SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Prezes Urzędu Ochrony Danych Osobowych
PU.0331.1.2023

Druk nr 3641

Warszawa, 30 sierpnia 2023 r.

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek,

uprzejmie przedkładam na ręce Pani Marszałek

- Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022.

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 (Dz. Urz. UE L 119 z 04.05.2016 str. 1 ze zmianą ogłoszoną w Dz. Urz. UE L 127 z 23.05.2018 str. 2), a także art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz.1781).

Zgodnie z treścią art. 50 ust. 1 przywołanej ustawy, Prezes Urzędu Ochrony Danych Osobowych raz w roku do dnia 31 sierpnia przedstawia Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu, sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.

.

Z wyrazami szacunku

(-) Jan Nowak

SPRAWOZDANIE Z DZIAŁALNOŚCI PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH W ROKU 2022

SPRAWOZDANIE Z DZIAŁALNOŚCI
PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
w ROKU 2022

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 od 1 stycznia 2022 r. do 31 grudnia 2022 r.

Zgodnie z art. 59 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2], każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje środków podjętych zgodnie z art. 58 ust. 2 RODO. Sprawozdania te są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem państwa członkowskiego. Są one udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych[3]. Powołany przepis jest uzupełniony przez art. 50 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[4], w myśl którego Prezes Urzędu Ochrony Danych Osobowych[5] raz w roku, do dnia 31 sierpnia przedstawia Sejmowi RP, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności, zawierające w szczególności informację 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 (ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych). Prezes UODO udostępnia sprawozdanie na swojej stronie podmiotowej Biuletynu Informacji Publicznej (ust. 2 ustawy z dnia 10 maja 2018 r. 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), dalej: „RODO" lub „ogólne rozporządzenie o ochronie danych".

3 Dalej także: „EROD".

4 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781), dalej: „ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych".

5 Dalej także: „Prezes UODO".

Spis treści

I. WPROWADZENIE 9

1. ŹRÓDŁA PRAWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH 9

2. URZĄD OCHRONY DANYCH OSOBOWYCH 14

2.1. Struktura organizacyjna 15

2.2. Pracownicy UODO 16

2.3. Budżet UODO za 2022 r. 17

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI 18

1. WPROWADZENIE 18

2. ZADANIA JEDNOSTEK ORGANIZACYJNYCH UODO 20

3. ORZECZNICTWO SĄDÓW ADMINISTRACYJNYCH W SPRAWACH DECYZJI LUB POSTANOWIEŃ ORGANU NADZORCZEGO 21

4. WYDAWANIE DECYZJI ADMINISTRACYJNYCH I ROZPATRYWANIE SKARG 26

4.1. Skargi 27

4.1.1. Sektor publiczny 31

4.1.2. Sektor prywatny 35

4.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa 42

4.1.4. Sektor finansów, telekomunikacji i ubezpieczeń 50

4.1.5. Postępowania transgraniczne 59

4.2. Zawiadomienie o podejrzeniu popełnienia przestępstwa 67

4.3. Skargi na działanie UODO 69

5. KONTROLA PRZESTRZEGANIA PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH 69

5.1. Aplikacje mobilne 70

5.2. Profilowanie 70

5.3. System Informacyjny Schengen, Wizowy System Informacyjny 71

5.4. Inspektor Ochrony Danych 72

5.5. Kontrole w wyniku zgłoszonego naruszenia 73

5.6. Decyzje administracyjne w postępowaniach kontrolnych 76

6. EGZEKUCJA ADMINISTRACYJNA – ZAPEWNIENIE WYKONANIA DECYZJI 76

7. OPINIOWANIE PROJEKTÓW AKTÓW PRAWNYCH I ROZPORZĄDZEŃ DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH 82

7.1. Ocena skutków dla ochrony danych 87

7.2. Test prywatności 87

7.3. Wyłączenia bądź ograniczenia praw osób, których dane dotyczą 93

7.4. Precyzyjne określenie ról podmiotów w procesie przetwarzania danych 94

7.5. Zbiory danych / łączenie baz danych 99

7.6. Korzystanie z nowych technologii przy przetwarzaniu danych osobowych 104

7.7. Przetwarzanie danych szczególnych kategorii 108

7.8. Środki porozumiewania się na odległość 112

7.9. Zautomatyzowane przekazywanie danych 113

7.10. Umowy międzynarodowe 115

7.11. Inne projekty aktów prawnych ... 116
7.12. Podsumowanie ... 124
8. ZGŁASZANIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ... 127
8.1. Najczęściej zgłaszane oraz typowe naruszenia w 2022 r. ... 129
8.2. Wyjaśnienia ... 132
8.3. Postępowania administracyjne ... 133
8.4. Decyzje administracyjne ... 134
9. ADMINISTRACYJNE KARY PIENIĘŻNE ... 138
9.1. Administracyjne kary pieniężne w postępowaniach kontrolnych ... 142
9.2. Administracyjne kary pieniężne w związku z naruszeniem ... 146
10. UPRZEDNIE KONSULTACJE ... 150
11. KODEKSY POSTĘPOWANIA ... 153
12. AKREDYTACJA PODMIOTÓW MONITORUJĄCYCH KODEKSY POSTĘPOWANIA ... 158
13. CERTYFIKACJA ... 160
14. PYTANIA PRAWNE, WNIOSKI O DOSTĘP DO INFORMACJI I WYSTĄPIENIA PREZESA UODO ... 161
14.1. Pytania prawne ... 161
14.1.1. Pytania prawne od administratorów i osób fizycznych ... 162
14.1.2. Pytania prawne od inspektorów ochrony danych ... 183
14.1.3. Działania informacyjno-edukacyjne podejmowane przez IOD ... 196
14.2. Wnioski o dostęp do informacji publicznej ... 201
14.3. Wystąpienia ... 204

III. DZIAŁALNOŚĆ EDUKACYJNO-INFORMACYJNA ... 210
1. DZIAŁALNOŚĆ EDUKACYJNA ... 210
1.1. Szkolenia zewnętrzne ... 211
1.2. Szkolenia wewnętrzne ... 211
1.3. Letnia Akademia Ochrony Danych Osobowych ... 212
1.4. Ogólnopolski program edukacyjny „Twoje dane Twoja sprawa” ... 213
1.5. Konferencje, seminaria, spotkania ... 219
2. DZIAŁALNOŚĆ INFORMACYJNA ... 227
2.1. Strona internetowa i media społecznościowe ... 227
2.2. Współpraca z mediami ... 232
2.3. Odpowiedzi na indywidualne pytania dziennikarzy ... 234
2.4. Newsletter UODO dla inspektorów ochrony danych - IOD ... 235
2.5. Infolinia UODO ... 236
2.6. Inne ... 237

