w związku z wykonywaniem swoich zadań może podejmować decyzje i działania co do sposobów przetwarzania danych osobowych.

Odpowiadając na pytania o prawidłowość łączenia funkcji IOD z funkcją radcy prawnego, organ nadzorczy powoływał się na odpowiedź na pytanie „Czy funkcję IOD można łączyć z wykonywaniem zawodu adwokata lub radcy prawnego?”[561]. Dodatkowo informował, że Krajowa Rada Radców Prawnych (KRRP) przekazała

[561] Odpowiedź ta opublikowana była na poprzedniej stronie internetowej UODO w zakładce IOD, a obecnie znaleźć ją można w Biuletynie UODO - wydaniu specjalnym: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

Prezesowi UODO opinię[562], zgodnie z którą ze względu na określone ryzyka, w szczególności związane z potencjalnym naruszeniem zasad etyki zawodowej oraz rozbieżnymi charakterystykami funkcji radcy prawnego oraz IOD, rekomenduje się niełączenie wykonywania tych ról w ramach jednego podmiotu (administratora danych/klienta).

We wszystkich odpowiedziach dotyczących nakładania na IOD innych zadań organ nadzorczy podkreślał, że administrator przed powierzeniem IOD dodatkowych zadań powinien dokonać analizy, czy IOD będzie w stanie wykonywać prawidłowo swoje obowiązki. Ocena, czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana z uwzględnieniem konkretnych okoliczności. Ponadto możliwość zaistnienia konfliktu powinna być stale monitorowana. Przyczyny zaistnienia takiego konfliktu mogą bowiem występować również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD. Nieprzeprowadzenie przez administratora analizy w powyższym zakresie może w konsekwencji spowodować naruszenie przepisów o ochronie danych osobowych[563]. Jednocześnie zgodnie z zasadą rozliczalności administrator powinien wykazać, że prawidłowo wykonuje obowiązki przewidziane w RODO oraz powinien potrafić uzasadnić, dlaczego przyjął określone rozwiązania.

W takich odpowiedziach organ nadzorczy zwracał również uwagę, że IOD – ze względu na swoją rolę fachowego doradcy i podmiotu w sposób niezależny monitorującego przestrzeganie przepisów o ochronie danych osobowych – powinien ze swej strony odpowiednio wcześnie identyfikować i sygnalizować administratorowi ryzyko wystąpienia konfliktu interesów.

### Ad 3. Pojęcie danych osobowych

Wśród pytań od inspektorów ochrony danych znalazły się również te dotyczące zakwalifikowania określonych informacji do danych osobowych. Odnosząc się do nich, organ nadzorczy zazwyczaj wskazuje kryteria, jakie należy wziąć pod uwagę w przypadku takich wątpliwości.

W odpowiedzi na pytanie, **czy informacje o barwie głosu danej osoby stanowią dane osobowe**[564], Urząd wskazał m.in., że takiej oceny należy dokonywać z uwzględnieniem wszystkich elementów definicji danych osobowych z art. 4 pkt 1 RODO oraz w odniesieniu do danego stanu faktycznego. Kluczowym kryterium, które powinno być brane pod uwagę, jest również to, kto dysponuje i np. komu udostępnia określone informacje na temat danej osoby. Zgodnie bowiem z definicją zawartą w ww. przepisie dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio

[562] Treść tej opinii jest dostępna pod następującym linkiem: https://kirp.pl/wp-content/uploads/2023/02/sk-19.01.2018-rw.pdf, https://obsil.kirp.pl/wp-content/uploads/2018/05/Opinia-z-28.03.2018-r.-IOD.pdf.
[563] Decyzje Prezesa UODO dot. tego zagadnienia: DKN.5131.7.2025, DKN.5131.4.2025, DKN.5131.15.2025.
[564] DPNT.502.43.2025.

zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przy interpretacji pojęcia danych osobowych warto mieć na uwadze orzeczenie TSUE z 20 grudnia 2017 r. w sprawie C-434/16 Peter Nowak przeciwko Data Protection Commissioner. W orzeczeniu tym TSUE opowiedział się za szerokim rozumieniem pojęcia danych osobowych: „Użycie w zawartej w art. 2 lit. a) dyrektywy 95/46 definicji „danych osobowych" wyrażenia „wszelkie informacje" odzwierciedla bowiem przyświecający unijnemu prawodawcy zamiar przypisania temu pojęciu szerokiego zakresu, nie ograniczając go do informacji wrażliwych czy też prywatnych, lecz rozszerzając go potencjalnie o informacje wszelkiego rodzaju, zarówno obiektywne, jak i subiektywne, w postaci opinii czy oceny, a jedynym warunkiem, które muszą one spełniać, jest to, aby „dotyczyły" danej osoby. Warunek ten jest zaś spełniony, gdy ze względu na swą treść, cel czy skutek dana informacja jest powiązana z daną osobą."

Wskazówki dotyczące pojęcia danych osobowych znaleźć można również w motywie 26 RODO, w którym wskazano, że: „Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej".

Podsumowując tę odpowiedź, organ nadzorczy wskazał, że niewątpliwie głos osoby należy uznać za dane osobowe, w przypadku gdy dla określonego podmiotu istnieje możliwość zidentyfikowania tej osoby. Przy ocenie prawdopodobieństwa powiązania danych z konkretną osobą należy miedzy innymi uwzględniać rozwój technologii umożliwiających przetwarzanie danych osobowych uzyskiwanych lub łączonych z różnych źródeł oraz to, kto może mieć dostęp do tych danych.

W odpowiedzi na pytanie IOD odnoszące się do możliwości udostępniania numerów ewidencyjnych działek na podstawie ustawy z 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko, organ nadzorczy odniósł się m.in. do zagadnienia, **czy numer ewidencyjny działki stanowi dane osobowe**[565].

W udzielonych wyjaśnieniach, organ nadzorczy podkreślił, że dokonanie tej oceny wymaga analizy konkretnej sytuacji uwzględniającej definicję danych osobowych zawartą w art. 4 pkt 1 RODO. Zaznaczył, że pomocne może być również powołane wyżej orzeczenie TSUE z 20 grudnia 2017 r. w sprawie C-434/16 Peter Nowak przeciwko Data Protection Commissioner, a także orzecznictwo sądów polskich. Odwołał się przy tym do wyroku Wojewódzkiego Sądu Administracyjnego

[565] DPNT.502.214.2025.

w Gorzowie Wielkopolskim z 26 czerwca 2024 r. (sygn. akt II SAB/Go 52/24), w którym sąd wskazał, że „ujawnienie numerów geodezyjnych poszczególnych działek gruntu może pozwolić na ustalenie właścicieli nieruchomości, stąd numery geodezyjne działek stanowią informacje podlegające ochronie ze względu na prywatność osób fizycznych, stosownie do przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych". Ponadto w ocenie Sądu, „numery geodezyjne działek gruntu, które bez nadzwyczajnego wysiłku dają się „powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, należą do kategorii danych osobowych. Podkreślenia przy tym wymaga, że przy obecnym stanie rozwoju techniki, w dobie istnienia rozmaitych sposobów uzyskiwania informacji, dysponowanie numerem działki pozwala na ustalenie tożsamości właściciela nieruchomości nawet laikowi przy dołożeniu minimum staranności i wykorzystaniu powszechnie dostępnych metod. To zaś może naruszać prywatność właścicieli działek gruntu. Potwierdzeniem powyższego jest również teza wyroku NSA z 16 października 2015 r.[566] według której „informacje o adresie nieruchomości dotyczą zidentyfikowanej bądź możliwej do zidentyfikowania osoby". Taką informację Sąd uznał za informację dotyczącą prywatności osoby fizycznej, która podlega ochronie."

W podsumowaniu organ nadzorczy wskazał, że biorąc pod uwagę powyższe informacje należy przyjąć, że w przedstawionej przez IOD sytuacji numer ewidencyjny działki stanowi dane osobowe, bo – jak wynika z przytoczonego wyżej orzecznictwa – jest możliwe zidentyfikowanie osoby na podstawie takiej informacji.

### Ad 4. Określenie statusu podmiotów w procesie przetwarzania danych osobowych

W jednym z pytań inspektor zwrócił się o pomoc w określeniu **roli społecznego inspektora pracy w procesie przetwarzania danych osobowych w związku z jego zadaniami** wynikającymi z ustawy z 24 czerwca 1983 r. o społecznej inspekcji pracy[567]. W odpowiedzi wskazano, że aby dokonać oceny w powyższym zakresie należy ustalić, w jakich sytuacjach społeczny inspektor pracy bierze udział w przetwarzaniu danych osobowych i w jaki sposób z danymi tymi postępuje, w tym czy i jakie dane osobowe są społecznemu inspektorowi pracy niezbędne do realizacji jego ustawowych zadań oraz w jaki sposób i przez kogo są one przetwarzane. Informacje te są potrzebne, aby ustalić, kto jest administratorem tych danych osobowych.

Jeżeli społeczny inspektor pracy potrzebuje dostępu do danych osobowych, administratorem których jest pracodawca, wówczas trudno uznać, że dostęp do tych danych powinien nastąpić na podstawie umowy powierzenia. Byłoby to sprzeczne z rolą społecznego inspektora pracy, którego kompetencje odnoszą się do kontrolowania pracodawcy w zakresie zapewniania przez niego bezpiecznych i higienicznych warunków pracy. Dodać należy, że społeczny inspektor pracy wykonuje własne ustawowe zadania. Tymczasem istotą umowy powierzenia jest

[566] I OSK 1986/14 (publ. orzeczenia.nsa.gov.pl., dalej: CBOSO).
[567] DOL.502.227.2024.

realizowanie procesów przetwarzania w imieniu administratora (tj. w celach przez niego określonych) przez inny, zewnętrzny podmiot. Społeczny inspektor pracy zaś realizuje cele społecznej inspekcji pracy (jako reprezentant pracowników).

Pewne wskazówki w zakresie dokonania oceny, skąd społeczny inspektor pracy pozyskuje dane znajdują się w art. 8 ustawy o społecznej inspekcji pracy. Zgodnie z ust. 1 i 2, społeczny inspektor pracy ma prawo wstępu w każdym czasie do pomieszczeń i urządzeń zakładu pracy dla wykonywania zadań określonych w powyższym przepisie. Społeczny inspektor pracy ma prawo żądać od kierownika zakładu pracy oraz oddziału (wydziału) i od pracowników informacji oraz okazania dokumentów w sprawach wchodzących w zakres jego działania. Przy czym zaznaczyć należy, że zgodnie z wyrokiem Trybunału Konstytucyjnego, sygn. akt K 6/15[568], przepis ten utracił moc w zakresie, w jakim nie uzależnia obowiązku udzielenia społecznemu inspektorowi pracy informacji oraz okazania mu dokumentów od uzyskania zgody pracownika w wypadkach, w których realizacja tego obowiązku wiązałaby się z udostępnieniem danych osobowych. Przepis ten został uznany za niezgodny z art. 47 Konstytucji RP, który stanowi, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Z treści przepisu art. 8 ustawy o społecznej inspekcji pracy można wywnioskować, że przepisy ustawy o społecznej inspekcji pracy uprawniają społecznego inspektora pracy do żądania informacji od pracodawcy. Społeczny inspektor pracy kontroluje pracodawcę w zakresie zapewnienia bezpiecznych i higienicznych warunków pracy na terenie zakładu pracy i w związku z tym ma prawo żądania informacji od niego. Przepis ten nie wspomina natomiast o możliwości uzyskiwania takiej informacji od związków zawodowych.

Natomiast w kontekście wątpliwości, czy społeczny inspektor pracy powinien podpisać taką umowę ze związkiem zawodowym, organ nadzorczy wskazał, że umowa powierzenia nie może być narzędziem do pozyskiwania danych osobowych w sytuacjach, w których przepisy prawa na to nie zezwalają (w tym przypadku ustawa o społecznej inspekcji pracy). Natomiast podpisywanie umowy powierzenia pomiędzy związkiem zawodowym a społecznym inspektorem pracy oznaczałoby, że nastąpiło scedowanie na niego zadań związku zawodowego. Tymczasem społeczny inspektor pracy ma własne ustawowe zadanie w ramach społecznej inspekcji pracy. Wobec czego podpisanie takiej umowy należy uznać za nieprawidłowe.

W doktrynie zauważa się, że przepisy ustawy o społecznej inspekcji pracy wskazują na silne związki społecznego inspektora pracy ze związkami zawodowymi, niemniej mają one określone ramy prawne, które nie naruszają niezależności społecznego inspektora pracy. Tytułem przykładu, w komentarzu do art. 16 ustawy o społecznej inspekcji pracy wskazano, że: „Z analizy poprzednich przepisów ustawy wynika, że działalność społecznych inspektorów pracy można zaliczyć do sfery działalności związkowej w tym sensie, że to ta organizacja w znacznym stopniu wpływa na to, kto będzie pełnił funkcję społecznego inspektora pracy i w jakim trybie będzie

[568] Wyrok Trybunału Konstytucyjnego z 26 kwietnia 2018 r. sygn. akt K 6/15 (Dz. U. poz. 830).

ów wybór przeprowadzony, ma też władczą kompetencję w zakresie rozwiązania stosunku pracy ze społecznym inspektorem pracy. Do wspomnianych płaszczyzn kompetencji zakładowej organizacji związkowej można dodać kompetencję wyższych struktur związkowych, które zostały zadekretowane w treści art. 16 u.s.i.p., zgodnie z którym ogólnokrajowe organizacje związkowe mogą określać wytyczne do działalności społecznych inspektorów pracy." A zatem, wskazane kompetencje związków zawodowych oraz ogólnokrajowych związków zawodowych nie wskazują, aby społeczny inspektor pracy realizował zadania związku zawodowego, a swoje własne, które wykonywane są w ramach społecznej inspekcji pracy.

Podsumowując organ nadzorczy wskazał, że wobec powyższych ustaleń zasadnie należy uznać, w kontekście brzmienia art. 8 ustawy o społecznej inspekcji pracy, to pracodawca (w zakresie danych osobowych, co do których jest administratorem) będzie nadawał upoważnienie społecznemu inspektorowi pracy w zakresie niezbędnym do wykonywania zadań określonych w ustawie o społecznej inspekcji pracy. Dodatkowo wskazano, że w przypadku nadawania upoważnień do przetwarzania danych osobowych osobom, których uprawnienia do przetwarzania danych osobowych wynikają z odrębnych przepisów, należy mieć na względzie cel, w jakim takie upoważnienia się nadaje. Wydawanie upoważnień może być bowiem jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych oraz kontroli nad procesem ich przetwarzania zgodnie z art. 29 i art. 32 ust. 4 RODO i dlatego należy go odróżnić od uprawnienia do dostępu do danych osobowych przyznanego określonym funkcjom czy zawodom przez przepisy prawa w związku z wykonywanymi przez nich obowiązkami lub zadaniami.

Kwestia wątpliwości co do statusu podmiotu pojawiła się również w pytaniu IOD związanym z realizacją procesu budowlanego[569], w tym koniecznością sporządzenia projektu budowlanego i uzyskania niezbędnych decyzji administracyjnych. W tym celu projektant otrzymuje od administratora/inwestora pełnomocnictwo do działania w jego imieniu, aby z właściwych urzędów np. zebrać dane osobowe właścicieli nieruchomości i na ich podstawie opracować, na potrzeby umowy, wniosek o decyzję o lokalizacji inwestycji, która jest potrzebna, żeby uzyskać pozwolenie na budowę i przekazać inwestorowi gotowy produkt w postaci decyzji administracyjnych (w tym o lokalizacji inwestycji, decyzji o pozwoleniu na budowę i projektu budowlanego z danymi osobowymi wspomnianych właścicieli nieruchomości). Wątpliwości IOD dotyczyły tego, **czy w ww. przypadku należy zawrzeć z projektantem umowę powierzenia, czy jednak będzie on odrębnym administratorem** (zbliżonym do statusu adwokata/radcy prawnego).

W odpowiedzi organ nadzorczy wskazał, że w celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, czy jednak istnieje konieczność zawarcia umowy powierzenia należy przede wszystkim dokonać analizy m.in. konkretnych przepisów mających zastosowanie w określonej sytuacji. Rodzaj i charakter kompetencji oraz obowiązków określonych w przepisach prawa

[569] DOL.502.6.2025.

przypisanych danemu podmiotowi, może być bowiem jednym z powodów uznania go za administratora.

Główne obowiązki inwestora zostały wskazane w art. 18 ust. 1 Prawa budowlanego. Analiza tych przepisów wskazuje, że niewątpliwie inwestor jest administratorem danych osobowych przetwarzanych w związku realizacją swoich zadań określonych w Prawie budowlanym.

W myśl przepisów RODO konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator w celu realizacji swoich celów (zadań) związanych z przetwarzaniem danych posługuje się innym, zewnętrznym podmiotem. Podmiot przetwarzający jest zobowiązany do stosowania się do instrukcji przekazanych przez administratora co najmniej w odniesieniu do celu przetwarzania oraz istotnych elementów sposobu przetwarzania.

Wobec powyższego organ nadzorczy wskazał, że w sytuacji, gdy projektant otrzymuje od inwestora pełnomocnictwo w celu realizacji ustawowych zadań inwestora, a nie swoich, uzasadnione jest uznanie, że działa on w imieniu i zgodnie z instrukcjami inwestora, a zatem jako podmiot przetwarzający. Będzie tak również w przypadku, gdy projektant na podstawie udzielonego pełnomocnictwa reprezentuje inwestora w postępowaniach administracyjnych mających na celu otrzymanie stosownych pozwoleń, decyzji, zgłoszeń koniecznych dla realizacji procesu budowy. Warto mieć na uwadze, że z zadań projektanta określonych w przepisach prawa (art. 20 Prawa budowlanego) nie wynika, aby projektant miał ustawowe zadania, takie jak wskazane w pytaniu, tj. reprezentowanie inwestora w postępowaniach administracyjnych. Trudno zatem uznać za zasadne twierdzenie, że status projektanta jest zbliżony do statusu adwokata.

### Ad. 5. Realizacja obowiązków wynikających z RODO

Pytania od inspektorów dotyczą też zadań wprost wynikających z RODO. Jako ich przykład można podać to dotyczące **dopuszczalności prowadzenia rejestru czynności przetwarzania wyłącznie w formie elektronicznej**[570].

W odpowiedzi organ nadzorczy wskazał, że inspektor słusznie przyjmuje, że prawodawca w RODO „uznał formę elektroniczną za pełnoprawną formę pisemną". W materiale „Wskazówki i wyjaśnienia dotyczące obowiązku z art. 30 ust. 1 i 2 RODO"[571] odnosiliśmy się do formy prowadzenia rejestru czynności przetwarzania danych osobowych (RCPD), wskazując, że stosownie do art. 30 ust. 3 RODO rejestry powinny być prowadzone w formie pisemnej. Przepis ten nie narzuca jednak wymagań dotyczących postaci, w jakiej rejestry powinny być prowadzone – może więc być zarówno papierowa, jak i elektroniczna. Ważne, żeby w każdym przypadku administrator lub podmiot przetwarzający był w stanie przedstawić wymagane w art. 30 ust. 1 i 2 RODO elementy w odniesieniu do wszystkich prowadzonych procesów przetwarzania danych osobowych, w sposób czytelny i przejrzysty. Rejestry te mają

[570] DPNT.502.204.2025.
[571] Dostępnym pod linkiem https://uodo.gov.pl/pl/383/214.

ułatwić organowi nadzorczemu kontrolę wszystkich procesów przetwarzania danych w organizacji, a administratorom i podmiotom przetwarzającym stałą weryfikację swojej działalności w zakresie przetwarzania danych osobowych oraz dokonywaniu oceny każdego nowo wprowadzanego lub modyfikowanego procesu na jak najwcześniejszym etapie. Istotne jest zatem, aby administrator lub podmiot przetwarzający był gotów pokazać, że posiada wymienione wyżej rejestry, i aby ich zawartość była zgodna z wymaganiami wskazanymi w art. 30 RODO.

Niezależnie od powyższego organ nadzorczy zwrócił uwagę, że mimo braku w przepisie art. 30 RODO regulacji dotyczącej aktualizacji rejestrów prowadzonych przez administratorów lub podmioty przetwarzające, konieczność ich aktualizacji wynika przede wszystkim z art. 24 RODO, który nakłada na administratora obowiązek przeglądu i uaktualniania wdrażanych przez niego środków zapewniających zgodność z RODO. Przemawia za tym również realizacja zasady rozliczalności (art. 5 ust. 2 RODO), w związku z obowiązkiem wynikającym z art. 30 ust. 4, zgodnie z którym administrator lub podmiot przetwarzający udostępniają rejestr na żądanie organu nadzorczego (weryfikacja nie tylko faktu jego prowadzenia, ale i poprawności przetwarzania, także w kontekście utrzymywania rejestrów w aktualności). Warto zatem, aby administrator przyjął w swojej organizacji konkretne zasady zatwierdzania i aktualizowania rejestru czynności przetwarzania danych.

### Ad. 6. Podstawa prawna do przetwarzania

Zgodnie z zasadą legalności (art. 5 ust. 1 lit. a RODO) podmiot może przetwarzać dane osobowe wyłącznie wtedy, gdy istnieje podstawa prawna przetwarzania danych osobowych. Przetwarzanie tzw. danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6 RODO. Zaś przetwarzanie szczególnych kategorii danych, określonych w art. 9 ust 1 RODO, jest co do zasady zabronione, chyba że spełniony jest jeden z warunków wskazanych w ust. 2 tego artykułu. Przez pryzmat ww. zasady w związku z przesłankami wskazanymi w art. 6 ust. 1 i art. 9 ust. 2 rozporządzenia 2016/679 ocenia się dozwolony charakter przetwarzania danych, odpowiednio zwykłych i szczególnych kategorii. W pytaniach od inspektorów ochrony danych wątpliwości dotyczą zazwyczaj tego, czy określone przepisy prawa dają podstawę do przetwarzania konkretnych danych osobowych, albo też czy rozważana przez administratora przesłanka, np. zgoda, będzie mogła mieć zastosowanie w danej sytuacji.

Przykładem takich wątpliwości może być pytanie, **czy przedszkole publiczne na etapie rekrutacji może pozyskiwać numery PESEL rodziców na potrzeby postępowania egzekucyjnego**[572]. W odpowiedzi organ nadzorczy poinformował, że zgodnie z przepisami ustawy – Prawo oświatowe brak jest podstaw do zbierania numerów PESEL rodziców dzieci na etapie rekrutacji do przedszkoli. Kwestia ta poruszona została w materiale pt. „Rodziców ważne wybory, czyli nabór do przedszkoli i szkół na rok szkolny 2020/2021”, opublikowanym na stronie internetowej UODO i był

[572] DPNT.502.200.2025. Materiał dotyczący tego zagadnienia opublikowany został również w Biuletynie UODO 1/2026.

tam dostępny do końca 2022 r. W materiale tym organ nadzorczy wskazał, że „do Prezesa UODO napływają w związku z prowadzonymi rekrutacjami pytania, sygnalizujące zbieranie przez szkoły danych, takich jak: numer PESEL, numer i seria dowodu osobistego rodziców kandydata. W tym wypadku zbieranie takich danych stanowi naruszenie nie tylko Prawa oświatowego, ale i zasad (m.in. legalizmu, proporcjonalności i minimalizacji), o których mowa w art. 5 RODO. Regulacje prawa oświatowego dotyczące treści wniosku o przyjęcie do przedszkola, szkoły (art. 150 i 151) nie wymieniają bowiem danych rodziców w postaci numeru PESEL, numeru i serii dowodu osobistego (w odróżnieniu od np. numeru PESEL kandydata), jako tych, które szkoła (przedszkole) może żądać w ramach rekrutacji”.

Można także dodać, że skoro przepisy ustawy Prawo oświatowe wprost wskazują, jakie dane osobowe ma zawierać wniosek o przyjęcie do przedszkola, szkoły i innych placówek oświatowych to wynikające z art. 152 uprawnienie organu prowadzącego publiczne przedszkola i inne placówki oświatowe do określenia wzoru wniosku lub zgłoszenia, o którym mowa w art. 150 i art. 151 ww. ustawy, nie może wykraczać poza to co regulują przepisy prawa, a zatem nie może zmieniać zakresu danych wymienionych w tych przepisach i celu dla którego są one pozyskiwane.

Ponadto ustawodawca w sytuacji, gdy uznaje konieczność podania numeru PESEL, ustanawia przepisy, które wprost nakładają obowiązek jego podania. Z takim przypadkiem mamy do czynienia w art. 27 § 1 pkt 2 ustawy o postępowaniu egzekucyjnym w administracji, który stanowi, że to tytuł wykonawczy ma zawierać numer PESEL. Zatem dopiero na etapie prowadzonego postępowania egzekucyjnego uzasadnione jest przetwarzanie numeru PESEL strony postępowania.

Organ nadzorczy zwrócił również uwagę, że numer PESEL to krajowy numer identyfikacyjny, który powinien podlegać szczególnej ochronie (zgodnie z art. 87 RODO). Pozyskiwanie takich danych na zapas, na wszelki wypadek, np. na potrzeby ewentualnego postępowania egzekucyjnego, które jest odrębnym postępowaniem, jest działaniem nadmiarowym, naruszającym zasadę legalizmu, zasadę ograniczenia celu oraz zasadę minimalizacji danych. Dopiero niewykonanie zobowiązania wynikającego z decyzji administracyjnej rozpoczęłoby bieg nowej procedury, prowadzonej zgodnie z przepisami o postępowaniu egzekucyjnym w administracji. I to na tym etapie legalne byłoby przetwarzanie numeru PESEL, który – zgodnie z art. 27 § 1 pkt 2 ustawy o postępowaniu egzekucyjnym w administracji – musi być zamieszczony w wystawionym tytule wykonawczym. Przepis ten jest zatem przesłanką legalizującą proces przetwarzania danych osobowych w odniesieniu do danych zawartych w wystawionym tytule wykonawczym.

Organ nadzorczy zwrócił też uwagę na przepisy ustawy z dnia 24 września 2010 r. o ewidencji ludności, które wskazują, jakim organom i na jakich zasadach oraz w jakim celu można udostępnić dane z rejestru PESEL (art. 46). Stanowią one w szczególności, 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 (art. 46 ust. 1 pkt 1), a także państwowym i samorządowym jednostkom organizacyjnym oraz innym podmiotom –

w zakresie niezbędnym do realizacji zadań publicznych określonych w odrębnych przepisach (art. 46 ust. 1 pkt 5).

W innym pytaniu IOD zwrócił się do Prezesa UODO z wątpliwościami w zakresie **wskazywania zgody jako podstawy prawnej przetwarzania danych osobowych pacjenta w celu wydania mu kopii dokumentacji medycznej przez placówkę medyczną**[573]. W odpowiedzi organ nadzorczy wskazał, że podstawą prawną przetwarzania danych osobowych przez placówkę medyczną w celu wydania dokumentacji medycznej jest art. 24 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Zgodnie z tym przepisem w celu realizacji prawa, o którym mowa w art. 23 ust. 1 ww. ustawy (tj. prawa pacjenta dostępu do dokumentacji medycznej), podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w niniejszym rozdziale oraz w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, a także zapewnić ochronę danych zawartych w tej dokumentacji. Tym samym spełniona jest określona w art. 9 ust. 2 lit. h RODO przesłanka uprawniająca do przetwarzania danych szczególnej kategorii m.in. wtedy, gdy zgodnie z przepisami prawa krajowego lub unijnego jest ono niezbędne do celów zapewnienia opieki zdrowotnej.

Jednocześnie podkreślił, że odbieranie zgody na przetwarzanie danych osobowych w sytuacji, gdy podstawą prawną przetwarzania danych osobowych – w tym samym zakresie i celu – jest określony przepis prawa, jest działaniem wprowadzającym osobę, która udziela zgody, w błąd. Jest ona bowiem przekonana, że to na tej podstawie przetwarzane są jej dane i gdy wycofa zgodę, to administrator zaprzestanie dalszego przetwarzania.

W kolejnym z pytań IOD zwrócił się o wskazówki w zakresie ustalenia **właściwej podstawy prawnej przetwarzania danych osobowych szczególnej kategorii znajdujących się w zgłoszeniu od sygnalisty**[574].

W przesłanych wyjaśnieniach organ nadzorczy wskazał, że gdy zgłoszenie sygnalisty obejmuje dane szczególnej kategorii, właściwą przesłanką spośród wskazanych w art. 9 ust 2 RODO wyjątków od zakazu przetwarzania takich danych wydaje się być art. 9 ust. 2 lit. g RODO w połączeniu z właściwymi przepisami dotyczącymi ochrony sygnalistów. Zgodnie z tym przepisem dozwolone jest przetwarzanie szczególnej kategorii danych osobowych gdy jest niezbędne 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.

Organ nadzorczy uzasadniając swoją opinię wskazał, że motyw 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii − której implementację stanowi polska ustawa o ochronie sygnalistów − nawiązuje do „interesu publicznego”. Zgodnie

[573] DPNT.502.13.2025.
[574] DPNT.502.128.2025.

z brzmieniem tego przepisu, osoby pracujące dla organizacji publicznej lub prywatnej lub utrzymujące kontakt z taką organizacją w związku ze swoją działalnością zawodową niejednokrotnie jako pierwsze dowiadują się o zagrożeniach lub szkodach dla interesu publicznego, do jakich dochodzi w tym kontekście. Zgłaszając naruszenia prawa Unii, które są szkodliwe dla interesu publicznego, osoby takie działają jako „sygnaliści" i tym samym odgrywają kluczową rolę w ujawnianiu takich naruszeń i zapobieganiu im oraz w ochronie dobra społecznego. Potencjalni sygnaliści często jednak rezygnują ze zgłaszania swoich zastrzeżeń lub podejrzeń z obawy przed działaniami odwetowymi. W związku z tym w coraz większym stopniu uznaje się, zarówno na poziomie unijnym, jak i międzynarodowym, znaczenie zapewnienia zrównoważonej i skutecznej ochrony sygnalistów. Doktryna również wskazuje, że celem ustawy o ochronie sygnalistów jest ujawnianie i eliminowanie naruszeń prawa w celu ochrony interesu publicznego[575].

### Ad. 7. Udostępnianie danych osobowych

Koleją kategorią spraw przedkładanych przez inspektorów ochrony danych były sprawy związane z rozpatrywaniem przez administratorów wniosków o udostępnienie danych osobowych.

Jedno z pytań dotyczyło problemu związanego z otrzymywaniem przez uczelnię od miejskich ośrodków pomocy społecznej i powiatowych centrum pomocy rodzinie **wniosków o udostępnienie danych osobowych studentów, którzy korzystają ze środków Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych w ramach realizacji Programu „Aktywny samorząd"**[576]. We wnioskach jest zawarta prośba dotycząca potwierdzenia faktu pobierania nauki przez konkretną osobę fizyczną. Pomioty te jako podstawę prawną do udostępniania takich danych wskazują umowę o dofinansowanie zawartą ze studentem. W ocenie IOD w analizowanym przez niego przypadku na uczelni nie ciąży obowiązek udostępnienia danych osobowych studenta, ponieważ uczelnia nie jest stroną wskazanej umowy. IOD poprosił o potwierdzenie poprawności jego stanowiska.

Odnosząc się do tego zagadnienia organ nadzorczy wskazał, że każdy wniosek o udostępnienie danych wymaga indywidualnej analizy. Rozpatrujący go administrator, który podejmuje ostateczną decyzję w tej sprawie, musi wziąć przy tym 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. Ponadto w przypadku podmiotów publicznych warto mieć na uwadze określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa, zgodnie z którą kompetencji organu publicznego nie można domniemywać, jeśli nie wynikają one wprost z przepisu prawa. Dlatego gdy o udostępnienie danych osobowych występuje podmiot realizujący

[575] J. Hajn, M. Sudoł [w:] Ochrona sygnalistów. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, J. Łuczak-Tarka, Warszawa 2025, art. 3.
[576] DPNT.502.98.2025.

zadania publiczne, powinien w pierwszej kolejności wskazać konkretne przepisy prawa uprawniające go do pozyskania danych.

Wobec powyższego organ nadzorczy poinformował, że słusznie IOD podważa prawidłowość praktyki wskazywania przez MOPS lub PCPR jako podstawy do udostępnienia danych studenta faktu zawarcia przez nie ze studentem umowy dofinansowania wypłacanego w ramach programu „Aktywny samorząd". Z przywołanych przez inspektora postanowień umownych wynikało, że dają one podstawę do domagania się przedstawienia określonych informacji jedynie od beneficjenta (studenta).

Ponieważ MOPS oraz PCPR są podmiotami publicznymi, to zgodnie z przywołaną powyżej zasadą praworządności, podstawa prawna do pozyskiwania przez nie informacji (w tym danych osobowych) co do zasady powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami. Przepisem prawa regulującym kwestie pozyskiwania informacji przez ośrodki pomocy społecznej jest w szczególności art. 105 ust. 1 ustawy o pomocy społecznej, który może być podstawą prawną do udostępniania danych osobowych przez uczelnie we wskazanych w tym przepisie celach. Ponadto organ nadzorczy zwrócił uwagę, że w przypadku rozstrzygania przez uczelnię dopuszczalności udostępnienia danych osobowych studentów decydujące znaczenie mogą mieć też przepisy ustawy Prawo o szkolnictwie wyższym i nauce oraz aktów wykonawczych do niej.

Podsumowując tę odpowiedź organ nadzorczy wskazał, że jeżeli wniosek o udostępnienie danych osobowych budzi wątpliwości pod względem jego podstaw prawnych, dobrym rozwiązaniem jest zwrócenie się do wnioskodawcy o wyjaśnienie tych wątpliwości. Jednocześnie administrator, do którego skierowano wniosek o udostępnienie danych, powinien również dokonać oceny, czy wnioskowane dane osobowe nie podlegają szczególnej regulacji w zakresie ich udostępniania. Zgromadzenie powyższych informacji pozwoli na dokonanie poprawnej analizy dopuszczalności takiego udostępnienia.

Inną kwestią podnoszoną przez IOD, a związaną z udostępnianiem danych osobowych, był **zakres informacji, jakie mogą być ujawniane na wniosek akcjonariuszy z rejestru akcjonariuszy**[577]. W odpowiedzi organ nadzorczy wskazał, że zgodnie z art. 328 (5) Kodeksu spółek handlowych (KSH) rejestr akcjonariuszy spółki akcyjnej jest jawny dla spółki i każdego akcjonariusza (par. 1). Podmioty wskazane w tym przepisie mają, po pierwsze, prawo dostępu do danych zawartych w rejestrze akcjonariuszy za pośrednictwem podmiotu prowadzącego rejestr akcjonariuszy (par. 2). Po drugie, mają prawo żądać wydania, w postaci papierowej lub elektronicznej, informacji z rejestru akcjonariuszy (par. 3). Art. 328 (3) KSH wskazuje z kolei, jakie dane zawiera rejestr akcjonariuszy.

Odnosząc się zatem do pytania inspektora, organ nadzorczy wskazał, że w świetle przytoczonych przepisów Kodeksu spółek handlowych akcjonariusz ma dostęp do rejestru akcjonariuszy z uwagi na jego jawność, a jego uprawnienie do

[577] DOL.502.229.2024.

wglądu w ten rejestr wynika wprost z art. 328 (5) KSH. Z przepisu tego nie wynika natomiast, aby można było mu ograniczać dostęp do jakichkolwiek informacji, które w rejestrze się znajdują.

**Ad. 8. Naruszenia ochrony danych**

Zagadnieniem budzącym wątpliwości IOD często jest kwestia postępowania w sprawach dotyczących naruszeń ochrony danych. Poniżej dla przykładu wskazano kilka odpowiedzi dotyczących tego zagadnienia udzielonych w 2025 r.

W odpowiedzi na pytanie IOD przedstawiające wątpliwości w zakresie **zakwalifikowania określonego zdarzenia jako naruszenie ochrony danych osobowych** organ nadzorczy wskazał[578], że oceny w tym zakresie należy dokonać przede wszystkim przez pryzmat definicji zawartej w art. 4 pkt 12 RODO. Dodatkowo odwołał się do decyzji z 9 grudnia 2020 r.[579] w której wskazał, że „z naruszeniem ochrony danych mamy do czynienia zarówno wówczas, gdy do zdarzenia dojdzie wskutek świadomego działania, jak i wtedy, gdy doprowadzi do niego nieumyślność. W związku z powyższym fakt, że do naruszenia doszło w wyniku błędu klienta, który przekazał agentowi nieprawidłowy adres mailowy, nie może mieć wpływu na ocenę tego zdarzenia i zakwalifikowanie go jako naruszenia ochrony danych osobowych. Jego skutkiem jest bowiem udostępnienie danych osobowych osobie nieuprawnionej, co oznacza, że doszło do naruszenia poufności danych". Przywołał również wskazówki zawarte w „Poradniku dotyczącym naruszeń ochrony danych osobowych"[580], gdzie wskazano również, że naruszenie ochrony danych osobowych pojawia się więc zawsze, gdy dochodzi do zdarzenia, które: 1) jest incydentem bezpieczeństwa; 2) dotyczy przetwarzanych danych osobowych; 3) może doprowadzić do ich nieuprawnionego zniszczenia, utracenia, zmodyfikowania, ujawnienia lub dostępu do nich. Tym samym naruszeniem ochrony danych osobowych nie jest zdarzenie, które nie spełnia któregoś z tych warunków. Co istotne dochodzi do niego bez względu na to, czy wystąpi przez przypadek (np. w wyniku błędu, zaniedbania lub nieprzewidzianej awarii technicznej) czy też na skutek celowego, bezprawnego działania.

Konkludując organ nadzorczy wskazał, że w przywołanej wyżej decyzji Prezesa UODO wyraźnie wskazano, że z naruszeniem ochrony danych osobowych możemy mieć do czynienia nawet w sytuacji niezawinionego działania administratora. Istotą bowiem takiego zdarzenia jest nieuprawnione ujawnienie danych osobowych skutkujące naruszeniem poufności danych.

Wątpliwości innego z inspektorów dotyczyły sposobu postępowania w przypadku, gdy **zgłoszenie dokonane przez sygnalistę dotyczy nieprawidłowości mogących stanowić naruszenie danych osobowych** (w rozumieniu art. 33 RODO) przetwarzanych przez podmiot przyjmujący to zgłoszenie[581]. W odpowiedzi organ nadzorczy wskazał, że procedowanie takiego

[578] DPNT.502.45.2025.
[579] Sygn. akt DKN.5131.5.2020 (https://uodo.gov.pl/decyzje/DKN.5131.5.2020).
[580] Zob. str. 8, https://uodo.gov.pl/pl/598/3563.
[581] DPNT.502.183.2025.

zgłoszenia powinno następować z uwzględnieniem zarówno regulacji odnoszących się do ochrony sygnalistów, jak i regulacji dotyczących procedowania naruszeń ochrony danych osobowych przewidzianych w RODO. Sam fakt, że informacja o potencjalnym naruszeniu ochrony danych osobowych pochodzi od sygnalisty, nie zwalnia administratora z obowiązku dokonania oceny naruszenia oraz ewentualnego zgłoszenia go do organu nadzorczego i poinformowania osób, których dane dotyczą.

Przepisy ustawy o sygnalistach nie zawierają regulacji wyłączających stosowanie przepisów RODO ani umożliwiających odroczenie w czasie realizacji obowiązków nałożonych na administratora na podstawie art. 33–34 RODO. W przypadku ustalenia, że zgłoszenie pochodzące od sygnalisty wskazuje na możliwość wystąpienia naruszenia ochrony danych osobowych, administrator jest zobowiązany niezwłocznie wszcząć procedurę oceny tego naruszenia, zgodnie z przepisami RODO, zapewniając przy tym ochronę poufności, o której mowa w ustawie o ochronie sygnalistów (art. 27). Procedura obsługi zgłoszenia sygnalisty i procedura dotycząca obsługi naruszeń ochrony danych powinny funkcjonować równolegle.

### Ad. 9. Przetwarzanie wizerunku

Zagadnieniem, które pojawiało się w pytaniach od inspektorów w okresie sprawozdawczym jest przetwarzanie wizerunku. W jednym z nich[582] IOD podzielił się swoimi wątpliwościami, co do sposobu określenie okresu przetwarzania (przechowywania) danych osobowych w postaci wizerunku. W odpowiedzi organ nadzorczy wskazał, że do tego zagadnienia UODO odnosił się już w materiale „Czy trzeba precyzyjnie określać okres przechowywania danych?”, który zmieszczony jest obecnie w Biuletynie UODO - Wydanie specjalne[583]. Wskazano tam m.in., że zgodnie z art. 5 ust. 1 lit. e RODO dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”).

Żeby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu (motyw 39 RODO). Kwestie okresu przechowywania danych zależne są od celu przetwarzania i jeśli okres przechowywania nie został określony w przepisach prawa, wówczas powinien zostać określony przez administratora mającego pełną wiedzę o danym procesie przetwarzania. Wskazanie okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, określenie kryteriów ustalania tego okresu, jest jedną z informacji podawanych podczas dopełniania

[582] DPNT.502.92.2025.
[583] Dostępnym pod linkiem: https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod.

obowiązku informacyjnego spełnianego wobec osoby, której dane dotyczą, na mocy art. 13 ust. 2 lit. a i art. 14 ust. 2 lit. a RODO.

Organ nadzorczy poinformował również, że w Wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679 (str. 46) wskazano, że „informacja o okresie przetwarzania powinna być sformułowana w taki sposób, aby osoba, której dane dotyczą, miała możliwość ocenienia – na podstawie własnej sytuacji – ile będzie trwał okres przechowania w przypadku określonych danych/celów. Ogólne stwierdzenie przez administratora, że dane osobowe będą przechowywane tak długo, jak jest to niezbędne do prawnie uzasadnionych celów przetwarzania, jest niewystarczające. W stosownych przypadkach należy ustalić różne okresy przechowywania dla różnych kategorii danych osobowych lub różnych celów przetwarzania, w tym okresy archiwizacji".

Organ nadzorczy zauważył również, że określenie tego okresu jest też wymagane w związku z obowiązkiem prowadzenia rejestru czynności przetwarzania (art. 30 ust. 1 lit. f RODO). Ponadto jak wskazuje się w doktrynie ogólną zasadą jest zakaz przechowywania danych osobowych w nieskończoność[584].

Podsumowując organ nadzorczy wskazał, że to do administratora należy decydowanie o tym, w jakim celu odbywa się przetwarzanie danych osobowych oraz zapewnienie, aby dane nie były przetwarzane dłużej niż do jego osiągnięcia. Zatem w przypadku danych osobowych przetwarzanych na podstawie zgody osoby, której dane dotyczą, ich przechowywanie jest dopuszczalne do czasu osiągnięcia celu, dla którego została udzielona. O tym, kiedy taki cel zostanie osiągnięty, decyduje administrator. Określony przez administratora okres przetwarzania danych może ulec skróceniu w przypadku wycofania zgody.

Zatem zapis w klauzuli informacyjnej, że dane osobowe w postaci wizerunku będą przetwarzane „do czasu wycofania zgody", nie jest zgodny z zasadą ograniczenia przechowywania, ponieważ w przypadku, gdyby zgoda nie została wycofana, dane byłyby przechowywane w nieskończoność. Administrator nie może zatem przechowywać danych bezterminowo tylko dlatego, że zgoda nie została formalnie odwołana.

Odnosząc się natomiast do zawartej w piśmie IOD informacji, że chodzi również o przetwarzanie danych osób niepełnoletnich, organ nadzorczy zwrócił uwagę, że dzieci wymagają szczególnej ochrony, ponieważ mogą być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. RODO stawia administratorom przetwarzającym dane dzieci szczególne wymagania, w tym m.in.:

- stanowi, że informacje i komunikaty powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć (motyw 58 RODO),
- wskazuje, że należy zapewnić dzieciom dostęp do ich danych oraz informacji na temat ich przetwarzania,

[584] P. Drobek [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 5.

– zakazuje przetwarzania danych polegającego na profilowaniu dzieci (motyw 71 RODO).

Administratorzy, przetwarzając dane osobowe dzieci, powinni też stosować dodatkowe środki zabezpieczające, aby chronić ich prywatność.

Zagadnienie dotyczące przetwarzania wizerunku pojawiło się również w pytaniu od IOD, **kto wyraża zgodę na przetwarzania wizerunku w stosunku do osoby całkowicie ubezwłasnowolnionej**[585]. W odpowiedzi organ nadzorczy wskazał, że w sprawie tej pierwszoplanowym problemem jest zapewnienie zgodności z podstawowymi zasadami określonymi w art. 5 ust. 1 RODO, w tym przypadku przede wszystkim zasadą minimalizacji (art. 5 ust. 1 lit. c RODO). Stosownie do niej administrator powinien gromadzić tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel ich pozyskiwania. Dane powinny być przetwarzane wyłącznie w takich przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami (motyw 39 RODO). Co ważne, administrator powinien dokonać oceny, czy dane rzeczywiście są konieczne do osiągnięcia celu najpóźniej w momencie ich zbierania. Przetwarzanie danych w zakresie zbędnym dla osiągnięcia celu będzie sprzeczne z RODO.

Z informacji przekazanych przez IOD wynikało, że administrator (placówka opiekuńcza) pozyskuje zgody podopiecznych w zakresie przetwarzania ich wizerunku, imienia i nazwiska w celu promocji administratora. W przedstawionej sprawie zastrzeżenie budzi przede wszystkim niezbędność wykorzystywania danych osobowych podopiecznych (imienia, nazwiska oraz ich wizerunku) do celu, jakim jest promowanie działalności placówki. Zamierzony cel można przecież osiągnąć np. poprzez ogólne informacje o inicjatywach, działaniach podejmowanych przez administratora, a nie przetwarzając tego rodzaju dane osobowe, zwłaszcza, że podopiecznymi tej placówki są osoby, które ze względu na swoją sytuację życiową wymagają szczególnej ochrony.

Organ nadzorczy wskazał, że nie można zatem pominąć tego zastrzeżenia i przejść do warunków dotyczących zgody bez spełnienia zasad określonych w art. 5 RODO, m.in. zasady rzetelności i minimalizacji danych, zwłaszcza że cel, jakim jest promocja działań ośrodka, można osiągnąć bez przetwarzania danych osobowych podopiecznych.

Jednocześnie organ nadzorczy wskazał, że w przypadku osoby całkowicie ubezwłasnowolnionej decyzje związane z przetwarzaniem jej danych, w tym te dotyczące realizacji jej praw, w imieniu podopiecznego podejmuje opiekun osoby całkowicie ubezwłasnowolnionej.

### Ad. 10. Działalność dziennikarska i radiowa

Jeden z inspektorów ochrony danych pełniący swoją funkcję w stacji radiowej zadał pytanie o możliwość **ponownego wykorzystania nagrań wypowiedzi określonej osoby w formie krótkich urywków dźwiękowych**, zwłaszcza czy

[585] DPNT.502.121.2025.

konieczna jest dodatkowa zgoda uczestnika takiej rozmowy, jeśli jego głos został już upubliczniony w audycji radiowej[586]. Odnosząc się do tego pytania organ nadzorczy zauważył, że należy ono przede wszystkim do materii prawa autorskiego i prasowego. Natomiast odpowiedź Prezesa UODO może odnosić się do przepisów o ochronie danych osobowych, które – nie jako jedyne – mogą znaleźć zastosowanie w tej sytuacji.

W przedstawionym przypadku należy przede wszystkim ustalić, w jakich celach będą przetwarzane dane osobowe (zapis foniczny rozmowy), a także jakie cele obejmuje zgoda wyrażona przez słuchacza. Ustalenie tych kwestii pozwoli dokonać następnie oceny, jakie przepisy prawa znajdą zastosowanie i czy na określone działania niezbędna jest odrębna zgoda w rozumieniu przepisów o ochronie danych osobowych.

Organ nadzorczy wskazał ponadto, że z perspektywy ochrony danych osobowych należy pamiętać, że jeżeli administrator przetwarza dane osobowe, np. publikuje je, to do jego zadań należy ocena celu przetwarzania danych, podstawy prawnej, zakresu ujawnianych danych oraz okresu, przez jaki będą przetwarzane. Administrator ma bowiem obowiązek przetwarzania danych osobowych zgodnie z określonymi w art. 5 RODO zasadami: legalności, rzetelności i przejrzystości, ograniczenia celu, adekwatności, prawidłowości, ograniczenia przechowywania oraz integralności i poufności.

Organ nadzorczy przypomniał również, że na podstawie art. 2 ust. 1 ustawy o ochronie danych osobowych do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy Prawo prasowe (u.p.p.), a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5-9, art. 11, art. 13-16, art. 18-22, art. 27, art. 28 ust. 2-10 oraz art. 30 RODO. Żeby jednak móc powoływać się na to wyłączenie, należy przede wszystkim ustalić, czy mamy do czynienia z działalnością polegającą na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, w tym czy określony materiał ma znamiona materiału prasowego w kontekście art. 2 ust. 1 u.o.d.o. i art. 7 ust. 2 pkt. 1 i 4 u.p.p. Zaznaczyć też należy, że jeśli planowana publikacja nie będzie spełniać warunków do uznania jej za materiał prasowy, to przepisy dotyczące przetwarzania danych osobowych, w tym regulujące przesłanki dopuszczalności ich przetwarzania (art. 6 ust. 1 i art. 9 ust. 2 RODO) oraz obowiązek informacyjny (art. 13, art. 14 RODO), powinny być stosowane w pełnym zakresie.

Organ nadzorczy podkreślił też, że wyłączenie stosowania ww. przepisów RODO nie oznacza, że dziennikarze nie muszą chronić praw osób, których dane przetwarzają, a jedynie że ochrona została ukształtowana inaczej. Działalność prasowa podlega bowiem regulacji prawa prasowego i tam ukształtowane są odmienne konstrukcje mające służyć ochronie osób, których dane są przetwarzane[587].

[586] DPNT.502.49.2025. Materiał dotyczący tego zagadnienia opublikowany został w Biuletynie UODO 6/2025.
[587] Zob. np. wyrok NSA z 7 września 2021 r., sygn. akt III OSK 2883/21.

Odnosząc się zaś do kwestii przesłanki zgody jako podstawy do przetwarzania danych (w tym do publikacji nagrań rozmów), organ nadzorczy zaznaczył, że w każdym przypadku opierania się na przesłance zgody należy zadbać o to, aby osoba, która taką zgodę ma wyrazić, dysponowała dokładnymi i pełnymi informacjami na temat tego, w jaki sposób jej dane (np. nagranie jej wypowiedzi) będą wykorzystywane (w tym m.in. w jakim celu/celach, w jakim zakresie, w jakim terminie, przez jaki okres). Informacje te są niezbędne, aby osoba ta mogła świadomie wyrazić swoją wolę.

Jest to o tyle istotne, że na gruncie prawa ochrony danych osobowych, aby zgoda mogła stanowić podstawę przetwarzania danych, muszą zostać spełnione bardzo konkretne warunki określone w art. 4 pkt 11 oraz w art. 7 RODO. 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. Dodatkowo w pkt 3.3.1 Wytycznych EROD 05/2020 dotyczących zgody na mocy rozporządzenia 2016/679 wskazano, że aby móc uznać, że zgoda jest „świadoma", należy poinformować osobę, której dane dotyczą, o określonych elementach kluczowych w celu dokonania wyboru.

**Ad. 11. Stosowanie nowych regulacji**

Jeśli chodzi o pytania odnoszące się do nowych przepisów prawa, to jako ich przykład podać można wątpliwości inspektora ochrony danych dotyczące **stosowania w praktyce art. $18^{3ca}$ – nowego przepisu ustawy z 26 czerwca 1974 r. – Kodeks pracy (dalej k.p.),** który zaczął obowiązywać od 24 grudnia 2025 r.[588]. Zgodnie z brzmieniem § 3 tego przepisu pracodawca zapewnia, aby ogłoszenia o naborze na stanowisko oraz nazwy stanowisk były neutralne pod względem płci, a proces rekrutacyjny przebiegał w sposób niedyskryminujący.

Oznacza to, że w treści ogłoszeń o pracę przy określaniu nazwy stanowiska pracodawcy będą mieli obowiązek stosować neutralny płciowo język, np. „specjalista/specjalistka", „sekretarz/sekretarka".

Ja słusznie wskazał inspektor, dokumentem skierowanym do osoby w procesie rekrutacji jest również klauzula informacyjna RODO. W opinii organu nadzorczego przyjęta przez inspektora konstrukcja użycia formy grzecznościowej „Pani/Pan" w takiej klauzuli spełnia wymogi zachowania neutralnej formy. Można również rozważyć wprowadzenie innej formy grzecznościowej, np. „Państwo".

W odpowiedzi wskazano ponadto, że wydaje się, że nie ma przeszkód, aby również w odniesieniu do innych kategorii osób, których dane osobowe są przetwarzane, zastosować te same standardy.

**Podsumowując tę część Sprawozdania** wskazać należy, że Prezes UODO niezmiennie dużą wagę przywiązuje do współpracy z inspektorami ochrony danych. Ich rola – co organ nadzorczy konsekwentnie podkreśla – ma bowiem fundamentalne

[588] DPNT.502.207.2025.

znaczenie dla budowy skutecznego systemu ochrony danych osobowych. Zgodnie z przepisami RODO polega ona głównie na fachowym wspieraniu administratorów w obszarze zapewnienia zgodnego z prawem przetwarzania danych osobowych, w tym monitorowaniu prowadzonego przetwarzania, a także na doradzaniu w zakresie obowiązków ciążących na administratorach i podmiotach przetwarzających. Niezwykle istotna jest również rola IOD jako punktu kontaktowego dla osób, których dane dotyczą, a także dla organu nadzorczego.

Dlatego w działaniach podejmowanych przez Prezesa UODO niezmiernie ważną kwestią było zarówno wspieranie IOD we właściwym wypełnianiu przez nich ich funkcji, w tym weryfikowanie przestrzegania przez podmioty powołujące IOD przepisów dotyczących funkcjonowania IOD, jak i udzielanie inspektorom konsultacji we wszelkich sprawach, którymi się zajmują.

Inspektorzy ochrony danych chętnie korzystają z konsultacji z UODO, przedstawiając problemy i wątpliwości, z którymi spotykają się w bieżącej pracy. W 2025 roku przedstawiane przez IOD zagadnienia dotyczyły bardzo zróżnicowanych zagadnień, w tym zwłaszcza: statusu i zadań inspektora ochrony danych, podstawy prawnej do przetwarzania, określenia statusu podmiotów w procesie przetwarzania danych osobowych, naruszeń ochrony danych, pojęcia danych osobowych, działalności dziennikarskiej i radiowej, przetwarzania wizerunku czy stosowania nowych regulacji prawnych.

Dużą i bardzo ważną grupę spośród ww. stanowiły pytania dotyczące kwestii związanych z właściwym rozumieniem funkcji IOD, w tym z prawidłowym umiejscowieniem ich w strukturze organizacji czy rozróżnieniem zdań IOD od zadań administratora, a także łączeniem tej funkcji z innymi zadaniami, np. z zadaniami: zastępcy głównego księgowego, kierownika ds. kontroli, pełnomocnika ds. sytemu zarządzania bezpieczeństwem informacji, radcy prawnego. Organ nadzorczy – mając na uwadze, że tylko kompetentny, właściwie usytuowany i niezależny IOD może skutecznie wpływać na przestrzeganie przepisów o ochronie danych osobowych w organizacji – z dużą uwagą podchodzi do tego rodzaju pytań i stara się w odpowiedziach przekazać jak najbardziej szczegółowe wskazówki poparte wytycznymi i orzecznictwem zarówno krajowym, jak i sądów unijnych.

W 2025 r. wiele pytań od inspektorów dotyczyło również problemów ze stosowaniem i interpretacją przepisów prawa, w tym również przepisów RODO. Przykładami mogą być pytania o rozumienie pojęcia danych osobowych w kontekście konkretnych stanów faktycznych (głos, nr działki), formy prowadzenia rejestru czynności przetwarzania, zakresu danych podawanych do wiadomości publicznej, sposobu formułowania klauzul obowiązku informacyjnego. Również takie pytania stanowią dla organu bardzo ważne źródło informacji na temat aktualnych problemów, z jakimi mierzą się inspektorzy.

Pytania przesyłane przez IOD poddawane były również analizie pod kątem potrzeby podjęcia przez Prezesa UODO reakcji na sygnalizowane przez IOD problemy, w szczególności poprzez skierowanie do właściwych podmiotów wystąpień postulujących zmianę przepisów prawa bądź stosowanej praktyki. Przykładem takich

działań są wystąpienia Prezesa UODO kierowane np. do Szefa Służby Cywilnej, Ministra Zdrowia, Ministra Sprawiedliwości czy Ministra Rozwoju i Technologii, opisane w części dotyczącej tego rodzaju działań organu nadzorczego.

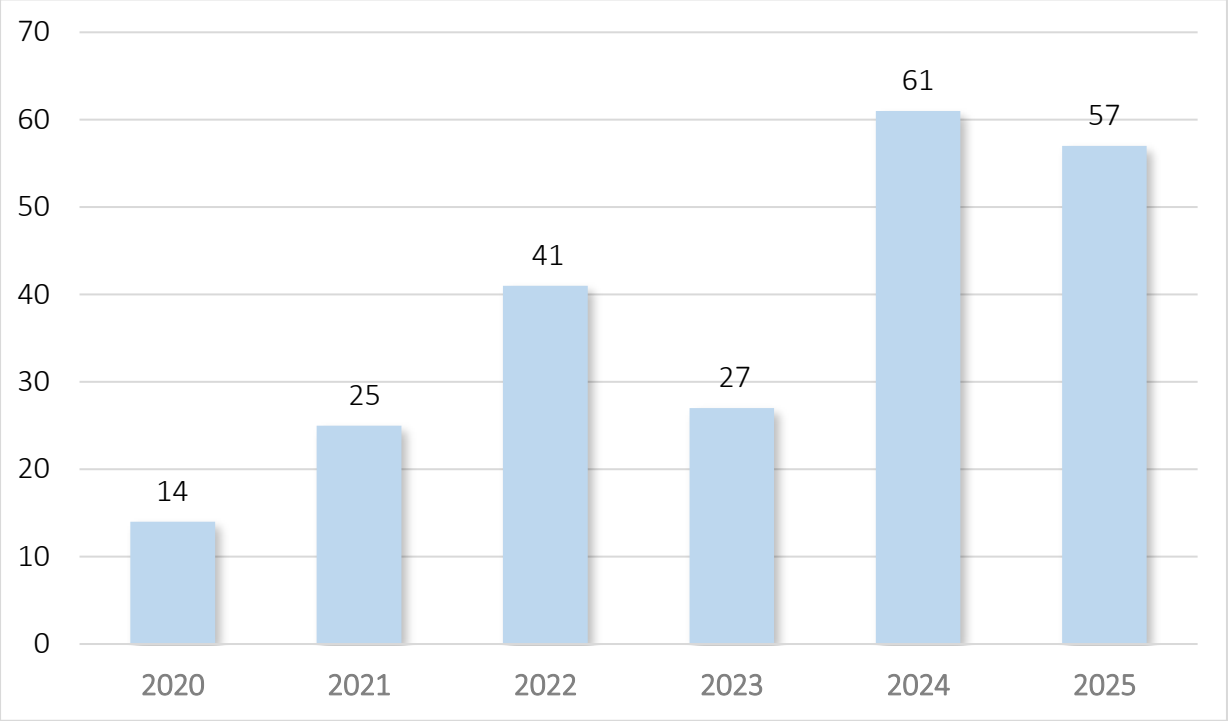
Warto również podkreślić, że odpowiedzi organu nadzorczego udzielane inspektorom często stanowią podstawę do przygotowywania materiałów służących edukowaniu inspektorów i innych podmiotów zobowiązanych do przestrzegania przepisów o ochronie danych osobowych. Mają one ułatwiać im wywiązywanie się z nałożonych przepisami RODO obowiązków i zadań, a także pomagać w wypracowaniu odpowiednich standardów i rozwiązań.

Indywidulne konsultacje z organem nadzorczym w sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem funkcji IOD stanowią istotną formę wsparcia inspektorów, służą wymianie doświadczeń, są też bardzo ważne dla ciągłego doskonalenia systemu ochrony danych osobowych.

### 18.3. Zapytania innych organów nadzorczych

Prezes UODO jest zobowiązany na podstawie przepisów RODO do udzielania odpowiedzi na pytania zadane mu przez inne organy nadzorcze z państw Unii Europejskiej. Obowiązki te realizowane są na podstawie mechanizmów spójności i współpracy uregulowanych w art. 63 i nast. RODO. Zapytania od innych organów nadzoru kierowane są do polskiego regulatora za pośrednictwem Systemu IMI (Internal Market Information System), tj. Systemu Wymiany Informacji na Rynku Wewnętrznym. Tą samą drogą przekazywane są odpowiedzi na zadane pytania.

W 2025 r. do Prezesa UODO wpłynęło **57 zapytań organów nadzorczych z innych państw.** Dla porównania, w 2024 r takich pytań wpłynęło 61, w 2023 r. - 27, w 2022 r. – 41, w 2021 r. – 25, zaś w 2020 r. – 14.




**Wykres 18:** Liczba pytań od organów nadzorczych innych państw skierowanych do Prezesa UODO w latach 2020–2025.

W 2025 roku organy nadzorcze zwracały się do Prezesa UODO z różnymi zagadnieniami. Pytania dotyczyły m.in. opinii polskiego organu nadzorczego w takich sprawach, jak:

- nakładanie kar administracyjnych przez organ ochrony danych osobowych na organy publiczne;
- Consent Management Platforms (CMP);
- możliwości zniesienia zakazu przetwarzania danych biometrycznych w środowisku pracy, w sytuacji gdy upoważnienie do zniesienia zakazu znajduje się w układzie zbiorowym pracy;
- działań prowadzonych przez Prezesa UODO dla administratorów danych osobowych w celu wsparcia w osiągnięciu zgodności z system ochrony danych osobowych;
- przetwarzania danych, takich jak materiał biologiczny (próbka genetyczna) przez biobanki.

Polski organ ochrony danych dokonał wnikliwej analizy przedłożonych pytań, a następnie przygotował stosowne odpowiedzi w języku angielskim i przekazał je do właściwych organów nadzorczych.

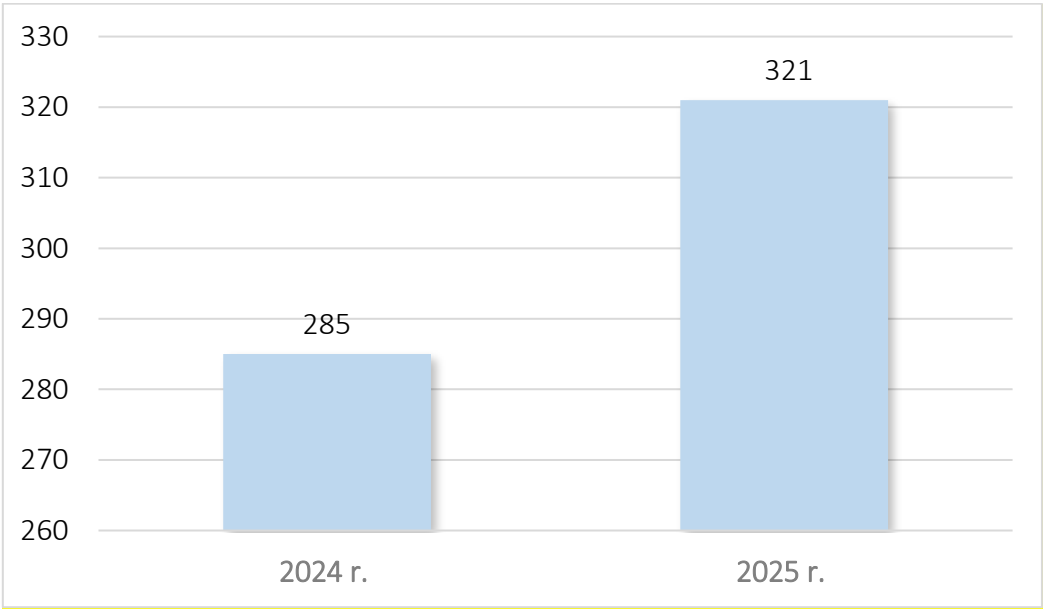
Udzielanie szczegółowych odpowiedzi umacnia współpracę z krajowymi organami nadzorczymi. Dzięki informacjom pozyskanym od innych organów nadzorczych wzrasta zrozumienie, jak RODO jest interpretowane w państwach członkowskich UE. Ponadto otrzymywane pytania pozwalają rozeznać się w bieżących

zagadnieniach, będących przedmiotem dyskusji innych organów nadzorczych. Pozwala to również na wypracowanie zharmonizowanych, wspólnych stanowisk przy uwzględnieniu ustawodawstwa krajowego.

### 18.4. 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 RP 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. 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 2025 r. do Urzędu Ochrony Danych Osobowych wpłynęło łącznie **321 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.



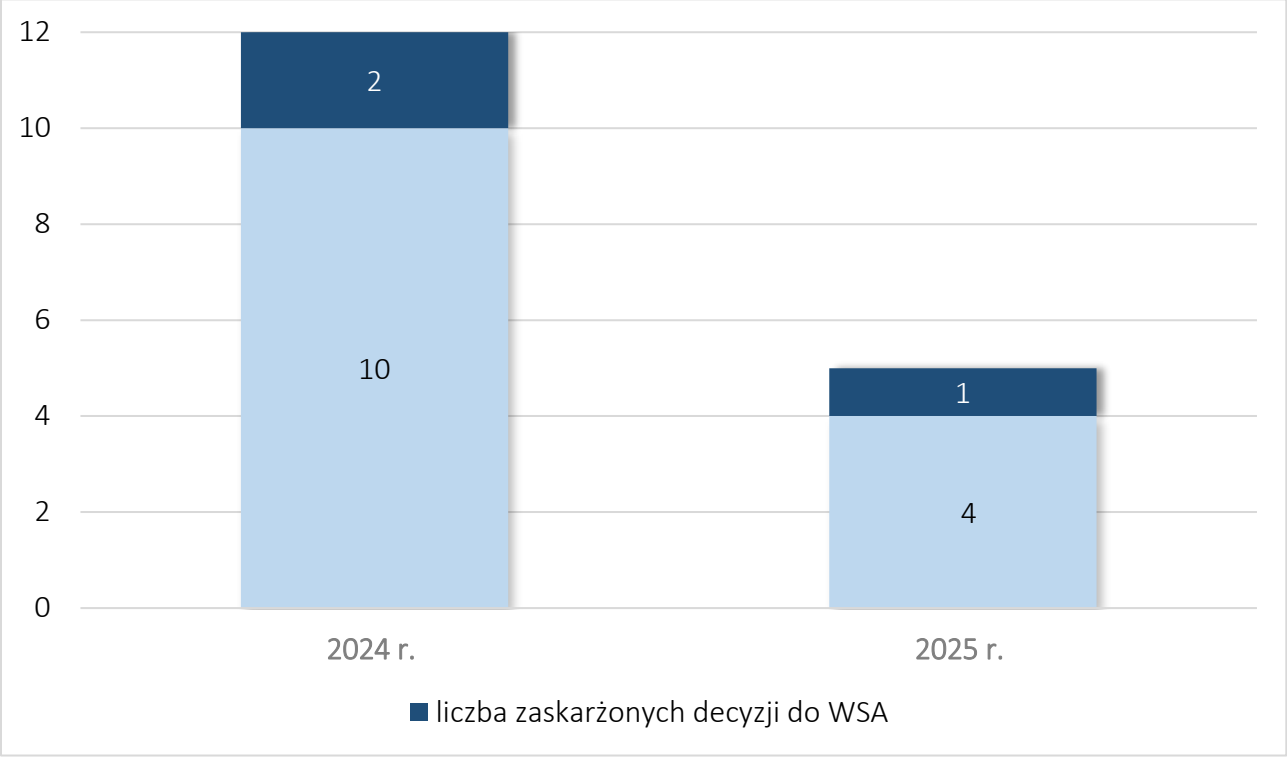

**Wykres 19:** Liczba wniosków o dostęp do informacji publicznej, które wpłynęły do Prezesa UODO w latach 2024–2025.

**Wnioski o informację dotyczyły m.in. danych statystycznych, takich jak:** liczba postępowań, liczba zgłoszonych skarg i naruszeń ochrony danych osobowych, liczba zawiadomień[589] 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, planu kontroli sektorowych 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 jedynie 4 decyzje o odmowie udostępnienia informacji publicznej. **Należy podkreślić, że tylko jedna (1) z powyższych decyzji została zaskarżona do Wojewódzkiego Sądu Administracyjnego w Warszawie. Po wniesieniu przez stronę skarżącą skargi kasacyjnej, Naczelny Sąd Administracyjny oddalił przedmiotową skargę, podzielając stanowisko organu.**




**Wykres 20:** Liczba decyzji wydanych przez Prezesa UODO w sprawie wniosków o dostęp do informacji publicznej w latach 2024–2025.

[589] Art. 94 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Udzielono także **50 informacji poza trybem udostępniania informacji publicznej**. Najczęściej były to pytania w zakresie współpracy z organami ścigania.

### 18.5. Skargi na działanie UODO

W 2025 r. udzielono odpowiedzi na **19 skarg na działanie Urzędu**. Skarżący najczęściej skarżyli się na zaniedbania lub nienależyte wykonywanie zadań przez Urząd albo przez jego pracowników, naruszenie praworządności lub interesów skarżących, a także na przewlekłość lub biurokratyczne załatwianie spraw. Skargi te były wyrazem niezadowolenia skarżących z rozstrzygnięć prowadzonych postępowań w UODO. W wyniku przeprowadzonych postępowań wyjaśniających dotyczących tych skarg, nie stwierdzono zasadności żadnej z nich.

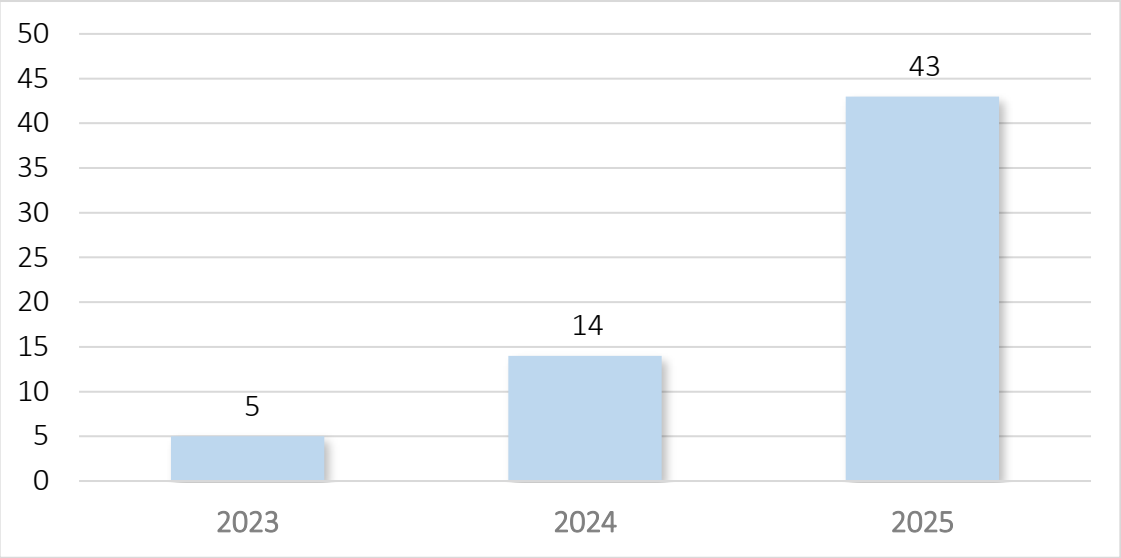
Wszystkie skargi z działu VIII K.p.a. zostały rozpatrzone w terminie przewidzianym w ustawie. Trzy skargi zostały przekazywane zgodnie z właściwością na podstawie art. 234 K.p.a. do rozpatrzenia w toku prowadzonych postępowań.

## 19. Wystąpienia Prezesa UODO

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 2025 roku Prezes UODO wystosował ogółem **43 wystąpienia** z określonymi wnioskami do różnych podmiotów: 35 wystąpień w sprawach skargowych, 8 w sprawach kontroli i naruszeń. Dla porównania w 2024 r. było ich 14.




**Wykres 21:** Liczba wystąpień Prezesa UODO skierowanych do różnych podmiotów w latach 2023–2025.

Impulsem do ich skierowania były zarówno własne analizy organu nadzorczego dokonywane w toku opiniowania aktów prawnych czy podczas oceny wpływu wyroków TSUE na przepisy prawa krajowego lub sposób ich interpretacji, ale także sygnały od inspektorów ochrony danych (IOD).

Zakres tematyczny wystąpień był bardzo różnorodny. Odnosiły się one m.in. do takich kwestii, jak:

- monitoring wizyjny w placówkach oświatowych[590]
- ujawnianie danych w związku z dotacjami dla związków sportowych[591],
- umieszczanie i przechowywanie odcisków palców w dowodach osobistych[592],
- wprowadzenie przepisów umożliwiających uzyskanie przez podmioty medyczne stosujące kodeksy postępowania albo posiadające certyfikaty w rozumieniu RODO dodatkowych punktów przy kontraktowaniu usług z NFZ[593];
- możliwość pozyskiwania przez przewoźników informacji o czasie pracy zatrudnianych maszynistów, którzy złożyli oświadczenie o zatrudnieniu u innego przewoźnika[594],
- ustawowe uregulowanie zakresu danych osobowych przetwarzanych na potrzeby realizacji programu ochrony powietrza[595],

[590] DPNT.413.21.2025; opisane i opublikowane na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3806.
[591] DPNT.413.4.2025; opisane i opublikowane na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3535.
[592] DPNT.413.8.2025.
[593] DPNT.413.22.2025; informacja w tej sprawie oraz treść pisma dostępne na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/138/3823.
[594] DPNT.413.36.2025.
[595] DPNT.413.6.2025; opisane i opublikowane na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3817.

- zapewnienie zgodności przetwarzania danych osobowych z przepisami prawa ochrony danych w rozgłośni regionalnej[596],
- zapobiegania występowaniu incydentów przy doręczaniu przesyłek pocztowych[597],
- zatrzymania dokumentacji medycznej zawierającej dane wrażliwe pacjentek[598],
- nieuprawnionego korzystania z bazy PESEL przez funkcjonariuszy Straży Granicznej[599],
- zagubienia bloczków mandatowych i notatników służbowych zawierających dane osobowe przez funkcjonariuszy policji[600],
- nieprawidłowości dotyczących zabezpieczenia danych osobowych na zewnętrznych nośnikach danych przez Państwową Inspekcję Sanitarną[601].

Poniżej opisane zostały najważniejsze wystąpienia

Jednym z zasadniczych problemów dostrzeganych w pracach opiniodawczych Prezesa Urzędu Ochrony Danych Osobowych jest brak przeprowadzania przez projektodawców (w zasadniczej większości rządowych procesów legislacyjnych) testu prywatności na etapie procesu legislacyjnego, jako elementu oceny skutków regulacji. W **wystąpieniu z 14 lutego 2025 r. skierowanym do Przewodniczącego Komitetu Stałego Rady Ministrów organ nadzorczy zwrócił się o podjęcie działań legislacyjnych mających na celu uzupełnienie Regulaminu pracy Rady Ministrów w zakresie obowiązku sporządzenia OSR prywatności do projektowanych aktów normatywnych**[602]. W ocenie Prezesa UODO wprowadzenie takiego wymogu prawnego przyczyniłoby się do zapewnienia zgodności z przepisami prawa UE odnoszącymi się do ochrony danych osobowych, ale przede wszystkim wymogów wynikających z Konstytucji RP. Przeprowadzenie testu prywatności byłoby szczególnie istotne zwłaszcza dla przypadków ekstensywnych systemów państwowych, rejestrów publicznych czy projektów integracji danych, ze względu na kontekst czy charakter przetwarzania, jego zakres, cele, zastosowane technologie oraz z uwagi na wysokie ryzyka naruszenia praw lub wolności osób, których dane będą przetwarzane. W wymiarze funkcjonalnym test prywatności pozwoliłby projektodawcom na tworzenie rozwiązań, narzędzi i systemów wyposażonych w konkretne środki organizacyjno-techniczne zapewniające bezpieczeństwo czy cyberbezpieczeństwo danych już na poziomie normatywnym. Przyjmowanie rozwiązań kompleksowych, zwłaszcza we wskazanych newralgicznych aspektach związanych z infrastrukturą krytyczną, eliminowałoby w znacznej mierze przerzucanie obowiązku ich wprowadzenia na administratorów lub użytkowników, co jest istotne

[596] DKN.5101.42.2025, DKN.5101.147.2025, DKN.219.2025.
[597] DKN.5101.47.2024.
[598] DKN.5101.55.2023.
[599] DKN.5101.485.2024.
[600] DKN.5101.66.2024.
[601] DKN.5101.414.2025.
[602] DOL.413.15.2024.

zwłaszcza w odniesieniu do nakładania praw i obowiązków na podmioty publiczne związane zasadą legalizmu, tj. działania na podstawie i w granicach prawa.

Pomimo że Przewodniczący KSRM nie przychylił się do postulatu uzupełnienia Regulaminu pracy Rady Ministrów o wprowadzenie obowiązku prawnego implementacji testu prywatności w OSR, to w odpowiedzi na wystąpienie podzielił stanowisko prezentowane przez organ nadzorczy, zgodnie z którym ocena skutków dla ochrony danych osobowych, jako element poprzedzający opracowanie projektu aktu normatywnego, jak również weryfikacja proporcjonalności planowanych rozwiązań prawnych dotyczących danych osobowych, są elementami niezbędnymi w procesie legislacyjnym, a ich przeprowadzenie stanowi obowiązek projektodawcy – wiążący wobec projektodawców bez względu na treść Regulaminu pracy Rady Ministrów. Pomimo nieprzyjęcia postulowanych zmian w Regulaminie na obecnym etapie, w przyszłości wzięta zostanie pod uwagę koncepcja jego zmiany, a do tego czasu podjęte zostaną inne, nie mniej skuteczne środki, mające na celu zwiększenie świadomości projektodawców w zakresie zapewnienia zgodności regulacji krajowych z RODO.

Inne ważne wystąpienie Prezesa UODO dotyczyło **ustawy o doręczeniach elektronicznych**[603]. Pierwotny jej projekt wprowadzający model e-doręczeń nie został przedłożony organowi nadzorczemu do zaopiniowania. Natomiast liczne sygnały wskazujące na wątpliwości dotyczące stosowania przyjętych przepisów były impulsem do skierowania do resortu cyfryzacji – pod koniec 2024 roku – wystąpienia z wnioskiem o stosowną nowelizację ustawy.

W 2025 r. prowadzona zaś była dalsza korespondencja z Ministrem Cyfryzacji w sprawie aktualnego stanu prac nad zmianą modelu dostępu do danych osobowych w związku z realizacją systemu e-doręczeń. Prezes UODO wskazywał, że funkcjonowanie systemu e-doręczeń w sposób, który eliminował będzie zagrożenia dla osób, których dane dotyczą, ma pierwszorzędne znaczenie z punktu widzenia zachowania ich prawa do prywatności.

Jedna z głównych uwag organu była związana z wykorzystywaniem przez pracownika korzystającego ze skrzynki e-doręczeń prywatnych narzędzi do celów służbowych (prywatnego profilu mObywatel, profilu zaufanego oraz osobistej bankowości elektronicznej). To powoduje, że w dowodzie wpływu korespondencji do danego organu, nadawca korespondencji otrzymuje nie tylko informacje identyfikujące adresata, czyli ten organ, ale także dane osobowe administratora konta – osoby fizycznej, która stworzyła dla organu skrzynkę do e-doręczeń. Oprócz imienia i nazwiska dowód e-doręczenia zawiera także numer PESEL tej osoby, którą – w przypadku organu – jest np. pracownik działu IT (który nie jest w żaden sposób zaangażowany w proces odbioru korespondencji). W korespondencji z resortem organ nadzorczy dopytywał, czy prowadzone są prace nad zmianą modelu dostępu do danych osobowych w związku z realizacją e-doręczeń celem dostosowania do zasad ochrony danych osobowych.

[603] DOL.413.7.2024.

22 sierpnia 2025 r. do Prezesa UODO wpłynął do zaopiniowania projekt ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD 236). Nie zawierał on jednak rozwiązań, na które wskazywał organ nadzorczy[604].

W 2025 roku **do Ministra Cyfryzacji** Prezes UODO skierował też **wystąpienie** w innej bardzo ważnej i wymagającej pilnego rozwiązania kwestii, tj. **wprowadzenia rozwiązań ustawowych, które zapewnią (zwłaszcza osobom fizycznym) skuteczną ochronę przed negatywnym wpływem deepfake'ów**[605].

Uzasadnieniem do jego przygotowania były zgłaszane Prezesowi UODO przypadki nadużyć spowodowanych stosowaniem technologii deepfake (w tym dotyczące osób małoletnich), a także analiza aktualnych regulacji prawnych, która uwidoczniła potrzebę pilnego przyjęcia przepisów przeciwdziałających szkodliwemu wykorzystaniu tej technologii.

W wystąpieniu Prezes UODO podkreślił, że postęp technologiczny, w tym rozwój sztucznej inteligencji, musi uwzględniać prawa i bezpieczeństwo obywateli oraz odpowiedzialność instytucji publicznych oraz prywatnych w budowaniu zaufania i odporności społecznej.

Organ nadzorczy wskazał, że technologia deepfake pozwala tworzyć nagrania, wideo i audio, które wydają się autentyczne, choć takimi nie są, i choć sama technologia jest neutralna i może służyć do tworzenia np. efektów specjalnych w filmach, to jednak może też prowadzić do nadużyć, w tym naruszania praw i wolności ludzi na niespotykaną dotychczas skalę. Wśród zagrożeń, jakie niesie ze sobą technologia deepfake, Prezes UODO wymienił wykorzystywanie wizerunku danej osoby bez jej wiedzy i zgody oraz kradzież tożsamości (ułatwia podszywanie się pod inne osoby). Technologia ta może posłużyć także do szantażu i nękania, gdyż umożliwia ukazanie osoby w sytuacjach, które w rzeczywistości nie miały miejsca. Prezes UODO zwrócił uwagę, że deepfake'i mogą posłużyć również do preparowania dowodów sądowych oraz stanowić zagrożenie dla bezpieczeństwa narodowego lub bezpieczeństwa systemów informacji podmiotów publicznych i prywatnych. Deepfake może być wykorzystywany do manipulacji politycznej (w szczególności podczas prowadzenia kampanii wyborczych), polaryzacji społecznej, zamieszek czy konfliktów. Innym przykładem może być omijanie systemów bezpieczeństwa, takich jak systemy uwierzytelniania biometrycznego.

Prezes UODO przywołał też przypadki dotychczas zgłaszanych mu nadużyć spowodowanych stosowaniem technologii deepfake. Były to:

- sprawa skargowa dotycząca zamieszczania na portalach społecznościowych fałszywych informacji odnoszących się do dziennikarki, osoby aktywnej publicznie – o jej śmierci, o tym, że została pobita przez męża oraz że trafiła do więzienia. W tej sprawie Prezes UODO wydał na podstawie RODO zakaz

[604] Opinia Prezesa UODO (DPNT.401.325.2025) została opisana w części „Opiniowanie projektów aktów prawnych dotyczących ochrony danych osobowych".
[605] DPNT.413.31.2025. Więcej informacji znaleźć można w materiałach dostępnych na stronie internetowej UODO pod linkami: https://uodo.gov.pl/pl/138/3886, https://uodo.gov.pl/pl/138/4061.

przetwarzania danych na 3 miesiące (maksymalny termin przewidziany prawem), postępowanie w tej sprawie prowadzi irlandzki organ nadzorczy,

- sprawa wygenerowania przez uczniów szkoły podstawowej fałszywego zdjęcia nagiej koleżanki.[606] W tej sprawie Prezes UODO zawiadomił Policję o możliwości popełnienia przestępstwa, jednak Policja odmówiła zajęcia się sprawą. Prezes UODO zmuszony był interweniować w tej sprawie u Prokuratora Generalnego,
- sygnały od lekarzy, którzy padli ofiarą oszustów korzystających z echnologii deepfake. Ich wizerunki i autorytet zostały wykorzystane w nieprawdziwych reklamach, w których medycy rzekomo zachęcali do przyjmowania określonych preparatów.

Prezes UODO zaznaczył, że aktualne regulacje prawne (krajowe i unijne) nie zapewniają narzędzi do pełnej i skutecznej ochrony przed skutkami takich nadużyć, np. poprzez szybkie usuwanie nielegalnych materiałów. Wskazał ponadto, że walka z tego typu zagrożeniami wymaga dostosowania przepisów do specyfiki technologii deepfake oraz ścisłej współpracy organów odpowiedzialnych za prawodawstwo oraz nadzór nad sztuczną inteligencją zarówno na poziomie krajowym, jak i międzynarodowym.

Organ nadzorczy zwrócił również uwagę, że niektóre państwa członkowskie (np. Dania, Belgia, Niderlandy czy Francja) we własnym zakresie podejmują próby dostosowywania prawa do szybko zmieniającej się rzeczywistości technologicznej, w tym w zakresie deepfake.

W ocenie Prezesa UODO również w polskim porządku prawnym niezbędne jest wprowadzenie przepisów prawa, które będą bezpośrednio odnosić się do rozpowszechniania szkodliwych treści w postaci deepfake'ów, zapewniając ofiarom możliwość skutecznego i szybkiego dochodzenia ochrony swoich praw.

Obecnie prawo polskie nie odnosi się wprost do specyfiki nowoczesnej technologii w tym zakresie. Przeciwdziałanie specyficznym zagrożeniom powodowanym przez deepfake'i wymaga opracowania szczegółowych zasad ponoszenia odpowiedzialności karnej i odszkodowawczej osób tworzących i rozpowszechniających szkodliwe deepfake'i, a także doprecyzowania obowiązków podmiotów administrujących platformami internetowymi. Celem zmian powinno być stworzenie bezpieczniejszego i bardziej przejrzystego środowiska cyfrowego.