IV. UCZESTNICTWO W PRACACH MIĘDZYNARODOWYCH ORGANIZACJI I INSTYTUCJI ZAJMUJĄCYCH SIĘ ZAGADNIENIAMI OCHRONY DANYCH OSOBOWYCH ... 241
1. WSPÓŁPRACA W RAMACH EROD ... 241
2. PODGRUPY EKSPERTÓW EROD ... 242
3. GRUPY ZADANIOWE EROD ... 245
4. SIEĆ INSPEKTORÓW OCHRONY DANYCH ... 245

5. NADZÓR NAD WIELKOSKALOWYMI SYSTEMAMI 246
6. PRACE EROD W 2022 R. 247
6.1. Wytyczne 248
6.2. Konsultacje prawodawcze i dokumenty skierowane do instytucji UE lub organów krajowych 249
6.3. Inne wskazówki i oświadczenia 249
6.4. Opinie dotyczące spójności 250
6.5. Wiążące decyzje 251
6.6. Współpraca organów i egzekwowanie prawa 251
7. WSPÓŁPRACA W RAMACH IMI 253
8. WNIOSKI PREJUDYCJALNE 259
9. PRZEKAZYWANIE DANYCH OSOBOWYCH POZA EOG 262
10. INNE SPRAWY 263
11. MIĘDZYNARODOWE WARSZTATY 264
12. POROZUMIENIE O WSPÓŁPRACY 264
13. WIZYTA STUDYJNA, 10-14.10.2022 R. 265
14. MIĘDZYNARODOWE KONFERENCJE, SEMINARIA I SPOTKANIA 265

V. PODSUMOWANIE 273
ZAŁĄCZNIK NR 1 ..... *287*
WYKAZ ADMINISTRACYJNYCH KAR PIENIĘŻNYCH NAŁOŻONYCH PRZEZ PREZESA UODO W 2022 R.
ZAŁĄCZNIK NR 2 ..... *288*
WYKAZ WYDARZEŃ OBJĘTYCH PATRONATEM PREZESA UODO W 2022 R.
ZAŁĄCZNIK NR 3 ..... *289*
WYKAZ KONFERENCJI, SEMINARIÓW, SPOTKAŃ I INNYCH WYDARZEŃ KRAJOWYCH I MIĘDZYNARODOWYCH Z UDZIAŁEM PREZESA UODO LUB JEGO PRZEDSTAWICIELI, ZORGANIZOWANYCH W 2022 R. W POLSCE PRZEZ UODO LUB INNE PODMIOTY.
ZAŁĄCZNIK NR 4 ..... *293*
WYKAZ WYDARZEŃ MIĘDZYNARODOWYCH I EUROPEJSKICH, W TYM POSIEDZEŃ PLENARNYCH EROD I PODGRUP, Z UDZIAŁEM PREZESA UODO LUB JEGO PRZEDSTAWICIELI, KTÓRE ODBYŁY SIĘ W 2022 R.

Szanowni Państwo,

zgodnie z ustawą z 10 maja 2018 r. o ochronie danych osobowych, przedkładam Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu sprawozdanie ze swojej działalności w roku 2022. Na mocy przepisu art. 59 ogólnego rozporządzenia o ochronie danych, sprawozdanie jest także udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

Niniejsze sprawozdanie przedstawia najważniejsze ustalenia dot. 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 2022 r. minął czwarty, pełny rok kalendarzowy bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych w polskim porządku prawnym. 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 nad funkcjonowaniem Urzędu Ochrony Danych Osobowych – jak jego obecna struktura organizacyjna sprawdza się w praktyce pod kątem wymagań, jakie stawia RODO.

Zapraszam do lektury sprawozdania z działalności polskiego organu ochrony danych osobowych w roku 2022, które jest nie tylko rzetelną informacją o działalności polskiego organu nadzorczego, ale również przedstawia proces analizy prawnej leżącej u podstaw podejmowania decyzji służących zwiększeniu poziomu bezpieczeństwa danych osobowych obywateli.

Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

I. WPROWADZENIE

1. Źródła prawa w zakresie ochrony danych osobowych

Podstawę prawną działania Prezesa UODO stanowią RODO i ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, a także wydane na jej podstawie akty wykonawcze:

- rozporządzenie Rady Ministrów z dnia 14 stycznia 2019 r. w sprawie wysokości wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym[6];
- rozporządzenie Rady Ministrów z dnia 20 marca 2019 r. w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych[7].

W 2016 r. w pakiecie legislacyjnym reformującym ramy prawne ochrony danych osobowych w UE, oprócz RODO została także przyjęta dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[8]. Dyrektywa, w odróżnieniu od rozporządzenia unijnego, wymagała implementacji w prawie krajowym poprzez przyjęcie odpowiedniej ustawy. Zgodnie z postanowieniami dyrektywy 2016/680 wszystkie państwa członkowskie UE miały ją wdrożyć do 6 maja 2018 r. W polskim systemie prawnym ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości została uchwalona 14 grudnia 2018 r.[9] i weszła w życie 6 lutego 2019 r.[10] Na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości wydano rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych[11].

6 Rozporządzenie Rady Ministrów z dnia 14 stycznia 2019 r. w sprawie wysokości wynagrodzenia członków Rady do Spraw Ochrony Danych Osobowych oraz liczby jej posiedzeń w roku kalendarzowym (Dz. U. z 2019, poz. 164).

7 Rozporządzenie Rady Ministrów z dnia 20 marca 2019 r. w sprawie wzoru legitymacji służbowej pracownika Urzędu Ochrony Danych Osobowych (Dz. U. z 2019, poz. 697).

8 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.), dalej: „dyrektywa 2016/680" lub „dyrektywa policyjna".

9 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r. poz. 1206), (dalej: „ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości").

10 Zgodnie z art. 108 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości jej art. 58 pkt 12 wszedł w życie 1 listopada 2019 r., zaś art. 82 pkt 5 w zakresie art. 25c-25h wszedł w życie po upływie roku od dnia ogłoszenia ustawy, tj. 23 stycznia 2020 r.