Dlatego organ nadzorczy wystąpił do Ministra Cyfryzacji o zainicjowanie prac, których celem będzie wprowadzenie w polskim porządku prawnym przepisów, które będą regulować odpowiedzialność prawną za rozpowszechnianie fałszywych treści w postaci deepfake'ów, a także zapewnią skuteczną ochronę danych osobowych.

W przesłanej 15 grudnia 2025 r. odpowiedzi na to wystąpienie Minister Cyfryzacji przedstawił działania, które w jego ocenie mogą służyć przeciwdziałaniu temu zjawisku. Jako ich przykład wskazał procedowaną nowelizację ustawy o świadczeniu usług drogą elektroniczną, mającą na celu umożliwienie stosowania przepisów

[606]Więcej informacji o tej sprawie można należć na stronie internetowej UODO pod linkami: https://uodo.gov.pl/pl/138/3727, https://uodo.gov.pl/pl/138/3984.

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).

W ocenie Prezesa UODO wskazane przez Ministra Cyfryzacji działania nie zapewniają jednak narzędzi do pełnej i skutecznej ochrony przed konsekwencjami nadużyć związanych z korzystaniem technologii umożliwiających generowanie deepfake. Umożliwią jedynie fragmentaryczną i niewystarczającą odpowiedź na te zagrożenia. Dlatego konieczne jest dokonania przeglądu dotychczas proponowanych rozwiązań i wypracowania bardziej spójnych ram prawnych zapewniających realną i skuteczną ochronę przed nadużyciami dokonanymi przy pomocy tej technologii, przede wszystkim poprzez wprowadzenie instrumentów szybkiego reagowania na takie przypadki oraz realną ochronę prawno-karną odnoszącą się wprost do zagrożeń wynikających ze stosowania deepfake'ów.

Z powyższych powodów Prezes UODO podtrzymał swoje stanowisko, że **niezbędne jest wprowadzenie przepisów prawa, które będą dostosowane do specyfiki technologii deepfake oraz będą bezpośrednio odnosić się do rozpowszechniania szkodliwych treści wytworzonych przy pomocy takich technologii**[607]**.**

**W wystąpieniu do Ministra Infrastruktury** Prezes UODO zwrócił się z wnioskiem o podjęcie działań mających na celu zapewnienie skutecznego stosowania przepisów o ochronie danych osobowych w związku z wykorzystywaniem kamer nasobnych przez kontrolerów biletów w środkach transportu publicznego[608]. Zauważając tendencję do wprowadzania przez różne podmioty odpowiedzialne za miejski transport publiczny monitoringu wizyjnego w postaci kamer nasobnych kontrolerów biletów, organ nadzorczy zwrócił uwagę na poważne wątpliwości pod względem dopuszczalności, zasadności, legalności i celowości wykorzystywania tego rodzaju urządzeń audio-wideo przez osoby upoważnione do kontroli dokumentów przewozu (biletów). Zasadniczo każdy rodzaj monitoringu wizyjnego stanowi wyjątkowo inwazyjną formę przetwarzania danych osobowych – w szczególności monitoring w formie kamer nasobnych, które wiążą się nie tylko z rejestrowaniem obrazu, ale także z nagrywaniem dźwięku. Instrumenty wykorzystywane w celu zapewnienia bezpieczeństwa – takie jak monitoring wizyjny – w swojej istocie głęboko ingerują w sferę konstytucyjnych praw jednostki, w tym przede wszystkim prawa do prywatności oraz prawa do autonomii informacyjnej. Dlatego też, zgodnie z prawem konstytucyjnym, muszą opierać się na przejrzystej i konkretnie określonej podstawie prawnej rangi ustawowej, przy jednoczesnym określeniu warunków zapewniających proporcjonalność i niezbędność stosowanych środków, a także gwarancje ochrony praw obywateli, które mogą zostać w konsekwencji ich stosowania naruszone. Także z przepisów rozporządzenia 2016/679 wynika wymóg jasno określonej, zgodnej

[607] Odpowiedź Prezesa UODO z 19 stycznia 2026 r. na pismo Ministra Cyfryzacji z 15 grudnia 2025 r. Więcej informacji na ten temat znajduje się na stronie internetowej UODO pod linkiem: https://uodo.gov.pl/pl/138/4061.
[608] DPNT.413.14.2025.

z porządkiem konstytucyjnym państwa członkowskiego podstawy prawnej przetwarzania, obejmującej stosowne elementy regulacji, zwłaszcza cel przetwarzania danych osobowych. Tymczasem przepisy ustawy Prawo przewozowe czy ustawy o publicznym transporcie zbiorowym nie zawierają norm prawnych, które w ocenie Prezesa UODO, mogłyby zostać uznane za wyczerpującą, zgodną z wymogami podstawę legalizującą przetwarzanie danych osobowych poprzez stosowanie kamer nasobnych w toku kontroli biletów i dokumentów przewozu.

W odpowiedzi na wystąpienie Minister Infrastruktury podzielił stanowisko Prezesa UODO, że przepisy ustawowe nie dają przewoźnikowi, organizatorowi publicznego transportu zbiorowego albo osobom przez nich upoważnionym do kontroli dokumentów przewozu uprawień do stosowania kamer nasobnych podczas dokonywania kontroli. Jednocześnie wskazał, że ze względu na konieczność zadbania o prawa pasażerów do zachowania prywatności i ochrony wizerunku nie podjął decyzji o wprowadzeniu uprawienia dla przewoźnika lub operatora do stosowania monitoringu audiowizualnego podczas kontroli[609].

Przepisy prawa powinny być regularnie oceniane i uaktualniane pod względem zmieniających się wyzwań oraz nowych zagrożeń w perspektywie ochrony danych osobowych wynikających z postępu technologicznego. Na ten aspekt organ nadzorczy zwrócił uwagę **w wystąpieniu skierowanym do Ministra Finansów i Gospodarki, wnioskując o podjęcie działań legislacyjnych mających na celu rewizję funkcjonującego obecnie modelu powszechnej dostępności danych osobowych osób fizycznych będących przedsiębiorcami zamieszczonych w Centralnej Ewidencji i Informacji o Działalności Gospodarczej**[610]. CEIDG stanowi zbiór wyjątkowo zróżnicowany co do rodzajów podmiotów, które podlegają obowiązkowi wpisu do rejestru. Obecnie funkcjonujący model nie różnicuje natomiast obowiązku wpisu ze względu na charakterystykę wykonywanej działalności, jej skalę czy rodzaj. Zakłada jednocześnie powszechną i obligatoryjną jawność danych wszystkich ewidencjonowanych przedsiębiorców. Funkcjonujący model nie uległ zasadniczym zmianom od początku funkcjonowania rejestru, a więc od 2011 roku. Tymczasem szybkiemu postępowi technologicznemu towarzyszy nieustanny rozwój procesów i metod przetwarzania danych osobowych. Pojawiły się nowe ryzyka związane z wykorzystywaniem danych osobowych pobieranych z CEIDG niezgodnie z ich pierwotnym przeznaczeniem. Narastają tendencje do podejmowania prób zautomatyzowanego pobierania danych z publicznych rejestrów (tzw. scrapingu), w celu łączenia ich z innymi danymi, profilowania, śledzenia czy też dalszego wykorzystywania w różnych zamiarach, także z zastosowaniem algorytmów sztucznej inteligencji. W przypadku wielu przedsiębiorców adres prowadzenia działalności gospodarczej jest jednocześnie adresem zamieszkania lub stałego pobytu – mieszkaniem albo domem rodzinnym. Ta okoliczność powoduje szereg zagrożeń dla

[609] Sprawa została opisana na stronie internetowej UODO w tekście dostępnym pod linkiem https://uodo.gov.pl/pl/138/4140.
[610] DPNT.413.32.2025; opisane i zamieszczone na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3841.

możliwości prowadzenia w sposób niezakłócony życia prywatnego i rodzinnego, począwszy od kierowania natarczywego marketingu, przez profilowanie, rozpowszechnianie informacji w sieci, po nachodzenie, szykanowanie, a w niektórych przypadkach kierowanie gróźb, zniewag, uporczywe nękanie, kradzieże tożsamości czy inne działania przestępcze. Zagrożenia te pozostają szczególnie istotne w przypadku przedsiębiorców, którzy ze względu na rodzaj prowadzonej działalności lub piastowanie określonych funkcji społecznych mogą być szczególnie narażani na niebezpieczne zachowania, jak np. lekarze, psycholodzy, publicyści, mediatorzy, audytorzy, księgowi, pośrednicy nieruchomości, terapeuci i inni. Prezes UODO poddał pod rozwagę implementację mechanizmu ograniczenia powszechności dostępu do danych adresowych małych i mikro przedsiębiorców, w przypadku gdy adres prowadzenia działalności jest jednocześnie miejscem zamieszkania, np. poprzez wprowadzenie możliwości zastrzeżenia danych, wprowadzenie dobrowolności ich ujawniania w bazie czy poprzez wprowadzenie trybu wnioskowego dostępu do danych adresowych – ograniczenia dostępu jedynie do podmiotów formalnie występujących o udostępnienie danych.

W reakcji na skierowane wystąpienie Minister Finansów i Gospodarki przeprowadził pogłębioną analizę, zwracając się do szerokiego grona podmiotów, w tym organów administracji publicznej, podmiotów reprezentujących obywateli (konsumentów) oraz organizacji przedsiębiorców. Z przedstawionych opinii wynika, że przyjęty w ustawie CEIDG model dostępności danych osobowych osób fizycznych będących przedsiębiorcami zamieszczonych w CEIDG nie powinien być istotnie zmieniany. Jednocześnie wyrażono jednak gotowość do rozważenia podjęcia innych działań zmierzających do ograniczenia ryzyk związanych z publikowaniem w CEIDG adresów będących jednocześnie adresami zamieszkania przedsiębiorców.

Odpowiadając na apele środowisk lekarskich, w których wyrażano szereg obaw o bezpieczeństwo osób wykonujących zawody medyczne w związku z narastającymi aktami agresji i przemocy, Prezes UODO skierował **wystąpienie do Minister Zdrowia z wnioskiem o podjęcie działań legislacyjnych ukierunkowanych na zmianę obecnie funkcjonującego modelu pełnej jawności dostępu do danych osobowych osób objętych obowiązkiem wpisu do Rejestru Podmiotów Wykonujących Działalność Leczniczą**[611]. Nie kwestionując racjonalnych celów funkcjonowania RPWDL jako systemu sprawowania społecznej kontroli, zapewnienia przejrzystości sektora medycznego, umożliwienia weryfikacji przez pacjentów osób wykonujących działalność leczniczą, Prezes UODO zwrócił uwagę, że osoby te – bez względu na wpis do RPWDL – pozostają pod ochroną prawną przewidzianą nie tylko przez Konstytucję RP, ale także przez rozporządzenie 2016/679. RPWDL jest ogólnodostępny – każda osoba, bez konieczności wykazywania interesu prawnego czy choćby faktycznego może uzyskać bezpośredni wgląd do ksiąg rejestrowych podmiotów leczniczych i praktyk zawodowych. Tymczasem dane korespondencyjne osób świadczących praktykę zawodową albo zarejestrowanych jako podmioty

[611] DPNT.413.37.2025; opisane i dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3882.

lecznicze w wielu przypadkach są tożsame z ich prywatnym adresem zamieszkania. W przypadku osób udzielających świadczeń zdrowotnych w miejscu zamieszkania, ujawnienie tych danych w rejestrze skutkuje upublicznieniem prywatnych danych adresowych, co wiąże się z szeregiem istotnych zagrożeń dla możliwości prowadzenia niezakłóconego życia prywatnego i rodzinnego. Zagrożenia te mogą przyjmować różną postać i skalę, począwszy od kierowania spamu lub uciążliwego marketingu, przez powielanie i rozpowszechnianie informacji w internecie, po czyny zabronione, jak uporczywe nękanie, kierowanie gróźb, zniewag, pomówienia, kradzieże tożsamości, na aktach przemocy i bezpośrednich zamachach na życie i zdrowie kończąc. Ze względu na charakterystykę prowadzonej działalności lekarze, pielęgniarki, fizjoterapeuci i inne osoby zobligowane do wpisu w rejestrze stanowią grupę zawodową szczególnie narażoną na wyżej wymienione zachowania bezprawne. Organ nadzorczy zaproponował wprowadzenie rozwiązań pozwalających na częściowe ograniczenie dostępu do danych osobowych osób fizycznych podlegających wpisowi do RPWDL poprzez udostępnianie ich jedynie w przypadkach określonych w ustawie oraz w trybie wnioskowym, np. na żądanie pacjenta.

Minister Zdrowia nie przychylił się do zaproponowanych zmian przepisów dotyczących funkcjonowania RPWDL.

Doświadczenia w obszarze opiniowania projektów informatycznych, a także aktów prawnych wprowadzających nowe rozwiązania w ramach transformacji cyfrowej państwa miały duży wpływ na przygotowanie i skierowanie do Ministra Cyfryzacji komplementarnego **wystąpienia dotyczącego konieczności przeglądu przepisów prawa regulujących przetwarzanie danych osobowych w rejestrach publicznych**[612], w którym organ wskazał na konieczność stanowienia odpowiednich rozwiązań mających zapewnić bezpieczeństwo i zgodność z prawem przetwarzania danych osobowych w rejestrach publicznych.

Organ nadzorczy zwrócił uwagę na problemy dotyczące wszystkich rejestrów publicznych: identyfikację i właściwe przypisanie ról w procesach przetwarzania danych podmiotów prowadzących rejestry; ocenę zakresu danych osobowych zawartych w rejestrach publicznych pod kątem ich faktycznej niezbędności; ocenę roli podmiotów i organów zaangażowanych w przetwarzanie danych osobowych w rejestrach publicznych, w tym sposobu zasilania rejestrów i zasad eksploatacji danych; ocenę przyjętego modelu jawności danych zgromadzonych w rejestrach publicznych, zwłaszcza w aspekcie upubliczniania numeru PESEL; ocenę przyjętych w niektórych rejestrach publicznych rozwiązań dotyczących dostępu do danych, ich wymiany, wykorzystywania przez innych administratorów i tzw. teletransmisji; ocenę wpływu aktów prawa Unii Europejskiej na rejestry publiczne.

Podkreślił także, że przy projektowaniu i kształtowaniu treści przepisów, a także sposobów przetwarzania danych nie mniej istotne są m.in: przygotowywanie oceny skutków dla ochrony danych na etapie projektowania rejestrów publicznych; uwzględnianie ochrony danych oraz domyślna ochrona danych w fazie projektowania

[612] DOL.413.11.2024; opisane i zamieszczone na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3968.

rejestrów; doprecyzowywanie zasad retencji danych; ustalenia dotyczące zautomatyzowanego podejmowanie decyzji, w tym profilowania oraz wykorzystania sztucznej inteligencji; zapewnienie bezpieczeństwa, prawidłowości, poufności i integralności danych osobowych w czasie użytkowania rejestrów publicznych, w tym w sytuacjach zagrożenia bezpieczeństwa państwa.

Przetwarzania danych osobowych w obszarze ochrony zdrowia dotyczyło **wystąpienie do Ministra Zdrowia z wnioskiem o podjęcie właściwych działań legislacyjnych w kierunku określenia właściwej podstawy prawnej dla udostępnienia danych medycznych w formacie spseudonimizowanym**[613]. Zwrócono uwagę na konieczność dostosowania aktualnych regulacji do przepisów dotyczących Europejskiej Przestrzeni Danych o Zdrowiu (EHDS) , które umożliwiają, w sytuacjach wyraźnie uzasadnionych oraz niezbędnych dla celów badań naukowych, przetwarzanie danych speudonimizowanych.

Prezes UODO wskazał, że w polskim systemie prawa aktualne regulacje nie przewidują rozwiązań umożliwiających przetwarzanie danych osobowych zawartych w dokumentacji medycznej do wtórnego ich wykorzystania w celach naukowych. Warunki udostępniania dokumentacji medycznej zostały określone w art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Zgodnie z tym przepisem udostępnienie dokumentacji medycznej szkole wyższej lub instytutowi badawczemu w celach naukowych może nastąpić „bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy". Nie jest zatem dopuszczalne udostępnienie danych osobowych zawartych w dokumentacji medycznej w sposób umożliwiający ustalenie tożsamości osoby, której ta dokumentacja dotyczy, a udostępnienie to może nastąpić to w celach naukowych i badawczych pod warunkiem dokonania anonimizacji danych osobowych w tej dokumentacji zawartych.

Prezes UODO podkreślał, że zgodnie z RODO przetwarzanie danych osobowych w celach naukowych wiąże się z koniecznością zagwarantowania ochrony praw i wolności osoby, której dane dotyczą. Wprowadzenie takich zabezpieczeń – jak wynika z art. 89 ust. 1 RODO – „polega na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikowanie osoby, której dane dotyczą, cele należy realizować w ten sposób".

W odpowiedzi na wystąpienie Prezesa UODO resort zdrowia poinformował o otwartości na współpracę z Urzędem w zakresie identyfikacji wszystkich przepisów wymagających zmiany tak, aby wdrożenie EHDS odbyło się z pełnym poszanowaniem praw pacjentów i z zachowaniem najwyższych standardów ochrony danych osobowych. Jednocześnie wskazano, że Ministerstwo Zdrowia jest na wstępnym etapie prac nad wdrażaniem rozporządzenia EHDS.

[613] DPNT.413.39.2025; opisane i zamieszczone na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3880.

W związku z sygnałami dotyczącymi podjęcia prac nad wprowadzeniem rozwiązań w zakresie stosowania urządzeń monitorujących pracę ratowników medycznych, Prezes UODO przedstawiał informacje i sugestie w celu **zapewnienia skutecznej ochrony danych osobowych w trakcie wypracowywania rozwiązań prawnych dotyczących zastosowania kamer nasobnych podczas wykonywania pracy przez ratowników medycznych**[614].

Prezes UODO podkreślał, że przetwarzanie danych w ramach interwencji ratunkowych może wiązać się z sytuacjami o szczególnie wrażliwym charakterze. Nakaz poszanowania godności i intymności pacjenta wynika zaś z przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz z art. 30 Konstytucji RP. Jednocześnie system monitoringu wizyjnego stanowi istotną ingerencję w prawa i wolności nie tylko osób poddawanych takiemu monitoringowi (wśród których znajdować się mogą również osoby trzecie), ale także może dotyczyć przetwarzania danych objętych tajemnicą lekarską oraz prowadzić do istotnej ingerencji w prawa i wolności ratowników medycznych wynikające z regulacji dotyczących praw określonych w Kodeksie pracy. Przy wprowadzaniu rozwiązań prawnych w tym obszarze należy zatem dokonać odpowiedniego wyważenia praw i interesów, tj. interesu publicznego z jednej strony oraz prawa do ochrony danych osobowych oraz prawa do prywatności osób fizycznych, z drugiej strony. W konsekwencji takiej oceny projektodawca powinien wykazać, dlaczego ingerencji w prawo do prywatności, prawo do autonomii informacyjnej lub inne prawo jednostki, nie można uniknąć, i czy taka ingerencja rzeczywiście jest niezbędna, a nie jedynie potencjalnie przydatna.

Ponadto, z punktu widzenia przepisów RODO, przyjmowane rozwiązania prawne powinny uwzględniać zasady przetwarzania danych osobowych, o których mowa w art. 5 tego aktu prawnego. Należy również pamiętać, że monitoring wizyjny może być wprowadzany wyłącznie wtedy, kiedy inne, mniej inwazyjne, metody zapewniania bezpieczeństwa pacjentom i pracownikom medycznym są niewystarczające. Konieczne jest także zapewnienie wysokich standardów bezpieczeństwa danych w związku z wykorzystywaniem urządzeń monitorujących.

Z odpowiedzi resortu zdrowia na wystąpienie Prezesa UDO wynikało, że nie została podjęta decyzja o wprowadzeniu monitoringu wizyjnego w pracy ratowników medycznych. W razie podjęcia prac w tym zakresie MZ będzie konsultowało wprowadzane rozwiązania z Urzędem[615].

W **wystąpieniu do Ministra Zdrowia w sprawie braku regulacji prawnych dotyczących zasad i sposobu wprowadzania zmian w dokumentacji medycznej dziecka, które zostało przysposobione**[616] Prezes UODO wskazał, że brak jest przepisów, które umożliwiałyby zmianę danych osobowych dziecka zawartych w dokumentacji medycznej w związku z koniecznością uwzględnienia takich okoliczności, jak dokonanie jego przysposobienia pełnego. Co ważne, dokumentacja medyczna, stosownie do przepisów ustawy o prawach pacjenta i Rzeczniku Praw

[614] DPNT.413.13.2025.
[615] Więcej informacji na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3651.
[616] DPNT.413.42.2025; więcej w Biuletynie UODO Nr 03/2026.

Pacjenta podlega ochronie prawnej, a podmiot udzielający świadczeń zdrowotnych ma obowiązek zapewnić ochronę danych gromadzonych w dokumentacji medycznej. Szczegółowe regulacje związane z zakresem dokumentacji medycznej oraz sposobem jej prowadzenia i przetwarzania zawartych w niej danych osobowych zawierają natomiast przepisy wykonawcze wydane na podstawie art. 30 wymienionej ustawy.

Działania w tej kwestii podjął także Rzecznik Praw Dziecka, który wskazał, że potencjalna zmiana mogłaby dotyczyć przepisów wykonawczych, tj. rozporządzeń dotyczących rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez uprawnione organy.

Ministerstwo Zdrowia podjęło inicjatywę legislacyjną, przedstawiając zmiany w rozporządzeniu Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (druk MZ 1879).

W swoich wystąpieniach Prezes UODO poruszał również inne kwestie dotyczące ochrony danych osobowych dzieci. W **wystąpieniu do Ministra Cyfryzacji zwrócił się z prośbą o rozważenie podjęcia prac legislacyjnych nad zmianami przepisów ustawy o ewidencji ludności w celu umożliwienia rodzicom lub opiekunom prawnym zastrzegania numeru PESEL osoby małoletniej**[617]. Prezes UODO podniósł, że obecny kształt przepisów ustawy o ewidencji ludności pozostawia istotną lukę w ochronie danych osobowych osób małoletnich w zakresie zastrzegania numeru PESEL, którą należałoby precyzyjnie uzupełnić. Tym bardziej że np. przepisy ustawy o dokumentach paszportowych czy ustawy o dowodach osobistych przyznają rodzicom i opiekunom prawnym prawo do wnioskowania o wydanie dowodu osobistego lub paszportu, a w przypadku ich utraty lub uszkodzenia prawo do ich unieważnienia, co jest odnotowywane w odpowiednim rejestrze. Podobne rozwiązania powinny być zatem zastosowane w ustawie o ewidencji ludności w odniesieniu do rejestru zastrzeżeń numeru PESEL dla osób małoletnich. Wypracowanie przepisów zapewniających ochronę danych osób małoletnich ma bowiem szczególne znaczenie w dobie postępującej cyfryzacji oraz coraz częstszych przypadków kradzieży danych.

W odpowiedzi na wystąpienie resort cyfryzacji zadeklarował gotowość do współpracy w celu wypracowania jak najlepszych rozwiązań w powyższym obszarze.

Osobną grupę stanowią wystąpienia związane z dokonywaną przez Prezesa UODO oceną wyroków TSUE. Niektóre z nich powodują bowiem konieczność dokonania zmian w przepisach prawa krajowego, na co Prezes UODO wskazuje w korespondencji kierowanej do właściwych podmiotów.

W związku z wyrokiem TSUE dotyczącym zajęcia przez policję telefonu komórkowego i próby jego odblokowania, w ramach prowadzonego dochodzenia[618], **Prezes UODO wystąpił do MSWiA w celu dokonania zmian w przepisach krajowych, które umożliwiają uzyskanie dostępu do informacji i danych (w tym**

[617] DPNT.413.29.2025; opisane i dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3821.
[618] Wyrok TSUE z 4 października 2024 r. C-548/21 w sprawie C.G. przeciwko Bezirkshauptmannschaft Landeck.

**danych telekomunikacyjnych) w toku przeprowadzania czynności operacyjno-rozpoznawczych**[619].

Jak wskazał, przyjęty w art. 19 ustawy o Policji model stosowania kontroli operacyjnej nie spełnia standardów ochrony prawa do prywatności i prawa do ochrony danych osobowych wynikających z orzecznictwa TSUE. Przepisy te nie zapewniają właściwej kontroli sądowej, gdyż aktualnie nie ma konieczności uzasadnienia przez sąd postanowienia o zarządzeniu kontroli, co w konsekwencji powoduje, że kontrola sądowa ma charakter iluzoryczny z punktu widzenia podmiotu danych. Ponadto przepisy nie przewidują możliwości poinformowania osoby, wobec której była przeprowadzona kontrola operacyjna, a także nie zapewniają możliwości złożenia środka odwoławczego. Dodatkowe zastrzeżenia budzi również katalog przestępstw, których podejrzenie popełnienia może stanowić podstawę do przeprowadzenia kontroli operacyjnej. Przepisy ustawy o Policji były także przedmiotem oceny Europejskiego Trybunału Praw Człowieka, który wyrokiem z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce[620] orzekł o naruszeniu art. 8 EKPC, tj. prawa do poszanowania życia prywatnego, rodzinnego oraz korespondencji.

Minister Spraw Wewnętrznych i Administracji podzielił pogląd dotyczący konieczności wprowadzenia zmian w zakresie sposobu ukształtowania nadzoru nad prowadzeniem kontroli operacyjnej w polskim porządku prawnym. Wskazał przy tym na podjęte działania legislacyjne dotyczące nowelizacji przepisów wykonawczych dotyczących stosowania kontroli operacyjnej. Wprowadzone zmiany odnoszą się do formularzy stanowiących załączniki do rozporządzeń, m.in. rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie kontroli operacyjnej prowadzonej przez policję[621] w zakresie dotyczącym: określenia we wniosku policji rodzaju narzędzia, za pomocą którego będzie stosowana kontrola operacyjna; funkcjonalności ww. narzędzia; zakresu danych, które są planowane do uzyskania w ramach kontroli operacyjnej; konieczności uzasadnienia w przypadku odmowy wyrażenia zgody przez Pierwszego Zastępcę Prokuratora Generalnego Prokuratora Krajowego /Prokuratora Okręgowego; koniczności uzasadnienia postanowienia sądu w zakresie zgody lub odmowy zarządzenia/ przedłużenia/odmowy zarządzenia/przedłużenia kontroli operacyjnej. Tożsame zmiany zostały wprowadzone do innych rozporządzeń dotyczących Straży Granicznej, Służby Ochrony Państwa, Biura Nadzoru Wewnętrznego.

W związku z wyrokiem TSUE z 30 stycznia 2024 r. wydanym w sprawie C-118/22 Prezes UODO zwrócił się **do Ministra Spraw Wewnętrznych i Administracji z wystąpieniem o dokonanie zmiany w przepisach prawa regulujących funkcjonowanie Krajowego Systemu Informacyjnego Policji (dalej „KSIP")**[622]. W ocenie Prezesa UODO obowiązujące przepisy ustawy o Policji, dotyczące

[619] DPNT.413.12.2025; sprawa opisana na stronie internetowej UODO w tekście dostępnym pod linkiem https://uodo.gov.pl/pl/138/3846.
[620] Skargi nr 72038/17 i 25237/18.
[621] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 marca 2025 r. zmieniające rozporządzenie w sprawie kontroli operacyjnej prowadzonej przez Policję (Dz. U. poz. 436).
[622] DPNT.413.11.2025; opisane i zamieszczone na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3899.

prowadzenia KSIP, nie nakładają na Komendanta Głównego Policji, jako administratora danych osobowych zgromadzonych w KSIP, obowiązku okresowego przeglądu danych. Ponadto ani przepisy ustawy o Policji, ani przepisy ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości nie przewidują przesłanek usunięcia danych osobowych z KSIP. Za taki warunek nie można uznać określonej w art. 24 ust. 1 pkt 2 ww. ustawy przesłanki „naruszenia przepisów ustawy", której właściwa interpretacja jest utrudniona. Wynika to z błędnej implementacji art. 16 ust. 2 dyrektywy 2016/680 do polskiego prawa i sprawia, że osoby, których dane dotyczą, zostały pozbawione jakiegokolwiek instrumentu prawnego do skutecznego żądania usunięcia przez organy policyjne danych zgromadzonych w KSIP. Potwierdza to orzecznictwo sądów administracyjnych, z którego wynika, że przepisy ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości wymagają od administratora jedynie zgodności działania z przepisami regulującymi wykonywanie ustawowych zadań Policji i ostatecznie do Komendanta Głównego Policji należy ocena potrzeby dalszego przetwarzania danych w KSIP. Komendant Główny Policji nie jest przy tym zobowiązany do podania szczegółowych przyczyn odmowy usunięcia danych, co jest niezgodne z art. 16 ust. 4 dyrektywy 2016/680 stanowiącym, że państwa członkowskie zapewniają, by administrator informował pisemnie osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych oraz o przyczynach tej odmowy. Ustawa o Policji nie zawiera także informacji o powyższych prawach podmiotu danych, jak też o prawie do usunięcia danych, którego w szczególności dotyczy omawiany wyrok TSUE. Przepisy ustawy o Policji nie określają również zakresu przetwarzanych danych ani maksymalnych okresów ich przetwarzania, co w praktyce może prowadzić do przetwarzania danych osobowych aż do śmierci podmiotu danych.

W tych okolicznościach Prezes UODO uznał za zasadne podjęcie inicjatywy legislacyjnej mającej na celu zmianę przepisów prawa dotyczących KSIP, tak by zapewniały one ochronę danych osobowych i prawo do prywatności.

W udzielonej odpowiedzi na powyższe wystąpienie, Minister Spraw Wewnętrznych i Administracji wskazał, że obowiązujące przepisy polskiego prawa są zgodne z wymaganiami wynikającymi ze wskazanego wyroku TSUE i nie podziela stanowiska Prezesa UODO.

**Wystąpienie do ministra cyfryzacji o rozważenie podjęcia prac legislacyjnych prowadzących do zmiany przepisów ustawy - Prawo komunikacji elektronicznej**[623] w zakresie zasad dostępu organów ścigania do danych objętych tajemnicą telekomunikacyjną miało na celu konieczność zapewnienia skutecznej ochrony prawa do prywatności i prawa do ochrony danych osobowych w związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej z 30 kwietnia 2024 r. w sprawie C-470/21 *La Quadrature du Net.* Prezes UODO zwracał już uwagę na znaczenie ww. wyroku Trybunału w korespondencji z Ministrem ds. Unii Europejskiej z 11 czerwca

[623] DPNT.413.9.2025.

2024 r. Uwagi te nie zostały uwzględnione w pracach nad Prawem komunikacji elektronicznej, które zastąpiło Prawo telekomunikacyjne.

Tymczasem Trybunał w ww. wyroku wskazał, że aby można było uznać dostęp do danych objętych tajemnicą telekomunikacyjną za niezbędny i adekwatny, powinny istnieć w prawie krajowym odpowiednie gwarancje w postaci kontroli niezależnego organu mającego status osoby trzeciej w stosunku do organu ubiegającego się o dane osobowe. W demokratycznym państwie prawa zasadność pozyskania danych telekomunikacyjnych powinna być poddana kontroli sądu lub niezależnego organu administracyjnego. Kontrola przeprowadzona przez te podmioty byłaby też zgodna z zasadą pogłębiania zaufania obywateli do państwa, gdyż eliminowałaby ryzyko nieproporcjonalnej ingerencji w prawa podstawowe. Według Prezesa UODO analiza przepisów ustawy Prawo komunikacji elektronicznej przez pryzmat wyroku TSUE z 30 kwietnia 2024 r. prowadzi do wniosku, że nie odpowiadają one standardom wynikającym z art. 7, 8, 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, a ograniczenie tajemnicy komunikacji elektronicznej nie spełnia warunku wynikającego z art. 15 ust. 1 dyrektywy 2002/58 w postaci niezbędności i proporcjonalności w społeczeństwie demokratycznym. Obowiązujące przepisy, powielają niezgodny z orzecznictwem sądów europejskich model m.in. retencji i udostępniania danych telekomunikacyjnych. Tym samym wymagają dostosowania do unijnych standardów ochrony prawa do prywatności.

Na kanwie wyroku TSUE z 13 marca 2025 r. w sprawie C-247/23 Deldits, dotyczącym prawa do sprostowania danych osobowych dotyczących tożsamości płciowej osoby fizycznej, Prezes UODO zwrócił się **do Minister do spraw Równości o podjęcie działań legislacyjnych dotyczących stworzenia odrębnej procedury sądowej, której przedmiotem byłoby zapewnienie realizacji prawa do sprostowania danych osobowych dotyczących tożsamości płciowej (uzgodnienia płci)**[624].

Aktualnie obowiązujące przepisy prawa polskiego – podobnie jak prawodawstwo węgierskie analizowane w wyroku przez Trybunał – nie określają wprost procedury zmiany płci metrykalnej. W świetle orzecznictwa polskich sądów przyjmuje się, że właściwym postępowaniem w zakresie ustalenia płci jest ogólny tryb przewidziany w art. 189 Kodeksu postępowania cywilnego. Każdorazowo uzyskany w postępowaniu cywilnym prawomocny wyrok sądowy stanowi podstawę wpisania wzmianki dodatkowej w akcie urodzenia powoda (powódki) w zakresie oznaczenia jego/jej płci. Zmiany w tym obszarze przyniosła uchwała Sądu Najwyższego (w składzie pełnej Izby Cywilnej) z 4 marca 2025 roku[625]. Zgodnie z tą uchwałą żądanie zmiany oznaczenia płci w akcie urodzenia podlega rozpoznaniu przez sąd w postępowaniu nieprocesowym przy zastosowaniu w drodze analogii art. 36 ustawy z 28 listopada 2014 r. – Prawo o aktach stanu cywilnego. W tym miejscu należy jednak wskazać, że zastosowanie tej uchwały budzi poważne zastrzeżenia i wątpliwości prawne. W składzie orzeczniczym zasiadali bowiem sędziowie Sądu Najwyższego wybrani

[624] DPNT.413.20.2025.
[625] Sygn. akt III CZP 6/24.

w wadliwej procedurze, co – w świetle utrwalonego już orzecznictwa Trybunału Sprawiedliwości UE i Europejskiego Trybunału Praw Człowieka – stanowić powinno okoliczność wykluczającą branie takiego orzeczenia pod uwagę.

Po zawetowaniu przez Prezydenta RP ustawy z 10 września 2015 r. o uzgodnieniu płci, która miała na celu stworzenie odrębnej procedury sądowej umożliwiającej uznanie tożsamości płciowej jako podstawy określenia płci osób, u których występuje niezgodność między tożsamością płciową a płcią metrykalną, w następnych latach nie zostały podjęte inicjatywy legislacyjne w tym przedmiocie.

Mimo że uwaga Prezesa UODO koncentruje się na problematyce ochrony danych osobowych, to sytuacja, w której w systemie prawa nie istnieje odrębna procedura umożliwiająca potwierdzenie tożsamości płciowej w oparciu o ustawowo określone przesłanki takiego ustalenia, nie wydaje się optymalna z punktu widzenia standardów wynikających z orzecznictwa TSUE, a przede wszystkim ETPCz. Biorąc pod uwagę wyraźne wskazanie przez Trybunał Sprawiedliwości UE, że państwo członkowskie nie może w celu podważenia prawa do sprostowania danych powoływać się na szczególne przepisy prawa krajowego przyjęte na podstawie art. 6 ust. 2 i 3 RODO, a jego art. 16 może być ograniczony jedynie na warunkach określonych w art. 23, analizowany wyrok wywołuje także skutki w odniesieniu do obszarów, w których prawo krajowe odrębnie reguluje kwestie sprostowania danych lub dokumentów. Jako przykład można wskazać na przepisy rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 30 grudnia 2016 r. w sprawie świadectwa pracy, które nie odnoszą się do kwestii sprostowania danych dotyczących tożsamości płciowej (uzgodnienia płci), a tym samym w tym zakresie zastosowanie znajdzie art. 16 RODO.

Mając na uwadze całokształt przytoczonych okoliczności Prezes UODO uznał za konieczne podjęcie działań legislacyjnych w powyższym zakresie i monitoruje ich postępy.

W związku ze wskazanym wyżej wyrokiem TSUE w sprawie C-247/23 Deldits odnoszącym się do prawa do sprostowania danych osobowych dotyczących tożsamości płciowej osoby fizycznej, Prezes UODO wystąpił również **do Minister Rodziny, Pracy i Polityki Społecznej, w sprawie sprostowania danych osobowych dotyczących tożsamości płciowej (uzgodnienia płci) w świadectwie pracy**[626]. Aktualnie brak jest jakichkolwiek regulacji prawnych, które umożliwiałyby realizację prawa do sprostowania danych osobowych w zakresie tożsamości płciowej osoby fizycznej. W kontekście wyroku TSUE bezpośrednie zastosowanie w tym zakresie znajdzie więc art. 16 RODO, który przewiduje prawo do sprostowania danych osobowych. Jak podkreślił Trybunał, państwo członkowskie nie może powoływać się na brak w prawie krajowym procedury prawnego uznania tożsamości płciowej jako powód odmowy realizacji prawa do sprostowania danych.

W odpowiedzi Minister Rodziny, Pracy i Polityki Społecznej uznała zasadność zgłaszanych postulatów *de lega ferenda* odnoszących się do osób transpłciowych i potrzebę uregulowania w tym zakresie ich sytuacji na rynku pracy. Wskazała

[626] DPNT.413.24.2025; opisane i zamieszczone na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/3801.

jednocześnie, że zmiany dotyczące świadectwa pracy powinny mieć charakter kompleksowy i obejmować wszystkie wypadki zmiany danych osobowych, skutkujące koniecznością wystawienia nowego świadectwa z uwzględnieniem zmienionych danych. Jednocześnie wskazano, że rozpoczęto konsultacje robocze z Minister ds. Równości oraz przedstawicielami środowisk osób transpłciowych i z Departamentem Ubezpieczeń Społecznych MRPiPS, w zakresie katalogu informacji zamieszczanych w świadectwie pracy, w szczególności w kontekście ich niezbędności dla ustalenia uprawnień z ubezpieczeń społecznych, które to konsultacje mają poprzedzać podjęcie prac legislacyjnych w tym obszarze.

W wielu przypadkach **wystąpienia Prezesa UODO są następstwem sygnałów dotyczących problemów ze stosowaniem przepisów prawa przekazanych przez inspektorów ochrony danych**. W takich sytuacjach organ nadzorczy analizuje przekazane przez inspektorów informacje i podejmuje decyzje co do dalszych działań, np. w postaci skierowania wystąpienia do odpowiedniego resortu. 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 Prezesa UODO. Powyższe działania stanowią jeden z przejawów współpracy Prezesa UODO i inspektorów ochrony danych, służącej doskonaleniu przestrzeni prawnej związanej z przetwarzaniem danych osobowych.

W wyniku takich sygnałów od inspektorów Prezes UODO w 2025 r. przygotował poniżej przedstawione wystąpienia.

W marcu 2025 r. do Ministra Rozwoju i Technologii Prezes UODO skierował wystąpienie **o podjęcie prac legislacyjnych prowadzących do zmiany przepisów ustawy z 5 lipca 2018 r. o ułatwieniach w przygotowaniu i realizacji inwestycji mieszkaniowych oraz inwestycji towarzyszących celem dostosowania ich do zasad ochrony danych osobowych** określonych w art. 5 RODO[627]. Analiza podjęta przez organ nadzorczy w związku z sygnalizowanymi mu problemami w stosowaniu przepisów ww. ustawy w zakresie obowiązku zamieszczania w treści dokumentów numerów ksiąg wieczystych i następnie ich publikacji wskazywała na potrzebę wprowadzenia stosownych zmian legislacyjnych w celu zapewnienia skutecznej ochrony danych osobowych. Przepisy ww. ustawy, po pierwsze, wymagają, aby w treści wniosku i uchwały wskazywać nieruchomości według katastru nieruchomości oraz księgi wieczystej, a po drugie, nakładają na organy obowiązek publikacji tych dokumentów, nie zawierając przy tym rozwiązań zapobiegających publikacji danych osobowych w zakresie wykraczającym poza dane niezbędne dla osiągnięcia celu publikacji tych dokumentów, w tym w zakresie danych niezbędnych do oznaczenia nieruchomości.

Poprzez opublikowanie numerów ksiąg wieczystych, np. na stronach internetowych Biuletynu Informacji Publicznej czy w wojewódzkim dzienniku urzędowym, dostęp do zawartych w księgach informacji może uzyskać każdy zainteresowany użytkownik Internetu. Łatwy dostęp do takich danych może prowadzić

[627] DPNT.413.15.2025.

do zagrożeń dla wielu osób, m.in. do ponownego wykorzystania danych osobowych niezgodnie z pierwotnymi celami przetwarzania, nieuprawnionego profilowania właścicieli nieruchomości czy kradzieży ich tożsamości.

W odpowiedzi na powyższe wystąpienie Ministerstwo poinformowało, że w najbliższych pracach legislacyjnych zostaną znowelizowane przepisy ustawy o ułatwieniach w przygotowaniu i realizacji inwestycji mieszkaniowych oraz inwestycji towarzyszących w sposób zapewniający poszanowanie zasad ochrony danych osobowych.

Kolejny sygnał od inspektora ochrony danych wymagający interwencji organu nadzorczego w postaci wystąpienia dotyczył konieczności zmiany przepisów prawa w zakresie **likwidacji depozytów niepodjętych przez osoby osadzone w aresztach śledczych oraz w zakładach karnych.** Podmioty te **–** ze względu na brak stosownych regulacji w kodeksie karnym wykonawczym i aktach wykonawczych – zobowiązane są stosować ww. przepisy ustawy o likwidacji niepodjętych depozytów. Tymczasem przewidziana w obowiązujących obecnie regulacjach procedura likwidacji przez areszty śledcze niepodjętych depozytów prowadzić może w niektórych sytuacjach do upublicznienia w dzienniku poczytnym w danej miejscowości lub w Biuletynie Informacji Publicznej informacji o osobach, które przebywały w areszcie i nie odebrały depozytów. Takie informacje pośrednio ujawniają, że osoby te zostały pozbawione wolności, a więc mogą prowadzić do przetwarzania danych o wyrokach skazujących, czynach zabronionych lub powiązanych środkach bezpieczeństwa, o których mowa w art. 10 RODO. Upublicznienie takich danych budzi wątpliwości z punktu widzenia proporcjonalności w odniesieniu do celu ich przetwarzania, jakim jest likwidacja depozytów. Takie działanie może także prowadzić do dyskryminacji i stygmatyzacji osób, których ww. dane dotyczą. Wystąpienie w tej sprawie skierowane zostało do Ministra Sprawiedliwości w czerwcu 2025 r.[628].

W odpowiedzi na nie Minister Sprawiedliwości (pismo z 15 września 2025 r.) zadeklarował gotowość do podjęcia współpracy mającej na celu opracowanie rozwiązań prawnych i organizacyjnych dotyczących likwidacji nieodebranych depozytów, które zapewnią zgodność z zasadami ochrony danych osobowych, w szczególności poprzez wyeliminowanie upubliczniania danych osobowych osób osadzonych w aresztach śledczych czy zakładach karnych, które nie odebrały depozytu.

W dalszej korespondencji w tej sprawie (pismo z dnia 25 września 2025 r.) Prezes UODO podzielił przedstawiony przez Ministra Sprawiedliwości pogląd, że ustawa o likwidacji depozytów jest aktem prawa regulującym zasady i tryb likwidacji niepodjętych depozytów znajdujących się w dyspozycji jednostek sektora finansów publicznych, zatem nie tylko zakładów karnych i aresztów śledczych, ale też innych podmiotów, w których upublicznienie pobytu osób fizycznych mogłoby zostać uznane za dyskryminujące lub stygmatyzujące. Wskazał również, że z powyższego powodu warto byłoby podejść do tego problemu systemowo i podjąć próbę rozwiązania go we

[628] DPNT.413.25.2025.

współpracy z innymi resortami, których zagadnienie to może dotyczyć, zwłaszcza z Ministerstwem Zdrowia, do którego już w 2022 r. skierował wystąpienie w tej spawie.

Z kolei w październiku 2025 r. Prezes UODO skierował do Dyrektora Izby Administracji Skarbowej wystąpienie, w którym zwrócił się o odniesienie się do kwestii **podstawy prawnej do działania Izby Administracji Skarbowej polegającego na udostępnieniu klientom urzędów skarbowych opłatomatów umożliwiających uiszczenie opłaty skarbowej**, dla pobierania której organem podatkowym właściwym w sprawach opłaty skarbowej jest wójt, burmistrz lub prezydent miasta, a tym samym podstawy prawnej do przetwarzania danych osobowych przez tę Izbę w celu poboru opłaty skarbowej oraz do przekazania tych danych ww. właściwemu organowi[629].

W odpowiedzi na wystąpienie Dyrektor IAS wskazał, że poprzez udostępnienie na terenie podległych jej urzędów skarbowych opłatomatów, umożliwiających dokonanie zapłaty opłaty skarbowej, dla której właściwym organem podatkowym jest wójt, burmistrz lub prezydent miasta, IAS nie przejęła od tych organów zadania poboru opłaty skarbowej ani też nie pobiera tejże opłaty skarbowej na swój rachunek bankowy bądź na rachunki bankowe podległych urzędów skarbowych. W ocenie IAS wprowadzenie przez Dyrektora IAS przedmiotowego mechanizmu dokonywania zapłaty opłaty skarbowej w siedzibie urzędu skarbowego stanowi realizację zadania ustawowego, o którym mowa w art. 2 ust. 5 ustawy o KAS, zgodnie z którym organy podatkowe mają obowiązek zapewnienia obsługi i wsparcia podatnika i płatnika w prawidłowym wykonywaniu obowiązków podatkowych.

Kwestia ta jest przedmiotem dalszych analiz organu nadzorczego.

W 2025 r. **kontynuowane** były też sprawy w zakresie **wystąpień z poprzednich okresów sprawozdawczych w sprawach zasygnalizowanych przez IOD**.

Prezes UODO ponownie zwrócił się do Szefowej Służby Cywilnej w Kancelarii Prezesa Rady Ministrów z prośbą o przedstawienie stanowiska w sprawie postulowanej zmiany przepisów rozporządzenia stanowiskowo - płacowego mającego na celu **wyodrębnienie stanowiska Inspektora Ochrony Danych w wykazie stanowisk urzędniczych w służbie cywilnej**[630].

Z wnioskiem o zainicjowanie prac legislacyjnych mających na celu nowelizację rozporządzenia Prezesa Rady Ministrów z 29 stycznia 2016 r. w sprawie określenia stanowisk urzędniczych, wymaganych kwalifikacji zawodowych, stopni służbowych urzędników służby cywilnej, mnożników do ustalania wynagrodzenia oraz szczegółowych zasad ustalania i wypłacania innych świadczeń przysługujących członkom korpusu służby cywilnej Prezes UODO wystąpił w 2024 r. Już wówczas wskazywał na potrzebę uzupełnienia wykazu stanowisk urzędniczych o stanowisko IOD[631].

W odpowiedzi na wystąpienie Szefowa Służby Cywilnej poinformowała, że rozpoczęto prace nad taką zmianą. Jak zaznaczyła, zakres nowelizacji tego

[629] DPNT.413.46.2025.
[630] DOL.413.6.2024.
[631] https://uodo.gov.pl/pl/138/3217.

rozporządzenia będzie szerszy i obejmie również inne postulaty zgłaszane przez różne instytucje. Zmiany rozporządzenia powiązane są z konsultacjami projektu Strategii Zarządzania Zasobami Ludzkimi w Służbie Cywilnej (więcej informacji pod linkiem: https://uodo.gov.pl/pl/138/3807). Projekt zmiany rozporządzenia stanowiskowo – płacowego pojawił się 16 lutego 2026 r. w wykazie prac legislacyjnych Prezesa Rady Ministrów[632]. W ocenie Prezesa UODO w projektowanej zmianie rozporządzenia dotyczącego stanowisk urzędniczych w służbie cywilnej należy doprecyzować przepisy dotyczące inspektorów danych osobowych oraz uwzględnić stanowisko zastępcy IOD[633].

Wobec braku odpowiedzi na wystąpienie z 24 sierpnia 2023 r., które dotyczyło podjęcia stosownych działań mających na celu **ograniczenie zakresu danych ujawnianych w spisie członków izby rolniczej uprawnionych do głosowania w związku z wyborami do walnych zgromadzeń izb rolniczych**[634]**,** Prezes UODO 2 lipca 2025 r. ponownie zwrócił się do Krajowej Rady Izb Rolniczych o ustosunkowanie się do powyższego wystąpienia.

W odpowiedzi Prezes KRIR wskazał, że zgodnie z art. 32 ustawy o izbach rolniczych szczegółowe zasady i tryb przeprowadzania wyborów do walnego zgromadzenia, w tym do rady powiatowej izby, określa, w drodze uchwały, Krajowa Rada Izb Rolniczych. Wskazał też, że uchwały Krajowej Rady Izb Rolniczych nie stanowią źródła powszechnie obowiązującego prawa, nie wiążą innych uczestników obrotu prawnego i mają walor wyłącznie aktów wewnętrznych. KRIR jedynie w celach porządkowych i pomocniczych, w uchwale nr 1/2023 z 22 lutego 2023 r., określiła wzór spisu wyborców. Jak wskazał Prezes KRIR brak jest przeszkód prawnych, by gminy, jako organy ustawowo odpowiedzialne za sporządzenie spisu, przyjęły własne wzory i umieszczały w nich takie dane, jakie uznają za stosowne, celem wypełnienia ustawowego obowiązku z art. 28 ustawy o izbach rolniczych. Niemniej KRIR, przygotowując proces wyborów w roku 2027, weźmie pod uwagę stanowisko Prezesa Urzędu Ochrony Danych Osobowych w sprawie spisu wyborców, dokonując stosownej zmiany uchwały w sprawie szczegółowych zasad i trybu przeprowadzania wyborów do walnych zgromadzeń izb rolniczych.

W związku z tym, że Prezes UODO nie otrzymał od Ministra Zdrowia odpowiedzi na ponowione **wystąpienie z 26 listopada 2024 r.**[635] oraz na pisma z 3 lutego 2025 r. oraz z 12 maja 2025 r. wskazujące na konieczność dostosowania do RODO obowiązujących regulacji prawnych w zakresie **likwidacji niepodjętych depozytów należących do pacjentów podmiotów udzielających świadczeń zdrowotnych,**

[632] https://www.gov.pl/web/premier/projekt-rozporzadzenia-prezesa-rady-ministrow-zmieniajacego-rozporzadzenie-w-sprawie-okreslenia-stanowisk-urzedniczych-wymaganych-kwalifikacji-zawodowych-stopni-sluzbowych-urzednikow-sluzby-cywilnej-mnoznikow-do-ustalania-wynagrodzenia-oraz-szczegolowych-zasad-ustalania-i-wyplacania-innych-swiadczen-przyslugujacych-czlonkom-korpusu-sluzby-cywilnej4.
[633] https://uodo.gov.pl/pl/138/4132.
[634] DOL.413.8.2023.
[635] DOL.413.19.2022.

3 października 2025 r. zwrócił się do Ministra Zdrowia o ustosunkowanie się do przedstawionego w wystąpieniu wniosku.

W przesłanej 9 grudnia 2025 r. odpowiedzi Minister Zdrowia poinformował o podjęciu prac w powyższym zakresie. W tym celu do wykazu prac Rady Ministrów został włączony projekt ustawy o świadczeniach kompensacyjnych wypłacanych z Funduszu Kompensacyjnego Zdarzeń Medycznych (UD341), w którym przewidziano wprowadzenie zmian w art. 39 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, a także dodanie art. 39a do tej ustawy w zakresie likwidacji depozytu i zakresu danych zamieszczanych w ogłoszeniu o zamiarze likwidacji, który nie będzie obejmować danych osobowych pacjenta.

Odnosząc się do powyższych informacji organ nadzorczy wskazał, że pozytywnie należy ocenić dążenie Ministerstwa do opracowania rozwiązań, które nie będą obejmować danych osobowych pacjenta. Jednocześnie jeszcze raz podkreślił, że upublicznienie takich danych może stygmatyzować osobę, której dane dotyczą, a tym samym stanowić poważną ingerencję w jej życie prywatne lub zawodowe. Ponadto jest nieadekwatne do celu ich przetwarzania, jakim jest likwidacja niepodjętego depozytu, a zatem nie spełnia wymagań potrzebnych dla zapewnienia przestrzegania zasady minimalizacji danych. Jednocześnie organ nadzorczy zauważył, że warto byłoby podejść do tego problemu systemowo i podjąć próbę rozwiązania go we współpracy z innymi resortami, których zagadnienie to może dotyczyć, w szczególności z Ministerstwem Sprawiedliwości (do którego 17 czerwca 2025 r. Prezes UODO skierował wystąpienie[636] w tej sprawie).

W 2025 r. kontynuowana była sprawa wystąpienia Prezesa UODO o podjęcie prac prowadzących do zagwarantowania, aby **przetwarzanie danych osobowych pozyskiwanych w związku z realizacją programu „Senior+”** odbywało się zgodnie z zasadami ochrony danych osobowych[637]. W odpowiedzi z 24 listopada 2025 r. Minister Rodziny, Pracy i Polityki Społecznej przekazała, że 30 września 2025 r. do wykazu prac Rady Ministrów (pod nr UD 315) wpisany został projekt nowelizacji ustawy o pomocy społecznej uwzględniający postulaty zawarte w ww. wystąpieniu. Przede wszystkim ma on wprowadzić regulację ustawową stanowiącą o rezygnacji z przeprowadzania rodzinnego wywiadu środowiskowego w przypadku udzielenia świadczenia w postaci uczestnictwa w zajęciach klubu samopomocy.

W 2025 r. Prezes UODO skierował ponowne wystąpienie do MSWiA o **podjęcie prac legislacyjnych w zakresie wprowadzenia zmian do ustawy z dnia 14 grudnia 2018 r**.[638], odnoszących się do inspektora ochrony danych, w celu zapewnienia prawidłowej implementacji dyrektywy 2016/680. Prezes Urzędu Ochrony Danych Osobowych już w wystąpieniu z 19 lipca 2022 r. sygnalizował Ministrowi Spraw Wewnętrznych i Administracji konieczność podjęcia takich prac. W odpowiedzi na nie

[636] DPNT.413.25.2025 - wystąpienie dotyczące podjęcie prac legislacyjnych mających na celu wprowadzenie stosownych regulacji prawnych w zakresie likwidacji niepodjętych depozytów należących do osób osadzonych w aresztach śledczych i zakładach karnych.
[637] DOL.413.9.2023.
[638] DOL.413.11.2022.

otrzymał pismo od Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych i Administracji, w którym wskazano, że: „zakres i charakter postulowanych zmian nie uzasadniają podjęcia odrębnej inicjatywy legislacyjnej. Tym samym zmiany w zakresie zadań inspektora ochrony danych mogą zostać wprowadzone w przyszłości przy okazji zamian przepisów o zbliżonym zakresie tematycznym w innych ustawach".

Mając na uwadze, że mimo upływu czasu, prace nad zmianą w ustawy z 14 grudnia 2018 r. w ww. zakresie nie zostały podjęte, Prezes UODO ponownie zasygnalizował konieczność ich nowelizacji. Przepisy ustawy z dnia 14 grudnia 2018 r. nie precyzują, jakie dane administratora powinny być przekazane przez niego do Prezesa UODO w związku z dokonywaniem zawiadomienia dotyczącego inspektora ochrony danych (wyznaczenia, odwołania, zmiany danych inspektora ochrony danych). Ponadto w ustawie z 14 grudnia 2018 r. brak jest przepisów, na mocy których administrator byłby zobowiązany do powiadomienia Prezesa UODO o każdej zmianie danych odnoszących się do administratora.

Prezes UODO w 2025 r. ponowił również wystąpienie do Ministry 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[639].

Zakres postulowanych zmian był przedstawiany Ministrze Edukacji przez Prezesa UODO w wystąpieniu z 24 grudnia 2024 r. oraz Ministrowi Edukacji i Nauki 24 sierpnia 2023 r. Prezes UODO wskazywał w tej korespondencji, że art. 90l ustawy o systemie oświaty − odnoszący się do przyznawania uczniom przez osoby fizyczne i osoby prawne inne niż jednostki samorządu terytorialnego ze środków własnych stypendiów za wyniki w nauce lub za osiągnięcia sportowe − nie zapewnia osobom, których dane dotyczą, odpowiednich gwarancji poszanowania ich praw i wolności. M.in. brak jest szczegółowych uregulowań dotyczących tego, kto, w jakim celu i jakie dane osobowe (również te dotyczące szczególnych kategorii) ma prawo przetwarzać, w tym, kto, komu, na jakich zasadach i w jakim trybie może je udostępniać. Nie określono również okresów retencji danych. Jednocześnie Prezes UODO podkreślał, że RODO 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.

W 2025 r. **interwencję** podobną do wystąpienia **Prezes UODO podjął w związku z sygnalizowanym mu problemem upowszechniania się sharentingu**, tj. nadmiernego udostępniania przez rodziców wizerunku i informacji o dzieciach w mediach społecznościowych. Postępowanie takie wynika czasami z dumy ze swoich pociech, a czasami jest podyktowane względami komercyjnymi, a jednocześnie rodzi

[639] DOL.413.4.2023.

liczne ryzyka, w tym m.in. wykorzystania zdjęć przez osoby niepowołane, kradzieży tożsamości, hejtu, naruszenia prywatności.

W lipcu 2025 r. Rzeczniczka Praw Dziecka skierowała do Prezesa UODO pismo w sprawie działalności Fundacji „Dzieci są z nami". Jej wątpliwości wzbudziła zgodność statutu fundacji z regulacjami zawartymi w Konwencji o prawach dziecka, Konstytucji RP oraz RODO. Podobna korespondencja wpłynęła od różnych fundacji, stowarzyszeń i osób fizycznych, które prowadzą działalność ukierunkowaną na obronę praw dzieci. Zwracano się w niej z prośbą o podjęcie przez Prezesa UODO działań w sprawie niniejszej fundacji[640]. Działania tej fundacji wzbudziły również wątpliwości Rzecznika Praw Obywatelskich, który 31 lipca 2025 r. pismo w tej sprawie[641] skierował do Ministra Cyfryzacji i do wiadomości kilku innych organów, w tym Prezesa UODO.

Po analizie Prezes UODO uznał, że działania wspomnianej fundacji, polegające na promowaniu sharentingu, mogą naruszać prawa dzieci do ochrony ich prywatności i nie powinny być legalnie realizowane. Dlatego do Ministerstwa Rodziny, Pracy i Polityki Społecznej, które (zgodnie z wpisem do Krajowego Rejestru Sądowego) sprawuje nadzór na wspomnianą fundacją, skierował pismo[642], w którym zwrócił się o rozważenie wystąpienia do KRS w celu oceny zgodności statutu fundacji z prawem krajowym. W odpowiedzi na to pismo Ministra Rodziny, Pracy i Polityki Społecznej wystąpiła do Prezydenta m.st. Warszawy, jako także wskazanego w Krajowym Rejestrze Sądowym organu nadzoru, o przekazanie wszelkich posiadanych informacji. Jednocześnie skierowała ona wniosek do sądu rejestrowego o wydanie orzeczenia co do zgodności działania fundacji z przepisami prawa. MRPiPS nawiązało również kontakt z Ministrem Cyfryzacji, który przedstawił informację o podejmowanych działaniach o charakterze cyberprofilaktyk w zakresie ochrony wizerunku dzieci w przestrzeni publicznej.

Podkreślić jednak należy, że kwestia zagrożeń, jakie wiążą się z sharentingiem, jest podnoszona przez Prezesa UODO przy każdej sposobności, w tym m.in. w materiałach edukacyjnych, podczas szkoleń i konferencji czy posiedzeń sejmowej Komisji ds. Dzieci i Młodzieży (dalej: DIM).

Podczas grudniowego posiedzenia tej komisji[643] posłowie przyjęli dezyderat ws. zwiększenia ochrony wizerunku małoletnich w przestrzeni cyfrowej, jak również powiązanego z tym zagadnieniem kompleksowego uregulowania kwestii sharentingu, w tym zasad publikowania treści z udziałem małoletnich, ochrony ich danych osobowych oraz pracy małoletnich w sieci, co Prezes UODO przyjął z zadowoleniem.

Dodatkowo Prezes UODO skierował do organów państwowych oraz do podmiotu niepublicznego realizującego zadania publiczne **8 wystąpień** zmierzających do zapewnienia skutecznej ochrony danych osobowych.

[640] DPNT.023.1017.2025, DPNT.023.1022.2025; DPNT.023.1034.2025; DPNT.023.1039.2025; DPNT.023.1066.2025; DPNT.023.1067.2025.
[641] Znak VII.501.113.2025.KK.
[642] DPNT.051.13.2025. Pismo dostępne na stronie UODO pod linkiem https://uodo.gov.pl/pl/138/3895.
[643] https://uodo.gov.pl/pl/138/4015.

W następstwie nieprawidłowości stwierdzonych w toku przeprowadzonej w jednej z regionalnych rozgłośni polskiego radia, kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, Prezes UODO zwrócił się do **Likwidatora Polskiego Radia S.A.**[644], do likwidatorów wszystkich **Rozgłośni Regionalnych Polskiego Radia S.A.** w likwidacji[645] oraz do **Likwidatora „Telewizji Polskiej" S.A.** w likwidacji[646], o zwrócenie uwagi pracownikom i współpracownikom na fakt, że brak zapewnienia zgodności przetwarzania danych osobowych z prawem przez radiofonię publiczną może prowadzić nie tylko do naruszenia praw lub wolności osób, których dane dotyczą, ale również do sytuacji zagrożenia zdrowia lub życia tych osób. Prezes UODO podniósł, że mając na uwadze szczególne zadania i powinności publicznej radiofonii i telewizji wynikające z realizacji powierzonych jej publicznie doniosłych celów, a także fakt, że ich realizacja nierozerwalnie powiązana jest z przetwarzaniem danych osobowych, brak zapewnienia zgodności przetwarzania danych osobowych z prawem może prowadzić nie tylko do naruszenia praw lub wolności osób, których dane dotyczą, ale również do sytuacji zagrożenia zdrowia lub życia tych osób. W odpowiedzi na wystąpienie, Likwidator Polskiego Radia S.A. w likwidacji, zagwarantował, że Polskie Radio S.A. w likwidacji dochowuje wszelkiej staranności aby naruszenia prawa w tej materii nie miały miejsca. Likwidatorzy Rozgłośni Regionalnych Polskiego Radia S.A. w likwidacji poinformowali o podejmowaniu przez nich szeregu działań mających na celu zapewnienie wysokiego poziomu ochrony danych osobowych, zgodnie z przepisami o ochronie danych osobowych. Z kolei Likwidator „Telewizji Polskiej" S.A. w likwidacji podkreślił, że uwagi Prezesa UODO stały się impulsem do rozpoczęcia wszechstronnej weryfikacji obowiązujących technicznych i organizacyjnych środków bezpieczeństwa stosowanych w działalności prasowej.

Kolejne wystąpienie w roku 2025 zostało skierowane do **Prokuratora Krajowego**[647] w związku z doniesieniami medialnymi oraz informacjami, jakie wpłynęły do Prezesa UODO w sprawie prowadzonych przez Prokuraturę Regionalną w Szczecinie działań dotyczących zatrzymania całej dokumentacji medycznej, zawierającej dane wrażliwe pacjentek lekarza ginekologa (a więc również tych, których nie dotyczyło toczące się postępowanie). Prezes UODO wskazał Prokuratorowi Krajowemu na konieczność zwrócenia uwagi kierownikom podległych Prokuratorowi Krajowemu powszechnych jednostek organizacyjnych prokuratury, że w świetle obowiązujących przepisów prawa przetwarzanie bez podstawy prawnej danych osobowych, w szczególności danych podlegających wzmożonej ochronie, w tym danych o stanie zdrowia, jest niedopuszczalne. Poinformował również, że wykonywanie jakichkolwiek operacji na danych osobowych znajdujących się w zatrzymanej dokumentacji medycznej bez podstawy prawnej, będzie procesem niezgodnym z prawem. W odpowiedzi na ww.

[644] DKN.5101.42.2025.
[645] DKN.5101.147.2025.
[646] DKN.5101.219.2025.
[647] DKN.5101.55.2023.

wystąpienie Prokurator Krajowy poinformował Prezesa UODO, że kwestie zabezpieczania dokumentacji medycznej były przedmiotem stanowisk kierowanych przez właściwe komórki organizacyjne Prokuratury Krajowej do prokuratorów prowadzących lub nadzorujących postępowania przygotowawcze.

W 2025 r. Prezes UODO dwukrotnie kierował wystąpienia do **Prezesa Poczty Polskiej S.A.**[648].

Pierwsze z nich było kontynuacją wystąpienia skierowanego w 2024 roku i odnosiło się do braku efektywności uprzednio wdrożonych przez Pocztę Polską środków mających zapobiegać występowaniu incydentów związanych z doręczeniem przesyłek pocztowych i rosnącej w dalszym ciągu skali zgłoszeń naruszeń ochrony danych osobowych, polegających na zagubieniu przesyłek przez Pocztę Polską S.A. Prezes UODO w swym wystąpieniu skupił się głównie na ww. incydentach w ramach realizacji usługi e-Doręczeń (w szczególności na etapie przygotowywania korespondencji, w tym również przekształcenia dokumentu elektronicznego w przesyłkę listową w ramach świadczenia publicznej usługi hybrydowej, dalej PUH, tj. odebrania od nadawcy dokumentu elektronicznego, drukowania oraz kopertowania korespondencji nadanej w postaci elektronicznej, a następnie doręczenia korespondencji do adresata). Prezes UODO podkreślił jak poważny problem dla administratorów (nadawców przesyłek) w kontekście obowiązku określonego w art. 33 ust. 1 rozporządzenia 2016/679 stanowią występujące liczne przypadki zagubienia przesyłek – również tych wysyłanych za pośrednictwem systemu e-Doręczeń. W związku z tym, że spośród wszystkich zgłaszanych Prezesowi UODO naruszeń ochrony danych osobowych znaczącą liczbę stanowią przypadki zagubienia przesyłek przez Pocztę Polską, w tym tych doręczanych obecnie w ramach usługi e-Doręczeń, w szczególności zagubionych na etapie przekształcenia dokumentu elektronicznego w przesyłkę listową w ramach świadczenia PUH, dlatego Prezes UODO zwrócił się do Poczty Polskiej o przedstawienie dodatkowych wyjaśnień w kwestii działań podejmowanych w związku z funkcjonowaniem PUH.

W kolejnym wystąpieniu skierowanym do Poczty Polskiej S.A. Prezes UODO z jednej strony pozytywnie ocenił zaproponowane uprzednio przez operatora pocztowego działania związane z usługą e-Doręczeń, jak m.in. zaktualizowanie dokumentacji analizy ryzyka w związku z uruchomieniem usługi e-Doręczeń. Z drugiej strony Prezes UODO ponownie podjął interwencję u Prezesa Poczty Polskiej, w związku z bardzo dużą skalą odnotowywanych przypadków zagubienia przesyłek przez Pocztę Polską, wydania przesyłek odbiorcom nieuprawnionym do ich odbioru, czy też doręczenia uszkodzonych przesyłek pocztowych, o czym świadczy liczba naruszeń ochrony danych osobowych w tym zakresie, zgłaszanych Prezesowi UODO zarówno przez administratorów z sektora prywatnego, z obszaru administracji publicznej czy przez wymiar sprawiedliwości. Prezes UODO podkreślił, jak szczególnie istotny jest to problem w kontekście doręczania korespondencji kierowanej do sądu, zawierającej obszerny i zróżnicowany katalog

[648] DKN.5101.47.2024.

danych osobowych, w tym dane szczególnej kategorii, wymienione w art. 9 ust. 1 rozporządzenia 2016/679, np. dane dotyczące zdrowia, oraz dane, o których mowa w art. 10 rozporządzenia 2016/679, tj. dane dotyczące wyroków skazujących i czynów zabronionych. W takich przypadkach często występuje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, wymagające zgodnie z treścią art. 34 ust. 1 rozporządzenia 2016/679 zawiadomienia osób, których dane dotyczą, o naruszeniu polegającym na zagubieniu, uszkodzeniu bądź nieprawidłowym doręczeniu przesyłki przez Pocztę Polską. W przypadku korespondencji związanej z postępowaniami sądowymi pojawia się również niebezpieczeństwo wystąpienia negatywnych skutków procesowych – w przypadku zagubienia części zawartości przesyłki, strona może zostać pozbawiona możliwości obrony swoich praw, a skutki mogą być nieodwracalne (niektóre dowody, np. oryginały pism, są przesyłane do postępowań drogą pocztową i są nie do odtworzenia w razie ich zagubienia lub zniszczenia). Należy również pamiętać o możliwości naruszenia dóbr osobistych w postaci chociażby wizerunku, które może wiązać się z dotkliwą ingerencją w sferę prywatności danej osoby.

Zdaniem Poczty Polskiej główną przyczyną nieprawidłowości, występujących podczas doręczania przesyłek są: niewłaściwe opakowania przesyłek stosowane przez nadawców, skutkujące ich uszkodzeniami podczas maszynowego opracowywania przesyłek w procesie ekspedycyjno-rozdzielczym, brak lub uszkodzenia oddawczych skrzynek pocztowych, czynniki ludzkie, wynikające z pośpiechu i nieuwagi pracowników doręczających przesyłki, ale też występujące wakaty i absencje w służbie doręczeń, które powodują konieczność zmian organizacji pracy.

Równocześnie w odpowiedzi wskazane zostały działania prewencyjne, jakie stosowane są przez operatora pocztowego celem wyeliminowania ryzyka naruszeń ochrony danych osobowych klientów. W ramach takich działań kierowane są do wspólnot mieszkaniowych, zarządców nieruchomości, właścicieli nieruchomości, pisma celem podjęcia montażu/naprawy uszkodzonych oddawczych skrzynek pocztowych oraz prowadzone są rozmowy z pracownikami, instruktaże, a także szkolenia przypominające zasady prawidłowego doręczania przesyłek.

W związku z pozyskanymi informacjami opisującymi proceder korzystania w sposób nieuprawniony z bazy PESEL przez funkcjonariuszy Straży Granicznej Prezes UODO skierował do **Komendanta Głównego Straży Granicznej**[649] wystąpienie mające na celu ukazanie administratorowi konieczności podjęcia działań w organizacji związanych m.in. z zapewnieniem terminowego zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą. W odpowiedzi Komendant Główny Straży Granicznej podkreślił, że Straż Graniczna wykonując zadania określone w ustawie przetwarza dane osobowe w zakresie niezbędnym do realizacji obowiązków służbowych. Natomiast dostęp do systemów teleinformatycznych jest

[649] DKN.5101.485.2024.

ściśle reglamentowany i odbywa się wyłącznie na podstawie nadanych imiennie upoważnień. W celu zapobiegania przypadkom nieuprawnionego wykorzystania danych osobowych systematycznie prowadzone są szkolenia z zakresu ochrony danych osobowych, bezpieczeństwa informacji i odpowiedzialności służbowej. W ramach stałego monitorowania i doskonalenia procesów przetwarzania danych osobowych okresowo oraz doraźnie kontrolowane i analizowane są logi systemowe użytkowników do systemów teleinformatycznych, co umożliwia m.in. identyfikację nieuprawnionych lub nietypowych operacji. W przypadku ich wykrycia, zgodnie z wewnętrznymi procedurami podejmowane są stosowne czynności wyjaśniające. Komendant Główny Straży Granicznej poinformował m.in. o prowadzonych i planowanych czynnościach monitorujących przetwarzanie danych osobowych w oddziałach Straży Granicznej, obejmujących sposób nadawania upoważnień i uprawnień do przetwarzania danych osobowych oraz ich obieg, sposób postępowania funkcjonariuszy z danymi osobowymi w czasie realizacji zadań służbowych. Obecnie opracowywany jest również program o charakterze edukacyjno-prewencyjnym dla całej Straży Granicznej, ukierunkowany na podnoszenie świadomości funkcjonariuszy w zakresie ochrony danych osobowych oraz wskazujący na konsekwencje w postaci odpowiedzialności służbowej i karnej w tym obszarze. Ponadto zagadnienia dotyczące ochrony danych osobowych są przekazywane także ustnie w ramach instruktażu do służby kierownikom zmiany w oddziałach Straży Granicznej oraz uwzględniane w toku przeprowadzanych kontroli służby. Wskazano również, że w ramach wdrażania systemu EES (Entry/Exit System) przez Straż Graniczną, na bieżąco prowadzone są szkolenia dla wszystkich funkcjonariuszy mających dostęp do interoperacyjnych systemów teleinformatycznych. Szkolenia obejmują m.in. bezpieczne korzystanie z tych systemów oraz bezpieczeństwo danych osobowych z naciskiem na kategoryczny zakaz wykorzystywania uprawnień do działań pozasłużbowych.

Kontynuując monitorowanie przestrzegania przepisów Prezes UODO skierował zapytanie do **Komendanta Głównego Policji**[650] dotyczące jego deklaracji na wystąpienie z 2024 roku. W przywołanym wystąpieniu Prezes UODO poruszył kwestię utraty przez funkcjonariuszy bloczków mandatowych i notatników służbowych zawierających dane osobowe. Komendant Główny Policji poinformował, że problematyka zdarzeń jest mu znana i zaplanowane zostało zastąpienie notatników służbowych ich elektronicznym odpowiednikiem. Zapytanie Prezesa UODO dotyczyło uzyskania informacji na jakim etapie znajduje się wdrażanie projektu teleinformatycznego „e-Notatnik”, a w szczególności, czy określono termin zakończenia realizacji tego projektu. Komendant Główny Policji wskazał, że realizacja projektu pn. „Budowa aplikacji informatycznej e-Notatnik” pozostaje na etapie przygotowania do uruchomienia, w czwartym kwartale 2025 roku oraz wstępnych testów Modułu dokumentacyjnego w środowisku

[650] DKN.5101.66.2024.

produkcyjnym, w jednostkach organizacyjnych Policji, które uczestniczyły wcześniej w pilotażu Modułu zadaniowego.

W roku 2025 do **Głównego Inspektora Sanitarnego**[651] zostało skierowane wystąpienie w związku z wydaniem decyzji nakładającej karę na powiatowego inspektora sanitarnego. W toku postępowania administracyjnego przeprowadzanego przez Prezesa UODO stwierdzone zostały nieprawidłowości dotyczące stosowanych środków organizacyjnych i technicznych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych, w tym danych przetwarzanych na zewnętrznych nośnikach danych.

W związku z powyższym Prezes UODO zwrócił się do Głównego Inspektora Sanitarnego o ustalenie i analizę, jakie dokładnie rozwiązania w obszarze bezpieczeństwa danych osobowych stosowane są przez Państwową Inspekcję Sanitarną, a w szczególności, czy i w jaki sposób te rozwiązania minimalizują ryzyko naruszenia praw lub wolności pacjentów także w kontekście możliwości zagubienia przez pracowników Inspekcji nośników danych zawierających dane osobowe.

# 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[652],
- upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO[653],
- 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[654].

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.

[651] DKN.5101.414.2025.
[652] Art. 57.1.b RODO.
[653] Art. 57.1.d RODO.
[654] Art. 57.1.e RODO.

## 1. Działalność edukacyjna

Działania edukacyjne są kluczowe dla budowania świadomości społeczeństwa i dlatego Prezes UODO nie ustaje w popularyzowaniu wiedzy o ochronie prywatności i danych osobowych.

Prezes UODO jest organizatorem lub współorganizatorem konferencji, seminariów, webinariów, szkoleń, spotkań, debat, konkursów wiedzy dla studentów i konkursów dla szkół i uczniów uczestniczących w programie edukacyjnym UODO „Twoje dane – Twoja sprawa", a także prowadzi prace nad poradnikami dotyczącymi ochrony danych osobowych, patronuje inicjatywom edukacyjnym organizowanym przez inne podmioty, a eksperci UODO wspierają swoją wiedzą ważne wydarzenia adresowane do różnych odbiorców, w tym do inspektorów ochrony danych.

W 2025 r. Prezes UODO i jego przedstawiciele uczestniczyli **w kilkuset wydarzeniach w kraju i za granicą,** organizowanych lub współorganizowanych przez Urząd bądź przez inne podmioty, z udziałem Prezesa UODO i jego ekspertów.

Pełny wykaz tych wydarzeń jest przedstawiony w załączniku nr 3 i 4 niniejszego Sprawozdania. Wydarzenia organizowane przez Prezesa UODO odbywały się z udziałem i przy wsparciu merytorycznym Społecznego Zespołu Ekspertów przy Prezesie UODO (SZE).

### 1.1. Kampanie edukacyjne

#### 1) XIX 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 ich prawach i obowiązkach oraz o zagrożeniach związanych z przetwarzaniem dotyczących ich danych osobowych w związku z rozwojem technologicznym.

Rada Europy promuje inicjatywy organizowane w ramach tego święta i zapewnia spójność działań odbywających się w tym Dniu. Każde państwo i/lub instytucja krajowa lub międzynarodowa może uczestniczyć w obchodach. Polska włączyła się w organizację Dnia Ochrony Danych Osobowych w 2007 r.

Wykaz wydarzeń zorganizowanych w 2025 r. z okazji XIX Dnia Ochrony Danych Osobowych:

**XIX Dzień Ochrony Danych Osobowych w Brukseli**

1. **28 stycznia 2025 r.** na zaproszenie Rady Europy, konferencji CPDP i Europejskiego Inspektora Ochrony Danych (EIOD), Mirosław Wróblewski, Prezes UODO, jego zastępczyni Agnieszka Grzelak oraz dyrekcja Departamentu Współpracy Międzynarodowej UODO, świętowali Dzień Ochrony Danych w Brukseli, uczestnicząc w specjalnej edycję CPDP – **Data Protection Day: A New Mandate for Data Protection**.

Konferencja dotyczyła wyzwań z obszaru nowych technologii, zagrożeń dla prywatności i innych praw podstawowych, a także innowacji i ram regulacyjnych.

2. **28.01.2025 r**. Obchody Dnia Ochrony Danych Osobowych w Brukseli w Stałym Przedstawicielstwie RP przy Unii Europejskiej.

Stałe Przedstawicielstwo RP przy UE i Ministerstwo Cyfryzacji, we współpracy z Radą Europy, CPDP i Europejskim Inspektorem Ochrony Danych, zorganizowali debatę poświęconą nowym technologiom, podczas której Prezes UODO wystąpił w panelu: „Do robots have personal data?: future of personal data protection in the age of AI and new technologies' development".

**Główne obchody w Polsce – 23 stycznia 2025 r.**

1. Prawidłowa ocena ryzyka dla ochrony danych osobowych była tematem przewodnim XIX Dnia Ochrony Danych Osobowych 2025 r. w Polsce.

Głównym punktem obchodów była konferencja na Uniwersytecie Warszawskim pt. „Ocena ryzyka a ochrona danych osobowych" (23.01.2025 r.), która była próbą odpowiedzi na pytanie, dlaczego analiza ryzyka jest tak istotna i jaki jest jej sens w procesie zarządzania i podejmowania strategicznych decyzji w organizacji. W programie konferencji znalazły się więc tematy dotyczące ryzyka w ujęciu prawnym, zarządzania ryzykiem w obszarze cyberbezpieczeństwa oraz ryzyka w obszarze ochrony danych osobowych. Szczególną uwagę poświęcono temu, w jaki sposób analiza może nie tylko pomóc w zrozumieniu potencjalnych zagrożeń, ale także przynieść znaczące korzyści organizacjom, firmom i instytucjom publicznym.

Organizatorem wydarzenia był Urząd Ochrony Danych Osobowych we współpracy z Uniwersytetem Warszawskim oraz Społecznym Zespołem Ekspertów przy Prezesie UODO.

2. Tradycyjne już podczas obchodów Dnia wręczona została Nagroda im. Michała Serzyckiego, przyznawana za wybitne osiągnięcia w zakresie edukacji i promocji ochrony danych osobowych.

Uroczystość wręczenia Nagrody odbyła się **25 lutego 2025 r.** W tym roku Nagrodę przyznano po raz ósmy, wyróżniając zaangażowanie, pomysłowość i skuteczność w szerzeniu idei świadomego korzystania z informacji i technologii. Dzięki tej inicjatywie wzmacniana jest społeczna świadomość roli, jaką pełni prawo do prywatności i ochrony danych osobowych we współczesnym, rozwiniętym technologicznie świecie.

Po zakończeniu części oficjalnej wręczenia Nagrody odbył się panel dyskusyjny pt. **„Ochrona wizerunku vs rozwój technologii – gdzie postawić granice?”**, poświęcony wyzwaniom związanym z ochroną wizerunku w kontekście dynamicznego rozwoju technologii. Panel poprowadził dr Mirosław Gumularz, Przewodniczący Społecznego Zespołu Ekspertów przy PUODO.

**Kalendarium wydarzeń towarzyszących**

W ramach XIX Dnia Ochrony Danych Osobowych zaplanowanych zostało wiele imprez towarzyszących obchodom tego święta.

**7.01.2024 r.** Apel Prezesa UODO do uczestników 15. edycji ogólnopolskiego programu edukacyjnego UODO „Twoje dane – Twoja sprawa”, w formie listu otwartego z zaproszeniem do aktywnego uczestnictwa w obchodach XIX Dnia Ochrony Danych Osobowych.

W odpowiedzi na apel szkoły aktywnie włączyły się w obchody XIX Dnia Ochrony Danych Osobowych, realizując wiele różnorodnych inicjatyw. Były to m.in. zajęcia lekcyjne, uroczyste apele, spotkania z ekspertami, szkolenia, konkursy, przedstawienia oraz edukacyjne gry i zabawy. Podejmowane działania kierowano zarówno do uczniów, jak i do przedstawicieli lokalnej społeczności. Uczniowie opracowali również różnorodne materiały, takie jak gazetki, prezentacje multimedialne oraz teksty literackie, poświęcone ochronie danych osobowych i bezpieczeństwu w Internecie. Łącznie uczestnicy Programu w ramach obchodów XIX Dnia Ochrony Danych Osobowych zrealizowali 449 inicjatyw[655].

**13.01.2025 r.** Agnieszka Grzelak, Zastępczyni Prezesa UODO, wraz ze współpracownikami, spotkała się ze studentami Akademii Leona Koźmińskiego w siedzibie UODO w Warszawie. Prezentacja zadań realizowanych przez organ nadzorczy, wyzwania i zagrożenia dla ochrony danych i prawa do prywatności w świetle nowych technologii, zwłaszcza sztucznej inteligencji, były głównym tematem tego spotkania. Studenci zapoznali się ze strukturą Urzędu i zadaniami, jakie realizują poszczególne departamenty organu nadzorczego.

**16.01.2025 r.** Uroczystość podpisania porozumienia pomiędzy Prezesem UODO a Prezesem Zarządu Polskiego Towarzystwa Legislacyjnego o współpracy na rzecz promowania zasad ochrony danych osobowych w działalności zawodowej legislatorów, w procesie stanowienia prawa.

**20.01.2025 r.** Konferencja „Dzień Ochrony Danych Osobowych”. Organizator: redakcja kwartalnika „ABI Expert”. Wystąpienie inaugurujące konferencję wygłosił Mirosław Wróblewski, Prezes UODO[656].

[655] Wykaz jest dostępny na stronie internetowej UODO pod adresem: https://uodo.gov.pl/pl/587/3796.
[656] https://odo.abi-expert.pl/

**24.01.2025 r.** Wykład Marioli Więckowskiej, członkini Społecznego Zespołu Ekspertów (SZE) przy Prezesie UODO, pt. *Proces monitorowania postępu technologicznego jako element rozliczalności stosowania zasady ochrony danych w fazie projektowania oraz domyślnej ochrony danych.* Był to drugi z cyklu wykładów „Ochrona danych i technologia", podczas którego zaproszeni eksperci SZE omawiają wybrane zagadnienia na styku nowych technologii i ochrony danych osobowych.

**28.01.2025 r.** Webinarium UODO dla rodziców w ramach programu edukacyjnego „Twoje dane – Twoja sprawa". Webinarium miało na celu uświadomienie rodzicom jak mądrze wspierać dzieci w cyfrowym świecie w obszarze ochrony danych osobowych i prywatności.

**29.01.2025 r.** Konferencja online Dzień Inspektora Ochrony Danych 2025. Organizator: Lubasz i Wspólnicy - Kancelaria Radców Prawnych sp. k. Wystąpienie otwierające wygłosił Konrad Komornicki, Zastępca Prezesa UODO, natomiast dyrektor Departamentu Kontroli i Naruszeń UODO przedstawił prezentację pt. „Rola IOD w procesie zgłaszania naruszeń ochrony danych osobowych".

**30.01.2026 r.** X Konferencja „IOD 2025 – wyzwania nowych technologii". Organizator: Stowarzyszenie SABI. Konrad Komornicki, Zastępca Prezesa UODO, podczas otwarcia konferencji wygłosił prelekcję na temat roli IOD i współpracy organu nadzorczego z Inspektorami.

**30-31.01.2025 r.** Inicjatywa edukacyjna Prezesa UODO z cyklu **„UODO rusza w kraj – województwo pomorskie"** – spotkanie z mieszkańcami oraz władzami wojewódzkimi i samorządowymi poświęcone ochronie danych osobowych w działalności jednostek samorządu terytorialnego (JST).

- **30 stycznia 2025 r.** Konferencja w Zespole Szkól nr 1 im. Stanisława Staszica w Kwidzynie oraz punkt konsultacyjno-informacyjny UODO dla lokalnej społeczności w Sądzie Rejonowym w Kwidzynie;
- **31 stycznia 2025 r. Trójmiasto** - spotkanie z administratorami i IOD z JST województwa pomorskiego w Gdyni oraz punkt konsultacyjno-informacyjny UODO w Urzędzie Miejskim w Gdańsku.

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:

**6.02.2025 r.** XI Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej, podczas którego odbyła się konferencja tematyczna dotyczącą zagadnień związanych z nowymi technologiami, sztuczną inteligencją i cyberbezpieczeństwem.

**27.03.2025 r.** Ogólnopolska Konferencja Naukowa Ochrony Danych Osobowych, która odbyła się na WPiA Uniwersytetu Mikołaja Kopernika w Toruniu. Organizatorzy:

Centrum Badań nad Cyberprzestępczością oraz Studenckie Koło Naukowe 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) Licytacja WOŚP – Mecz Tenisa Stołowego z Prezesem UODO**

*Odpowiedzialność za ochronę danych nie może być odbijaniem piłeczki. Wygraną jest bezpieczeństwo obywatela i jego danych* – pod takim hasłem Prezes UODO włączył się w akcję Wielkiej Orkiestry Świątecznej Pomocy (WOŚP) organizując mecz tenisa stołowego dla uczestnika licytacji na rzecz wsparcia onkologii i hematologii dziecięcej. Akcja odbywała się w ramach 33. Finału WOŚP. Kwota z licytacji została w całości przekazana na Wielką Orkiestrę Świątecznej Pomocy.

**3) Warsztaty edukacyjne dla dzieci w ramach programu „Lekcje o finansach", 14.11.2025 r. oraz 3 i 6.12.2025 r.**

Główny cel warsztatów edukacyjnych, które odbyły się w UODO w ramach tego ogólnopolskiego programu, to wsparcie działań Ministerstwa Finansów w edukacji uczniów szkół podstawowych w zakresie funkcjonowania instytucji publicznych, przestrzeganie zasad bezpieczeństwa danych osobowych podczas różnych transakcji finansowych dokonywanych przez dzieci oraz rozwijanie wśród nich świadomości i odpowiedzialności w tym obszarze. UODO, jako instytucja zaangażowana w edukację, regularnie wspiera tego typu inicjatywy, dzieląc się swoją ekspercką wiedzą z zakresu ochrony danych osobowych.

W siedzibie Urzędu Ochrony Danych Osobowych odbyły się zajęcia edukacyjne dla uczniów szkół podstawowych z Małopolski (14.11.2025 r.), Mazowsza (3.12.2025 r.) oraz województwa zachodniopomorskiego (5.12.2025 r.). W zajęciach uczestniczyło w sumie ponad 100 dzieci. Podczas wizyty uczniowie zapoznali się z zagadnieniami dotyczącymi ochrony danych osobowych, praw przysługujących osobom fizycznym oraz roli UODO jako organu stojącego na straży prawa do prywatności. Lekcje ukierunkowane były na rozwijanie u dzieci kompetencji w zakresie rozumienia roli państwa, instytucji publicznych oraz zasad bezpiecznego i odpowiedzialnego funkcjonowania w społeczeństwie informacyjnym. Uczniowie dowiedzieli się, jak dużą wartość stanowią dane osobowe, ważne jest dbanie o prywatność oraz jakie prawa przysługują im w zakresie ochrony dotyczących ich danych osobowych.

**4) Kampania „Więcej szacunku dla młodego wizerunku"**

Od 10 grudnia 2024 r. Prezes UODO jest partnerem kampanii Rzecznika Praw Dziecka „Więcej szacunku dla młodego wizerunku". W ramach tej inicjatywy

przeprowadzone zostały w 2025 r. badania pod tym samym tytułem. Podczas spotkania, które odbyło się w Centrum Prasowym PAP (11.12.2025 r.) Zespół Badawczy Biura Rzecznika Praw Dziecka przedstawił raport z badań, zawierający nie tylko dane statystyczne, ale również opinie i doświadczenia nastolatków, rodziców i wychowawców na temat udostępniania wizerunku dzieci i młodzieży w internecie.

Pośród dorosłych najczęściej publikujących wizerunek dziecka w internecie, aż **42 % to jego rodzice,** 30 % nastolatków nie było w ogóle pytanych przez rodziców o zgodę, a dla szkół zamieszczających zdjęcia uczniów na stronach internetowych, decydująca jest jedynie zgoda rodzica, z reguły podpisywana na początku roku szkolnego. Wśród powodów publikowania wizerunków nastolatków było coraz powszechniejsze **zjawisko sharentingu**, a także **promocja placówki oświatowej czy organizacji sportowej.** W raporcie tym widać całe spektrum zjawisk związanych z prezentowaniem zdjęć dzieci w internecie. Mamy tu też opis, jak czują się z tym młodzi ludzie i na jakie ryzyka są narażeni.

W raporcie wyraźnie wybrzmiewa, że **nastolatkowie chcą mieć prawo do decydowania o tym, czy ich wizerunek może być upubliczniony.**
Wyniki badań można sprowadzić do 1 bardzo ważnego wniosku:
**Dzieci potrzebują wsparcia w rozwoju cyfrowym i wzmocnienia ich pozycji w sieci.** Potrzebna jest tu szeroko zakrojona edukacja, rozwijanie programów edukacyjnych w zakresie ochrony prywatności i danych osobowych, w szczególności wizerunku. Programy powinny być skierowane zarówno do **dzieci**, **rodziców, opiekunów**, jak i **instytucji**. Potrzebne jest przekazanie dobrych praktyk oraz nieustające informowanie o zagrożeniach.

### 1.2. Współpraca ze szkołami wyższymi

W 2025 r. Prezes Urząd Ochrony Danych Osobowych kontynuował współpracę ze szkołami wyższymi i organizacjami studenckimi. 28 października 2025 r. podpisał z Akademią im. Jakuba z Paradyża w Gorzowie Wielkopolskim porozumienie o współpracy na rzecz promowania zasad ochrony danych osobowych i prawa do prywatności. Natomiast z organizacjami studenckimi odbyły się trzy spotkania w siedzibie UODO z udziałem Agnieszki Grzelak, Zastępczyni Prezesa UODO. Uczestnikami dwóch spotkań byli studenci ALK w Warszawie:

- **13 stycznia 2025 r.** w ramach odchodów XIX Dnia Ochrony Danych Osobowych oraz **21 października 2025 r**., poświęconego zagadnieniom ochrony danych osobowych na styku prawa karnego i kompetencji Prezesa UODO w tym zakresie.
- **2 kwietnia 2025 r.** – spotkanie ze społecznością Studenckiego Koła Naukowego Praw Człowieka IUS HOMINI.

Z kolei Prezes UODO Mirosław Wróblewski, w analizowanym roku 2025 r. uczestniczył w spotkaniach ze studentami dwóch uczelni.

**24 marca 2025 r.** na zaproszenie Prorektora ds. Dydaktycznych i Jakości Kształcenia Akademii Sztuki Wojennej spotkał się z kadrą dydaktyczno-naukową Wydziału Zarządzania i Dowodzenia ASzWoj, a także studentami i słuchaczami Studencko-Doktoranckiego Koła Naukowego Zarządzania i Jakości tej uczelni.




Natomiast **19 maja 2025 r.** uczestniczył w spotkaniu seminaryjnym ze studentami Collegium Medicum UJ w Krakowie, podczas którego wygłosił wykład „Współczesne wyzwania dla ochrony danych osobowych w systemie ochrony zdrowia". Organizatorem spotkania było Studenckie Koło Naukowe Prawo w Zdrowiu, Collegium Medicum Uniwersytetu Jagiellońskiego w Krakowie.

Tematem spotkań ze studentami i kadrą były współczesne wyzwania dla ochrony prywatności, zagrożenia cyfrowego świata oraz niebezpieczeństwa dla danych osobowych i wolności osobistej, jakie niosą nowe technologie, ze szczególnym uwzględnieniem sztucznej inteligencji. Studenci uczestniczący w spotkaniach w siedzibie UODO, dodatkowo mieli okazję zapoznać się ze strukturą Urzędu i zadaniami, jakie realizują poszczególne departamenty organu nadzorczego, zapoznać się z ofertą praktyk i perspektywą pracy w UODO.

### 1.3. Współpraca UODO z ZUS

W 2025 roku Urząd Ochrony Danych Osobowych we współpracy z Zakładem Ubezpieczeń Społecznych kontynuował cykl seminariów - spotkań eksperckich, których celem było pogłębianie wiedzy dotyczącej ochrony danych osobowych w kontekście działań administracji publicznej, wyzwań technologicznych oraz relacji z otoczeniem. Współpraca obu instytucji obejmowała prezentacje trendów, dyskusje nad praktycznymi aspektami przetwarzania informacji oraz debatę nad sposobami łączenia transparentności działalności publicznej z ochroną danych osobowych.

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.

W ramach współpracy UODO z ZUS odbyły się następując wydarzenia:

1) **Seminarium „Automatyzacja procesów administracyjnych z wykorzystaniem sztucznej inteligencji: jak zapewnić zgodność z ochroną danych osobowych?”, 22.05.2025 w Poznaniu.**




Seminarium poświęcone było wyzwaniom i możliwościom związanym z automatyzacją procesów administracyjnych, w szczególności z wykorzystaniem narzędzi opartych na sztucznej inteligencji oraz zagadnieniom związanym z wdrażaniem rozwiązań technologicznych w administracji publicznej z perspektywy ochrony danych osobowych. Istotnym wątkiem dyskusji była sygnalizowana potrzeba uwzględniania zasad ochrony danych już na etapie projektowania systemów informatycznych, w tym przeprowadzania ocen ryzyka i ocen skutków dla ochrony danych. Wskazywano na konieczność zapewnienia przejrzystości procesów automatycznego przetwarzania danych oraz zachowania odpowiedniego nadzoru człowieka nad systemami wykorzystującymi sztuczną inteligencję. Zwrócono uwagę na potrzebę współpracy między instytucjami publicznymi oraz na rolę działań edukacyjnych w tym zakresie, w szczególności wymiany informacji na temat dobrych praktyk w obszarze bezpiecznego i odpowiedzialnego stosowania nowych technologii, co buduje zaufanie obywateli do administracji publicznej.

2) **Seminarium „Wyzwania w udzielaniu informacji publicznej. Jak pogodzić transparentność i ochronę danych osobowych?”, 25.06.2025 r. w Lublinie.**




Tematyka dotycząca udzielania informacji publicznej w kontekście przepisów o ochronie danych osobowych była przedmiotem dyskusji podczas tego wydarzenia, zaś panele tematyczne dotyczyły granic prawa dostępu do informacji publicznej oraz narzędzi ochrony danych, takich jak anonimizacja czy pseudonimizacja. W wystąpieniach akcentowano kwestie praktyczne związane z identyfikacją danych osobowych w dokumentach udostępnianych jako informacja publiczna, a także przedstawiano sposoby stosowania technicznych i proceduralnych środków, które pozwalają jednocześnie przestrzegać prawa do informacji publicznej i chronić prywatność obywateli. Podkreślano znaczenie właściwego stosowania tych narzędzi w celu zachowania równowagi między jawnością działań instytucji publicznych a ochroną danych osobowych.

3) **Seminarium „Rewolucja technologiczna w relacji z klientami - jak budować rozwiązania technologiczne w relacji z klientami", 2.10.2025 r. w Rzeszowie.**




Celem seminarium było omówienie zagadnień związanych z wykorzystaniem nowoczesnych technologii w relacjach z klientami oraz ich zgodnością z przepisami o ochronie danych osobowych. Program obejmował trzy panele tematyczne: „Personalizacja i prywatność: jak znaleźć równowagę w relacji z klientem?", „Nowoczesne technologie w obsłudze klienta: jak projektować zgodne z RODO procesy?" oraz „Praktyka a aspekty prawne w świetle rozwoju nowych technologii – wyzwania w kontakcie z klientami". W seminarium uczestniczyli eksperci Urzędu Ochrony Danych Osobowych, w tym przedstawiciele Społecznego Zespołu Ekspertów przy Prezesie UODO oraz ZUS, a także specjaliści z zakresu nowych technologii, sztucznej inteligencji i cyberbezpieczeństwa.

4) **Konferencja „Nowe wyzwania prawne: regulacje, zadania regulatorów i ochrona danych", 27.11.2025 r. w Warszawie.**




Wydarzenie miało na celu kompleksowe omówienie aktualnych i przyszłych problemów prawnych związanych z ochroną danych osobowych, z uwzględnieniem nowych regulacji, roli organów nadzorczych oraz wyzwań wynikających z rozwoju technologii. Podczas konferencji omówiono kwestie związane z najnowszymi aktami prawnymi w Unii Europejskiej oraz ich wpływ na praktykę ochrony danych. Podkreślano wagę rozumienia społecznego i technologicznego kontekstu korzystania z narzędzi, takich jak sztuczna inteligencja, co ma kluczowe znaczenie nie tylko dla prawidłowej implementacji różnych aktów prawnych, w tym AI Act, ale także dla właściwej oceny zgodności działań z zasadami ochrony danych. Dyskusje koncentrowały się na praktycznych wyzwaniach dotyczących współpracy organów nadzorczych w warunkach globalnej cyfryzacji i transgranicznych przepływów danych. Eksperci wskazywali na konieczność rozwijania mechanizmów współpracy w celu skutecznego reagowania na wyzwania związane z cyberprzestępczością i bezpieczeństwem informacji. Poruszono także kwestie związane z Konwencją Budapeszteńską i rolą rozporządzeń unijnych, które w zamierzeniu mają ułatwić działania regulatorów na arenie międzynarodowej, choć ich pełna implementacja i praktyczne stosowanie nadal stanowią wyzwanie. Nie zabrakło też prognoz dotyczących kierunków rozwoju otoczenia regulacyjnego oraz implikacji wynikających z nowych aktów prawnych. Eksperci zgodnie wskazywali, że ochrona danych osobowych w obecnym systemie prawnym znajduje się w ciągłym procesie dostosowywania do zmian technologicznych i społecznych, a dialog pomiędzy

regulatorami, przedsiębiorstwami i środowiskiem akademickim jest kluczowy dla efektywnego stosowania przepisów w praktyce.

### 1.4. 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.

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.

Wśród zadań kontynuowanych w 2025 roku przez Zespół była aktualizacja poradnika ds. zgłaszania naruszeń[657]. Wśród innych ważnych tematów podejmowanych w pracach SZE znalazła się kwestia zagrożenia cyberbezpieczeństwa, które jest nierozerwalnie związane z przetwarzaniem danych osobowych. Ochronę danych osobowych należy traktować jako istotny element systemu bezpieczeństwa i obronności kraju, dlatego Prezes UODO wraz z Zespołem analizuje propozycje rozwiązań w tym zakresie, w szczególności dotyczących analizy ryzyk, z którymi mogą spotkać się administratorzy w poszczególnych branżach.

W analizowanym 2025 roku członkowie Zespołu uczestniczyli w **43 wydarzeniach**, jak konferencje/seminaria, debaty i spotkania robocze, byli współorganizatorami 14 wydarzeń, odbyli 6 wykładów w ramach webinariów eksperckich, a także byli konsultantami różnych dokumentów. Społeczny Zespół uczestniczył też aktywnie w licznych panelach, debatach oraz wspierał merytorycznie Urząd przy organizowaniu cyklu akcji regionalnych „UODO rusza w kraj". Pełny wykaz aktywności Społecznego Zespołu Ekspertów jest opublikowany i na bieżąco aktualizowany w specjalnej zakładce na stronie internetowej UODO[658].

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[659]. Przewodniczącym Zespołu jest dr Mirosław Gumularz. Udział w pracach SZE ma charakter społeczny.

---

[657] https://uodo.gov.pl/pl/138/3561.
[658] https://uodo.gov.pl/pl/582.
[659] https://uodo.gov.pl/pl/138/3114. Skład Społecznego Zespołu Ekspertów został powiększony zarządzeniem Prezesa UODO z 23 stycznia 2025 r. o kolejnego członka, zaś w 2026 r. dołączył kolejny. W chwili obecnej Zespół liczy 17 członków.

## 1.5. Grupa robocza ds. sztucznej inteligencji

Podczas jubileuszowego spotkania Prezesa UODO i Społecznego Zespołu Ekspertów przy Prezesie UODO, które odbyło się 9 czerwca 2025 r., Zespół przedstawił sprawozdanie roczne ze swej działalności i ustalił priorytety przyszłych działań.

Podczas tego spotkania została powołana Grupa robocza ds. sztucznej inteligencji Społecznego Zespołu Ekspertów przy Prezesie UODO, w skład której wchodzi 11 członków. Przewodniczącym Grupy został dr Ireneusz Wochlik. Powołanie Grupy stanowi realizację jednego z kluczowych elementów przyjętego przez Prezesa UODO „Planu działań w zakresie wsparcia zgodnego z przepisami o ochronie danych osobowych projektowania i wdrażania systemów sztucznej inteligencji". Plan ten zakłada edukację, współpracę i wsparcie praktyczne dla budowy odpowiedzialnego systemu AI w Polsce, zgodnego z europejskimi standardami ochrony danych. Koordynatorem prac nad sztuczną inteligencją ze strony SZE został dr hab. Dominik Lubasz.

W obszarze zainteresowania nowo powstałej Grupy znajdują się takie kwestie, jak poprawa procesów zarządzania danymi, edukacja i szkolenia, pomoc dla sektorów problemowych (samorządy, medycyna, edukacja, nauka, kultura, małe i średnie przedsiębiorstwa). Działania Grupy skupią się także na rozwoju współpracy międzysektorowej, promowaniu innowacji, uświadamianiu o roli organu nadzorczego – zgodnie z wyzwaniami ujętymi m.in. w raportach Europejskiej Rady Ochrony Danych i w założeniach Strategii Cyfryzacji Polski do 2035 r. – w kontekście rozwoju i stosowania sztucznej inteligencji. Ponadto działania Prezesa UODO i SZE oraz Grupy obejmą opracowanie, wdrażanie i wykorzystywanie AI w organizacjach.

W składzie grupy roboczej znaleźli się eksperci zewnętrzni, reprezentujący różne dziedziny.

Pierwszym bardzo ważnym zadaniem podjętym przez Grupę we współpracy z SZE oraz ekspertami UODO, było opracowanie ankiety dotyczącej potrzeb instytucji i organizacji w obszarze wykorzystania sztucznej inteligencji oraz zapewnienia właściwej ochrony danych osobowych przy stosowaniu tej technologii. Celem tego badania była identyfikacja potrzeb administratorów w obszarze wykorzystania sztucznej inteligencji (SI) oraz oczekiwań związanych z zapewnieniem właściwej ochrony danych osobowych. W ankiecie udział wzięło 447 podmiotów, co świadczy o dużym zapotrzebowaniu rynku na działania ukierunkowane na ochronę danych osobowych w kontekście wykorzystania technologii sztucznej inteligencji i zaufaniu do Urzędu Ochrony Danych Osobowych.

Na podstawie wyników tego ogólnopolskiego badania powstał „Raport Strategiczny - Badanie potrzeb organizacji w zakresie wykorzystania sztucznej inteligencji i ochrony danych osobowych"[660], opracowany przez Grupę roboczą ds. sztucznej inteligencji. Badanie dostarcza pierwszego w Polsce przekrojowego obrazu gotowości instytucji publicznych i prywatnych do odpowiedzialnego wdrażania

[660] https://uodo.gov.pl/pl/file/7022.

sztucznej inteligencji zgodnie z RODO oraz AI Act. Pokazuje między innymi, że 17 proc. organizacji biorących udział w badaniu już korzysta ze sztucznej inteligencji. Pozostałe podmioty albo w ogóle nie korzystają z takich rozwiązań, albo są na etapie testów bądź planują ich wdrożenie.

Wyniki ankiety będą wsparciem dla działań edukacyjno-informacyjnych Urzędu Ochrony Danych Osobowych w odpowiedzialnym, zgodnym z prawem wdrażaniu narzędzi sztucznej inteligencji[661].

### 1.6. Współpraca z kościołami i związkami wyznaniowymi

Współpraca Prezesa UODO z niezależnymi organami nadzorczymi powołanymi na podstawie art. 91 RODO, od marca 2024 r. ulega dynamicznemu rozwojowi. Potwierdza to liczba wydarzeń z udziałem ekspertów UODO, opisanych w podrozdziale 1.14 części III niniejszego Sprawozdania oraz ujętych formie wykazu w załączniku nr 3.

Kluczowe znaczenie miało seminarium eksperckie „Aktualne wyzwania ochrony danych osobowych w związkach wyznaniowych w Polsce" (7.05.2025 r.) skierowane do wszystkich związków wyznaniowych funkcjonujących w naszym kraju. Efektem tego wydarzenia było zawarcie porozumienia pomiędzy Prezesem UODO a KIODO Polskiego Autokefalicznego Kościoła Prawosławnego o współpracy i wzajemnym przekazywaniu informacji (15.10.2025 r.). Wspomniane porozumienie to drugi tego typu dokument podpisany z kościołem. 7 maja 2019 roku podpisane zostało porozumienie Prezesa Urzędu Ochrony Danych Osobowych z Kościelnym Inspektorem Ochrony Danych reprezentującym Kościół katolicki.

Na szczególne wyróżnienie zasługuje współpraca Prezesa UODO **z KIOD Kościoła katolickiego**, w ramach której – oprócz wymiany informacji – podejmowane są również działania edukacyjne podnoszące świadomość w zakresie ochrony danych osobowych. Przykład - szkolenie dla Inspektorów Ochrony Danych zorganizowane przez Kościelnego Inspektora Ochrony Danych i Fundację Konferencji Episkopatu Polski Bona Fama we współpracy z Prezesem Urzędu Ochrony Danych Osobowych (6.05.2025 r.). Współpraca Prezesa UODO z KIOD Kościoła katolickiego wyróżnia się na tle innych organów nadzorczych w Unii Europejskiej. Na wyróżnienie zasługuje udział Głównego koordynatora ds. ochrony danych osobowych w Kościołach i związkach wyznaniowych w UODO w międzynarodowej konferencji naukowej „Axiology of the Legal System: Theory and Practice" (25-26.11.2025 r.) zorganizowanej przez Papieski Uniwersytet Gregoriański w Rzymie. Ekspert UODO przedstawił na konferencji podstawy prawne, cele i praktyczne aspekty współpracy Prezesa UODO i KIOD zorganizowanej na uczelni, która od wieków kształci duchownych z całego świata, w tym byłych Papieży Kościoła katolickiego.

Ponadto w 2025 r. Prezes UODO podjął współpracę naukową z Chrześcijańską Akademią Teologiczną w Warszawie poprzez organizację wizyty studyjnej w siedzibie

[661] Więcej informacji dotyczących zagadnień i wydarzeń związanych ze sztuczną inteligencją znaleźć można na stronie www.uodo.gov.pl w zakładce Sztuczna inteligencja: https://uodo.gov.pl/pl/p/sztuczna-inteligencja

Urzędu. Przytoczone przykłady świadczą o zwiększonym zainteresowaniu Kościołów i innych związków wyznaniowych tematyką ochrony danych osobowych i zapotrzebowaniem na praktyczne szkolenia z zakresu cyberzagrożeń i cyberhigieny. Ważne jest bowiem budowanie świadomości zarówno duszpasterzy, jak i wiernych – zwłaszcza młodzieży działającej w różnych organizacjach przykościelnych lub studiujących na uczelniach religijnych czy wydziałach teologicznych uczelni świeckich - a także członków stowarzyszeń i kół naukowych.

## 1.7. Szkolenia

### 1.7.1. Szkolenie Krajowego Punktu Kontaktowego programów Twinning i TAIEX dla UODO, 13.01.2025 r.

Radca generalny w Ministerstwie Spraw Zagranicznych i zarazem koordynator programów Twinning i TAIEX przeprowadził szkolenie dla pracowników UODO, podczas którego przedstawił procedurę składania wniosków oraz przygotowania oferty programowej przez Urząd. Omówił także kwestie związane z przebiegiem i realizacją umowy. Szkolenie wprowadzające otworzyło przez UODO możliwość nawiązania współpracy z instytucjami w Polsce, zaangażowanymi w realizację projektów twinningowych oraz TAIEX, po to by czerpać wiedzę z doświadczeń i najlepszych praktyk w celu tworzenia podstaw pod przyszłe projekty UODO w tym zakresie.

### 1.7.2. Szkolenia dla legislatorów RCL, 18.03.2025 r., 25.03.2025 r., 6.05.2025 r. oraz dla pracowników Biura RCL, 29.04.2025 r.

W 2025 r. eksperci Urzędu Ochrony Danych Osobowych przeprowadzili serię szkoleń z zakresu ochrony danych osobowych i wyzwań technologicznych dla Rządowego Centrum Legislacji. Ta inicjatywa to m.in. efekt porozumienia jakie zawarł Prezes UODO Mirosław Wróblewski z Prezes Rządowego Centrum Legislacji Joanną Knapińską. Celem współpracy jest wymiana doświadczeń i dobrych praktyk związanych z kształceniem prawników oraz upowszechnianie wiedzy o stanowieniu prawa, zwłaszcza dotyczącego ochrony danych osobowych i prywatności.

Tematyka szkoleń obejmowała zagadnienia dotyczące wpływu RODO na przepisy krajowe, ocenę skutków dla ochrony danych w procesie tworzenia przepisów prawa (projekty legislacyjne), a także przykłady dobrych praktyk oraz błędów przy wdrażaniu przepisów o ochronie danych osobowych w prawie krajowym. W zakresie wyzwań technologicznych omówiono realizację zasady poufności w praktyce RCL oraz zwrócono uwagę na wagę współpracy legislatorów z innymi podmiotami w procesie analizy ryzyka dla ochrony danych osobowych przy wykorzystaniu algorytmów sztuczej inteligencji w legislacji. Natomiast pracownicy Biura RCL na szkoleniu uzyskali wiedzę na temat ochrony danych osobowych w organizacji pracy, analizowali przyczyny najczęstrzych naruszeń ochrony danych na wybranych przykładach oraz ich konsekwencje.

Odbyły się trzy spotkania, w tym dwa szkolenia dla legislatorów RCL i jedno dla pracowników Biura RCL. Uczestniczyło w nich 110 osób – 86 legislatorów i 24 pracowników Biura.

Z kolei eksperci RCL przeprowadzili szkolenie dla pracowników UODO zajmujących się legislacją na temat technik prawodawczych. Tytuł szkolenia „ABC zasad techniki prawodawczej" (5.03.2025 r.).

### 1.7.3. Szkolenia dla legislatorów Polskiego Towarzystwa Legislacji (PTL), 3.04.2025 r., 15.04.2025 r. oraz 12.05.2025 r.

Cykl szkoleń UODO dla legislatorów PTL zainaugurowało wystąpienie Prezes Polskiego Towarzystwa Legislacji Ewy Kossakowskiej i Zastępczyni Prezesa UODO Agnieszki Grzelak, podczas warsztatów z zakresu ochrony danych osobowych, które odbyły się w Biurze RPO (3.04.2025 r.). Tematyka szkoleń obejmowała orzecznictwo TSUE i ETPCz w odniesieniu do ochrony prywatności i danych osobowych, wpływ RODO na przepisy krajowe, zasady ochrony danych w projektach legislacyjnych oraz wpływ nowych technologii na proces stanowienia prawa. Omówione zostały przykłady dobrych praktyk oraz błędów przy projektowaniu przepisów oraz podkreślono wagę współpracy legislatorów z innymi podmiotami na rzecz dobrej legislacji.

Szkolenia z zakresu ochrony danych osobowych to wynik porozumienia podpisanego 16 stycznia 2025 r. o współpracy Urzędu Ochrony Danych Osobowych z Polskim Towarzystwem Legislacji.

### 1.7.4. Szkolenie dla kościelnych inspektorów ochrony danych, 6.05.2025 r.

Organizatorami szkolenia dla kościelnych inspektorów ochrony danych osobowych, które we współpracy z Prezesem UODO obyło się 6 maja 2025 r. w siedzibie Caritas, byli Kościelny Inspektor Ochrony Danych i Fundacja Konferencji Episkopatu Polski Bona Fama. Podczas tego spotkania pracownicy UODO przedstawili najnowszy poradnik Urzędu dotyczący zgłaszania naruszeń (wersja z lutego 2025 r.), a także wygłosili prelekcje o przetwarzaniu danych osobowych w mediach społecznościowych przez instytucje i podmioty kościelne oraz o ujawnianiu danych z postępowań kościelnych. Była to okazja do zapoznania się z problematyką funkcjonowania tych podmiotów na styku prawa wewnątrzkościelnego i prawa powszechnie obowiązującego w Polsce.

Szkolenie było efektem porozumienia o współpracy i wzajemnym przekazywaniu informacji zawartego pomiędzy Prezesem UODO i KIOD w 2019 r. w zakresie działań edukacyjnych, promujących godność człowieka zgodnie z nauczaniem Kościoła, ochronę danych osobowych i realizację obowiązków wynikających z prawa kościelnego i świeckiego.

### 1.7.5. Szkolenie UODO dla NIL, online, 17.06.2025 r.

W nawiązaniu do podpisanego porozumienia Prezesa UODO z Prezesem Naczelnej Rady Lekarskiej, Urząd Ochrony Danych Osobowych przeprowadził online szkolenie w ramach NIL IN – Sieci Lekarzy Innowatorów. Spotkanie to odbywało się w ramach tzw. „Wtorków z Innowacjami" – cyklu otwartych szkoleń skierowanych do lekarek, lekarzy oraz wszystkich członków społeczności NIL IN. Projekt ten współtworzony jest z Centralnym Ośrodkiem Badań, Innowacji i Kształcenia (COBIK

NIL) działającym przy Naczelnej Izbie Lekarskiej. Celem jest dostarczanie wiedzy na temat nowych technologii i innowacji w medycynie oraz wspieranie tych, którzy chcą kształtować jej przyszłość. 17 czerwca 2025 r. szkolenie na temat: „Wyzwań prawnych stojących przed wtórnym przetwarzaniem danych osobowych, w szczególności dla celu badań naukowych w EHDS" poprowadził ekspert UODO.

### 1.7.6. V Warsztaty Szkoleniowe pt. „Spotkania z RODO". Poznań, 16.10.2025 r.

Warsztaty zostały zorganizowane przez e-OSM Consulting Sp. z o.o. z myślą o praktykach ochrony danych osobowych i bezpieczeństwa informacji. Tematyka prelekcji skupiała się na aktualnych wyzwaniach związanych z cyfryzacją, sztuczną inteligencją, bezpieczeństwem informacji oraz stosowaniem przepisów RODO - ze szczególnym uwzględnieniem sektora finansowego. Kanwą wystąpienia eksperta UODO był artykuł pt. „Jaka jest rola IOD w odniesieniu do oceny skutków dla ochrony danych". Wystąpienie otwierające wygłosił Mirosław Wróblewski, Prezes UODO. Podczas tego wydarzenia poruszono również zagadnienia monitoringu wizyjnego w kontekście ochrony danych osobowych, sztucznej inteligencji w odniesieniu do wymagań RODO, retencji danych oraz cyberbezpieczeństwa.

### 1.7.7. Szkolenie koordynatorów Programu „Twoje dane – Twoja sprawa", 22–23.10.2025 r.

Cyklicznymi szkoleniami organizowanymi od 16 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 22–23.10.2025 r. rozpoczęło jego XVI edycję. W trakcie dwóch dni konferencji uczestnicy wysłuchali wystąpień ekspertów ds. sztucznej inteligencji i edukacji oraz liderów programu „Twoje dane – Twoja sprawa", którzy od lat biorą w nim udział i z zaangażowaniem dzielą się swoimi doświadczeniami oraz wiedzą. Motywem przewodnim XVI edycji Programu była ochrona danych osobowych w dobie dynamicznego rozwoju nowych technologii, ze szczególnym uwzględnieniem sztucznej inteligencji.

### 1.7.8. Szkolenie dla NRA, online, 8.12.2025 r.

Zasady przetwarzania danych klientów kancelarii adwokackich i ich pracowników w świetle RODO oraz wyzwania wynikające z wprowadzania nowych technologii w pracy kancelarii, były głównym tematem szkolenia UODO dla przedstawicieli Naczelnej Rady Adwokackiej. Podczas szkolenia przedstawione zostały przykłady naruszeń ochrony danych osobowych oraz omówiono sposoby, jak im skutecznie zaradzić. Uczestnicy szkolenia dowiedzieli się też, jak przebiega proces kontroli przetwarzania danych osobowych w podmiotach i jak się do niej przygotować.

Podsumowaniem tego wydarzenia była prezentacja dotycząca międzynarodowych kontaktów kancelarii adwokackich, które powinny przebiegać z zachowaniem przepisów RODO.

### 1.7.9. Szkolenie dla pracowników Krajowego Biura Wyborczego, online, 12.12.2025 r.




Szkoleniem zorganizowanym 12 grudnia 2025 r. dla pracowników Krajowego Biura Wyborczego i jego delegatur z terenu, zainaugurowany został cykl szkoleń dla pracowników biur poselskich i senatorskich oraz biur partii politycznych, które odbyły się już w nadchodzącym 2026 r. Intencją tego przedsięwzięcia były odnotowane liczne przypadki ujawniania danych osób fizycznych podczas kampanii wyborczej. Mając na uwadze dynamikę procesu związanego z wyborami, towarzyszące mu emocje, jego ogromny zasięg w związku z organizacją wyborów zarówno na obszarze RP, jak również poza granicami naszego kraju, Prezes UODO Mirosław Wróblewski uznał za konieczne przypomnienie członkom komitetów wyborczych i pracownikom biur, podstawowe zasady ochrony danych osobowych i prawa do prywatności, które powinny być przestrzegane w kampanii wyborczej. Upublicznienie danych osobowych obywateli niepełniących funkcji publicznych może mieć daleko idące konsekwencje dla tych osób, ze względu na wspomniany zasięg kampanii wyborczej i możliwość niekontrolowanego rozpowszechnienia ujawnionych danych w sferze cyfrowej. Dodatkowo, zainteresowanie opinii publicznej przypadkami naruszeń ochrony danych oraz kierowane do Urzędu Ochrony Danych Osobowych pytania od przedstawicieli mediów, co do podjętych przez organ kroków, dodatkowo skłoniły Prezesa UODO do podjęcia decyzji o konieczności zintensyfikowania działań edukacyjnych przypominających o zasadach ochrony danych i prawa do prywatności w przebiegu kampanii wyborczej. W sumie przeszkolonych miało zostać 1300 osób.

Podczas szkolenia dla pracowników biura KBW i jego delegatur poruszono tematy związane z bezpiecznym przetwarzaniem danych osobowych podczas procesu wyborczego, prezentując obszary największego ryzyka dla ochrony danych osobowych. Zwrócono uwagę między innymi na kwestie monitoringu wizyjnego

w lokalach wyborczych, który nie zawsze jest skutecznie wyłączany, powoływania inspektorów ochrony danych przez komitety wyborcze, a także przedstawiono mechanizmy sprawnego wykrywania i obsługi naruszeń.

## 1.8. Projekty, programy

### 1.8.1. Ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa”

#### 1) XV edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa” w roku szkolnym 2024/2025 oraz rozpoczęcie XVI edycji w roku szkolnym 2025/2026.

Program „Twoje dane – Twoja sprawa” jest największym ogólnopolskim przedsięwzięciem edukacyjnym Prezesa Urzędu Ochrony Danych Osobowych, realizowanym w sposób systemowy. Uczestniczą w nim szkoły podstawowe, ponadpodstawowe oraz placówki doskonalenia nauczycieli.

Celem Programu jest wspieranie uczniów i pedagogów w zdobywaniu oraz rozwijaniu praktycznych umiejętności w obszarze ochrony danych osobowych, prawa do prywatności oraz kompetencji cyfrowych, niezbędnych we współczesnym świecie. Stanowi źródło wiedzy i dobrych praktyk dla kadry pedagogicznej 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.

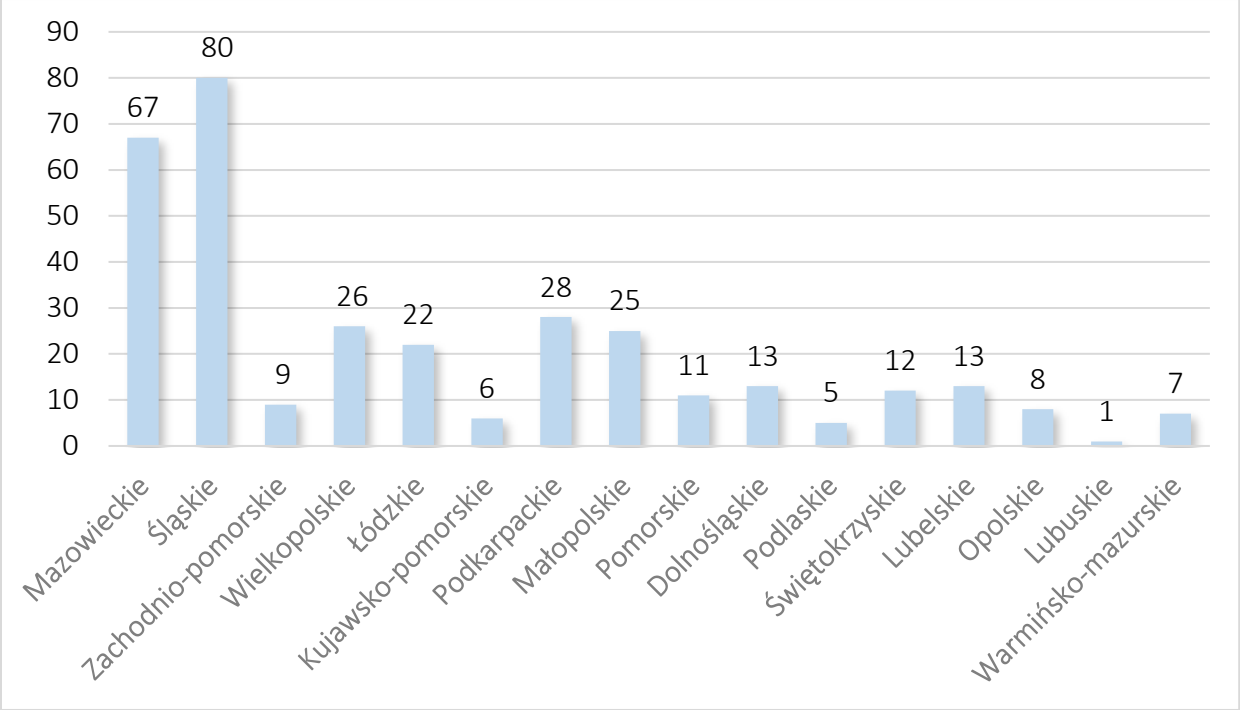
W roku 2025 Urząd Ochrony Danych Osobowych realizował XV edycję Programu i rozpoczął jego XVI edycję. Każda z nich organizowana jest zgodnie z kalendarzem roku szkolnego.

## 2) XV edycja programu „Twoje dane – Twoja sprawa” – rok szkolny 2024/2025




XIV edycja programu edukacyjnego „Twoje dane – Twoja sprawa” była realizowana pod hasłem ochrony wizerunku dzieci i młodzieży. Koncentrowała się na edukacji dzieci i młodzieży w obszarze ochrony prywatności i danych osobowych w mediach społecznościowych, ze szczególnym uwzględnieniem zagadnień dotyczących ochrony wizerunku najmłodszych. Wizerunek stanowi bowiem element danych osobowych i podlega szczególnej ochronie oraz poszanowania ze strony rówieśników i osób dorosłych odpowiedzialnych za bezpieczeństwo młodych ludzi.

W roku szkolnym 2024/2025, w XV edycji Programu, udział wzięły 352 placówki oświatowe, w tym 221 szkół podstawowych, 127 szkół ponadpodstawowych oraz 4 placówki doskonalenia nauczycieli. Rekrutacja uczestników rozpoczęła się 1 września 2024 r. i trwała do końca października. Najwięcej zgłoszeń wpłynęło z województwa śląskiego (80) oraz mazowieckiego (67).




**Wykres 21:** Liczba placówek biorących udział w XV edycji Programu „Twoje dane – Twoja sprawa” z podziałem na województwa.

- liczba zrealizowanych inicjatyw edukacyjnych – 6 213, w tym 4 378 lekcji poświęconych ochronie danych osobowych i prywatności;
- liczba uczniów biorących udział w zajęciach – 61 348,
- liczba przeszkolonych nauczycieli – 3 630,
- liczba nauczycieli zaangażowanych w działania – 2 291.

### 3) Cykl webinariów

W roku szkolnym 2024/25 kontynuowano organizację zajęć edukacyjnych dla dzieci, młodzieży i koordynatorów Programu. W 2025 r. w ramach Programu przeprowadzono w formie online 5 ogólnopolskich spotkań, których niekwestionowanym atutem jest formuła zdalna oraz różnorodność tematów podkreślających rolę ochrony prywatności i danych osobowych w codziennym życiu, w szczególności w kontekście zagadnień związanych ze sztuczną inteligencją. Spotkania odbywały się w podziale na **#ODOlekcje**, kierowane do uczniów oraz **RODO w szkolnej ławce**, które były skierowane do dorosłych odbiorców – w zależności od tematyki: do rodziców, nauczycieli lub dyrektorów. Tematyka i sposób realizacji lekcji dostosowane były do wieku i potrzeb uczniów oraz aktualnych trendów. Zajęcia prowadzili eksperci UODO, przedstawiciele zaproszonych instytucji oraz liderzy Programu.

- „RODO w szkolnej ławce. Świadomość rodzica i dobre wsparcie dla dziecka – ważne informacje o danych osobowych i prywatności w cyfrowym świecie". Otwarta lekcja (8.01.2025 r.);
- ODOlekcja „Naruszenie prywatności w mediach społecznościowych – mediacje jako sposób rozwiązywania konfliktów" (5.03.2025 r.);
- „RODO w szkolnej ławce. Bieżące tematy związane z ochroną danych osobowych w sektorze oświaty" (21.03.2025 r.);
- „Webinarium o naruszeniach ochrony danych osobowych. Omówienie zagadnienia w kontekście aktualizacji poradnika UODO". Webinarium otwarte (28.03.2025 r.);
- ODOlekcja „Cyfrowy ślad – jak mądrze chronić wizerunek?" (2.04.2025 r.).

### 4) Cykl porad „Warto wiedzieć" dla uczestników Programu

Adresatami cyklu porad „Warto wiedzieć" są uczniowie, nauczyciele oraz rodzice. Treści z założenia są opracowane w krótkiej i zrozumiałej formie, dostosowanej do potrzeb grupy docelowej. W 2025 roku przygotowane materiały obejmowały następującą tematykę:

- „Bezpieczeństwo w cyfrowym świecie. Jak dbać o prywatność w internecie?" (28.01.2025 r.);
- „Świadomość rodzica to dobre wsparcie dla dziecka. Jak wspierać dzieci w ochronie prywatności?" (28.01.2025 r.),
- „AI w placówkach oświatowych a dane osobowe. Jak chronić dane osobowe w edukacji w dobie rozwoju sztucznej inteligencji?" (27.02.2025 r.);
- „Ochrona prywatności i mediacja w konfliktach" (28.03.2025 r.);
- „Cyfrowy ślad - co warto o nim wiedzieć i jak go kontrolować?" (28.04.2025 r.);
- „Jak na co dzień dbać o prawa człowieka swoje i innych?" (10.12.2025 r.).

Systematyczne udostępnianie materiałów edukacyjnych pozwala uczestnikom Programu na zdobywanie aktualnej wiedzy na temat ochrony danych osobowych oraz

bezpiecznego korzystania z nowych technologii. Materiały porad wykorzystywano podczas zajęć z uczniami, spotkań z rodzicami, przy tworzeniu gazetek szkolnych, a także publikowano na stronach internetowych szkół.

### 5) Dodatkowe inicjatywy edukacyjne UODO w ramach XV edycji programu „Twoje dane – Twoja sprawa”

W ramach XV edycji programu „Twoje dane – Twoja sprawa” zrealizowano różnorodne działania edukacyjne oraz promocyjne, których celem było podniesienie poziomu świadomości społecznej w obszarze ochrony danych osobowych.

Kuratoria oświaty wsparły działania promocyjne XV edycji mające na celu skierowanie informacji na temat Programu do jak największej liczby szkół. Dzięki współpracy z Urzędem m.st. Warszawy oraz Urzędem Miasta Krakowa emitowano na ekranach komunikacji miejskiej materiały promocyjne.

Program „Twoje dane – Twoja sprawa” od wielu lat jest realizowany pod patronatem Ministra Edukacji. Współpraca z Ministerstwem Edukacji Narodowej doprowadziła do **rozszerzenia podstaw programowych kształcenia ogólnego o zagadnienia związane z ochroną danych osobowych, które od 1 września 2025 roku zostały włączone do kolejnych przedmiotów. Zagadnienia związane z ochroną danych osobowych i prywatności oraz zasadami zachowania higieny cyfrowej będą omawiane nie tylko na lekcjach informatyki i etyki, ale także w ramach edukacji zdrowotnej i obywatelskiej.**

Istotnym elementem Programu jest współpraca z Rzecznikiem Praw Dziecka, obejmująca wspólne inicjatywy edukacyjne i badawcze dotyczące ochrony danych osobowych dzieci i młodzieży. Organizowane wspólnie działania mają na celu wzmacnianie podmiotowości dzieci oraz ochronę ich praw w obszarze ochrony prywatności i przetwarzania danych osobowych. W 2025 roku współpraca dotyczyła szczególnie ochrony wizerunku dzieci. Prezes UODO wspiera inicjatywy wzmacniające świadomość cyfrową najmłodszych, ich rodziców oraz instytucji odpowiedzialnych za bezpieczeństwo najmłodszych.

Ważnym krokiem w dalszym rozwoju Programu było podpisanie 23 maja 2025 roku porozumienia o współpracy pomiędzy Prezesem Urzędu Ochrony Danych Osobowych a Prezeską Fundacji Polskich Linii Lotniczych. Współpraca obejmuje realizację inicjatyw edukacyjnych, których celem jest rozwijanie kompetencji społecznych związanych z bezpiecznym podróżowaniem, ochroną prywatności i danych osobowych oraz zwiększanie świadomości różnych grup społecznych w tym zakresie.

W ramach Programu podejmowana była również współpraca oraz konsultacje z placówkami doskonalenia nauczycieli m.in. z Ośrodkiem Rozwoju Edukacji oraz Warszawskim Centrum Innowacji Edukacyjno-Społecznych i Szkoleń. Celem współpracy z tymi podmiotami była realizacja działań na rzecz doskonalenia systemu oświaty i podnoszenia jakości edukacji w obszarze kształcenia.

Dzięki współdziałaniu z różnorodnymi instytucjami, organizacjami i placówkami oświatowymi program „Twoje dane – Twoja sprawa” stanowi trwały fundament

budowania rzeczywistości, w której młodzi ludzie świadomie i odpowiedzialnie podchodzą do ochrony swoich danych osobowych, zarówno w przestrzeni cyfrowej, jak i w życiu codziennym. Realizowane w ramach Programu szkolenia, udostępniane materiały dydaktyczne, webinaria oraz merytoryczne wsparcie ekspertów UODO sprzyjają pogłębianiu wiedzy i rozwojowi kompetencji pracowników placówek biorących udział w inicjatywie.

Ponadto szkoły zaangażowały się w obchody Dnia Ochrony Danych Osobowych, organizując w okresie styczeń–luty 2025 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 oraz lokalnej społeczności. Uczniowie przygotowali także materiały edukacyjne, takie jak gazetki szkolne, prezentacje multimedialne oraz teksty literackie, poruszające tematykę ochrony danych osobowych i bezpieczeństwa w sieci. W sumie uczestnicy Programu zorganizowali 449 inicjatyw. Ich wykaz jest dostępny na stronie internetowej Urzędu Ochrony Danych Osobowych pod adresem: https://uodo.gov.pl/pl/587/3796.

### 6) „UODO rusza w kraj”

W ramach spotkań wojewódzkich „UODO rusza w kraj” zorganizowano konferencje, w których udział wzięli również uczestnicy Programu. Spotkania odbyły się 30 stycznia 2025 r. w Zespole Szkół nr 1 im. Stanisława Staszica w Kwidzynie oraz 21 marca 2025 r. w Szkole Podstawowej nr 17 im. 21 Brygady Strzelców Podhalańskich w Rzeszowie.

Eksperci UODO, przedstawiciele szkół, jednostek samorządu terytorialnego oraz mieszkańcy dyskutowali o kluczowych wyzwaniach i dobrych praktykach w zakresie ochrony danych osobowych najmłodszych.

### 7) Promocja Programu oraz propagowanie wiedzy o ochronie danych osobowych podczas różnorodnych wydarzeń

Materiały informacyjne i edukacyjne Programu „Twoje dane – Twoja sprawa” były udostępniane podczas różnorodnych wydarzeń organizowanych i współorganizowanych przez Urząd Ochrony Danych Osobowych:

- „UODO rusza w kraj” (Trójmiasto, 30-31.01.2025 r.),
- „UODO rusza w kraj” (Rzeszów, 20-21.03.2025 r.),
- „UODO rusza w kraj” (Poznań, 20-21.05.2025 r.),
- Konferencja „Profilaktyka przyszłości naszych dzieci w erze cyfrowej” (2.06.2025 r.),
- Konferencja „Uwaga! Smartfon” (Lublin, 4.06.2025 r.),
- Festiwal Pol&Rock (Czaplinek-Broczyno, 30.07.2025 - 2.08.2025 r.),
- „Turniej Wsi Gminy Skierniewice" (3.08.2025 r.) w Szkole Podstawowej w Miedniewicach,

- Piknik Edukacyjny (27.09.2025 r.) w Zespole Szkół im. Krzysztofa Kamila Baczyńskiego w Tłuszczu,
- Konferencja UODO „Bezpieczne dane dzieci i młodzieży oraz nowe kierunki rozwoju w obszarze kultury fizycznej. Jak sprostać współczesnym wyzwaniom?” (Kraków, 10.10.2025 r.),
- „UODO rusza w kraj” (Olsztyn, 16-17.10.2025 r.),
- Kongres Dzieci i Młodzieży organizowany przez Rzeczniczkę Praw Dziecka (Warszawa, 15-16.12.2025 r.).

## 8) Konkursy i podsumowanie XV edycji Programu




Celem konkursów było upowszechnienie wiedzy o ochronie danych osobowych i prawa do prywatności wśród uczniów i nauczycieli oraz popularyzacja działań edukacyjnych na rzecz ochrony danych osobowych i prywatności dzieci. Konkursy w ramach XV edycji Programu zostały ogłoszone 28 stycznia 2025 r. Zgłoszono do nich 7 inicjatyw oraz 149 prac uczniów w formie komiksów. Nadesłane prace pokazały, jak istotną rolę odgrywają działania edukacyjne, które nie tylko przybliżają prawa wynikające z RODO, lecz także rozwijają umiejętność współdziałania, wzajemny szacunek oraz kształtują poczucie odpowiedzialności za siebie i innych. W konkursach skierowanych do uczniów pod hasłem „Superbohaterowie prywatności” oraz „Dzień z życia danych osobowych”, nagrodzono prace ukazujące praktyczne sposoby dbania o bezpieczeństwo danych osobowych. W roku szkolnym 2024/2025 statuetkę „Złotego Pióra” oraz I miejsce w konkursie na najlepszą inicjatywę edukacyjną otrzymał Zespół Szkół nr 1 im. Stanisława Staszica w Kwidzynie za projekt warsztatów połączonych z opracowaniem gry planszowej „Odoland. Gra o Twoje dane osobowe”. Drugie miejsce zajęła Szkoła Podstawowa im. Jana Brzechwy w Świbie za organizację „II Międzyszkolnego konkursu wiedzy o ochronie danych osobowych, bezpieczeństwie w sieci, prawach autorskich i AI na sportowo”, przygotowanego z okazji Dnia Ochrony Danych Osobowych. Trzecie miejsce przypadło Szkole Podstawowej Specjalnej z Oddziałami Przedszkolnymi nr 7 w Rybniku za projekt warsztatów edukacyjnych „Dane osobowe – informacje o Tobie”. Najlepsze autorskie scenariusze zajęć zostały włączone do bazy materiałów edukacyjnych Programu.

Uroczyste wręczenie nagród w konkursach odbyło się 27 maja 2025 r. w Centrum Konferencyjnym Lotniska Chopina w Warszawie i stanowiło zwieńczenie XV edycji Programu. Wydarzenie było okazją do podsumowania roku intensywnej i owocnej współpracy oraz zaprezentowania najciekawszych i najbardziej wartościowych praktyk edukacyjnych. Jednocześnie zwrócono uwagę na ważne wyzwania związane z ochroną prywatności dzieci i młodzieży w realiach cyfrowego

świata. W uroczystości uczestniczyły przedstawicielki patronów honorowych Programu – Ministerstwa Edukacji Narodowej oraz Biura Rzeczniczki Praw Dziecka. Nagrody wręczyły: prof. Agnieszka Grzelak, Zastępczyni Prezesa UODO, Katarzyna Lubnauer, Wiceministra Edukacji, Anna Figurniak, Dyrektorka Generalna Biura Rzeczniczki Praw Dziecka oraz Katarzyna Hernandez, Dyrektorka Zespołu Edukacji Cyfrowej i Bezpieczeństwa w Sieci w Biurze Rzeczniczki Praw Dziecka.

### 9) Tytuł Inicjatywy Edukacyjnej Roku

Program został uhonorowany tytułem Inicjatywy Edukacyjnej Roku. To wyjątkowe wyróżnienie przyznawane jest przez Kapitułę Konkursu Nauczyciel Roku, w której zasiadają dotychczasowi laureaci konkursu organizowanego od 24 lat przez „Głos Nauczycielski" we współpracy z Ministerstwem Edukacji Narodowej. Tytuł Inicjatywy Edukacyjnej Roku przyznawany jest instytucjom i organizacjom prowadzącym szczególnie istotne działania na rzecz edukacji i młodzieży. Stanowi potwierdzenie, że program „Twoje dane – Twoja sprawa" odpowiada na rzeczywiste wyzwania współczesnej szkoły oraz skutecznie wspiera nauczycieli w realizacji ich misji edukacyjnej. Uroczyste wręczenie nagród odbyło się 7 października 2025 r. na Zamku Królewskim w Warszawie, podczas gali finałowej konkursu Nauczyciel Roku 2025.



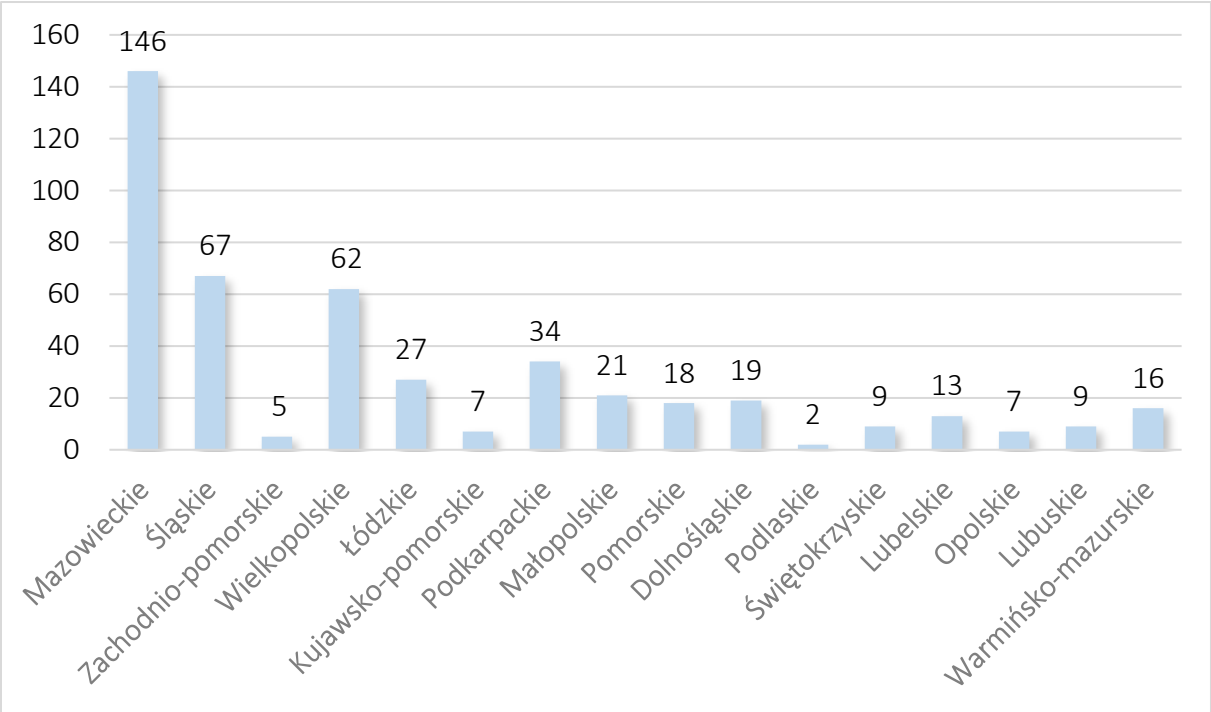

### 10) Udział w posiedzeniach Sejmowej Komisji do Spraw Dzieci i Młodzieży

Prezes Urzędu Ochrony Danych Osobowych stawia na pierwszym miejscu ochronę praw dzieci do prywatności i bezpieczeństwa w cyberprzestrzeni. Współpraca UODO z Sejmową Komisją do Spraw Dzieci i Młodzieży koncentruje się na wzmacnianiu ochrony prywatności i danych osobowych najmłodszych, szczególnie w środowisku cyfrowym. Obejmuje ona wymianę wiedzy eksperckiej, udział przedstawicieli UODO w posiedzeniach komisji oraz wspólne działania na rzecz edukacji i kształtowania bezpiecznych standardów prawnych i społecznych dla dzieci i młodzieży. Urząd Ochrony Danych Osobowych angażuje się w posiedzenia komisji, które mają związek również z tematami poruszanymi podczas trwania Programu, takimi jak uzależnienie dzieci i młodzieży od gier online, ochrony wizerunku małoletnich w przestrzeni cyfrowej, ochroną przed technologią deepfake'ów, a także wskazują na konieczność kompleksowego uregulowania kwestii sharentingu i ogólnie – aktywności dzieci w internecie.

### 11) XVI edycja programu „Twoje dane – Twoja sprawa", rok szkolny 2025/2026

Do XVI edycji Programu przystąpiło 485 placówek oświatowych, w tym 342 szkoły podstawowe, 135 szkół ponadpodstawowych oraz 8 placówek doskonalenia

nauczycieli. Najwięcej uczestników pochodziło z województwa mazowieckiego (146 placówek).




**Wykres 22:** Liczba placówek biorących udział w XVI edycji Programu „Twoje dane – Twoja sprawa" z podziałem na województwa.

Dwudniową konferencją szkoleniową online pt. „Prywatność i sztuczna inteligencja w edukacji" (22-23.10.2025 r.) zainaugurowana została XVI edycja Programu. Wydarzenie miało charakter otwarty i dostępny dla wszystkich osób zainteresowanych. Do wystąpienia podczas konferencji zostali zaproszeni między innymi przedstawiciele patronów honorowych Programu, Monika Horna – Cieślak, Rzeczniczka Praw Dziecka oraz Katarzyna Lubnauer, sekretarz stanu w Ministerstwie Edukacji Narodowej. Zaproszenie do udziału w konferencji przyjęła również posłanka Monika Rosa, przewodnicząca Sejmowej Komisji ds. Dzieci i Młodzieży oraz Joanna Bochniarz, prezeska Fundacji Polskich Portów Lotniczych. W trakcie dwóch dni konferencji uczestnicy mieli okazję wysłuchać wystąpień ekspertów ds. sztucznej inteligencji i edukacji oraz liderów programu „Twoje dane – Twoja sprawa", którzy od lat biorą w nim udział i z zaangażowaniem dzielą się swoimi doświadczeniami oraz wiedzą. Motywem przewodnim XVI edycji Programu była ochrona danych osobowych w dobie dynamicznego rozwoju nowych technologii, ze szczególnym uwzględnieniem sztucznej inteligencji. Materiały i proponowane działania edukacyjne miały na celu przekazanie praktycznych wskazówek, w jaki sposób świadomie i odpowiedzialnie korzystać z narzędzi opartych na sztucznej inteligencji, jak dbać o swój wizerunek, chronić dane i informacje wrażliwe, a także jak podejmować przemyślane decyzje przy wyborze aplikacji i rozwiązań cyfrowych.

Szczegóły XVI edycji programu „Twoje dane – Twoja sprawa” zostaną opisane w następnym roku sprawozdawczym.

### 12) Podsumowanie i wnioski

Program „Twoje dane – Twoja sprawa” jest inicjatywą, która przyczynia się do podniesienia świadomości na temat ochrony danych osobowych, wzrostu zainteresowania tematem ochrony prywatności w życiu każdego człowieka oraz do kształtowania postaw odpowiedzialnego korzystania z technologii wśród młodego pokolenia**.** Dzięki temu Programowi wzrasta świadomość uczniów w zakresie ich praw związanych z ochroną danych osobowych oraz umiejętność wykorzystania zdobytej wiedzy w praktyce. Program stwarza ponadto możliwości rozwoju kompetencji nauczycieli, zapewnia dostęp do aktualnych i wiarygodnych informacji, a także sprzyja wymianie doświadczeń oraz dobrych praktyk z ekspertami.

Inicjatywy podejmowane w ramach Programu miały zróżnicowany zakres zagadnień, często wykraczający poza obowiązującą podstawę programową i cieszyły się dużym zainteresowaniem wśród uczestników. Oferta edukacyjna była dostosowana do uczniów w różnym wieku, o różnych zainteresowaniach oraz uwzględniała również uczniów ze szczególnymi potrzebami. W zajęciach uczestniczyło ponad 60 000 uczniów, natomiast blisko 6 000 nauczycieli zostało przeszkolonych i aktywnie włączyło się w realizację działań. Zorganizowano ponad 4 000 lekcji oraz wiele innych przedsięwzięć popularyzujących wiedzę na temat ochrony danych osobowych. Najciekawsze inicjatywy zostały wyróżnione w konkursach organizowanych przez Prezesa UODO.

Praktyczne podejście do zajęć oraz możliwość wymiany doświadczeń zostało docenione wśród uczestników, którzy dzięki udziałowi w Programie zdobyli użyteczną wiedzę z zakresu ochrony danych osobowych. Nauczyciele zwracali uwagę na istotną rolę edukacji dotyczącej ochrony danych osobowych oraz deklarowali zamiar kontynuacji udziału w Programie w kolejnych latach. Realizacja Programu wpływa na zmianę postaw uczestników, którzy stają się bardziej świadomi i odpowiedzialni w kwestii ochrony prywatności.

Program przyczynia się również do zwiększenia zaangażowania nauczycieli w prowadzenie innowacyjnych i atrakcyjnych zajęć z uczniami, poświęconych ochronie prywatności. Kontynuacja programu „Twoje dane -Twoja sprawa” w kolejnych latach, umożliwi dalsze podnoszenie świadomości społecznej w zakresie ochrony danych osobowych.

## 1.8.2. Współpraca z francuskim organem nadzorczym - CNIL

W styczniu 2025 r. CNIL przekazał Urzędowi Ochrony Danych Osobowych informację o pozytywnej decyzji Komisji Europejskiej dla finansowania projektu **aplikacji FantomApp**. UODO współpracuje z CNIL w sprawie jej polskiej wersji. FantomApp to aplikacja edukacyjna dla młodzieży, skierowana do osób w wieku od 10 do 15 lat, ale dostępna jest też dla wszystkich zainteresowanych. Aplikacja została sfinansowana przez Unię Europejską w ramach programu „Obywatele, Równość,

Prawa i Wartości" (CERV). Osiem europejskich organów ochrony danych wyraziło zainteresowanie projektem i poparło go, w tym Prezes UODO.

FantomApp to: narzędzia i samouczki, które pomogą młodzieży chronić konta i „uporządkować" obecność w sieci, porady i treści, które pomogą w razie jakichkolwiek problemów, bezpłatna i bezpieczna aplikacja, która nie zbiera żadnych danych (oprócz adresu IP, który jest niezbędny do działania aplikacji i rodzaju używanego urządzenia). Aplikację FantomApp w wersji polskiej będzie można pobrać bezpłatnie ze sklepów App Store i Google Play. Aktualnie dostępna jest w wersji francuskiej i angielskiej: www.fantomapp.org.

Treści aplikacji FantomApp zostaną przetłumaczone i dostosowane do języków krajów partnerskich, co umożliwi jak największej liczbie młodych Europejczyków skuteczniejszą ochronę swojej prywatności. Wdrożenie polskiej wersji aplikacji, dostosowanej na potrzeby użytkowników w Polsce, planowane jest w 2026 r.

### 1.8.3. Projekt wizyt studyjnych dotyczący Aktu w sprawie zarządzania danymi (DGA)

W marcu 2025 r. Urząd Ochrony Danych Osobowych otrzymał pozytywną decyzję ze strony Komisji Europejskiej w sprawie finansowania projektu **„Data Governance Act implementation – study visit project"** w ramach inicjatywy flagowej PACE (Public Administration Cooperation Exchange – Wymiana w zakresie współpracy w administracji publicznej) Instrumentu Wsparcia Technicznego (Technical Support Instrument – TSI). Realizacja projektu obejmuje organizację dwóch wizyt studyjnych, trwających po 5 dni roboczych dla 5 pracowników UODO, w trakcie których odbywać się będzie wymiana doświadczeń i krajowych perspektyw w zakresie wdrażania Aktu w sprawie zarządzania danymi (DGA). Organizacja serii wizyt studyjnych dotyczących wdrażania DGA ma na celu wsparcie, współpracę i zapewnienie transgranicznej wymiany najlepszych praktyk pomiędzy Polską, Finlandią i Węgrami. Instytucjami przyjmującymi są: fińska Agencja Transportu i Komunikacji Traficom (The Finnish Transport and Communications Agency Traficom) oraz węgierski Krajowy Urząd Ochrony Danych i Wolności Informacji (organ ochrony danych, The National Authority for Data Protection and Freedom of Information – NAIH).

Realizacja projektu przyczyni się w bezpośredni sposób do bardziej efektywnego wdrożenia DGA w Polsce, umożliwiając czerpanie z dobrych praktyk podmiotów mających doświadczenie w tym zakresie[662].

### 1.8.4. Cyberbezpieczny Urząd

W 2025 r. Urząd Ochrony Danych Osobowych rozpoczął realizację projektu pt. Cyberbezpieczny Urząd w ramach instrumentu wsparcia „Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo

[662] Wizyty studyjne zrealizowane zostały w marcu i kwietniu 2026 r., relacja będzie zawarta w przyszłorocznym sprawozdaniu z działalności polskiego organu ds. ochrony danych osobowych.

Cyberbezpieczeństwo - Cyberbezpieczny Rząd". Projekt ten realizowany jest ze środków Krajowego Planu Odbudowy i Zwiększania Odporności[663]. Realizacja projektu ma bezpośredni związek z celami strategicznymi KPO i stanowi odpowiedź na zidentyfikowane potrzeby z zakresu cyberbezpieczeństwa.

Celem projektu była weryfikacja wdrożonych zabezpieczeń oraz dostosowanie ich do rozwiązań zgodnych z aktualnymi standardami. W szczególności zaś - zwiększenie świadomości pracowników w zakresie bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) a co w rezultacie powinno się przełożyć na zwiększenie efektywności ich pracy.

Zakres projektu grantowego został podzielony na trzy obszary:

- organizacyjny, którego zadaniem była ocena oraz udoskonalenia istniejących w UODO rozwiązań w zakresie Systemu Zarządzania Bezpieczeństwem Informacji;
- kompetencyjny, w ramach którego pracownicy Urzędu uczestniczyli w szkoleniach podnoszących ich kwalifikacje cyfrowe przy wsparciu podmiotów zewnętrznych, uwzględniając szczególną rolę Instytucji jako organu nadzorczego;
- innowacyjny, wdrażający nowe rozwiązania techniczne uwzględniające rozwój technologii oraz mitygację ryzyk. W obszarze tym podjęte zostały działania audytowe mające na celu identyfikację luk i realizację działań naprawczych, w tym rekonfigurację istniejących rozwiązań lub wdrożenie nowych.

W założeniu wszystkie ww. elementy obszarów objętych tym projektem mają wpłynąć na poprawę bezpieczeństwa infrastruktury sieciowej Urzędu Ochrony Danych Osobowych. Cyberbezpieczeństwo jest bowiem procesem ciągłym, wymagającym stałego monitorowania, rozwoju oraz dostosowywania do nowych warunków. Dlatego Urząd podjął decyzję o usłudze stałego monitorowania sieci teleinformatycznej. W pierwszym etapie zaplanowane było wdrożenie usługi zewnętrznego centrum monitorowania i ochrony infrastruktury teleinformatycznej (SOC), a następnie zbudowanie kompetencji pracowników Urzędu, tak aby samodzielnie wykorzystywali wdrożoną technologię do wykrywania, analizowania i reagowania na incydenty. Kolejną bardzo ważną sprawą było wdrożenie dodatkowych mechanizmów zabezpieczających dane, w szczególności wdrożenie dodatkowych kopii zapasowych w zewnętrznych zasobach tj. chmurze obliczeniowej w modelu Cold Storage. Usługa ta miała zabezpieczyć Urząd przed ewentualnymi incydentami powstałymi w wewnętrznym środowisku teleinformatycznym.

## 1.9. Konkursy

W analizowanym 2025 roku organ nadzorczy był organizatorem i patronem konkursów z dziedziny prawa do prywatności i ochrony danych osobowych.

[663] https://uodo.gov.pl/pl/614/3856.

### 6) XIII Konkurs na esej dla studentów kierunków prawa, administracji, informatyki oraz zarządzania




Komisja konkursowa złożona z ekspertów UODO, specjalistów Krajowej Izby Radców Prawnych (KIRP), przy partnerstwie merytorycznym Kancelarii Kobylańska Lewoszewski Mednis sp. j., po raz trzynasty wyłoniła laureatów w konkursie na esej dla studentów prawa, administracji, informatyki oraz zarządzania. Temat kazusu „Dostęp uczelni do danych na prywatnych urządzeniach elektronicznych studentów" dotyczył kwestii granic ochrony prywatności w kontekście korzystania z prywatnych urządzeń podczas egzaminów oraz refleksji nad wymogami prawnymi dotyczącymi ochrony danych osobowych. Podstawą oceny wniosków sformułowanych przez autorów nadesłanych prac, były m.in. komunikaty i decyzje Prezesa UODO, cytowana literatura, orzecznictwo międzynarodowe oraz ogólne rozporządzenie o ochronie danych (RODO). Prace uczestników oceniała komisja konkursowa złożona z ekspertów UODO, przedstawicieli Krajowej Izby Radców Prawnych oraz partnera merytorycznego konkursu.

Uroczystość wręczenia nagród odbyła się 25 czerwca 2025 r. w siedzibie UODO. Laureatom przyznano nagrody rzeczowe. Wyróżnieni studenci – w ramach nagrody specjalnej – mogli wziąć udział w przygotowanym przez ekspertów UODO dwutygodniowym programie szkoleniowym w Urzędzie Ochrony Danych Osobowych. Podczas tej uroczystości podkreślono wysoki poziom merytoryczny nadesłanych prac oraz interdyscyplinarny charakter tematyki konkursu, który łączył zagadnienia prawne, technologiczne i zarządcze. Zwrócono uwagę na znaczenie takich inicjatyw w pogłębianiu wiedzy studentów na temat ochrony danych osobowych oraz w kształtowaniu umiejętności praktycznego stosowania przepisów RODO w rzeczywistych sytuacjach prawnych i technologicznych.

### 7) Global Privacy and Data Protection Awards 2025



Urząd Ochrony Danych Osobowych został doceniony na arenie międzynarodowej, otrzymując wyróżnienie w prestiżowym konkursie Global Privacy and Data Protection Awards 2025. Nagroda została przyznana w kategorii „Education and Awareness" za projekt „Wizerunek dziecka w internecie. Publikować czy nie?" zrealizowany wspólnie z Fundacją Orange. Celem publikacji jest podniesienie świadomości dorosłych – w tym rodziców, nauczycieli oraz instytucji pracujących z dziećmi – na temat ryzyk związanych z publikowaniem wizerunku najmłodszych w sieci. Poradnik zawiera praktyczne wskazówki: jak konstruować zgodę na publikację zdjęć, jakie mity funkcjonują wokół prawa do wizerunku, jakie pytania warto zadać sobie przed zamieszczeniem treści w sieci.

Wyjaśnia również pojęcia takie jak „sharenting” czy „troll parenting” i wskazuje alternatywne sposoby przedstawiania dzieci w mediach społecznościowych, bez narażania ich na utratę prywatności. Wyróżnienie dla UODO to dowód na to, że polskie działania edukacyjne w obszarze ochrony danych osobowych spotykają się z uznaniem na forum globalnym. Wyróżnienie w konkursie Global Privacy Awards 2025 to zarówno prestiżowy sukces UODO, jak i potwierdzenie wagi tematu ochrony wizerunku dzieci, gdzie za każdym opublikowanym zdjęciem dziecka, stoi przed dorosłym odpowiedzialność za prywatność i godność dziecka.

Uroczyste ogłoszenie zwycięzców i wyróżnionych odbyło się podczas 47. Konferencji Global Privacy Assembly (GPA), która odbyła się 15–19 września 2025 r. w Seulu (Korea Południowa).

## 1.10. Porozumienia o współpracy

### 1) Polskie Towarzystwo Legislacji, 16.01.2025 r.

Prezes UODO, Mirosław Wróblewski podpisał w imieniu Urzędu Ochrony Danych Osobowych porozumienie z Polskim Towarzystwem Legislacji reprezentowanym przez Ewę Kossakowską, prezes Zarządu oraz Mariusza Lachowskiego, skarbnika PTL. Celem współpracy między instytucjami jest wzmocnienie znaczenia ochrony danych osobowych w procesie legislacyjnym. W szczególności 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.

### 2) Rządowe Centrum Legislacji, 27.01.2025 r.

Porozumienie o współpracy między Prezesem UODO a Rządowym Centrum Legislacji reprezentowanym przez dr Joannę Knapińską, prezes RCL, zostało podpisane w celu wymiany doświadczeń i dobrych praktyk związanych z kształceniem prawników oraz upowszechnienia wiedzy w obszarze zagadnień związanych ze stanowieniem prawa. Strony wyraziły wolę promowania wiedzy na temat legislacji, ze szczególnym naciskiem na ochronę danych osobowych m.in. poprzez organizację wykładów, spotkań, konferencji i projektów naukowych, wymianę doświadczeń, wiedzy i dobrych praktyk oraz uwzględnienie danych osobowych przy rozwoju nowych technologii w legislacji.

### 3) Naczelna Izba Lekarska, 26.03.2025 r.

Prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski podpisał z Łukaszem Jankowskim, prezesem Naczelnej Rady Lekarskiej, porozumienie o współpracy w zakresie ochrony danych osobowych w działalności podmiotów medycznych. Porozumienie zawarto 26 marca 2025 r., w dniu wejścia w życie Europejskiej przestrzeni danych dotyczących zdrowia (EHDS) – rozporządzenia Parlamentu Europejskiego.

Współpraca między instytucjami będzie dotyczyć m.in.: zapewnienia spójnego stosowania obowiązującego prawa, uwzględniającego ocenę skutków regulacji dla

ochrony danych osobowych, zacieśnienia współpracy przy wdrażaniu Europejskiej przestrzeni danych dotyczących zdrowia w zakresie posiadanych kompetencji i uprawnień, wspierania rozwoju innowacji, badań, wymiany wiedzy, doświadczeń i dobrych praktyk w przedmiocie bezpieczeństwa danych medycznych. Na bazie podpisanego porozumienia NIL oraz UODO zamierzają wspierać się w działaniach na rzecz promowania zasad ochrony danych osobowych w sektorze zdrowia, a także uczestniczyć we wspólnych projektach i inicjatywach. Zobowiązują się też do wzajemnego wsparcia w działaniach na rzecz wdrożenia EHDS, związanego z budową jednolitego rynku elektronicznej dokumentacji medycznej, która ułatwi bezpieczne świadczenie usług opieki zdrowotnej w całej Unii Europejskiej oraz zapewni spójny, wiarygodny i skuteczny system wykorzystania danych medycznych na potrzeby badań naukowych, innowacji, kształtowania polityki i działań regulacyjnych.

**4) Fundacja Polskich Portów Lotniczych, 23.05.2025 r.**

Mirosław Wróblewski, prezes UODO i Joanna Bochniarz, prezes Fundacji Polskich Portów Lotniczych, 23 maja 2025 roku zawarli porozumienie o współpracy.

Strony zobowiązały się m.in. do wspólnej organizacji wydarzenia kończącego XV edycję ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa" (27.05.2025 r.). Współpraca obejmie również realizację inicjatyw edukacyjnych, których celem będzie rozwijanie kompetencji społecznych związanych z bezpiecznym podróżowaniem, ochroną prywatności i danych osobowych oraz zwiększanie świadomości różnych grup społecznych w tym zakresie.

**5) KIODO Polski Autokefaliczny Kościół Prawosławny, 15.10.2025 r.**

Prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski i Kościelny Inspektor Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego (PAKP) ks. Andrzej Lewczak, 15 października 2025 r. podpisali porozumienie o współpracy i wzajemnym przekazywaniu informacji. Dokument ten ma swoją wyjątkową rangę ze względu na to, że PAKP to drugi pod względem liczebności Kościół w Polsce.

Porozumienie określa zasady, zakres i formę współpracy między Prezesem UODO a KIODO, zwłaszcza w obszarze działań edukacyjnych, szkoleniowych oraz informacyjnych prowadzonych dla zapewnienia ochrony praw osób fizycznych w związku z przetwarzaniem danych osobowych.

Porozumienie zostało podpisane z uwzględnieniem przewidzianej w Konstytucji RP zasady autonomii i niezależności kościołów i innych związków wyznaniowych jakim jest PAKP, a także innych aktów normatywnych stanowiących o stosunku państwa polskiego do tego Kościoła. Dokument opiera się również na oświadczeniach PAKP dotyczących stosowania zasad ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (RODO) oraz realizuje możliwość (przewidzianą w ustawie o ochronie danych osobowych z 2018 r.) zawarcia porozumienia o współpracy między Prezesem UODO a niezależnym organem nadzorczym

powołanym na podstawie art. 91 ust. 2 RODO, odnoszącego się do nadzoru nad kościołami i związkami wyznaniowymi, które stosują szczegółowe zasady ochrony danych pod warunkiem ich dostosowania do RODO. Podpisany dokument odwołuje się do konieczności pogodzenia ochrony danych z korzystaniem z podstawowego prawa do wolności religijnej, zagwarantowanego w prawie międzynarodowym, europejskim i polskim. Porozumienie jest efektem współpracy Prezesem UODO z przedstawicielami różnych Kościołów i związków wyznaniowych w Polsce, czego wyrazem było seminarium eksperckie Prezesa UODO pt. „Aktualne wyzwania ochrony danych osobowych w związkach wyznaniowych w Polsce" (7.05.2025 r.).

**6) Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim, 28.10.2025 r.**

Rektor Akademii im. Jakuba z Paradyża w Gorzowie Wielkopolskim i Prezes Urzędu Ochrony Danych Osobowych podjęli oficjalną współpracę na rzecz promowania zasad ochrony danych osobowych i prawa do prywatności, podpisując 28 października 2025 r. porozumienie w tej sprawie.

Współpraca obejmować będzie prowadzenie wspólnych przedsięwzięć o charakterze naukowo-badawczym, rozwojowym i edukacyjnym, wspólne publikacje, wymianę materiałów naukowych i dydaktycznych, a także organizację konferencji, szkoleń czy warsztatów. W planach jest realizacja studenckich praktyk zawodowych dla studentów Akademii im. Jakuba z Paradyża w Gorzowie Wielkopolskim, zgodnie z właściwym programem studiów oraz ramowym programem studenckich praktyk zawodowych. Głównym celem podpisanego porozumienia jest wzajemne świadczenie pomocy w ramach swoich kompetencji. Szczegółowe zasady współpracy oraz wspólnych przedsięwzięć podejmowanych na podstawie podpisanego porozumienia, będą regulowane w odrębnych umowach pomiędzy Stronami.

**7) Główny Inspektor Sanitarny, 30.10.2025 r.**

Celem porozumienia podpisanego przez Prezesa UODO z Głównym Inspektorem Sanitarnym jest wzmocnienie współdziałania między obiema instytucjami, w szczególności w obszarach związanych z przetwarzaniem danych osób chorych oraz osób wyznaczonych do kontaktu przez pacjenta. Zgodnie z postanowieniami porozumienia współpraca będzie realizowana zarówno na szczeblu centralnym, jak i terenowym, przy pełnym poszanowaniu kompetencji i obowiązków każdej ze stron. UODO i GIS będą wymieniać informacje istotne dla przeciwdziałania naruszeniom prawa w zakresie przetwarzania danych osobowych oraz wspólnie działać na rzecz podnoszenia wiedzy i świadomości w tym obszarze.

W ramach współpracy planowanie jest organizowanie konferencji, seminariów, szkoleń i innych inicjatyw edukacyjnych poświęconych ochronie danych osobowych, a także wzajemne udostępnianie materiałów informacyjnych i szkoleniowych. Strony zobowiązały się również do uwzględnienia tematyki ochrony danych osobowych w programach organizowanych wydarzeń oraz do wymiany doświadczeń i dobrych praktyk.

**8) Naczelna Rada Adwokacka, 6.11.2025 r.**

Mirosław Wróblewski, prezes Urzędu Ochrony Danych Osobowych oraz Przemysław Rosati, prezes Naczelnej Rady Adwokackiej podpisali porozumienie o współpracy na rzecz ochrony praw i wolności obywatelskich w zakresie prawa do prywatności i ochrony danych osobowych. Strony zobowiązały się do wspólnego promowania zasad ochrony danych osobowych w procesie tworzenia i stosowania prawa oraz podejmowania wspólnych inicjatyw edukacyjnych. Przewidziano także możliwość wspólnego udziału ekspertów obu instytucji w tych przedsięwzięciach oraz współpracę przy projektach związanych z rozwojem nowych technologii, w szczególności z wykorzystaniem sztucznej inteligencji, w procesie stosowania prawa. Strony wyraziły wolę wspierania się w pracach nad publikacjami popularyzującymi wiedzę o ochronie danych osobowych, zwłaszcza w kontekście zmian legislacyjnych.

Współpraca Urzędu Ochrony Danych Osobowych z Naczelną Radą Adwokacką ma przyczynić się do wzmocnienia kultury ochrony danych osobowych w środowisku prawniczym oraz pogłębienia świadomości znaczenia prawa do prywatności w praktyce sądowej, w demokratycznym państwie prawnym.

**9) Ministerstwo Cyfryzacji, 24.11.2025 r.**

Prezes UODO i Minister Cyfryzacji podpisali porozumienie w sprawie współpracy przy zgłaszaniu naruszeń ochrony danych osobowych za pomocą systemu S46 – systemu teleinformatycznego wspierającego działanie krajowego systemu cyberbezpieczeństwa.

Porozumienie zakłada, że organy właściwe ds. cyberbezpieczeństwa oraz Prezes UODO będą korzystać z systemu S46 do realizacji swoich ustawowych zadań.

Minister Cyfryzacji, który jest organem właściwym do spraw cyberbezpieczeństwa dla sektora infrastruktury cywilnej, zapewni odpowiednie funkcje, pozwalające m.in. zgłaszać do Prezesa Urzędu naruszenia ochrony danych osobowych przez podmioty objęte krajowym systemem cyberbezpieczeństwa, które używają systemu S46, zintegrować S46 z innymi systemami stosowanymi przez Prezesa UODO, a także wysyłać raporty bezpośrednio z systemu S46. Na mocy tego porozumienia wszyscy współadministratorzy danych przetwarzanych w systemie S46 (w tym Minister Cyfryzacji i Prezes UODO) zobowiązani są do samodzielnego wypełniania praw oraz obowiązków wynikających z RODO. Porozumienie będzie obowiązywało od dnia wejścia w życie znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa, której przepisy upoważnią Prezesa UODO do korzystania z systemu S46 w celu realizacji jego zadań.

## 1.11. Poradniki

### Poradnik dotyczący naruszeń ochrony danych osobowych




W okresie od 21 maja do 21 czerwca 2024 r. Prezes UODO przeprowadził 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. Ostateczny kształt poradnikowi nadał Prezes UODO Mirosław Wróblewski. 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.[664]

W celu przybliżenia tematyki ww. zaktualizowanego poradnika, Urząd Ochrony Danych Osobowych zorganizował dwa webinaria w formule online. Pierwsze z nich odbyło się 28 marca 2025 r. z udziałem blisko 1500 osób.

Drugie webinarium, stanowiące kontynuację pierwszego spotkania, odbyło się 16 maja 2025 r. Jego głównym celem było udzielenie odpowiedzi na pytania zgłoszone przez uczestników podczas pierwszego webinarium oraz omówienie praktycznych przykładów dotyczących treści poradnika.

Oba webinaria zostały nagrane i udostępnione na stronie internetowej UODO, co umożliwiło zapoznanie się z ich treścią również osobom, które nie mogły uczestniczyć w spotkaniach na żywo.

## 1.12. Nagroda im. Michała Serzyckiego

Nagroda im. Michała Serzyckiego jest wyróżnieniem Prezesa Urzędu Ochrony Danych Osobowych przyznawanym osobom i organizacjom, które swoją działalnością przyczyniają się do poszerzania świadomości na temat prawa do prywatności i ochrony danych osobowych. Od 2018 r. nagroda ta jest wręczana co roku podczas obchodów Dnia Ochrony Danych Osobowych. Nazwa nagrody ma wymiar symboliczny, gdyż Polska włączyła się w obchody tego święta w 2007 roku, a więc w czasie, gdy patron nagrody – Michał Serzycki – zajmował stanowisko Generalnego Inspektora Ochrony Danych Osobowych III kadencji. Jednym z rezultatów jego działań

[664] https://uodo.gov.pl/pl/598/3563.

było zainicjowanie na szeroką skalę działalności informacyjnej i edukacyjnej organu ds. ochrony danych osobowych.