11 Rozporządzenie Prezesa Rady Ministrów z dnia 31 maja 2019 r. w sprawie trybu i sposobu realizacji zadań przez inspektora ochrony danych (Dz. U. z 2019 r. poz. 1041)., rozporządzenie weszło w życie 6 czerwca 2019 r.

Pomimo wejścia w życie 25 maja 2018 r. przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych i uchylenia wcześniejszej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[12], w zakresie stosowania dyrektywy 2016/680 niektóre przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych zostały utrzymane w mocy. Zgodnie z art. 175 ustawy z 10 maja 2018 r. o ochronie danych osobowych, art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziały 4, 5 i 7 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, zachowały moc w odniesieniu do przetwarzania danych osobowych przez właściwe organy i służby w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu, do dnia wejścia w życie przepisów wdrażających dyrektywę 2016/680[13].

Na mocy art. 57 RODO Prezes UODO:

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

12 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.).

13 Wskazane w komentowanym artykule przepisy utraciły moc 6 lutego 2019 r., (z wyjątkami, o których mowa w przypisie 9. powyżej), z dniem wejścia w życie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, implementującej przepisy dyrektywy policyjnej do krajowego porządku prawnego.

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

Wraz z powyższymi zadaniami, Prezesowi UODO przysługuje wiele **uprawnień**. Na mocy art. 58 RODO - należą do nich: uprawnienia w zakresie prowadzonych postępowań, uprawnienia naprawcze, uprawnienia w zakresie wydawania zezwoleń oraz uprawnienia doradcze.

14 Dalej także: „EROD".

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

1. nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;
2. prowadzenie postępowań w formie audytów ochrony danych;
3. dokonywanie przeglądu udzielonych certyfikacji na mocy art. 42 ust. 7 RODO;
4. zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia RODO;
5. uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;
6. uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego.

Do uprawnień naprawczych przyznanych na mocy art. 58 ust. 2 RODO zalicza się:

1. wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu, dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
2. udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania;
3. nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO;
4. nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazanie sposobu i terminu;
5. nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
6. wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
7. nakazanie na mocy art. 16, 17 i 18 RODO sprostowania bądź usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 RODO powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

8. cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43 RODO, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
9. zastosowanie, oprócz lub zamiast środków, o których mowa w niniejszym ustępie, administracyjnej kary pieniężnej na mocy art. 83 RODO, zależnie od okoliczności konkretnej sprawy;
10. nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze (art. 58 ust. 3 RODO):

1. udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 36 RODO;
2. wydawanie, z własnej inicjatywy lub na wniosek, opinii przeznaczonych dla parlamentu narodowego, rządu państwa członkowskiego lub – zgodnie z prawem państwa członkowskiego – innych instytucji i organów oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych;
3. zezwalanie na przetwarzanie zgodnie z art. 36 ust. 5 RODO, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;
4. opiniowanie i zatwierdzanie projektów kodeksów postępowania zgodnie z art. 40 ust. 5 RODO;
5. akredytowanie podmiotów certyfikujących na podstawie art. 43 RODO;
6. udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5 RODO;
7. przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d) RODO;
8. zezwalanie na klauzule umowne, o których mowa w art. 46 ust. 3 lit. a) RODO;
9. zezwalanie na uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b) RODO;
10. zatwierdzanie wiążących reguł korporacyjnych na mocy art. 47 RODO.

Nie są to jedyne zadania i kompetencje należące do polskiego organu nadzorczego. Dodatkowe obowiązki Prezesa UODO wynikają również z innych przepisów europejskich i krajowych. Na system ochrony danych osobowych składają się także przepisy szczególne innych ustaw, które regulują kwestie związane z przetwarzaniem danych osobowych przez różne podmioty. Podmioty publiczne, w myśl zasady praworządności wyrażonej w art. 7

Konstytucji RP[15], działają wyłącznie na podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień.

Z chwilą rozpoczęcia obowiązywania od 25 maja 2018 r. RODO i ustawy z 10 maja 2018 r. o ochronie danych osobowych zasadniczej zmianie uległ dotychczasowy sposób podejścia do ochrony danych osobowych. Nowe regulacje spowodowały konieczność samodzielnej oceny przez administratorów ryzyka wiążącego się z przetwarzaniem danych osobowych dla praw i wolności osób, których dane dotyczą oraz wdrożenia przez te podmioty odpowiednich środków technicznych i organizacyjnych odpowiadających zidentyfikowanym ryzykom w taki sposób, aby możliwa była ich minimalizacja. Analiza spraw, którymi Prezes UODO zajmował się w okresie analizowanego roku 2022, w tym w szczególności zgłaszanych skarg i pytań prawnych oraz naruszeń, które wpływały do organu w wyniku zgłoszeń dokonywanych przez administratorów, pozwoliło na zidentyfikowanie związanych z ochroną danych osobowych w związku ze stosowaniem RODO problemów, które najczęściej pojawiały się zarówno po stronie podmiotów danych, jak i administratorów.

2. Urząd Ochrony Danych Osobowych

Urząd Ochrony Danych Osobowych[16] zapewnia wykonanie zadań wynikających z kompetencji Prezesa UODO określonych w RODO i w ustawie z dnia 10 maja 2018 r. ochronie danych osobowych, a także w innych przepisach powszechnie obowiązującego prawa.

Na mocy art. 34 ust. 1 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Prezes UODO jest organem właściwym w sprawie ochrony danych osobowych. Zgodnie z art. 34 ust. 2 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Prezes UODO jest organem nadzorczym w rozumieniu:

- RODO;
- dyrektywy 2016/680;
- rozporządzenia 2016/794[17].

Statutowe komórki organizacyjne UODO noszą następujące nazwy: Departament Orzecznictwa i Legislacji (DOL), Departament Współpracy Międzynarodowej i Edukacji (DWME), Departament Kontroli i Naruszeń (DKN), Departament Komunikacji Społecznej (DKS), Departament Skarg (DS), Departament Kar i Egzekucji (DKE), Departament Informatyki (DIF), Departament Nowych Technologii (DNT), Departament Organizacyjny (DO), Departament Administracyjny (DA), Dział Finansowy, Dział Audytu i Kontroli Wewnętrznej, Dział Kadr, Zespół Radców Prawnych, Samodzielne Stanowisko Inspektora

15 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.), dalej: „Konstytucja RP".
16 Dalej także: „UODO".
17 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. U. UE. L. z 2016 r. Nr 135, str. 53 z późn. zm.), dalej: „rozporządzenie 2016/794".