Nagroda przyznawana jest w oparciu o oryginalność i skalę działania, przewidywany czas i trwałość efektów, skuteczność zarządzania oraz dotarcie do grup docelowych przy użyciu odpowiedniej komunikacji w obszarze ochrony danych i prywatności. Brana jest również pod uwagę współpraca z partnerami i organizacjami społecznymi, a także umiejętność wywołania długotrwałych zmian w zachowaniu i postawach społecznych.

W 2025 r. nagrodę im. Michała Serzyckiego przyznano już po raz ósmy. Wyróżnienie otrzymali: Katarzyna Szymielewicz, Prezeska Fundacji Panoptykon, dr Konrad Ciesiołkiewicz, zastępca przewodniczącej Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15, a także Helsińska Fundacja Praw Człowieka i Fundacja Panoptykon.

Dotychczas nagrodą im. Michała Serzyckiego wyróżniono 18 osób i 5 instytucji.

## 1.13. Konferencje, seminaria, spotkania

W analizowanym roku sprawozdawczym organ nadzorczy organizował konferencje, seminaria i spotkania, 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) **Konferencja (Bez)PRAWA osób transpłciowych w Polsce. Jak przetwarzać dane osobowe osób transpłciowych i skutecznie przeciwdziałać dyskryminacji ze względu na tożsamość płciową w zatrudnieniu? Warszawa, 28.02.2025 r.**




Organizatorem tego wydarzenia był Prezes UODO we współpracy z Fundacją Trans-Fuzja, organizacją Open for Business oraz Społecznym Zespołem Ekspertów przy Prezesie UODO. Celem konferencji było zwrócenie uwagi na problematykę naruszeń praw osób transpłciowych w obszarze zatrudnienia, w szczególności w kontekście przetwarzania ich danych osobowych, ochrony prywatności oraz przeciwdziałania dyskryminacji w miejscu pracy. Organizatorzy podkreślali, że kwestie te pozostają w ścisłym związku z godnością człowieka i realizacją praw podstawowych, a jednocześnie stanowią istotne wyzwanie praktyczne dla pracodawców i administratorów danych.

Podczas otwarcia konferencji wskazano na znaczenie równego traktowania wszystkich osób zatrudnionych oraz na odpowiedzialność instytucji publicznych i prywatnych za tworzenie bezpiecznego i niedyskryminującego środowiska pracy. Podkreślono, że ochrona danych osobowych, wynikająca m.in. z przepisów RODO, nie ma charakteru wyłącznie formalnego, lecz służy zapobieganiu realnym szkodom, takim jak stygmatyzacja, naruszenie prywatności czy wykluczenie społeczne.

Znaczna część konferencji została poświęcona praktycznym problemom związanym z przetwarzaniem danych osób transpłciowych w zatrudnieniu, w tym danym identyfikacyjnym, informacjom dotyczącym płci oraz dokumentacji pracowniczej. Eksperci zwracali uwagę na konieczność stosowania zasady minimalizacji danych, ograniczenia dostępu do informacji wrażliwych oraz zapewnienia aktualności i rzetelności danych, w szczególności w sytuacjach, gdy dane nie odzwierciedlają tożsamości danej osoby. Wskazywano również na prawo do sprostowania danych jako istotny instrument ochrony praw jednostki. Ważnym elementem dyskusji była też kwestia przeciwdziałania dyskryminacji w miejscu pracy, zarówno na poziomie przepisów wewnętrznych, jak i codziennej praktyki organizacyjnej. Same regulacje prawne nie są wystarczające, jeśli nie towarzyszy im odpowiednia świadomość, szkolenia oraz jasne procedury reagowania na przypadki nierównego traktowania. Zwrócono uwagę na rolę pracodawców w kształtowaniu kultury organizacyjnej opartej na poszanowaniu różnorodności i godności pracowników.

Konferencja zakończyła się podkreśleniem potrzeby dalszej edukacji oraz współpracy między instytucjami publicznymi, organizacjami społecznymi i sektorem prywatnym. Ochrona danych osobowych osób transpłciowych oraz przeciwdziałanie bezprawnym praktykom w zatrudnieniu powinny być traktowane jako integralna część realizacji praw człowieka i standardów państwa prawa, a nie wyłącznie jako obowiązek administracyjny.

**2) Konferencja „Europejska przestrzeń danych dotyczących zdrowia – wyzwanie dla Europy". Warszawa, 26.03.2025 r.**




26 marca, w dniu wejścia w życie Europejskiej przestrzeni danych dotyczących zdrowia (EHDS) – rozporządzenia Parlamentu Europejskiego – odbyła się konferencja „Europejska przestrzeń danych dotyczących zdrowia – wyzwanie dla Europy. Wdrażanie rozwiązań w erze AI, Big Data i medycyny spersonalizowanej". Organizatorami wydarzenia byli Prezes Urzędu Ochrony Danych Osobowych wraz z Wydziałem Prawa i Administracji Uniwersytetu Warszawskiego (UW), Wydziałem Medycznym UW, Instytutem Nauk Prawnych Polskiej Akademii Nauk oraz Naczelną Izbą Lekarską.

Konferencja została poprzedzona wykładem na temat problematyki biobankowania i danych medycznych w erze sztucznej inteligencji. W Polsce nadal nie ma ustawy o biobankowości, natomiast można się odwoływać do standardów jakości i kodeksów postępowania w tym obszarze. Wśród najważniejszych tematów konferencji, podzielonej na cztery panele tematyczne, pojawiły się kwestie związane z: modelami wdrażania EHDS w państwach członkowskich UE; wyzwaniami, które stoją przed Polską w ramach tego rozporządzenia, w tym z koniecznością stworzenia odpowiedniej infrastruktury i bezpiecznego środowiska przetwarzania; problemami

wokół wyznaczania organów ds. dostępu do danych dotyczących zdrowia w państwach członkowskich oraz ich roli w przetwarzaniu tych danych; z zadaniami organów nadzorczych w kontekście rozporządzenia (w tym roli UODO), szeregiem zagadnień dotyczących wtórnego wykorzystywania danych, zagadnień prawnych, które będą się pojawiać w ramach obowiązywania EHDS oraz z przewidywanym wpływem rozporządzenia na dostępność produktów leczniczych czy kwestią zapewnienia środków finansowych.

Istotnymi zagadnieniami dotykającymi kwestii EHDS, które pojawiły się w trakcie wystąpień panelowych, to ważna uwaga, że rozporządzenie to nie jest jedyną wspólną przestrzenią Unii Europejskiej, jeśli chodzi o przepływ danych, bo podobna dotyczy też choćby finansów, energetyki, przemysłu czy administracji publicznej. Co więcej, EHDS stanowi wyłom w stosowaniu art. 9 RODO, ponieważ w europejskiej przestrzeni danych dotyczących zdrowia występuje możliwość przetwarzania danych osobowych szczególnej kategorii na rzecz badań oraz innowacji bez pytania o zgodę osób, których dane te dotyczą, co stanowi pewnego rodzaju zmianę trendu w polityce UE. Instytucjami, które w Polsce będą kontrolować proces przetwarzania danych medycznych, zapewniając do tego infrastrukturę, będą m.in. Regionalne Centra Medycyny Cyfrowej.

Wydarzenie stało się też miejscem, w którym wybrzmiała potrzeba współpracy różnych podmiotów, zarówno w sektorze prywatnym, jak i publicznym, w celu efektywnego wdrożenia założeń rozporządzenia. W wykładach i dyskusjach wzięli udział eksperci Urzędu Ochrony Danych Osobowych oraz Społecznego Zespołu Ekspertów (SZE) przy Prezesie UODO.

### 3) V Data Economy Congress. Warszawa, 26-27.03.2025 r.

Konferencja poświęcona była nowym modelom gospodarki danych, ich przetwarzaniu, wykorzystaniu oraz wyzwaniom biznesowym, prawnym i technologicznym związanym z rozwojem ekosystemu danych. Prezes Urzędu Ochrony Danych Osobowych uczestniczył w panelu dyskusyjnym zatytułowanym **„Wyzwania związane z regulacjami prawnymi**”, który dotyczył wpływu najnowszych ram regulacyjnych, w tym unijnego Data Act (Akt w sprawie danych) oraz AI Act (Akt o sztucznej inteligencji), na funkcjonowanie organizacji oraz społeczeństwa w kontekście przetwarzania i udostępniania danych. W swoim wystąpieniu podkreślił, że skuteczne stosowanie rozwiązań wynikających z Data Act i AI Act wymaga ich harmonizacji z Rozporządzeniem o ochronie danych osobowych (RODO). Dlatego działania legislacyjne na poziomie europejskim oraz inicjatywy podejmowane przez Urząd Ochrony Danych Osobowych akcentują konieczność spójnego łączenia tych ram, tak aby promować innowacje oparte na danych i zapewniać wysoki standard ochrony praw osób, których dane są przedmiotem przetwarzania.

### 4) Banking & Insurance Forum. Warszawa, 15.04.2025 r.

Obecność Prezesa UODO w gronie ekspertów debaty eksperckiej zatytułowanej **„Przeciwdziałanie przestępstwom w świecie cyfrowym”**, pozwoliła

na przedstawienie perspektywy organu nadzorczego oraz podkreślenie znaczenia zgodności działań instytucji finansowych z przepisami o ochronie danych osobowych w warunkach dynamicznego rozwoju technologii cyfrowych oraz podkreśliła znaczenie bezpieczeństwa informacji w sektorach o szczególnym znaczeniu dla funkcjonowania państwa i gospodarki.

W swoim wystąpieniu podkreślił, że nawet najbardziej wyrafinowane ataki cyfrowe nie pozostają bez reakcji organu ochrony danych osobowych, ponieważ istnieją odpowiednie narzędzia prawne, które należy stosować w każdym takim przypadku. W tym kontekście wskazał na decyzję, jaką podjął jako organ nadzorczy w 2024 r. dotyczącą zakazu rozpowszechniania wizerunku osób fizycznych przez Meta Platforms. Wskazał, że kluczowym aspektem ochrony danych jest rozpoznawanie systemowych przyczyn naruszeń w środowisku cyfrowym. Problem ten w dużej mierze wynika z niedostatecznej kultury organizacyjnej, w tym braku systematycznych audytów systemów informatycznych. Zwrócił też uwagę na wyzwania wynikające z rozwoju sztucznej inteligencji oraz jej wpływu na stosowane zabezpieczenia cyfrowe. Wiele rozwiązań, które jeszcze niedawno były uznawane za skuteczne, szybko traci swoją efektywność, czego przykładem są wcześniej stosowane metody weryfikacji głosowej klientów. Wskazano przy tym na istotną rolę odpowiednio ukierunkowanej edukacji cyfrowej, prowadzonej z wykorzystaniem zrozumiałego języka dostosowanego do wieku i kompetencji odbiorców.

**5) Seminarium eksperckie „Aktualne wyzwania ochrony danych osobowych w związkach wyznaniowych w Polsce. Warszawa, 7.05.2025 r.**

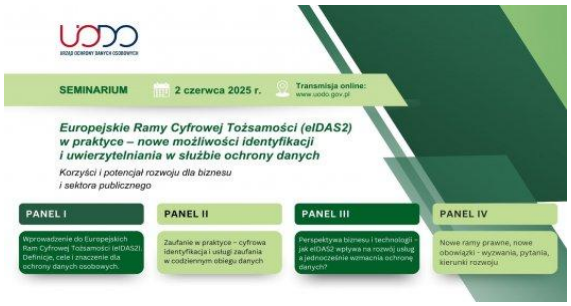
Niezależność regulacji dotyczących ochrony danych osobowych w związkach wyznaniowych, współpraca z UODO oraz relacje między prawem wewnętrznym kościołów a RODO – to główne tematy tego wydarzenia, które przebiegało w formule debaty nad aktualnymi wyzwaniami ochrony danych osobowych przez związki wyznaniowe w Polsce.

Kościelny Inspektor Ochrony Danych Osobowych w Polskim Autokefalicznym Kościele Prawosławnym (AKP) zapoznał uczestników konferencji z sytuacją ochrony danych osobowych w tym związku wyznaniowym podkreślając, że autonomia i niezależność kościołów i związków wyznaniowych w postępowaniu z danymi osobowymi zawsze wiąże się z jeszcze większą odpowiedzialnością wewnętrzną za ochronę danych osobowych wiernych. W Kościele Ewangelicko-Augsburskim i Kościele Ewangelicko-Reformowanym, które są do siebie zbliżone pod względem liczby wiernych, w 2020 r. została utworzona Ewangelicka Komisja Ochrony Danych Osobowych, funkcjonująca jako niezależny organ kolegialny, zaś wspólnota Kościoła Bożego w Polsce, mimo swojego skromnego zasięgu, przeprowadziła pełną cyfryzację zgromadzonych danych i należy do Międzykościelnej Komisji Ochrony Danych Osobowych, w której łączy się dziewięć ewangelickich związków wyznaniowych.

W kolejnej części debaty poruszono temat sztucznej inteligencji i możliwości jej wykorzystania w nauczaniu kościołów i związków wyznaniowych oraz w służbie wiernym w kontekście wspierania ich życia duchowego, poprzez np. aplikacje religijne, chatboty, algorytmy analizujące treść Pisma Świętego i in. Podkreślono rolę

inspektorów danych osobowych w Kościele katolickim i ich niezależność, nad którą czuwa Europejska Komisja Konferencji Episkopatów (CCEE), a także przedstawiono temat związany z funkcjonowaniem ksiąg parafialnych w Kościele, będących zbiorem danych osobowych wiernych. Seminarium kończył apel, by drogą do rozwiązywania wszelkich wątpliwości wokół ochrony danych w związkach wyznaniowych była nieustająca współpraca między nimi a Urzędem Ochrony Danych Osobowych.

### 6) Seminarium UODO „Europejskie Ramy Cyfrowej Tożsamości (eIDAS2) w praktyce". Warszawa, 2.06.2025 r.




Seminarium UODO pt. „Europejskie Ramy Cyfrowej Tożsamości (eIDAS2) w praktyce – nowe możliwości identyfikacji i uwierzytelniania w służbie ochrony danych. Korzyści i potencjał rozwoju dla biznesu i sektora publicznego", było okazją do zaprezentowania korzyści płynących z wdrożenia nowych rozwiązań, szczególnie w kontekście rosnącego zapotrzebowania rynku na identyfikację elektroniczną i powszechne udostępnianie danych. Program wydarzenia obejmował cztery panele dyskusyjne, poświęcone m.in. definicjom i znaczeniu Europejskich Ram Cyfrowej Tożsamości, praktycznym aspektom cyfrowej identyfikacji i usług zaufania, perspektywie biznesu i technologii, a także nowym obowiązkom prawnym[665].

Europejskie Ramy Cyfrowej Tożsamości (eIDAS 2.0) to rozporządzenie Parlamentu Europejskiego i Rady Europejskiej, które ustanawia standardy dla identyfikacji i uwierzytelniania cyfrowego w UE. Dokument ma za zadanie przede wszystkim ułatwić korzystanie z usług on-line.

Organizatorem seminarium był Prezes UODO we współpracy ze Społecznym Zespołem Ekspertów (SZE), którego członkowie aktywnie uczestniczyli w tym wydarzeniu. W panelu zatytułowanym „Wprowadzenie do Europejskich Ram Cyfrowej Tożsamości (eIDAS2). Definicje, cele i znaczenie dla ochrony danych osobowych", głos zabrał ekspert SZE prezentując wykład pt. „Wspólny język zaufania: identyfikacja, uwierzytelnienie, atrybuty (…). Uporządkowanie pojęć w kontekście danych osobowych i interoperacyjności". Z kolei w panelu pod nazwą „Perspektywa biznesu i technologii – jak eIDAS2 wpływa na rozwój usług, a jednocześnie wzmacnia ochronę danych?", wystąpił również członek Społecznego Zespołu Ekspertów przy Prezesie UODO**,** wygłaszając prelekcję pt. „Wyzwania techniczne i organizacyjne w tworzeniu spójnego ekosystemu tożsamości cyfrowej".

### 7) IV edycja Konferencji „Uwaga! Smartfon". Lublin, 4.06.2025 r.

O tym dlaczego warto się uczyć na cudzych błędach rozmawiano podczas konferencji zorganizowanej przez Fundację Projekt PL. Ekspert UODO poprowadził warsztaty pt. „Co poszło nie tak?" na temat wiedzy o cyfrowych zagrożeniach

[665] https://uodo.gov.pl/pl/138/3708.

i cyfrowej higienie i roli nowoczesnych technologii w życiu społecznym. Wydarzenie poświęcone było zagadnieniom cyfryzacji i nadmiernemu korzystaniu z urządzeń ekranowych przez dzieci i młodzież. Podczas konferencji otwarte było stoisko wystawiennicze UODO, na którym można było zasięgnąć porady oraz zapoznać się z działalnością Urzędu.

### 8) Konferencja Międzynarodowa w ramach CEEDPA. Kraków, 12-13.06.2025 r.




Dyskusja wokół zagadnień związanych z bezpieczeństwem oraz ochroną danych osobowych w kontekście rozwijającej się technologii kwantowej i wykorzystywania komputerów kwantowych, była głównym tematem międzynarodowej konferencji pt. „Technologie kwantowe: zagrożenia, wyzwania i szanse dla cyberbezpieczeństwa i ochrony danych osobowych", która odbywała się w ramach 23. corocznego spotkania Grupy Państw Europy Środkowo-Wschodniej (CEEDPA) zrzeszającej organy ochrony danych z tego regionu. W konferencji CEEDPA uczestniczyli przewodniczący Grupy oraz przedstawiciele organów ochrony danych z państw Unii Europejskiej i spoza niej. Organizatorami wydarzenia byli: Urząd Ochrony Danych Osobowych i Uniwersytet Jagielloński. Konferencja otrzymała patronat polskiej prezydencji w Radzie UE[666].

Organizatorzy i uczestnicy wydarzenia postawili sobie za cel przedstawienie podstawowych zasad działania technologii kwantowych oraz ram prawnych, w jakich rozwiązania kwantowe mogą znaleźć bezpieczne zastosowanie z poszanowaniem zasad ochrony danych osobowych i prywatności. Szyfrowane dane, infrastruktura krytyczna, metody dostępu do danych – to wszystko staje dziś pod znakiem zapytania, gdy weźmiemy pod uwagę, że komputery nowej generacji będą w stanie błyskawicznie złamać zabezpieczenia i zapewnić dostęp do chronionych danych. Ma to fundamentalne znaczenie np. przy przetwarzaniu danych w takich dziedzinach, jak bezpieczeństwo publiczne, ochrona zdrowia czy finanse. Uczestnicy debat zgodnie podkreślali konieczność rozwoju oprogramowania postkwantowego, które będzie odpowiedzią na zagrożenia wynikające z mocy obliczeniowej komputera kwantowego użytego do przełamania zabezpieczeń.

W perspektywie szybkiego rozwoju technologii kwantowych, skuteczna ochrona prywatności i danych osobowych stanowi ogromne wyzwanie dla suwerenności cyfrowej Unii Europejskiej i bezpieczeństwa narodowego. Dlatego ważnym tematem konferencji było przedstawienie aktualnych działań podejmowanych przez UE w celu ochrony danych osobowych w związku z technologią kwantową – w szczególności kwestie już istniejących oraz oczekiwanych regulacji prawnych wobec tej technologii – a także wyzwania stojące przed administratorami oraz wspierającymi ich inspektorami ochrony danych. Uczestnicy konferencji zgodni byli co do tego, że RODO stanowi

[666] https://uodo.gov.pl/pl/531/3741.

dobry przykład prawodawstwa w odniesieniu do tej technologii, ponieważ wskazuje ważne zasady, które mogą mieć zastosowanie. Mając to na uwadze, tworzenie nowych regulacji o ochronie danych osobowych w kontekście rozwoju technologii kwantowych uznano za nieuzasadnione. Dyskutowano natomiast o zwiększeniu wachlarza szkoleń i różnych inicjatyw edukacyjnych, w celu zapewnienia wykwalifikowanych specjalistów z zakresu technologii kwantowych.

W podsumowującej części konferencji prelegenci zastanawiali się nad dalszym rozwojem kryptografii kwantowej i postkwantowej, omówili wyzwania związane z bezpieczeństwem klasycznych algorytmów szyfrowania, wykorzystaniem postkwantowej kryptografii w portfelach tożsamości cyfrowej i blockchainie. Zastanawiali się również nad potencjałem połączenia sztucznej inteligencji z obliczeniami kwantowymi i kierunkiem zmian wyznaczanym przez National Institute of Standards and Technology (NIST) i Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

### 9) Turniej Wsi Gminy Skierniewice. Miedniewice, 3.08.2025 r.

Turniej Wsi Gminy Skierniewice to lokalne wydarzenie sportowo-rekreacyjne zorganizowane na terenie Gminy Skierniewice, integrujące mieszkańców okolicznych miejscowości. W rywalizacji brały udział drużyny reprezentujące sołectwa lub instytucje z gminy, a konkurencje miały charakter zarówno sportowy (np. piłka nożna, siatkówka, biegi), jak i zabawowo-sprawnościowy. Podczas tego wydarzenia, UODO wystąpił ze swoją strefą wystawienniczą, gdzie uczestnicy mogli zasięgnąć porady oraz konsultacji z zakresu ochrony danych osobowych i prawa do prywatności. Dla najmłodszych przygotowane zostały gry i zabawy, podczas których tematy związane z bezpieczeństwem danych osobowych najmłodszych były im prezentowane w sposób przystępny, dostosowany do ich wieku i możliwości poznawczych. Wydarzenie pokazało, że nawet podczas imprez sportowo-rekreacyjnych można rozmawiać o ochronie danych osobowych i podnosić świadomość mieszkańców w tym zakresie.

### 10) Q-CON Quantum Conference. Gdańsk, 29.08.2025 r.




Tematem przewodnim Quantum Conference 2025 były wyzwania stojące przed przemysłem kwantowym, w szczególności w zakresie wsparcia dla startupów, a także konkurencja na globalnym rynku. Strategie UE – regulacje, deregulacje i inicjatywy wspierające rozwój technologii kwantowych oraz post-quantum cryptography – były tematem debat podczas tego wydarzenia. Prezes UODO Mirosław Wróblewski wygłosił prelekcję pt. „Navigating GDPR deregulation. What startups need to know" („Odnaleźć drogę w deregulacji RODO. Co muszą wiedzieć start-upy") w części otwierającej spotkanie. Podkreślił, że technologie kwantowe dają możliwości długoterminowej ochrony danych, co zwiększy zaufanie klientów we wszystkich branżach. Ale technologia

kwantowa to także potencjalne zagrożenie, gdyż komputery kwantowe będą umiały złamać powszechnie dziś stosowane algorytmy kryptograficzne, co więcej: będą mogły odszyfrować dane historyczne, a większość organizacji nie jest jeszcze dzisiaj przygotowana na wdrożenie zabezpieczeń postkwantowych. *„Era kwantowa to z jednej strony ogromna szansa na lepszą kontrolę nad danymi i większe bezpieczeństwo dla obywateli, z drugiej – ryzyko choćby dla możliwości realizacji praw wynikających z przepisów RODO, takich jak np. prawo do bycia zapomnianym (odnośnie do danych z przeszłości)"* – powiedział Mirosław Wróblewski podczas tego spotkania. Prezes UODO wyjaśnił również w tej perspektywie propozycje zmian, które chce wprowadzić Komisja Europejska w związku z uproszczeniem RODO dla małych i średnich przedsiębiorstw, w tym start-upów. Miałyby one pozwolić na dostosowanie przepisów do realiów funkcjonowania mniejszych podmiotów, by pomóc im wdrażać innowacje cyfrowe, takie jak technologia kwantowa. Jako istotne punkty do dyskusji prezes Urzędu przedstawił wnioski z konferencji UODO i Uniwersytetu Jagiellońskiego z czerwca 2025 r. dotyczącej wyzwań, jakie stawia rzeczywistość kwantowa, oraz treść deklaracji z 23. Spotkania Grupy ochrony danych z Europy Środkowo-Wschodniej, która wskazała na konieczność wzmocnienia organów ochrony danych oraz wsparcia dla MŚP i organizacji pozarządowych w kontekście nadchodzącej rewolucji kwantowej.

W trakcie gdańskiej konferencji głos zabrał także mec. Roman Bieda, członek Społecznego Zespołu Ekspertów przy Prezesie UODO, który zaprezentował temat „The EU Quantum Strategy and the Post-Quantum Cryptography Roadmap: Legal and Policy Perspectives" („Strategia kwantowa Unii Europejskiej i mapa drogowa dla postkwantowej kryptografii: perspektywa prawna i polityczna").

**11) XXXIV Forum Ekonomiczne w Karpaczu, 2-4.09.2025 r.**

Prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski, jego zastępca Konrad Komornicki wraz ze współpracownikami byli gośćmi XXXIV Forum Ekonomicznego w Karpaczu, uczestnicząc w kilku debatach poświęconych kluczowym wyzwaniom gospodarki cyfrowej, ochronie danych osobowych oraz nowym technologiom. Urząd Ochrony Danych Osobowych był jednym z partnerów instytucjonalnych forum, organizując panel na temat technologii kwantowych moderowany przez członka Społecznego Zespołu Ekspertów przy Prezesie UODO. Podczas dyskusji poświęconej sztucznej inteligencji eksperci UODO podkreślali, że niezależnie od tego, jak stosowanie AI pomaga we wzroście gospodarczym, w codziennym życiu, w poprawie kondycji finansowej i organizacyjnej przedsiębiorstw, to najważniejsze jest, żeby na końcu tego procesu znajdowała się ludzka inteligencja. W panelu „Cyfryzacja w Polsce: szansa na rozwój czy zagrożenie dla bezpieczeństwa?" przedstawione zostały statystyki zgłoszeń incydentów cybernetycznych zgłaszanych codziennie w Polsce, zaś podczas panelu „Równe ramy prawne i konkurencyjne na rynku e-commerce" Prezes UODO omówił działania Urzędu Ochrony Danych Osobowych dotyczące platform sprzedażowych, w tym platform chińskich. Podkreślił przy tym konieczność prowadzenia działań legislacyjnych na poziomie UE, aby lepiej chronić dane klientów platform.

W ramach Forum Cyberbezpieczeństwa, którego gospodarzem było Ministerstwo Cyfryzacji oraz NASK, Mirosław Wróblewski mówił o wyzwaniach regulacyjnych i możliwościach rozwoju rynku zarządzania danymi w Polsce w kontekście Data Governance Act, a także o nowych wyzwaniach dla Urzędu Ochrony Danych Osobowych związanych z nowymi kompetencjami wynikającymi z tego aktu.

Ostatniego dnia Forum Ekonomicznego odbyła się debata „Nowa waluta świata – jak bezpiecznie zarządzać danymi?", która dotyczyła ryzyk nadużyć danych oraz wskazywała na potrzebę jasnych regulacji i standardów etycznych w tym obszarze. Jej uczestnikiem był Konrad Komornicki, zastępca Prezesa UODO, który podkreślił jak ważnym czynnikiem w zarządzaniu danymi jest edukacja. Omówił też przepisy prawne, które występują na każdym etapie zarządzania danymi, począwszy od ich pozyskania, przechowywania, ochrony, wdrożenia, aktualizowania, aż do zarchiwizowania. Podmioty, które w praktyce będą je odpowiedzialnie stosować, w znacznym stopniu zminimalizują ryzyka związane z utratą poufności przetwarzanych danych.

**12) IX Krajowy Kongres Sekretarzy. Warszawa, 30.09-1.10.2025 r.**

Hasło IX Kongresu brzmiało: *Sekretarz przyszłości – nowe regulacje, wyzwania i możliwości".* Debaty i rozmowy o wyzwaniach, z jakimi mierzy się samorząd oraz kierunkach jego rozwoju toczyły się w gronie przedstawicieli rządu, samorządu, biznesu i ekspertów. W związku z obecnością Prezesa UODO na Kongresie, odbył się specjalny panel dyskusyjny pod nazwą „Ochrona danych osobowych - cyfrowe rozwiązania, outsourcing w samorządzie terytorialnym, aktualne podejście do ochrony danych osobowych z uwzględnieniem rozwiązań cyfrowych". W trakcie panelu omówione zostały zasady przetwarzania danych osobowych w kontekście zastosowania cyfrowych rozwiązań w samorządzie terytorialnym i ich zabezpieczenia. Podkreślano, że ochrona danych osobowych w samorządzie terytorialnym musi charakteryzować się całościowym, kompleksowym podejściem administratora danych, uwzględniającym charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, a także – mieć na uwadze obecne i prognozowane rozwiązania w sferze cyfrowej.

Organizatorem wydarzenia była Fundacja Rozwoju Demokracji Lokalnej im Jerzego Regulskiego, we współpracy z Krajową Rady Forów Sekretarzy.

**13) 6. edycja Cyber24 Day. Warszawa, 2.10.2025 r.**

Szósta edycja konferencji Cyber24 Day poświęcona była cyberbezpieczeństwu, cyfryzacji i nowym technologiom. Wśród tematów dominowały zagadnienia dotyczące innowacjom w siłach zbrojnych, rozwojowi polskiej sztucznej inteligencji i technologii kwantowych, a także roli biznesu w digitalizacji państwa, w tym przemysłu. Prezes Urzędu Ochrony Danych Osobowych, Mirosław Wróblewski, wziął udział w panelu dyskusyjnym zatytułowanym **„Co z tą szkołą. Technologia w rękach dzieci"**. Dyskusja koncentrowała się na wyzwaniach prawnych i społecznych dotyczących ochrony danych osobowych dzieci w kontekście korzystania przez nie z nowych

technologii cyfrowych i związanych z tym wyzwaniach prawnych i społecznych. Prezes UODO zwrócił szczególną uwagę na kwestię udostępniania w mediach społecznościowych zdjęć dzieci, podkreślając brak refleksji ich rodziców nad tym, w jaki sposób fotografie te mogą być dalej rozpowszechniane przez algorytmy sztucznej inteligencji i wykorzystywane bez ich zgody oraz wiedzy. Podkreślił, że obrazy mogą być przetwarzane w sposób, który wykracza poza intencje rodziców i samo publikowanie zdjęć może powodować realne ryzyko naruszenia prywatności i bezpieczeństwa danych najmłodszych.

### 14) VI Data Economy Congress. Warszawa, 6-7.10.2025 r.




Podczas Kongresu dyskutowano o kluczowych zagadnieniach związanych z wykorzystywaniem sztucznej inteligencji w administracji i usługach publicznych, jak m.in. transfer wiedzy do gospodarki, międzynarodowe przestrzenie danych w kontekście AI oraz znaczenie ochrony danych osobowych w relacjach z klientami i interesariuszami. Prezes Urzędu Ochrony Danych Osobowych, Mirosław Wróblewski, uczestnicząc w panelu **„AI w sektorze publicznym – innowacje, usługi, państwo”,** wskazał na zagrożenia organizacyjne i prawne związane z wdrażaniem AI w kontekście implementacji AI Act (Aktu o sztucznej inteligencji) oraz zwrócił uwagę na współzależność tego aktu prawnego z innymi regulacjami unijnymi, takimi jak eIDAS2 (Europejskie Ramy Tożsamości Cyfrowej). W świetle ryzyk związanych z powszechnym wykorzystaniem modeli sztucznej inteligencji, Prezes UODO podkreślił wagę ochrony danych osobowych w budowaniu zaufania społecznego do nowych technologii. W szczególności podkreślił rolę Europejskiej Rady Ochrony Danych oraz przedstawił działania Urzędu Ochrony Danych Osobowych, w tym powołanie w 2025 r. Grupy roboczej ds. sztucznej inteligencji w ramach funkcjonującego Społecznego Zespołu Ekspertów przy Prezesie UODO. Celem tej grupy jest monitorowanie wyzwań związanych z AI i opracowywanie rekomendacji w zakresie ochrony danych osobowych.

### 15) Konferencja „Bezpieczne dane dzieci i młodzieży oraz nowe kierunki rozwoju w obszarze kultury fizycznej. Jak sprostać współczesnym wyzwaniom? Kraków, 10.10.2025 r.




10 października 2025 r. w Krakowie, w Akademii Kultury Fizycznej im. Bronisława Czecha, odbyła się konferencja szkoleniowo-metodyczna pt. **„Bezpieczne dane dzieci i młodzieży oraz nowe kierunki rozwoju w obszarze kultury fizycznej. Jak sprostać współczesnym wyzwaniom?”**, zorganizowana przez Urząd

Ochrony Danych Osobowych we współpracy *z* Krakowskim Szkolnym Ośrodkiem Sportowym (KSOS), w ramach obchodów 60-lecia placówki.

Konferencja zgromadziła przedstawicieli środowiska sportowego, nauczycieli wychowania fizycznego, ekspertów ds. ochrony danych osobowych, prawników oraz specjalistów od nowych technologii. Jej celem była analiza zagadnień związanych z ochroną danych osobowych dzieci i młodzieży funkcjonujących w środowisku sportowym oraz omówienie wyzwań, jakie niesie ze sobą rozwój technologii cyfrowych w kontekście bezpieczeństwa informacji.

Podczas sesji dotyczącej ochrony danych osobowych i RODO w instytucjach sportowych podkreślano konieczność świadomego podejścia do zgody na przetwarzanie danych młodych sportowców oraz zasad dotyczących udostępniania ich wizerunku. Omówiono znaczenie higieny cyfrowej oraz rolę narzędzi takich jak Dyżurnet.pl w reagowaniu na zagrożenia związane z publikacją treści w sieci. W dyskusjach zwracano szczególną uwagę na to, jak aplikacje sportowe i technologie cyfrowe, choć wspierające aktywność fizyczną, jednocześnie mogą sprzyjać niezamierzonemu ujawnianiu informacji osobowych, co wymaga świadomego i odpowiedzialnego ich wykorzystywania. W drugiej części sesji eksperci omawiali wykorzystanie sztucznej inteligencji w sporcie jako wyzwanie dla ochrony danych osobowych, analizując zagrożenia wynikające z obecności młodych osób w cyberprzestrzeni oraz wpływ nowoczesnych technologii na prywatność. Poruszono także kwestie związane z higieną cyfrową, podkreślając, że aktywność fizyczna i edukacja w zakresie bezpiecznego korzystania z technologii cyfrowych mogą iść w parze jako elementy sprzyjające zdrowiu i bezpieczeństwu dzieci. Na konferencji przypomniano również o działaniach edukacyjnych podejmowanych przez UODO i jego partnerów, mających na celu podnoszenie świadomości o ochronie danych osobowych wśród dzieci, młodzieży i osób dorosłych pracujących z tymi grupami. Dialog między ekspertami prawnymi, sportowcami oraz nauczycielami jest bowiem istotnym elementem budowania bezpieczeństwa danych w środowiskach młodych ludzi.

**16) Konferencja „Rola sądów w demokratycznym państwie prawa. Diagnoza i perspektywy". Warszawa, 23.10.2025 r.**

Konferencja była okazją do wymiany poglądów na temat roli sądów w systemie demokratycznym, ochrony praw obywatelskich oraz wyzwań stojących przed władzą sądowniczą. W panelu eksperckim przedstawiciele nauki i praktyki prawa wskazywali na konieczność zidentyfikowania najistotniejszych problemów wpływających na efektywność i niezależność sądownictwa, podkreślili wpływ czynników politycznych na funkcjonowanie sądów i potrzebę wypracowania rozwiązań ograniczających jej upolitycznienie. Prelegenci byli zgodni, że przywrócenie prawidłowego funkcjonowania wymiaru sprawiedliwości stanowi jedno z kluczowych zadań dla przyszłości państwa prawa i jest nierozerwalnie związane z kondycją polskiej demokracji.

Organizatorami wydarzenia byli: Senat RP i WPiA UW we współpracy z Kołem Naukowym prawa Konstytucyjnego „Legislator”.

**17) Konferencja Naukowa „DGA – Innowacyjne zarządzanie danymi". Warszawa, 24.10.2025 r.**



W 2025 r. trwały intensywne prace nad przepisami ustawy o zarządzaniu danymi, która ma na celu zapewnienie pełnego stosowania unijnego Aktu w sprawie zarządzania danymi (DGA) w polskim porządku prawnym. Akt ten jest kluczowym elementem „Europejskiej strategii w zakresie danych", którego celem jest zwiększenie dostępności danych oraz ułatwienie ich ponownego wykorzystywania przy jednoczesnym zapewnieniu wysokiego poziomu zaufania i ochrony danych osobowych oraz tajemnic handlowych. DGA odnosi się do rożnych zagadnień, łącząc w sobie prawo informacyjne, w tym otwartość danych z tematyką danych osobowych i zagadnieniami praw własności intelektualnej, tajemnic prawnie chronionych oraz problematyki świadczenia usług pośrednictwa danych, a także altruizmu danych. Waga tych zagadnień poruszona została podczas konferencji naukowej, poświęconej omówieniu aktualnego stanu wdrożenia DGA w polskim porządku prawnym.
Organizatorami wydarzenia byli: Urząd Ochrony Danych Osobowych, WPiA Uniwersytetu Łódzkiego, WPiA UKSW w Warszawie oraz Społeczny Zespół Ekspertów przy Prezesie UODO.

**18) Seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO". Warszawa, 6.11.2025 r.**

Organizatorem wydarzenia był Prezes Urzędu Ochrony Danych Osobowych we współpracy z Naczelną Radą Adwokacką oraz Stowarzyszeniem Sędziów Polskich „Iustitia". Seminarium stworzyło przestrzeń do dialogu pomiędzy przedstawicielami środowisk prawniczych, naukowych i praktyki sądowej, odpowiadając na wyzwania związane z dynamicznym rozwojem orzecznictwa w obszarze ochrony danych osobowych oraz koniecznością budowania spójnej praktyki stosowania RODO w postępowaniach cywilnych. W opinii Prezesa UODO, Mirosława Wróblewskiego, dyskusje dotyczące cywilnoprawnych ścieżek ochrony danych osobowych nie odbywają się często, mimo rosnącego znaczenia tej ścieżki postępowania w praktyce prawnej. Wskazał również na zwiększającą się liczbę skarg wpływających do Urzędu, co z jednej strony świadczy o wzroście świadomości obywateli w zakresie ochrony danych osobowych, a z drugiej strony wskazuje na potrzebę pogłębionej współpracy między organami nadzorczymi a sądami w kontekście aplikacji przepisów RODO. W jednym z paneli dyskutowano m.in. o udziale Prezesa UODO w postępowaniu cywilnym sądowym oraz o znaczeniu kształtowania praktyki sądowej w taki sposób, aby uwzględniała interesy osób, których dane dotyczą. Stała współpraca i wymiana doświadczeń między instytucjami nadzorczymi a środowiskiem prawniczym są kluczowe dla budowania spójnej praktyki stosowania przepisów RODO

w postępowaniach cywilnych, co sprzyja jednolitej praktyce prawnej oraz zwiększaniu świadomości w zakresie ochrony danych osobowych w systemie cywilnym.

Podkreśleniem wagi tematu konferencji było podpisanie porozumienia o współpracy pomiędzy Urzędem Ochrony Danych Osobowych a Naczelną Radą Adwokacką (6.11.2026 r.) w obszarze ochrony praw i wolności obywatelskich, ze szczególnym uwzględnieniem prawa do prywatności i ochrony danych osobowych. Celem podpisanego porozumienia jest pogłębienie w środowisku prawniczym znaczenia przepisów RODO w praktyce sądowej i prawnej.

### 19) PAIH Forum Biznesu 2025. Warszawa, 6.11.2025 r.

Podczas spotkania poruszone zostały zagadnienia związane z ochroną konkurencji i konsumentów, ochroną środowiska, bezpieczeństwem produktów, regulacjami celnymi, ochroną danych osobowych, pomocą publiczną oraz kosztami przesyłek. Eksperci omówili także sposoby skutecznego kształtowania i egzekwowania przepisów, aby wspierać rozwój uczciwej i zrównoważonej gospodarki cyfrowej w Polsce i w Europie. W panelu dyskusyjnym, którego tematem było „Kształtowanie i egzekwowanie przepisów krajowych i unijnych w celu zapewnienia równych warunków konkurencji i konsumentów, ochrony środowiska, bezpieczeństwa produktów, ceł, ochrony danych osobowych, pomocy publicznej i kosztów przesyłek”, wystąpił Konrad Komornicki, zastępca prezesa UODO,
Organizatorem wydarzenia była Izba Gospodarki Elektronicznej.

### 20) Konferencja „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach”. Warszawa, 19.11.2025 r.




Liczne interwencje Prezesa UODO w sprawie groźnych incydentów dotyczących ujawnienia przez media danych osobowych, w szczególności tych dotyczących osób małoletnich, było główną przyczyną zorganizowania tego wydarzenia. Kluczowe wątki i spostrzeżenia, które wybrzmiały podczas konferencji dotyczyły konieczności zachowania równowagi pomiędzy interesem publicznym a prawami jednostki, co w praktyce dziennikarskiej oznacza współistnienie wolności wypowiedzi z jednej strony a prawem do prywatności z drugiej. Dziennikarze często błędnie zakładają, że RODO ich nie dotyczy. Tymczasem działalność prasowa nie jest całkowicie wyłączona spod zasad ochrony danych osobowych. Szczególnie problematyczne jest wąskie lub nieprawidłowe rozumienie pojęcia „dane osobowe”, sprowadzane jedynie do imienia i nazwiska, mimo że identyfikacja może następować również poprzez kontekst, głos czy wizerunek. Podczas konferencji wyraźnie rozróżniono ciekawość opinii publicznej od rzeczywistego interesu publicznego, podkreślając, że ten drugi nie może usprawiedliwiać ingerencji w sferę prywatną osób niepełniących funkcji publicznych. Szczególnej ochrony wymagają dzieci, ofiary przestępstw, świadkowie oraz osoby

słabsze — w ich przypadku interes publiczny częściej przemawia za anonimizacją niż za ujawnieniem tożsamości. Zwrócono również uwagę, że archiwa redakcyjne są obszarem największych napięć z RODO, zwłaszcza w kontekście prawa do bycia zapomnianym, anonimizacji starszych materiałów oraz długiego okresu przechowywania treści, które po latach mogą ponownie nabrać aktualności. Prawo do bycia zapomnianym zarysowano jako ważny, lecz problematyczny element relacji między ochroną danych a misją mediów, a nie jako proste uprawnienie do usuwania treści. Postawiono pytanie, jak powinno ono funkcjonować w odniesieniu do materiałów prasowych — zarówno archiwalnych publikacji, jak i materiałów roboczych oraz źródłowych. Podkreślono, że są to sytuacje wymagające odmiennego podejścia i nie mogą być oceniane jednolicie.

Podkreślono, że ochrona danych w mediach nie kończy się na publikacji materiału, lecz obejmuje również zaplecze techniczne, przechowywanie nagrań, dostęp do plików i procedury redakcyjne. Media przetwarzają dziś dane osobowe na wielu nośnikach — od laptopów i serwerów, przez kamery, dyktafony i karty pamięci, po archiwa cyfrowe — a największym ryzykiem pozostaje nie sama technologia, lecz czynnik ludzki, brak standardów oraz chaos organizacyjny.

Mając na uwadze powagę zagadnień związanych z zapewnieniem skutecznej ochrony danych osobowych w działalności dziennikarskiej, w UODO powstał dokument pn. „Wnioski Prezesa UODO z Konferencji „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach", który wyszczególnia problematyczne, niedoregulowane obszary działalności mediów, gdzie występuje niebezpieczeństwo naruszenia realnej ochrony danych osobowych.

Organizatorzy konferencji: Prezes UODO i Społeczny Zespół Ekspertów przy Prezesie UODO.

### 21) IV Konferencja Naukowa pt. „Bezpieczeństwo informacji w organizacji i jej zasobów". Katowice, 26.11.2025 r.




Konferencja poświęcona była bezpieczeństwu informacji i ochronie danych osobowych w organizacjach. Tematyka debat skupiała się na wyzwaniach, jakie niesie rozwój technologii cyfrowych dla ochrony danych w administracji publicznej, edukacji i biznesie. Podczas wydarzenia omawiane były m.in. takie zagadnienia, jak: etyczne aspekty związane z przetwarzaniem danych osobowych w placówkach oświatowych i na uczelniach publicznych, zmiany roli IOD po ośmiu latach od wprowadzenia RODO, nowoczesne technologie jako wyzwania w administracji publicznej, zasoby ludzkie a bezpieczeństwo w organizacjach, cyberataki w administracji. Omówiono opinię EROD nr 28 z 2024 r. zawierającą uwagi dotyczące wykorzystania danych osobowych w modelach sztucznej inteligencji oraz orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej odnoszące się do takich danych jak: dynamiczny adres IP, ocena na egzaminie z komentarzem egzaminatora, nr VIN pojazdu, nr przypisany do użytkownika internetu w celu wysyłania mu

spersonalizowanej reklamy. Wskazano też obszary, w których wykorzystanie sztucznej inteligencji jest najpowszechniejsze i jakie wiążą się z tym korzyści i zagrożenia.

Uczestnicy konferencji mogli również skorzystać z konsultacji prawnych z zakresu ochrony danych osobowych, prowadzonych przez eksperta Urzędu Ochrony Danych Osobowych.

Organizatorem wydarzenia był Urząd Ochrony Danych Osobowych we współpracy z Katedrą Prawa Gospodarczego Wydziału Finansów Uniwersytetu Ekonomicznego w Katowicach we współpracy z GUS, Śląskim Urzędem Wojewódzkim, Ministerstwem Sportu i Turystyki.

### 22) Konferencja „Nowe Horyzonty Biometrii – Bezpieczeństwo, Tożsamość, Rozwój". Warszawa, 26.11.2025 r.




Prezes Urzędu Ochrony Danych Osobowych, Fundacja AI One Health oraz Społeczny Zespół Ekspertów przy Prezesie UODO byli organizatorami tego wydarzenia. W ostatnich latach technologie biometryczne zyskały na znaczeniu, stając się kluczowym elementem różnych systemów, w tym systemów bezpieczeństwa. Na popularność biometrii wpływa przede wszystkim wygoda stosowania tej technologii, która – opierając się na unikalnych cechach danej osoby – wydaje się bezpieczna, bo trudna do podrobienia. Warto jednak zauważyć, że rozwój tej technologii wiąże się z zagrożeniami, które wymagają analizy. W przypadku wycieku danych biometrycznych może dojść do trwałej utraty tożsamości, gdyż cechy biologiczne są niezmienne.

Na konferencję składały się trzy panele dyskusyjne. Pierwszy dotyczył biometrii w medycynie oraz jej potencjalnych korzyści i zagrożeń, drugi - cyfrowego portfela tożsamości i jego znaczenia dla sprawnego funkcjonowania państwa, natomiast trzeci panel poświęcony był wykorzystaniu biometrii w środowisku pracy i Smart-City, z uwzględnieniem granic biometrycznego monitoringu i prawa konsumenta w erze biometrii.

Konferencja miała na celu promowanie odpowiedzialnego rozwoju biometrii, wymianę wiedzy międzysektorowej w tej dziedzinie, analizę wyzwań prawnych i etycznych związanych ze stosowaniem omawianej technologii. Prelegenci skupiali się na prezentacji dobrych praktyk i innowacji dla bezpiecznego wykorzystywania biometrii, wzmocnieniu współpracy międzynarodowej w tym obszarze oraz kształtowaniu świadomości społecznej o ryzykach biometrii i sztucznej inteligencji.

Wydarzenie zostało objęte patronatem honorowym przez Ministerstwo Zdrowia oraz Ministerstwo Cyfryzacji.

## 23) Konferencja UODO i Rady Europy na temat sztucznej inteligencji. Warszawa, 10.12.2025 r.




Międzynarodowa konferencja „The Role of the Council of Europe's Framework Convention on Artificial Intelligence in the Protection of Privacy and Personal Data – Legal, Ethical and Social Challenges in the AI Era" odbyła się w siedzibie UODO.

To pierwsze tego typu wydarzenie w Polsce w pełni poświęcone znaczeniu Konwencji Ramowej o Sztucznej Inteligencji w kontekście ochrony danych osobowych oraz wyzwań prawnych, etycznych i społecznych, jakie niesie dynamiczny rozwój AI. Konwencja miała charakter wzmacniający wobec obowiązujących przepisów, a jej rolą jest stworzenie spójnych ram interpretacyjnych i uzupełnienie istniejących instrumentów ochrony praw człowieka. Wiele uwagi poświęcono metodologii HUDERIA, która ma służyć ocenie wpływu systemów AI na prawa człowieka, praworządność i demokrację. O tym, jak bardzo ważny jest to temat potwierdziły badania, w których większość respondentów, w szczególności z sektora publicznego, nie potrafiła ocenić, czy stosowane przez nich systemy AI przetwarzają dane osobowe. Organizacje zgłosiły potrzebę większego wsparcia w obszarze AI, w tym szkoleń dla zarządów oraz praktycznych wytycznych dotyczących wdrażania systemów opartych na sztucznej inteligencji. W panelu poświęconym analizie relacji pomiędzy Konwencją Ramową o AI a przepisami dotyczącymi ochrony danych osobowych podkreślano, że aby konwencja mogła spełniać swoją rolę, jej postanowienia muszą być właściwie powiązane z mechanizmami ochrony danych. Obecnie pomiędzy regulacjami istnieją jeszcze obszary wymagające doprecyzowania. Zwrócono również uwagę na znaczenie wspólnego rozumienia ryzyka związanego z AI. Jak podkreślano, wszyscy uczestnicy procesu powinni posługiwać się „tą samą mapą", co pozwoli na bardziej przewidywalne i odpowiedzialne stosowanie sztucznej inteligencji. Wskazano także na konieczność horyzontalnych rozwiązań prawnych ułatwiających funkcjonowanie przedsiębiorstw, zwłaszcza z sektora MŚP. Podczas konferencji zaprezentowane zostały wyniki badania UODO przeprowadzonego przez Grupę roboczą ds. sztucznej inteligencji, powstałą w ramach Społecznego Zespołu Ekspertów przy Prezesie UODO. Badanie to wykazało, że niski poziom świadomości dotyczący przetwarzania danych osobowych w systemach AI jest jedną z głównych barier utrudniających ich bezpieczne wdrażanie. Organizacje często nie potrafią ocenić, czy dane osobowe rzeczywiście są wykorzystywane podczas prac nad rozwiązaniami AI, co tworzy ryzyko niezgodności z przepisami. Dlatego potrzebne są szkolenia wykraczające poza klasyczne ujęcie ochrony danych osobowych, obejmujące ocenę ryzyka, analizę cyklu życia systemów AI oraz zasady praktycznego wdrażania modeli. Konieczne jest też zapewnienie odpowiedniego wyjaśnienia działania modeli oraz zgodności z wymaganiami Konwencji 108+ Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Analizując rolę sztucznej

inteligencji w systemie wymiaru sprawiedliwości uznano, że AI może znacząco usprawnić procesy administracyjne oraz analityczne w sądach. Przedstawiono przykład Hiszpanii, gdzie automatyzacja procedur pozwoliła skrócić proces przyznawania obywatelstwa z pięciu lat do pięciu miesięcy, co pokazuje potencjał technologii w przyspieszaniu działania instytucji publicznych.

Uczestnicy konferencji zgodni byli, że punktem wyjścia dla wdrażania AI musi być zdefiniowanie problemu, który technologia ma rozwiązać, a nie sama dostępność nowego narzędzia. Konwencja Ramowa i metodologia HUDERIA stanowią dla instytucji wymiaru sprawiedliwości i szerzej rozumianego sektora publicznego istotny, wspólny punkt odniesienia, także poza Europą. Konferencja potwierdziła konieczność budowania spójnych, praktycznych i opartych na prawach człowieka ram prawnych, które umożliwią odpowiedzialne i bezpieczne wdrażanie sztucznej inteligencji. Zarówno wyniki badania UODO, jak i głosy ekspertów pokazały, że rozwój AI wymaga ścisłej współpracy krajowej i międzynarodowej oraz inwestycji w kompetencje organizacji publicznych, prywatnych i użytkowników. UODO będzie kontynuować działania wspierające podmioty w dostosowaniu się do nowych wyzwań i standardów związanych ze sztuczną inteligencją w zakresie związanym z ochroną danych.

Organizatorem wydarzenia był Urząd Ochrony Danych Osobowych we współpracy z SZE, Radą Europy i Europejską Komisją na rzecz Efektywności Wymiaru Sprawiedliwości (CEPEJ).

### 1.14. UODO rusza w kraj

„UODO rusza w kraj” – to inicjatywa Prezesa UODO, której celem jest przybliżenie mieszkańcom Polski problematyki ochrony danych osobowych oraz lepszego rozpoznania problemów z jakimi mierzą się lokalne społeczności i jednostki samorządu terytorialnego (JST) w różnych regionach naszego kraju. Urząd Ochrony Danych Osobowych nie posiada jednostek terenowych, a dzięki tej akcji ma możliwość lepiej poznać lokalne problemy związane z ochroną danych osobowych i lepszego ich zrozumienia. W ramach programu organizowane są spotkania w różnych częściach kraju, skierowane do wielu grup społecznych. Uczestnikami są m.in. uczniowie, studenci, nauczyciele, przedstawiciele administracji publicznej, przedsiębiorcy, seniorzy oraz organizacje społeczne. Dzięki temu inicjatywa dociera zarówno do osób prywatnych, jak i instytucji odpowiedzialnych za przetwarzanie danych osobowych. Spotkania organizowane są zarówno na prośbę wybranych podmiotów (i we wskazanym przez nich zakresie, z wyraźnym zaznaczeniem potrzeb grupy docelowej), jak i z inicjatywy samego Urzędu, który wychodzi do JST z propozycjami spotkań czy dedykowanych szkoleń. Spotkania odbywają się w ramach uzgodnień dokonywanych z władzami wojewódzkimi i samorządowymi. Impulsem do uruchomienia programu było sprawozdanie Najwyższej Izby Kontroli opublikowane w 2024 r. wskazujące na systemowe problemy ochrony danych osobowych w polskich JST.

Cele inicjatywy to:

- lepsze zrozumienie przez kadrę UODO lokalnych problemów ochrony danych osobowych;
- zwiększenie świadomości społeczeństwa w zakresie ochrony danych osobowych oraz promowanie właściwych praktyk związanych z przetwarzaniem danych;
- umożliwienie mieszkańcom odwiedzanego regionu uzyskania bezpośrednio porady ze strony wykwalifikowanych ekspertów UODO;
- nawiązanie przez Urząd bezpośrednich kontaktów z administratorami danych osobowych i inspektorami danych, w tym przede wszystkim współpracy z samorządem terytorialnym.

Podczas spotkań uczestnicy mogą pogłębić wiedzę o prawach wynikających z RODO, zasadach przetwarzania danych osobowych, w tym w zakresie dotyczącym dostępu do danych czy możliwości ich zmiany i usunięcia, a także obowiązkach administratorów danych. Istotnym elementem jest również edukacja w zakresie bezpieczeństwa w Internecie, ochrony wizerunku, szczególnie w odniesieniu do osób najmłodszych w zakresie zagrożeń takich jak m.in. deepfake, phishing czy wycieki danych. Omawiane są także aktualne wyzwania związane z nowymi technologiami i mediami społecznościowymi.

Ważnym elementem programu jest również prowadzenie bezpośredniego dialogu z uczestnikami spotkań, udzielanie odpowiedzi na pytania, rozwiewanie wątpliwości interpretacyjnych i analiza konkretnych przypadków związanych ze stosowaniem RODO w praktyce. Taka forma kontaktu umożliwia lepsze zrozumienie przepisów oraz pomaga w rozwiązywaniu bieżących problemów, z jakimi mierzą się różne środowiska.

Program ma charakter praktyczny i interaktywny – oprócz prelekcji organizowane są warsztaty, szkolenia, konferencje (często we współpracy z uczelniami wyższymi lub organizacjami branżowymi) oraz konsultacje, które umożliwiają uczestnikom analizowanie konkretnych sytuacji. Dzięki temu „UODO rusza w kraj" nie tylko przekazuje wiedzę, ale również pomaga w jej zastosowaniu w codziennym życiu.

O działaniach w ramach programu „UODO rusza w kraj" Urząd informuje na swojej stronie internetowej i na platformie X. Na potrzeby programu tworzy liczne materiały promocyjne, które udostępnia partnerom akcji.

1) W 2025 roku pierwszym kierunkiem akcji „UODO rusza w kraj" było **województwo pomorskie,** gdzie 30-31 stycznia, w ramach opisanego wcześniej XIX Dnia Ochrony Danych Osobowych, odbywały się spotkania z mieszkańcami oraz władzami wojewódzkimi i samorządowymi tego rejonu. Uruchomione też zostały punkty konsultacyjno-informacyjne UODO w Kwidzynie, Gdańsku i Gdyni. Natomiast w Zespole Szkól nr 1 im. Stanisława Staszica w Kwidzynie zorganizowana została konferencja dla dyrektorów szkół, nauczycieli, rodziców oraz władz lokalnych, podczas której omówiono aktualne wyzwania dotyczące ochrony danych osobowych w sektorze oświaty. Szczególne miejsce w programie zajmowała promocja Programu

edukacyjnego UODO „Twoje dane – Twoja sprawa", realizowanego przez Zespół Szkół nr 1 w Kwidzynie oraz debata uczniów na temat publikacji wizerunku w internecie.

W ramach akcji „UODO rusza w kraj" w województwie pomorskim Prezes Urzędu Mirosław Wróblewski uczestniczył w spotkaniu z przedstawicielami Okręgowej Izby Radców Prawnych.

2) **Województwo podkarpackie** było kolejnym etapem akcji „UODO rusza w kraj" (20-21.03.2025 r.). Podczas spotkania z przedstawicielami Okręgowej Izby Radców Prawnych (OIRP) w Rzeszowie oraz prezydentem Miasta Rzeszowa powołano w tym mieście **terenowy punkt konsultacyjny UODO**, który oficjalnie rozpoczął działalność 15 grudnia 2025 r. Ponadto Urząd Ochrony Danych Osobowych we współpracy z OIRP w Rzeszowie, Wojewodą Podkarpackim oraz Społecznym Zespołem Ekspertów przy Prezesie UODO zorganizował w Rzeszowie konferencję naukową pt. „Bezpieczeństwo informacji w organizacji", poświęconą m.in. nowoczesnym technologiom i roli Inspektora Ochrony Danych w organizacji. Poruszono w niej tematy związane z cyberbezpieczeństwem, sztuczną inteligencją w medycynie, ochroną danych osobowych w turystyce oraz oświacie. Wydarzeniu towarzyszyła prezentacja inicjatyw edukacyjnych realizowanych przez Szkołę Podstawową nr 17 w Rzeszowie, która jest uczestnikiem XV edycji programu UODO Twoje dane – Twoja sprawa. Ponadto prowadzone były rozmowy na tematy związane z powszechnym udostępnianiem w Internecie danych osobowych dzieci i młodzieży, w tym ich wizerunku.

3) W **województwie wielkopolskim** działania Urzędu Ochrony Danych Osobowych w ramach ogólnopolskiej inicjatywy „UODO rusza w kraj", obejmowały serię spotkań, konsultacji i dyskusji skierowanych do przedstawicieli administracji publicznej, lokalnych organizacji oraz mieszkańców regionu (20-21 maja 2025 r).

W trakcie spotkania z przedstawicielami jednostek administracji publicznej, które odbyło się w Urzędzie Marszałkowskim Województwa Wielkopolskiego, eksperci UODO zaprezentowali kwestie związane z aktualnymi wyzwaniami dotyczącymi przetwarzania danych osobowych w działalności podmiotów publicznych, określili rolę i pozycje inspektorów ochrony danych w podmiotach publicznych oraz ich współpracę z UODO. Prezes Mirosław Wróblewski wskazał na konieczność systemowej ochrony praw dzieci w internecie, które określił jako wyzwanie o charakterze cywilizacyjnym oraz zaakcentował, że Urząd wspiera inicjatywy zmierzające do skutecznej weryfikacji wieku użytkowników w środowisku cyfrowym.

W ramach działań skierowanych do mieszkańców regionu, w umówionych punktach konsultacyjnych, możliwe było skorzystanie z bezpłatnych porad ekspertów UODO. Osoby uczestniczące miały okazję uzyskać odpowiedzi na pytania dotyczące ochrony danych osobowych, praktycznych aspektów RODO oraz poznać rozwiązania służące zapewnieniu odpowiedniego poziomu ochrony danych w sferze prywatnej i zawodowej.

Z kolei w Poznaniu odbyło się spotkanie z seniorami, podczas którego omówiono tematy związane z nowymi technologiami i sztuczną inteligencją oraz ich wpływu na ochronę danych osobowych. Poruszono również kwestię praw osób starszych

w kontekście korzystania z usług cyfrowych, a eksperci UODO udzielali praktycznych porad i wskazówek dotyczących bezpiecznego przetwarzania danych.

W trakcie pobytu w Poznaniu odbyło się również spotkanie z przedsiębiorcami pod hasłem „Ochrona danych osobowych w prowadzeniu działalności gospodarczej". Podczas sesji poruszono tematykę aktualnych wyzwań stojących przed przedsiębiorcami w zakresie stosowania przepisów RODO, a eksperci UODO udzielali praktycznych porad i wskazówek ułatwiających prawidłowe zarządzanie danymi w firmach.

Na zakończenie wizyty odbyło się również spotkanie z członkami Okręgowej Izby Radców Prawnych w Poznaniu, podczas którego dyskutowano m.in. wokół tematyki zasad ochrony danych osobowych w procesie stanowienia prawa.

4) Kolejny przystanek akcji „UODO rusza w kraj" odbył się w **województwie warmińsko-mazurskim (16-17 października 2025 r.)** we współpracy z Wydziałem Prawa i Administracji UWM oraz lokalnymi partnerami społecznymi i samorządowymi. Wizyta obejmowała serię spotkań, konferencję naukową, warsztaty, konsultacje prawne oraz dialog ekspercki między Urzędem a lokalnymi partnerami.

Pierwszego dnia akcji, 16 października 2025 r., w Centrum Ekspozycyjnym Stara Kotłownia w Olsztynie, odbyła się konferencja naukowa pt. „**Bezpieczeństwo informacji w organizacji i jej zasobów**", adresowana zarówno do przedstawicieli administracji publicznej, jak i środowiska akademickiego, przedsiębiorców oraz instytucji oświatowych. Tematyka konferencji objęła szerokie spektrum zagadnień związanych z bezpieczeństwem informacji, przetwarzaniem danych osobowych w organizacjach oraz wyzwaniami wynikającymi z wykorzystywania nowoczesnych technologii, w tym odniesień do zastosowań sztucznej inteligencji i ich wpływu na ochronę prywatności. Poruszono też kwestie ochrony danych małoletnich i ich wizerunku, obowiązków organizacji wobec dostawców zewnętrznych, roli inspektorów ochrony danych w strukturach organizacyjnych oraz praktycznych aspektów przetwarzania danych w warunkach cyfryzacji. Program konferencji uwzględniał również dyskusje o dobrych praktykach oraz o tym, jak instytucje – zarówno publiczne, jak i prywatne – mogą efektywnie odpowiadać na ryzyka związane z wykorzystaniem danych w codziennej działalności.

Natomiast w Urzędzie Miasta Olsztyna odbywały się bezpłatne porady prawne i konsultacje prowadzone przez pracowników infolinii UODO, podczas których mieszkańcy regionu mogli uzyskać praktyczne wskazówki dotyczące swoich praw, sposobów reagowania na ewentualne naruszenia ich danych osobowych oraz mechanizmów ochrony prywatności w codziennym życiu.

Drugiego dnia, 17 października 2025 r., w Warmińsko-Mazurskim Urzędzie Wojewódzkim odbyło się spotkanie skierowane przede wszystkim do przedstawicieli administracji publicznej województwa, inspektorów ochrony danych, administratorów oraz przewodniczących rad jednostek samorządu terytorialnego i Sejmiku Województwa. Spotkanie koncentrowało się na wymianie doświadczeń oraz omówieniu praktycznych wyzwań, które napotykają organy administracji w procesach implementacji zasad ochrony danych, planowania działań kontrolnych i reagowania na naruszenia.

5) W **województwie lubuskim (28 października 2025 r.)** Urząd Ochrony Danych Osobowych kontynuował ogólnopolską akcję edukacyjno-informacyjną „UODO rusza w kraj". W Gorzowie Wielkopolskim przedstawiciele Urzędu realizowali program spotkań i rozmów na temat aktualnych wyzwań związanych z ochroną danych w sektorze publicznym i prywatnym oraz na temat wpływu technologii, w tym sztucznej inteligencji, na kształtowanie bezpieczeństwa informacji. Pierwszym punktem wizyty było spotkanie z przedstawicielami administracji publicznej województwa lubuskiego w siedzibie Lubuskiego Urzędu Wojewódzkiego, które stanowiło okazję do omówienia praktycznych aspektów stosowania przepisów o ochronie danych osobowych w jednostkach samorządu terytorialnego oraz administracji zespolonej, z uwzględnieniem roli inspektorów ochrony danych i systemów bezpieczeństwa informacji. Prezes UODO, Mirosław Wróblewski, wraz z pracownikami Urzędu, wzięli udział w otwartym spotkaniu dla mieszkańców Gorzowa Wielkopolskiego, które odbyło się w Akademii im. Jakuba z Paradyża. Tematem przewodnim dyskusji były prawne ramy ochrony danych w związku z dynamicznym rozwojem technologii cyfrowych oraz rosnącym znaczeniem sztucznej inteligencji, a także zagadnienia związane z zachowaniem prywatności i etycznym wykorzystaniem informacji.

Ważnym punktem programu było również spotkanie ekspertów UODO z przedsiębiorcami z regionu województwa lubuskiego, zorganizowane w siedzibie Zachodniej Izby Przemysłowo-Handlowej. Rozmowy dotyczyły praktycznych wyzwań związanych z ochroną danych osobowych w działalności małych i średnich przedsiębiorstw, m.in. konieczności wdrażania rozwiązań zwiększających ich bezpieczeństwo oraz dostosowywania procesów przetwarzania do obowiązujących standardów prawnych.

Podczas wizyty w województwie lubuskim doszło także do podpisania porozumienia o współpracy pomiędzy UODO a Akademią im. Jakuba z Paradyża, które zakładało wspólne działania w obszarze edukacji, badań naukowych, działalności promocyjnej, wydawniczej oraz organizacji praktyk studenckich.

6) **„UODO rusza w kraj" – województwo mazowieckie (5 listopada 2025 r.)**

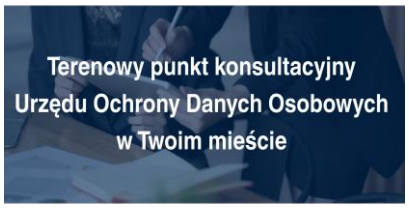
Urząd Ochrony Danych Osobowych zrealizował kolejną odsłonę ogólnopolskiej inicjatywy edukacyjno-konsultacyjnej „UODO rusza w kraj" w województwie mazowieckim, odwiedzając miasto Płock. Program wizyty miał na celu przybliżenie zasad ochrony danych osobowych, prywatności i bezpieczeństwa informacji osobom z różnych środowisk oraz instytucjom publicznym.

W ramach działań otworzono punkt porad, a podczas wizyty w Akademii Mazowieckiej odbył się wykład pt. **„Wyzwania związane z przetwarzaniem danych osobowych w działalności podmiotów publicznych"**, W trakcie wykładu omówiono aktualne problemy i praktyczne aspekty związane z działalnością administracji publicznej w kontekście ochrony danych osobowych, przybliżając uczestnikom kluczowe zasady bezpiecznego i zgodnego z prawem przetwarzania informacji. Podczas wizyty w Płocku, Prezes UODO Mirosław Wróblewski podkreślił, że ochrona danych osobowych stanowi fundament bezpieczeństwa państwa, ponieważ rejestry publiczne są potencjalnym celem ataków ze względu na zgromadzone w nich ogromne ilości danych osobowych. W ramach „UODO rusza w kraj" w województwie

mazowieckim odbyły się spotkania prowadzone przez specjalistów UODO, poświęcone roli inspektorów ochrony danych w podmiotach publicznych, współpracy z Urzędem, wyzwaniom związanym z nowymi technologiami oraz praktycznym wskazówkom dotyczącym dbania o prywatność, także wśród osób starszych.

Prezes UODO planuje odwiedzić wszystkie województwa do końca 2026 r., a następnie kontynuować program w kolejnych miejscowościach, w ramach uzgodnień z władzami wojewódzkimi i samorządowymi.

### 1.15. Terenowy punkt konsultacyjny w Rzeszowie




Urząd Ochrony Danych Osobowych nie posiada struktur terenowych, co utrudnia obywatelom bezpośredni kontakt z Urzędem i możliwość stacjonarnego załatwienia sprawy. Podczas realizowanych od 2024 roku wyjazdów w ramach akcji „UODO rusza w kraj", do prezesa UODO docierały sygnały o potrzebie jeszcze większej obecności Urzędu w terenie. Z tego względu podjęta została decyzja o uruchomieniu pilotażowo pierwszego terenowego punktu konsultacyjnego Urzędu Ochrony Danych Osobowych. Dzięki otwartości i współpracy z Okręgową Izbą Radców Prawnych w Rzeszowie, punkt rozpoczął działalność 15 grudnia 2025 r. w siedzibie tego samorządu. Punkt konsultacyjny będzie czynny przez jeden dzień w godzinach 11:00-15:00, raz na dwa miesiące. Będzie prowadzony bezpłatnie i bez konieczności dokonywania zapisów, aby każdy zainteresowany mógł swobodnie skorzystać ze wsparcia ekspertów UODO. Na miejscu będzie również możliwość złożenia skargi do Prezesa UODO i uzyskanie informacji o przysługujących prawach. W zamierzeniu tego pilotażu, obecność ekspertów UODO w terenie miała również ułatwić pracownikom UODO zbieranie informacji zwrotnych, co do potrzeb społeczeństwa w zakresie ochrony danych osobowych i poprawy ich bezpieczeństwa. Kolejne ewentualne pilotażowe punkty konsultacyjne będą organizowane stopniowo, zależnie od potrzeb obywateli oraz możliwości organizacyjnych UODO.

Efekty działania terenowego punktu konsultacyjnego UODO w Rzeszowie zostaną przedstawione m.in. parlamentowi.

### 1.16. 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 pn. „Ochrona danych osobowych i technologia"[667]. Wykłady eksperckie członków Społecznego Zespołu Ekspertów przy Prezesie UODO kontynuowane były w 2025 roku.

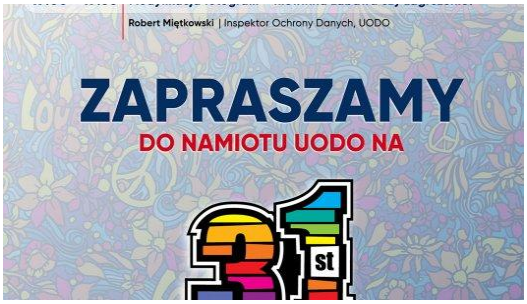
- *„Proces monitorowania postępu technologicznego jako element rozliczalności stosowania zasady ochrony danych w fazie projektowania oraz domyślnej*

[667] Nagranie wykładu dostępne jest pod linkiem: https://uodo.gov.pl/pl/592/3478.

*ochrony danych”* (24.01.2025 r.) Temat wykładu skupiał się na zastosowaniu zasady Privacy by Design w kontekście aktualnych trendów technologicznych oraz związanych z nimi zagrożeń dla ochrony danych osobowych. W wykładzie poruszono m.in. kwestie zagrożeń związanych ze stosowaniem systemów sztucznej inteligencji, a także omówiono zagadnienia dotyczące metod i technik anonimizacji i stosowania technologii wspierających prywatność (PETs). Wykład zawierał podstawowe wskazówki jak tworzyć narzędzia SI zgodnie z RODO.

- *„Technologie kwantowe – szanse i zagrożenia dla ochrony prywatności i danych osobowych”* (21.02.2025 r.). Czym są technologie kwantowe, jak działa komputer kwantowy oraz trendy rozwojowe budowy takich komputerów były głównym tematem tego wykładu. Omówiono w nim także algorytmy kwantowe, obecne możliwości komunikacji kwantowej oraz kryptografię kwantową i postkwantową. Drugą część wykładu poświęcono politykom Unii Europejskiej w zakresie technologii kwantowych, zaprezentowano Manifest Kwantowy, plan Europejskich Obliczeń Wielkiej Skali, projekty oraz strategie kwantowe w państwach europejskich.
- *„Krajobraz aktualnych zagrożeń w UE”* (14.04.2025 r.). W wykładzie tym zaprezentowano aktualny stan zagrożeń dla cyberbezpieczeństwa i ochrony danych osobowych w Unii Europejskiej, który wynika z raportów Agencji ENISA i CERT Polska. Przedstawiono najpowszechniejsze obecnie formy cyberataków jak phishing czy ransomeware, a także omówiono działanie grup ATP.
- *„Projektowanie systemów AI w modelu data protection by design zgodne z zasadami godnej zaufania AI* (30.05.2025 r.). W prezentacji przedstawione zostało unijne podejście do regulacji systemów sztucznej inteligencji, w tym Wytyczne Grupy Ekspertów wysokiego szczebla ds. sztucznej inteligencji, założenia Aktu w sprawie sztucznej inteligencji oraz przewidzianą w nim kwalifikację systemów SI. Omówione zostały obowiązki wynikające z RODO przy opracowaniu i stosowaniu systemów SI, a także wzorcowy model ochrony danych w fazie projektowania w kontekście opracowywania i stosowania systemów sztucznej inteligencji. Ważnym punktem tego wykładu było przedstawienie relacji między oceną skutków dla ochrony danych a oceną skutków systemów sztucznej inteligencji dla praw podstawowych.
- *„Ochrona danych w systemach sztucznej inteligencji* (20.06.2025 r.). Prelegent tego wykładu skupił się na tematyce przetwarzania danych osobowych w systemach SI z perspektywy RODO i Aktu w sprawie sztucznej inteligencji. Wyjaśnił zasady działania SI oraz różnice między klasycznym programowaniem a uczeniem maszynowym. Omówił pojęcie „podmiotu stosującego” oraz jego obowiązki wynikające z Aktu w sprawie sztucznej inteligencji. Podkreślił przy tym, że operacje na danych są głównym źródłem ryzyka naruszenia praw lub wolności osób fizycznych oraz podał przykłady zagrożeń. Następnie przedstawił listę kontrolną, którą podmioty stosujące mogą wykorzystać przy weryfikacji dostawców systemów SI.

### 1.17. Pol’and’Rock Festiwal




Pośród ponad 120 różnych instytucji uczestniczących w 31. edycji festiwalu Pol’and’Rock, który trwał od 30 lipca do 2 sierpnia 2025 r., obecny był Prezes UODO i jego przedstawiciele. Podobnie jak w ubiegłym roku, Urząd Ochrony Danych Osobowych aktywnie włączył się w edukacyjną część festiwalu, organizując własną strefę w Akademii Sztuk Przepięknych, w której przedstawiciele UODO przez cztery dni udzielali porad i konsultacji z zakresu ochrony danych osobowych. Gospodarzami tej strefy – oprócz pracowników Urzędu i ekspertów związanych z UODO, byli także członkowie Społecznego Zespołu Ekspertów przy Prezesie UODO.

Wydarzenie to stało się przestrzenią do poważnych rozmów o prawie do prywatności i ochrony danych osobowych, o cyberbezpieczeństwie i o nowych technologiach. Dużym zainteresowaniem odwiedzających cieszyły się panele tematyczne poświęcone kwestiom ochrony danych osobowych w kontekście praw obywatelskich i bieżących problemów społecznych, a także zagadnienia związane z RODO, w tym prawo do bycia zapomnianym. Nie zabrakło kwestii związanych z internetem, takich jak higiena cyfrowa, deepfake, ryzyko związane z aplikacjami internetowymi. Eksperci związani z UODO opowiadali o śladzie cyfrowym pozostawianym przez użytkowników portali społecznościowych. Edukowali też w kwestii bezpieczeństwa danych z dowodu osobistego.

Istotnym tematem poruszanym w strefie UODO były prawa dzieci w perspektywie ich obecności w internecie. W spotkaniach poświęconych tym zagadnieniom uczestniczył Konrad Ciesiołkiewicz z Państwowej Komisji do spraw Przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15. Pomiędzy kolejnymi wydarzeniami w namiocie UODO odbywały się quizy, gry symultaniczne i scenki edukacyjne oraz można było rozwiązywać krzyżówki i zagrać w kalambury.

W programie przewidziany był też wywiad z Prezesem UODO na temat wyzwań stojących przed ochroną danych osobowych, a także rozmowa między prezesem UODO Mirosławem Wróblewskim a przewodniczącym Społecznego Zespołu Ekspertów przy Prezesie UODO Mirosławem Gumularzem pt. „Dane jako waluta. Ochrona danych dziś i jutro”.

Udział Urzędu Ochrony Danych Osobowych w festiwalu Pol’and’Rock, podobnie jak ogólnopolska akcja edukacyjna pn. „UODO rusza w kraj”, to możliwość bezpośredniego spotkania i rozmów z ludźmi, a dla Urzędu – lepszego dopasowania działań informacyjnych i edukacyjnych, odpowiadających potrzebom społeczeństwa.

## 2. Działalność informacyjna

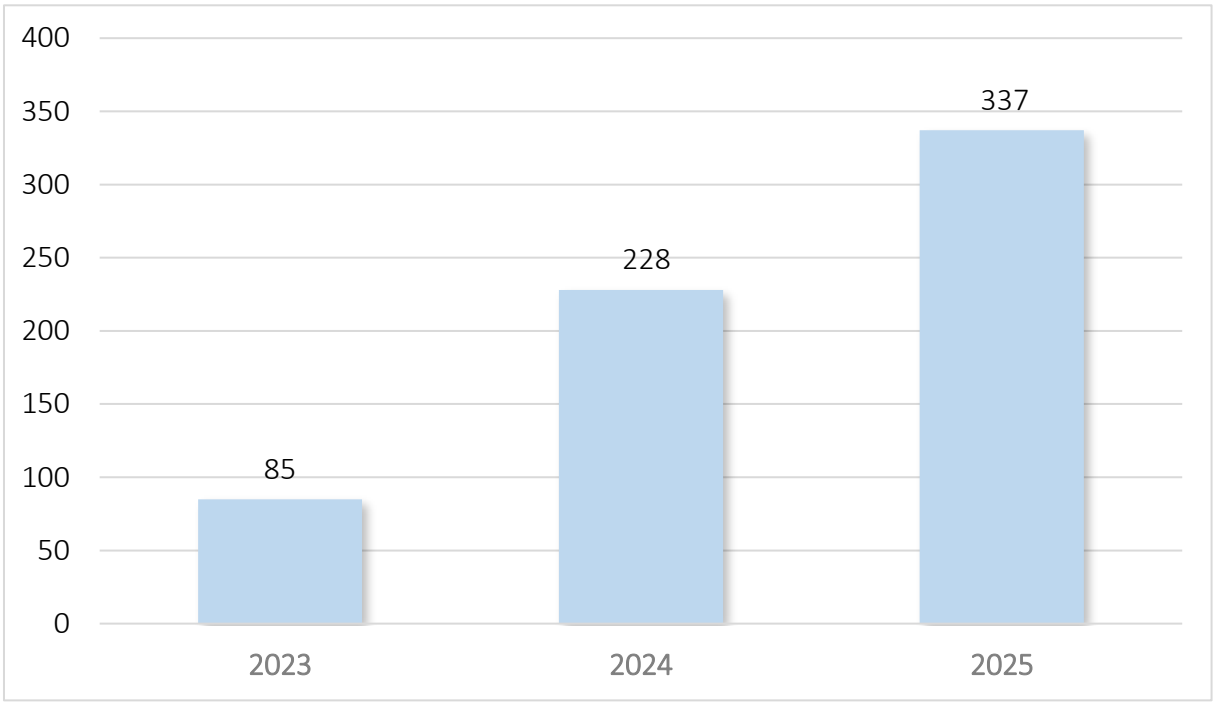
Działalność informacyjna UODO opiera się na informowaniu społeczeństwa o zadaniach organu nadzorczego, odnoszących się do monitorowania i przestrzegania

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. Wykonując to zadanie, eksperci UODO przekładają specjalistyczne zagadnienia dotyczące ochrony prywatności i danych osobowych na język zrozumiały dla wszystkich obywateli. Wiedzę o tym, z czym mierzą się obywatele, UODO czerpie z codziennego monitoringu mediów oraz z pytań dziennikarzy.

Jednostką odpowiedzialną za komunikaty i materiały multimedialne publikowane na stronie uodo.gov.pl oraz w mediach społecznościowych jest Departament Komunikacji Społecznej.

## 2.1. Komunikaty

W 2025 roku sformułowanie „Urząd Ochrony Danych Osobowych” pojawiło się w mediach w ponad 24 tysiącach publikacji, natomast na internetowej stronie organu uodo.gov.pl opubikowanych zostało **337** komunikatów. To o 109 więcej niż w roku 2024 i o 252 więcej niż w roku 2023.




**Wykres 23:** Porównanie liczy komunikatów opublikowanych na stronie internetowej UODO w latach 2023-2025.

Komunikaty były wykorzystywane przez media, a o wysokiej jakości teksów przygotowywanych w UODO świadczy fakt, że tylko w dwóch przypadkach rzecznik prasowy UODO musiał zwracać się do mediów o sprostowanie i doprecyzowanie informacji zawartych w artykule prasowym.

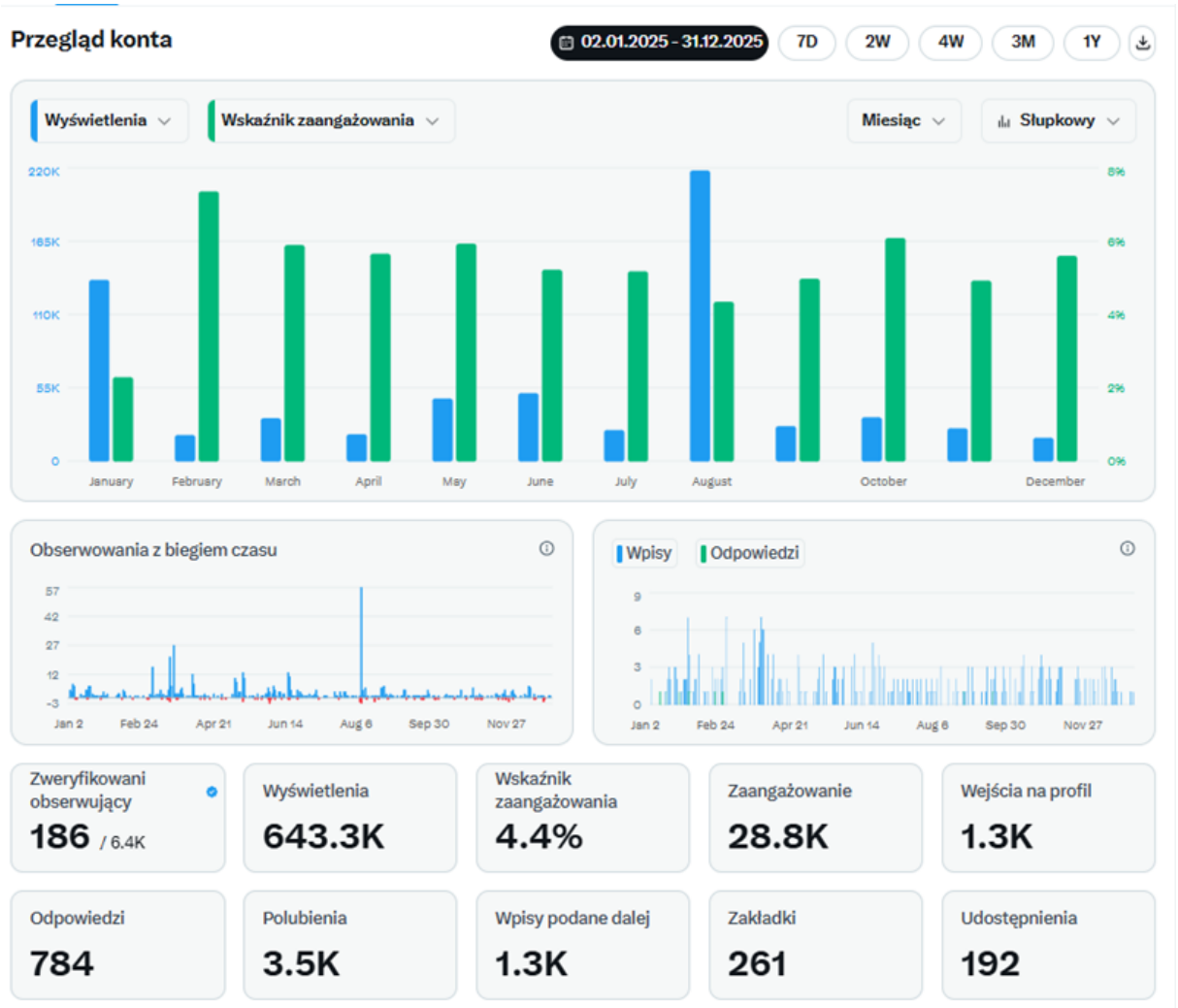
UODO komunikował przede wszystkim bieżącą działalność organu nadzorczego, w tym decyzje Prezesa UODO, jego udział w licznych konferencjach i spotkaniach, a także w pracach legislacyjnych, działaniach edukacyjnych i o współpracy z innymi instytucjami.

## 2.2. Social media

W 2025 r. Urząd prowadził działania informacyjne w social mediach:

- na platformie X opublikował 467 postów;
- na platformie Mastodon 467 postów;
- na platformie LinkedIn 227 postów, gdzie w 2025 przybyło 3 624 nowych obserwujących i łącznie jest ich obecnie 7 437;
- na YouTube, na który opublikowano 22 długie filmy oraz 23 shorty.