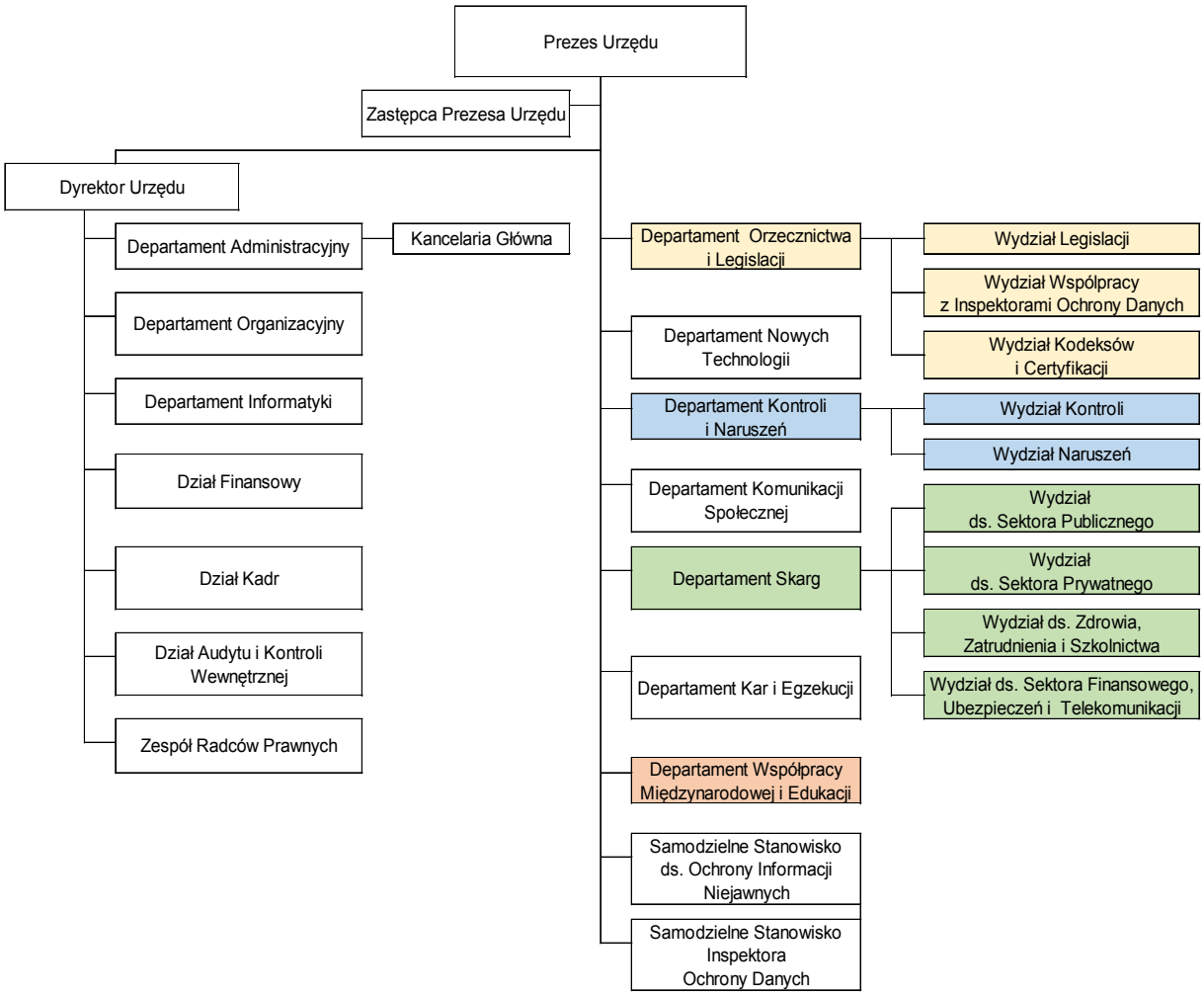
Ochrony Danych oraz Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych.

W trzech departamentach wyodrębnione zostały **wydziały**, które zajmują się sprawami z określonych sektorów. I tak, w Departamencie Orzecznictwa i Legislacji, powstały trzy wydziały: Wydział Legislacji, Wydział Współpracy z Inspektorami Ochrony Danych oraz Wydział Kodeksów i Certyfikacji. W Departamencie Kontroli i Naruszeń znajduje się Wydział Kontroli i Wydział Naruszeń, zaś w Departamencie Skarg – Wydział ds. Sektora Publicznego, Wydział ds. Sektora Prywatnego, Wydział ds. Zdrowia, Zatrudnienia i Szkolnictwa oraz Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji.

2.1. Struktura organizacyjna

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

Strukturę organizacyjną Urzędu Ochrony Danych Osobowych przedstawia poniższa ilustracja:



18 https://uodo.gov.pl/pl/487/2251

2.2. Pracownicy UODO

Stan zatrudnienia w Urzędzie Ochrony Danych Osobowych na dzień 1 stycznia 2022 r. (nie wliczając Prezesa UODO i jego Zastępcy) wynosił 247,85 etatu (tj. 252 osoby)[19]. Natomiast zatrudnienie w UODO na dzień 31 grudnia 2022 r. wynosiło 237,80 etatu (tj. 243 osoby). Na koniec 2022 r. na stanowiskach merytorycznych zatrudnionych było 211 osób, a na stanowiskach pomocniczych 32 osoby. Wyższe wykształcenie posiadało 212 pracowników, w tym 134 legitymowało się wykształceniem wyższym prawniczym.

Liczba pracowników zatrudnionych w poszczególnych jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych na dzień 31 grudnia 2022 r. przedstawiała się następująco:

1) Dyrektor Urzędu – 1 osoba,
2) Departament Orzecznictwa i Legislacji – 27 osób (27,0 etatów), w tym:
   - Wydział Legislacji – 7 osób (7,0 etatów),
   - Wydział Współpracy z Inspektorami Ochrony Danych – 4 osoby (4,0 etaty),
   - Wydział Kodeksów i Certyfikacji – 4 osoby (4,0 etaty),
3) Departament Współpracy Międzynarodowej i Edukacji – 12 osób (12,00 etatów),
4) Departament Kontroli i Naruszeń – 43 osoby (43,0 etaty) w tym:
   - Wydział Kontroli – 12 osób (12,0 etatów),
   - Wydział Naruszeń – 25 osób (25,0 etatów),
5) Departament Komunikacji Społecznej – 14 osób (13,3 etatu),
6) Departament Skarg – 78 osób (77,05 etatu), w tym:
   - Wydział ds. Sektora Publicznego – 11 osób (11,0 etatów),
   - Wydział ds. Sektora Prywatnego – 20 osób (20,0 etatów),
   - Wydział ds. Sektora Zdrowia, Zatrudnienia i Szkolnictwa – 17 osób (17,0 etatów),
   - Wydział ds. Sektora Finansowego, Ubezpieczeń i Telekomunikacji – 18 osób (18,0 etatów),
7) Departament Kar i Egzekucji – 9 osób (9,0 etatów),
8) Samodzielne Stanowisko ds. Ochrony Informacji Niejawnych – 2 osoby (1,33 etatu),
9) Samodzielne Stanowisko Inspektora Ochrony Danych – 1 osoba (1,0 etat),
10) Departament Administracyjny – 24 osoby (23,0 etaty),
11) Departament Organizacyjny – 6 osób (6,0 etatów),

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

12) Departament Informatyki – 8 osób (6,82 etaty),

13) Departament Nowych Technologii – 4 osoby (4,0 etaty),

14) Dział Finansowy – 5 osób (5,0 etatów),

15) Dział Kadr – 4 osoby (4,0 etaty),

16) Dział Audytu i Kontroli Wewnętrznej – 1 osoba (0,5 etatu),

17) Zespół Radców Prawnych – 3 osoby (3,0 etaty),

18) Radca – 1 osoba (0,8 etatu).

2.3. Budżet UODO za 2022 r.

Budżet UODO ustalony w ustawie budżetowej na 2022 r. wynosił: 41 713 tys. zł, w tym:

- wynagrodzenia 26 281 tys. zł
- pochodne od wynagrodzeń 5 603 tys. zł
- wydatki majątkowe 2 555 tys. zł
- pozostałe wydatki 7 274 tys. zł

Wydatki zrealizowane przez UODO w 2022 r. w kwocie 40 270 tys. zł, w tym:

- wynagrodzenia 25 529 tys. zł
- pochodne od wynagrodzeń 4 650 tys. zł
- wydatki majątkowe 1 910 tys. zł
- pozostałe wydatki 8 181 tys. zł

II. OCHRONA DANYCH OSOBOWYCH OBYWATELI

1. Wprowadzenie

Każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo to zostało zagwarantowane w art. 51 Konstytucji RP, art. 8 Karty praw podstawowych Unii Europejskiej[20], a także w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej[21]. Szczegółowe normy służące realizacji tego prawa wprowadza przede wszystkim RODO, określając zasady przetwarzania danych, związane z tym obowiązki administratorów oraz prawa osób, których dane dotyczą.

Za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Osobą możliwą do zidentyfikowania jest taka, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

RODO stosuje się do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz w przypadku przetwarzania w sposób inny niż zautomatyzowany, np. w formie tradycyjnej – papierowej, jeżeli dane stanowią lub mogą stanowić część zbioru[22].

Dane osobowe dzielą się na trzy kategorie:

1) **dane tzw. zwykłe**, takie jak: imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail, itp.;

2) **szczególne kategorie danych osobowych** (uprzednio zwane **danymi wrażliwymi**), wymienione w art. 9 RODO, tj. dane ujawniające:
   - pochodzenie rasowe lub etniczne,
   - poglądy polityczne,
   - przekonania religijne lub światopoglądowe,
   - przynależność do związków zawodowych,
   - dane genetyczne,
   - dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
   - dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;

3) dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych

20 Karta praw podstawowych Unii Europejskiej (Dz. U. UE. C. z 2007 r. Nr 303, str. 1 z późn. zm.), dalej: „KPP".

21 Traktat o funkcjonowaniu Unii Europejskiej. Rzym 25.03.1957 r. (Dz. U. z 2004 r. Nr 90, poz. 864/2 z późn. zm.), dalej: „TFUE".

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

środków bezpieczeństwa, wymienione w art. 10 RODO (uprzednio również zaliczane do **danych wrażliwych**).

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

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

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

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

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

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

- celu przetwarzania;
- odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- kategoriach odnośnych danych osobowych;
- w miarę możliwości planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe – o kryteriach ustalania tego okresu;
- prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych jej dotyczących oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- prawie wniesienia skargi do organu nadzorczego;
- źródle, z którego pozyskane zostały dane osobowe;
- zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W przypadku przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej osoba, której dane dotyczą, ma prawo do informacji o zabezpieczeniach związanych z przekazaniem.

Równie istotnym uprawnieniem jest wskazane w art. 16 RODO prawo do sprostowania danych nieprawidłowych oraz prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

2. Zadania jednostek organizacyjnych UODO

Do zadań jednostek organizacyjnych Urzędu Ochrony Danych Osobowych należy w szczególności: rozpatrywanie skarg w sprawach wykonania przepisów 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.

Departament Kontroli i Naruszeń prowadzi działania kontrolne na podstawie przygotowanych wcześniej projektów planów kontroli. Przeprowadzane czynności kontrolne podsumowywane były w odpowiednich protokołach oraz pismach dokumentujących poszczególne czynności kontrolne. W razie stwierdzenia uchybień prowadzone były postępowania administracyjne. W przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych, nakładane były administracyjne kary pieniężne.

Ważnym zadaniem nałożonym na organ nadzorczy przepisami ogólnego rozporządzenia jest także realizacja obowiązków i uprawnień przez administratorów i inspektorów ochrony danych. Zadania te 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 podejmowaniu działań informacyjno-edukacyjnych, przyczyniających się do budowania świadomości prawnej w zakresie obowiązków wynikających z przepisów o ochronie danych osobowych. Ważnym zadaniem jest także przyjmowanie wniosków o uprzednie konsultacje i zgłoszeń naruszeń ochrony danych osobowych oraz podejmowanie czynności wobec administratorów i podmiotów przetwarzających w celu powiadomienia o naruszeniu ochrony danych osób, których dane dotyczą.