**Statystyki X:**

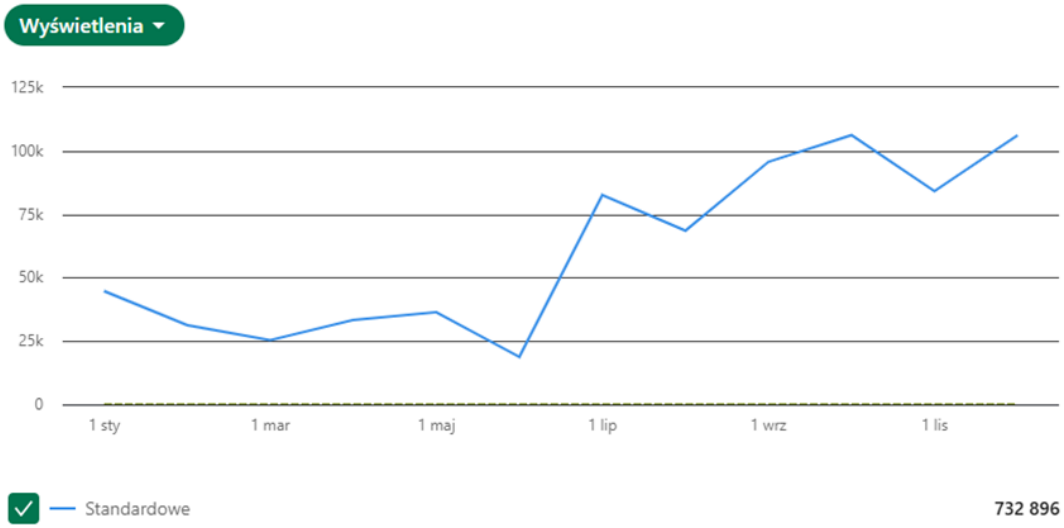


Poniżej, post o największej ilości wyświetleń, dotyczący jawności danych osobowych w CEIDG z 08.08.2025:



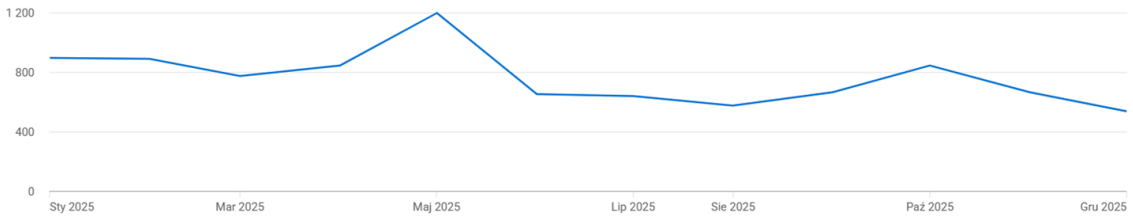

**Statystyki LinkedIn:**

227 opublikowanych postów w okresie od 01.01.2025 – 31.12.2025




**Statystyki youtube:**

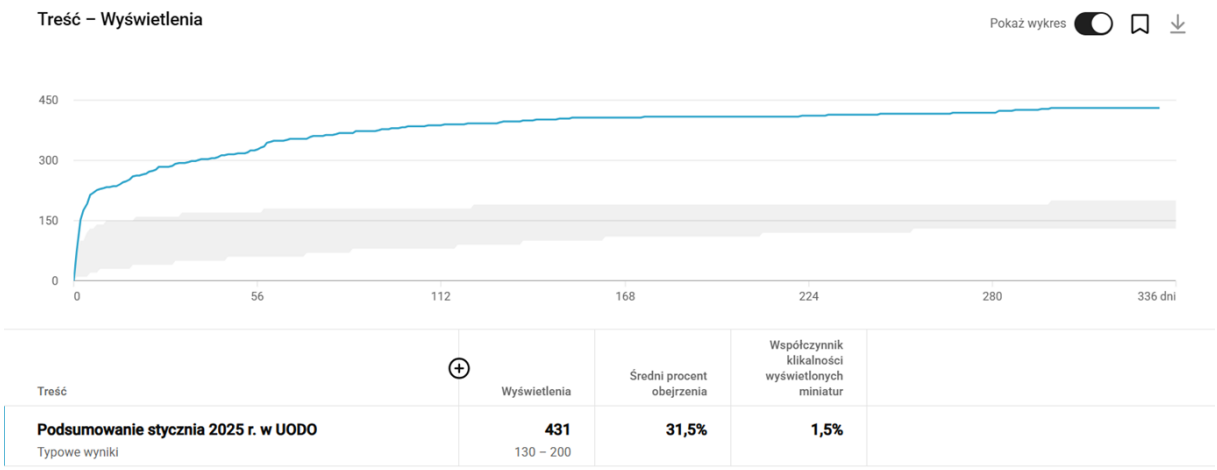
- w 2025 przybyło +99 subskrybentów;
- w 2025 roku opublikowano 22 długie filmy.




| Typ treści | Wyświetlenia | Średni procent obejrzenia | Współczynnik klikalności wyświetlonych miniatur |
|---|---|---|---|
| **Łącznie** | **9 205** | **16,3%** | **2,2%** |
| Filmy | 9 205 100% | 16,3% | 2,2% |

**Film o największej ilości wyświetleń w 2025 r.**

Podsumowanie stycznia 2025 w UODO – film opublikowano 03.02.2025 r.




| Treść | Wyświetlenia | Średni procent obejrzenia | Współczynnik klikalności wyświetlonych miniatur |
|---|---|---|---|
| **Podsumowanie stycznia 2025 r. w UODO**<br>Typowe wyniki | **431**<br>130 – 200 | **31,5%** | **1,5%** |

**SHORTY:**

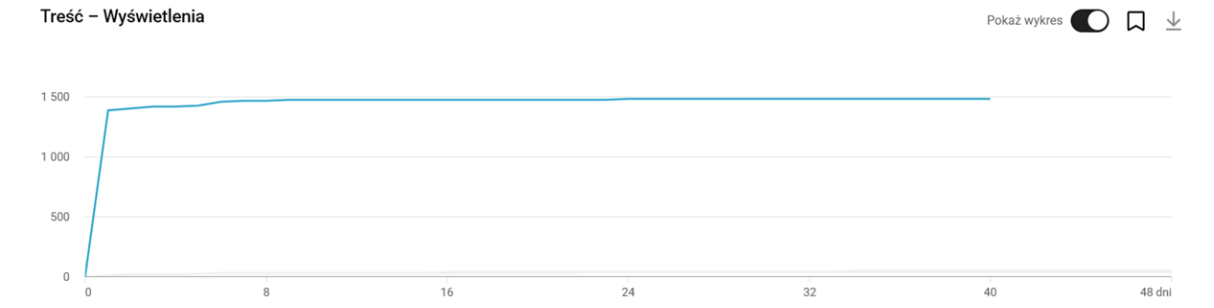
23 opublikowane shorty w 2025 r.




| Typ treści | Wyświetlenia | Średni procent obejrzenia | Współczynnik klikalności wyświetlonych miniatur |
|---|---|---|---|
| **Łącznie** | **3 009** | **90,1%** | **5,5%** |
| Shorts | 3 009 100% | 90,1% | 5,5% |

**Short o największej ilości wyświetleń**

Krajowy System Informacyjny Policji wymaga zmian – short opublikowano 20.11.2025 r.




| Treść | Wyświetlenia | Średni procent obejrzenia | Współczynnik klikalności wyświetlonych miniatur |
|---|---|---|---|
| **Krajowy System Informacyjny Policji wymaga zmian**<br>Typowe wyniki | **1 486**<br>30 – 60 | **65,9%** | **5,8%** |

## 2.3. Multimedia

W 2025 r. w UODO powstało 38 filmów video, których nagraniem, montażem i transkrykcją zajmowal się Departament Komunikacji Społecznej UODO. Ponadto opracowano także 72 relacje z konferencji, webinariów, szkoleń i wykładów organizowanych i współorganizowanych przez UODO oraz 81 dokumentacji fotograficznych z tych wydarzeń. Materiały te stanowiły bazę do późniejszych publikacji.

## 2.4. Biuletyn

Biuletynu UODO zawiera przegląd najważniejszych decyzji, orzeczeń sądowych, a także informacje o pracach i rozstrzygnięciach na forum europejskim i międzynarodowym. Na jego łamach znalazly się też wyjaśnienia budzących wątpliwości kwestii związanych ze stosowaniem RODO w praktyce.

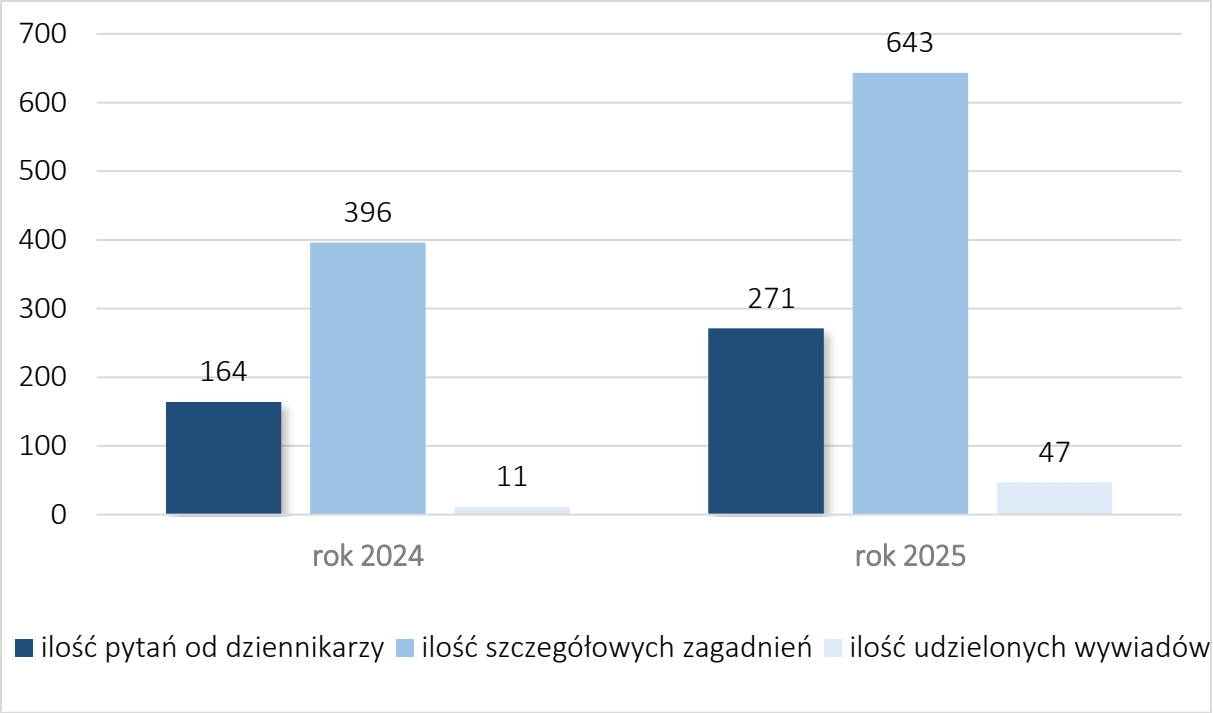
W 2025 r. opublikowano 10 edycji Biuletynu UODO, w których znalazło się 10 wywiadów z ekspertami i ponad 120 materiałów merytorycznych poruszających tematykę ochrony danych osobowych, prawa i nowych technologii. To łącznie ponad 450 stron, na których UODO komunikuje się z osobami zainteresowanymi tematyką ochrony danych osobowych. Materiały w Biuletynie mają szczególny charakter, gdyż nigdy nie dublują się z tymi dostępnymi na stronie internetowej Urzędu.

Na początku 2025 r. ukazał się numer specjalny Biuletynu zawierający archiwalne pytania inspektorów ochrony danych wraz z odpowiedziami Urzędu z okresu 31.08.2018 r. – 12.05.2022 r. To ponad 280 stron materiału stanowiącego odpowiedzi na niemal 170 podzielonych tematycznie pytań.

Na koniec 2025 roku biuletyn subskrybowało 3 358 osób. Biuletyn jest dostępny na stronie internetowej ww.uodo.gov.pl dzięki czemu dociera nie tylko do subskrybentów. Zainteresowanie poruszaną w nim tematyką jest widoczne nie tylko wśród ekspertów zajmujących się problematyką ochrony danych osobowych, ale także wśród mediów, dla których tematy omawiane w Biuletynie UODO stanowią często inspirację do przygotowania własnych materiałów. Świadczą o tym liczne cytowania w mediach i częste sytuacje powoływania się na prezentowane w nim stanowiska Urzędu czy dodatkowe pytania od dziennikarzy.

## 2.5. Kontakty z mediami

W okresie sprawozdawczym udzielono odpowiedzi na 271 pytań od dziennikarzy, w ramach których łącznie zadano 643 szczegółowe pytania. Prezes UODO oraz pracownicy UODO udzielili 47 wywiadów. Ponadto eksperci Departamentu Komunikacji Społecznej udzielali wsparcia pracownikom UODO w kontaktach z mediami, w tym w udzielaniu wypowiedzi i wywiadów.




**Wykres 23:** Zestawienie liczby pytań od dziennikarzy i udzielonych wywiadów w latach 2024-2025,

W 2025 r. dziennikarze często pytali o zagadnienia związane z prawną ochroną przed wykorzystaniem danych osobowych, a w szczególności przed deepfake'ami. Temat ten poruszany był bardzo często w związku z powiadomieniem organów ścigania przez Prezesa UODO, w sprawie przerobienia zdjęcia małoletniej uczennicy przy użyciu narzędzia sztucznej inteligencji i rozpowszechnianie go w mediach społecznościowych przez znajomych ze szkoły.

Dziennikarzy interesowały również zagadnienia związane z ochroną danych dzieci w serwisach społecznościowych, w szczególności w kontekście coraz częstszego zjawiska sharentingu.

W dalszym ciągu duże zainteresowanie wzbudzały tematy dotyczące stosowania monitoringu wizyjnego np. monitoringu miejskiego oraz w instytucjach publicznych (placówkach zdrowotnych i oświatowych), a także legalności używania kamer nasobnych.

Pojawiały się również pytania o legalność przetwarzania numerów PESEL (np. przy odbiorze odpadów w PSZOK) i ujawnianie tego numeru w różnych bazach, biuletynach informacji publicznej czy dokumentach, które nie zostały prawidłowo zanonimizowane. Media pytały także o ujawnianie danych osobowych bez podstawy prawnej w mediach społecznościowych (zdjęcia, zdęcia dokumentów, nr rejestracyjne pojazdów).

W okresie kampanii wyborczej na urząd Prezydenta Rzeczypospolitej Polski zainteresowanie dziennikarzy budziło ujawnianie danych osobowych przez komitety wyborcze i działania Prezesa UODO w tym zakresie. Chodzi tu m.in. o ujawnienie danych właściciela mieszkania, które przejął jeden z kandydatów na urząd prezydenta, legalność udostępnienia informacji o stanie zdrowia lub danych osób publicznych, dotyczących ich sfery życia prywatnego.

Media zgłaszały się również po komentarze dotyczące kar nałożonych przez Prezesa UODO, m.in. na Komendanta Głównego Policji, Centrum Medyczne Ujastek czy komitety wyborcze.

Dziennikarzy interesowały sprawy dotyczące naruszeń ochrony danych. Zazwyczaj pytania koncentrowały się na tym, czy dany podmiot zgłosił naruszenie i jaką poniesie odpowiedzialność np. za wyciek danych. W przypadku głośnych spraw pytali o szczegóły z nimi związane, w tym o działania podjęte przez UODO. Dziennikarzy interesowała też legalność praktyk dużych podmiotów gospodarczych i to czy określony sposób przetwarzania danych był analizowany przez UODO np. zbieranie danych biometrycznych.

Dziennikarze zagraniczni zainteresowani byli uzyskaniem informacji, czy Prezes UODO prowadzi postępowania wobec wskazanych podmiotów. Pytali też o status postępowań administracyjnych , czy też o stanowisko Prezesa UODO wobec krajowej ustawy wdrożeniowej dotyczącej rozporządzenia AI Act.

Rok 2025 upłynął nabardzo intensywnych kontaktach Prezesa UODO z mediami lokalnymi, głównie w związku z działaniami związanymi z promocją akcji „UODO rusza w kraj” oraz częstą obecnością przedstawicieli Urzędu na wydarzeniach organizowanych poza Warszawą.

### 2.6. Prosty język w skomplikowanych sprawach

W 2025 r. w Urzędzie Ochrony Danych Osobowych zakończył się cykl wewnętrznych szkoleń dotyczących tego, jak lepiej komunikować się z obywatelami także w pismach urzędowych. W czasie tych szkoleń, które miały formę warsztatów, zwracano uwagę na zasady dostępności cyfrowej. Wspólnie zastanawiano się też, jak przedstawiać trudną materię prawną w sposób jasny, klarowny i zrozumiały, aby odbiorca treści mógł sprawnie wykonać swoje obowiązki i korzystać ze swoich praw.

## 2.7. Infolinia UODO

Infolinia Urzędu Ochrony Danych Osobowych zapewnia powszechny i szybki dostęp do informacji dotyczących ochrony danych osobowych. Pełni funkcję informacyjno-doradczą oraz stanowi podstawowy kanał komunikacji z interesariuszami. Jest pierwszym punktem kontaktu oraz wstępnego poradnictwa prawnego, umożliwiając uzyskanie wsparcia bez konieczności osobistej wizyty w siedzibie Urzędu. UODO posiada jedną lokalizację w kraju i nie ma stałych punktów zamiejscowych, co dodatkowo podkreśla znaczenie infolinii w obsłudze obywateli z całej Polski, zwłaszcza osób wykluczonych cyfrowo lub wymagających szczególnego wsparcia.

Infolinia funkcjonuje codziennie w godzinach 10–14, zapewniając stałą dostępność i sprawną reakcję na zgłaszane potrzeby. Z pytaniami zwracają się zarówno osoby fizyczne, jak i podmioty prawne. Konsultanci dokonują wstępnej analizy przedstawianych zagadnień, zadają pytania doprecyzowujące oraz wskazują możliwe rozwiązania dotyczące stosowania przepisów RODO. Charakter świadczonych usług ma wymiar specjalistyczny, ponieważ poruszane kwestie często obejmują różne obszary prawa. Bezpłatność infolinii ma istotne znaczenie dla osób, które nie mogą skorzystać z komercyjnych usług prawnych. Dla wielu dzwoniących kontakt telefoniczny stanowi pierwszy krok do skutecznego rozwiązania problemu, pozwalając uniknąć zbędnych kosztów, czasu oraz dodatkowych obciążeń emocjonalnych.

Pracownicy infolinii posiadają wiedzę z zakresu ochrony danych osobowych, którą systematycznie uzupełniają uczestnicząc w specjalistycznych szkoleniach oraz monitorując aktualny stan prawny, w tym orzecznictwo krajowe i europejskie, oraz wydane przez Prezesa UODO decyzje administracyjne. W zakresie udzielanych konsultacji prawnych współpracują z innymi departamentami UODO, korzystając z ich merytorycznego wsparcia. Przekazują informacje o procedurze składania skarg i wniosków, prawidłowym wypełnianiu i przesyłaniu formularzy zgłoszeń naruszeń oraz zgłoszeń powołania, odwołania i innych zmian w odniesieniu do inspektora ochrony danych, a także wskazują osobom poszukującym informacji przydatne opracowania na stronie internetowej. Informują także o wydarzeniach edukacyjnych z dziedziny ochrony danych osobowych, w tym o szkoleniach i konferencjach organizowanych lub współorganizowanych przez UODO oraz o wydarzeniach organizowanych przez podmioty zewnętrzne z udziałem ekspertów Urzędu.

Infolinia z jednej strony służy pomocą w upowszechnianiu wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO, z drugiej zaś - upowszechnia wśród osób, których dane dotyczą, wiedzę o przysługujących im prawach. Dzięki infolinii kierownictwo Urzędu może na bieżąco identyfikować najczęściej pojawiające się problemy i adekwatnie reagować na potrzeby obywateli.

Tematyka rozmów przeprowadzonych z ekspertami infolinii była bardzo różnorodna. Najczęściej zadawane pytania dotyczyły (oprócz pytań o stan sprawy toczącej się w Urzędzie) następujących zagadnień:

• monitoring wizyjny,
• prawidłowe postępowanie w przypadku naruszeń,
• procedura zgłoszenia IOD,
• przetwarzanie danych osobowych przez pracodawców,
• przetwarzanie danych osobowych przez spółdzielnie i wspólnoty mieszkaniowe,
• niechciany telemarketing,
• kopiowanie (skanowanie) dokumentów tożsamości przez banki.

Pracownicy infolinii dzielili się dodatkowo swoją wiedzą i doświadczeniem z zakresu ochrony danych osobowych w ramach różnych inicjatyw UODO, w tym programu edukacyjnego UODO „Twoje dane Twoja sprawa" oraz akcji „UODO rusza w kraj". Pracownik infolinii prowadził również obsługę pilotażowego terenowego punktu informacyjno – konsultacyjnego UODO, uruchomionego 15 grudnia 2025 r. w Rzeszowie.

W 2025 roku pracownicy infolinii przeprowadzili **14476 rozmów**. Podkreślenia wymaga, że na jedno połączenie często składało się kilka pytań dotyczących różnych i nierzadko skomplikowanych prawnie zagadnień. Było to widoczne szczególnie wtedy, gdy do ekspertów infolinii z prośbą o wskazówki zwracali się inspektorzy ochrony danych.

Obecnie prowadzone są prace nad wdrożeniem rozwiązań opartych na sztucznej inteligencji, których celem jest dalsza optymalizacja jakości obsługi infolinii.

# 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 (EROD), 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, Europejskiego Inspektora Ochrony Danych (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. Dokumenty te są tworzone w celu promowania wspólnego rozumienia RODO

i dyrektywy 2016/680. W ramach prac w EROD pracownicy UODO biorą również udział w doradzaniu Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych w Unii Europejskiej (UE). Opracowane stanowiska oraz projekty dokumentów są następnie przedmiotem dyskusji i zostają przyjęte na comiesięcznych posiedzeniach plenarnych EROD. Porządki obrad i komunikaty z sesji plenarnych są publikowane na stronie internetowej UODO.

W 2025 roku, w ramach prac podgrup i grup zadaniowych EROD, przedstawiciele polskiego organu nadzorczego wraz z reprezentantami pozostałych organów, opracowali szereg dokumentów w celu promowania wspólnego rozumienia RODO.

**Wytyczne i zalecenia:**

1. Wytyczne 01/2025 w sprawie pseudonimizacji;
2. Wytyczne 02/2025 dotyczące przetwarzania danych osobowych za pomocą technologii blockchain;
3. Wytyczne 03/2025 dotyczące wzajemnych zależności między aktem o usługach cyfrowych (DSA) a ogólnym rozporządzeniem o ochronie danych osobowych;
4. Wspólne wytyczne dotyczące wzajemnych powiązań między aktem o rynkach cyfrowych a ogólnym rozporządzeniem o ochronie danych (RODO);
5. Wytyczne 02/2024 dotyczące art. 48 RODO – w 2025 roku została przyjęta finalna wersja tych wytycznych, po konsultacjach publicznych;
6. Zalecenia 1/2025 dotyczące Światowego kodeksu antydopingowego WADA na 2027 rok;
7. Zalecenia 2/2025 dotyczące podstaw prawnych do tworzenia kont użytkowników na stronach e-commerce.

**Opinie i oświadczenia:**

1. Opinia 01/2025 w sprawie projektu decyzji francuskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych Grupy Coface;
2. Wspólna opinia EROD-EIOD nr 01/2025 w sprawie wniosku dotyczącego rozporządzenia w sprawie środków upraszczających procedury dla MŚP i średnich przedsiębiorstw, w szczególności w odniesieniu do obowiązku prowadzenia dokumentacji zgodnie z art. 30 ust. 5 RODO;
3. Opinia 2/2025 w sprawie projektu decyzji szwedzkiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych administratora danych w ramach grupy Alfa Laval;
4. Opinia 3/2025 w sprawie projektu decyzji francuskiego organu nadzorczego dotyczącej kryteriów certyfikacji Lexing;
5. Opinia 4/2025 w sprawie projektu decyzji fińskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych grupy Nokia;
6. Opinia 5/2025 w sprawie projektu decyzji fińskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych podmiotu przetwarzającego danych w ramach Grupy Nokia;
7. Opinia 06/2025 w sprawie przedłużenia obowiązywania decyzji wykonawczych Komisji Europejskiej wydanych na mocy RODO i dyrektywy LED dotyczących

odpowiedniego poziomu ochrony danych osobowych w Zjednoczonym Królestwie (art. 70);

8. Opinia 07/2025 w sprawie projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 w sprawie odpowiedniej ochrony danych osobowych przez Europejską Organizację Patentową (art. 70);
9. Opinia 8/2025 w sprawie projektu decyzji norweskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych grupy Statkraft;
10. Opinia 9/2025 w sprawie projektu decyzji francuskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych podmiotu przetwarzającego danych w ramach Grupy Worldline;
11. Opinia 10/2025 w sprawie projektu decyzji francuskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych administratora danych w ramach grupy Worldline;
12. Opinia 11/2025 w sprawie projektu decyzji holenderskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych grupy Signify;
13. Opinia 12/2025 w sprawie projektu decyzji holenderskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych administratora danych w grupie ASML;
14. Opinia 13/2025 w sprawie projektu decyzji holenderskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych administratora danych w ramach grupy Aramex;
15. Opinia 14/2025 w sprawie projektu decyzji norweskiego organu nadzorczego dotyczącej wiążących reguł korporacyjnych administratora danych w ramach grupy Wilh. Wilhelmsen;
16. Opinia 15/2025 w sprawie projektu decyzji austriackiego organu nadzorczego dotyczącej kryteriów certyfikacji BDO Consulting GmbH;
17. Opinia 16/2025 w sprawie projektu decyzji organu nadzorczego dla Nadrenii Północnej-Westfalii dotyczącej kryteriów certyfikacji TÜV IT;
18. Opinia 26/2025 w sprawie projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 w sprawie odpowiedniego poziomu ochrony danych osobowych w Zjednoczonym Królestwie;
19. Opinia 27/2025 w sprawie projektu decyzji wykonawczej Komisji Europejskiej na podstawie dyrektywy (UE) 2016/680 w sprawie odpowiedniej ochrony danych osobowych przez Zjednoczone Królestwo – przyjęta w dniu 16 października 2025 roku;
20. Opinia 28/2025 w sprawie projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 w sprawie odpowiedniego poziomu ochrony danych osobowych w Brazylii – przyjęta 4 listopada 2025 roku;
21. Oświadczenie 1/2025 w sprawie zapewnienia wieku;
22. Oświadczenie 2/2025 dotyczące wdrażania dyrektywy w sprawie wykorzystywana danych dotyczących przelotu pasażera (danych PNR) w świetle wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w sprawie C-817/19;

23. Oświadczenie 4/2025 w sprawie Zaleceń Komisji Europejskiej dot. projektu niewiążących modelowych warunków umownych dotyczących udostępniania danych na mocy aktu w sprawie danych.

**Inne dokumenty:**

1. Stanowisko w sprawie wzajemnego oddziaływania przepisów dotyczących ochrony danych i prawa konkurencji – przyjęte 16 stycznia 2025 roku;
2. Sprawozdanie dotyczące korzystania z usług zewnętrznych ekspertów SPE w 2024 roku – przyjęte 13 marca 2025 roku.

## 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 (Coordinated Enforcement Framework – 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 2025 r., EROD wybrała temat „prawo do usunięcia danych”. Co roku organy nadzorcze wchodzące w skład EROD w ramach CEF przeprowadzają badanie poświęcone wybranemu wcześniej tematowi. W 2025 r. 32 organy ochrony danych w całym Europejskim Obszarze Gospodarczym (w tym EIOD) wszczęły skoordynowane postępowania oceniając, czy formalne postępowanie wyjaśniające było uzasadnione, lub przeprowadzając działania mające na celu ustalenie faktów. Na akcję odpowiedziało 764 administratorów. Sprawozdanie EROD z CEF z 2025 roku wskazuje, że administratorzy danych napotykają liczne trudności w prawidłowej realizacji prawa do usunięcia danych osobowych. Najczęściej problemy wynikają z braku odpowiednich procedur wewnętrznych do obsługi wniosków oraz z niewystarczającego informowania osób o sposobie realizacji ich praw. Zwrócono również uwagę na stosowanie przez niektórych administratorów nieskutecznych metod anonimizacji, zamiast faktycznego usuwania danych. Istotnym wyzwaniem okazało się także określanie właściwych okresów przechowywania danych oraz zapewnienie ich skutecznego usuwania, szczególnie w środowiskach obejmujących kopie zapasowe, gdzie proces ten jest bardziej skomplikowany.

Dodatkowe trudności wynikają z faktu, że prawo do usunięcia danych nie ma charakteru bezwzględnego. Administratorzy muszą każdorazowo oceniać, czy istnieją podstawy do realizacji wniosku, a także analizować, czy usunięcie danych nie naruszy innych praw, obowiązków prawnych lub uzasadnionych interesów. W praktyce

wymaga to przeprowadzania złożonych analiz i wyważania różnych praw oraz wolności. W odpowiedzi na zidentyfikowane problemy opracowano liczne wytyczne, dokumenty i wzory procedur, które mają wspierać administratorów w zapewnianiu zgodności z RODO oraz ułatwiać osobom fizycznym korzystanie z przysługującego im prawa do usunięcia danych. Działania te mają również przyczynić się do bardziej jednolitego stosowania i egzekwowania przepisów o ochronie danych osobowych w całym Europejskim Obszarze Gospodarczym. UODO również zamieścił na swojej stronie internetowej komunikat na ten temat.

**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 2025 r. EROD przedstawiła dwa nowe projekty SPE – „Law & Compliance in AI Security & Data Protection" oraz „Fundamentals of Secure AI Systems with Personal Data", których celem jest podnoszenie kompetencji prawnych i technicznych w zakresie zgodnego z RODO projektowania, wdrażania i nadzorowania systemów sztucznej inteligencji.

**3) Wymiana informacji w ramach mechanizmu wzajemnej pomocy (art. 61 RODO)**

Zgodnie z art. 61 RODO organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania rozporządzenia oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. W ramach tego mechanizmu, zapytania od innych organów nadzorczych kierowane są do polskiego organu nadzorczego za pośrednictwem Systemu IMI (Internal Market Information System), tj. Systemu Wymiany Informacji na Rynku Wewnętrznym. Tą samą drogą przekazywane są odpowiedzi na przedłożone zapytania.

W 2025 roku organy nadzorcze zwracały się do Prezesa UODO z różnymi zagadnieniami. Pytania dotyczyły m.in. opinii polskiego organu nadzorczego w takich sprawach, jak:

- nakładanie kar administracyjnych przez organ ochrony danych osobowych na organy publiczne;
- Consent Management Platforms (CMP);
- możliwości zniesienia zakazu przetwarzania danych biometrycznych w środowisku pracy, w sytuacji gdy upoważnienie do zniesienia zakazu znajduje się w układzie zbiorowym pracy;
- działań prowadzonych przez Prezesa UODO dla administratorów danych osobowych w celu wsparcia w osiągnięciu zgodności z system ochrony danych osobowych;

- przetwarzania danych, takich jak materiał biologiczny (próbka genetyczna) przez biobanki.

UODO udzielił odpowiedzi na te oraz inne pytania spływające w ramach systemu IMI. Przygotowanie szczegółowych odpowiedzi przez UODO umacnia współpracę z krajowymi organami nadzorczymi Europejskiego Obszaru Gospodarczego (EOG). Dzięki informacjom pozyskanym od innych organów nadzorczych wzrasta zrozumienie, jak RODO jest interpretowane w państwach członkowskich. Ponadto otrzymywane pytania pozwalają zapoznać się z bieżącymi zagadnieniami, będącymi przedmiotem dyskusji innych organów nadzorczych. Pozwala to również na wypracowanie zharmonizowanych, wspólnych stanowisk przy uwzględnieniu ustawodawstwa krajowego.

Informacje na temat ilości notyfikacji IMI, otrzymanych skarg oraz rozpatrzonych spraw w ramach systemu IMI, znajdują się w sekcji 10. „Działania dotyczące postępowań transgranicznych".

**4) Przekazywanie danych osobowych poza EOG**

W 2025 r. polski organ nadzorczy otrzymał informacje i zapytania od organów nadzorczych z EOG, odnoszące się do spraw dotyczących zatwierdzania wiążących reguł korporacyjnych w ponad 50 różnych grupach kapitałowych rozpoznawanych przez inne organy nadzorcze z EOG jako organy wiodące.

Wspomniane wyżej informacje i zapytania od organów nadzorczych z EOG dotyczyły w szczególności zgłoszenia ewentualnych zastrzeżeń odnośnie do ustanowienia organu wiodącego w ramach danej procedury zatwierdzania wiążących reguł korporacyjnych (WRK), analizy dokumentacji dotyczących projektów WRK na różnych etapach ich rozpatrywania, tj. na etapie wspólnej oceny, na etapie współpracy (w odniesieniu do skonsolidowanych projektów konkretnych WRK, będących rezultatem współpracy organu wiodącego i współrecenzentów) oraz na etapie przyjmowania opinii przez EROD, w tym jako członek zespołów projektowych przygotowujących projekty opinii EROD dot. projektów decyzji organów nadzorczych z EOG w sprawie zatwierdzenia projektów WRK. Polski organ nadzorczy otrzymywał również informacje dotyczące zaktualizowanych wersji zatwierdzonych już wcześniej WRK.

W 2025 r. kontynuowano rozpatrywanie wniosków o zatwierdzenie WRK dla administratorów oraz dla podmiotów przetwarzających, które wpłynęły do Prezesa UODO w 2023 r.

W 2025 r. Prezes UODO wydał dwie decyzje dot. zatwierdzenia aktualizacji WRK dla administratora i podmiotu przetwarzającego.

**5) Inne sprawy**

W 2025 r. Prezes UODO zajmował się również sprawami – zarówno o zasięgu krajowym, jak i międzynarodowym – dotyczącymi innych kwestii niż te wskazane powyżej.

## 3. Udział Prezesa UODO w pracach nad pakietami Omnibus

Pakiety Omnibus Komisji Europejskiej to zestawy propozycji legislacyjnych, które jednym aktem zmieniają wiele obowiązujących przepisów jednocześnie. W 2025 roku Prezes UODO brał udział w pracach nad pakietem Omnibus IV oraz Omnibus VII (Digital oraz AI).

### 1) Omnibus IV

W 2025 roku Prezes UODO aktywnie uczestniczył w pracach związanych z wnioskiem Komisji Europejskiej w sprawie uproszczenia obowiązku prowadzenia dokumentacji zgodnie z rozporządzeniem (UE) 2016/679 (RODO). 21 maja 2025 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenia (UE) 2016/679 („RODO"), (UE) 2016/1036, (UE) 2016/1037, (UE) 2017/1129, (UE) 2023/1542 oraz (UE) 2024/573 w odniesieniu do rozszerzenia niektórych środków łagodzących dostępnych dla małych i średnich przedsiębiorstw („MŚP") na małe przedsiębiorstwa o średniej kapitalizacji („SMC") oraz dalszych środków upraszczających. W tym samym dniu Komisja formalnie skonsultowała się z EROD i EIOD zgodnie z art. 42 ust. 2 rozporządzenia (UE) 2018/17252.

W maju 2025 roku rozpoczęły się wspólne prace EROD i EIOD nad opinią na temat propozycji Komisji Europejskiej. UODO uczestniczył w tych pracach jako członek EROD. Po przeprowadzeniu wewnętrznych konsultacji, UODO przekazał uwagi do wniosku Komisji Europejskiej, które następnie znalazły swoje odzwierciedlenie w liście[668] EROD i EIOD do Komisji Europejskiej oraz we wspólnej opinii EROD i EIOD[669], przyjętej w lipcu 2025 roku.

W opinii poparto ogólny cel wniosku, jakim jest zmniejszenie obciążeń administracyjnych dla MŚP i SMC, o ile dążenie do tego celu nie spowoduje osłabienia ochrony praw podstawowych osób fizycznych, w szczególności podstawowego prawa do ochrony danych osobowych. Proponowane zmiany w RODO, mające na celu uproszczenie i wyjaśnienie obowiązku prowadzenia rejestru przetwarzania, mają charakter ukierunkowany i ograniczony oraz nie wpływają na podstawowe zasady i inne obowiązki wynikające z RODO. Jednocześnie przypomniano o znaczeniu podstawowego prawa do ochrony danych osobowych oraz o konieczności zapewnienia, by w świetle art. 52 Karty Praw Podstawowych Unii Europejskiej uproszczenie było proporcjonalne, wyważone i oparte na konieczności. W tym kontekście zwrócono uwagę, że wniosek nie zawiera oceny skutków proponowanych zmian w RODO dla praw podstawowych, którą należało przeprowadzić.

---

[668] List EROD i EIOD w sprawie projektu wniosku Komisji Europejskiej dotyczącego uproszczenia prowadzenia dokumentacji zgodnie z RODO, https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-letter-european-commission-draft-proposal_en.

[669] Wspólna opinia EROD i EIOD nr 01/2025 w sprawie wniosku dotyczącego rozporządzenia w sprawie środków upraszczających procedury dla MŚP i małych przedsiębiorstw o średniej kapitalizacji, w szczególności w odniesieniu do obowiązku prowadzenia dokumentacji zgodnie z art. 30 ust. 5 RODO, https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-012025-proposal_en.

W opinii poparto działania mające na celu wyjaśnienie i uproszczenie warunków, w których miałoby zastosowanie odstępstwo przewidziane w art. 30 ust. 5 RODO, poprzez określenie, że odstępstwo to nie miałoby zastosowania do przetwarzania, które „może powodować wysokie ryzyko". Aby uniknąć nieporozumień, zaproponowano Komisji Europejskiej, aby w motywach wyjaśniła ona, że rejestr przetwarzania będzie obowiązkowy wyłącznie w odniesieniu do tych czynności przetwarzania, które „mogą powodować wysokie ryzyko".

W opinii podkreślono, że przetwarzanie danych osobowych objętych art. 9 i 10 RODO ma istotne znaczenie dla oceny, czy przetwarzanie to może wiązać się z wysokim ryzykiem. W związku z tym zasugerowano, aby Komisja Europejska zmieniła brzmienie motywu 10 w celu wyjaśnienia, że przetwarzanie do celów przewidzianych w art. 9 ust. 2 lit. b) RODO nie wymagałoby prowadzenia rejestru czynności przetwarzania, chyba że ocena wskazuje, że przetwarzanie to może wiązać się z wysokim ryzykiem.

W odniesieniu do obowiązku prowadzenia dokumentacji wynikającego z art. 30 RODO, podkreślono, że oprócz ułatwiania wykazania zgodności z przepisami po fakcie, dokumentacja dotycząca czynności przetwarzania stanowi bardzo przydatny środek wspierający przestrzeganie wielu wymogów RODO. Zachęcono zatem przedsiębiorstwa i organizacje zatrudniające mniej niż 750 osób, które nie prowadzą przetwarzania danych wysokiego ryzyka, do wyboru najbardziej odpowiednich metod, które w odpowiedni sposób wspierają zgodność z obowiązkami wynikającymi z RODO i nie mają negatywnego wpływu na prawa osób, których dane dotyczą.

Podkreślono także, że przyjęte zostaną dalsze wyjaśnienia dotyczące tego, dlaczego nowy próg dotyczący przedsiębiorstw lub organizacji zatrudniających mniej niż 750 osób byłby odpowiedni w przypadku RODO. Zalecono także wyjaśnienie w motywie, że termin „organizacja" objęty proponowanym odstępstwem na mocy art. 30 ust. 5 RODO nie obejmuje organów i podmiotów publicznych.

UODO aktywnie współpracował w sprawie propozycji zmian w ramach Omnibus IV również z Ministerstwem Cyfryzacji, przygotowując uwagi do propozycji dotyczących ochrony danych osobowych na potrzeby opracowania stanowiska rządu Rzeczypospolitej Polskiej.

### 2) Omnibus VII

Jak wspomniano na wstępie, w 2025 roku Prezes UODO aktywnie uczestniczył również w pracach związanych z wnioskiem Komisji Europejskiej dotyczącym zmiany RODO - tzw. „Digital Omnibus" w ramach pakietu Omnibus VII. 19 listopada 2025 r. Komisja Europejska przedstawiła wniosek dotyczący pakietu „Digital Omnibus"[670], zmieniający szeroki zakres unijnego prawodawstwa cyfrowego, w tym RODO;

[670] Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie zmiany rozporządzeń (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektyw 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram prawnych oraz uchylenia rozporządzeń (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 i dyrektywy (UE) 2019/1024 (akt zbiorczy prawa cyfrowego), zob. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=comnat:COM_2025_0837_FIN.

rozporządzenie w sprawie jednolitego portalu cyfrowego; rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii; akt w sprawie danych; dyrektywę o prywatności i łączności elektronicznej; dyrektywę w sprawie cyberbezpieczeństwa; dyrektywę NIS 2 oraz akt o zarządzaniu danymi. Jak wspomniano, pakiet ten obejmował również zmiany do Aktu o sztucznej inteligencji, co skutkowało przygotowaniem odrębnej opinii EROD i EIOD dotyczącej zagadnień związanych z AI. W listopadzie 2025 roku, rozpoczęły się wspólne prace EROD i EIOD nad opinią na temat wniosku Komisji Europejskiej. UODO uczestniczył w tych pracach jako członek EROD poprzez aktywny udział w podgrupach ekspertów EROD. Po przeprowadzeniu wewnętrznych konsultacji, UODO przekazywał uwagi do wniosku Komisji Europejskiej, które następnie znalazły swoje odzwierciedlenie we wspólnej opinii EROD i EIOD[671], przyjętej na początku 2026 roku. Jest to opinia dotycząca pakietu Omnibus VII w zakresie części „Digital".

We wspólnej opinii poparto cel wniosku, jakim jest uproszczenie przestrzegania przepisów dotyczących cyfryzacji, wzmocnienie skutecznego wykonywania praw osób fizycznych oraz zwiększenie konkurencyjności UE. Podkreślono również znaczenie tego, by proponowane uproszczenia doprecyzowały obowiązki i zapewniły pewność prawną, przy jednoczesnym utrzymaniu zaufania oraz wysokiego poziomu ochrony praw i wolności osób fizycznych.

W związku z tym przyjęto proponowane zmiany w następujących kwestiach:

- badania naukowe, w szczególności wprowadzenie definicji; wyjaśnienie, że art. 6 ust. 4 RODO nie musi mieć zastosowania; a także nowe (ograniczone) odstępstwo od obowiązku informowania;
- nowy wyjątek dotyczący przetwarzania szczególnych kategorii danych na potrzeby uwierzytelniania biometrycznego, w przypadku gdy środki weryfikacji pozostają pod wyłączną kontrolą danej osoby;
- zawiadomienia o naruszeniu ochrony danych i oceny skutków dla ochrony danych („DPIA"), w szczególności podwyższenie progu powiadomienia i wydłużenie terminu, a także ustanowienie wspólnych szablonów i wykazów dotyczących zawiadomień o naruszeniu ochrony danych i DPIA. Jednakże EROD powinna być w pełni upoważniona zarówno do przygotowywania, jak i zatwierdzania takich dokumentów, a EIOD powinien otrzymać odpowiednie kompetencje na mocy rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii.

Jednocześnie uważa się, że poniższe proponowane zmiany budzą poważne obawy, ponieważ będą miały negatywny wpływ na poziom ochrony

[671] Wspólna opinia EROD-EIOD nr 2/2026 w sprawie wniosku dotyczącego rozporządzenia w sprawie uproszczenia ram prawnych dotyczących technologii cyfrowych (pakiet „Digital Omnibus"), https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en.

przysługujący osobom fizycznym, spowodują niepewność prawną i/lub utrudnią stosowanie prawa w praktyce:

- proponowane zmiany w definicji danych osobowych zawęziłyby pojęcie danych osobowych i miałyby negatywny wpływ na podstawowe prawo do ochrony danych. Proponowane zmiany wykraczają daleko poza ukierunkowaną modyfikację RODO, „poprawkę techniczną" lub zwykłą kodyfikację orzecznictwa TSUE. Z tych powodów stanowczo wzywa się Komisję Europejską, aby nie przyjmowała proponowanych zmian w definicji danych osobowych;
- określenie, co nie jest już danymi osobowymi po pseudonimizacji, ma również bezpośredni wpływ na zakres stosowania unijnego prawa o ochronie danych i nie powinno być przedmiotem aktu wykonawczego.

Warunkowo poparto również główny cel wniosku dotyczący proponowanych zmian w następujących kwestiach, choć zaznaczono, że konieczne są pewne ulepszenia:

- powoływanie się na prawnie uzasadniony interes w kontekście sztucznej inteligencji: ponieważ EROD wyraźnie potwierdziła to już w swojej opinii nr 28/2024 w sprawie modeli sztucznej inteligencji, nie wydaje się konieczne wprowadzanie konkretnego przepisu w tej sprawie. Wspólna opinia zawiera jednak konkretne sugestie, w tym dotyczące oceny prawnie uzasadnionego interesu oraz prawa do wniesienia sprzeciwu, na wypadek gdyby Komisja Europejska zechciała wprowadzić tę zmianę;
- wyjątek dotyczący przypadkowego i resztkowego przetwarzania szczególnych kategorii danych w kontekście sztucznej inteligencji: EROD i EIOD uznają, że w przypadku gromadzenia danych na potrzeby szkolenia, testowania i walidacji niektórych systemów lub modeli sztucznej inteligencji nie zawsze można uniknąć resztkowego i przypadkowego przetwarzania szczególnych kategorii danych. We wspólnej opinii zaleca się kilka ulepszeń, takich jak odniesienie do „przypadkowego i resztkowego" przetwarzania w treści normatywnej, wyjaśnienie zakresu odstępstwa oraz zapewnienie zabezpieczeń w całym cyklu życia danych;
- ograniczenie prawa dostępu: wyjaśnienie, co stanowi nadużycie prawa, jest pożądane, jednak nie powinno się go wiązać z wykonywaniem prawa dostępu w celach innych niż ochrona danych, ponieważ RODO ma również na celu ochronę innych podstawowych praw i wolności. We wspólnej opinii zawarto konkretne sugestie, takie jak powiązanie „nadużycia prawa" z istnieniem zamiaru nadużycia. Ponadto EROD i EIOD podkreślają, że art. 12 ust. 5 RODO znajduje obecnie odzwierciedlenie w art. 57 ust. 4 RODO i że należy to utrzymać. W związku z tym organy nadzorcze powinny nadal mieć możliwość odmowy podjęcia działań w sprawie skargi lub nałożenia rozsądnej opłaty na takich samych warunkach, na jakich administrator danych mógłby odmówić uwzględnienia wniosku o dostęp, pod warunkiem że uwzględnione zostaną uwagi dotyczące art. 12 ust. 5 RODO;

- nowe odstępstwo dotyczące przejrzystości: uproszczenie wymogów informacyjnych i zmniejszenie obciążeń administracyjnych, zwłaszcza dla MŚP, jest mile widziane, jednak we wspólnej opinii sugeruje się wprowadzenie wyjaśnień w celu zapewnienia pewności prawnej, skutecznego zmniejszenia obciążeń oraz zagwarantowania, że osoby fizyczne nadal będą mogły otrzymywać informacje dotyczące swoich danych;
- zautomatyzowane podejmowanie decyzji w sprawach indywidualnych: należy utrzymać zasadniczy zakaz, zgodnie z wyjaśnieniami TSUE. We wspólnej opinii zawarto konkretną propozycję utrzymania tej zasady z pewnymi wyjątkami. EROD i EIOD z przyjmują cel, jakim jest wyjaśnienie wyjątków od obecnego zakazu, ale sugerują zmiany, aby uniknąć sugerowania, że zautomatyzowane podejmowanie decyzji jest co do zasady dozwolone zawsze, gdy istnieje umowa, niezależnie od tego, czy jest to „konieczne". Przedstawiają również sugestie dotyczące dalszego wyjaśnienia, na czym polega ocena „konieczności".

Zmiany dotyczące dyrektywy o prywatności i łączności elektronicznej (ePrivacy).

Zdecydowanie poparto cel wniosku, jakim jest zapewnienie rozwiązania regulacyjnego mającego na celu przeciwdziałanie „zmęczeniu zgody" i nadmiernemu mnożeniu się banerów dotyczących plików cookie oraz uproszczenie przepisów mających zastosowanie do ochrony urządzeń końcowych użytkowników końcowych. Zaakceptowano fakt, że wniosek ma na celu zapewnienie ograniczonych dodatkowych odstępstw od ogólnego zakazu przechowywania danych osobowych w urządzeniach końcowych lub uzyskiwania do nich dostępu (z zastrzeżeniem konkretnych zaleceń) oraz to, że nadzór nad tymi kwestiami zostanie powierzony organom nadzorczym ustanowionym zgodnie z RODO w celu dalszego wspierania spójności regulacyjnej. Wyrażono jednak obawy, że proponowane rozdzielenie przepisów dotyczących dostępu do informacji w urządzeniach końcowych i ich przechowywania w różnych instrumentach prawnych może prowadzić do niepewności prawnej. We wspólnej opinii przedstawiono również dodatkowe zalecenia mające na celu zwiększenie pewności prawnej, zminimalizowanie ryzyka oraz wspieranie odpowiedzialnych innowacji, w tym poprzez dodanie wyjątku dotyczącego reklamy kontekstowej. We wspólnej opinii podkreślono, że powierzenie organom ochrony danych nadzoru nad tymi nowymi przepisami nie może zostać zrealizowane bez zapewnienia skutecznych uprawnień naprawczych.

Prezes UODO uczestniczył również w przygotowaniu odrębnej wspólnej opinii EROD i EIOD dotyczącej zmian wprowadzanych przez pakiet Omnibus VII w odniesieniu do Aktu o sztucznej inteligencji[672]. Opinia obejmowała szeroki zakres zagadnień, w tym: ocenę wpływu proponowanych zmian na system nadzoru nad AI, analizę przetwarzania danych szczególnych kategorii na potrzeby wykrywania

[672] Wspólna opinia EROD-EIOD nr 1/2026 w sprawie wniosku dotyczącego rozporządzenia w zakresie uproszczenia wdrażania zharmonizowanych przepisów dotyczących sztucznej inteligencji (pakiet „Digital Omnibus w obszarze AI"), zob. link: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12026-proposal_en.

i korygowania biasu, ocenę zasad rejestracji systemów AI, rolę organów ochrony danych w unijnych piaskownicach regulacyjnych, a także współpracę AI Office z organami nadzorczymi. W opinii podkreślono również znaczenie właściwego uregulowania roli FRABs i MSAs, zapewnienia spójności nadzoru, a także potrzebę wzmocnienia wymogów dotyczących przejrzystości, dokumentacji technicznej oraz zarządzania ryzykiem. Uwzględniono ponadto kwestie związane z AI literacy oraz harmonogramem wdrażania przepisów dotyczących systemów wysokiego ryzyka. Prace wymagały pogłębionej oceny wpływu proponowanych rozwiązań na ochronę danych osobowych.

Prezes UODO aktywnie współpracował w sprawie pakietu zmian Omnibus VII również z Ministerstwem Cyfryzacji, przygotowując uwagi do propozycji dotyczących ochrony danych osobowych na potrzeby opracowania stanowiska rządu Rzeczypospolitej Polskiej.

## 4. Platformy z Chin

W 2025 r. Prezes UODO przeprowadził wewnętrzną analizę polityk prywatności największych chińskich platform sprzedażowych, koncentrując się na ich zgodności z wymogami RODO, w szczególności w zakresie przejrzystości przetwarzania danych oraz podstaw prawnych. Stwierdzono, że większość analizowanych podmiotów spełnia podstawowe obowiązki informacyjne, jednak w niektórych przypadkach zauważono zbyt ogólne zapisy dotyczące m.in. transferów danych. Ocena wykazała także różnice w podejściu do realizacji praw osób, których dane dotyczą, zwłaszcza w zakresie prawa do usunięcia danych. Analiza obejmowała również działania prowadzone przez inne podmioty, w tym inne organy nadzorcze.

## 5. Certyfikacja

Prezes UODO był zaangażowany również w rozwój mechanizmów certyfikacji na poziomie krajowym i europejskim. W 2025 roku rozpoczęły się szczegółowe dyskusje z podmiotem zainteresowanym opracowaniem kryteriów certyfikacji, w tym jego roli w procesie certyfikacji.

Na poziomie europejskim w ramach prac Podgrupy ds. Zgodności, e-Administracji i Zdrowia EROD, Prezes UODO uczestniczył poprzez śledzenie dyskusji i przekazywanie uwag w pracach nad zatwierdzeniem 4 mechanizmów certyfikacji, dla których EROD wydała w 2025 roku opinię. Dodatkowo w przypadku jednego z nich - greckiego mechanizmu certyfikacji Centrum Europejskiego Prawa Konstytucyjnego Fundacji Tsatsos (C.E.C.L), Prezes UODO po raz pierwszy sprawował rolę recenzenta kryteriów certyfikacji i uczestniczył jako sprawozdawca w pracach nad opinią w sprawie zatwierdzenia kryteriów (wcześniej organ nadzorczy uczestniczył w pracach nad dokumentem dotyczącym dodatkowych wymogów akredytacji, ale nie zatwierdzenia kryteriów certyfikacji).

W działaniach certyfikacyjnych w ramach EROD istotne były również prace nad mechanizmem Europrivacy, służącym jako narzędzie do przekazywania danych do krajów trzecich. Te prace wymagały koordynacji między podgrupami ds. Zgodności,

eAdministracji i Zdrowia i ds. Użytkowników IT. Nowe kryteria będą pierwszym tego typu mechanizmem.

Ponadto Prezes UODO zaangażował się w prace nad promocją certyfikacji oraz rozpowszechnianiem wiedzy na ten temat. Na poziomie krajowym objawiało się to poprzez tłumaczenie już istniejącego dorobku edukacyjnego UODO (webinaria) na język angielski. Na poziom EROD, UODO został zaangażowany w roli sprawozdawcy we wspólne prace organów nadzorczych dotyczące promocji certyfikacji. Prace zostały zainicjowane na warsztatach certyfikacyjnych, które odbyły się w czerwcu 2025 roku w Berlinie. Przedstawiciele UODO aktywnie uczestniczyli w warsztatach dzieląc się perspektywą UODO na kwestie certyfikacji.

W grudniu 2025 r. odbyło się pierwsze spotkanie zespołu sprawozdawców. W ramach działań zespołu sprawozdawców, zgormadzona przez EROD wiedza dotycząca mechanizmów i systemów certyfikacji ma zostać upubliczniona w przystępnej formie, w sposób, który wyjaśniałby ewentualne wątpliwości podmiotów zainteresowanych certyfikacją RODO. Ponadto celem prac zespołu jest ułatwienie merytorycznego wsparcia dla podmiotów, które już zaangażowały się w mechanizmy certyfikacji RODO.

## 6. Inne działania w zakresie uregulowań dotyczących danych

W grudniu 2025 r. Prezes UODO został poproszony przez Ministerstwo Cyfryzacji o uwagi do stanowiska Rządu RP w sprawie Europejskiej Strategii w Zakresie Danych. Po konsultacjach wewnętrznych, uwagi zostały przekazane. Dotyczyły one między innymi konieczności pełnego zachowania kompetencji organów nadzorczych w zakresie dotyczącym danych osobowych, jasnego określania ram współpracy między UODO a innym organami regulacyjnymi oraz technik anonimizacji i pseudonimizacji.

Ponadto Prezes UODO zaangażował się w prace nad wytycznymi EROD dotyczącymi punktów stycznych między Aktem w sprawie danych a RODO, przekazując uwagi zespołowi sprawozdawców. Wymiana uwag odbywała się jeszcze zanim sprawozdawcy uzyskali mandat do prac nad wytycznymi.

## 7. Monitorowanie rozwoju nowych technologii

Prezes UODO analizuje sygnały otrzymywane od innych organów nadzorczych za pośrednictwem systemu wymiany informacji na rynku wewnętrznym IMI, dotyczące planów administratorów względem wprowadzania nowych technologii i nowych czynności przetwarzania na oferowanych przez nich usługach. W wyniku takich działań Prezes UODO może lepiej przygotować się do ewentualnych działań nadzorczych, a także edukacyjnych i informacyjnych. Przykładem może być komunikat wydany 30 kwietnia 2025 r. dotyczący możliwości wyrażenia sprzeciwu wobec przetwarzania danych na potrzeby rozwoju sztucznej inteligencji przez użytkowników Meta.

UODO był zaangażowany także w działania dot. zbierania informacji i szerzenia świadomości na temat zagrożeń związanych z korzystaniem z chińskiej aplikacji oferującej usługi Chatbot AI – DeepSeek.

## 8. Warsztaty

### 1. Europejskie Warsztaty Skargowe, 17-19.11.2025 r.

W Europejskich Warsztatach Skargowych (ECHW 2025), które odbyły się 17–19 listopada 2025 r. w Prisztinie w Kosowie, uczestniczył Prezes UODO i ekspert Departamentu Współpracy Międzynarodowej UODO.

Organizatorem ECHW 2025 była Agencja ds. Informacji i Prywatności w Kosowie. Warsztaty służyły wymianie wiedzy i doświadczeń na temat spraw skargowych rozpatrywanych przez organy nadzorcze i porównaniu procedur, jakie mają zastosowanie w takich postępowaniach. Celem spotkania było również usprawnienie rozpatrywania skarg transgranicznych.

Ekspert UODO przedstawił prezentację „Handling Deepfake Cases – Practical Experiences" oraz poprowadził panel dyskusyjny „Deepfake and AI generated content – a challenge for personal data protection". W ramach prezentacji oraz w trakcie panelu dyskusyjnego omówiono problematykę treści wykorzystujących technologię deepfake, jakie pojawiają się m.in. na platformach społecznościowych. Zwrócono uwagę, że operatorzy platform społecznościowych domagają się, by skargi na wykorzystanie czyjegoś wizerunku w mediach społecznościowych kierować bezpośrednio do autora takiego wpisu. Dyskusji poddane zostały ponadto zależności między RODO (które reguluje przetwarzanie danych osobowych) a Aktem o usługach cyfrowych (które dotyczy nielegalnych treści i obowiązków platform).

### 2. Trzeci Bootcamp EROD na temat AI & AI Auditing, 1–2.10.2025 r.

Trzecia edycja Bootcamp EROD poświęcona była audytowi systemów sztucznej inteligencji. Wydarzenie obejmowało warsztaty techniczne dotyczące analizy SDK w aplikacjach mobilnych z wykorzystaniem narzędzi takich jak Pirogue, pcapng-utils, har-analyzer-vuejs oraz Ogre. W trakcie Bootcampu przeprowadzono szkolenia mające na celu wyjaśnienie sposobu funkcjonowania sztucznej inteligencji oraz z programów SPE 2024 skierowanych do inspektorów ochrony danych i specjalistów technicznych. Zrealizowano również praktyczny warsztat tworzenia algorytmu AI oraz zaprezentowano zagadnienia związane z audytem prywatności modeli AI, w tym projekt PANAME. Omówiono doświadczenia EIOD w zakresie nadzoru nad systemami sztucznej inteligencji, a także przeanalizowano kwestie uprzedzeń algorytmicznych, technik unlearningu oraz prywatności różnicowej. Przedmiotem dyskusji były również ryzyka związane z technologiami OCR i NER oraz dużymi modelami językowymi, jak również kierunki prac SPE planowane na 2026 r.

Udział w Bootcampie umożliwił pogłębienie wiedzy w zakresie audytu systemów sztucznej inteligencji, testowania prywatności modeli, oceny ryzyk oraz wykorzystania praktycznych narzędzi wspierających nadzór nad tym obszarem.

## 9. Udział UODO w pracach organów i organizacji międzynarodowych

### 9.1. Komitet Konsultacyjny Konwencji nr 108

Członkostwo UODO w Radzie Europy w ramach Komitetu Konsultacyjnego Konwencji nr 108 (T-PD)

W 2025 roku przedstawiciele UODO wzięli udział w 48. (17-19.06.2025) i 49. (5-7.11.2025) posiedzeniu plenarnym Komitetu T-PD. W ramach przygotowań do posiedzenia plenarnego T-PD Rady Europy, które odbyło się 17 czerwca 2025 roku, Prezes UODO opracował uwagi do art. 11 Konwencji 108. Przedstawiciele UODO przygotowali stanowisko oraz wzięli czynny udział w dyskusji na 49. posiedzeniu plenarnym T-PD.

Przygotowane materiały dotyczyły przede wszystkim transgranicznych przepływów danych, w tym stosowania Modelowych Klauzul Umownych (MCC), wdrażania art. 14 Konwencji 108+, a także potrzeby opracowania praktycznych wytycznych i wzmocnienia współpracy między Komitetem a krajowymi organami nadzorczymi. Odniesiono się również do wyzwań związanych z ochroną danych w kontekście dużych modeli językowych (LLM), w szczególności ryzyk wynikających z wykorzystywania danych do trenowania systemów AI, oraz do zagadnień związanych z neurotechnologią, takich jak przetwarzanie danych neuronowych i wynikające z tego zagrożenia dla prywatności oraz praw podstawowych.

Podczas 48. posiedzenia Komitetu Konwencji 108 (T-PD) skoncentrowano się na rozwoju standardów ochrony danych w kontekście nowych technologii. Przyjęto wytyczne dotyczące art. 11 Konwencji 108, zatwierdzono raport dotyczący dużych modeli językowych oraz kontynuowano prace nad wytycznymi w obszarze neuronauk. Równolegle omawiano kwestie związane z ratyfikacją Konwencji 108+, transgranicznymi transferami danych oraz współpracą międzynarodową. Z kolei podczas 49. posiedzenia nacisk położono na działania operacyjne i strategiczne, w tym stan ratyfikacji Konwencji 108+, rozwój narzędzi wspierających transfery danych oraz przygotowanie programu prac na lata 2026–2029. Kontynuowano również prace nad wytycznymi dotyczącymi dużych modeli językowych i neuronauk, podkreślając znaczenie ochrony danych szczególnie wrażliwych. Omówiono także bieżące inicjatywy międzynarodowe, wzmacniając rolę Rady Europy jako globalnego punktu odniesienia w obszarze ochrony danych.

### 9.2. Global Privacy Assembly - GPA

Udział w pracach GPA

- W 2025 roku Prezes UODO opracował uwagi do projektu Rezolucji GPA w sprawie planu działania na rzecz współpracy organów nadzorczych, w tym wymiany najlepszych praktyk i opracowania praktycznych wskazówek wspierających skuteczne

wdrażanie przepisów o ochronie danych w różnych porządkach prawnych”[673] (17.04.2025), przyjęte na konferencji w Batumi, która odbyła się 8 maja 2025 r.

- Jak już o tym wspomniano w niniejszym Sprawozdaniu, **Urząd Ochrony Danych Osobowych otrzymał wyróżnienie w ramach Giovanni Butarelli Award i GPA Global and Privacy Awards 2025.** Nagroda została przyznana w kategorii „Education and Awareness” za projekt „Wizerunek dziecka w internecie. Publikować czy nie?” zrealizowany wspólnie z Fundacją Orange. Uroczyste ogłoszenie zwycięzców i wyróżnionych odbyło się podczas 47. Konferencji GPA, która miała miejsce 15–19 września 2025 roku w Seulu (Korea Południowa). Celem projektu było podniesienie świadomości dorosłych – w tym rodziców, nauczycieli oraz instytucji pracujących z dziećmi – na temat ryzyk związanych z publikowaniem wizerunku najmłodszych w sieci. Projekt zwraca uwagę, że zdjęcia i nagrania dzieci, nawet udostępniane w dobrej wierze, mogą prowadzić do poważnych zagrożeń: hejtu, cyberprzemocy, kradzieży tożsamości czy nieuprawnionego wykorzystania wizerunku. Poradnik zawiera praktyczne wskazówki: jak konstruować zgodę na publikację zdjęć, jakie mity funkcjonują wokół prawa do wizerunku, jakie pytania warto zadać sobie przed zamieszczeniem treści w sieci. Wyjaśnia również pojęcia takie jak „sharenting” czy „troll parenting” i wskazuje alternatywne sposoby przedstawiania dzieci w mediach społecznościowych, bez narażania ich prywatności. Wyróżnienie dla UODO to dowód na to, że polskie działania edukacyjne w obszarze ochrony danych osobowych spotykają się z uznaniem na forum globalnym. Przedstawicielka UODO uczestniczyła w pracach w tzw. Grupie Oceny GPA.
- Prezes UODO uczestniczył w **47. Dorocznej konferencji GPA w Seulu (15-19.09.2025)**, podczas której podpisał „Wspólne oświadczenie dotyczące tworzenia wiarygodnych ram zarządzania danymi sprzyjających rozwojowi innowacyjnej i przyjaznej dla prywatności sztucznej inteligencji”. Sygnatariuszami tego dokumentu jest 20 państw członkowskich GPA. Podczas tego spotkania przyjęto 3 ww. rezolucje dotyczące: nadzoru człowieka nad AI, wykorzystania danych do trenowania modeli oraz ochrony danych w edukacji cyfrowej. Jak już wspomniano, w ramach nagród GPA wyróżniono m.in. UODO w kategorii „Education and Awareness” za podradnik, którego angielskojęzyczna wersja nosiła tytuł: „The Image of a child on the Internet. To publish or not to publish”). Uruchomiono też nową nagrodę łączącą prywatność i prawa człowieka jako inicjatywę wzmacniającą postrzeganie prywatności jako prawa podstawowego.

### 9.3. Grupa Berlińska

Uczestnictwo w pracach Grupy Berlińskiej (International Working Group on Data Protection and New Technologies)

W 2025 roku przedstawiciele UODO uczestniczyli w dwóch spotkaniach Grupy Berlińskiej:

[673] Ang. „Resolution on the Action Plan for the Further Collaboration Activities of the DPAs, Including Sharing Best Practices and Developing Practical Guidance to Support the Effective Implementation of Data Protection Laws Across Jurisdictions” – 17.04.2025 r.).

- **75. spotkanie Grupy Berlińskiej. Tbilisi (Gruzja), 1-3.07.2025 r.** koncentrowało się na nowych technologiach i ich wpływie na ochronę danych, m.in. neurotechnologii, rozszerzonej rzeczywistości, chmurze obliczeniowej, technologiach 6G oraz zarządzaniu zgodą (opt-out). Omawiano także kierunki przyszłych prac, w tym AI (np. modele open source, agentowa AI), dane syntetyczne i tożsamość cyfrową.
- **76. spotkanie Grupy Berlińskiej. Montevideo (Urugwaj), 18-20.11.2025 r.** dotyczyło głównie praktyk regulacyjnych i strategii państw w obszarze AI i danych, a także konkretnych zagadnień technologicznych, takich jak chmura, dane syntetyczne, 6G, dane pośmiertne oraz globalne mechanizmy opt-out. Spotkanie podkreśliło rosnące znaczenie AI, współpracy międzynarodowej i budowania wspólnych standardów ochrony danych.

Na obydwu spotkaniach przedstawiciel UODO przedstawił raport krajowy dotyczący działań Prezesa UODO w minionym półroczu. Ponadto przedstawiciele UODO rozpoczęli działania nakierowane na organizację 77. spotkania Grupy Berlińskiej, które odbędzie się w Warszawie (czerwiec 2026 r.).

### 9.4. Postępowania transgraniczne

Działania dotyczące postępowań transgranicznych

W ramach działalności Wydziału ds. Postępowań Transgranicznych w Urzędzie Ochrony Danych Osobowych dokonano wstępnej analizy **2665 notyfikacji IMI**, w ramach których Prezes UODO został wskazany jako odbiorca lub jeden z odbiorców notyfikacji.

Po dokonaniu wstępnej analizy ww. notyfikacji oraz załączonej dokumentacji, Prezes UODO ustalił swoją rolę w:

- **927 notyfikacjach** „A56 – Ustalanie LSA i CSA” jako organ nadzorczy, którego sprawa nie dotyczy;
- **304 notyfikacjach** „A56 – Ustalanie LSA i CSA” jako organ nadzorczy, którego sprawa dotyczy,;
- **22 notyfikacjach** „A56 – Ustalanie LSA i CSA” jako wiodący organ nadzorczy właściwy do rozpatrzenia sprawy.

Pozostałe notyfikacje dotyczyły w szczególności:

- przyjęcia projektów decyzji lub ostatecznych decyzji przez organy nadzorcze;
- informacji o postępach w sprawach skargowych prowadzonych przez Prezesa UODO w charakterze organu, do którego skarga wpłynęła lub wiodącego organu nadzorczego – w takim wypadku notyfikacje były rejestrowane i powiązane w systemie EZD z odpowiednimi postępowaniami;
- wiążących reguł korporacyjnych oraz certyfikacji;
- ogólnych wniosków o informację oraz zapytań prawnych innych organów – w takim wypadku pracownicy DWM współpracowali z pozostałymi Departamentami w przygotowaniu odpowiedzi;

- informacji przekazywanych przez organ irlandzki do wszystkich organów nadzorczych dotyczących prowadzonych przez ten organ czynności z urzędu.

Do Prezesa UODO wpłynęło ponadto **łącznie 56 skarg** na podmioty mające siedzibę w innym państwie członkowskich, których przedmiotem było przetwarzania transgraniczne.

- **41 skarg** zostało przekazanych bezpośrednio do Wydziału ds. Postępowań Transgranicznych;
- **8 skarg** zostało przekazanych przez Departament Wstępnej Kontroli Skarg i Naruszeń, natomiast
- **7 skarg** zostało przekazanych przez Departament Skarg.

Przetłumaczona dokumentacja skargowa zastała następnie przekazana w systemie IMI do wiodących organów nadzorczych.
W Wydziale ds. Postępowań Transgranicznych UODO zakończono **67 spraw**, w tym:

- **4 sprawy** *ad acta* lub bez rozpoznania;
- **20 spraw** w ramach decyzji administracyjnych;
- **7 spraw** w ramach postanowień administracyjnych;
- **36 spraw** w wyniku współpracy z wiodącymi organami nadzorczymi poprzez przekazanie skarżącym wypracowanych wspólnie rozstrzygnięć.

### 9.5. Współpraca w ramach IMI

Prowadzenie postępowań w charakterze wiodącego organu nadzorczego (LSA) w następstwie przekazania skarg od organów poprzez system wymiany informacji na rynku wewnętrznym (IMI)

Od 25 maja 2018 r. organy nadzorcze korzystają z systemu wymiany informacji na rynku wewnętrznym[674], 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.

Na początku listopada 2025 r., w następstwie rozmów wewnętrznych dotyczących podejścia w stosunku do przekazywanych do Prezesa UODO skarg przez inne organy nadzorcze, zawierających braki formalne w rozumieniu ustawy – Kodeks postępowania administracyjnego (K.p.a.), wypracowane zostało zgodne stanowisko w świetle panującej zasady wzajemnego uznawania skarg wynikającej m.in. z *wewnętrznego dokumentu EROD 6/2020 dot. wstępnych czynności w celu*

[674] Ang. *Internal Market Information System*, dalej: „system IMI” lub „IMI”.

*rozpatrzenia sprawy: dopuszczalność oraz ocena skarg*, a wymogów wobec pism skargowych wynikających z przepisów K.p.a.

Przyjęto koncepcję wzajemnego uznawania skarg, tj. w sytuacji, gdy skarga w ocenie organu ją przyjmującego nie ma braków formalnych, organ do którego zostaje ona przekazana nie powinien ponownie weryfikować jej pod kątem braków formalnych i przystąpić do jej rozpatrzenia.

W świetle tych ustaleń, Prezes UODO przystąpił do wszczęcia i aktywnego prowadzenia postępowań w sprawie skarg przekazanych przez inne organy nadzorcze w ramach Systemu IMI, w których Prezes UODO działa w charakterze wiodącego organu nadzorczego.

### 9.6. Data Protection Framework

Wpływ i przekazanie skargi

W kwietniu 2025 r. wpłynęła do Prezesa Urzędu skarga skierowana do amerykańskiego biura urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych - ODNI CLPO (Office of the Director of National Intelligence Civil Liberties Protection Officer). Skarżąca podnosiła, że amerykańskie agencje wywiadowcze stosowały na niej narzędzia rozpoznania radioelektronicznego, które wiązało się z licznymi konsekwencjami natury fizycznej. Skarżąca zażądała usunięcia jej danych osobowych znajdujących się w Stanach Zjednoczonych oraz przekazania w formie pisemnej potwierdzenia tego faktu, a także zadośćuczynienia finansowego odnoszącego się poniesionego uszczerbku psychicznego.

Zgodnie z punktem 1) regulaminu wewnętrznego dotyczącego współpracy i odpowiednich ról krajowych organów nadzorczych oraz sekretariatu EROD, w odniesieniu do składania skargi w ramach mechanizmu dochodzenia roszczeń dostępnego dla osób fizycznych z UE w związku z domniemanymi naruszeniami prawa Stanów Zjednoczonych, w odniesieniu do ich danych gromadzonych przez władze tego kraju właściwe w sprawach bezpieczeństwa narodowego (z 17.04.2024 r.), do zadań Prezesa UODO, jako organu przyjmującego skargę, należy m.in. weryfikacja tożsamości skarżącego, sprawdzenie, czy skarga spełnia warunki określone w sekcji 4. lit. k) ppkt (i) – (iv) Rozporządzenia Wykonawczego 14086 oraz weryfikacja kompletności skargi w świetle rozporządzenia wykonawczego oraz dyrektywy Wspólnoty Wywiadowczej (dyrektywa ICD 126). Jeśli skarga zostanie uznana za kompletną, to następuje przekazanie jej do sekretariatu EROD w zaszyfrowanej formie oraz powiadomienie skarżącego o odpowiedzi CLPO otrzymanej za pośrednictwem sekretariatu EROD.

W listopadzie 2025 r. Prezes UODO uznał skargę za kompletną oraz dokonał jej tłumaczenia na język angielski, a dokumentacja skargowa została przekazana do zaszyfrowania przez Departament Informatyki i Cyberbezpieczeństwa UODO. 15 grudnia 2025 r. skarga została przekazana do Sekretariatu EROD, który następnie przekazał ją do ODNI CLPO. 12 stycznia 2026 r. Prezes UODO został poinformowany przez Sekretariat EROD, że ODNI CLPO uznało skargę za „qualifying complaint”

w rozumieniu Intelligence Community Directive 126, Section E.1.c., w związku z czym CLPO rozpocznie postępowanie wyjaśniające.

### 9.7. Rozporządzenie proceduralne

W 2025 r. Prezes UODO rozpoczął prace nad wdrożeniem w Urzędzie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/2518 z dnia 26 listopada 2025 r. w sprawie ustanowienia dodatkowych przepisów proceduralnych dotyczących egzekwowania rozporządzenia (UE) 2016/679. Tak zwane rozporządzenie proceduralne wprowadza jednolite zasady prowadzenia postępowań w sprawach transgranicznego przetwarzania danych osobowych. W toku prac nad wdrożeniem przygotowano i przedstawiono prezentację, w ramach której omówiono obecnie stosowaną procedurę opartą na mechanizmie OSS (art. 60 RODO), wskazując jej kluczowe etapy oraz problemy wynikające z braku krajowych regulacji dostosowanych do wymogów unijnych.

Szczególną uwagę poświęcono wyzwaniom proceduralnym, takim jak brak podstaw prawnych do wstępnej oceny skarg, trudności w doręczeniach czy kolizje między K.p.a. a obowiązkami wynikającymi z RODO. W dalszej części przedstawiono główne założenia rozporządzenia, w tym definicję dopuszczalności skargi, obowiązek sporządzenia wstępnej konkluzji przez organ przyjmujący skargę, procedury uproszczone (wczesne rozstrzyganie, prosta współpraca) oraz nowe terminy i zasady wymiany informacji między organami. Podkreślono również konieczność zmian w prawie krajowym, aby zapewnić zgodność z nowymi regulacjami i efektywność mechanizmu współpracy organów nadzorczych.

Prezentacja dotycząca rozporządzenia proceduralnego była działaniem własnym, analogicznym do inicjatyw własnych o których informacje przychodzą do nas z innych organów nadzorczych – poszczególne organy, m.in. francuski organ - CNIL, również prowadzą prace wewnętrzne mające przygotować ich urząd na zmiany związane z rozporządzeniem proceduralnym.

## 10. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2025 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) 33. Wiosenna Konferencja Europejskich Organów Ochrony Danych. Batumi, 6-9.05.2025 r.

Gospodarzem 33. Wiosennej Konferencji Europejskich Organów Ochrony Danych (zwanej dalej „Wiosenną Konferencją”), był gruziński organ ochrony danych. W wydarzeniu uczestniczyły prof. Agnieszka Grzelak, Zastępczyni Prezesa Urzędu

Ochrony Danych Osobowych oraz ekspertka Departamentu Współpracy Międzynarodowej, a także przedstawiciele europejskich organów ochrony danych i różnych instytucji europejskich, w tym EUROPOLU, EUROJUSTU, EUROSTATU i EIOD. Hasło przewodnie wydarzenia brzmiało: „Najcenniejszym skarbem danej osoby jest jej tożsamość".

Gospodarze i goście konferencji omówili szereg istotnych tematów, w tym regulację sztucznej inteligencji i ram prawnych ochrony danych na szczeblu krajowym, europejskim i globalnym, ochronę prywatności i danych osobowych dzieci, wpływ nowoczesnego rozwoju technologicznego i sztucznej inteligencji na prawo do prywatności, wyzwania w zakresie ochrony danych osobowych związane ze zdrowiem oraz rolę inspektorów ochrony danych i specjalistów ds. prywatności. Podczas tego wydarzenia przyjęto *Rezolucję w sprawie planu działania dotyczącego dalszych działań w zakresie współpracy,* której współwnioskodawcą był UODO. Pod głosowanie poddano także kwestię akredytacji dwóch organów nadzorczych ds. ochrony danych - Andaluzji oraz Kosowa, wynikiem którego było przyjęcie obu rezolucji w sprawie akredytacji wskazanych organów jako członków Wiosennej Konferencji Europejskich Organów Ochrony Danych.

Pod koniec każdego dnia konferencji odbyły się dwa równoległe wydarzenia towarzyszące: „Ochrona danych w Gruzji – wyzwania i szanse" oraz „Ocena wpływu sztucznej inteligencji na prawa podstawowe: od wymogów prawnych do wdrożenia". Kataloński model FRIA (ang. Fundamental Rights Impact Assessment; ocena wpływu na prawa podstawowe)".

Wiosenna Konferencja odbywa się od 1991 r. i odgrywa kluczową rolę w dyskusji na temat pojawiających się tendencji w zakresie prywatności i ochrony danych. Wydarzenie to promuje konstruktywny dialog między europejskimi organami ochrony danych a praktykami w tej dziedzinie, tworząc silną platformę umożliwiającą sprostanie zarówno wyzwaniom, jak i możliwościom w przestrzeni ochrony danych. Konferencja jest znana jako kluczowe wydarzenie poświęcone przeglądowi standardów europejskich w zakresie ochrony danych osobowych oraz wymianie najlepszych praktyk w całej Europie. Dlatego warto podkreślić znaczenie uczestnictwa przedstawicieli UODO w powyższym wydarzeniu, albowiem Wiosenne Konferencje są najważniejszym, corocznym spotkaniem wszystkich rzeczników ochrony danych osobowych z państw członkowskich UE, innych państw europejskich oraz przedstawicieli Komisji Europejskiej, Rady Europy oraz innych organów zajmujących się ochroną danych osobowych. Poszczególne konferencje poświęcone są różnym aspektom ochrony danych osobowych w Europie, a ich uczestnicy podejmują działania ukierunkowane nie tylko na wdrażanie unijnych przepisów, ale również na monitorowanie ich przestrzegania w poszczególnych krajach. To coroczne wydarzenie jest ważnym spotkaniem, podczas którego organy regulacyjne współpracują w celu poprawy środków ochrony danych[675].

[675] Więcej informacji można znaleźć na stronie: https://www.dpaspringconference.org/.

**2) 23. Spotkanie Grupy Organów Ochrony Danych Europy Środkowej i Wschodniej. Kraków i Lusławice, 12-13.06.2026 r.**

W Krakowie i Lutosławicach odbyło się 23. Spotkanie Grupy organów ochrony danych Europy Środkowej i Wschodniej (CEEDPO), zorganizowane przez UODO. Podczas wydarzenia Prezes UODO i przedstawiciele organów nadzorczych z Europy Środkowo-Wschodniej podpisali deklarację w sprawie wzmocnienia organów ochrony danych, zapewnienia równowagi regulacyjnej oraz wsparcia dla małych i średnich przedsiębiorstw i organizacji pozarządowych.

Sygnatariusze Deklaracji wskazali, że zarówno małe i średnie przedsiębiorstwa, jak i organizacje pozarządowe borykają się z podobnymi wyzwaniami w stosowaniu złożonych przepisów o ochronie danych. Uczestnicy zobowiązali się do promowania uproszczeń i zmniejszenia obciążeń administracyjnych przy pełnym poszanowaniu praw osób fizycznych.

W Deklaracji podkreślono m.in.:

- potrzebę przeprowadzenia rzetelnej oceny planowanych zmian legislacyjnych, w tym propozycji deregulacyjnych przepisów o ochronie danych, opartej na badaniach i analizach wpływu na różne sektory;
- konieczność wspierania organizacji pozarządowych, które podobnie jak MŚP często dysponują ograniczonymi zasobami wdrożeniowymi;
- wzmocnienie niezależnych organów nadzorczych poprzez zwiększenie ich finansowania i potencjału doradczego, tak aby mogły skutecznie wspierać różnorodne grupy interesariuszy;
- kontynuację współpracy i wymiany wiedzy pomiędzy organami ochrony danych z regionu Europy Środkowo-Wschodniej.

Deklaracja zakłada, że regulacje prawne w obszarze ochrony danych powinny ewoluować w sposób, który wspiera działalność gospodarczą i społeczną oraz innowacje, zachowując jednocześnie wysoki standard ochrony prywatności i poszanowania praw jednostki.

W ramach spotkania CEEDPO odbyła się:

**3) Międzynarodowa konferencja pt. „Technologie kwantowe: zagrożenia, wyzwania i szanse dla cyberbezpieczeństwa i ochrony danych osobowych". Kraków, 12.06.2025 r.** (opisana również w części III rozdz. 2.13 Sprawozdania).

Prezes UODO był współorganizatorem tej Międzynarodowej konferencji, poświęconej technologiom kwantowym oraz ich wpływowi na ochronę danych osobowych.

Program konferencji obejmował cztery panele tematyczne, w ramach których omówiono kluczowe zagadnienia związane z rozwojem i zastosowaniem technologii kwantowych. Dyskusje koncentrowały się na:

- aspektach technicznych, w tym zagrożeniach dla współczesnej kryptografii oraz rozwoju rozwiązań postkwantowych;
- wymiarze politycznym i strategicznym, obejmującym kwestie suwerenności cyfrowej oraz potrzebę opracowania europejskiej strategii w obszarze technologii kwantowych;
- relacji pomiędzy technologiami kwantowymi a przepisami o ochronie danych osobowych, ze szczególnym uwzględnieniem zasady neutralności technologicznej oraz standardów ochrony danych;
- wyzwaniach i kierunkach rozwoju kryptografii kwantowej i postkwantowej, a także roli instytucji takich jak NIST i ENISA.

W trakcie konferencji podkreślono konieczność odpowiedniego przygotowania się na zmiany wynikające z rozwoju technologii kwantowych, w szczególności poprzez wzmacnianie kompetencji oraz działania edukacyjne w tym obszarze.

#### 4) Posiedzenie Grupy wysokiego szczebla EROD. Helsinki, 1-2.07.2025 r.

W posiedzeniu Grupy wysokiego szczebla EROD uczestniczyły prof. Agnieszka Grzelak, Zastępczyni Prezesa UODO oraz ekspertka Departamentu Współpracy Międzynarodowej UODO.

Podczas wydarzenia 2 lipca 2025 r. EROD przyjęła przełomowe oświadczenie w sprawie zwiększenia jasności, wsparcia i zaangażowania. W dokumencie tym przedstawiono nowe inicjatywy mające na celu ułatwienie przestrzegania RODO, w szczególności dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, zwiększenie spójności i zacieśnienie współpracy międzyregulacyjnej.

EROD potwierdziła kluczową rolę ochrony danych w przestrzeganiu europejskich wartości, ochronie praw podstawowych oraz wspieraniu zorientowanego na człowieka wykorzystania danych osobowych. Zobowiązała się do wcześniejszego i bardziej proaktywnego współdziałania z zainteresowanymi stronami, w tym do publicznego informowania o wynikach konsultacji publicznych. EROD zobowiązała się również do zapewnienia jaśniejszych, bardziej praktycznych i dostępnych wskazówek oraz do odpowiedniego zaktualizowania swoich metod pracy. Nowe narzędzia będą obejmowały zharmonizowane szablony, praktyczne zasoby, takie jak listy kontrolne i często zadawane pytania (FAQ), oraz wspólny szablon powiadomienia o naruszeniu ochrony danych."[676]

EROD zwiększy również spójność w stosowaniu i egzekwowaniu RODO oraz pogłębi współpracę z innymi organami regulacyjnymi niebędącymi organami ochrony danych w celu sprostania prawnym i praktycznym wyzwaniom pojawiającym się w sprawach międzysektorowych.

#### 5) 47. Konferencja Global Privacy Assembly (GPA). Seul, 15-19.09.2025 r.

Global Privacy Assembly –- to coroczne spotkanie przedstawicieli organów ochrony danych i prywatności z całego świata. W tegorocznej edycji w Seulu, której

[676] Cyt. za: EDPB, *Annual Report 2025*, str. 13, tłum. własne.

gospodarzem był koreański organ ochrony danych Personal Information Protection Commission (PIPC), uczestniczyli regulatorzy, eksperci i partnerzy z organizacji międzynarodowych. Konferencja obejmowała zarówno sesje zamknięte dla członków GPA, jak i wydarzenia otwarte, podczas których omawiano kluczowe wyzwania związane z ochroną prywatności – od nowych modeli reklamy ukierunkowanej, przez sztuczną inteligencję i rozwój globalnych standardów ochrony danych osobowych, po regulację systemów sztucznej inteligencji w obszarze edukacji.

Ważnym punktem programu był konkurs Global Privacy and Data Protection Awards, w ramach którego wyróżniane były inicjatywy podejmowane przez organy nadzorcze na całym świecie w obszarze edukacji, innowacji i egzekwowania prawa. Jak już o tym wcześniej wspomniano w innej części niniejszego Sprawozdania, w tegorocznej edycji tego konkursu wyróżniony został poradnik UODO pt. „Wizerunek dziecka w internecie. Publikować czy nie?", przygotowany we współpracy z Fundacją Orange. Udział UODO w GPA 2025 i otrzymane wyróżnienie wpisują się w szerszy kontekst działań Polski na rzecz międzynarodowej współpracy w zakresie ochrony danych. Konferencja w Seulu pokazała, że edukacja i budowanie świadomości społecznej są równie ważne jak tworzenie i egzekwowanie regulacji czy rozwój technologicznych narzędzi ochrony prywatności. Dzięki takim inicjatywom jak projekt „Wizerunek dziecka w internecie. Publikować czy nie?", Polska miała swój wkład w globalną debatę na temat praw dzieci w cyfrowym świecie – i stała się przykładem, jak skutecznie łączyć prawo, etykę i praktyczne rozwiązania w ochronie danych osobowych.

### 6) III Konferencja z cyklu Artificial Inteligence and Education pt. „Ensuring Quality Education in the AI Era – Introducing the Council of Europe Compass for AI and Education". Strasburg, 18-19.10.2026 r.

Organizatorem tego wydarzenia, które odbyło się w siedzibie Rady Europy w Strasburgu, był Departament Edukacji RE. Celem konferencji było zaprezentowanie „Kompasu Rady Europy dotyczącego sztucznej inteligencji i edukacji". Dokument przybrał formę wytycznych, które pomogą państwom członkowskim, instytucjom edukacyjnym, nauczycielom, uczniom i podmiotom sektora prywatnego wdrażać odpowiedzialne, etyczne i zorientowane na człowieka wykorzystanie sztucznej inteligencji w edukacji, zgodnie z zasadami praw człowieka, demokracji i praworządności. Według autorów dokumentu, cztery elementy okazują się niezbędne do zapewnienia, że integracja sztucznej inteligencji w edukacji promuje i chroni prawa człowieka, demokrację i praworządność, jednocześnie wzmacniając pozycję uczniów, nauczycieli i instytucji poprzez odpowiedzialne, zorientowane na człowieka i zgodne z wartościami wykorzystanie i zrozumienie technologii sztucznej inteligencji.

**Główne punkty przewodnie Kompasu:**

1) <u>Umiejętność korzystania ze sztucznej inteligencji.</u>

W ramach tego filaru opracowywany został projekt zalecenia Komitetu Ministrów RE w sprawie umiejętności korzystania ze sztucznej inteligencji. Projekt zalecenia

wskazuje, że na umiejętność korzystania ze sztucznej inteligencji składają się trzy wymiary:

- technologiczny (jak działa sztuczna inteligencja i jak można ją rozwijać),
- praktyczny (jak można skutecznie wykorzystywać sztuczną inteligencję) oraz
- ludzki (wpływ sztucznej inteligencji na ludzi, prawa człowieka, demokrację i praworządność). Rzadko w pełni uwzględniany wymiar ludzki ma kluczowe znaczenie dla proponowanej umiejętności korzystania z AI z trzech powodów:
  - aby zapewnić, że umiejętność korzystania z AI odzwierciedla podstawowe wartości Rady Europy,
  - ponieważ rzadko przywiązuje się do niego wystarczającą wagę oraz
  - ponieważ wiedza techniczna i praktyczne umiejętności w zakresie AI szybko stają się nieaktualne.

2) Regulacje i zarządzanie.

Departament Edukacji Rady Europy, zlecając w 2024 roku przeprowadzenie badania przygotowawczego dotyczącego opracowania instrumentu prawnego, podkreślał w nim rosnące wykorzystanie technologii sztucznej inteligencji w systemach edukacyjnych oraz ich wpływ na praktyki edukacyjne. Wyniki badania pokazały, że bez odpowiednich zabezpieczeń systemy sztucznej inteligencji mogą stanowić zagrożenie dla praw dzieci pod względem dostępu do wysokiej jakości edukacji. Podczas drugiej konferencji roboczej „Regulowanie stosowania systemów sztucznej inteligencji w edukacji" (24–25.10.2024 r.), omówiono główne elementy instrumentu prawnego i otoczenie regulacyjne. W oparciu o wyniki konferencji i badania przygotowawcze w **czerwcu 2025 r**. **rozpoczęto prace nad wnioskiem dotyczącym opracowania projektu instrumentu prawnego regulującego wykorzystanie systemów sztucznej inteligencji w edukacji.**

3) Nauczanie, uczenie się i ocenianie z wykorzystaniem sztucznej inteligencji.

W ramach tego filaru opracowywany został zestaw narzędzi politycznych dotyczących sztucznej inteligencji i edukacji. Jego głównym celem było udzielenie decydentom, instytucjom i nauczycielom wskazówek dotyczących podejmowania świadomych, opartych na dowodach i odpowiedzialnych decyzji dotyczących nauczania i uczenia się z wykorzystaniem sztucznej inteligencji oraz na jej temat, zgodnie z wizją i standardami Rady Europy w zakresie wysokiej jakości edukacji.

4) Ocena technologii edukacyjnych, w tym systemów sztucznej inteligencji w edukacji.

Wraz z coraz większym upowszechnianiem się sztucznej inteligencji w systemach edukacyjnych w całej Europie, pilna stała się potrzeba stworzenia spójnych, opartych na prawach mechanizmów oceny technologii edukacyjnych. Bez skoordynowanego podejścia sztuczna inteligencja może pogłębiać nierówności, podważać intencje pedagogiczne i naruszać prawa podstawowe, takie jak prawo do prywatności, autonomii i niedyskryminacji. W oparciu o tę obserwację Departament Edukacji zlecił przeprowadzenie studium wykonalności w celu oceny potrzeby i wykonalności europejskiego systemu przeglądu. W studium wykonalności europejskich ram odniesienia dla oceny technologii edukacyjnych przeprowadzono kompleksowy przegląd istniejących ram oceny technologii edukacyjnych, czerpiąc zarówno z sektora

publicznego, jak i prywatnego, a także z badań naukowych. Zaleca się w nim ramy odniesienia, które składają się zarówno z podstawowego zestawu ponadnarodowych kryteriów oceny, jak i zestawu zaleceń, które należy elastycznie stosować w ramach krajowej praktyki.

W trakcie konferencji przedstawienie zostały również zmiany w polityce i przykłady wykorzystania sztucznej inteligencji w państwach członkowskich. Uczestnicy zostali włączeni w prace nad dopracowaniem poszczególnych elementów dokumentu. Poprzez warsztaty i pracę w grupach, organizatorzy zaprosili uczestników do podzielenia się różnorodnymi i krytycznymi spojrzeniami na wpływ sztucznej inteligencji na jakość edukacji i jej zapewnienie. W konkluzji wskazano na konieczność stworzenia mechanizmów wspólnego zarządzania SI, poprzez zaangażowanie rządów, instytucji edukacyjnych, społeczeństwa obywatelskiego, firm technologicznych, a także uczniów, nauczycieli i środowiska lokalnego, w kształtowanie i monitorowanie wykorzystania sztucznej inteligencji w edukacji.

### 7) Konferencja „The Way Forward”. Lublana, 18-19.11.2025 r.

Konferencja „The Way Forward” zamykająca Europejski Rok Edukacji Cyfrowej Obywateli 2025, zorganizowana została w ramach projektu pod nazwą *DIGI.DR – Wzmacnianie obywatelstwa cyfrowego w instytucjach edukacyjnych* we współpracy z Ministerstwem Edukacji Słowenii i Departamentem Edukacji Rady Europy. Dyskusje podczas sesji plenarnych i prowadzonych równolegle warsztatów koncentrowały się na kluczowych tematach, a mianowicie:

- **edukacji medialnej i informacyjnej** – przeciwdziałanie dezinformacji, budowanie konstruktywnych komunikatów w środowiskach cyfrowych, wzmacnianie pozycji młodzieży w zakresie budowania odpowiedzialności medialnej;
- **dobremu samopoczuciu online** – kształtowanie właściwych nawyków cyfrowych, etykiety informacyjnej promującej demokrację i prawa człowieka oraz zachowanie równowagi między czasem spędzanym przed ekranem a zdrowiem psychicznym;
- **prawu obowiązującemu w sieci** – w obszarze etycznej i prawnej odpowiedzialności platform społecznościowych, wzmacnianiu aktywnego obywatelstwa cyfrowego i świadomości konsumenckiej.

Uczestnicy dzielili się swoimi historiami sukcesu, dobrymi praktykami i materiałami; omawiali innowacyjne środki reagowania; wymieniali się pomysłami na działania i mechanizmy raportowania, strategie komunikacji, współpracę partnerów i przyszłą ocenę planu działania na rzecz przyszłości edukacji w zakresie obywatelstwa cyfrowego (2027–2031). Podczas warsztatu **Consumer Awareness as a Key Competence of a Digital Citizen** przedstawicielka UODO przedstawiła prezentację, w której omówiła działania polskiego organu nadzorczego w obszarze ochrony danych osobowych dzieci, a po jej wystąpieniu wyświetlony został film promujący program „Twoje dane – Twoja sprawa”.

W trakcie konferencji zaprezentowano Projekt **Mapy Drogowej Edukacji na rzecz Obywatelstwa Cyfrowego (2027-2031), wraz z jego celami i kluczowymi założeniami.** Mapa drogowa będzie wspierać państwa członkowskie we włączaniu edukacji na rzecz obywatelstwa cyfrowego do głównego nurtu edukacji. Uwagi i opinie przekazane przez uczestników podczas konferencji zostaną uwzględnione w ostatecznej wersji mapy drogowej, która zostanie przedłożona Komitetowi Ministrów do przyjęcia w 2026 roku.

### 8) Międzynarodowa konferencja „Axiology of the Legal System: Theory and Practice". Rzym, 25-26.11.2025 r.

Główny koordynator w UODO ds. ochrony danych w Kościołach i związkach wyznaniowych uczestniczył w międzynarodowej konferencji naukowej „Axiology of the Legal System: Theory and Practice", która 25 - 26 listopada 2025 r. odbyła się na Papieskim Uniwersytecie Gregoriańskim w Rzymie. W trakcie swojego wystąpienia przedstawiciel Prezesa UODO zaprezentował strukturę, podstawy prawne oraz cele współpracy pomiędzy Prezesem Urzędu Ochrony Danych Osobowych a Kościelnym Inspektorem Ochrony Danych (KIOD). Przedstawił także kluczowe obszary współpracy pomiędzy Prezesem Urzędu a KIOD w latach 2024 – 2025 w zakresie działań edukacyjnych, naukowych i szkoleniowych i zarysował ich praktyczny wymiar z ostatnich miesięcy (wymiana informacji ws. wyroków sądów administracyjnych i linii orzeczniczej, podział kompetencji ws. działań nadzorczych).

Konferencję zorganizował Wydział Prawa Kanonicznego Papieskiego Uniwersytetu Gregoriańskiego w Rzymie. Spotkanie, w którym wzięli udział specjaliści z zakresu prawa międzynarodowego reprezentujący ośrodki akademickie w Europie, stało się okazją do wymiany poglądów na temat aksjologicznych podstaw systemów prawnych.

### 9) Stakeholder Event on Anonymisation and Pseudonymisation, 12.12.2025 r.

Przedstawiciele UODO wzięli udział w wydarzeniu EROD poświęconym anonimizacji i pseudonimizacji, zorganizowanym w związku z wyrokiem TSUE w sprawie EROD v. SRB. Spotkanie miało na celu zebranie opinii interesariuszy oraz wsparcie prac EROD nad opracowaniem wytycznych w tym obszarze.

W trakcie wydarzenia przeprowadzono dyskusję nad implikacjami wyroku TSUE dla praktyki anonimizacji oraz dokonano wymiany doświadczeń pomiędzy przedstawicielami organów nadzorczych, środowiska akademickiego i sektora prywatnego. Omówiono również wyzwania techniczne i prawne związane z pseudonimizacją. Przeanalizowano również kierunki dalszych prac EROD w ramach programu na lata 2024–2025.

## 11. Skoordynowany nadzór nad wielkoskalowymi systemami informacyjnymi UE

Istotnym obszarem działalności Prezesa UODO w 2025 r. pozostawała współpraca międzynarodowa w ramach art. 62 rozporządzenia 2018/1725[677], 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 współpracują w ramach swoich kompetencji, w celu zapewnienia skutecznego nadzoru nad wielkoskalowymi systemami informatycznymi oraz organami i jednostkami organizacyjnymi Unii Europejskiej. Skoordynowane działania obejmują m.in. wspólne kontrole i dochodzenia oraz prace nad wspólną metodologią.

W tym celu powołano **Komitet Skoordynowanego Nadzoru (CSC),** który prowadzi działania nadzorcze w odniesieniu do:

- Systemu Informacyjnego Schengen (SIS),
- Systemu Wjazdu/Wyjazdu (EES),
- Europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS),
- Europejskiego systemu przekazywania informacji z rejestrów karnych dotyczącego osób niebędących obywatelami UE (ECRIS-TCN),
- Interoperacyjności systemów EES, ETIAS, ECRIS-TCN, EURODAC, SIS i VIS, a także
- działalności Eurojust, Prokuratury Europejskiej (EPPO), Europolu, systemu Prüm II oraz systemu wymiany informacji na rynku wewnętrznym (IMI).

Jednym z istotnych zagadnień było doprecyzowanie stosowania przepisów dotyczących cykli audytowych w wielkoskalowych systemach informatycznych UE. W tym zakresie Komitet przyjął rekomendacje dotyczące sposobu obliczania tych cykli, w szczególności w odniesieniu do maksymalnych odstępów między audytami oraz momentu ich zakończenia, jako punktu wyjścia dla planowania kolejnych działań nadzorczych. Rekomendacje te przyczyniają się do ujednolicenia praktyki stosowania prawa UE, przy jednoczesnym zachowaniu elastyczności organów nadzorczych w dostosowywaniu harmonogramów kontroli do krajowych uwarunkowań organizacyjnych i priorytetów nadzorczych.

W 2025 r. szczególne znaczenie dla prac Komitetu miało uruchomienie 12 października Systemu Wjazdu/Wyjazdu (EES), które w praktyce wiąże się z rozpoczęciem bieżącego nadzoru nad funkcjonowaniem systemu.

Prezes Urzędu uczestniczył także w posiedzeniach wyspecjalizowanych grup, w tym Grupy ds. Koordynacji Nadzoru nad Systemem Informacji Celnej (CIS),

[677] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 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. U. UE L z 2018 r. poz. 295.

służącego zapobieganiu, wykrywaniu i ściganiu naruszeń unijnego prawa celnego i rolnego oraz Grupy ds. Koordynacji Nadzoru nad systemem Eurodac, który zawiera odciski palców osób ubiegających się o ochronę międzynarodową w państwach członkowskich UE i krajach współpracujących.

Udział Prezesa Urzędu w pracach grupy ds. Eurodac został dodatkowo wzmocniony wyborem przedstawicielki UODO – Marii Jędy, Głównej Koordynatorki ds. Wielkoskalowych Systemów Informacyjnych UE – na Zastępczynię Przewodniczącej podczas 42. posiedzenia Grupy.

Ponadto przedstawicielka Prezesa Urzędu uczestniczyła 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[678]. W ramach tych ocen dokonuje się analizy sposobu wdrażania i stosowania dorobku Schengen, w szczególności w odniesieniu do systemów SIS i VIS, a także analizuje się rolę organów ochrony danych w nadzorze nad podmiotami korzystającymi z tych systemów. Mechanizm ten stanowi istotny element zapewnienia, że państwa członkowskie stosują przepisy Schengen skutecznie i zgodnie z podstawowymi zasadami ochrony danych. Za jego wdrażanie odpowiadają wspólnie państwa członkowskie i Komisja Europejska, przy wsparciu właściwych organów i jednostek organizacyjnych Unii.

**Realizacja praw osób w wielkoskalowych systemach informacyjnych UE**

Rozporządzenia Unii Europejskiej ustanawiające wielkoskalowe systemy informacyjne nakładają na państwa członkowskie obowiązek publikowania statystyk dotyczących realizacji praw osób, których dane dotyczą. W związku z tym Prezes Urzędu Ochrony Danych Osobowych uwzględnia w niniejszym sprawozdaniu dane za 2025 r. dotyczące realizacji tych praw w Systemie Informacyjnym Schengen (SIS)[679] oraz Wizowym Systemie Informacyjnym (VIS)[680]. Dane te mają charakter statystyczny i pochodzą od organów właściwych do realizacji tych praw. Prezes Urzędu Ochrony Danych Osobowych nie przedstawia danych dotyczących realizacji tych praw za jego pośrednictwem, gdyż w prawie krajowym nie przewidziano trybu realizacji tych uprawnień zgodnie z art. 17 dyrektywy (UE) 2016/680.

Prezentowane statystyki dotyczą wykonywania przez osoby, których dane dotyczą, prawa dostępu do danych, ich sprostowania oraz usunięcia danych przetwarzanych niezgodnie z prawem. W Polsce, zgodnie z ustawą o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, realizacja tych praw w krajowym komponencie Systemu

[678] Rozporządzenie Rady (UE) 2022/922 z dnia 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.

[679] Art. 19 rozporządzenia 2018/1860, art. 54 ust. 4 rozporządzenia 2018/1861 oraz art. 68 ust. 4 rozporządzenia 2018/1862

[680] Art. 4 ust. 3 zdanie trzecie Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz. U. UE L z 2008 r. poz. 218, ze zm.

Informacyjnego Schengen (SIS) oraz Wizowego Systemu Informacyjnego (VIS) należy do Komendanta Głównego Policji – centralnego organu technicznego Krajowego Systemu Informatycznego, pełniącego funkcję administratora danych przetwarzanych za jego pośrednictwem[681].

Ponadto, zgodnie z ustawą o cudzoziemcach, Szef Urzędu do Spraw Cudzoziemców rozpatruje wnioski cudzoziemców, których dane zostały umieszczone w SIS do celów odmowy wjazdu i pobytu[682].

Zakres tych wniosków obejmuje w szczególności:

- uzyskanie informacji o umieszczeniu danych w SIS,
- informacje o okresie obowiązywania wpisu oraz jego podstawie prawnej i faktycznej,
- sprostowanie danych niekompletnych, nieaktualnych lub nieprawdziwych,
- usunięcie danych przetwarzanych z naruszeniem przepisów prawa, w tym rozporządzenia (UE) 2018/1861.

Poniżej przedstawiono dane statystyczne w omawianym zakresie dotyczące polskiego komponentu SIS i VIS:

| **System Informacyjny Schengen** | | | | |
|---|---|---|---|---|
| **Zrealizowane wnioski o dostęp** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1860** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1861** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1862** | **Brak wpisu dotyczącego wnioskodawcy w Systemie Informacyjnym Schengen (SIS)** |
| Liczba złożonych do administratora wniosków o udzielenie dostępu | 43 | 666 | 82 | 656 |
| Liczba przypadków, w których udzielono dostępu do danych | 43 | 120 | 74 | 253 |
| **Zrealizowane wnioski o sprostowanie** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1860** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1861** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1862** | **Brak wpisu dotyczącego wnioskodawcy w SIS** |
| Liczba złożonych do administratora danych wniosków o sprostowanie | 0 | 13 | 0 | 12 |

[681] Art. 10 ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, Dz. U. z 2023 r. poz. 1355.
[682] Art. 444 ust. 1 ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach, Dz. U. z 2025 r. poz. 1079.

| | | | | |
|---|---|---|---|---|
| nieprawidłowych danych | | | | |
| Liczba przypadków, w których dane zostały sprostowane | 0 | 0 | 0 | 0 |
| **Zrealizowane wnioski o usunięcie danych** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1860** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1861** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1862** | **Brak wpisu dotyczącego wnioskodawcy w SIS** |
| Liczba złożonych do administratora danych wniosków o usunięcie danych przechowywanych niezgodnie z prawem | 34 | 203 | 12 | 125 |
| Liczba przypadków, w których dane zostały usunięte | 1 | 11 | 0 | 28 |
| **Zakończone sprawy sądowe** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1860** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1861** | **Wpis dotyczący osoby, której dane dotyczą, na podstawie rozporządzenia (UE) 2018/1862** | |
| Liczba wszczętych postępowań sądowych | | 20 | | |
| Liczba spraw, w których sąd orzekł na korzyść wnioskodawcy | | 0 | | |

| **Wizowy System Informacyjny** | | | | | | |
|---|---|---|---|---|---|---|
| **Rodzaj wniosku** | | **Udzielenie dostępu** | **Sprostowanie** | **Uzupełnienie** | **Usunięcie danych** | **Ograniczenie przetwarzania danych** |
| Liczba złożonych do administratora wniosków | | 73 | 0 | 0 | 1 | 0 |
| Działania podjęte w odpowiedzi na te wnioski | Brak wpisu dotyczącego wnioskodawcy | 54 | 0 | 0 | 1 | 0 |
| | Udzielono informacji o | 7 | 0 | 0 | 0 | 0 |

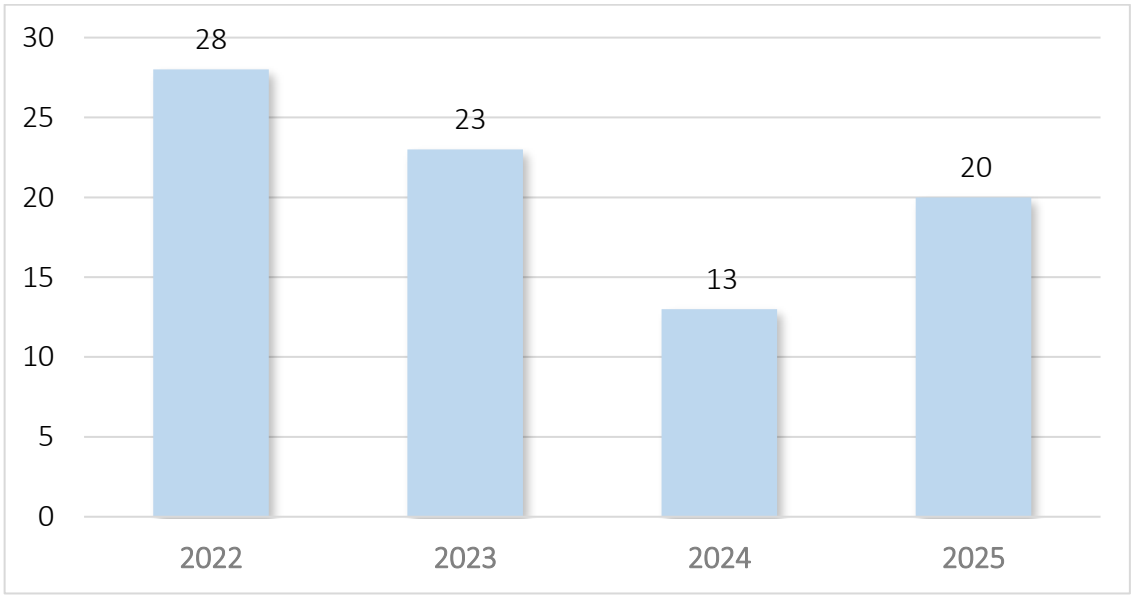
| | | | | | | |
|---|---|---|---|---|---|---|
| | zetwarzaniu danych w VIS | | | | | |
| | Wniosek nie spełniał warunków formalnych | 12 | 0 | 0 | 0 | 0 |

## 12. Wnioski prejudycjalne

W ramach 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.

Organ nadzorczy dokonuje – niezależnie od powyższego – regularnego przeglądu wszystkich postępowań inicjowanych przez TSUE pod kątem zagadnień z zakresu ochrony danych osobowych.

W 2025 r. do polskiego organu nadzorczego wpłynęło **20 wniosków prejudycjalnych skierowanych do TSUE** przez sądy z różnych państw Unii Europejskiej. Dla porównania w 2024 r. było ich 13, 2023 r. - 23, a w 2022 r. – 28.




**Wykres 24:** Liczba wniosków prejudycjalnych skierowanych do TSUE przez sądy państw UE, które wpłynęły do polskiego organu nadzorczego w latach 2022-2025.

W 2025 r. Prezes UODO dokonał analizy 19 opisanych poniżej wniosków prejudycjalnych. Warto zwrócić uwagę na sprawy: C-798/24 Jautiva, C-12/25 Bisdom Gent, C-222/25 Rahapesu Andmebüroo, C-427/25 Uffida, C-568/25 Universal Versand, C-594/25 Vodafone GmbH, C-654/25 Undelam, ponieważ mogą one wpłynąć na wykładnię przepisów prawa obowiązujących również w Polsce, kształtując sposób interpretacji kluczowych regulacji oraz standardy stosowane w praktyce krajowej.

1. **C-798/24 Jautiva** – wniosek związany był z łotewskimi przepisami odnoszącymi się do rejestru handlowego, w którym ujawniane są informacje dotyczące akcjonariuszy spółek akcyjnych – Prezes UODO uznał udział w postępowaniu za zasadny. W sprawie tej TSUE dokona oceny proporcjonalności rozwiązania, zgodnie z którym dane osobowe akcjonariuszy są powszechnie dostępne w publicznym rejestrze. Odpowiedź TSUE na pytanie sądu łotewskiego będzie miała istotne znaczenie z punktu widzenia zapewnienia gwarancji dla ochrony danych osobowych akcjonariuszy spółek[683].

2. **C-5-25 Pilev** – sprawa dotyczyła bułgarskich regulacji dotyczących ustalania tożsamości oskarżonego. Zgodnie z nimi przewodniczący składu orzekającego publicznie ustala dane osobowe oskarżonego, które następnie trafiają do protokołu i akt sprawy dostępnych stronom – w ocenie organu nadzorczego udział w postępowaniu nie był zasadny[684].

3. **C-12/25 Bisdom Gent** – pytania prejudycjalne, które zadał sąd odsyłający, powstały w związku z zaskarżoną decyzją belgijskiego organu nadzoru, który nakazał usunąć wpisy z księgi chrztów. W Polsce skorzystano z rozwiązanych przewidzianych w art. 91 RODO. Przyjęto bowiem, że w dniu wejścia w życie RODO istniały szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem ich danych przez Kościół rzymskokatolicki, zatem mogą być one nadal stosowane pod nadzorem niezależnego organu nadzorczego – został on powołany jako organ odrębny (Kościelny Inspektor Ochrony Danych)[685]. Natomiast w Belgii Kościół nie skorzystał z wyjątku, o którym mowa w art. 91 RODO. Pytania prejudycjalne belgijskiego sądu zmierzają do uzyskania odpowiedzi na pytanie o rozgraniczenie praw człowieka. Chodzi o zawarte w art. 8 Karty Praw Podstawowych Unii Europejskiej prawo do ochrony danych osobowych oraz gwarantowane w art. 10 Karty oraz art. 9 Konwencji o ochronie praw człowieka i podstawowych wolności wolność myśli, sumienia i religii[686].

4. **C-40/25 CRIF** – sprawa dotyczyła przetwarzania danych osobowych, które zostały nabyte od innego podmiotu przez biuro informacji kredytowej i kwestii

[683] DPNT.0623.2.2025.
[684] DPNT.0623.4.2025.
[685] Znalazło to potwierdzenie w licznych wyrokach NSA (por. wyrok z 25.05.2022 r., sygn. akt III OSK 2273/21; z 14.07.2022 r., sygn. akt III OSK 2776/21; z 18.11.2022 r., sygn. akt III OSK 2461/21; z 13.03.2025 r. sygn. akt III OSK 6698/21; z 28.05.2025 r., sygn. akt III OSK 985/22).
[686] DPNT.0623.5.2025.

poinformowania osoby, której dane dotyczą, o pozyskaniu danych oraz zmianie celu przetwarzania. Organ nadzorczy nie rekomendował udziału w sprawie[687].

5. **C-185/25 Waldfelber** – sprawa dotyczyła przetwarzania danych osobowych przez szkołę wyższą oraz związanego z nim pojęcia administratora i jego odpowiedzialności, a także kwestii związanych z prawem dostępu do informacji przetwarzanych przez szkołę. Organ nadzorczy nie rekomendował udziału w sprawie[688].

6. **C-205/25 Bayerisches Landesamt für Datenschutzaufsicht** – sprawa dotyczyła postępowania prowadzonego przez organ nadzorczy w Bawarii, w czasie którego doszło do naruszenia danych osobowych skarżącego. Organ zastosował środki naprawcze. Skarżący zażądał szczegółowych informacji o podjętych działaniach, lecz organ odmówił, twierdząc, że nie ma on prawa dostępu do akt i zbiorów danych organu. Organ nadzorczy nie rekomendował udziału w sprawie[689].

7. **C-214/25 Your personal driver** – sprawa dotyczyła spółki świadczącej usługi wynajmu samochodów z kierowcą na podstawie wcześniejszej rezerwacji. Prawo włoskie wymagało, aby kierowca posiadał elektroniczny formularz zawierający m.in. dane pojazdu, kierowcy, szczegóły trasy oraz dane klienta. Włoski organ nadzorczy uznał, że przepisy te mogą naruszać zasadę ograniczenia celu przetwarzania i umożliwiać śledzenie oraz identyfikację klientów. Prezes UODO nie rekomendował udziału w sprawie[690].

8. **C-222/25 Rahapesu Andmebüroo** – w tej sprawie osoba, której dane dotyczą, zwróciła się do jednostki analityki finansowej w Estonii o udostępnienie informacji, czy estońskim lub zagranicznym instytucjom kredytowym bądź zagranicznym organom przekazano dotyczące jej informacje w związku z podejrzeniem prania pieniędzy. Przepisy estońskiego prawa uniemożliwiały przekazywanie takich informacji, przez co żądanie podmiotu danych nie zostało spełnione. Skutkowało to skargą na decyzję organu do sądu administracyjnego, który zastosował środek tymczasowy, na mocy którego zobowiązał organ do przekazania posiadanych informacji. Podstawą decyzji sądu administracyjnego było to, że brak jest przepisu krajowego, który wyłączałby obowiązek przekazania danych, oraz że nie można odmówić przekazania danych, powołując się bezpośrednio na art. 23 RODO. Jednostka analityki finansowej odmówiła jednak przekazania jakichkolwiek informacji skarżącemu, wskazując, że utrzymywanie w tajemnicy wszystkich danych przekazywanych i zbieranych przez jednostkę służy do skutecznej walki z przestępczością i terroryzmem. W tym stanie faktycznym powstało pytanie co do warunków skorzystania przez osobę, której dane dotyczą,

[687] DPNT.0623.7.2025.
[688] DPNT.0623.8.2025.
[689] DPNT.0623.9.2025.
[690] DPNT.0623.10.2025.

z prawa dostępu do danych przetwarzanych przez jednostkę analityki finansowej. Organ nadzorczy rekomendował udział w postępowaniu[691].

9. **C-273/25 Erser** – sprawa dotyczyła pozyskania przez skraperów publicznie dostępnych danych użytkowników Facebooka, ich połączenia z numerami telefonów i opublikowania w internetowych bazach danych, w tym w darknecie. Poszkodowany domagał się od Facebooka odszkodowania za utratę kontroli nad danymi. Prezes UODO nie rekomendował udziału w sprawie[692]. Ostatecznie została ona wykreślona z rejestru spraw TSUE.

10. **C-317/25 Groupe Canal+** –sprawa dotyczyła spółki prowadzącej marketing elektroniczny z wykorzystaniem danych osobowych pozyskanych przez dostawców usług internetowych od ich abonentów. Zgoda na przetwarzanie danych obejmowała także „partnerów" podmiotu zbierającego dane, jednak partnerzy ci nie byli wskazani z nazwy ani w formularzu, ani pod linkiem, ani w inny sposób. Organ nadzorczy nie rekomendował udziału w sprawie[693].

11. **C-427/25 Uffida** – sprawa dotyczyła wniosku prokuratora o zgodę na pozyskanie danych telematycznych, w tym adresu IP oraz dat i godzin dostępu do profilu na Facebooku, w związku z postępowaniem o podszywanie się pod inną osobę. Sąd odmówił, uznając, że w przypadku przestępstw zagrożonych niską karą prawo krajowe nie pozwala na dostęp do takich danych. Organ nadzorczy nie rekomendował udziału w sprawie[694]. Jest ona jednak istotna ze względu na konieczność zajęcia przez TSUE stanowiska w kwestii tego, czy dostęp do danych o ruchu w sieci internetowej – w celu ustalenia tożsamości osoby fizycznej podejrzanej o podszywanie się pod inną osobę – stanowi na tyle poważną ingerencję w sferę danych osobowych, że powinien być dopuszczalny wyłącznie w odniesieniu do „poważnych przestępstw".

12. **C-458/25 Onderwijsgroep Zusters der Christelijke Scholen Zuid-Kempen vzw** – sprawa dotyczyła nałożenia przez belgijski organ ochrony danych administracyjnej kary pieniężnej na subwencjonowaną, niepubliczną instytucję oświatową. Organ uznał, że choć szkoła jest organem publicznym w świetle prawa krajowego, nie ma takiego statusu w rozumieniu przepisów unijnych, co pozwala na jej ukaranie. Organ nadzorczy nie rekomendował udziału w sprawie[695].

13. **C-416/25 Freie und Hansestadt Hamburg MC** – sprawa dotyczyła prawa dostępu do informacji zawartych w aktach postępowania sądowego w sprawie

[691] DPNT.0623.12.2025.
[692] DPNT.0623.14.2025.
[693] DPNT.0623.15.2025.
[694] DPNT.0623.20.2025.
[695] DPNT.0623.21.2025.

o wykroczenie drogowe polegające na przekroczeniu dozwolonej prędkości. Organ nadzorczy nie rekomendował udziału w sprawie[696].

14. **C- 528/25 Firmenauskunft P.U.R. GmbH** – sprawa dotyczyła tego, czy przepisy krajowe muszą zapewniać ochronę przed niezamawianymi połączeniami reklamowymi także osobom fizycznym prowadzącym działalność gospodarczą. Organ nadzorczy nie rekomendował udziału w sprawie[697].

15. **C-523/25 Stichting Data Bescherming Nederland (SDBN)** – sprawa dotyczyła fundacji działającej w imieniu osób poszkodowanych wskutek naruszenia prywatności, a zasadniczą kwestią było, czy państwo członkowskie może wprowadzać w prawie krajowym bardziej szczegółowe wymogi dotyczące dopuszczalności takich organizacji do wytaczania powództw w imieniu poszkodowanych – w ocenie organu nadzorczego udział w postępowaniu był zasadny[698].

16. **C-568/25 Universal Versand** – sprawa dotyczyła stosowania przez sprzedawcę internetowego wewnętrznego scoringu przy tzw. niepewnych metodach płatności (tj. zakupu na fakturę z odroczonym terminem płatności lub na raty). Dane do scoringu były pozyskiwane od zewnętrznego biura informacji kredytowej. Na tej podstawie sprzedawca określał prawdopodobieństwo braku płatności przez kupującego. Jeżeli wynik scoringu lub sama informacja z biura były negatywne, system sprzedawcy mógł automatycznie odmówić oferowania metody płatności na raty lub na fakturę, proponując klientowi płatność kartą płatniczą lub PayPalem. Klient miał prawo zażądać manualnej weryfikacji decyzji i jej zakwestionowania. Na tej płaszczyźnie powstał problem dotyczący tego, czy decyzja o niemożności skorzystania przez kupującego z określonej metody płatności, ale nie całkowite zamknięcie mu drogi do zawarcia umowy, „wywołuje wobec [klienta] skutki prawne” lub „w podobny sposób istotnie na niego wpływa”- w rozumieniu art. 22 ust. 1 RODO. Organ nadzorczy nie rekomendował udziału w sprawie[699].

17. **C- 594/25 Vodafone GmbH** – stan faktyczny sprawy dotyczył przekazywania przez operatora telekomunikacyjnego danych klienta do podmiotu zewnętrznego (SCHUFA), celem dokonywania oceny zdolności kredytowej klienta w związku z zawarciem, wykonaniem lub rozwiązaniem umowy. Przekazywanie tych danych odbywało się bez zgody osoby, której dane dotyczą. Jednak administrator danych uważa, że przekazanie danych pozytywnych do biur informacji kredytowej po zawarciu umowy o świadczenie usług telefonii komórkowej wynika z ochrony uzasadnionych interesów i służy w szczególności zapobieganiu oszustwom. Wspólne gromadzenie pozytywnych danych ma zasadnicze

[696] DPNT.0623.22.2025.
[697] DPNT.0623.24.2025.
[698] DPNT.0623.25.2025.
[699] DPNT.0623.27.2025.

znaczenie dla operatorów telefonii komórkowej, ponieważ zwiększa szansę na wykrycie nieuczciwych klientów przed zawarciem umowy, bowiem jedynie istnienie wspólnej bazy danych umożliwia im sprawdzenie (prawdziwej) tożsamości danej osoby i ustalenie, czy próbuje ona zawrzeć umowy o świadczenie usług telefonii komórkowej przy użyciu swojego rzeczywistego czy też fałszywego nazwiska. W tym kontekście TSUE zostało zadane pytanie prejudycjalne, czy art. 6 ust. 1 lit. f RODO uzasadnia przekazywanie pozytywnych danych przez operatorów telefonii komórkowej działającym na podstawie prawa prywatnego biurom informacji kredytowej bez zgody osób, których dane dotyczą, w każdym przypadku, gdy biura te wykorzystują przekazane dane również do tworzenia profili (scoring). Organ nadzorczy nie rekomendował udziału w sprawie[700].

18. **C- 654/25 Undelam** – postępowanie główne w sprawie dotyczyło sytuacji, w której osoby wykorzystywały urządzenia techniczne celem wyselekcjonowania operatorów stron internetowych korzystających z Google Fonts (katalogu czcionek udostępnianym przez Google operatorom stron internetowych do użytku) bez zmiany ustawień domyślnych, przez co dane odwiedzających witryny wysyłane były na serwer Google. Osoby identyfikujące takie witryny celowo je później odwiedzały i wzywały ich operatorów do zaniechana naruszenia dóbr osobistych poprzez nieuprawnione przekazywanie adresów IP do Google USA i do zapłaty określonej kwoty celem odstąpienia poszkodowanego od dochodzenia roszczeń na drodze sądowej. Sytuacja ta zrodziła konieczność doprecyzowania m.in. tego, czy takie działanie osoby, której dane dotyczą, zasługuje na ochronę na podstawie art. 82 ust. 1 RODO. Organ nadzorczy nie rekomendował udziału w sprawie[701].

19. **C- 676/25 Viva Credit** – postępowanie dotyczyło prawa dostępu do danych, a przede wszystkim kwestii: kiedy realizacja tego prawa obejmuje obowiązek udostępnienia przez administratora danych osobowych kopii umów pożyczek łączących osobę, której dane dotyczą, i administratora. Organ nadzorczy nie rekomendował udziału w sprawie[702].

**Wpływ na przepisy polskiego prawa wyroków wydanych przez TSUE/Sąd UE/EFTA**

W 2025 r. organ nadzorczy dokonał analizy wpływu na przepisy polskiego prawa 8 wyroków wydanych przez TSUE. Dodatkowo przeanalizowano 4 wyroki Sądu UE i 1 Trybunału EFTA.

[700] DPNT.0623.28.2025.
[701] DPNT.0623.30.2025.
[702] DPNT.0623.33.2025.

1. **C-416/23 Österreichische Datenschutzbehörde** – w wyroku z 9 stycznia 2025 r. Trybunał Sprawiedliwości, odpowiadając na pytanie austriackiego trybunału administracyjnego, uznał, że zawarte w art. 57 ust. 4 RODO pojęcie „żądania" obejmuje skargi, o których mowa w art. 57 ust. 1 lit. f i art. 77 ust. 1 RODO. Ponadto Trybunał wskazał, że żądań nie można uznać za „nadmierne" w rozumieniu art. 57 ust. 4 tego rozporządzenia wyłącznie ze względu na ich liczbę w określonym okresie, ponieważ skorzystanie z możliwości przewidzianej w tym przepisie jest uzależnione od wykazania przez organ nadzorczy istnienia zamiaru nadużycia po stronie osoby, która wniosła te żądania. W przypadku zaś gdy organ nadzorczy ma do czynienia z nadmiernymi żądaniami, może on w drodze uzasadnionej decyzji wybrać między pobraniem opłaty w rozsądnej wysokości wynikającej z kosztów administracyjnych a odmową podjęcia takich żądanych działań, uwzględniwszy wszystkie istotne okoliczności i upewniwszy się, że dokonany wybór ma odpowiedni, niezbędny i proporcjonalny charakter. W ocenie Prezesa UODO wyrok ten ma istotne znaczenie przy wykładni art. 57 ust. 4 RODO, nie wymaga zaś zmiany obowiązującego w Polsce prawa[703].

2. **C-394/23 Mousse** – w wyroku z 9 stycznia 2025 r. TSUE orzekł, że przetwarzanie danych osobowych dotyczących form grzecznościowych odnoszących się do klientów przedsiębiorstwa przewozowego, mające na celu personalizację komunikacji handlowej w oparciu o tożsamość płciową, nie wydaje się ani obiektywnie konieczne, ani istotne dla prawidłowego wykonania umowy, w związku z czym nie można go uznać za niezbędne do jej realizacji. Tych danych nie można również uznać za niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora danych lub przez stronę trzecią, jeżeli: o realizowanym prawnie uzasadnionym interesie nie poinformowano owych klientów w momencie zbierania tych danych lub, rzeczonego przetwarzania nie dokonano w granicach tego, co jest ściśle niezbędne do realizacji owego prawnie uzasadnionego interesu, a także gdy w świetle wszystkich istotnych okoliczności prawa podstawowe i wolności wspomnianych klientów mogą mieć nadrzędny charakter wobec rzeczonego prawnie uzasadnionego interesu, między innymi z uwagi na ryzyko dyskryminacji ze względu na tożsamość płciową. W ocenie Prezesa UODO wyrok nie będzie powodował konieczności dokonania zmiany w przepisach prawa polskiego[704]

3. Połączone sprawy **T-70/23, T-84/23 i T-111/23 Data Protection Commission przeciwko Europejskiej Radzie Ochrony Danych** – wyrok sądu UE, który zapadł 29 stycznia 2025 r., dotyczył decyzji EROD w sprawach odnoszących się do przetwarzania danych osobowych przez podmioty prowadzące aplikacje i portale społecznościowe, takie jak Facebook i WhatsApp. Prezes UODO nie dostrzegł zasadności złożenia odwołania od wyroku[705].

[703] DOL.0623.26.2023.
[704] DOL.0623.24.2023.
[705] DPNT.023.3.2025.

4. **C- 383/23 ILVA A/S** – w wyroku z 13 lutego 2025 r. TSUE ocenił, czy art. 83 ust. 4-6 RODO należy interpretować w ten sposób, że przy nakładaniu grzywny na przedsiębiorstwo pod uwagę należy brać całkowity roczny światowy obrót grupy przedsiębiorstw, do której należy to przedsiębiorstwo, czy też jedynie całkowity roczny światowy obrót samego tego przedsiębiorstwa. Co do sposobu obliczania wysokości kary administracyjnej na podstawie powołanych przepisów Trybunał podniósł, że określenie maksymalnej kwoty administracyjnej kary pieniężnej należy odróżnić od samego sposobu obliczenia kwoty kary pieniężnej nakładanej przez organ nadzorczy za konkretne naruszenie rozporządzenia 2016/679. Ustalenie wysokości kary administracyjnej jest zależne także od wielu innych czynników, które organ nadzorczy powinien uwzględnić, takich jak np. charakter, waga i czas trwania naruszenia, liczba poszkodowanych osób, których dane dotyczą, rozmiar poniesionych przez nie szkód, umyślność bądź nieumyślność naruszenia itd. Tylko uwzględnienie istotnych okoliczności indywidualnych dotyczących konkretnego naruszenia przepisów RODO, przy jednoczesnym uwzględnieniu zdolności ekonomicznej podmiotu naruszającego przepisy, może zapewnić trzy funkcje kary: jej skuteczność, proporcjonalność i walor odstraszający. Przy ocenie tych warunków należy zaś wziąć pod uwagę, czy adresat ten stanowi część przedsiębiorstwa w rozumieniu art. 101 i 102 TFUE. Natomiast w przypadku nałożenia kary pieniężnej za naruszenie rozporządzenia 2016/679 na administratora danych osobowych, który jest przedsiębiorstwem lub jego częścią, maksymalna kwota kary pieniężnej zostaje określona na podstawie odsetka całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego tego przedsiębiorstwa. W ocenie Prezesa UODO wyrok TSUE nie powoduje konieczności zmiany obowiązujących przepisów prawa, ale ma znaczenie dla wykładni art. 83 ust. 4-6 RODO[706].

5. **C-247/23 Deldits** – w wyroku z 13 marca 2025 r. TSUE wskazał na dwie istotne kwestie. Po pierwsze, prawo osoby, której dane dotyczą, do uaktualniania przetwarzanych informacji stanowi istotny element ochrony tej osoby w obszarze przetwarzania danych osobowych i obejmuje także dane dotyczące tożsamości płciowej. Po drugie, państwo członkowskie nie może powoływać się na szczególne przepisy krajowe przyjęte na podstawie art. 6 ust. 2 i 3 RODO w celu ograniczenia prawa do sprostowania danych zagwarantowanego w art. 8 ust. 2 Karty praw podstawowych Unii Europejskiej. Przepisy szczególne, o których mowa powyżej, mają jedynie na celu doprecyzowanie stosowania przepisów zawartych w rozporządzeniu 2016/679, a nie odstąpienie od nich. Prawo do sprostowania danych określone w art. 16 RODO może zostać ograniczone jedynie po spełnieniu warunków wskazanych w art. 23 tego rozporządzenia. Ponadto TSUE zwrócił uwagę na to, że państwo członkowskie nie może powoływać się na brak w prawie krajowym procedury prawnego uznania

[706] DOL.0623.25.2023.

tożsamości transpłciowej jako na powód odmowy realizacji prawa do sprostowania. W tym względzie TSUE zaznaczył, że o ile prawo Unii nie narusza kompetencji państw członkowskich w dziedzinie stanu cywilnego osób i prawnego uznawania ich tożsamości płciowej, o tyle przy wykonywaniu tej kompetencji państwa te powinny przestrzegać prawa Unii. Co istotne, Trybunał podkreślił, że art. 16 RODO nie precyzuje w żadnym stopniu, jakich dowodów może wymagać administrator w celu wykazania, że przetwarzane dane osobowe są nieprawidłowe. Wskazał, że dotychczasowe orzecznictwo potwierdza możliwość zobowiązania podmiotu danych, który żąda ich sprostowania, do przedstawienia istotnych i wystarczających dowodów, racjonalnie wymaganych do wykazania nieprawidłowości określonych informacji. W tym kontekście TSUE orzekł, że w przypadku wykonywania prawa do sprostowania danych osobowych dotyczących tożsamości płciowej osoby fizycznej zawartych w rejestrze publicznym, podmiot danych może być zobowiązany do przedstawienia takich dowodów, które w rozsądny sposób można od niego wymagać, aby wykazać nieprawidłowość tych danych. W ocenie Prezesa UODO wyrok TSUE wywołuje potrzebę zmiany obowiązujących przepisów prawa. Będzie miał także wpływ na wykładnię art. 16 RODO[707]. W związku z tym wyrokiem TSUE Prezes UODO skierował wystąpienie legislacyjne do Ministry ds. Równości[708].

6. **T-183/23** – Sąd UE w wyroku z dnia z dnia 16 lipca 2025 r. stwierdził nieważność decyzji EROD z 7 lutego 2023 r. w zakresie odmowy udzielenia skarżącej dostępu do akt przygotowujących przyjęcie wiążącej decyzji dotyczącej Meta Platforms Ireland Ltd. Skarżąca spółka domagała się wglądu do akt i prawa do bycia wysłuchaną, a EROD twierdziła, że jej decyzja nie wpływa na sytuację spółki. Sąd stwierdził, że prawo dostępu do akt nie zależy od potencjalnego negatywnego wpływu na wnioskodawcę i jest niezależne od prawa do bycia wysłuchanym. Prezes UODO nie rekomendował odwołania się od wyroku sądu[709].

7. **T-553/23** – wyrok z dnia 3 września 2025 r. dotyczył oddalenia skargi o stwierdzenie nieważności decyzji wykonawczej Komisji w sprawie tzw. EU–US Data Privacy Framework (DPF)[710]. Prezes UODO rekomendował złożenie odwołania z uwagi na błędną interpretację standardu ochrony danych wymaganego przez prawo Unii Europejskiej w odniesieniu do transferu danych do Stanów Zjednoczonych. Sąd zaniżył poprzeczkę w kwestii dopuszczalnej ingerencji w prawo do prywatności, akceptując rozwiązania nie w pełni

[707] DOL.0623.17.2023.
[708] DPNT.413.20.2025; szersze omówienie tego wystąpienia zamieszczone zostało w części poświęconej wystąpieniom Prezesa UODO.
[709] DPNT.0623.16.2025.
[710] Decyzja wykonawcza komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA (notyfikowana jako dokument nr C(2023) 4745), Dz. Urz. UE L 231/118.

spełniające wymogi art. 7 i 8 Karty praw podstawowych Unii Europejskiej, a także przyznał nadmierny kredyt zaufania mechanizmom odwoławczym, które nie odpowiadają standardom art. 47 Karty. Ponadto orzeczenie ignoruje istotną część dorobku orzeczniczego ETPC i TSUE, a także rekomendacje wyspecjalizowanych organów, co rodzi ryzyko utrwalenia w obrocie prawnym rozwiązań sprzecznych z zasadą *essential equivalence* (tj. równoważności ochrony wymaganej przez RODO przy przekazywaniu danych do państw trzecich)[711].

8. **C- 655/23 Quirin Privatbank AG** – w wyroku TSUE z 4 września 2025 r. wskazano, że rozporządzenie 2016/679 nie zawiera przepisów, które w sposób wyraźny lub dorozumiany zapewniałyby osobie, której dane dotyczą, prawo do uzyskania w postępowaniu sądowym nakazu zobowiązującego administratora danych do zaniechania w przyszłości podobnych naruszeń przepisów rozporządzenia, tj. prewencyjnego środka ochrony prawnej. Jednak pomimo braku zawarcia w art. 82 ust. 1 RODO takiej „klauzuli upoważniającej", celem ustawodawcy unijnego nie było ograniczenie prawodawstw krajowych, które przewidują powództwo o zaniechanie niezgodnego z prawem przetwarzania danych osobowych w przyszłości. Celem rozporządzenia 2016/679 jest bowiem zapewnienie jak najwyższego stopnia ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Trybunał orzekł również, że pojęcie „szkody niemajątkowej" użyte w art. 82 ust. 1 RODO obejmuje również szeroko rozumiane „negatywne odczucia osoby", która utraciła kontrolę nad swoimi danymi i obawia się konsekwencji tego zdarzenia. TSUE podkreślił jednak, nawiązując do swojego dorobku orzeczniczego, że samo naruszenie rozporządzenia 2016/679 nie wystarcza do przyznania prawa do odszkodowania na podstawie jego art. 82 ust. 1. Poszkodowany zobligowany jest do udowodnienia nie tylko, że doszło do naruszenia RODO, ale również, że wyrządziło ono szkodę i istnieje związek przyczynowo - skutkowy pomiędzy tym zdarzeniem a doznaną szkodą. Ponadto TSUE stwierdził w wyroku, że stopień winy administratora nie ma wpływu na ustalenie wysokości odszkodowania za wyrządzenie szkody niemajątkowej na podstawie art. 82 ust. 1 RODO. W ocenie Prezesa UODO wyrok TSUE nie powoduje konieczności zmiany obowiązujących przepisów prawa, będzie miał jednak wpływ na wykładnię przepisu art. 82 ust. 1 RODO, zwłaszcza co do rozumienia pojęcia szkody i zasad odpowiedzialności administratora[712].

9. **C-654/23 Inteligo Media SA** – wyrokiem z 13 listopada 2025 r. Trybunał dokonał interpretacji art. 13 ust. 1 i 2 dyrektywy 2002/58/WE (o prywatności i łączności elektronicznej) dotyczącego zasad przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej w zakresie

[711] DPNT.0623.23.2025.
[712] DOL.0623.31.2023.

prowadzenia marketingu bezpośredniego. Trybunał uznał, że powołane przepisy należy interpretować w ten sposób, że wydawca publikacji internetowej otrzymuje adres poczty elektronicznej użytkownika „w kontekście sprzedaży produktu lub usługi" w rozumieniu tego artykułu. Trybunał odniósł się do sytuacji, w której „użytkownik tworzy nieodpłatnie na platformie internetowej tego wydawcy konto uprawniające go do uzyskania bezpłatnego dostępu do pewnej liczby artykułów związanych z tą publikacją i do otrzymywania nieodpłatnie za pośrednictwem poczty elektronicznej codziennego biuletynu informacyjnego zawierającego streszczenie zmian legislacyjnych omówionych w artykułach zawartych w publikacji, w tym linki do tych artykułów, a także do uzyskania odpłatnie dostępu do dodatkowych artykułów i analiz zawartych w rzeczonej publikacji". Trybunał uznał, że „przekazywanie takiego biuletynu informacyjnego stanowi wykorzystanie poczty elektronicznej „na potrzeby marketingu bezpośredniego" w odniesieniu do „podobnych produktów lub usług" w rozumieniu tego przepisu". Ponadto Trybunał odniósł się do wzajemnych relacji zachodzących pomiędzy art. 13 ust. 2 dyrektywy a art. 95 rozporządzenia 2016/679. Trybunał orzekł, że „w przypadku, gdy administrator danych osobowych wykorzystuje adres poczty elektronicznej użytkownika w celu wysłania mu niezamówionego komunikatu zgodnie z tym art. 13 ust. 2 dyrektywy, warunki zgodności przetwarzania z prawem przewidziane w art. 6 ust. 1 tego rozporządzenia nie mają zastosowania". Trybunał wskazał na art. 95 i motyw 173 rozporządzenia 2016/679, podkreślając, że RODO „nie nakłada na osoby fizyczne ani prawne dodatkowych obowiązków co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają określonym w dyrektywie 2002/58 szczegółowym obowiązkom mającym ten sam cel". W ocenie Trybunału „w art. 13 ust. 2 dyrektywy 2002/58 uregulowano kompleksowo zarówno warunki i cele przetwarzania danych, jak i prawa osoby, której te dane dotyczą, a także nałożono na administratora tych danych „szczegółowe obowiązki" w rozumieniu art. 95 RODO. W konsekwencji zgodność z prawem przetwarzania danych osobowych dokonywanego w ramach komunikatu objętego zakresem stosowania tego art. 13 ust. 2 można ustalić na podstawie tego przepisu, bez konieczności dokonywania jej oceny w świetle warunków przewidzianych w art. 6 ust. 1 lit. a)–f) RODO". W ocenie Prezesa UODO wyrok ma istotny wpływ na wykładnię przepisów krajowych i może prowadzić do zmiany praktyki stosowania prawa[713].

10. **C-492/23 Russmedia** – w wyroku z 2 grudnia 2025 r. Trybunał uznał, że operator internetowej platformy handlowej, jako administrator (w rozumieniu art. 4 pkt 7 RODO) danych osobowych zawartych w ogłoszeniach publikowanych na jego stronie, stosownie do treści art. 5 ust. 2, art. 24-26 RODO, ma obowiązek – przed opublikowaniem ogłoszeń, za pomocą odpowiednich środków

[713] DOL.0623.32.2023.

technicznych i organizacyjnych – zidentyfikować ogłoszenia zawierające dane wrażliwe w rozumieniu art. 9 ust. 1 wspomnianego rozporządzenia, dokonać weryfikacji, czy użytkownik będący reklamodawcą, zamierzający zamieścić takie ogłoszenie, jest osobą, której dane wrażliwe znajdują się w tym ogłoszeniu, a jeśli tak nie jest, odmówić opublikowania tego ogłoszenia, chyba że ów użytkownik będący reklamodawcą może wykazać, że osoba, której dane dotyczą, wyraziła wyraźną zgodę na opublikowanie rozpatrywanych danych na tej internetowej platformie handlowej, zgodnie z art. 9 ust. 2 lit. a, lub że zachodzi jeden z pozostałych wyjątków przewidzianych we wspomnianym art. 9 ust. 2 lit. b–j. Trybunał, mając na uwadze okoliczność, że kłamliwa i krzywdząca reklama będąca przedmiotem postępowania głównego została powielona w innych witrynach internetowych o treściach reklamowych, które opublikowały ją ze wskazaniem źródła, orzekł, że operator internetowej platformy handlowej, jako administrator ma obowiązek – w myśl art. 32 RODO – stosować odpowiednie zabezpieczenia techniczne i organizacyjne, aby uniemożliwić kopiowanie i niezgodne z prawem publikowanie w innych witrynach internetowych opublikowanych na tej platformie ogłoszeń zawierających dane wrażliwe. Trybunał odniósł się do relacji przepisów dyrektywy 2000/31 z rygorami RODO – dotyczących odpowiedzialności usługodawców będących pośrednikami – uznając, że art. 1 ust. 5 lit. b dyrektywy 2000/31/WE oraz art. 2 ust. 4 RODO należy interpretować w ten sposób, że operator internetowej platformy handlowej, jako administrator zawartych w ogłoszeniach publikowanych na jego internetowej platformie handlowej danych osobowych, nie może powoływać się w odniesieniu do naruszenia obowiązków wynikających z art. 5 ust. 2 oraz art. 24–26 i 32 tego rozporządzenia na art. 12–15 dyrektywy 2000/31 dotyczące odpowiedzialności usługodawców będących pośrednikami. W ocenie Prezesa UODO analizowany wyrok ma istotne znaczenie dla oceny odpowiedzialności serwisów internetowych, w tym mediów społecznościowych za treści publikowane na platformach internetowych. Ponadto wyrok determinuje konieczność podjęcia działań legislacyjnych w zakresie regulacji zapewniających ochronę przed treściami nieprawdziwymi, tzw. deepfake'ami[714].

11. Połączone sprawy **T-318/24 i T-362/24** – sprawa dotyczyła dostępu do danych kandydata do pracy w instytucjach unijnych. Sąd UE 3 grudnia 2025 r. stwierdził, że decyzja odmawiająca kandydatowi informacji, kto konkretnie zapoznał się z jego danymi oraz usunięcie jego danych po upływie wskazanego wcześniej terminu była prawidłowa. Nie rekomendowaliśmy odwołania się od wyroku Sądu[715].

[714] DOL.0623.28.2023.
[715] DPNT.0623.32.2025.

12. **E-5/25 Silbernagl** – sprawa dotyczyła ochrony przed zwolnieniem, jaką przyznają inspektorom ochrony danych przepisy RODO oraz wewnętrzne uregulowania litewskie.

16 grudnia 2025 r. Trybunał EFTA wydał wyrok dotyczący interpretacji art. 38 ust. 3 zdanie drugie RODO w kontekście ochrony inspektorów ochrony danych (IOD) przed odwołaniem i karaniem w związku z wykonywaniem ich zadań. Trybunał zauważył, że rozporządzenie nie definiuje pojęć takich jak „zwolniony (odwołany)", „ukarany" ani „za wykonanie zadania" i nie określa skutków prawnych naruszenia tego przepisu. Podkreślono, że państwa EOG mogą wprowadzać bardziej ochronne przepisy dotyczące odwołania IOD, o ile są zgodne z prawem EOG i RODO, przy czym ochrona ta nie może utrudniać osiągnięcia celów rozporządzenia. Trybunał orzekł, że przepisy krajowe mogą zarówno umożliwiać rozwiązanie umowy o pracę z IOD bez uzasadnionego powodu – jeśli nie wynika to z wykonywania zadań IOD – jak i wymagać uzasadnionej przyczyny do rozwiązania umowy, o ile nie zagraża to celom rozporządzenia. Stwierdzono również, że pojęcie „zwolniony" obejmuje rozwiązanie umowy o pracę, a sądy krajowe powinny interpretować prawo krajowe w sposób umożliwiający zniesienie bezprawnych skutków naruszenia przepisu, pozostawiając państwom EOG określenie konkretnych skutków prawnych w ich porządkach prawnych. W opinii Prezesa UODO wyrok ten wraz z wcześniejszymi orzeczeniami TSUE wskazuje, że polskie prawo wymaga doprecyzowania przepisów chroniących IOD przed odwołaniem za wykonywanie zadań, w tym określenia skutków naruszenia zakazu odwołania. Prezes UODO rekomenduje wprowadzenie takich regulacji do ustawy o ochronie danych osobowych z 2018 r., aby objęły one IOD zatrudnionych zarówno na podstawie umowy o pracę, jak i umów o świadczenie usług, w tym inspektorów działających w kontekście zapobiegania i zwalczania przestępczości. Wyrok Trybunału EFTA powinien skłonić polskiego ustawodawcę do wdrożenia skutecznych środków ochrony IOD[716].

13. **C-65/23 K GmbH** – w wyroku TSUE z 19 grudnia 2024 r. zostało wskazane, że w sytuacji, gdy państwa członkowskie korzystają z przyznanego im w art. 88 RODO uprawnienia do wprowadzenia bardziej szczegółowych przepisów dotyczących przetwarzania danych osobowych pracowników, powinny to robić w taki sposób, aby nie naruszać treści ani celów RODO, w tym tego, jakim jest zagwarantowanie wysokiego poziomu ochrony praw i wolności osób, których dotyczy takie przetwarzanie. W związku z tym przepisy przyjęte przez państwo członkowskie na podstawie art. 88 RODO powinny uwzględniać aspekt ochrony praw i wolności pracowników w odniesieniu do przetwarzania ich danych osobowych przez pracodawców. Ponadto w omawianym wyroku TSUE uznał, że niezależnie od zakresu uznania, jaki art. 88 RODO pozostawia stronom porozumienia zbiorowego, jako źródła prawa pracy, możliwość sprawowania kontroli sądowej względem takiego porozumienia, podobnie jak kontroli

[716] DPNT.0623.13.2025.

odnoszącej się do normy prawa krajowego przyjętej na podstawie tego przepisu, powinna dotyczyć przestrzegania wszystkich warunków i ograniczeń określonych w przepisach RODO w odniesieniu do przetwarzania danych osobowych, bez żadnego ograniczenia tej kontroli. Zgodnie z zasadą pierwszeństwa prawa Unii, jeżeli sąd krajowy dojdzie do wniosku, że przepisy krajowe, na podstawie których rozpatruje sprawę, nie spełniają warunków i ograniczeń wynikających z rozporządzenia, powinien odstąpić od stosowania tych przepisów. W konsekwencji, wobec braku bardziej szczegółowych przepisów spełniających wymagania art. 88 RODO, przetwarzanie danych osobowych w związku z zatrudnieniem jest bezpośrednio regulowane tym rozporządzeniem. Trybunał wskazał też, że to sąd krajowy rozpatrujący konkretną sprawę jako jedyny jest właściwy do dokonania wykładni prawa krajowego oraz weryfikacji, czy przepisy prawa krajowego spełniają warunki i ograniczenia określone w szczególności w powołanym przepisie. Biorąc pod uwagę, że polskie prawo pracy charakteryzuje się hierarchicznością aktów, to porozumienia zbiorowe nie mogą stać w sprzeczności z aktami prawa pracy rzędu wyższego, a przepisy porozumień zbiorowych oraz regulaminów i statutów nie mogą być mniej korzystne dla pracowników niż przepisy Kodeksu pracy oraz innych ustaw i aktów wykonawczych. Przepisy polskiego prawa pracy nie przewidują ograniczeń kontroli sądowej co do zgodności treści porozumienia zbiorowego z obowiązującymi przepisami prawa, w tym w zakresie postanowień objętych również regulacją rozporządzenia 2016/679. W świetle powyższego, w ocenie Prezesa UODO wyrok TSUE nie powoduje konieczności zmiany obowiązujących przepisów prawa, ale ma znaczenie dla wykładni art. 88 RODO oraz przepisów prawa pracy[717].

## 13. Ochrona danych osobowych przed sądami cywilnymi

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 dnia 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).

[717] DOL.0623.8.2023

Uprawnienie osoby, której dane dotyczą, o którym mowa w art. 79 i 82 RODO powiązane jest z konkretnymi obowiązkami i uprawnieniami Prezesa UODO oraz sądów powszechnych. Zasadniczą kwestią dla właściwej ich realizacji jest wymiana informacji między sądami a Prezesem UODO w oparciu o zasady określone w art. 94 ustawy z 10 maja 2018 r. o ochronie danych osobowych. Konsekwencją informacji przekazanej przez sąd o wniesieniu pozwu oraz o prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 lub art. 82 RODO jest obowiązek poinformowania sądu przez Prezesa UODO o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona, a także obowiązek niezwłocznego poinformowania sądu przez Prezesa Urzędu o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia. Rzetelna realizacja tego obowiązku przez sądy i Prezesa UODO jest niezwykle istotna, bowiem może wpłynąć na dalszy przebieg postępowania sądowego i skorzystanie przez Prezesa Urzędu z uprawnień wynikających dla niego z art. 98 i 99 ustawy z 10 maja 2018 r. o ochronie danych osobowych. I tak, mając na uwadze treść pierwszego z przywołanych w poprzednim zdaniu przepisów, Prezes Urzędu może inicjować postępowania sądowe w sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, które mogą być dochodzone wyłącznie w postępowaniu przed sądem, albo wstępować do postępowań w każdym ich stadium – w obydwu sytuacjach wymagana jest zgoda powoda, a do Prezesa Urzędu będą miały zastosowanie odpowiednio przepisy ustawy z 17 listopada 1964 r. Kodeks postępowania cywilnego[718] o prokuratorze. Drugim istotnym uprawnieniem Prezesa Urzędu, o którym mowa w art. 99 ww. ustawy, jest możliwość przedstawiania sądowi istotnego dla sprawy poglądu w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych jeżeli uzna on, że przemawia za tym interes publiczny.

Natomiast obowiązki sądów, które muszą zostać podjęte na skutek informacji przekazanej przez Prezesa UODO określone zostały w art. 95, 96 i 97 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Jak wynika z doświadczeń Prezesa Urzędu, realizacja obowiązku informacyjnego wynikającego z art. 94 ustawy o ochronie danych osobowych jest nadal źródłem wielu wątpliwości i to zarówno ze strony Prezesa Urzędu, jak i sądów powszechnych. Podstawową kwestią, wymagającą rozstrzygnięcia jest zakres przekazywanych przez sądy informacji, który nie jest często wystarczający dla identyfikacji w UODO spraw dotyczących tego samego naruszenia przepisów o ochronie danych osobowych, a które toczą się przed Prezesem Urzędu lub sądem administracyjnym albo zostały zakończone. Przyczyną takiego stanu rzeczy jest bardzo ogólna treść art. 94 ust. 1 ustawy o ochronie danych osobowych, z której nie wynika, jakie konkretnie informacje sąd ma obowiązek przekazywać do Prezesa

[718] Dz.U. z 2024 r. poz. 1568 ze zm.

Urzędu. Rozstrzygnięcia również wymaga, czy na podstawie tego przepisu sądy mogą przesyłać do Prezesa Urzędu np. zanonimizowane kopie pozwów.

Dlatego w 2025 roku Prezes Urzędu, kontynuując prowadzoną od 2022 r. korespondencję z Prezesami Sądów Apelacyjnych na temat sposobu, zakresu treści oraz znaczenia realizacji przez sądy powszechne obowiązków, o których mowa w art. 94 ust. 1 ustawy z 10 maja 2018 r. o ochronie danych osobowych[719], zaproponował sądom trzy możliwości w zakresie informowania Prezesa UODO i poprosił sądy o ocenę tych rozwiązań. Do dyskusji został również zaproszony Minister Sprawiedliwości.

Pierwszy wariant przedstawiony przez Prezesa Urzędu zakładał przekazywanie informacji przez sądy z wykorzystaniem formularzy, które zostały opracowane w UODO, z uwzględnieniem wniosków z dotychczasowej korespondencji prowadzonej z sądami apelacyjnymi. Druga możliwość zaproponowana przez Prezesa Urzędu to również wzory formularzy dla sądów, ale rozbudowane o kilkanaście pytań zamkniętych, przewidujące również ewentualną możliwość dopisania alternatywnej odpowiedzi przez sędziego. Trzecią propozycją, którą przedstawił Prezes Urzędu, to możliwość przesyłania przez sądy kopii zanonimizowanych pozwów, zawierających wszystkie informacje potrzebne zarówno dla realizacji obowiązku informowania przez Prezesa Urzędu o toczącym się bądź zakończonym postępowaniu, jak również skorzystania przez niego z uprawnień przewidzianych w art. 98, czy 99 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Dodatkową opcją, którą Prezes Urzędu zaproponował sądom do oceny, było połączenie wskazanych propozycji, tj. przekazywanie skrótowego opisu sprawy i dołączanie do niego kopii pozwu. Należy wskazać, że wszyscy Prezesi Sądów Apelacyjnych przedstawili stanowiska odnośnie do inicjatywy zaproponowanej przez organ nadzorczy, a treść przesłanych uwag wskazuje, że została ona pozytywnie odebrana. Należy przy tym podkreślić, że zdecydowana większość apelacji wyraziła przychylną opinię co do możliwości wykorzystywania w komunikacji, o której mowa w art. 94 ust. 1 ustawy o ochronie danych osobowych, przygotowanych w UODO formularzy (czyli pierwszego wariantu z tych zaproponowanych przez Prezesa Urzędu). Dodatkowo niektórzy z Prezesów Sądów Apelacyjnych wskazali, że w uzasadnionych okolicznościach (np. gdy informacje zawarte w przesłanych przez sądy formularzach okażą się niewystarczające), sądy mogłyby również przekazywać zanonimizowane kopie pozwów lub prawomocnych orzeczeń kończących postępowania z uzasadnieniem.

Swoje stanowisko w sprawie przedstawił również Minister Sprawiedliwości, który opowiedział się co do zasady za jednolitą praktyką realizacji przez sądy nałożonych na nie obowiązków, zaznaczył jednak, że ze względu na treść art. 94 ust. 1 ustawy o ochronie danych osobowych, sposób ich realizacji będzie zależał tylko od sądów. W piśmie skierowanym do Prezesa UODO podkreślił, że informacje przekazywane przez sądy powinny być na tyle wystarczające by pozwoliły dokonać Prezesowi Urzędu analizy w zakresie tożsamości spraw, a więc tożsamości stron, żądania pozwu i podstaw roszczenia (naruszenia przepisów o ochronie danych osobowych).

[719] DOL.413.12.2021.

Informacje określające stan faktyczny, rodzaj i sposób naruszenia pozwolą Prezesowi Urzędu na ustalenie czy zachodzi tożsamość postępowań. Minister Sprawiedliwości wskazał także, że nie widzi uzasadnienia prawnego do przesyłania przez sądy odpisów pozwów, orzeczeń kończących postępowania, treści uzasadnienia, bądź podawania adresów stron, gdyż nie wynika to wprost z przepisów prawa. Jeśli chodzi o zaproponowane przez Prezesa Urzędu wzory formularzy, Minister Sprawiedliwości pozostawił ich stosowanie do decyzji sądów.

Ostateczne wzory formularzy, zmienione nieco na podstawie uwag zgłoszonych przez sądy, zostały przesłane przez Prezesa UODO do sądów z zastrzeżeniem, że mogą one stanowić pomocne narzędzie, wspierające realizację przez sądy obowiązków wynikających z art. 94 ust. 1 ustawy o ochronie danych osobowych, a ze względu na niezależność sądów – do decyzji sądów pozostawiona zostaje możliwość ich wykorzystywania. Wzory tych formularzy są dostępne na stronie internetowej UODO[720].

W 2025 r. do Prezesa Urzędu wpłynęło **71 zawiadomień z sądów**, na podstawie art. 94 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych o toczących się postępowaniach i o postępowaniach, w których zapadły prawomocne orzeczenia. Sądy w większości przypadków, informując o wszczętych postępowaniach, powołują ogólne przepisy RODO lub Kodeksu cywilnego (K.c.) wskazywane przez strony (art. 82 RODO, art. 24 K.c.), co na tym etapie związane jest jeszcze z nieustalonym stanem faktycznym i prawnym.

W zakresie uprawnień Prezesa Urzędu, wynikających z art. 98 ust. 2 ustawy ochronie danych osobowych, organ nadzorczy analizuje możliwość przedstawienia istotnego poglądu albo wzięcia udziału w postępowaniach sądowych.

W 2025 r. organ nadzorczy przeprowadził taką analizę w odniesieniu do **8 spraw**[721], w których albo skarżący zwrócili się z prośbą o wstąpienie Prezesa Urzędu do postępowania, bądź też Prezes Urzędu zwracał się do stron z wnioskiem o wyrażenie zgody na jego wstąpienie. Są to postępowania już zainicjowane przez same strony, które zwracają się do Prezesa UODO z wnioskiem o przystąpienie do toczącego się postępowania i wzmocnienie przedstawionych przez nich argumentów prawnych. Są to zwykle sprawy pojedynczych osób, występujących z cywilnymi żądaniami odszkodowania czy zadośćuczynienia. W jednej z takich spraw Prezes Urzędu informował Sąd Apelacyjny o wydanej przez siebie nieprawomocnej decyzji nakładającej na administratora określoną karę pieniężną, czekając na podjęcie przez sąd właściwych decyzji procesowych.

**Seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO.”**

[720] https://uodo.gov.pl/pl/138/3937.
[721] DOL.552.1.2024; DPNT.550.29.2025; DPNT.550.68.2025; DPNT.550.71.2025; DPNT.550.5.2025; DOL.054.5.2024; DPNT.550.69.2025; DPNT.550.1.2025.

W celu wymiany poglądów i doświadczeń na temat uprawnień i obowiązków organu nadzorczego i sądów określonych w rozdziale 10 ustawy o ochronie danych osobowych, zorganizowane zostało przez Prezesa UODO, Naczelną Radą Adwokacką oraz Stowarzyszeniem Sędziów Polskich „Iustitia", seminarium (6.11.2025 r.) pt. „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO"[722].

Przedstawiciele świata prawa, nauki i praktyki podzielili się swoimi obserwacjami i propozycjami rozwiązań, odpowiadającymi na wyzwania związane z dynamicznym rozwojem orzecznictwa w obszarze ochrony danych osobowych, a także zabrać głos w dyskusji dotyczącej doniosłej roli sądów i Prezesa UODO w kształtowaniu jednolitego, spójnego z RODO orzecznictwa. Wystąpienia prelegentów potwierdziły wątpliwości m.in. w zakresie: sposobu właściwej wymiany informacji pomiędzy sądami powszechnymi a Prezesem Urzędu, pozycji Prezesa UODO w postępowaniu cywilnym, a także znaczenia dla postępowania sądowego istotnego poglądu dla sprawy, który może przedstawiać sądowi Prezes Urzędu, jeśli uzna, że przemawia za tym interes publiczny. Prezes Urzędu wskazał, że dotychczasowa praktyka w stosowaniu przepisów rozdziału 10 ustawy o ochronie danych osobowych i stanowiska zaprezentowane podczas seminarium wymagają rozważenia konieczności przeprowadzenia zmian legislacyjnych w tym obszarze. Z kolei Prezes „Iustitii" wskazał na potrzebę szkoleń sędziów na temat stosowania przepisów o ochronie danych osobowych. Podczas seminarium zasygnalizowany został również poważny problem dotyczący ochrony danych osobowych podczas rozpraw w salach sądowych. Przewidziano, że pokłosiem tego wydarzenia będzie specjalna publikacja w prasie prawniczej.

# V. Wnioski wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych

Rok 2025 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,

[722] Nagranie wydarzenia oraz obszerna relacja z jego przebiegu są dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/531/3958.

- 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, w sprawach dotyczących ochrony danych osobowych,
- uspójnienie wykładni przepisów prawa dotyczących ochrony danych osobowych,
- przekazanie administratorom jasnych wskazówek, jak w praktyce stosować przepisy o ochronie danych osobowych bez podejmowania działań nadmiernie ich obciążających.

Analiza działań podjętych w 2025 roku pozwala stwierdzić, że wiele w tym zakresie już udało się osiągnąć.

Do tego stanu rzeczy niewątpliwie przyczyniły się zainicjowane przez Prezesa UODO zmiany w stukturze organizacyjnej Urzędu, które były odpowiedzią na zmieniające się otoczenie oraz nowe wyzwania i zadania stojące przed organem nadzorczym. U podstaw zmian w organizacji UODO leżało przekonanie Prezesa UODO, że skuteczna ochrona danych osobowych wymaga nie tylko regulacji prawnych, ale także aktywnego zaangażowania społecznego, edukacji oraz współpracy międzysektorowej. Dlatego powołanie nowych jednostek organizacyjnych w UODO stanowiło bardzo ważny krok na drodze realizacji działań o charakterze społecznym i rozwojowym Urzędu, które prowadzone na obszarze kraju miały też swój wydźwięk europejski i międzynarodowy.

Przykładem było spotkanie z ambasodorami państw Unii Europejskiej (17.02.2025 r.) zorganizowane przez nowo powstały w UODO Departament Projektów Społecznych i Zrównoważonego Rozwoju (DPSZR). Spotkanie miało na celu nawiązanie relacji z przedstawicielami państw Unii Europejskiej na rzecz współpracy w zakresie wzmocnienia ochrony danych osobowych obywateli UE. Wpływ, jaki wywiera UODO na system stanowienia prawa w zakresie ochrony danych osobowych w Polsce i na świecie sprawił, że współpraca polskiego organu ze środowiskiem międzynarodowym nabrała szczególnego znaczenia.

Dynamiczny rozwój technologii, postępująca cyfryzacja usług publicznych i prywatnych, rosnące znaczenie cyberbezpieczeństwa, zwiększająca się liczba incydentów naruszeń ochrony danych oraz wpływu skarg powodują, że ochrona danych osobowych wymaga specjalistycznego podejścia systemowego i zarazem interdyscyplinarnego, opartego na współpracy wielu podmiotów – zarówno na poziomie krajowym, jak i międzynarodowym. W tym kontekście nowo powstałe jednostki organizacyjne w stukturze UODO odgrywają kluczową rolę w podejmowaniu nowych wyzwań, identyfikowaniu nowych zagrożeń, inicjowaniu działań edukacyjnych, regulacyjnych, prewencyjnych i organizacyjnych usprawniających pracę Urzędu, a także zapewniających skuteczną koordynację wszystkich przedsięwzięć UODO, będących odpowiedzią na wyzwania i aktualne potrzeby.

Konieczność wzmocnienia strukturalnego Urzędu Ochrony Danych Osobowych, wiąże się z nowymi obowiązkami i kompetencjami Prezesa UODO, wynikającymi z **Aktu o zarządzaniu danymi (DGA)** oraz **Aktu o usługach cyfrowych (DSA)**. UODO, przyjmując nowe kompetencje wynikające z DGA będzie zajmował się także danymi nieosobowymi. W odpowiedzi na to zadanie utworzono w Urzędzie wyspecjalizowaną komórkę organizacyjną – Departament Innowacji i Zarządzania Danymi.
Zgodnie ze statutem Urzędu do zadań departamentu należą:

- koordynacja i prowadzenie działań mających na celu przygotowanie Urzędu do wykonywania przez Prezesa Urzędu zadań organu właściwego do spraw usług pośrednictwa danych i organu właściwego do spraw rejestracji organizacji altruizmu danych oraz innych zadań wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 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 ze zm.);
- działań mających na celu przygotowanie Prezesa Urzędu Ochrony Danych Osobowych do wykonywania nowych uprawnień wynikających z ustawy o zarządzaniu danymi (DGA);
- prowadzenie badań i analiz w zakresie wdrażania europejskiej strategii dotyczącej danych;
- rozwijanie współpracy z sektorem publicznym i prywatnym, a także z pośrednikami danych i organizacjami zajmującymi się altruizmem danych w zakresie ustawy o zarządzaniu danymi;
- Współpraca z właściwymi organami państw członkowskich
- Współpraca z Europejską Radą ds. Innowacji w zakresie Danych oraz Komisją Europejską oraz
- współpraca z innymi departamentami Urzędu Ochrony Danych Osobowych.

Departament Innowacji i Zarządzania Danymi skupił się na udziale w procesie legislacyjnym dotyczącym ustawy o zarządzaniu danymi oraz ustawy o danych, a także na podnoszeniu świadomości społecznej, m.in. poprzez publikacje cyklu artykułów zatytułowanych „Nowe podejście do zarządzania danymi” w Biuletynie UODO, a także organizując webinarium zatytułowane „Nowe uprawnienia Prezesa Urzędu Ochrony Danych Osobowych” i konferencję naukową: „DGA – innowacyjne zarządzanie danymi”. Inne działania to obszar dotyczący reklam politycznych online w kontekście rozporządzenia 2024/900 i tworzenie przewodników dotyczących tematów związanych z ochroną danych osobowych.

DGA wprowadza szereg mechanizmów mających zapewnić bezpieczny i przejrzysty przepływ danych, w szczególności poprzez:

- uregulowanie zasad ponownego wykorzystywania określonych kategorii danych pozostających w posiadaniu podmiotów sektora publicznego, które podlegają ochronie praw osób trzecich (tzw. dane chronione);

- ustanowienie ram prawnych dla działalności dostawców usług pośrednictwa w zakresie danych w celu zwiększenia zaufania między podmiotami udostępniającymi i korzystającymi z danych;
- zachęcanie do udostępniania danych w interesie publicznym (altruizm danych);
- ustanowienie Europejskiej Rady ds. Innowacji w zakresie Danych, której zadaniem jest wspieranie spójnego stosowania przepisów i wymiany dobrych praktyk między państwami członkowskimi.

Nowe zadania wymagać będą w szczególności organizacji szkoleń, konferencji, seminariów i inych inicjatyw edukacyjnych, prowadzonych w ramach współpracy z innymi podmiotami oraz wymiany informacji na gruncie krajowym, europejskim i międzynarodowym. Konieczne jest wsparcie finansowe dla działań edukacyjno-informacyjnych o nowym zadaniu UODO, jako organu właściwego do spraw usług pośrednictwa danych oraz jako organu właściwego do spraw rejestracji organizacji usług altruizmu danych.

W związku z reorganizacją przeprowadzoną w Urzędzie Ochrony Danych Osobowych od początku 2025 etapem **wstępnej kontroli skarg** zajmuje się Departament Wstępnej Kontroli Skarg i Naruszeń, do którego wpływają wszystkie krajowe skargi składane przez osoby, których dane dotyczą. Zadaniem tego departamentu jest weryfikacja skarg pod względem braków formalnych, ewentualne wezwanie do ich uzupełnienia, a następnie, po stwierdzeniu kompletności skarg, przekazanie ich do Departamentu Skarg w celu rozpatrzenia i wydania decyzji administracyjnej.

Reorganizacja Urzędu, w tym wyodrębnienie Wydziału Wstępnej Kontroli Skarg w ramach nowopowstałego departamentu, pozwoliła na lepszy podział zadań wśród pracowników, w tym poprzez optymalne wykorzystanie ich predyspozycji. Jednocześnie – wobec stale wzrastającej liczby skarg – okazała się niezwykle potrzebna, zarówno Urzędowi dla zachowania jego efektywności, jak i interesantom, poprzez usprawnianie ich obsługi. W tym drugim zakresie m.in. podjęto kontakty telefoniczne z wnoszącymi podania, równolegle z zachowaniem form przewidzianych ustawą Kodeks postępowania administracyjnego.

Skupienie uwagi grupy pracowników UODO na etapie wstępnej weryfikacji skarg pozwoliło na wypracowanie lepszej metodologii pracy na pierwszym etapie kontaktu z osobami zwracającymi się o interwencję Prezesa UODO. Przełożyło się to na dopracowanie i ujednolicanie wzorów pism kierowanych do interesantów, uwzględniających zasady prostego języka – by były łatwiejsze w odbiorze i zapewniały bardziej precyzyjną komunikację.

Choć zróżnicowanie wpływających do Prezesa UODO skarg wskazuje na wzrost świadomości obywateli odnośnie ich praw wynikających z RODO, to Prezes UODO dostrzega potrzebę dalszych działań edukacyjnych, rozpowszechniania informacji o zakresie swoich kompetencji oraz zakresie stosowania przepisów RODO. Liczba kierowanych do organu żądań, które wykraczają poza jego kompetencje, pozwala stwierdzić, że Prezes UODO jest postrzegany przez obywateli jako organ mogący

zająć się sprawami w zakresie zdecydowanie szerszym niż tylko ochrona danych osobowych.