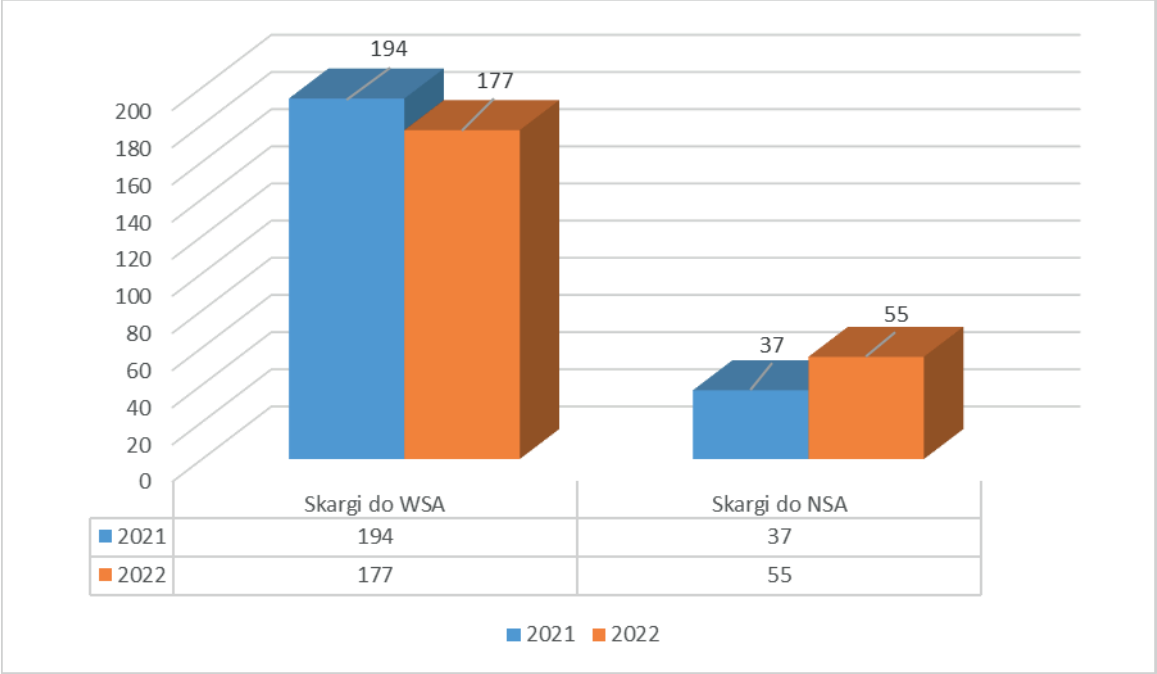
Art. 57 RODO wskazuje także na inne ważne zadanie organu nadzorczego – upowszechnianie i podnoszenie w społeczeństwie wiedzy z zakresu ochrony danych osobowych. Realizacja tego zadania została również ujęta w obowiązkach spoczywających na jednostkach organizacyjnych Urzędu Ochrony Danych Osobowych.

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

Przegląd przykładowego orzecznictwa dotyczącego decyzji Prezesa UODO wydanych w sprawach skargowych należy rozpocząć od wskazania, że w roku 2022 odnotowano wzrost wydanych decyzji w sprawach skargowych w stosunku do lat poprzednich oraz zaobserwowano mniejszą liczbę wnoszonych skarg na decyzje organu do Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie.

W roku 2022 skarga taka została wniesiona w **177** przypadkach, zaś w roku 2021 odnotowano **194** takie skargi. Wzrósł natomiast wskaźnik zaskarżalności do Naczelnego Sądu Administracyjnego (NSA) wyroków wydanych w 2022 r. przez WSA w Warszawie w sprawach decyzji Prezesa Urzędu Ochrony Danych Osobowych dot. skarg.

W roku 2022 do NSA wniesiono **55 skarg**.



Wykres 1: Decyzje wydane w postępowaniach skargowych – zaskarżone do WSA w Warszawie i NSA.

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

W roku 2022 WSA w Warszawie rozstrzygał w sprawie skarg na decyzje Prezesa UODO, które dotyczyły przetwarzania danych osobowych na podstawie art. 105a ust. 3 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe[23].

WSA w wyroku z dnia **18 stycznia 2022 r**.[24] podzielił stanowisko organu przyjęte w zaskarżonej decyzji i podkreślił, że choć ustawodawca nie stworzył żadnych szczególnych wymogów formalnych, co do sposobu i treści poinformowania klienta lub byłego klienta banku o zamiarze przetwarzania jego danych, nie oznacza to całkowitej dowolności w tym zakresie. Sąd stwierdził, że w każdym wypadku sposób ten powinien umożliwić zweryfikowanie faktu poinformowania klienta banku o zamierzonym przetwarzaniu jego danych osobowych lub też przynajmniej potwierdzenie, że klientowi umożliwiono zapoznanie się z taką informacją. Sąd powołał się w tym zakresie na wyrok NSA z dnia 27 sierpnia 2019 r., I OSK 2514/17, w którym stwierdza się, że prawidłowa wykładnia zawartego w art.

23 Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2022 r. poz. 2324 z późn. zm.), dalej: „prawo bankowe".
24 II SA/Wa 3584/21.

105a ust. 3 prawa bankowego zwrotu „poinformowania tej osoby" winna uwzględnić nie tylko treść normy zawartej w art. 61 § 1 Kodeksu cywilnego[25], ale także tę część normy zawartej w art. 105a ust. 3 prawa bankowego, która ustanawia dodatkowy trzydziestodniowy termin na wykonanie zobowiązania. Sąd uznał, że poinformowanie adresata oświadczenia winno, z uwagi na wspomniany powyżej dodatkowy trzydziestodniowy termin na wykonanie zobowiązania, nastąpić w ten sposób, by można było ustalić początek biegu tego terminu. Dopiero bowiem bezskuteczny upływ owego trzydziestodniowego dodatkowego terminu upoważnia bank do przetwarzania danych osobowych w oparciu o przepis art. 105a ust. 3 Prawa bankowego. Sąd wskazał także, iż nadanie powiadomienia, o którym mowa w art. 105a ust. 3 prawa bankowego listem poleconym nie pozwala na ustalenie początku biegu wskazanego terminu. Skoro to bank wywodzi skutki prawne z powiadomienia strony o zamiarze przetwarzania jej danych osobowych stanowiących tajemnicę bankową bez jej zgody, to musi wykazać, że bezskutecznie upłynęło 30 dni od daty poinformowania strony o tym zamiarze. Wykazanie tej okoliczności wymaga jednak – co oczywiste – wykazania początku biegu owego trzydziestodniowego terminu.