W 2025 r. wydaniem decyzji administracyjnej w **sprawach skargowych** zakończyło się **2020 spraw.** W porównaniu do 2024 roku, w którym wydanych zostało 1670 decyzji, liczba ta wyraźnie wzrosła. Wzrost ten jest wynikiem ww. reorganizacji, przeprowadzonej w Urzędzie Ochrony Danych Osobowych, dzięki której w Departamencie Skarg skoncentrowano się na czynnościach dokonywanych w toku wszczętych postępowań oraz na wydawaniu decyzji administracyjnych, kończących postępowania. Departament Wstępnej Kontroli Skarg i Naruszeń przejął bowiem od Departamentu Skarg kompetencje w zakresie wstępnej kontroli skarg, w zakresie kierowania wezwań o uzupełnienie braków formalnych skarg. W wyniku przekazania tego etapu prac nad sprawami skargowymi do ww. departamentu, do Departamentu Skarg trafiają skargi pozbawione braków formalnych. Taka zmiana organizacyjna w Urzędzie była uzasadniona koniecznością optymalizacji procesu rozpatrywania wnoszonych skarg, z uwagi na coroczny znaczący wzrost ich liczby. **Łączna liczba spraw zakończonych w Departamencie Skarg w roku 2025 wyniosła 2291.**

Wśród skarg na podmioty z **sektora publicznego** liczne dotyczyły zarzutu bezpodstawnego udostępnienia danych osobowych, w tym ich udostępnienia w Biuletynie Informacji Publicznej[723]. Prezes UODO rozpatrywał skargi na działanie podmiotów publicznych, w tym ministrów, starostów, wójtów i burmistrzów, a także na działania organów kolegialnych, tj. rady gminy i powiatu oraz komorników. Rozstrzygnięte sprawy dotyczyły również przetwarzania danych osobowych przez spółdzielnie mieszkaniowe, wspólnoty mieszkaniowe oraz podmioty świadczące usługi bieżącego administrowania nieruchomością.

Pośród spraw z **sektora prywatnego** odnotowano, podobnie jak w poprzednich latach, znaczną liczbę spraw dotyczących przetwarzania danych w związku z prowadzonymi działaniami marketingowymi, monitoringiem czy też udostępnieniem danych osobowych podmiotowi nieuprawnionemu. Liczne sprawy dotyczyły także realizacji praw osób, których dane dotyczą, wynikających z RODO.

Podobne do lat poprzednich trendy utrzymały się także w **sektorze finansów**. Skargi z tego sektora dotyczyły dopuszczalności przetwarzania danych stanowiących tajemnicę bankową po wygaśnięciu zobowiązania wynikającego z umowy w celu oceny zdolności kredytowej i analizy ryzyka kredytowego bez zgody podmiotu danych, przetwarzania danych w zakresie wynikającym z zapytań kredytowych niezakończonych zawarciem umowy kredytu, czy też dopuszczalności przetwarzania danych osobowych w celach windykacyjnych oraz archiwizacyjnych po zakończeniu stosunków gospodarczych.

Skargi na podmioty z **sektora zdrowia** często dotyczyły uzyskiwania przez lekarzy dostępu do danych zgromadzonych na Platformie Usług Elektronicznych Zakładu Ubezpieczeń Społecznych[724] bez podstawy prawnej i dalszego przetwarzania

[723] Dalej także BIP.
[724] Dalej: PUE ZUS.

zlokalizowanych na tej platformie danych, przetwarzania danych w celu wystawienia e-recept, publikowania danych osobowych osób wykonujących zawody medyczne na portalach internetowych.

Wśród spraw z **sektora zatrudnienia** dominowały natomiast sprawy dotyczące nieuprawnionego przetwarzania przez pracodawców danych osobowych pracowników i byłych pracowników oraz przetwarzania danych osobowych z wykorzystaniem różnych form monitoringu, w tym monitoringu wizyjnego prowadzonego przez pracodawców, w tym z pominięciem spełnienia obowiązków informacyjnych.

W ramach **sektora szkolnictwa** najczęstszymi zarzutami podnoszonymi w skargach były zarzuty dotyczące nieprawidłowości w administrowaniu danymi osobowymi zarówno uczniów jak i ich rodziców, w tym ujawnienia informacji o dziecku rodzicom innych dzieci, udostępnienia danych przez dyrektorów lub nauczycieli placówek szkolnych na rzecz osób trzecich, np. za pośrednictwem dziennika elektronicznego, nieuprawnionej publikacji wizerunku ucznia na portalu społecznościowym.

Ponadto 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. 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 większa liczba wnoszonych skarg wskazuje na zauważalny wzrost świadomości w zakresie ochrony danych osobowych, 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. Analiza wniesionych skarg wykazała, że skarżący nie zawsze potrafią właściwie określić naruszenie przepisów RODO, przez co zdarza się, że ich żądania wykraczają poza kompetencje Prezesa UODO. W roku 2025, podobnie jak w latach poprzednich, 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 kierowanych do stron postępowania pismach organ informował wówczas, 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 większości spraw administratorzy udzielają wyczerpujących wyjaśnień i odpowiedzi na pytania Prezesa UODO w toku prowadzonych postępowań. Jednocześnie administratorzy wciąż często popełniają błędy w zakresie wskazania prawidłowej podstawy prawnej przetwarzania danych osobowych oraz konkretnych przepisów prawa regulujących określone procesy przetwarzania.

Podkreślić należy, że Prezes UODO podejmuje 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 ich liczba stale i znacząco rośnie. Poza ograniczonymi możliwościami kadrowymi, również duża liczba wnoszonych skarg wpływa na czas trwania postępowań prowadzonych przez Prezesa UODO. Pomimo jednak znacznego wzrostu liczby skarg wniesionych do Prezesa UODO w 2025 r., wzrosła również liczba decyzji administracyjnych wydanych w sprawach skargowych dzięki podjętym przez Prezesa UODO działaniom i wzmożonym wysiłkom pracowników UODO. W większości spraw sądy administracyjne podzielały stanowiska zajmowane przez organ w sprawach skargowych, oddalając skargi na decyzje Prezesa UODO, co świadczy o wysokiej jakości merytorycznej wydawanych w sprawach skargowych rozstrzygnięć.

Pozwala to na sformułowanie wniosku o przyjętym przez Prezesa UODO właściwym kierunku optymalizacji pracy, co pozwoliło na zachowanie wysokiej jakości merytorycznej rozstrzygnięć organu nadzorczego. Zasadne jest zatem kontynuowanie tego kierunku w zakresie spraw skargowych w kolejnych latach, któremu towarzyszyć musi jednak nieuchronnie wzmocnienie zasobów kadrowych Urzędu.

Na koniec należy podkreślić, że dla ochrony osoby, której dane dotyczą 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 ich danych w sposób niezgodny z przepisami RODO.

W odniesieniu do **wstępnej kontroli naruszeń** wskazać należy, że rośnie świadomość wśród administratorów, którzy nie po raz pierwszy zgłaszają organowi nadzorczemu naruszenie ochrony danych osobowych. Notyfikując kolejne naruszenia, administratorzy w większości przypadków potrafili trafnie ocenić, czy wystąpiło wysokie ryzyko naruszenia dla praw lub wolności osób fizycznych oraz stwierdzić wskutek dokonanej analizy, czy należy zawiadomić osoby o naruszeniu ochrony 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).

Niemniej jednak należy odnotować znaczący wzrost liczby zgłoszeń naruszeń ochrony danych osobowych kierowanych do Prezesa UODO w 2025 r. Tendencja ta potwierdza rosnącą świadomość administratorów w zakresie obowiązku notyfikacji incydentów, a jednocześnie obrazuje utrzymujące się wyzwania w obszarze bezpieczeństwa przetwarzania danych osobowych. Zwiększona liczba notyfikacji wymaga dalszej optymalizacji procesów wewnętrznych, w szczególności w zakresie wstępnej kwalifikacji zgłoszeń oraz ich odpowiedniej priorytetyzacji. Utrzymanie sprawności wstępnej kwalifikacji zgłoszonych naruszeń ochrony danych osobowych przy rosnącym obciążeniu ich liczbą pozostaje jednym z kluczowych wyzwań organu.

Analiza zgłoszeń wskazuje, że najczęstsze przyczyny naruszeń obejmowały: incydenty cyberbezpieczeństwa, w tym ataki ransomware oraz nieuprawniony dostęp do systemów, błędy ludzkie skutkujące nieuprawnionym ujawnieniem danych osobowych, a także niedostateczne zabezpieczenia organizacyjne i techniczne. Wnioski te potwierdzają potrzebę dalszego wzmacniania kultury bezpieczeństwa informacji oraz zarządzania ryzykiem w organizacjach.

Doświadczenia wynikające z analizy zgłoszonych naruszeń ochrony danych osobowych wskazują, że istotna liczba naruszeń mogłaby zostać ograniczona poprzez: właściwą ocenę ryzyka przed wdrożeniem nowych procesów przetwarzania danych osobowych, regularne szkolenia personelu oraz stosowanie adekwatnych środków technicznych i organizacyjnych.

W ostatnich latach obserwuje się wyraźny wzrost świadomości administratorów danych w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych. Administratorzy oraz podmioty przetwarzające wdrażają polityki bezpieczeństwa informacji, procedury reagowania na naruszenia ochrony danych osobowych oraz odpowiednie środki techniczne i organizacyjne służące zabezpieczeniu przetwarzania danych. Coraz powszechniejsze staje się także prowadzenie ewidencji osób upoważnionych do przetwarzania danych, stosowanie mechanizmów nadawania i weryfikacji uprawnień dostępowych, okresowe przeglądy upoważnień oraz kontrola dostępu do systemów informatycznych i dokumentacji papierowej. Pomimo powyższego nadal dochodzi do naruszeń ochrony danych osobowych, wynikających w szczególności z błędów ludzkich, niewystarczającego nadzoru nad procesami przetwarzania, nieprawidłowej konfiguracji systemów teleinformatycznych oraz działań osób trzecich, w tym sprawców cyberataków.

Jednocześnie postępująca cyfryzacja usług publicznych i prywatnych, rosnąca skala przetwarzania danych w systemach teleinformatycznych oraz dynamiczny rozwój technologii przetwarzania informacji, w tym narzędzi wykorzystujących sztuczną inteligencję, generują nowe wyzwania dla systemu ochrony danych osobowych.

Zwiększa się liczba incydentów bezpieczeństwa informatycznego, takich jak phishing, ransomware, przejęcia kont użytkowników czy nieuprawnione pozyskiwanie danych z usług online. Wykorzystanie rozwiązań opartych na sztucznej inteligencji, w szczególności systemów automatycznego profilowania, analizy behawioralnej i przetwarzania dużych zbiorów danych, powoduje konieczność pogłębionej oceny ryzyka dla praw i wolności osób fizycznych oraz wymaga od administratorów stałego podnoszenia poziomu zabezpieczeń, monitorowania procesów przetwarzania oraz dostosowywania środków ochrony do zmieniającego się charakteru zagrożeń.

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.

Orzecznictwo sądów administracyjnych w znacznej mierze potwierdza prawidłowość podejmowanych przez Prezesa UODO czynności oraz trafność wydawanych rozstrzygnięć, utrzymując w mocy decyzje organu. Wskazuje to na zgodność działań nadzorczych z obowiązującymi przepisami oraz na prawidłową ocenę ryzyka i skutków naruszeń ochrony danych osobowych. Wydawane decyzje mają istotny wpływ na poziom bezpieczeństwa systemu ochrony danych osobowych w Polsce. Stanowią one instrument egzekwowania przepisów prawa, lecz również ważne źródło wiedzy dla administratorów danych i podmiotów przetwarzających. Uzasadnienia decyzji zawierają bowiem szczegółowe wskazania dotyczące standardów należytej staranności, adekwatnych środków technicznych i organizacyjnych oraz właściwych praktyk w zakresie zarządzania ryzykiem, przyczyniając się do podnoszenia poziomu zgodności z przepisami o ochronie danych osobowych.

Niezmiennie priorytetem dla Prezesa UODO pozostaje zapewnienie wysokiego poziomu ochrony praw i wolności osób fizycznych oraz budowanie kultury zgodności z przepisami o ochronie danych osobowych w życiu publicznym i gospodarczym.

**Opiniowanie projektów aktów prawnych** pod kątem zgodności z prawem ochrony danych jest bardzo ważnym zadaniem Prezesa UODO. 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.

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.

Na podstawie analizy opinii legislacyjnych Prezesa UODO wyróżnić można kwestie, które budzą problemy, a także wskazać powtarzające się uchybienia. Wiele z nich stanowi powielenie tendencji zauważonych w latach ubiegłych. W roku 2025 z jeszcze większą siłą uwidoczniły się jednak liczne trudności związane głównie z wdrażaniem nowych technologii, a także stałą rozbudową systemów cyfrowych oraz operacji przetwarzania opartych o rozbudowane rejestry państwowe.

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.

Analiza działań podjętych w 2025 roku pozwala stwierdzić, że wiele w tym zakresie już udało się osiągnąć.

Konsekwentne działania organu nadzorczego w obszarze złożonych procesów legislacyjnych, zapewniające wielu różnym środowiskom wsparcie **eksperckie na etapie tworzenia oraz stosowania prawa**, przynoszą zamierzone rezultaty. Niemniej wymagały intensywnego i wieloetapowego zaangażowania organu nadzorczego – od współpracy na etapie tworzenia przepisów prawa, poprzez aktywny udział w licznych konferencjach uzgodnieniowych i komisjach prawniczych organizowanych przez projektodawców, aż po udział w pracach parlamentu.

Podejmowane działania skutkują nie tylko przyjmowaniem regulacji zgodnych ze standardami ochrony danych ustanowionych na mocy RODO, lecz także przyczyniają

się do usprawnienia wykonywania obowiązków wynikających z tych przepisów. Wzrasta świadomość projektodawców dotycząca problematyki ochrony danych osobowych, która przekłada się na wyższy standard ochrony praw osób, których dane dotyczą, oraz minimalizuje ryzyko sankcji administracyjnych nakładanych na podmioty odpowiedzialne za procesy przetwarzania.

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.

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.

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.

Aktywność organu to również działania podejmowane z własnej inicjatywy, często dotyczące regulacji prawnych o doniosłym znaczeniu dla praw i wolności osób, podmiotów praw objętych takimi regulacjami. Proces ten w znacznym stopniu wyklucza możliwość wprowadzania rozwiązań kolidujących ze standardami i zasadami RODO.

Taką inicjatywą objęto **projekt ustawy o zmianie ustawy o działalności leczniczej oraz niektórych innych ustaw**[725], którego rozwiązania wiązały się z przetwarzaniem danych osobowych w elektronicznej dokumentacji medycznej. Zwrócono m.in. uwagę na przetwarzanie w niej numeru PESEL identyfikującego osobę trzecią, tj. wystawcę, oraz na przekazywanie pełnej dokumentacji medycznej służbom statystyki publicznej. Proces legislacyjny tej regulacji nie zakończył się, można jednak z zadowoleniem odnotować uwzględnienie najistotniejszych postulatów organu, tj. zrezygnowanie z przekazywania pełnej karty służbom statystyki publicznej, zapowiedziane przez projektodawcę w toku uzgodnień projektu ustawy na początku 2026 r.

Pomijanie Prezesa UODO w procesie opiniowania i uzgodnień projektów aktów normatywnych dotyczących przetwarzania danych osobowych jest negatywnym zjawiskiem, wciąż powtarzającym się na przestrzeni wielu lat. Niepokojącym i niedopuszczalnym zwłaszcza wtedy, gdy regulacja w sposób oczywisty wiąże się z materią ochrony danych osobowych. Ignorowanie obowiązku konsultowania z organem takich dokumentów jest nie tylko naruszeniem ustawowym, ale również pozbawia projektodawcę eksperckiego stanowiska organu, które jest gwarantem prawidłowej implementacji RODO w przyjmowanych przepisami rozwiązaniach. W kolejnym roku organ nadzorczy utrzyma tę praktykę przystępowania do procesów legislacyjnych z urzędu celem zapewnienia wysokich standardów ochrony danych osobowych.

Podobnie niekorzystnym zjawiskiem jest **przedstawienie projektu do zaopiniowania przez Prezesa UODO dopiero na zaawansowanym etapie prac legislacyjnych.** Takie działanie 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.

Przykładem może tu być dotyczący niezwykle istotnych kwestii **projekt ustawy o zmianie ustawy o systemie ubezpieczeń społecznych**[726], przekazany dopiero na etapie sejmowego procesu legislacyjnego. Wątpliwości Prezesa UODO dotyczyły zasadności przekazywania podmiotom prywatnym takich danych, jak m.in. informacje

[725] DPNT.401.413.2025.
[726] DPNT.401.193.2025.

o stanie rozliczeń należnych składek, do poboru których uprawniony jest ZUS. Pomimo doniosłości projektowanej regulacji nie uwzględniono postulatów organu.

Nadal powszechnym problemem pozostaje **brak prawidłowej identyfikacji obszaru ochrony danych osobowych w procesach legislacyjnych**. Niewłaściwe ich rozpoznanie istotnie wpływa na przyjmowanie norm naruszających określone w RODO zasady i zwiększone ryzyko dla praw lub wolności osób fizycznych. Problem ten szczególnie wybrzmiewa w regulacjach mających istotne znaczenie z punktu widzenia praw podstawowych, konstytucyjnych praw i wolności jednostek, a jednocześnie podmiotów danych.

Organ nadzorczy niezmiennie zaleca korzystanie z narzędzi, jakich dostarcza RODO (przeprowadzenie testu prywatności, oceny wpływu planowanych rozwiązań na ochronę danych), a twórcy przepisów coraz częściej przyjmują te zalecenia.

Stałe podnoszenie przez Prezesa UODO kwestii oceny skutków dla ochrony danych przyniosło skutek, bowiem wydaje się, że projektodawcy coraz częściej uwzględniają ten postulat i dokonują oceny skutków dla ochrony danych dotyczącej przetwarzania opartego na projektowanych przepisach czy to w pierwotnej wersji projektu przedstawionej do zaopiniowania, czy to w kolejnej jego wersji, na skutek zgłoszonej rzez organ nadzorczy uwagi. Przykładem takiej sprawy jest przywołany wyżej **projekt ustawy o zabezpieczeniu socjalnym osób wykonujących zawód artystyczny**[727] – uwzględniając uwagi organu nadzorczego, projektodawca zdecydował się uzupełnić projekt o ocenę skutków dla ochrony danych, co przyniosło wymierne korzyści dla treści planowanych regulacji.

Podobnie jak w roku poprzednim, utrzymującym się niestety trendem w opiniowanych projektach aktów prawnych było tworzenie przepisów przewidujących przetwarzanie znacznej ilości danych osobowych **w państwowych rejestrach i za pomocą systemów teleinformatycznych, prowadzące do łączenia różnych baz i rejestrów oraz ich udostępniania innym podmiotom publicznym**, bez koniecznej analizy wszystkich aspektów przetwarzania, bez oceny wiążących się z tym ryzyk, w tym przeprowadzenia oceny skutków dla ochrony danych.

Przykładem takiej sprawy jest **projekt ustawy zmieniającej ustawę o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw** oraz **ustawa o finansach publicznych**[728], w którym projektodawca nie wykazał niezbędności przetwarzania danych osobowych w sposób umożliwiający ich ujawnienie w centralnym rejestrze umów (CRU) do celu związanego z wykonaniem zadania realizowanego w interesie publicznym. W CRU mają być bowiem gromadzone i publikowane dane osobowe oraz dane finansowe szerokiego kręgu podmiotów, w tym osób fizycznych, będących stronami umów z jednostkami sektora finansów publicznych. Udostępnienie danych osobowych za pomocą narzędzia umożliwiającego przeszukiwanie i publiczne udostępnienie informacji wiąże się z ryzykiem dowolnego i dalszego ich przetwarzania w celach niezwiązanych z jawnością wydatków publicznych. Ryzyko dotyczyło też

[727] DPNT.401.155.2025.
[728] DPNT.401.97.2025.

łączenia danych, zasobów danych, profilowania osób fizycznych, wnioskowania o ich sytuacji życiowej.

W okresie sprawozdawczym ważnym działaniem Prezesa UODO, mającym wpływ na kształtowanie prawidłowych rozwiązań związanych z przetwarzaniem danych osobowych, było zgłaszanie (w formie głosu doradczego) uwag do projektów informatycznych w procesie informatyzacji państwa. Efekty tych prac były wymierne – twórcy projektów deklarowali wykonanie testu prywatności, często też wykonywanego na różnych etapach wdrażania, co pozytywnie oceniano.

Dobrym przykładem był projekt informatyczny „SDD 1.0. – system do prowadzenia postępowań dyscyplinarnych w samorządzie komorniczym”[729]. Nie tylko przewidywał przeprowadzenie testów prywatności na różnych etapach wdrażania systemu, ale również ogólne założenia dotyczące bezpieczeństwa, zakładające trójwarstwowy model ochrony informacji oparty o przejrzyste określenie ról i odpowiedzialności w tym zakresie. Organ nadzorczy przywiązuje szczególną wagę do aspektów związanych z ochroną danych w wymiarze obejmującym bezpieczeństwo narodowe, wskazując na potrzebę odporności systemów o znaczeniu istotnym dla funkcjonowania państwa.

Wciąż utrzymującą się tendencją było niedostateczne uwzględnianie przez projektodawców zasad przetwarzania określonych w art. 5 RODO. Przejawia się to na przykład poprzez ustanawianie w projektowanych przepisach otwartych katalogów przetwarzanych danych osobowych, co jest rozwiązaniem wątpliwym z punktu widzenia zasady minimalizacji (art. 5 ust. 1 lit. c RODO) czy poprzez niewystarczające określenie celu (celów) przetwarzania danych na podstawie tych przepisów, co jest problematyczne ze względu na zasadę ograniczenia celu (art. 5 ust. 1 lit. b RODO). Aktualnym i często przewijającym się problemem pozostaje też ustanawianie w projektowanych regulacjach obowiązku przetwarzania numeru PESEL, również wtedy, gdy jego przetwarzanie nie wydaje się niezbędne do osiągnięcia zamierzonego celu, co ma znaczenie zwłaszcza z punktu widzenia ww. zasady minimalizacji. Właściwe wdrożenie zasad przetwarzania danych osobowych z art. 5 RODO w projektowanym akcie prawnym jest tym bardziej istotne w przypadku regulacji prawnych dotyczących przetwarzania danych osobowych małoletnich oraz seniorów.

**Wpływ nowych technologii** był przedmiotem szczególnego zainteresowania organu nadzorczego, odzwierciedlonym w licznych opiniach do tworzonych regulacji. Cyfryzacja procesów przetwarzania nie może negatywnie wpływać na prawa i wolności osób fizycznych. W tym kontekście organ nadzorczy zwracał uwagę na konieczność przeprowadzania pogłębionej analizy projektowanych rozwiązań pod względem wpływu, jaki wywiera dla praw osób, których dane dotyczą, w tym na zapewnienie przejrzystości stosowanych mechanizmów związanych z zastosowaniem algorytmów sztucznej inteligencji, bezpieczeństwem i środkami kontroli. Ciekawym przykładem jest opinia do **projektu ustawy o zmianie ustawy o świadczeniach opieki zdrowotnej**

[729] DPNT.060.33.2025.

**finansowanych ze środków publicznych i niektórych innych ustaw**[730] dotycząca asystenta głosowego (voiceboty) – automatyzacji połączeń telefonicznych. Prezes UODO zwrócił w niej uwagę, że nie określono warunków, celów czy zasad, na jakich „wirtualny asystent" miałby funkcjonować ani do jakich zasobów system SI będzie miał dostęp i jakie dane będzie pozyskiwał.

Temat związany ustanawianiem przepisów regulujących wykorzystywanie rozwiązań cyfrowych z pewnością będzie się rozwijał i stanowił przedmiot szczególnego zainteresowania organu w kolejnym roku.

W kategorii wyzwań należy również postrzegać wdrożenie przepisów rozporządzenia Parlamentu Europejskiego i Rady UE w sprawie **europejskiej przestrzeni danych dotyczących zdrowia**[731]. 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 m.in. stworzenie dla tego aktu dobrego otoczenia regulacyjnego w polskim prawodawstwie.

W roku 2025 ważnym wątkiem w opiniach legislacyjnych Prezesa UODO były też **nowe kompetencje** tego organu wynikające z aktów europejskich. Konieczność ich właściwego urzeczywistnienia w przepisach prawa krajowego i współpraca Prezesa UODO w z projektodawcami na tym polu wciąż pozostanie aktualnym i istotnym wątkiem w najbliższym czasie.

Rok 2025 w działalności Prezesa UODO był bardzo istotny z punku widzenia **wystąpień legislacyjnych.** W tym czasie organ nadzorczy wielokrotnie kierował do właściwych resortów korespondencję mającą prowadzić do zmiany wadliwych z punktu widzenia RODO i prawa do prywatności rozwiązań prawnych. W minionym roku wystąpienia te dotyczyły bardzo wielu różnorodnych zagadnień, w tym m.in. przetwarzania danych osobowych w rejestrach i systemach informatycznych, co stanowi obszar krytyczny w kontekście bezpieczeństwa danych osobowych i prawa do prywatności. Postulaty zgłaszane przez Prezesa UODO w wystąpieniach często nie spotykają się, niestety, ze zrozumieniem ze strony adresatów wystąpień, niemniej w niektórych przypadkach właściwe resorty dostrzegają sygnalizowany problem i deklarują współpracę w tym zakresie.

Przykładem takiej sprawy jest **wystąpienie dotyczące zapewnienie skutecznego stosowania przepisów o ochronie danych osobowych w związku z wykorzystywaniem kamer nasobnych przez kontrolerów biletów w środkach**

[730] DPNT.401.101.2025.

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

**transportu publicznego**[732]. W odpowiedzi na wystąpienie Minister Infrastruktury przychylił się do stanowiska Prezesa UODO i ze względu na konieczność zadbania o prawa pasażerów do zachowania prywatności i ochrony wizerunku osoby resort nie podjął decyzji o wprowadzeniu uprawienia dla przewoźnika lub operatora do stosowania monitoringu audiowizualnego podczas kontroli biletów i dokumentów przewozu.

Warto podkreślić, że w wielu przypadkach wystąpienia Prezesa UODO są następstwem sygnałów dotyczących problemów ze stosowaniem przepisów prawa przekazanych przez inspektorów ochrony danych.

Osobną grupę stanowią wystąpienia związane z dokonywaną przez Prezesa UODO **oceną wyroków TSUE**. Niektóre z nich powodują bowiem konieczność dokonania zmian w przepisach prawa krajowego, na co Prezes UODO w 2025 r. wskazywał w korespondencji kierowanej do poszczególnych resortów.

Działania te organ nadzorczy realizował zgodnie z założeniem z 2024 r., kiedy to w odpowiedzi na swoje wystąpienie skierowane do Ministra do spraw Unii Europejskiej[733] uzyskał informację, że odpowiedzialność za wdrożenie wyroków TSUE spoczywa na ministrach właściwych merytorycznie ze względu na tematykę danej sprawy.

Jednocześnie Prezes UODO za potrzebne uznaje **stałe upowszechnianie wiedzy na temat orzecznictwa TSUE, ETS i 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.

W roku 2025 organ nadzorczy niezmiennie dużą wagę – podobnie jak w latach ubiegłych – przywiązywał do **współpracy z inspektorami ochrony danych** oraz do właściwego rozumienia funkcji inspektora ochrony danych, a także prawidłowego ukształtowania jego roli w procesie ochrony danych osobowych, w tym rozdzielenia zadań administratora i inspektora ochrony danych.

Prezes UODO, doceniając rolę inspektorów ochrony danych w procesie zapewnienia prawidłowej ochrony danych osobowych, z uwagą podchodził i podchodzi do realizacji przez administratorów ich obowiązków dotyczących funkcjonowania IOD i identyfikuje występujące w tym obszarze trudności i wątpliwości. W swoich działaniach organ nadzorczy przede wszystkim podkreśla, że podmioty zobowiązane do wyznaczenia inspektora powinny mieć na uwadze, że RODO w art. 37 – 39 nakłada

[732] DPNT.413.14.2025.
[733] DOL.413.14.2024.

na administratorów konkretne obowiązki związane nie tylko z wyznaczaniem inspektora ochrony danych, ale również z wyborem do pełnienia tej funkcji osoby posiadającej właściwe kwalifikacje, a także z zapewnieniem, aby wyznaczony inspektor mógł niezależnie i prawidłowo realizować swoje zadania. Obowiązki te ciążą na administratorze niezależnie od tego, czy IOD jest pracownikiem administratora, czy też pełni swoją funkcję na podstawie umowy o świadczenie usług (motyw 97 rozporządzenia 2016/679).

Dlatego zapewnienie właściwych warunków do wykonywania zadań IOD, w tym również na poziomie regulacji prawnych, jest jednym z niezmiennych celów działań podejmowanych przez Prezesa UODO. W 2025 roku przykładami takich działań były:

1) ponowne wystąpienie Prezesa UODO do Szefowej Służby Cywilnej o zmianę przepisów rozporządzenia stanowiskowo – płacowego, której celem jest wyodrębnienie stanowiska inspektora ochrony danych w wykazie stanowisk urzędniczych w służbie cywilnej[734],
2) ponowne wystąpienie do MSWiA o podjęcie prac nad nowelizacją przepisów odnoszących się do roli inspektora ochrony danych w służbach zajmujących się zwalczaniem przestępczości[735],
3) zgłoszenie uwag do projektu rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy w zakresie umiejscowienia i opisu zawodu inspektora ochrony danych[736],
4) wyrażenie opinii w sprawie postępowania przed Trybunałem EFTA w sprawie E-5/25 Silbernagl (ochrona danych osobowych – podstawy zwolnienia inspektora ochrony danych), która dotyczyła zakresu ochrony przed zwolnieniem, jaką przyznają inspektorom ochrony danych art. 38 ust. 3 zdanie drugie RODO oraz regulacje krajowe. Prezes UODO rekomendował udział Polski w tym postępowaniu, wskazywał przy tym, że orzeczenie Trybunału w tej sprawie może mieć znaczenie nie tylko w zakresie stosowania art. 38 ust. 3 zdanie drugie RODO, ale również może mieć wpływ na zakres i kierunek doprecyzowania w polskim porządku prawnym regulacji dotyczących odwoływania IOD[737],
5) udział w pracach EROD dotyczących aktualizacji Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (243 WP), które zostały wydane w 2017 roku. Potrzeba ich przeglądu i aktualizacji związana jest m.in. z rozwojem dorobku orzeczniczego organów nadzorczych i sądów oraz zmianą stanu prawnego, a także z problemami sygnalizowanymi organom przez administratorów, inspektorów oraz reprezentujące ich stowarzyszenia.

W 2025 r. Prezes UODO podejmował też wiele działań, których celem było zwiększenie świadomości w zakresie statusu i prawidłowego funkcjonowania **inspektorów ochrony danych**. Były one kierowane zarówno do podmiotów

[734] DOL.413.6.2024.
[735] DOL.413.11.2022.
[736] DPNT.401.275.2025.
[737] DPNT.0623.13.2025.

zobowiązanych do wyznaczenia IOD, jak też do samych inspektorów. Jako przykłady takiej aktywności wskazać można:

1) prezentowanie na spotkaniach z inspektorami i administratorami w ramach akcji „UODO rusza w kraj" wystąpień poświęconych roli i niezależnej pozycji IOD oraz współpracy inspektorów ochrony danych z UODO. Spotkania te były też okazją do rozmów na temat aktualnej sytuacji i problemów inspektorów pełniących swoją funkcję przede wszystkim w jednostkach samorządu terytorialnego oraz terenowych jednostkach administracji zespolonej, a także do dyskusji o możliwych rozwiązaniach służących zapewnieniu prawidłowego wykonywania zadań przez IOD oraz przestrzegania prawa w tym zakresie,
2) zamieszczenie w „Poradniku UODO dotyczącym naruszeń ochrony danych osobowych" rozdziału informującego o tym, jaką rolę odgrywają inspektorzy ochrony danych w procesie obsługi naruszeń[738]. Podkreślono tam m.in, że IOD powinien być niezwłocznie informowany o zaistnieniu naruszenia, aby umożliwić mu monitorowanie procesu jego obsługi od najwcześniejszego etapu. Wskazano również, jak określić zadania IOD związane z obsługą naruszeń, tak aby ustrzec go od działania w konflikcie interesów,
3) zatwierdzenie 24 listopada 2025 r. „Kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencje badania opinii i rynku", w którym twórcy kodeksu zawarli regulacje poświęcone roli inspektora ochrony danych. Dostrzegając szczególny wpływ IOD na właściwe ukształtowanie procesów przetwarzania danych osobowych w organizacji, która go powołuje, poświęcili mu osobny rozdział. Zgodnie z jego postanowieniami agencje badawcze, które przystąpią do stosowania kodeksu, mają m.in. obowiązek wyznaczenia IOD[739].

Aby inspektorzy ochrony danych mogli właściwie wykonywać swoje zadania i służyć powołującym ich podmiotom realną pomocą, administratorzy muszą zapewnić im niezależność, w tym odpowiednie wsparcie oraz zapobieganie konfliktom interesów. Kwestie te były i nadal będą przedmiotem zainteresowania oraz działań podejmowanych przez Prezesa UODO, w tym zwłaszcza działań związanych z egzekwowaniem powyższych obowiązków.

W 2025 r. nieprawidłowe wypełnianie przez administratorów obowiązków dotyczących IOD było powodem nałożenia przez organ nadzorczy:

1) upomnienia dla administratora, który nie zapewnił IOD właściwych warunków do prawidłowego i niezależnego wypełniania zadań oraz nie wdrożył środków organizacyjnych lub technicznych, pozwalających na rozliczanie IOD z wykonania jego zadań wynikających z przepisów RODO (decyzja z 2 kwietnia 2025 r. w sprawie DKN.5110.14.2022)[740],

[738] Poradnik dostępny jest pod linkiem: https://uodo.gov.pl/pl/598/3563.
[739] Treść kodeksu dostępna jest pod linkiem: https://uodo.gov.pl/pl/426/1110.
[740] Więcej informacji pod linkiem: https://uodo.gov.pl/pl/138/3597.

2) kary za wyznaczenie do pełnienia funkcji IOD osoby zajmującej stanowisko prezesa zarządu, a tym samym niezapewnienie, aby wykonywane przez IOD inne zadania i obowiązki nie powodowały konfliktu interesów (decyzja z 12 września 2025 r. w sprawie DKN.5131.7.2025)[741].

W 2025 r. Prezes UODO podejmował wiele różnorodnych działań, których celem było zapewnienie inspektorom ochrony danych warunków do prawidłowego wypełniania ich funkcji oraz podnoszenie świadomości administratorów i podmiotów przetwarzających co do ich obowiązków związanych z wyznaczenia IOD, a także co do korzyści płynących z posiadania przez organizację takiego eksperckiego wsparcia.

Pomimo wpływających do Prezesa UODO sygnałów o nieprawidłowościach, warto też zauważyć, że proces budowania świadomości w zakresie przetwarzania i ochrony danych osobowych oraz roli IOD postępuje. Liczne stanowiska i zalecenia oraz działania egzekucyjne Prezesa UODO co do przestrzegania przepisów RODO dotyczących IOD, a także konferencje i szkolenia, współpraca z inspektorami ochrony danych oraz środowiskami zajmującymi się tą tematyką, a także generalny wzrost zainteresowania cyberbezpieczeństwem i nowymi technologiami, pozwalają żywić nadzieję na coraz bardziej odpowiedzialne i zgodne z prawem podejście kierownictwa podmiotów publicznych i prywatnych do zadań i obowiązków wynikających z RODO, w tym tych odnoszących się do inspektorów ochrony danych.

W planach Prezesa UODO na kolejne lata przewidziana jest kontynuacja działań na rzecz zwiększania świadomości, co do roli i statusu IOD, zwłaszcza co do przewidzianych w RODO gwarancji niezależnego wykonywania tej funkcji. Nadal organ nadzorczy będzie aktywnie wspierał inspektorów – udzielał im indywidualnych konsultacji, publikował na stronie internetowej i w Biuletynie UODO materiały edukacyjne, organizował szkolenia i konferencje, kierował wystąpienia w sygnalizowanych przez IOD sprawach. Ponadto w 2026 r. organ nadzorczy zamierza czynnie uczestniczyć w pracach EROD nad zmianą Wytycznych dotyczących IOD. Kwestie wyznaczania IOD i zapewnienia im możliwości prawidłowego wykonywania zadań były i nadal będą też przedmiotem działań związanych z egzekwowaniem obowiązków przewidzianych w rozporządzeniu 2016/679, w tym działań kontrolnych.

Ważnym działaniem będzie także kontynuowanie **wsparcia dla inicjatyw pracujących nad kodeksami postępowania**.

Warto podkreślić, że kodeksy postępowania to ważny instrument ułatwiający osiąganie zgodności z RODO i podnoszenie poziomu ochrony danych osobowych.

Kodeks, który jest właściwie przygotowany (m.in. nie jest jedynie powtórzeniem przepisów RODO, a przede wszystkim doprecyzowuje problemowe kwestie

[741] Treść decyzji dostępna jest pod linkiem: https://orzeczenia.uodo.gov.pl/search?dcr=rodo&rn=DKN.5131.7.2025&page=1.

z uwzględnieniem specyfiki danej branży), przynosi wiele korzyści[742]. 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 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[743].

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

[742] 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.).

[743] Więcej informacji na temat błędów najczęściej popełnianych podczas przygotowywania kodeksu postępowania można znaleźć na stronie internetowej UOFO pod linkiem https://uodo.gov.pl/pl/426/2789.

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.

Jednocześnie warto zaznaczyć, że Polska plasuje się w czołówce Europy pod względem liczby zatwierdzonych kodeksów postępowania[744]. Prezes UODO zatwierdził bowiem już trzy takie dokumenty. To tyle samo, ile organy nadzorcze w Niemczech i Hiszpanii, a więcej niż np. we Francji.

Istotnym 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.

W 2025 r. – podobnie jak w latach ubiegłych – zakres tematyczny **pytań dotyczących wykładni prawa** lub właściwej praktyki kierowanych do Prezesa UODO był bardzo szeroki i dotyczył różnych aspektów przetwarzania danych osobowych. Wątpliwości dotyczyły nie tylko stosowania RODO, ale także innych, szczególnych przepisów prawa.

Wiele z pytań dotyczyło m.in.:

1. stosowania monitoringu wizyjnego,
2. przetwarzania danych osobowych przez pracodawców,
3. przetwarzania danych szczególnych kategorii, w tym danych dotyczących zdrowia przetwarzanych w dokumentacji medycznej,
4. możliwości udostępniania danych innym podmiotom,
5. określania ról podmiotów w konkretnych procesach przetwarzania danych.

Analizując treść wpływających pytań zauważyć można, że z każdym rokiem pojawiające się w nich zagadnienia coraz rzadziej dotyczą kwestii podstawowych, a odnoszą się do coraz bardziej złożonych problemów.

Odpowiedzi organu nadzorczego często stanowią podstawę do przygotowywania materiałów informacyjno-edukacyjnych, podnoszących świadomość w zakresie ochrony danych osobowych, a także ułatwiających administratorom i podmiotom przetwarzającym oraz inspektorom ochrony danych wywiązywanie się z nałożonych przepisami RODO obowiązków i zadań, a także wypracowanie odpowiednich standardów i rozwiązań.

Ta praktyka będzie kontynuowana w roku 2026.

[744] Ogólnie liczba zatwierdzonych kodeksów postępowania w UE nie jest duża, a wiele krajów nie ma żadnego.

Wciąż obserwowaną i 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.

W roku 2025 kontynuowana była **ocena 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 ym zakresie, w 2025 r. w UODO prowadzony były prace 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.

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 miał na celu realizację bardziej spójnego stosowania przepisów o ochronie danych osobowych przez sądy, aby prawa osób, których dane dotyczą, były właściwie respektowane.

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 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 w 2024 roku przez Prezesa UODO opinia do **Strategii Cyfryzacji Polski do 2035 r**.[745] 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 z 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.

[745] DOL.401.502.2024.

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.

Analizując kwestię zamierzeń i wyzwań nie można pominąć postępującej **cyfryzacji i automatyzacji przetwarzania danych osobowych**, które uwypukliły znaczenie, jakie będzie miało zrozumienie kwestii informatycznych i technologicznych dla oceny rozwiązań prawnych.

Rozwój technologiczny powoduje m.in. to, że informacje, które dziś postrzegamy jako neutralne, wkrótce mogą stać się danymi osobowymi. Nietrudno wyobrazić sobie, że w wyniku połączenia przez sztuczną inteligencję różnych anonimowych – wydawałoby się – informacji może dojść do wygenerowania danych osobowych.

Jednocześnie ochrona danych nie jest już odrębnym obszarem, lecz zagadnieniem, które należy rozpatrywać z uwzględnieniem wielu aspektów, zwłaszcza technologicznych. W praktyce oznacza to, że ocena zgodności będzie coraz częściej wymagała spojrzenia na kilka aktów prawnych jednocześnie.

Prezes UODO wielką wagę przywiązuje do uwzględniania w swoich działaniach technologicznego wymiaru ochrony danych. Jako organ nadzorujący musi identyfikować i rozumieć najnowocześniejsze technologie wykorzystywane do przetwarzania danych osobowych, aby zachęcać do uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych w procesie innowacji. Jednocześnie musi dokładnie analizować i rozumieć zarówno potencjalne zagrożenia, jak i możliwości oferowane przez powstające technologie.

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.

Ponadto ważne jest, by nie reagować na wiele zjawisk po fakcie, lecz działać proaktywnie i w miarę możliwości uprzedzać trendy technologiczne, które często są trudne do przewidzenia. Istotne będzie przy tym antropocentryczne podejście do nowych technologii. Trzeba bowiem na nowo **znaleźć równowagę między**

**innowacjami a prawami człowieka**. W świecie algorytmów, automatyzacji i globalnych platform w centrum musi pozostać człowiek, jego prywatność, godność i realna możliwość decydowania o swoich danych.

Wsparciem dla tym wyzwań jest **edukacja i podnoszenie świadomosci społeczeństwa.**

W ramach poszerzania zasięgu, pobudzania kreatywności i aktywności, Prezes Urzędu Ochrony Danych Osobowych inicjuje wydarzenia edukacyjne skierowane do odbiorców w różnym wieku – zarówno dzieci, młodzieży, osób dorosłych, jak i seniorów. Treścią skierowanych do nich wydarzeń były zagadnienia związane z ochroną dotyczących ich danych osobowych **w obliczu dynamicznego rozwoju technologii informatycznych i zagrożeń wynikających z nieumiejętnego korzystania z nich.**

Prezes UODO organizuje i współorganizuje takie wydarzenia, jak konferencje, seminaria, spotkania, a także przygotowuje publikacje, udziela porad prawnych, wywiadów dla przedstawicieli mediów, przygotowuje akcje edukacyjne z cyklu „UODO rusza w kraj", Dzień Ochrony Danych Osobowych oraz realizuje program edukacyjny dla szkół „Twoje dane – Twoja sprawa".

Działania te 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.

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 wspomnianej już **„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 przeprowadził 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:
- nieuprawniony dostęp do kont nauczycielskich w dziennikach elektronicznych;
- kradzież haseł dostępowych do dzienników elektronicznych;

- 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 szkolnej, 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 powinno 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[746].

Przykładem jest ww. program edukacyjny „**Twoje dane – Twoja sprawa**”, realizowany nieprzerwanie od 16 lat. Program adresowany jest nie tylko do uczniów i ich rodziców, nauczycieli czy przedstawicieli ośrodków doskonalenia nauczycieli, ale również do seniorów i środowisk lokalnych, przyczyniając się do pogłębienia współpracy z różnymi organizacjami i instytucjami.

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 kilka tysięcy lekcji i różnorodnych wydarzeń skierowanych do uczniów, nauczycieli, rodziców, seniorów i środowiska

[746] Art. 57.1.b RODO.

lokalnego. W każdej jego edycji bierze udział około kilkadziesiąt tysięcy uczniów, a kilka tysięcy nauczycieli zostaje zaangażowanych w działania związane z programem. Dla przykładu, w XV edycji Programu w roku szkolnym 2024/2025 odnotowano ponad 61 tysięcy uczniów uczestniczących w programie oraz zrealizowno ponad 6 tysięcy inicjatyw edukacyjnych z zakresu ochrony danych osobowych.

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.

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, w szczególności związanych z zastosowaniem w edukacji algorytmów sztucznej inteligencji.**

Jak pokazują przykłady, 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 inicjatywa Prezesa UODO związana z **ochroną wizerunku młodych sportowców.** W październiku 2025 r. UODO zorganizował 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. Celem konferencji było zwrócenie uwagi na odpowiedzialność placówek działających na rzecz dzieci i młodzieży, które z jednej strony aktywizują i wspierają

ich 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. Ważnym przesłaniem tego wydarzenia było wspieranie dzieci w budowaniu przekonania, że mają prawo do prywatności i prawo podejmowania decyzji w sprawach, które ich dotyczą.

Prezes UODO sformułował szereg wniosków pokonferencyjnych, w których zawarł istotne postulaty dotyczące zapewnienia skutecznej ochrony wizerunku młodych sportowców:

1. Niepublikowanie lub ograniczenie publikacji zdjęć młodych sportowców do 18 r. ż. Obecnie zbyt wiele informacji o tej grupie można znaleźć w internecie, w tym dane szczególnej kategorii.
2. Niedopuszczalność, aby warunkiem uczestnictwa w imprezie sportowej lub wejścia w poczet klubu sportowego było wyrażenie przez sportowca (pełnoletniego) lub jego rodziców w przypadku osoby niepełnoletniej, zgody na publikację wizerunku.
3. Prawo żądania korekty własnego wizerunku utrwalonego na zdjęciu lub prawo odmowy jego opublikowania.
4. Zakaz nieodpowiedniej modyfikacji wizerunku bez uprzedniej zgody sportowca (pełnoletniego) lub jego rodziców (gdy jest niepełnoletni).
5. Tworzenie baz danych zawierających dane dot. zdrowia sportowców (waga, wzrost), zawierających szeroki zakres danych i informacji o zdrowiu.
6. Doprecyzowanie w przepisach zasad dostępu do danych.
7. Doprecyzowanie okresu retencji danych, np. do czasu zakończenia nauki w szkole, przejścia do innego klubu sportowego, itd.
8. Zakaz stosowania (przez organizatorów imprez sportowych) w klauzulach zgody nieprecyzyjnych, niejasnych, szerokich pojęć, jak „udostępnianie nieograniczone czasowo, ilościowo, terytorialnie, wielokrotnie”; osoby trzecie, które uzyskują „stosowne upoważnienia” nieodpłatne „do wielokrotnego korzystania z wizerunku na wszystkich znanych polach eksploatacji”, tj. głosu, wyglądu, wypowiedzi w dowolnej liczbie egzemplarzy, itd.
9. Zbyt szeroki zakres danych opiekuna/rodzica w treści klauzuli zgody (wystarczy jego imię, nazwisko, adres, dane do kontaktu – bez podawania nr PESEL rodzica/opiekuna podpisującego klauzulę).
10. Prawo odmowy zgody na publikację wizerunku w wybranych akcjach marketingowych, reklamowych, promocyjnych (zwłaszcza gdy niekoniecznie są one bezpośrednio związane ze sportem, np. odżywki, napoje, kosmetyki…).

Równolegle organ nadzorczy prowadzi **działania legislacyjne – między innymi analizując i przygotowując opinie do projektów aktów prawnych dotyczące małoletnich.** Dla przykładu - wybrane opinie z 2025 r.

W odniesieniu do **projektu rozporządzenia MEN w sprawie sposobu nauczania szkolnego oraz zakresu treści dotyczących wiedzy o życiu seksualnym człowieka, o zasadach świadomego i odpowiedzialnego**

**rodzicielstwa, o wartości rodziny, życia w fazie prenatalnej oraz metodach i środkach świadomej prokreacji zawartych w podstawie programowej kształcenia ogólnego**[747] postulaty Prezesa UODO zostały uwzględnione. Mając na uwadze działania podejmowane przez MEN w związku z wprowadzeniem do szkół nowego przedmiotu „edukacja zdrowotna" ważne było, 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 zdobywali 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[748].

Dodatkowo, w opiniach legislacyjnych UODO dotyczących **obywatelskiego projektu ustawy o ochronie małoletnich przed treściami pornograficznymi w Internecie i o zmianie ustawy – Prawo telekomunikacyjne**[749] oraz **rządowego projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie**[750], organ nadzorczy odniósł się szczegółowo do zapewnienia wieku użytkownika, która miałaby chronić małoletnich przed treściami szkodliwymi. W opinii do projektu wskazałem na potrzebę stosowania przejrzystych, skutecznych i adekwatnych do wieku środków identyfikacji. W tym kontekście odwołaliśmy 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. W Oświadczeniu 1/2025 Europejska Rada Ochrony Danych podkreśliła, że skuteczne zapewnienie wieku w środowisku cyfrowym jest niezbędne do ochrony dzieci, ale musi być realizowane w sposób zgodny z RODO – w szczególności z **zasadą minimalizacji danych oraz koniecznością stosowania bezpiecznych i proporcjonalnych mechanizmów weryfikacji**[751].

W tym kontekście ważną rolę odgrywa **nowelizacja rozporządzenia eIDAS2**, które weszło w życie w maju 2024 r. Jego kluczowym elementem było wprowadzenie Europejskiego Portfela Tożsamości Cyfrowej – narzędzia, które umożliwi obywatelom potwierdzanie wybranych atrybutów (np. wieku) bez ujawniania pełnych danych

[747] DPNT 401.36.2025.
[748] 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.
[749] DPNT.401.13.2025.
[750] DPNT.401.59.2025.
[751] Materiał ten został udostępniony na stronie internetowej https://uodo.gov.pl/pl/537/3624. Dodatkowo opracowano i opublikowano uproszczoną grafikę prezentującą wspomniane zasady w przystępny sposób.

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 bezpieczeństwa dzieci w świecie cyfrowym. W związku z tym Urząd planuje organizację 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.

Urząd Ochrony Danych Osobowych działa na rzecz edukacji cyfrowej dzieci w ramach **Digital Education Working Group (DEWG), 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 około 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 wreszcie 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**”.**

Lista inicjatyw edukacyjnych Prezesa Urzędu Ochrony Danych Osobowych podejmowanych na rzecz ochrony danych osobowych dzieci i młodzieży 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.

Podkreślenia wymaga, że ww. informacje o działaniach edukacyjnych adresowanych do najmłodszych członków społeczeństwa, Prezes UODO przekazywał **sejmowej Komisji do Spraw Dzieci i Młodzieży (DIM)**, w posiedzeniach której

aktywnie uczestniczył. Zagadnienia, które były tematem posiedzeń komisji DIM dotyczyły:

- prowadzonych spraw z zakresu sytuacji dzieci i młodzieży w cyberkonfliktach – odporność placówek oświatowych, organizacji społecznych zajmujących się dziećmi i młodzieżą: ochrona danych osobowych, liczba i rodzaje cyberataków, inne specyficzne wyzwania (5.05.2025 r.);
- prezentacja zaktualizowanych danych z raportu oraz inicjatywy monitoringu aktywności dzieci w środowisku cyfrowym pt. „Internet dzieci" (6.11.2025 r.);
- technologia deepfake – wyzwania i konieczne regulacje w kontekście ochrony wizerunku" (17.12.2025 r.).

W odniesieniu do **technologii deepfake'ów** Prezes UODO wyraził opinię, że obowiązujące w polskim porządku prawnym regulacje nie są dostosowane do specyfiki technologii deepfake i treści generowanych przez sztuczną inteligencję. Nie zapewniają także możliwości skutecznego przeciwdziałania negatywnemu ich oddziaływaniu na ludzi. Sama technologia wydaje się być neutralna, jednak łatwy do niej dostęp oraz skuteczność w wykorzystywaniu jej do różnych celów, nierzadko niezgodnych z prawem i etyką, może prowadzić do naruszeń praw i wolności ludzi na niespotykaną dotąd skalę – kradzież tożsamości, szantaż, nękanie (wskutek ukazywania osoby w sytuacjach, które w rzeczywistości nie miały miejsca), oszustwa, preparowanie dowodów sądowych, manipulacji politycznej (w szczególności podczas prowadzenia kampanii wyborczej), polaryzacji społecznej, może też wpływać na nastroje społeczne i doprowadzić do zamieszek, być zagrożeniem dla bezpieczeństwa systemów informacji podmiotów publicznych i prywatnych, a w konsekwencji dla bezpieczeństwa narodowego.

Niezbędne jest zatem wprowadzenie przepisów prawa, które będą bezpośrednio odnosić się do rozpowszechniania szkodliwych treści w postaci deepfake'ów. Stanowisko w tej sprawie Prezes UODO przedstawił w wystąpieniu do wicepremiera i ministra cyfryzacji Krzysztofa Gawkowskiego, w którym przywołał przypadki dotychczas zgłaszanych do organu nadzorczego nadużyć, spowodowanych stosowaniem technologii deepfake:

1) **sprawa skargi dziennikarki** dotyczącej zamieszczenia na portalach społecznościowych fałszywych informacji o jej śmierci, a także o tym, że została pobita przez męża czy że trafiła do więzienia. W tej sprawie Prezes UODO wydał postanowienie zobowiązujące spółkę Meta Platforms Ireland Limited do wstrzymania na 3 miesiące (maksymalny termin przewidziany prawem) wyświetlania na terytorium RP na Facebooku i Instagramie, fałszywych reklam wykorzystujących prawdziwe dane oraz wizerunek dziennikarki oraz Rafała Brzoski. W marcu 2025 r. firma Meta wycofała skargi na postanowienia UODO w tej sprawie; w konsekwencji WSA w Warszawie umorzył postępowanie. Skutkiem tego wyroku, Meta Platforms Ireland Limited**,** wdrożyła narzędzia mające na celu ochronę wizerunku znanych osób oraz użytkowników mediów społecznościowych przed oszustwami reklamowymi wykorzystywanymi przez wyłudzaczy.

Rozwiązanie to oparte jest na bezpiecznej, odrębnej bazie danych opracowanej na podstawie profili znanych osób utworzonych na platformach społecznościowych Meta. Jeśli obraz zawarty w bazie danych zostanie wykryty w zeskanowanej reklamie, zostanie zainicjowana odpowiednia procedura, po której materiał zostanie usunięty. Narzędzie to ma na celu wzmocnienie ochrony zarówno osób, których wizerunek jest wykorzystywany, jak i użytkowników, którzy pod wpływem takich informacji mogą przekazywać swoje dane lub pieniądze oszustom. Użytkowników, którzy są zaniepokojeni niewłaściwym wykorzystaniem ich danych w reklamach typu „celeb bait", zachęca się do zgłoszenia problemu Meta, klikając trzy kropki obok takiej, pojawiającej się reklamy, wybierając „Zgłoś reklamę" i postępując zgodnie z instrukcjami wyświetlanymi na ekranie.

2) **sprawa wygenerowania przez uczniów szkoły podstawowej fałszywego zdjęcia nagiej koleżanki oraz zachęcania innych osób do jego zamawiania na platformie Instagram.** W mojej ocenie sprawcy mogli dopuścić się modyfikowania oraz następczego ujawnienia wizerunku małoletniej koleżanki, co może zostać uznane za przetwarzanie danych osobowych w postaci wizerunku tej osoby w sytuacji, gdy nie jest to dopuszczalne. Takie działanie może również zostać określone jako produkowanie, posiadanie oraz rozpowszechnianie treści pornograficznych z udziałem rzeczywistej osoby w wieku poniżej lat 18. W tej sprawie Prezes UODO zawiadomił Policję o możliwości popełnienia przestępstwa**,** jednak Policja odmówiła zajęcia się sprawą.
3) **sygnały od lekarzy, którzy padli ofiarą oszustów korzystających z technologii deepfake.** Ich wizerunki i autorytet zostały wykorzystane w nieprawdziwych reklamach, w których medycy mieli zachęcać do przyjmowania określonych preparatów.

Jednakże przepisy prawa w obecnym kształcie **nie zapewniają dostatecznej ochrony przed deepfake'ami** m.in. dlatego, że nie odnoszą się wprost do specyfiki tej technologii. Przepisy ustawy o prawie autorskim i prawach pokrewnych wymagają zgody na rozpowszechnianie wizerunku, a Kodeks cywilny reguluje ochronę dóbr osobistych, w tym wizerunku i głosu. Z kolei RODO traktuje wizerunek jako dane osobowe wymagające ochrony. Jeśli weźmiemy pod uwagę Kodeks karny to wykorzystanie deepfake'a może wypełniać znamiona np. czynu zabronionego kradzieży tożsamości (art. 190a § 2), zmuszania do określonego zachowania (art. 191), rozpowszechnienia wizerunku nagiej osoby bez zgody (art. 191a), publicznej prezentacji lub produkcji, rozpowszechniania, przechowywania i posiadania treści pornograficznych (art. 202), zniesławienia lub zniewagi (art. 212 i 216) lub oszustwa (art. 286). Z kolei akt w sprawie sztucznej inteligencji wprowadził w art. 50 ust. 4 wymóg oznaczania treści deepfake jako „sztucznie generowane lub zmanipulowane".

Żadna z wymienionych regulacji prawnych nie zapewnia narzędzi do pełnej i skutecznej ochrony przed skutkami nadużyć związanych z deepfake'ami; nie gwarantuje np. szybkiego usuwania nielegalnych materiałów. Tymczasem skutki tych

nadużyć we współczesnym świecie zdominowanym przez internet i media społecznościowe są niezwykle dotkliwe (zwłaszcza gdy ofiarami są osoby małoletnie), identyfikowanie twórców deepfake'ów jest często bardzo utrudnione, procedury sądowe trwają zbyt długo, a brak szczegółowych przepisów odnoszących się wprost do deepfake'ów dodatkowo utrudnia ściganie sprawców i skuteczne dochodzenie praw przez ofiary.

Prezes UODO wyraził pilną potrzebę zainicjowania prac, których celem będzie wprowadzenie w polskim porządku prawnym przepisów w pełni regulujących odpowiedzialność prawną za rozpowszechnianie fałszywych treści w postaci deepfake'ów, zapewnienie skutecznej ochrony danych osobowych oraz wsparcie dla ofiar cyberprzestępców. Ochrona prywatności i bezpieczeństwa w dobie deepfake'ów wymaga bowiem kompleksowych działań na poziomie technologicznym, prawnym, edukacyjnym i psychologicznym.

Przykłady niezbędnych rozwiązań dotyczących ochrony prawnej przed szkodliwymi deepfake'ami:

- zobowiązanie platform technologicznych, internetowych oraz społecznościowych do instalowania systemów automatycznego i skutecznego wykrywania oraz oznaczania deepfake'ów;
- wspieranie działań oddolnych, polegających na wypracowaniu standardów oraz dobrych praktyk w zakresie weryfikacji autentyczności treści, oznaczania fałszywych materiałów i reagowania na zgłoszenia użytkowników;
- można też rozważyć wprowadzenie w krajowym systemie prawa rozwiązań podobnych do kodeksów postępowania, przewidzianych w rozporządzeniu 2016/679;
- wsparcie ofiar cyberprzestępstw opartych na deepfake'ach poprzez stworzenie dla nich specjalnych programów pomocy psychologicznej;
- opracowanie szczegółowych zasad ponoszenia odpowiedzialności karnej i odszkodowawczej osób tworzących i rozpowszechniających szkodliwe deepfake'i;
- doprecyzowanie obowiązków podmiotów administrujących platformami internetowymi;
- osoby, których dane osobowe (np. wizerunek) zostały wykorzystane w fałszywych materiałach, powinny mieć możliwość szybkiego i łatwego zgłaszania naruszeń, żądania natychmiastowego usunięcia treści z platform online oraz uzyskania zadośćuczynienia za poniesione szkody.

W kontekście odpowiedzialności witryn internetowych za treści publikowane na ich stronach wypowiedział się Trybunał Sprawiedliwości Unii Europejskiej, który w wyroku z 2 grudnia 2025 r. (C-492/23) w sprawie **serwisu Russmedia** orzekł, że operator internetowej platformy handlowej, jako administrator danych osobowych zawartych w ogłoszeniach publikowanych na jego stronie, powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby przed opublikowaniem ogłoszenia

można było sprawdzić, czy zawierają dane szczególnych kategorii (np. dane o poglądach, seksualności czy dotyczących zdrowia). A jeżeli ogłoszenie czy reklama zawiera takie dane, to operator takiej strony ma obowiązek zweryfikować czy są to dane reklamodawcy lub ogłoszeniodawcy. W przeciwnym razie osoba zamieszczająca wpis z danymi innej osoby musi wykazać, że dysponuje zgodą osoby, której dane dotyczą. W przypadku, gdy oba te warunki nie są spełnione, operator takiej strony powinien uniemożliwić publikację takiego ogłoszenia czy reklamy.

Treść tego wyroku daje solidne podstawy domagania się od dostawców usług internetowych wdrożenia środków technicznych i organizacyjnych pozwalających identyfikować ogłoszenia zawierające dane szczególnych kategorii oraz zweryfikować, czy użytkownik, który zamierza opublikować takie ogłoszenie, jest osobą, której dane dotyczą.

Wyrok ten ma ogromne znaczenie dla serwisów internetowych, w tym mediów społecznościowych. Serwisy tego typu nie mogą się teraz tłumaczyć, że nie mają wpływu na treść ogłoszeń czy postów z danymi. Nie mogą zasłaniać się tym, że jedynie świadczą usługę „hostingowania" ogłoszeń. Dostarczają bowiem odpowiednie narzędzia do publikacji danych, a więc decydują o tym, w jaki sposób mogą być np. wyświetlane. Biorąc pod uwagę powszechne zjawisko tzw. „celeb bait", a więc wykorzystywania danych, w tym wizerunku, znanych sposób do generowania fałszywych reklam, właściciele mediów społecznościowych będą musieli zweryfikować czy publikując daną treść mają zgodę osoby, której dane ujawniają, na przetwarzanie jej danych. Jeżeli zgody nie ma, to publikacja nie może być możliwa. To rozwiązanie uchroni nie tylko np. znane osoby przed bezprawnym wykorzystywaniem ich wizerunku, ale i użytkowników mediów społecznościowych przed narażeniem się np. na straty finansowe. Często takie nieprawdziwe reklamy czy ogłoszenia zachęcają do ryzykownych inwestycji, co najczęściej wiąże się ze stratami finansowymi albo do wyłudzeniem danych od internautów do celów przestępczych.

Jest to szczególnie ważny wyrok, w obliczu braku na poziomie unijnym przepisów dotyczących zwalczania deepfake'ów.

Dotychczas Unia Europejska nie wprowadziła jednolitych regulacji dotyczących środków ochrony prawnej przed szkodliwymi deepfake'ami, co utrudnia egzekwowanie odpowiedzialności. Wobec tego państwa członkowskie we własnym zakresie podejmują próby dostosowywania prawa do szybko zmieniającej się rzeczywistości technologicznej. I takie zadanie stoi również przed polskim ustawodawcą.

Ważnym krokiem w polskiej legislacji było przyjęcie **nowelizacji ustawy o świadczeniu usług drogą elektroniczną,** która wprowadza do polskiego porządku prawnego przepisy Aktu o usługach cyfrowych (DSA). Dzięki ustawie wprowadzającej założenia DSA, nagminne publikowanie fałszywych treści, w tym materiałów typu deepfake, może zostać skuteczniej ograniczone. I choć nie wyeliminuje to problemu w całości, stanowi jednak istotny krok w kierunku realnego wzmocnienia ochrony prawnej i odpowiedzialności w przestrzeni cyfrowej. Celem zmian jest stworzenie

bezpieczniejszego i bardziej przejrzystego środowiska cyfrowego zgodnego z europejskimi standardami.

Podsumowując, obecne ramy prawne Unii Europejskiej, w tym akt w sprawie sztucznej inteligencji, oraz polskie przepisy krajowe, takie jak Kodeks cywilny, Kodeks karny czy prawo autorskie zapewniają jedynie wybiórczą i niewystarczającą odpowiedź na wielopłaszczyznowe zagrożenia ze strony tej technologii. Konieczne jest wprowadzenie w polskim porządku prawnym przepisów, które będą regulować odpowiedzialność prawną za rozpowszechnianie fałszywych treści w postaci deepfake'ów, a także zapewnią skuteczną ochronę danych osobowych. Urząd Ochrony Danych Osobowych oferuje wsparcie eksperckie dla tych zadań, w zakresie oceny zgodności przyjmowanych w tym zakresie regulacji z przepisami prawa ochrony danych osobowych.

Postęp technologiczny, w tym rozwój sztucznej inteligencji, musi uwzględniać prawa i bezpieczeństwo obywateli oraz odpowiedzialność instytucji publicznych i prywatnych w budowaniu zaufania i odporności społecznej. Ogromną rolę odgrywa tu **edukacja**, gdzie poprzez budowanie świadomości i kompetencji dotyczących zagrożeń związanych z deepfake'mi, sposobów rozpoznawanie fałszywych treści oraz rozwijanie i doskonalenie umiejętności obrony przed nimi, można skutecznie zawalczyć z tym zjawiskiem. Kluczowe jest więc budowanie społecznej odporności na manipulacje ze strony sztucznej inteligencji.

Przykładem jest opisany już wcześniej **ogólnopolski program edukacyjny UODO „Twoje dane – Twoja sprawa".** Podczas wielu wydarzeń z lat 2024-2025 organizowanych w ramach tego Programu, omawiana była problematyka *deepfake* w kontekście ochrony danych osobowych i bezpieczeństwa w sieci:

- #ODOlekcja czyli lekcja o ochronie danych osobowych dla uczniów szkół ponadpodstawowych: *„Deepfake: fałszywa rzeczywistość w sieci – czy jesteś na to gotowy?"* (31.01.2024 r.);
- szkolenie otwierające XV edycję programu *„Twoje dane – Twoja sprawa"* (24–25.10.2024 r.);
- przygotowany został materiał w ramach cyklu porad *„Warto wiedzieć"* dla uczniów pt. *„Ryzyko udostępniania wizerunku dzieci w sieci"* (**grudzień 2024 r.);**
- konferencja szkoleniowa *„Prywatność i sztuczna inteligencja w edukacji"*, inaugurująca XVI edycję programu „Twoje dane – Twoja sprawa*"* (22–23.10.2025 r.);
- webinarium Prezesa UODO dla uczniów szkół podstawowych i ponadpodstawowych: *„Twój wizerunek i Twoje dane – jak nie stracić kontroli, korzystając z nowych aplikacji?" (*20.11.2025 r.).

Przestrzenią do poważnych rozmów z młodzieżą na temat cyberbezpieczeństwa w związku z rozwojem technologii cyfrowych, był festiwal **Pol'and'Rock, podczas którego Urząd Ochrony Danych Osobowych zorganizował warsztaty na temat sztucznej inteligencji oraz punkt konsultacyjny.**

O ochronie danych, w tym wizerunku w kontekście sztucznej inteligencji eksperci UODO mówili również podczas spotkania z dziećmi z Paczkowa poszkodowanymi w powodzi, które zorganizowała Fundacja „Odzyskaj siebie" (27.09.2025), ze studentami Akademii Leona Koźmińskiego w ramach obchodów XIX Dnia Ochrony Danych Osobowych (13.01.2025 r.), a także podczas „Lekcji o finansach", które w amach programu Ministerstwa Finansów, trzykrotnie odbyły się w siedzibie UODO.

Ponadto Prezes UODO współpracuje z Rzeczniczką Praw Dziecka w zakresie inicjatyw edukacyjnych i badawczych dotyczących ochrony danych osobowych dzieci i młodzieży, a także z Fundacją Orange i samorządami prawniczymi.

W ramach współpracy z różnymi środowiskami, UODO organizuje własne oraz wspiera inicjatywy edukacyjne innych podmiotów na rzecz budowania kultury ochrony danych osobowych wśród dzieci i młodzieży oraz środowiska lokalnego. U podłoża współpracy leży przekonanie o konieczności wypracowania wspólnej strategii przeciwdziałania zagrożeniom, ograniczenie skali i dotkliwości nadużyć związanych z deepfake'ami, fake nude, celeb bait czy ogólnie - z nieuprawnionym wykorzystaniem wizerunku. Niekontrolowane wykorzystywanie tych technologii z użyciem sztucznej inteligencji, stanowi bowiem poważne zagrożenie dla praw jednostki, demokracji oraz bezpieczeństwa i zaufania publicznego.

Konieczne jest również pochylenie się nad tematem związanym z wykorzystywaniem **systemów sztucznej inteligencji w edukacji.** W opinii organu takie narzędzia jak adaptacyjne platformy edukacyjne, czy generatywne aplikacje AI, takie jak ChatGPT, zmieniają oblicze sal lekcyjnych na całym świecie. Chociaż technologie te oferują potencjalne korzyści, takie jak spersonalizowane nauczanie i efektywność administracyjną, to stwarzają również poważne zagrożenia – zwłaszcza dla praw dzieci, ochrony ich prywatności i danych osobowych, równości w edukacji i wartości demokratycznych.

Obecne ramy regulacyjne nie uwzględniają w wystarczającym stopniu zarówno wrażliwości dzieci, specyfiki ich rozwoju poznawczego ani też szczególnych wyzwań związanych ze środowiskiem edukacyjnym. Większość systemów sztucznej inteligencji wykorzystywanych w edukacji nie jest przyjazna dzieciom, nie zostały bowiem przetestowane na szeroką skalę i są coraz częściej wdrażane do infrastruktury cyfrowej szkół i uniwersytetów bez odpowiedniego nadzoru – i to w szybkim tempie, często bez solidnych zabezpieczeń lub przejrzystej oceny. Technologie te obejmują adaptacyjne systemy nauczania, analitykę predykcyjną, zautomatyzowane narzędzia do nadzorowania egzaminów oraz generatywne narzędzia do tworzenia treści opartych na sztucznej inteligencji. Chociaż są one promowane jako środki poprawiające wyniki nauczania, budzą uzasadnione obawy, wymienione poniżej:

- brak niezależnych badań: brak analizy ryzyka zastosowania sztucznej inteligencji w edukacji, nie ma rzetelnej i niezależnej oceny bezpieczeństwa, skuteczności ani skutków długoterminowego wpływu sztucznej inteligencji w środowisku edukacyjnym; narzędzia są często wprowadzane w oparciu

o niepotwierdzone twierdzenia lub promocję komercyjną, a nie o rzetelne badania;

- erozja praw dziecka: dzieci są szczególnie narażone ze względu na swoją niedojrzałość rozwojową i brak zdolności do samodzielnego podejmowania decyzji, wiele systemów sztucznej inteligencji nie jest projektowanych z uwzględnieniem danych, potrzeb ani praw dzieci i może nieumyślnie powodować szkody psychologiczne, poznawcze lub społeczne;
- przejrzystość i odpowiedzialność: systemy sztucznej inteligencji stosowane w szkołach często działają w sposób nieprzejrzysty, co utrudnia nauczycielom, rodzicom, a nawet decydentom zrozumienie procesów decyzyjnych lub ograniczenie ryzyka;
- wpływy komercyjne: interesy komercyjne często dyktują projektowanie i wdrażanie narzędzi sztucznej inteligencji, co może skutkować niezgodnością priorytetów, w tym inwazyjnymi praktykami w zakresie ochrony danych osobowych, nadmiernym poleganiem na automatyzacji i podważaniem uczciwości badawczej;
- cyfrowa przepaść: wykorzystanie sztucznej inteligencji w edukacji może pogłębiać nierówności, zwłaszcza w przypadku uczniów niepełnosprawnych, pochodzących ze środowisk znajdujących się w niekorzystnej sytuacji społeczno-ekonomicznej oraz posługujących się językami mniejszościowymi; koszty, wymagania infrastrukturalne i ograniczenia językowe często wykluczają grupy marginalizowane;

Sposobem regulacji systemów sztucznej inteligencji w edukacji jest prawnie wiążący instrument międzynarodowy opracowany przez Radę Europy, dyskutowany podczas konferencji RE z cyklu Artificial Inteligence and Education, której trzecia edycja odbyła się 18-19 października 2025 r. w Strasburgu. Podstawowe założenia tej regulacji obejmują następujące wskazania:

- priorytetowe traktowanie praw człowieka: zapewnienie, aby aplikacje sztucznej inteligencji przestrzegały praw dzieci, w tym prawa do prywatności, swobody działania, wolności myśli i ochrony przed krzywdą, zgodnie z postanowieniami Konwencji ONZ o Prawach Dziecka i Europejskiej Konwencji Praw Człowieka;
- przejrzystość i nadzór: wymaganie od twórców sztucznej inteligencji i instytucji edukacyjnych ujawnienia sposobu działania systemów sztucznej inteligencji, w tym źródeł danych, algorytmów i procesów decyzyjnych; nieodłącznym elementem byłyby także niezależne audyty;
- skuteczne i bezpieczne narzędzia edukacyjne oraz odpowiedzialność: przestrzeganie etycznych standardów zamówień publicznych i jasny podział odpowiedzialności za szkody spowodowane niewłaściwym wykorzystaniem sztucznej inteligencji;
- ochrona demokratycznego uczestnictwa i celów edukacyjnych: podkreślenie roli edukacji w promowaniu demokratycznego, krytycznego myślenia

i autonomii uczniów; zapobieganie automatyzacji myślenia pedagogicznego w sposób, który ogranicza ludzką sprawczość i utrwala szkodliwe uprzedzenia.

Rolą sprawiedliwej edukacji jest zmniejszenie przepaści cyfrowej poprzez zapewnienie placówkom edukacyjnym dostępu do systemów sztucznej inteligencji, integracyjności językowej i kulturowej oraz dostosowanie do potrzeb osób uczących się, które są niepełnosprawne lub pochodzą ze środowisk defaworyzowanych.

Inicjatywy edukacyjne Prezesa UODO wpisują się w zakreślony powyżej kierunek niezbędnych działań na rzecz podnoszenia świadomości w zakresie prawidłowego wykorzystania sztucznej inteligencji w edukacji. Podjęte w tym obszarze działania Prezesa UODO opierają się w dużej mierze na współpracy z wieloma podmiotami zaangażowanymi w tej proces. Współpraca z Ministerstwem Edukacji, Rzeczniczką Praw Dziecka, sejmową Komisją do spraw Dzieci i Młodzieży oraz z różnymi fundacjami i stowarzyszeniami, pozwala na szeroką perspektywę w podejściu do usług cyfrowych adresowanych do najmłodszych członków społeczeństwa.

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.

UODO będzie nadal wspierać inicjatywy edukacyjne i prowadzić działania na rzecz budowania kultury ochrony danych osobowych wśród uczniów, nauczycieli, rodziców i środowiska lokalnego. Troska o prawa dzieci do prywatności i ochrony ich danych osobowych pozostaje jednym z kluczowych priorytetów działalności Urzędu Ochrony Danych Osobowych. Walka o podmiotowość i prawa człowieka – w szczególności w odniesieniu do najmłodszych – stanowi bowiem główny kierunek polityki edukacyjnej realizowanej przez UODO.

W podsumowaniu aktywności organu na polu edukacji należy wskazać, że celem wszystkich inicjatyw edukacyjnych Prezesa UODO – zarówno zrealizowanych, jak i planowanych - oraz udziału jego ekspertów w wydarzeniach edukacyjnych organizowanych przez inne podmioty, było podkreślenie wagi ochrony danych osobowych, które służy:

- **ochronie prywatności i godności jednostki** – dane osobowe dotyczą bezpośrednio człowieka, jego życia prywatnego, zdrowia, finansów czy relacji społecznych. Ich właściwa ochrona pozwala zachować kontrolę nad własną tożsamością i prywatnością;
- **zapobieganiu nadużyciom i przestępstwom –** niewłaściwe wykorzystanie danych może prowadzić do kradzieży tożsamości, oszustw finansowych, wyłudzeń czy cyberataków. Silna ochrona zmniejsza to ryzyko;

- **budowie zaufania społecznego i biznesowego** – klienci, pracownicy i obywatele chętniej korzystają z usług instytucji i firm, które odpowiedzialnie przetwarzają dane i dbają o ich bezpieczeństwo;
- **zapewnieniu zgodności przetwarzania danych z przepisami prawa** – regulacje takie jak RODO nakładają obowiązki na organizacje i instytucje, a ich przestrzeganie chroni przed sankcjami prawnymi i finansowymi;
- **wzmacnianiu odpowiedzialności organizacji** – ochrona danych wymusza tworzenie procedur bezpieczeństwa, szkolenie pracowników i świadome zarządzanie informacją;
- **ochronie godności i praw człowieka** – prawo do ochrony danych osobowych jest związane z podstawowymi prawami człowieka, w tym prawem do prywatności i autonomii informacyjnej;
- **zapewnieniu bezpieczeństwa w środowisku cyfrowym** – w dobie cyfryzacji, mediów społecznościowych i usług online coraz większa ilość danych trafia do sieci, dlatego ich ochrona staje się niezbędna dla bezpiecznego funkcjonowania społeczeństwa.

W odniesieniu do planowanych działań edukacyjnych organu podkreślenia wymaga ważna inicjatywa Senatu RP, który podjął uchwałę ustanawiającą 2027 rok **Rokiem Świadomości i Bezpieczeństwa Informacyjnego.** Cel tej inicjatywy, którym jest zwiększenie kompetencji cyfrowych, walka z dezinformacją oraz poprawa bezpieczeństwa informacyjnego społeczeństwa, wpisuje się w zadania edukacyjno-informacyjne organu do spraw ochrony danych osobowych, który w oparciu o współpracę z podmiotami zaangażowanymi w edukację w Polsce i na świecie, podejmuje działania na rzecz podnoszenia świadomości i uczenia krytycznego myślenia w świecie zautomatyzowanych mediów.

Prezes Mirosław Wróblewski zadeklarował Pani Marszalek Małgorzacie Kidawie-Błońskiej swoje pełne poparcie dla tej inicjatywy, gotowość Urzędu Ochrony Danych Osobowych do współpracy z Senatem i podjęcie wspólnych inicjatyw edukacyjno – informacyjnych. W piśmie do Pani Marszałek zakreślił możliwe obszary współpracy UODO z Senatem:

- ramach programu edukacyjnego UODO „Twoje dane – Twoja sprawa”, poprzez organizację wspólnych wydarzeń tematycznych, jak konferencje, wykłady, szkolenia, warsztaty edukacyjne, a także konkursy dla uczniów i konkursy na najlepszą inicjatywę edukacyjną szkół, które co roku organizowane są w ramach tego programu. Ich uwieńczeniem byłaby Gala Finałowa Konkursów Prezesa UODO organizowanych w kolejnej, XVII edycji programu w roku szkolnym 2026/2027.
- cykliczne wykłady na temat bezpieczeństwa online i praw cyfrowych oraz odpowiedzialnego korzystania z narzędzi komunikacji elektronicznej, dla różnych grup społecznych. Wykłady odbywałyby się przy wsparciu merytorycznym ekspertów Urzędu Ochrony Danych Osobowych i Społecznego Zespołu Ekspertów przy Prezesie UODO, a także

- wspólna praca nad opracowaniem kalendarium wydarzeń Roku Świadomości i Bezpieczeństwa Informacyjnego, które zawierać będzie propozycje działań edukacyjnych służących rozwijaniu kompetencji medialnych, cyfrowych i informacyjnych, skierowanych do wszystkich grup społecznych i wiekowych.

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.

# VI. Podsumowanie

W 2025 r. działania Prezesa UODO koncentrowały się wokół kilku wiodących tematów, w tym postępującej cyfryzacji i rozwoju sztucznej inteligencji, ochrony danych osobowych dzieci, ochrony danych dotyczących zdrowia, poprawy jakości stanowionego prawa oraz wzmacniania rozliczalności administratorów. Istotny wymiar systemowy miały także działania obszarze ochrony danych osobowych podejmowane także na rzecz zapewnienia praworządności, skutecznej ochrony sądowej oraz dostosowania zasad dostępu organów publicznych do danych do standardów wynikających z prawa Unii Europejskiej i orzecznictwa sądów europejskich.

## 1. Nowe technologie i ochrona dzieci

### Technologiczny wymiar zgodności

W 2025 r. technologiczny wymiar ochrony danych był widoczny przede wszystkim w opiniach Prezesa UODO dotyczących regulacji i przedsięwzięć informatycznych. Organ wymagał, aby cyfryzację poprzedzały testy prywatności lub oceny skutków dla ochrony danych, analiza niezbędności i proporcjonalności oraz określenie celów systemu, zakresu danych, zasobów objętych dostępem, środków kontroli i odpowiedzialności poszczególnych podmiotów. Przykładowo, w projekcie SDD 1.0, służącym prowadzeniu postępowań dyscyplinarnych w samorządzie komorniczym, pozytywnie oceniono testy prywatności przewidziane na kolejnych etapach wdrożenia i trójwarstwowy model ochrony informacji. W projekcie voicebota dla ochrony zdrowia Prezes UODO zakwestionował natomiast brak określenia warunków i celów działania asystenta, pozyskiwanych danych oraz zasobów, do których system miał uzyskać dostęp.

Działania te potwierdziły, że zgodność systemu cyfrowego nie może być oceniana wyłącznie na podstawie deklarowanego celu i podstawy prawnej. Przy profilowaniu, analizie behawioralnej i przetwarzaniu dużych zbiorów danych konieczne jest zbadanie faktycznego sposobu działania technologii, w tym możliwości wygenerowania danych osobowych przez połączenie informacji uznawanych

oddzielnie za anonimowe. Ocena powinna łączyć RODO z wymaganiami cyberbezpieczeństwa, zarządzania danymi i regulacji usług cyfrowych oraz obejmować cały cykl projektowania i wykorzystywania systemu.

Praktyczny charakter miało także zaangażowanie UODO w rozbudowę systemu S46 w obszarze krajowego systemu cyberbezpieczeństwa w związku z wdrażaniem dyrektywy NIS 2. Planowane umożliwienie zgłaszania za jego pośrednictwem również naruszeń ochrony danych ma utworzyć wspólny kanał notyfikacji incydentów, ograniczyć obciążenia administratorów i usprawnić współpracę organów odpowiedzialnych za bezpieczeństwo cyfrowe. W tym zakresie należy podkreślić, że UODO zawarł specjalne porozumienie z Ministrem Cyfryzacji, określające zasady współpracy między organami państwa.

**AI w edukacji i deepfake**

Ochronę dzieci przed ryzykiem związanym z AI podejmowano w 2025 r. podczas konferencji, webinariów i warsztatów oraz we współpracy z Ministerstwem Edukacji, Rzeczniczką Praw Dziecka i sejmową Komisją do Spraw Dzieci i Młodzieży. Prezes UODO zwracał uwagę, że adaptacyjne platformy edukacyjne, analityka predykcyjna, automatyczny nadzór nad egzaminami i narzędzia generatywne są wdrażane bez dostatecznych badań, przejrzystości i nadzoru. Praktyczny standard powinien obejmować analizę ryzyka, przejrzystość źródeł danych i procesów decyzyjnych, niezależne audyty, jasny podział odpowiedzialności i zachowanie kontroli człowieka.

W grudniu 2025 r. Prezes UODO przedstawił problem deepfake'ów sejmowej komisji oraz wystąpił do ministra cyfryzacji o podjęcie prac nad regulacjami zapewniającymi skuteczną ochronę ofiar. Działania te wynikały m.in. ze spraw fałszywych reklam wykorzystujących wizerunek, wygenerowania nagiego wizerunku małoletniej oraz sygnałów od lekarzy, których wizerunki wykorzystano w oszustwach. Postulaty obejmowały wykrywanie i oznaczanie deepfake'ów, szybkie zgłaszanie i usuwanie treści, doprecyzowanie odpowiedzialności platform i twórców oraz wsparcie ofiar. Akt w sprawie sztucznej inteligencji wprowadza obowiązek oznaczania takich treści, a DSA może wzmacniać odpowiedzialność w środowisku usług cyfrowych, lecz przepisy te nie rozwiązują wszystkich pojawiających się problemów..

**Zapewnienie wieku, ochrona wizerunku i edukacja cyfrowa**

W opiniach dotyczących projektów aktów prawnych mających chronić małoletnich przed treściami szkodliwymi Prezes UODO podkreślał, że weryfikacja (zapewnienie) wieku musi być skuteczna, przejrzysta, proporcjonalna i zgodna z zasadą minimalizacji danych. Odwoływał się przy tym do Oświadczenia EROD 1/2025 oraz możliwości wynikających z eIDAS2 i Europejskiego Portfela Tożsamości Cyfrowej, pozwalających potwierdzić atrybut wieku bez ujawniania pełnej tożsamości.

Ochrona dzieci w środowisku cyfrowym obejmowała również zasady wykorzystywania ich wizerunku. W odniesieniu do młodych sportowców formułowano postulaty ograniczenia publikowania zdjęć, zakazu uzależniania udziału w zawodach

lub klubie od zgody na rozpowszechnianie wizerunku oraz precyzyjnego określenia zasad dostępu do danych i okresów ich przechowywania.

Uzupełnieniem rozwiązań prawnych i technicznych pozostają działania edukacyjne UODO. Program „Twoje dane – Twoja sprawa" obejmuje co roku około kilka tysięcy lekcji i wydarzeń, kilkadziesiąt tysięcy uczniów i kilka tysięcy nauczycieli. Od września 2025 r. ochrona danych została uwzględniona – na wniosek Prezesa UODO – również w programie przedmiotów takich, jak edukacja obywatelska i edukacja zdrowotna w szkołach podstawowych, a dalszy rozwój programu ma koncentrować się na bezpiecznym korzystaniu z usług cyfrowych i narzędzi AI.

**Odporność cyfrowa placówek oświatowych**

Zgodnie z planem kontroli sektorowych Prezes UODO kontrolował w 2025 r. administratorów przetwarzających dane dzieci. Działaniom tym towarzyszyła analiza zgłoszeń dotyczących szkół: przejęć kont nauczycieli, kradzieży haseł do dzienników elektronicznych, publikowania dokumentów na publicznych platformach i ataków ransomware. Powtarzające się problemy obejmowały brak procedur i szkoleń, korzystanie z prywatnych skrzynek oraz niedostateczne stosowanie uwierzytelniania dwuskładnikowego i szyfrowania. Wnioski miały bezpośredni wymiar praktyczny: szkoły powinny zapewniać służbowe kanały komunikacji, zarządzać dostępem i regularnie szkolić pracowników z cyberhigieny.