Także w wyroku WSA w Warszawie z dnia **15 lutego 2022 r**.[26] sąd podzielił stanowisko Prezesa UODO i zauważył, że kwestia wykładni zawartego w art. 105a ust. 3 Prawa bankowego zwrotu „od poinformowania tej osoby przez bank" była przedmiotem rozważań NSA w wyroku z dnia 27 sierpnia 2019 r. wydanym w sprawie sygn. akt I OSK 2514/17 i WSA w Warszawie. WSA zgodził się z organem, że sporządzenie i wysłanie pisma nie jest równoznaczne z jego doręczeniem skutkującym poinformowaniem o zamiarze przetwarzania danych stanowiących tajemnicę bankową bez zgody, po wygaśnięciu zobowiązania. WSA zaznaczył, że istotnie, jak wskazał organ, przepisy powszechnie obowiązujące nie formułują obowiązku wysłania informacji, o której mowa w art. 105a ust. 3 prawa bankowego w szczególnej formie i to do podmiotu informującego należy wybór formy przekazania odbiorcy komunikatu o zamiarze przetwarzania danych osobowych bez jego zgody, jednakże to również na podmiocie informującym ciąży równocześnie obowiązek wykazania, że ustawowy obowiązek w tym zakresie został wypełniony.

W powyższym wyroku WSA wyraził również swoje stanowisko dotyczące skorzystania przez organ z uprawnienia naprawczego, o którym mowa w art. 58 ust. 2 lit. b) RODO, tj. upomnienia. Sąd stwierdził, że skoro organ nie nałożył na podmiot, który złożył skargę na decyzję kary pieniężnej, jak domagał się tego wnioskodawca w postępowaniu przed Prezesem UODO, a udzielił – wobec stwierdzonego naruszenia RODO – jedynie upomnienia oznacza, że naruszenie uznał za niewielkie, uwzględniając wskazania motywu 148 RODO. Zdaniem sądu, sam fakt udzielenia upomnienia, a nie nałożenia administracyjnej kary pieniężnej wskazuje, że organ wziął pod uwagę charakter, wagę oraz czas trwania naruszenia, uwzględniając przy tym, że przetwarzanie danych naruszało RODO po wycofaniu (odwołaniu) przez wnioskodawcę zgody.

25 Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2022 r. poz. 1360 z późn. zm.), dalej: dalej: „k.c.".
26 II SA/Wa 3139/21.

WSA zgodził się ze stanowiskiem Prezesa UODO także w wyroku z dnia **4 maja 2022 r.**[27], w którym uznał, że wskazane powiadomienie, 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. Okoliczności te nie mogą budzić wątpliwości, bo od ich zaistnienia zależy uprawnienie banku do przetwarzania danych osobowych. Wysłanie tzw. listu poleconego nie pozwala na bezsporne przyjęcie, że powiadomienie istotnie dotarło do adresata. Jeżeli bank wywodzi skutki prawne z powiadomienia strony o zamiarze przetwarzania jej danych osobowych, to musi wykazać, że bezskutecznie upłynęło 30 dni od daty poinformowania strony o tym zamiarze. Wykazanie tej okoliczności wymaga wykazania początkowego biegu ww. terminu.

W wyroku tym sąd zgodził się z organem co do tego, że upomnienie jest środkiem, który poza wskazaniem podmiotowi na nieprawidłowość w procesie przetwarzania danych osobowych, której się dopuścił ma także charakter prewencyjny. Oznacza to, że udzielenie upomnienia za nieprawidłowości w procesie przetwarzania danych osobowych, który zaistniał w czasie obowiązywania przepisów RODO pozwala na to, aby bank zweryfikował swoje procesy przetwarzania w taki sposób, aby wykluczyć podobne naruszenia w przyszłości. Powyższe jest o tyle istotne dla samego banku, że może uchronić go w przyszłości przed stosowaniem przez organ innych uprawnień naprawczych, m.in. administracyjnej kary pieniężnej. Uregulowane w art. 58 ust. 2 RODO uprawnienia znajdują zatem zastosowanie, gdy stan naruszenia obecnie nie istnieje. Sąd wskazał ponadto, że upomnienie nie jest jedynym środkiem naprawczym o charakterze prewencyjnym – podobny charakter ma ostrzeżenie, o którym mowa w art. 58 ust. 2 lit. a) RODO.

Wyrok dotyczący przetwarzania danych w związku z windykacją należności

W wydanym w dniu **20 maja 2022 r**.[28] wyroku WSA w Warszawie wskazał, że zasadne jest uznanie przez organ, że skuteczność zawarcia umowy między spółką a wnioskodawcą (wobec np. zamieszczenia na stronie internetowej jedynie treści umowy), czy spór w sprawie ewentualnego spłacenia przezeń należności – przed przekazaniem jego danych osobowych innym spółkom do windykacji – nie może być przedmiotem sprawy prowadzonej przez Prezesa UODO. Rolą wyspecjalizowanego organu administracji jest w danej sprawie jedynie ocena, czy administratorzy danych osobowych (podmioty zarządzające) dysponują systemem eliminującym przetwarzanie danych, które nie są niezbędne w kontekście prowadzonej działalności oraz czy realnie go stosują. Poza granicami sprawy musi pozostawać, czy zasadne jest stanowisko określonego podmiotu, co to wiążących go z konkretnym kontrahentem zobowiązań. Kwestie te mogą być rozstrzygane tylko w postępowaniach przed sądami powszechnymi. Nie mogły więc podlegać – niejako równolegle – ocenie w sprawie administracyjnej – w przedmiocie ochrony danych osobowych. Umożliwiałoby to wprost formułowanie odmiennych konstatacji, co do tych samych stanów faktycznych. Takie

27 II SA/Wa 3781/21.
28 II SA/Wa 2742/21.

rozumienie kompetencji danego, wyspecjalizowanego organu administracji nie może być akceptowane w kontekście reguł praworządności.

WSA stwierdził ponadto, że nie do zaakceptowania jest wykładnia regulacji oparta na założeniu występowania kilku konkurencyjnych procedur, gdzie może podlegać ocenie ta sama kwestia – np. realizacja obowiązku informacyjnego wobec bezprawnego przyjęcia danych. Skoro postępowanie w przedmiocie naruszenia ochrony danych osobowych jest prowadzone z urzędu, zaś osoby, których dotyczą przejęte dane nie są w nich stronami – nie do akceptowania jest koncepcja, aby to samo zdarzenie – naruszenie integralności danych, w następstwie czego nastąpiło ich nieuprawnione pozyskanie (przetworzenie przez osobę nieuprawnioną) – mogło być oceniane w odrębnych postępowaniach, prowadzonych wobec skarg osób, których dane przyjęto.