## 2. Dane dotyczące zdrowia

Ochrona danych dotyczących zdrowia pozostawała jednym z najistotniejszych obszarów działalności Prezesa UODO, zarówno w postępowaniach skargowych i naruszeniowych, jak i w opiniowaniu projektowanych rozwiązań cyfrowych oraz działaniach edukacyjnych. Podejmowane sprawy dotyczyły przede wszystkim legalności dostępu do danych, ograniczenia ich zakresu oraz kontroli nad dalszym wykorzystywaniem informacji medycznych. Skargi odnosiły się m.in. do dostępu lekarzy bez podstawy prawnej do danych zgromadzonych na Platformie Usług Elektronicznych ZUS, przetwarzania danych przy wystawianiu e-recept oraz publikowania w internecie danych osób wykonujących zawody medyczne. W pracach nad elektroniczną dokumentacją medyczną Prezes UODO m.in. zakwestionował przetwarzanie numeru PESEL wystawcy dokumentu oraz przekazywanie pełnej dokumentacji służbom statystyki publicznej.

**Europejska przestrzeń danych dotyczących zdrowia (EHDS)**

Problemy związane z dostępem do dokumentacji medycznej i jej dalszym wykorzystywaniem nabierają szczególnego znaczenia w związku z wdrażaniem rozporządzenia 2025/327 w sprawie EHDS. Ma ono ułatwić wymianę elektronicznych danych zdrowotnych w Unii Europejskiej oraz wspierać opiekę zdrowotną, zarządzanie zdrowiem publicznym i innowacje medyczne. Prezes UODO wskazywał jednak na ryzyka wynikające ze skali systemu, zwłaszcza związane z pseudonimizacją, łączeniem baz danych i korzystaniem z usług chmurowych. Krajowe regulacje wdrażające EHDS powinny zatem precyzyjnie określać cele i warunki dostępu do

danych, zasady ich dalszego wykorzystywania oraz wymagane zabezpieczenia, tak, aby realizacja celów systemu nie prowadziła do obniżenia standardu ochrony danych dotyczących zdrowia.

### 3. Systemowe gwarancje praworządności

W 2025 r. działania Prezesa UODO obejmowały również systemowe gwarancje praworządności w obszarze dostępu państwa do danych. W wystąpieniach do MSWiA i Ministra Cyfryzacji wskazywano, że zasady kontroli operacyjnej oraz dostępu organów ścigania do danych objętych tajemnicą telekomunikacyjną nie zapewniają dostatecznej niezależnej kontroli, zawiadomienia osoby ani skutecznego środka odwoławczego. Zmian wymaga także funkcjonowanie KSIP, w szczególności brak maksymalnych okresów retencji, obowiązku okresowej weryfikacji danych i skutecznego prawa żądania ich usunięcia. Prezes UODO wiązał te problemy z nieprawidłową implementacją dyrektywy 2016/680; w prawie krajowym nadal nie ustanowiono również trybu pośredniego wykonywania praw za pośrednictwem organu nadzorczego.

Systemowego uporządkowania wymaga ponadto relacja między postępowaniami przed Prezesem UODO i sądami powszechnymi. W 2025 r. opracowano formularze usprawniające wymianę informacji na podstawie art. 94 ustawy o ochronie danych osobowych, wskazując jednocześnie na potrzebę zmian legislacyjnych zapewniających spójność rozstrzygnięć i skuteczną ochronę sądową. Organ analizował także wykonywanie orzeczeń TSUE i ETPC oraz występował o dostosowanie prawa krajowego do standardów europejskich w zakresie odnoszącym się do ochrony danych osobowych.

### 3. Ochrona danych na etapie tworzenia prawa

W opiniach legislacyjnych Prezesa UODO z 2025 r. powtarzały się problemy takie jak: otwarte katalogi danych, nieprecyzyjne cele, nadmierne wykorzystywanie numeru PESEL oraz przenoszenie istotnych elementów przetwarzania do aktów wykonawczych. Szczególne ryzyko wiązało się z rozbudową rejestrów, łączeniem baz i udostępnianiem danych bez pełnej analizy procesów. W projekcie centralnego rejestru umów zakwestionowano brak wykazania niezbędności publicznego udostępniania danych oraz ryzyko ich dalszego wykorzystywania, profilowania i wnioskowania o sytuacji życiowej osób.

Projekty nadal często trafiały do opiniowania przez Prezesa UODO bardzo późno albo z pominięciem konsultacji. Prezes UODO podejmował więc interwencje także z własnej inicjatywy i konsekwentnie wymagał testów prywatności oraz ocen skutków dla ochrony prywatności. Działania te przynosiły wymierne rezultaty: ograniczano zakres planowanego przetwarzania albo uzupełniano projekty o ocenę skutków. Porozumienia z Rządowym Centrum Legislacji i Polskim Towarzystwem Legislacji mają wzmacniać kompetencje projektodawców i włączać ochronę danych w początkową fazę procesu prawodawczego.

## 4. Inspektorzy ochrony danych (IOD), kodeksy postępowania

W 2025 r. Prezes UODO łączył wsparcie IOD z egzekwowaniem obowiązków wobec administratorów. Kierował wystąpienia dotyczące pozycji IOD w służbie cywilnej, uczestniczył w aktualizacji wytycznych EROD ich dotyczących oraz prowadził szkolenia i konsultacje. Zastosowano również środki egzekucyjne: upomnienia za niezapewnienie IOD warunków do niezależnego wykonywania zadań oraz kary za powierzenie tej funkcji prezesowi zarządu, co powodowało konflikt interesów. Praktyczne znaczenie – co podkreśla Prezes UODO – ma wczesne włączanie IOD w procesy decyzyjne oraz zapewnienie mu niezależności, odpowiednich zasobów i dostępu do informacji.

W listopadzie 2025 r. zatwierdzono kodeks dla prywatnych agencji badania opinii i rynku; łącznie w Polsce zatwierdzono trzy kodeksy. Kodeks jest użyteczny wtedy, gdy konkretyzuje obowiązki dla danej branży, rozstrzyga rzeczywiste problemy i zapewnia skuteczny monitoring, a nie tylko powtarza RODO.

## 5. Skargi, naruszenia i kierunek dalszych działań

### Skargi do Prezesa UODO

W 2025 r. wydaniem decyzji zakończono 2020 spraw skargowych, wobec 1670 w 2024 r., a łącznie w Departamencie Skarg zakończono 2291 spraw. Skargi dotyczyły m.in. bezpodstawnego udostępniania danych przez podmioty publiczne, marketingu, monitoringu, nieuprawnionego ujawnienia danych oraz realizacji praw osób. W szkolnictwie powtarzały się zarzuty ujawniania informacji o dzieciach, przekazywania danych przez dzienniki elektroniczne i publikowania wizerunku uczniów. Część żądań wykraczała poza kompetencje organu, co potwierdziło potrzebę dalszej edukacji o zakresie prawa do skargi.

### Naruszenia ochrony danych

Znacząco wzrosła liczba zgłoszeń naruszeń.

Najczęstsze przyczyny obejmowały ransomware, nieuprawniony dostęp do systemów, phishing, przejęcia kont, błędy ludzkie, nieprawidłową konfigurację oraz niewystarczające zabezpieczenia i nadzór. Praktyka naruszeń potwierdziła potrzebę oceny ryzyka przed uruchomieniem procesu, procedur reagowania, szkoleń, ewidencjonowania upoważnień, regularnych przeglądów dostępu i ciągłego monitorowania zabezpieczeń, zwłaszcza w systemach wykorzystujących AI.

### Zmiany organizacyjne w Urzędzie

Reorganizacja UODO odpowiadała na rosnącą liczbę skarg i naruszeń oraz nowe kompetencje wynikające z DGA i DSA. Wyodrębniono Departament Wstępnej Kontroli Skarg i Naruszeń, a Departament Innowacji i Zarządzania Danymi uczestniczył w pracach nad wdrażaniem DGA i przygotowywał Urząd do zadań obejmujących także dane nieosobowe. Rozwój nowych ram - EHDS, aktu w sprawie AI, DSA, DGA, eIDAS2 i regulacji wdrażających NIS 2 - wymaga dalszego łączenia kompetencji prawnych, technicznych i organizacyjnych.

**Priorytety na kolejne lata**

Priorytetami pozostają usprawnienie obsługi skarg i naruszeń, wzmocnienie zasobów kadrowych, współpraca z IOD i projektodawcami oraz przygotowanie do stosowania nowych regulacji cyfrowych w kontekście rozwoju nowych technologii. Rozwój sztucznej inteligencji i publicznych systemów zautomatyzowanego przetwarzania danych wymaga wyprzedzającego identyfikowania zagrożeń i ochrony danych w fazie projektowania. Szczególne znaczenie nadal ma ochrona dzieci przez regulację usług cyfrowych, kontrole, edukację i wzmacnianie odporności placówek oświatowych.

# ZAŁĄCZNIKI

**Załącznik nr 1:**

**Wykaz administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2025 r.**

| Lp. | Data decyzji | Departament UODO prowadzący postępowanie | Sygnatura | Wysokość kary w zł |
|---|---|---|---|---|
| 1. | 17.01.2025 | Departament Kontroli i Naruszeń | DKN.5131.4.2024 | 687 534,75 |
| 2. | 17.01.2025 | Departament Kontroli i Naruszeń | DKN.5131.4.2024 | 458 356,50 |
| 3. | 06.03.2025 | Departament Kontroli i Naruszeń | DKN.5112.10.2024 | 56 824,00 |
| 4. | 17.03.2025 | Departament Kontroli i Naruszeń | DKN.5131.1.2025 | 100 000,00 |
| 5. | 17.03.2025 | Departament Kontroli i Naruszeń | DKN.5131.1.2025 | 27 124 816,00 |
| 6. | 19.03.2025 | Departament Skarg | DS.523.4750.2023 | 75 000,00 |
| 7. | 01.04.2025 | Departament Kontroli i Naruszeń | DKN.5131.10.2023 | 29 043,00 |
| 8. | 01.04.2025 | Departament Kontroli i Naruszeń | DKN.5131.10.2023 | 4 630,00 |
| 9. | 14.04.2025 | Departament Kar i Egzekucji | DOKE.561.2.2024 | 25 255,00 |
| 10. | 03.06.2025 | Departament Kontroli i Naruszeń | DKN.5131.30.2022 | 5 000,00 |
| 11. | 03.06.2025 | Departament Kontroli i Naruszeń | DKN.5131.30.2022 | 10 000,00 |
| 12. | 17.06.2025 | Departament Kontroli i Naruszeń | DKN.5131.48.2022 | 66 500,00 |
| 13. | 23.06.2025 | Departament Kar i Egzekucji | DKE.561.1.2025 | 18 941,00 |
| 14. | 23.06.2025 | Departament Kontroli i Naruszeń | DKN.5130.4179.2020 | 94 286,00 |
| 15. | 23.06.2025 | Departament Kontroli i Naruszeń | DKN.5130.4179.2020 | 42 429,00 |
| 16. | 23.06.2025 | Departament Kontroli i Naruszeń | DKN.5130.4179.2020 | 47 143,00 |
| 17. | 23.06.2025 | Departament Kontroli i Naruszeń | DKN.5130.4179.2020 | 1 632 063,00 |
| 18. | 23.06.2025 | Departament Kontroli i Naruszeń | DKN.5130.4179.2020 | 13 600 528,00 |
| 19. | 23.06.2025 | Departament Kontroli i Naruszeń | DKN.5130.4179.2020 | 1 700 066,00 |
| 20. | 04.07.2025 | Departament Kontroli i Naruszeń | DKN.5131.17.2022 | 32 832,00 |
| 21. | 23.07.2025 | Departament Kontroli i Naruszeń | DKN.5112.6.2020 | 18 416 400,00 |
| 22. | 12.09.2025 | Departament Kontroli i Naruszeń | DKN.5131.7.2025 | 11 365,00 |
| 23. | 15.10.2025 | Departament Kontroli i Naruszeń | DKN.5131.3.2025 | 40 514,00 |
| 24. | 23.10.2025 | Departament Kontroli i Naruszeń | DKN.5131.17.2024 | 7 700,00 |
| 25. | 23.10.2025 | Departament Kontroli i Naruszeń | DKN.5131.17.2024 | 13 200,00 |
| 26. | 15.11.2025 | Departament Kontroli i Naruszeń | DKN.5131.3.2024 | 20 000,00 |
| 27. | 25.11.2025 | Departament Kontroli i Naruszeń | DKN.5112.27.2022 | 7 577,00 |
| 28. | 25.11.2025 | Departament Kontroli i Naruszeń | DKN.5112.27.2022 | 3 157,00 |
| 29. | 08.12.2025 | Departament Kar i Egzekucji | DOKE.561.11.2024 | 14 816,00 |

| | | | | |
|---|---|---|---|---|
| 30. | 22.12.2025 | Departament Kar i Egzekucji | DOKE.561.6.2023 | 12 964,00 |
| 31. | 29.12.2025 | Departament Kontroli i Naruszeń | DKN.5131.5.2024 | 40 000,00 |
| 32. | 29.12.2025 | Departament Kontroli i Naruszeń | DKN.5131.5.2024 | 38 000,00 |

**Załącznik nr 2:**

## Wykaz wydarzeń objętych patronatem Prezesa UODO w 2025 r.

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 1. | 20.01.2026 | VI Konferencja „Dzień Ochrony Danych Osobowych". Organizator: Redakcja „ABI Expert". | Warszawa |
| 2. | 29.01.2026 | Konferencja „Dzień Inspektora Ochrony Danych 2025". Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych. | online |
| 3. | 30.01.2025 | X Konferencja „IOD 2025 – wyzwania nowych technologii". Organizator: SABI – Stowarzyszenie Inspektorów Ochrony Danych Osobowych. | Warszawa |
| 4. | 6.02.2025 | XI Dzień Otwarty Urzędu Ochrony Danych Osobowych. Organizator: Akademia WSB w Dąbrowie Górniczej. | Dąbrowa Górnicza |
| 5. | 27-28.02.2026 | V Konferencja Przedsiębiorców. Organizator: Manager Business Hub. | Trojanów |
| 6. | 4.03.2025 | VI Konferencja „Cybersec & Compliance w Zdrowiu". Organizatorzy: Koalicja AI w Zdrowiu, Polska Federacja Szpitali. | Warszawa |
| 7. | 5-6.03.2025 | Konferencja „Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej". Organizator: Instytut Nauk Prawnych Polskiej Akademii Nauk. | Warszawa |
| 8. | 26-27.03.2025 | Data Economy Congress. Organizator: MM Conferences Polska. | Warszawa |
| 9. | 27.03.2025 | II Ogólnopolska Konferencja Naukowa Ochrony Danych Osobowych Uniwersytetu Mikołaja Kopernika w Toruniu. Organizatorzy: Centrum Badań nad Cyberprzestępczością, Wydział Prawa i Administracji UMK w Toruniu, Studenckie Koło Naukowe Ochrony Danych Osobowych, Koło Naukowe Prawa Międzynarodowego Publicznego i Ochrony Praw Człowieka. | Toruń |
| 10. | 23-25.04.2025 | XVIII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: Krajowe Stowarzyszenie Ochrony Informacji Niejawnych. | Krynica Morska |
| 11. | 21.05.2025 | Konferencja „7 lat RODO – czas na deregulację?" Organizator: Lubasz i Wspólnicy - Kancelaria Radców Prawnych. | online |
| 12. | 22.05.2025 | Konferencja „Cyberhigiena i cyberochrona - w administracji, biznesie i oświacie". Organizator: SIODO - Stowarzyszenie Inspektorów Ochrony Danych Osobowych. | Warszawa |
| 13. | 21-22.05.2025 | Konferencja „Prawa człowieka w obliczu kryzysów globalnych". Organizator: Katedra Prawa Międzynarodowego Publicznego i Prawa Unii Europejskiej WPiA UWM oraz Studenckie Koło Naukowe Praw Człowieka "Ius Homini". | online |
| 14. | 30.05.2025 | Ogólnopolska Konferencja Kół Naukowych „Prawo do prywatności w erze mediów społecznościowych". Organizator: Koło Naukowe Studentów Prawa Katolickiego Uniwersytetu Lubelskiego. | Lublin |
| 15. | 4.06.2025 | Konferencja ,,Uwaga! Smartfon". Organizator: Fundacja Projekt PL. | Lublin |
| 16. | 10.06.2025 | Szkolenie „Dziecko w sieci – Odpowiedzialny Rodzic, Bezpieczne Dziecko". Organizator: Akademia Nauk Stosowanych w Nowym Sączu. | Nowy Sącz |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 17. | 11-12.06.2025 | Kongres Bezpieczeństwo Polski - KBP Rzeszów 2025. Organizator: MM Conferences Polska. | Rzeszów-Jasionka |
| 18. | 13.06.2025 | X Podkarpackie Forum Audytu. Audyt zarządzania kryzysowego i bezpieczeństwa informacji. Organizator: Wydział Ekonomii i Finansów Uniwersytetu Rzeszowskiego. | Rzeszów-Zalesie |
| 19. | 30.06-31.12.2025 | Scamming Out 2.0! – Kampania przeciw oszustwom internetowym. Organizator: Bonnier Business Polska sp. z o. o. | online |
| 20. | 4.09.2025 | ETH Legal. Organizator: ETH Poland. | Warszawa |
| 21. | 18-19.09.2025 | Konferencja „AI TASK FORCE IN DIALOGUE". Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych. | online |
| 22. | 18-19.09.2025 | Coroczne Spotkanie Inspektorów Ochrony Danych uczelni zrzeszonych w Konferencji Rektorów Akademickich Uczelni Medycznych (KRAUM). Organizator: Uniwersytet Rzeszowski. | Rzeszów |
| 23. | 29-30.09.2025 | Konferencja PINT25 – Prawo i Nowe Technologie. Organizator: Okręgowa Izba Radców Prawnych w Krakowie. | Kraków |
| 24. | 30.09-1.10.2025 | IX Krajowy Kongres Sekretarzy. Organizator: Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego. | Warszawa |
| 25. | 1 i 15.10.2025 | XIV Konwent Ochrony Danych i Informacji. Organizator: FORSAFE Sp. z o. o. | Łódź/online |
| 26. | 2.10.2025 | Cyber24 Day. Organizator: Grupa Defence24 Sp. z o. o. | Warszawa |
| 27. | 6-7.10.2025 | 6. Edycja Economy Congress. Organizator: MMC Polska. | Warszawa |
| 28. | 13-14.10.2025 | 14. edycja Trusted Economy Forum - CommonSign 2025. Organizator: Medien Service. | Warszawa |
| 29. | 22-23.10.2025 | Banking & Insurance Forum. Organizator: MMC Polska. | Warszawa |
| 30. | 22-23.10.2025 | 6. Międzynarodowe Targi Technologii Miejskich Smart City Expo Poland. Organizator: Lentewenc Sp. z .o.o. | Warszawa |
| 31. | 09-12.2025 r. | Ogólnopolski konkurs dla szkół podstawowych ,,Więcej szacunku dla młodego wizerunku". Organizator: Biuro Rzecznika Praw Dziecka. | - |
| 32. | 20.11.2025 | Konferencja „Adwokat dla oświaty - wyzwania współczesnej edukacji". Organizator: Okręgowa Rada Adwokacka w Warszawie. | Warszawa |
| 33. | 21.11-12.12.2025 | Ogólnopolski konkurs prawa UE (OKPE). Organizator: ELSA Gdańsk. | - |
| 34. | 1-3.12.2025 | Międzynarodowe Sympozjum Naukowe pt. „Cyberthreats and disinformation". Organizator: Uniwersytet Jana Długosza w Częstochowie. | Częstochowa |
| 35. | 11.12.2025 | IX Ogólnopolska Konferencja Naukowa Prawa Medycznego pt. „Wyzwania prawa medycznego w dobie cyfryzacji, bezpieczeństwa i etyki". Organizator: Europejskie Stowarzyszenie Studentów Prawa ELSA Rzeszów. | Rzeszów |
| 36. | 18.11.2025 | Projekt ALK pn. „Ochrona Danych Osobowych w Ubezpieczeniach" oraz cykl webinariów i konferencji w ramach tego projektu: „Jak przygotować się do kontroli Prezesa UODO" (18.11.2025), „Jak przygotować się do kontroli administratora danych?" (20.01.2026), Konferencja „Praktycznie o ochronie danych osobowych w ubezpieczeniach" (24.03.2026). Organizator: Centrum Ubezpieczeń Gospodarczych Akademii Leona Koźmińskiego w Warszawie. | Warszawa / online |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 37. | | Serwis „Prezydencja” na portalu RynekZdrowia.pl. Organizator: Polskie Towarzystwo Wspierania Przedsiębiorczości SA. | |
| 38. | | 5. edycja kampanii edukacyjnej „Cyberbezpieczeństwo”. Organizator MediaPlanet Publishing House Sp. z o.o. | |
| 39. | | Projekt „Bezpieczne zakupy”. Organizator: Izba Gospodarki Elektronicznej (e-Izba). | |

**Załącznik nr 3:**

## Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2025 r. w Polsce przez UODO lub inne podmioty

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 40. | 8.01.2025 | Spotkanie Prezesa UODO z przedstawicielami Fundacji Panoptyko. Organizator: UODO. | Warszawa |
| 41. | 13.01.2025 | Spotkanie ze studentami w siedzibie UODO. Organizator: UODO w ramach obchodów XIX Dnia Ochrony Danych Osobowych 2025. | Warszawa |
| 42. | 14.01.2025 | Spotkanie prezesa UODO z Prezesem Naczelnej Izby Lekarskiej. | Warszawa |
| 43. | 14.01.2025 | Spotkanie Prezesa UODO z przedsiębiorcami zrzeszonymi w Konfederacji Lewiatan. Organizator: UODO. | Warszawa |
| 44. | 15.01.2025 | Konferencja ,,Zasada niedyskryminacji dzieci i młodzieży w politykach publicznych, mediach cyfrowych, edukacji i zarządzaniu". | Warszawa |
| 45. | 20.01.2025 | 6. edycja Konferencji ABI Expert pt. „Dzień Ochrony Danych Osobowych” | Warszawa |
| 46. | 23.01.2025 | Konferencja „Ocena ryzyka a ochrona danych osobowych”. Organizatorzy: UODO, Społeczny Zespół Ekspertów przy Prezesie UODO, Uniwersytet Warszawski. | Warszawa |
| 47. | 24.01.2025 | Wykład ekspercki pt. „Proces monitorowania postępu technologicznego jako element rozliczalności stosowania zasady ochrony danych w fazie projektowania oraz domyślnej ochrony danych”, wygłoszony przez członkinię SZE przy Prezesie UODO, w ramach obchodów XIX Dnia Ochrony Danych Osobowych. | online |
| 48. | 29.01.2025 | Konferencja „Dzień Inspektora Ochrony Danych 2025”. Organizator: Kancelaria Lubasz i Wspólnicy Kancelaria Radców Prawnych sp. k. | Łódź/online |
| 49. | 30.01.2025 | Konferencja „IOD 2025 – wyzwania nowych technologii”. Organizator: SABI. | Warszawa |
| 50. | 30-31.01.2025 | „UODO rusza w kraj” – województwo pomorskie. Organizator: UODO. | Kwidzyn Gdańsk Gdynia |
| 51. | 6.02.2025 | XI Dzień Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej. | Dąbrowa Górnicza |
| 52. | 17.02.2025 | Spotkanie z ambasadorami państw Unii Europejskiej. | Warszawa |
| 53. | 18.02.2025 | Konferencja pt.: „Jak otoczenie regulacyjne wpływa na rozwój AI? Perspektywa biznesu, regulatorów i użytkowników”. Organizator” Uczelnia Techniczno-Handlowa im. H. Chodkowskiej. | Warszawa online |
| 54. | 21.02.2025 | Wykład ekspercki pt. „Technologie kwantowe – szanse i zagrożenia dla ochrony prywatności”. Organizator: UODO. | online |
| 55. | 25.02.2025 | Konferencja ,,Zwalczanie treści nielegalnych w sieci – między bezpieczeństwem i wolnością". Organizator: ALK w Warszawie. | Warszawa |
| 56. | 27-28.02.2025 | V Konferencja Biznesowa dla Przedsiębiorców TALARIA 2025. Organizator: Manager Business Hub. | Trojanów |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 57. | 28.02.2025 | Konferencja (Bez)Prawa osób transpłciowych w Polsce. Jak przetwarzać dane osobowe osób transpłciowych i skutecznie przeciwdziałać dyskryminacji ze względu na tożsamość płciową w zatrudnieniu?". Organizatorzy: UODO, Fundacja Trans-Fuzja, Open for Business, Społeczny Zespół Ekspertów (SZE) przy Prezesie UODO. | Warszawa |
| 58. | 3-4.03.2025 | X Europejski Kongres Samorządów. Organizator: Instytut Studiów Wschodnich. | Mikołajki |
| 59. | 6.03.2025 | Wykład ekspercki pt. „Technologie kwantowe – szanse i zagrożenia dla ochrony prywatności i danych osobowych" wygłoszony przez członka SZE przy Prezesie UODO. | online |
| 60. | 10.03.2025 | Konferencja ZUS „Podkarpacie dla biznesu". Organizator: ZUS w Rzeszowie we współpracy z WSPiA Rzeszowską Szkołą Wyższą. | Rzeszów |
| 61. | 13.03.2025 | Sympozjum Ministerstwa Sprawiedliwości „Utrwalanie czynności procesowych w postępowaniu karnym za pomocą urządzeń rejestrujących obraz i dźwięk". | Warszawa |
| 62. | 19.03.2025 | Posiedzenie Naczelnej Rady Pielęgniarek i Położnych. | Warszawa |
| 63. | 20.03.2025 | Walne Zebranie Członków Polskiego Towarzystwa Legislacji w siedzibie Senatu RP. | Warszawa |
| 64. | 20-21.03.2025 | „UODO rusza w kraj" – województwo podkarpackie. Organizator: UODO we współpracy z OIRP, Wojewodą Podkarpackim i Społecznym Zespołem Ekspertów przy Prezesie UODO. | Rzeszów |
| 65. | 24.03.2025 | Spotkanie z kadrą i studentami Akademii Sztuki Wojennej. | Warszawa |
| 66. | 26.03.2025 | Konferencja „Europejska przestrzeń danych dot. zdrowia – wyzwanie dla Europy. Wdrażanie rozwiązań w dobie AI, Big Data i medycyny spersonalizowanej". Organizator: Wydział Medyczny UW. | Warszawa |
| 67. | 26-27.03.2025 | 5. Data Economy Congress. Organizator: MMC Polska. | Warszawa |
| 68. | 27.03.2025 | Ogólnopolska Konferencja Naukowa Ochrony Danych Osobowych. Organizatorzy: Centrum Badań nad Cyberprzestępczością oraz Koło Naukowe Ochrony Danych Osobowych na WPiA UMK w Toruniu. | Toruń |
| 69. | 28.03.2025 | Webinarium – „Zaktualizowany poradnik UODO dot. naruszeń ochrony danych". Organizator: UODO, SZE. | online |
| 70. | 1.04.2025 | Spotkanie Prezesa UODO z Prezesem GUS. | Warszawa |
| 71. | 2.04.2025 | Webinarium w ramach programu "Twoje dane - Twoja sprawa". Organizator: UODO. | online |
| 72. | 2.04.2025 | Spotkanie z członkami Studenckiego Koła Naukowego Praw Człowieka IUS HOMINI w siedzibie UODO. | Warszawa |
| 73. | 3.04.2025 | Spotkanie inaugurujące cykl warsztatów z zakresu ochrony danych osobowych dla przedstawicieli PTL. Organizator: UODO. | Warszawa |
| 74. | 3.04.2025 | XII Forum Inspektorów Ochrony Danych. Organizator: Wielkopolski Ośrodek Kształcenia i Studiów Samorządowych. | Poznań |
| 75. | 3.04.2025 | FORUM ROZWOJU URZĘDNIKÓW. Organizator: KSAP im. Prezydenta Rzeczypospolitej Polskiej Lecha Kaczyńskiego. | Watszawa |
| 76. | 7.04.2025 | Konferencja „Wykorzystanie nowoczesnych technologii w geodezji i kartografii". Organizator: Główny Geodeta Kraju. | Ożarów Mazowiecki |
| 77. | 10.04.2025 | Konferencja „Dzień Ochrony Danych Osobowych w sektorze medycznym". | Warszawa |
| 78. | 11.04.2025 | Konferencja "Centralny Rejestr Umów JSFP jako narzędzie jawności życia publicznego. Plany i Wyzwania". | Warszawa |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| | | Organizatorzy: Ministerstwo Finansów, WPiA UŁ, WPiA UKSW w Warszawie. | |
| 79. | 14.04.2025 | Wykład ekspercki pt. „Wyzwania dla bezpieczeństwa danych w kontekście rozwoju nowych technologii". Organizator: UODO. | online |
| 80. | 14.04.2025 | Debata „Okrągły Stół dla rejestrów medycznych – dokąd zmierzamy?". Organizator: UODO. | Warszawa |
| 81. | 15-16.04.2025 | Banking & Insurance Forum. Organizator: MMC Polska. | Warszawa |
| 82. | 15.04.2025 | Warsztaty legislacyjne dla przedstawicieli PTL. Organizator: UODO. | Warszawa |
| 83. | 23-25.04.2025 | XVII Kongres Ochrony Informacji Niejawnych, Biznesowych i Danych Osobowych. Organizator: KSOIN. | Krynica Morska |
| 84. | 24.04.2025 | Konferencja pt. Cel – lepsze prawo. Ocena skutków zmian w Regulaminie Sejmu z 26 lipca 2024 r. Organizator: Kancelaria Sejmu RP. | Warszawa |
| 85. | 29.04.2025 | Szkolenie UODO dla pracowników biura Rządowego Centrum Legislacji. | Warszawa |
| 86. | 6.05.2025 | Szkolenie dla Inspektorów Ochrony Danych, zorganizowane przez Kościelnego Inspektora Ochrony Danych i Fundację Konferencji Episkopatu Polski Bona Fama we współpracy z Prezesem Urzędu Ochrony Danych Osobowych, | Warszawa |
| 87. | 7.05.2026 | Seminarium eksperckie „Aktualne wyzwania ochrony danych osobowych w związkach wyznaniowych w Polsce. Organizator: UODO | Warszawa |
| 88. | 12.05.2025 | Szkolenie UODO dla przedstawicieli PTL. Organizator: UODO. | Warszawa |
| 89. | 13.05.2025 | Posiedzenie plenarne Rady Działalności Pożytku Publicznego. Debata pt. „RODO w organizacjach pozarządowych? Może czas na uproszczenia?" Organizator: KPRM. | online |
| 90. | 16.05.2025 | Spotkanie dot. bezpieczeństwa danych dzieci w środowisku cyfrowym - Krajowy Cech Fotografów. Organizator: UODO. | Warszawa |
| 91. | 16.05.2025 | Webinarium – „Zaktualizowany poradnik UODO dot. naruszeń ochrony danych". Organizator: UODO, SZE. | online |
| 92. | 19.05.2025 | Spotkanie seminaryjne ze studentami pt. „Współczesne wyzwania dla ochrony danych osobowych w systemie ochrony zdrowia". Organizatorzy: Studenckie Koło Naukowe prawo w Zdrowiu, Collegium Medicum UJ | Kraków |
| 93. | 19.05.2025 | Konferencja Legal Summit. | Kraków |
| 94. | 19-23.05.2025 | Szkolenie UODO dla funkcjonariuszy Straży Granicznej, | Warszawa |
| 95. | 20.05.2025 | Uroczystość wręczenia Nagrody Głównego Inspektora Pracy im. Haliny Krahelskiej na Zamku Królewskim w Warszawie. | Warszawa |
| 96. | 20-21.05.2025 | „UODO rusza w kraj" – województwo wielkopolskie. Organizator: UODO. | Poznań |
| 97. | 21.05.2025 | V Ogólnopolski Kongres Pacjent w Centrum Uwagi. Organizator: DOZ.S.A. | Warszawa |
| 98. | 22.05.2025 | Gala Nagrody Korczaka. Organizator: Uczelnia Korczaka. | Warszawa |
| 99. | 22.05.2025 | Seminarium „Automatyzacja procesów administracyjnych z wykorzystaniem sztucznej inteligencji: jak zapewnić zgodność z ochroną danych osobowych?". Organizatorzy: UODO i ZUS. | Poznań |
| 100. | 22.05.2025 | Konferencja „Cyberhigiena i cyberochrona – w administracji, biznesie i oświacie". Organizator: SIODO - | Warszawa |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| | | - Stowarzyszenie Inspektorów Ochrony Danych Osobowych. | |
| 101. | 24.05.2025 | Ogólnopolskie spotkanie Inspektorów Ochrony Danych Osobowych OIRP w Białymstoku i KIRP. | Białystok |
| 102. | 27.05.2025 | XV edycja programu „Twoje dane – Twoja sprawa" - ceremonia wręczania nagród konursowych. Organizator: UODO. | Warszawa |
| 103. | 28.05.2025 | Konferencja pt. „Forum Innowacyjnych Zamówień Publicznych 2025". Organizator: Narodowe Centrum Badań i Rozwoju. | Warszawa |
| 104. | 29.05.2025 | Konferencja pt. „Ewolucja roli inspektora ochrony danych w świetle nowych wyzwań". Organizator: Związek Firm Ochrony Danych Osobowych. | online |
| 105. | 30.05.2025 | Wykład ekspercki pt. „Uwzględnienie ochrony danych przy projektowaniu systemów sztucznej inteligencji". Organizator: UODO. | online |
| 106. | 2.06.2025 | Konferencja „Europejskie Ramy Cyfrowej Tożsamości (eIDAS2) w praktyce. Nowe możliwości identyfikacji i uwierzytelniania w służbie ochrony danych. Korzyści i potencjał rozwoju dla biznesu i sektora publicznego. Organizator: UODO we współpracy z SZE. | Warszawa online |
| 107. | 3.06.2025 | Europejski Kongres Finansowy „Data is the new oil: Ochrona obywatela, rozwój biznesu, napęd gospodarki". Organizator: Biuro Informacji Kredytowej S.A. | Sopot |
| 108. | 4.06.2025 | IV edycja konferencji „Uwaga! Smartfon". Organizator: Fundacja Projekt PL. | Lublin |
| 109. | 9.06.2025 | Posiedzenie SZE oraz posiedzenie Grupy Roboczej SZE ds. Sztucznej Inteligencji. Organizator: UODO. | Warszawa online |
| 110. | 10-11.06.2025 | Forum Bezpieczeństwa, pt. „Inwestycje podwójnego przeznaczenia". Organizatorzy: Fundacja Forum Bezpieczeństwa, Stowarzyszenie Przeciwko Nadużyciom Gospodarczym Antifraud oraz Międzynarodowy Instytut Społeczeństwa Obywatelskiego. | Łódź |
| 111. | 12-13.06.2025 | Konferencja „Technologie kwantowe: zagrożenia, wyzwania i szanse dla cyberbezpieczeństwa i ochrony danych osobowych". Organizatorzy: UODO i UJ. | Kraków |
| 112. | 13.06.2025 | Konferencja „AI w Metropoliach. Tworzenie, integracja i zarządzanie infrastrukturą AI jako zadanie związku metropolitarnego". Organizator: WPiA UG. | Gdańsk |
| 113. | 13.06.2025 | Webinarium „Import dóbr kultury na teren Unii Europejskiej. Co nowa regulacja oznacza dla rynku sztuki?". Organizator: Ministerstwo Kultury i Dziedzictwa Narodowego. | online |
| 114. | 13.06.2025 | X Podkarpackie Forum Audytu pt. „Audyt zarządzania kryzysowego i bezpieczeństwa informacji". Organizator: UODO oraz Wydział Ekonomii i Finansów Uniwersytetu Rzeszowskiego. | Rzeszów |
| 115. | 13.06.2025 | Konferencja pt. „Jak budować kulturę ochrony dzieci i młodzieży w środowisku mediów cyfrowych". Organizator: Sejmowa Komisja do Spraw Dzieci i Młodzieży – DIM we współpracy z Uczelnią Korczaka i UW. | Warszawa |
| 116. | 16.06.2025 | Spotkanie w MSWiA pod hasłem „Cyberbezpieczeństwo danych osobowych". | Warszawa |
| 117. | 17.06.2025 | Szkolenie nt. „Wyzwań prawnych stojących przed wtórnym przetwarzaniem danych osobowych, w szczególności dla celu badań naukowych w EHDS". Organizatorzy: NIL, UODO, Centralny Ośrodek Badań, Innowacji i Kształcenia oraz Sieć Lekarzy Innowatorów. | online |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 118. | 18.06.2025 | Spotkanie dot. współpracy z Ośrodkiem Rozwoju Edukacji (ORE) w zakresie edukacji o ochronie danych osobowych. | online |
| 119. | 20.06.2025 | Wykład ekspercki pt. „Ochrona danych w systemach sztucznej inteligencji – operacje na danych osobowych z perspektywy podmiotu stosującego". Organizator: UODO. | online |
| 120. | 23.06.2025 | Spotkanie programowe dot. przygotowania konferencji z Ministerstwem Sprawiedliwości pt. „Ochrona danych osobowych dziecka – uczestnika postępowania karnego i cywilnego - w przestrzeni medialnej". | Warszawa |
| 121. | 23.06.2025 | Konferencja pt. „Deklaracje a doświadczenia: Jak młodzi oceniają przestrzeganie swoich praw?". Organizator: Biuro Rzecznika Praw Dziecka. | Warszawa |
| 122. | 25.06.2025 | Seminarium „Wyzwania w udzielaniu informacji publicznej. Jak pogodzić transparentność i ochronę danych osobowych?". Organizatorzy: UODO i ZUS. | Lublin |
| 123. | 25.06.2025 | Obchody 249 rocznicy Amerykańskiego Święta Niepodległości pn. „United in Friendship and Freedom – Zjednoczeni w Przyjaźni i Wolności". Organizator: Amerykańska Izba Handlowa w Polsce (AmCham). | Warszawa |
| 124. | 25.06.2025 | Uroczystość wręczenia nagród laureatom XIII konkursu UODO na esej dla studentów. Organizator: UODO. | Warszawa |
| 125. | 26.06.2026 | Letnie Spotkanie - Piknik Lewiatana. Organizator: Konferencja Lewiatan. | Warszawa |
| 126. | 26.06.2025 | Konferencja MedSec Summit 2025. Organizator Medien Service. | Warszawa |
| 127. | 04.07.2025 | Posiedzenie Rady Programowej 6 ed. DATA ECONOMY CONGRESS. | Warszawa |
| 128. | 8.07.2025 | Spotkanie eksperckie w sprawie naboru Instrumentu Wsparcia Technicznego TSI 2026. | online |
| 129. | 23.06.2025 | Spotkanie programowe dot. przygotowania konferencji z Ministerstwem Sprawiedliwości. | Warszawa |
| 130. | 25.07.2025 | Webinarium UODO „Nowe uprawnienia Prezesa Urzędu Ochrony Danych Osobowych". Organizator: UODO | online |
| 131. | 29.07.2025 | Spotkanie w UODO w sprawie projektu dot. organizacji wizyt studyjnych ws. wdrożenia Aktu o sztucznej inteligencji. | Warszawa |
| 132. | 30.07-2.08.2025 | 31. Pol'and'Rock Festival. Organizator: Fundacja Wielka Orkiestra Świątecznej Pomocy. | Lotnisko Czaplinek-Broczyno |
| 133. | 31.07.2025 | Spotkanie organizacyjne dotyczące warsztatów szkoleniowych w ramach II Fazy szkoleń S-AIP. | online |
| 134. | 03.08.2025 | Turniej Wsi Gminy Skierniewice. Organizator: Wójt Gminy Skierniewice. | Miedniewice |
| 135. | 29.08.2025 | Konferencja ,,Q-Con Quantum Conference". | Gdańsk |
| 136. | 2-4.09.2025 | XXXIV Forum Ekonomiczne w Karpaczu. | Karpacz |
| 137. | 04.09.2025 | ETH Legal. | Warszawa |
| 138. | 09.09.2025 | Posiedzenie Grupy Roboczej SZE ds. SI. | Warszawa online |
| 139. | 9.09.2025 | Konferencja Jubileuszowa Agencji Oceny Technologii Medycznych i Taryfikacji pt. „Siła dowodów kształtuje przyszłość". | Warszawa |
| 140. | 10.09.2025 | Szkolenie pn. „RODO w sporcie – inauguracja poradnika dla podmiotów sportowych. Innowacje w sporcie: CSR i AI". Organizator: Instytut Sportu - PIB. | Warszawa |
| 141. | 11.09.2025 | Konferencja pt. „Workers' Data, Collective Bargaining, and the Platform Economy". Organizator: zespół badawczy projektu GDPoweR. | Warszawa |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 142. | 15.09.2025 | Konferencja pt.: „Epidemia przemocy wobec kobiet w cyberprzestrzeni". Organizatorzy: Sejmowa Komisja Polityki Społecznej i Rodziny oraz Uczelnia Korczaka. | Warszawa. |
| 143. | 18.09.2025 | Konferencja AI TASK FORCE. | online |
| 144. | 18.09.2025 | Spotkanie Inspektorów Ochrony Danych uczelni zrzeszonych w KRAUM. | Rzeszów |
| 145. | 22.09.2025 | II Konferencja „RODOwskazy w Falentach". Organizator: Stowarzyszenie Praktyków Ochrony Danych. | Falenty |
| 146. | 22.09.2025 | Konferencja naukowa pn. „Bezpieczeństwo dokumentów publicznych". Organizatorzy: Akademia Policji w Szczytnie, Departament Spraw Obywatelskich MSWiA, Centrum Personalizacji Dokumentów MSWiA, Centralne Laboratorium Kryminalistyczne Policji, Centrum Szkolenia Straży Granicznej w Kętrzynie i PWPW S.A. | Szczytno |
| 147. | 23-26.09.2025 | XIV Warsztaty Legislacyjne. Organizator: Dyrektor Generalny Służby Więziennej. | Jurata |
| 148. | 24.09.2025 | Seminarium „Cyberhigiena i cyberochrona w oświacie i kulturze". | Poznań |
| 149. | 24.09.2025 | Posiedzenie Komisji do Spraw Dzieci i Młodzieży, Sejm RP. | Warszawa |
| 150. | 24.09.2025 | Spotkanie z przedstawicielami Ośrodka Rozwoju Edukacji. | online |
| 151. | 25.09.2025 | Warsztat – Śniadanie AI. Organizator: Peak Legal. | Warszawa |
| 152. | 25-26.09.2025 | III Ogólnopolska Konferencja Naukowa Prawa Medycznego, Farmaceutycznego, Bioetyki i Zarządzania w Ochronie Zdrowia. Organizator: Uniwersytet Gdański. | Gdańsk |
| 153. | 25-29.09.2025 | Szkolenie Studium Architektury Informacyjnej Państwa. | online |
| 154. | 27.09.2025 | Piknik edukacyjny w Zaspole Szkół im. Krzysztofa Kamila Baczyńskiego w Tłuszczu. | Tłuszcz |
| 155. | 29-30.09.2025 | Konferencja PINT25 – Prawo i Nowe Technologie. Organizator: Okręgowa Izba Radców Prawnych w Krakowie. | Kraków |
| 156. | 30.09.2025 | Konferencja ,,Wpływ Aktu w sprawie sztucznej inteligencji na funkcjonowanie administracji publicznej". Organizator: INP PAN. | Warszawa |
| 157. | 30.09.2025 | Inauguracja roku akademickiego 2025/2026 w SGGW. | Warszawa |
| 158. | 30.09-1.10.2025 | IX Krajowy Kongres Sekretarzy. Organizatorzy: Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego oraz Krajowa Rada Forów Sekretarzy JST. | Warszawa |
| 159. | 01.10.2025 | XIV Konwent Ochrony Danych i Informacji pod hasłem „KoRODOwrotek. Run IOD Run". Organizator: FORSAFE Sp. z o.o. | Łódź |
| 160. | 02.10.2025 | 6. edycja Konferencji Cyber24Day. Organizator: Defence24 Sp. z o.o. | Warszawa |
| 161. | 02.10.2025 | Szkolenie Studium Architektury Informacyjnej Państwa. Organizatorzy: Ministerstwo Cyfryzacji, NASK-PIB. | online |
| 162. | 02.10.2025 | Seminarium „Rewolucja technologiczna w relacji z klientami – jak budować rozwiązania technologiczne w relacji z klientami?". Organizatorzy: UODO i ZUS. | Rzeszów |
| 163. | 6-7.10.2025 | 6. Data Economy Congress. Organizator: MMC Polska. | Warszawa |
| 164. | 07.10.2025 | Inauguracja roku akademickiego 2025/2026 w Akademii Leona Koźmińskiego | Warszawa |
| 165. | 7-10.2025 | Gala finałowa konkursu Nauczyciel Roku. Organizator: UODO | Warszawa |
| 166. | 08.10.2025 | Spotkanie z przedstawicielami samorządów zawodowych - strategia działań edukacyjnych. | online |
| 167. | 09.10.2025 | Szkolenie Studium Architektury Informacyjnej Państwa. | online |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 168. | 10.10.2025 | Konferencja „Bezpieczne dane dzieci i młodzieży oraz nowe kierunki rozwoju w obszarze kultury fizycznej. Jak sprostać współczesnym wyzwaniom?”. Organizatorzy: UODO we współpracy z Krakowskim Szkolnym Ośrodkiem Sportowym im. Szarych Szeregów oraz Rektorem Akademii Kultury Fizycznej im. Bronisława Czecha. | Kraków |
| 169. | 10.10.2025 | Konferencja pt. „Adwokat dla Przedsiębiorcy. Biznes, Innowacje i Odpowiedzialność”. Organizatorzy: Okręgowa Rada Adwokacka w Warszawie, Sekcja Praktyków Prawa ORA w Warszawie, Prokuratoria Generalna oraz Ministerstwo Rozwoju i Technologii. | Warszawa |
| 170. | 10.10.2025 | Inauguracja roku akademickiego 2025/2026 na Uniwersytecie Vizja. | Warszawa |
| 171. | 10.10.2025 | Spotkanie z profesorem Adamem Behanem na Wydziale Informatyki i Telekomunikacji AGH w Krakowie. | Kraków |
| 172. | 13.10.2025 | Trusted Economy Forum - CommonSign 2025. | Warszawa |
| 173. | 14.10.2025 | Konferencja „AI Summit Poland 2025”. Organizator: Evention. | Warszawa |
| 174. | 14.10.2025 | Konferencja The Hack Summit 2025. Organizatorzy: Fundacja Academic Partners wraz z Dowództwem Komponentu Wojsk Obrony Cyberprzestrzeni. | Warszawa |
| 175. | 15.10.2025 | Posiedzenie Sejmowej Komisji Sprawiedliwości i Praw Człowieka. | Warszawa |
| 176. | 15.10.2025 | Warsztaty - XIV Konwentu Ochrony Danych i Informacji. Organizator: FORSAFE Sp. z o.o. | online |
| 177. | 16.10.2025 | Konferencja „Etyczne podstawy odpowiedzialnego biznesu”. Organizator: ALK w Warszawie. | Warszawa |
| 178. | 16.10.2025 | Warsztaty szkoleniowe „Spotkania z RODO". Organizator: e-QSM Consulting. | Poznań |
| 179. | 16.10.2025 | Konferencja naukowa „Bezpieczeństwo informacji w organizacji i jej zasobów”. Organizator: UODO we współpracy z UWM w Olsztynie. | Olsztyn |
| 180. | 16-17.10.2025 | „UODO rusza w kraj” – województwo warmińsko-mazurskie. Organizatorzy: UODO, WPiA UWM w Olsztynie. | Olsztyn |
| 181. | 21.10.2025 | Sympozjum ORLEN CyberSec Forum 2025. | Warszawa |
| 182. | 21.10.2025 | Spotkanie ze studentami ALK w siedzibie UODO. | Warszawa |
| 183. | 23.10.2025 | Konferencja „30. edycja Banking & Insurance Forum”. Organizator: Rada Programowa Insurance Forum. | Warszawa |
| 184. | 23.10.2025 | Konferencja „Prywatnośći sztuczna inteligencja w edukacji – XVI edycja programu Twoje dane – Twoja sprawa”. | Warszawa |
| 185. | 24.10.2025 | Konferencja Naukowa „DGA – Innowacyjne zarządzanie danymi”. Organizatorzy: UODO, WPiA Uniwersytetu Łódzkiego, WPiA UKSW w Warszawie oraz Społeczny Zespół Ekspertów przy Prezesie UODO. | Warszawa |
| 186. | 27.10.2025 | Spotkanie dyrekcji UODO z dyrekcją KBW. Organizator: UODO. | Warszawa |
| 187. | 28.10.2025 | „UODO rusza w kraj” – województwo lubuskie. Organizator: UODO. | Gorzów Wielkopolski |
| 188. | 03.11.2025 | Konferencja naukowa pod Honorowym Patronatem Marszałka Sejmu RP pt. „Państwo demokratyczne w dobie sztucznej inteligencji". | Warszawa |
| 189. | 04.11.2025 | Forum Edukacji Dorosłych. Organizator: Fundacja Rozwoju Demokracji Lokalnej (FRDL). | Warszawa |
| 190. | 05.11.2025 | Spotkanie w ramach projektu Visegrad Alliance for Digital Rights and Disinformation Defense. Organizator spotkania: Uniwersytet Szczeciński. | online |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 191. | 05.11.2025 | „UODO rusza w kraj" – województwo mazowieckie. Organizator: UODO. | Płock |
| 192. | 06.11.2025 | Seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO". Organizatorzy: UODO, NRA, Stowarzyszenie Sędziów Polskich „Iustitia". | Warszawa |
| 193. | 06.11.2025 | Konferencja Med Smart pt. „Med Smart Science Forum". | Warszawa |
| 194. | 06.11.2025 | PAIH Forum Biznesu 2025. Organizator: Izba Gospodarki Elektroniczne. | Warszawa |
| 195. | 12.11.2025 | Konferencja Research@. | Warszawa |
| 196. | 12.11.2025 | Wizyta studyjna studentów Chrześcijańskiej Akademii Teologicznej w siedzibie UODO. | Warszawa |
| 197. | 14.11.2025 | Konferencja „Privacy, AI and Innovation Roundtable". Organizator: Kancelaria Bird & Bird. | Warszawa |
| 198. | 14.11.2025 | Warsztaty edukacyjne w ramach programu „Lekcje o finansach". Organizator: UODO we współpracy z Ministerstwem Finansów. | Warszawa |
| 199. | 17.11.2025 | Konferencja AIP pt. „Architektura Informacyjna Państwa – filar cyfrowej transformacji". | Warszawa |
| 200. | 19.11.2025 | Forum Fundacji Orange „W kierunku uważności". Organizator: Fundacja Orange. | Warszawa |
| 201. | 19.11.2025 | Konferencja „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach". Organizatorzy: UODO, SZE przy Prezesie UODO. | Warszawa |
| 202. | 20.11.2025 | XX Kongres Przemysłu i Rynku Motoryzacyjnego. Organizator: Stowarzyszenie Dystrybutorów i Producentów Części Motoryzacyjnych (SDCM). | Warszawa |
| 203. | 20.11.2025 | Konferencja „Adwokat dla oświaty - wyzwania współczesnej edukacji". Organizatorzy: Sekcja Prawa Oświatowego przy Okręgowej Radzie Adwokackiej w Warszawie, Izba Adwokacka w Warszawie, Sekcje Praktyków Prawa Okręgowej Rady Adwokackiej w Warszawie. | Warszawa |
| 204. | 24.11.2025 | XVII Konferencja Naukowa BwI 2025 „Cyberodpowiedzialność". Organizator: UKSW w Warszawie. | Warszawa |
| 205. | 24.11.2025 | Konferencja ,,Między faktem a feedem. Prezentacja raportu z badań jakościowych dotyczących podatności młodzieży na dezinformację i teorie spiskowe". Organizatorzy: Uczelnia Korczaka, Centrum Analiz Społeczeństwa Informacyjnego, Sejmowa Komisja do Spraw Dzieci i Młodzieży. | Warszawa |
| 206. | 26.11.2025 | IV Konferencja Naukowa „Bezpieczeństwo informacji w organizacji i jej zasobów". Organizatorzy: UODO, GUS, Ministerstwo Sportu i Turystyki, Śląski Urząd Wojewódzki, Uniwersytet Ekonomiczny w Katowicach. | Katowice |
| 207. | 26.11.2025 | XI edycja Forum Bezpieczeństwa Telekomunikacyjnego. Organizator: Orange Polska. | Warszawa |
| 208. | 26.11.2025 | XXXVII edycja Nagrody Głównego Inspektora Pracy im. Haliny Krahelskiej. | Warszawa |
| 209. | 26.11.2025 | Konferencja pt. „Nowe horyzonty biometrii – bezpieczeństwo, tożsamość, rozwój". Organizatorzy: Urząd Ochrony Danych Osobowych, Fundacja AI One Health oraz Społeczny Zespół Ekspertów przy Prezesie UODO. | Warszawa |

| Lp. | Data | Wydarzenie | Miejsce |
|---|---|---|---|
| 210. | 27.11.2025 | Konferencja „Nowe wyzwania prawne: regulacje, zadania regulatorów i ochrona danych”. Organizatorzy: UODO, ZUS. | Warszawa |
| 211. | 28.11.2025 r. | Konferencja „Sztuczna inteligencja w szkolnictwie wyższym i nauce”. Organizator: WPAiE UWr. | Wrocław |
| 212. | 1-3.12.2025 | Sympozjum „Cyberzagrożenia & Dezinformacja”. Organizator: Uniwersytet Jana Długosza w Częstochowie. | Częstochowa |
| 213. | 02.12.2025 | Warszawski Dialog na Rzecz Demokracji. Organizator: Ministerstwo Spraw Zagranicznych. | online |
| 214. | 02.12.2025 | II Spotkanie dot. AI, pt. „Biometria a AI Act. Kategoryzacja biometryczna vs. Identyfikacja biometryczna”. Organizator: PeakLegal.pl | Warszawa |
| 215. | 03.12.2025 | Spotkanie w MEN dot. ochrony wizerunku dzieci w kontekście działalności placówek edukacyjnych | Warszawa |
| 216. | 03.12.2025 | Wizyta uczniów szkoły podstawowej w siedzibie UODO w ramach programu MF „Lekcje o finansach”. Organizator: UODO. | Warszawa |
| 217. | 3-4.12.2025 | XII Krajowe Forum Ochrony Infrastruktury Krytycznej. Organizator: Rządowe Centrum Bezpieczeństwa – RCB we współpracy z KPRM. | Warszawa |
| 218. | 3 i 6.12.2025 | Warsztaty edukacyjne w ramach programu „Lekcje o finansach”. Organizator: UODO we współpracy z Ministerstwem Finansów. | Warszawa online |
| 219. | 04.12.2025 | XI. Konferencja Wydawnictwa C.H.Beck „Ochrona danych osobowych”. | online |
| 220. | 08.12.2025 | Szkolenie dla Naczelnej Rady Adwokackiej (NRA). Organizator: UODO. | Warszawa |
| 221. | 09-10.2025 | Szkolenie dla Inspektorów Ochrony Danych i specjalistów ds. ochrony danych. | Złote Brzozy |
| 222. | 10.12.2025 | Konferencja „Oświatowy parasol cyberbezpieczeństwa 2.0”. Organizator: CBZC – Centralne Biuro Zwalczania Cyberprzestępczości. | Katowice |
| 223. | 10.12.2025 | Spotkanie Rady Programowej Wydziału Bezpieczeństwa Narodowego w Akademii Sztuki Wojennej. | Warszawa |
| 224. | 10.12.2025 | Międzynarodowa konferencja „The Role of the Council of Europe’s Framework Convention on Artificial Intelligence in the Protection of Privacy and Personal Data – Legal, Ethical and Social Challenges in the AI Era”. Organizator: UODO we współpracy z SZE, Radą Europy i Europejską Komisją na rzecz Efektywności Wymiaru Sprawiedliwości (CEPEJ). | Warszawa |
| 225. | 12.12.2025 | Szkolenie UODO dla pracowników Krajowego Biura Wyborczego i jego delegatur. | online |
| 226. | 15.12.2025 | Otwarcie pierwszego terenowego punktu konsultacyjnego UODO w Rzeszowie. | Rzeszów |
| 227. | 15-16.12.2025 | Kongres Dzieci i Młodzieży. Organizator: Rzecznik Praw Dziecka. | Warszawa |
| 228. | 16.12.2025 | Konferencja ,,Taki Sam Start: e-commerce a gospodarka Polski". Organizator: e-Izba. | Warszawa |
| 229. | 17.12.2025 | Konferencja twinningowa 2025. Organizator: MSZ. | Warszawa |
| 230. | 17.12.2025 | Posiedzenie Sejmowej Komisji do Spraw Dzieci i Młodzieży. | Warszawa |
| 231. | 19.12.2025 | Seminarium Mistrzowskie pt. Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej a prawo krajowe: europeizacja prawa polskiego i rola sądów, Organizator: Uniwersytet Jagielloński. | Kraków |

**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 2025 r.**

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 1. | 10.01.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa do Usunięcia (CEF Right of Erasure) Europejskiej Rady Ochrony Danych. | online |
| 2. | 14.01.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 3. | 14-15.01.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 4. | 15.01.2025 | Future of Privacy Forum (FPF) - Forum Przyszłości Prywatności (FPF). | online |
| 5. | 16.01.2025 | 101. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | online |
| 6. | 19-24.01.2025 | Ewaluacja Schengen w obszarze ochrony danych osobowych. | Berno |
| 7. | 21.01.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 8. | 22.01.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 9. | 23.01.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG), w części z udziałem Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 10. | 24.01.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-Regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 11. | 27.01.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych w sprawie wytycznych dotyczących przetwarzania danych osobowych w celach badań naukowych. | online |
| 12. | 27-29.01.2025 | XIX Dzień Ochrony Danych Osobowych. | Bruksela |
| 13. | 29.01.2025 | Spotkanie Grupy Zadaniowej ds. ChatGPT (ChatGPT ESG) Europejskiej Rady Ochrony Danych. | online |
| 14. | 29.01.2025 | Posiedzenie Grupy Roboczej ds. Ochrony Danych Osobowych Rady UE (DAPIX). | Bruksela |
| 15. | 29-30.01.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 16. | 30.01.2025 | Spotkanie Grupy Zadaniowej ds. Administracyjnych Kar Pieniężnych (Fining Taskforce - FINING TF) Europejskiej Rady Ochrony Danych. | online |
| 17. | 31.01.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa do Usunięcia (CEF Right of Erasure) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 18. | 05.02.2025 | Spotkanie Grupy Roboczej Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee, CSC) | online |
| 19. | 11.02.2025 | 102. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | Bruksela |
| 20. | 12.02.2025 | Konferencja w Stałym Przedstawicielstwie RP przy UE „Towards A Safer Online Enviroment for Youth" („Ku bezpieczniejszemu środowisku online dla młodzieży"). | Bruksela |
| 21. | 13.02.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) Europejskiej Rady Ochrony Danych. | online |
| 22. | 14.02.2025 | Spotkanie Grupy Roboczej Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee, CSC) | online |
| 23. | 17.02.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement – TF INT) Europejskiej Rady Ochrony Danych. | online |
| 24. | 18-19.02.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych – (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 25. | 18-19.02.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 26. | 19.02.2025 | Spotkanie Grupy Zadaniowej ds. ChatGPT (ChatGPT TF) Europejskiej Rady Ochrony Danych. | online |
| 27. | 20.02.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 28. | 25.02.2025 | Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych. | online |
| 29. | 26-27.02.2025 | Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF ESG) Europejskiej Rady Ochrony Danych. | online |
| 30. | 28.02.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa do Usunięcia (CEF Right of Erasure) Europejskiej Rady Ochrony Danych. | online |
| 31. | 03.03.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 32. | 04.03.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup - BTLE ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 33. | 04.03.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 34. | 05.03.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) Europejskiej Rady Ochrony Danych. | online |
| 35. | 05-06.03.2025 | Posiedzenie Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee – CSC ESG) - Europejskiej Rady Ochrony Danych. | Bruksela |
| 36. | 05.03.2025 | Wspólna sesja certyfikacyjna z udziałem Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) oraz Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 37. | 05.03.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FM ESG) Europejskiej Rady Ochrony Danych. | online |
| 38. | 06.03.2025 | Spotkanie Grupy zadaniowej ds. Administracyjnych Kar Pieniężnych (Taskforce Fining – TF FINING) Europejskiej Rady Ochrony Danych. | online |
| 39. | 11.03.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG), w części z udziałem Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 40. | 12.03.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 41. | 13.03.2025 | 103. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | online |
| 42. | 14.03.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 43. | 17.03.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement – TF INT) Europejskiej Rady Ochrony Danych. | online |
| 44. | 18-23.03.2025 | 1 sesja stażowa Erasmus dla pracowników administracji publicznej. | Bruksela |
| 45. | 19.03.2025 | Spotkanie przygotowawcze Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych przed konferencją z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (The European Union Agency for Cybersecurity ENISA). | online |
| 46. | 20.03.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) ze zdalnym udziałem członków Podgrupy Ekspertów ds. Technologii (Technology -TECH ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 47. | 21.03.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa do Usunięcia (CEF Right of Erasure) Europejskiej Rady Ochrony Danych. | online |
| 48. | 24.03.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych w sprawie wytycznych dotyczących badań. | online |
| 49. | 25.03.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FM ESG) Europejskiej Rady Ochrony Danych. | online |
| 50. | 25.03.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 51. | 25.03.2025 | Szkolenie dla członków Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) z zakresu redagowania dokumentów Europejskiej Rady Ochrony Danych. | online |
| 52. | 26.03.2025 | Spotkanie Grupy Zadaniowej ds. ChatGPT (ChatGPT TF) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 53. | 27.03.2025 | Spotkanie Grupy Roboczej Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC). | online |
| 54. | 27.03.2025 | Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users ESG) Europejskiej Rady Ochrony Danych. | online |
| 55. | 27.03.2025 | Szkolenie członków Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) z zakresu redagowania dokumentów Europejskiej Rady Ochrony Danych. | online |
| 56. | 01.04.2025 | Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory SAESG) w sprawie wytycznych dotyczących powiązań między ustawą o rynku cyfrowym (DMA) a ogólnym rozporządzeniem o ochronie danych (RODO). | online |
| 57. | 01-02.04.2025 | Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement -ENF ESG ) Europejskiej Rady Ochrony Danych. | Bruksela |
| 58. | 02.04.2025 | Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement - ENF ESG) z udziałem członków Podgrupy Ekspertów ds. Współpracy (Cooperation- COOP ESG) Europejskiej Rady Ochrony Danych. | online |
| 59. | 03.04.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health- CEH ESG) Europejskiej Rady Ochrony Danych w sprawie wytycznych dotyczących badań naukowych. | online |
| 60. | 04.04.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych w sprawie wytycznych dotyczących badań naukowych. | online |
| 61. | 08.04.2025 | 104. Posiedzenie Plenarne Europejskiej Rady Ochrony Danych. | online |
| 62. | 09.04.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation- CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 63. | 10.04.2025 | Połączone spotkanie *ad hoc* Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ESG) oraz Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 64. | 10.04.2025 | Spotkanie Grupy Zadaniowej ds. Administracyjnych Kar Pieniężnych (Taskforce Fining ) Europejskiej Rady Ochrony Danych. | Bruksela |
| 65. | 10.04.2025 | Spotkanie Grupy Roboczej Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC). | online |
| 66. | 10-11.04.2025 | Spotkanie inauguracyjne zespołu sprawozdawców aktualizacji wytycznych dotyczących inspektorów ochrony danych. | Haga |
| 67. | 14.04.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement - INT ESG) Europejskiej Rady Ochrony Danych. | online |
| 68. | 15.04.2025 | Posiedzenie Grupy Roboczej ds. Ochrony Danych Osobowych (DAPIX) Rady UE. | Bruksela |
| 69. | 16.04.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 70. | 23.04.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| | | Health - CEH ESG) z udziałem członków Podgrupy Ekspertów ds. Technologii (Technology -TECH ESG) Europejskiej Rady Ochrony Danych. | |
| 71. | 23-24.04.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 72. | 24.04.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 73. | 25.04.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 74. | 29.04.2025 | Spotkanie Grupy Roboczej Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC) | online |
| 75. | 29.04.2025 | Wspólne spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement ENF) i Podgrupy Ekspertów ds. Współpracy (Cooperation COOP) Europejskiej Rady Ochrony Danych inicjujące prace wspólnego zespołu wdrożeniowego (joint implementation team, JIT). | online |
| 76. | 29-30.04.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers ITS), w części z udziałem Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement BTLE) oraz w części z udziałem Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health CEH) Europejskiej Rady Ochrony Danych. | online |
| 77. | 30.04.2025 | Wspólne spotkanie ekspertów ds. interakcji i współpracy międzyregulacyjnej (Cross-regulatory Interplay & Cooperation CIC ESG) i Podgrupy Ekspertów ds. Technologii – (Technology -TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 78. | 05.05.2025 | 105. Posiedzenie Plenarne Europejskiej Rady Ochrony Danych. | online |
| 79. | 06-07.05.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 80. | 6-9.05.2025 | Wiosenna Konferencja Europejskich Organów Ochrony Danych. | Batumi |
| 81. | 07.05.2025 | Wspólne Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 82. | 11.05.2025 | Sympozjum Prywatności w Wenecji. | Wenecja |
| 83. | 12-13.05.2025 | Warsztaty o trendach generatywnej AI. | Berlin |
| 84. | 13.05.2025 | Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF ESG) Europejskiej Rady Ochrony Danych. | online |
| 85. | 13.05.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 86. | 14.05.2025 | Spotkanie Grupy Zadaniowej ds. ChatGPT Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 87. | 15.05.2025 | Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 88. | 15.05.2025 | Privacy Symposium. | Wenecja |
| 89. | 15-16.05.2025 | Konferencja ,,The future od democracy in the digital era: the results of the infolead project". | Florencja |
| 90. | 19.05.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 91. | 20-21.05.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 92. | 22.05.2025 | Spotkanie Podgrupy ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) z udziałem członków Podgrupy Ekspertów ds. Technologii (Technology -TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 93. | 26-27.05.2025 | Druga edycja Dialogu Politycznego Wysokiego Szczebla w ramach Sojuszu Cyfrowego UE-LAC na temat e-administracji. | Tallin |
| 94. | 26.05.2025 | Wspólne spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) i Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 95. | 26-28.05.2025 | Europejskie Forum Edukacji Cyfrowej Obywateli. | Strasburg |
| 96. | 26.05.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych w sprawie wytycznych dot. badań naukowych. | online |
| 97. | 27.05.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych dotyczące aktualizacji wytycznych Komisji Europejskiej w sprawie modelowych postanowień umownych w akcie w sprawie danych oraz przygotowujące do spotkania Europejskiej Rady Innowacyjności w zakresie danych. | online |
| 98. | 28.05.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FM ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 99. | 02-04.06.2025 | Sieć Rzeczników (Communications Network) - coroczne spotkanie | Bruksela |
| 100. | 03.06.2025 | Wspólne spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) oraz Podgrupy ekspertów ds. mediów społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych w sprawie konsultacji publicznych Art. 28 Aktu o usługach cyfrowych. | online |
| 101. | 03-04.06.2025 | 106. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | Bruksela |
| 102. | 03-08.06.2025 | Konferencja Caribbean Dialogue. Organizator: DIGITAL ALLIANCE EU-LAC POLICY DIALOGUES. | Kingston |
| 103. | 04.06.2025 | Wspólne Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| | | (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | |
| 104. | 10.06.2025 | Posiedzenie Grupy ds. Koordynacji Nadzoru nad EURODAC (EURODAC Supervision Coordination Group). | Bruksela |
| 105. | 10.06.2025 | Posiedzenie Grupy ds. Koordynacji Nadzoru nad Systemem Informacji Celnej (CIS Supervision Coordination Group). | Bruksela |
| 106. | 10-11.06.2025 | Posiedzenie Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee – CSC) | Bruksela |
| 107. | 11.06.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) Europejskiej Rady Ochrony Danych. | online |
| 108. | 11-13.06.2025 | Warsztaty Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych. | Berlin |
| 109. | 12.06.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 110. | 12-13.06.2025 | Spotkanie Grupy Organów Ochrony Danych Państw Europy Środkowej i Wschodniej. Organizator: UODO. | Kraków Lutosławice |
| 111. | 13.06.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 112. | 16.06.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 113. | 16.06.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 114. | 16.06.2025 | Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users) Europejskiej Rady Ochrony Danych. | Bruksela |
| 115. | 16-19.06.2025 | 48. Posiedzenie plenarne Komitetu Konwencji 108 Rady Europy. | Strasburg |
| 116. | 17.06.2025 | Spotkanie Podgrupy Ekspertów ds. egzekwowania Prawa (Enforcement – ENF ESG) Europejskiej Rady Ochrony Danych. | online |
| 117. | 17.06.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 118. | 17-18.06.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 119. | 18.06.2025 | Spotkanie członków Podgrupy Ekspertów ds. Współpracy (Cooperation - COOP ESG) Europejskiej Rady Ochrony Danych należących do wspólnego zespołu wdrożeniowego (joint implementation team, JIT). | online |
| 120. | 18-20.06.2025 | Udział w projekcie europejskim: „Sprawiedliwość, prawa podstawowe i sztuczna inteligencja” (Justice Fundamental Rights and Artificial Intelligence). | Paryż |
| 121. | 19.06.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych - aktualizacja klauzul modelowych. | online |
| 122. | 20.06.2025 | Spotkanie ad hoc Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 123. | 23.06.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement - TF INT) Europejskiej Rady Ochrony Danych. | online |
| 124. | 25.06.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 125. | 26.06.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions -KEYP ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 126. | 27.06.2025 | Spotkanie *ad hoc* Podgrupy ekspertów ds. kluczowych przepisów (Key Provisions -KEYP) Europejskiej Rady Ochrony Danych. | online |
| 127. | 30.06-4.07.2025 | Udział w spotkaniu Grupy Berlińskiej 75th MEETING of the „Berlin Group" – International Working Group on Data Protection in Technology - (IWGDPT). | Tbilisi |
| 128. | 01.07.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 129. | 1-3.07.2025 | Spotkanie na wysokim szczeblu Europejskiej Rady Ochrony Danych. | Helsinki |
| 130. | 02-03.07.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 131. | 04.07.2025 | Spotkanie Grupy Zadaniowej ds. Administracyjnych Kar Pieniężnych (Taskforce Fining – TF FINING) Europejskiej Rady Ochrony Danych. | online |
| 132. | 04.07.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa do Usunięcia (CEF rights to erasure) Europejskiej Rady Ochrony Danych. | online |
| 133. | 07.07.2025 | Spotkanie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory - SA ESG) Europejskiej Rady Ochrony Danych w sprawie wytycznych wyjaśniających interakcję między ustawą o usługach cyfrowych (DSA) a RODO. | online |
| 134. | 08.07.2025 | 107. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | online |
| 135. | 09.07.2025 | Spotkanie Grupy Zadaniowej ds. ChatGPT (Generative AI Enforcement Taskforce GAIE-TF) Europejskiej Rady Ochrony Danych. | online |
| 136. | 09.07.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FM ESG) Europejskiej Rady Ochrony Danych. | online |
| 137. | 11.07.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG), w części z udziałem Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych | online |
| 138. | 16.07.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 139. | 18.07.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych. | online |
| 140. | 23.07.2025 | Połączone spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) oraz Podgrupy Ekspertów ds. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| | | Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | |
| 141. | 24.07.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement – TF INT) Europejskiej Rady Ochrony Danych. | online |
| 142. | 31.07.2025 | Wspólne spotkanie przedstawicieli Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) oraz przedstawicieli Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 143. | 02.09.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 144. | 05.09.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 145. | 09-10.09.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 146. | 09-10.09.2025 | Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement - ENF ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 147. | 11.09.2025 | 108. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | online |
| 148. | 12.09.2025 | Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych. | online |
| 149. | 15.09.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation CIC ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 150. | 15.09.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement - TF INT) Europejskiej Rady Ochrony Danych. | online |
| 151. | 15-19.09.2025 | 47. Międzynarodowa Konferencja Global Privacy Assembly - GPA. | Seul |
| 152. | 16.09.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 153. | 16-17.09.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 154. | 17.09.2025 | Posiedzenie Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC). | online |
| 155. | 18.09.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation - COOP ESG) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 156. | 19.09.2025 | Spotkanie Grupy Zadaniowej ds. Administracyjnych Kar Pieniężnych (Taskforce Fining - FINING TF) Europejskiej Rady Ochrony Danych. | online |
| 157. | 22.09.2025 | Spotkanie Grupy Skoordynowanego działania w zakresie korzystania z usług opartych na chmurze w sektorze publicznym, z udziałem członków Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement - ENF ESG) oraz członków Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 158. | 22.09.2025 | Improving the implementation of the AI Act in Poland – study visit project | online |
| 159. | 22.09.2025 | Wspólna spotkanie *ad hoc* Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) i Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 160. | 23.09.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 161. | 23.09.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG), Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG), Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 162. | 23-27.09.2025 | Spotkanie inicjatywy współpracy UE i krajów latynoamerykańskich oraz karaibskich. | Antigua |
| 163. | 24.09.2025 | Spotkanie Grupy Zadaniowej ds. ChatGPT (Taskforce on ChatGPT ESG) Europejskiej Rady Ochrony Danych. | online |
| 164. | 24.09.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FM ESG) Europejskiej Rady Ochrony Danych. | online |
| 165. | 24.09.2025 | Wspólne spotkanie *ad hoc* Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) i Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 166. | 25.09.2025 | Wspólne spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users - IT ESG), Podgrupy ekspertów ds. współpracy (Cooperation - COOP ESG) oraz Podgrupy ekspertów ds. egzekwowania prawa (Enforcement - ENF ESG) Europejskiej Rady Ochrony Danych. | online |
| 167. | 25.09.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 168. | 26.09.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 169. | 29-30.09.2025 | Konferencja RAID 2025 - dotyczące sztucznej inteligencji, Internetu i regulacji danych. | Bruksela |
| 170. | 30.09-02.10.2025 | Warsztaty nt. współpracy między organami ochrony danych w zakresie audytu systemów AI i wdrażania skutecznych mechanizmów nadzorczych. | Bruksela |
| 171. | 01.10.2025 | Udział w warsztatach pt.: Osobista superinteligencja. | Berlin |
| 172. | 01-02.10.2025 | Konferencja „Dni Prywatności". Panel dyskusyjny „Dane w erze sztucznej inteligencji". Spotkanie z przedstawicielami czeskiego organu nadzorczego. | Praga |
| 173. | 07-08.10.2025 | 109. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | Bruksela |
| 174. | 07-09.10.2025 | Konferencja „Europejskie Forum Edukacji Cyfrowej Obywateli". | Strasburg |
| 175. | 08.10.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 176. | 10.10.2025 | Spotkania *ad hoc* Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 177. | 10.10.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa Dostępu (CEF Right of Access ) Europejskiej Rady Ochrony Danych. | online |
| 178. | 14-15.10.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 179. | 14-15.10.2025 r. | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 180. | 15.10.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych z udziałem członków Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions -KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 181. | 16.10.2025 | Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych. | online |
| 182. | 16.10.2025 | 110. Plenarne Posiedzenie *ad hoc* Europejskiej Rady Ochrony Danych. | online |
| 183. | 17.10.2025 | Spotkanie dot. PACE - Data Governance Act Implementation. | online |
| 184. | 17.10.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FMESG) Europejskiej Rady Ochrony Danych. | online |
| 185. | 18-19.10.2025 | Konferencja „Ensuring Quality Education in the AI Era – Introducing the Council of Europe Compass for AI and Education". | Strasburg |
| 186. | 20.10.2025 | Połączone spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement - INT TF), Podgrupy Ekspertów ds. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| | | Współpracy (Cooperation - COOP ESG), Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement - ENF ESG) oraz Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | |
| 187. | 20-21.10.2025 | Szczyt Europejski CIPL pt. „Tworzenie kolejnego modelu cyfrowego zarządzania”. | Amsterdam |
| 188. | 21.10.2025 | Spotkanie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement - ENF ESG) Europejskiej Rady Ochrony Danych. | online |
| 189. | 22.10.2025 | Spotkanie Podgrupy Ekspertów ds. Współpracy (Cooperation - COOP ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 190. | 22.10.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 191. | 23.10.2025 | Spotkanie Grupy Zadaniowej ds. Administracyjnych Kar Pieniężnych (Taskforce Fining) Europejskiej Rady Ochrony Danych. | Bruksela |
| 192. | 23.10.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 193. | 24.10.2025 | Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users ESG) Europejskiej Rady Ochrony Danych. | online |
| 194. | 27.10.2025 | Spotkanie Zespołu Sprawozdawców Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) dot. opinii EROD w sprawie greckich kryteriów certyfikacji. | online |
| 195. | 29.10.2025 | Spotkanie Grupy Zadaniowej ds. Generatywnej Sztucznej Inteligencji (Generative AI Enforcement Taskforce - GAIE TF) Europejskiej Rady Ochrony Danych. | online |
| 196. | 29-30.10.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement (BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 197. | 03.11.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych dotyczące projektów opinii EROD dla mechanizmów certyfikacji procedowanych w drugim oknie czasowym przewidzianym dla oceny tych mechanizmów. | online |
| 198. | 03-05.11.2025 | 49. Posiedzeniu plenarne Komitetu Konwencji 108 Rady Europy. | Strasburg |
| 199. | 04.11.2025 | 111. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | online |
| 200. | 05.11.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-dministracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) z udziałem Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) Europejskiej Rady Ochrony Danych. | online |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 201. | 06.11.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 202. | 07.11.2025 | Spotkanie Zespołu Sprawozdawców Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) dot. opinii EROD w sprawie greckich kryteriów certyfikacji. | online |
| 203. | 10.11.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 204. | 10.11.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement - TF INT) Europejskiej Rady Ochrony Danych. | online |
| 205. | 12.11.2025 | Spotkanie Podgrupy ekspertów ds. technologii (Technology - TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 206. | 12.11.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG) z udziałem przedstawicieli Podgrupy Ekspertów ds. Kluczowych Przepisów, Podgrupy Ekspertów ds. Interakcji i Współpracy EMiędzyregulacyjnej, oraz Podgrupy ekspertów ds. Granic, Podróży i Egzekwowania Prawa Europejskiej Rady Ochrony Danych w sprawie wspólnych wytycznych dotyczących współzależności między Aktem o sztucznej inteligencji (AI Act) a przepisami o ochronie danych. | online |
| 207. | 13.11.2025 | Spotkanie Grupy Roboczej Komitetu Skoordynowanego Nadzoru (Coordinated Supervision Committee - CSC). | online |
| 208. | 14.11.2025 | Spotkanie Grupy Skoordynowanego Działania w zakresie Prawa do Usunięcia (CEF rights to erasure) Europejskiej Rady Ochrony Danych. | online |
| 209. | 17-19.11.2025 | Udział w Europejskich Warsztatach Skargowych. | Kosowo |
| 210. | 18.11.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 211. | 18-19.11.2025 | Konferencja „The Way Forward" w ramach projektu DIGI.DR. zamykająca Europejski Rok Edukacji Cyfrowej Obywateli. | Lublana |
| 212. | 18-21.11.2025 | Spotkanie Grupy Berlińskiej. | Montevideo |
| 213. | 19.11.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) Europejskiej Rady Ochrony Danych. | online |
| 214. | 19-20.11.2025 | Udział w konferencji: Big Data Conference Europe 2025. | Wilno |
| 215. | 20.11.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FM ESG) Europejskiej Rady Ochrony Danych. | online |
| 216. | 25-26.11.2025 | Międzynarodowa konferencja „Axiology of the legal System: Theory and Practice" Organizator: Wydział Prawa Kanonicznego Papieskiego Uniwersytetu Gregoriańskiego w Rzymie. | Rzym |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 217. | 27.11.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) z udziałem przedstawicieli Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions (KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 218. | 27.11.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement (BTLE ESG) Europejskiej Rady Ochrony Danych. | online |
| 219. | 2-3.12.2025 | 112. Posiedzenie plenarne Europejskiej Rady Ochrony Danych. | Bruksela |
| 220. | 04.12.2025 | Spotkanie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media - SOCM ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 221. | 04.12.2025 | Wspólne spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) i Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych. | online |
| 222. | 05.12.2025 | Spotkanie *ad hoc* Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) z udziałem członków Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) Europejskiej Rady Ochrony Danych. | online |
| 223. | 05.12.2025 | Spotkanie Podgrupy Ekspertów ds. Interakcji i Współpracy Międzyregulacyjnej (Cross-regulatory Interplay & Cooperation - CIC ESG) Europejskiej Rady Ochrony Danych. | online |
| 224. | 05.12.2025 | Spotkanie Grupy Skoordynowanego Działania w Zakresie Prawa do Usunięcia (CEF Rights to Erasure) Europejskiej Rady Ochrony Danych. | online |
| 225. | 08.12.2025 | Spotkanie Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International Engagement - TF INT) Europejskiej Rady Ochrony Danych. | online |
| 226. | 10.12.2025 | Spotkanie Podgrupy ekspertów ds. egzekwowania prawa (Enforcement - ENF ESG) Europejskiej Rady Ochrony Danych. | online |
| 227. | 10-12.12.2025 | Cykl warsztatów dot. klasyfikacji systemów sztucznej inteligencji jako wysokiego ryzyka. Organizator: Biuro ds. sztucznej inteligencji Komisji Europejskiej. | online |
| 228. | 11.12.2025 | Spotkanie Grupy Zadaniowej ds. Administracyjnych Kar Pieniężnych (Taskforce Fining) Europejskiej Rady Ochrony Danych. | online |
| 229. | 11.12.2025 | Spotkanie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement - BTLE ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 230. | 11.12.2025 | Międzynarodowy Szczyt Sztucznej Inteligencji 2025 | Bruksela |

| Lp. | Data | Konferencja/Seminarium/Spotkanie | Miejsce |
|---|---|---|---|
| 231. | 11-12.12.2025 | Spotkanie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health CEH ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 232. | 12.12.2025 | Piąte posiedzenie Grupy Wysokiego Szczebla ds. Ustawy o Rynkach Cyfrowych (DMA) | Bruksela |
| 233. | 12.12.2025 | Spotkanie Podgrupy Ekspertów ds. Użytkowników IT (IT Users ESG) Europejskiej Rady Ochrony Danych. | online |
| 234. | 15.12.2025 | Spotkanie Podgrupy Ekspertów ds. Technologii (Technology - TECH ESG) Europejskiej Rady Ochrony Danych. | online |
| 235. | 16-17.12.2025 | Spotkanie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers - ITS ESG) Europejskiej Rady Ochrony Danych, w części z udziałem Grupy Zadaniowej ds. Zaangażowania Międzynarodowego (International engagement - INT TF) i w części z udziałem Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health - CEH ESG) | online |
| 236. | 16-17.12.2025 | Spotkanie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions - KEYP ESG) Europejskiej Rady Ochrony Danych. | Bruksela |
| 237. | 18.12.2025 | Spotkanie Podgrupy Ekspertów ds. Finansowych (Financial Matters - FMESG) Europejskiej Rady Ochrony Danych. | online |

**Załącznik nr 5:**

## Działalność Urzędu Ochrony Danych Osobowych w 2025 r. w liczbach

| | | **2025 r.** |
|---|---|---|
| **DECYZJE** | **skargowe** | 2020 |
| | **karowe** | 20 |
| | **dotyczce kontroli i naruszeń** | 31 |
| | **wydane w ramach współpracy międzynarodowej** | 20 |
| | **dotyczące kodeksu postępowania** | 1 |
| | **OGÓŁEM** | 2092 |
| **SKARGI** | **Liczba skarg, które wpłynęły do Prezesa UODO** | **12883** |
| | **Liczba zakończonych postępowań skargowych OGÓŁEM** | **7831** |
| **Liczba skarg z podziałem na sektory:** | **prywatny** | 594 |
| | **finansowy, ubezpieczeń i telekomunikacji** | 401 |
| | **zdrowia, zatrudnienia i szkolnictwa** | 390 |
| | **publiczny** | 499 |
| | **skargi o charakterze transgranicznym** | 56 |
| **NARUSZENIA** | **Liczba zgłoszeń naruszeń ochrony danych** | **22435** |
| **ADMINISTRACYJNE KARY PIENIĘŻNE** | **Liczba administracyjnych kar pieniężnych nałożonych przez Prezesa UODO** | 32 |
| | **Liczba decyzji dot. kar pieniężnych** | 20 |
| | **ŁĄCZNA KWOTA KAR w zł** | 64 436 940,25 |
| **KONTROLE** | **Liczba kontroli** | 76 |
| | **Liczba sprawdzeń stosowania przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości** | 20 |
| **PROJEKTY AKTÓW PRAWNYCH** | **Liczba zaopiniowanych projektów aktów prawnych** | 981 |

| | | 2025 r. |
|---|---|---|
| | | |
| **Uprzednie konsultacje** | **Liczba wniosków o uprzednie konsultacje** | 4 |
| **Kodeksy postępowania** | **Liczba zatwierdzonych kodeksów postępowania** | 1 |
| **Akredytacja** | **Liczba wniosków o akredytację podmiotów monitorujących kodeksy postępowania** | 1 |
| **PYTANIA dotyczące wykładni prawa** | **Liczba pytań od administratorów i osób fizycznych** | 1815 |
| | **Liczba pytań od IOD** | 218 |
| | **Liczba pytań od organów nadzorczych z innych państw** | 57 |
| | **OGÓŁEM** | 2090 |
| **Wnioski prejudycjalne** | **Liczba wniosków prejudycjalnych skierowanych do TSUE przez sądy z różnych państw UE, które wpłynęły do polskiego organu nadzorczego** | 20 |
| **WYSTĄPIENIA** | **Liczba wystąpień w trybie art. 52 ust. 1 ustawy o ochronie danych osobowych** | **43** |
| **Zawiadomienia o popełnieniu przestępstwa** | **Liczba zawiadomień** | 8 |
| **Sprawy przed sądami administracyjnymi** | **Liczba decyzji Prezesa UODO zaskarżonych do WSA w Warszawie** | **218** |
| | **Liczba decyzji zaskarżonych do NSA** | **63** |
| | **Liczba wyroków uchylających decyzję Prezesa UODO** | **69** |
| | **Liczba wyroków utrzymujących w mocy decyzje Prezesa UODO** | **181** |