Wyrok w sprawie decyzji dotyczącej spełnienia obowiązku z art. 15 RODO

W 2022 r. wyrokiem z dnia **9 marca 2022 r.**[29] WSA w Warszawie oddalił skargę na decyzję Prezesa UODO, w której organ nakazał operatorowi telekomunikacyjnemu spełnienie obowiązku informacyjnego poprzez przekazanie informacji wskazujących cele przetwarzania jego danych osobowych, kategorie odnośne danych osobowych, odbiorców i kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności informacji o odbiorcach z państw trzecich lub organizacjach międzynarodowych i wszelkich dostępnych informacjach o źródle danych osobowych. Sąd podzielił stanowisko organu nadzorczego stwierdzając, że nie było podstawy do wydania decyzji nakazowej. W trakcie postępowania administracyjnego podmiot skarżony nie wykazał, że podmiot wnioskujący nie był osobą, za którą się podaje ani również nie stwierdził, że ma choćby minimalne wątpliwości w tym zakresie. Osoba ta podała skarżonemu podmiotowi swoje dane w zakresie imienia i nazwiska, pełnej nazwy firmy, która jest stroną umowy, wraz z adresem, który widnieje również w aneksie do umowy o świadczenie usług telekomunikacyjnych, podała swój numer PESEL, który jest zgodny z numerem PESEL widniejącym na wskazanym aneksie do umowy, podała numer telefonu (stacjonarny) i numer faksu, a także złożyła podpis, który pozwalał na jej zweryfikowanie z podpisem złożonym na aneksie.

Wyrok w sprawie legalności przetwarzania danych ucznia w celu realizacji obowiązku nauczaną w formie zdalnej

W wyroku z **19 kwietnia 2022 r**.[30] WSA w Warszawie podtrzymał decyzję Prezesa UODO, w której organ stwierdził legalność przetwarzania danych osobowych ucznia w zakresie imienia, nazwiska i adresu e-mail na potrzeby zdalnego nauczania zgodnie z art. 6 ust. 1 lit. e RODO w celu realizacji obowiązku nauki w formie zdalnej w związku z art. 35 i art. 30c Prawa oświatowego, w związku z § 1 ust. 1 rozporządzenia Ministra Edukacji Narodowej

29 II SA/Wa 1496/21.
30 II Sa/Wa 2259/21.

z dnia 12 sierpnia 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. z 2020 r. poz. 1389) i z § 1 rozporządzenia Ministra Edukacji Narodowej z dnia 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. z 2020 r. poz. 493) oraz udostępnienia tych danych osobowych na rzecz operatora platformy służącej do prowadzenia nauczania zdalnego zgodnie z art. 28 ust. 3 RODO i prawidłowość realizacji wobec skarżącego obowiązków informacyjnych wynikających z art. 13 i art. RODO, w związku z kwestionowanym procesem przetwarzania. W przedmiotowym wyroku sąd w pełni podzielił stanowisko organu, dokonując oceny prawidłowości działania organu przez pryzmat kompetencji wynikających z przepisów ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego[31], ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz RODO.

Wyrok w sprawie procesu przetwarzania danych, który miał miejsce przed rozpoczęciem stosowania RODO

Do UODO wpływają często skargi na proces przetwarzania danych osobowych, który jak często okazuje się w toku postępowania miał miejsce w czasie, gdy nie obowiązywały jeszcze przepisy RODO. W jednej ze spraw, w których zaskarżono decyzję Prezesa UODO wydaną w tego typu sprawie, WSA wyrokiem z **18 maja 2022 r**.[32] oddalił skargę uznając między innymi, że organ prawidłowo umorzył postępowanie co do zdarzeń mających miejsce przed wejściem w życie przepisów RODO, ze względu na brak elementu materialnoprawnego (brak normy prawnej mogącej być podstawą oceny merytorycznej), oraz co do kwestii udostępnienia przez pracodawcę danych związanych z procesem negatywnej weryfikacji pracownika na rzecz innych spółek, ze względu na to, że pomiędzy spółkami nie dochodziło do wymiany informacji dotyczącej weryfikacji skarżącego w procesie zatrudnienia. Sąd uznał ponadto, że Prezes UODO prawidłowo ocenił kwestie związane z podstawami przetwarzania danych skarżącego przez spółki, w stosunku do których skarżący świadczył pracę.

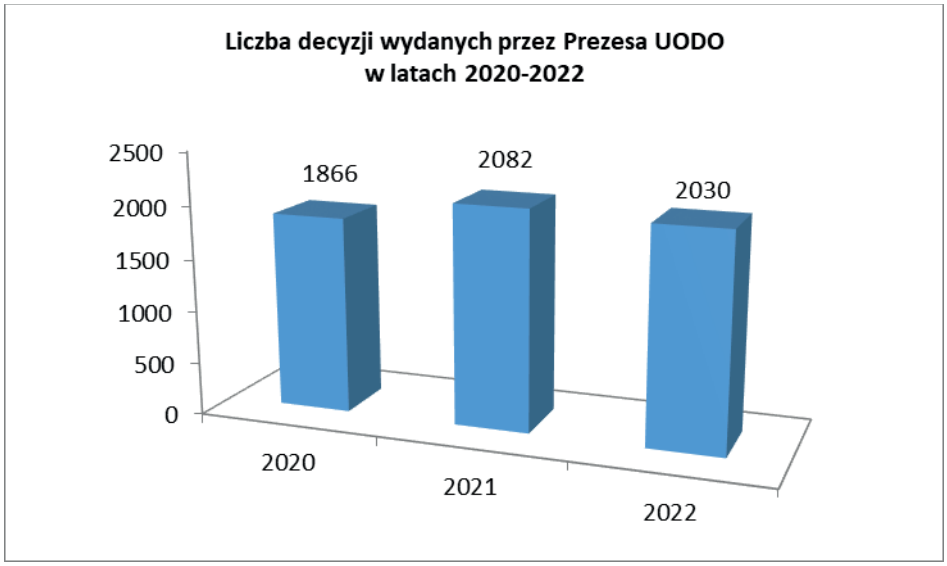
4. Wydawanie decyzji administracyjnych i rozpatrywanie skarg

Postępowanie dotyczące naruszenia przepisów o ochronie danych osobowych, wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej, toczy się według przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, zgodnie z przepisami 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

31 Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2023 r. poz. 775 z późn. zm.), dalej: „k.p.a".
32 II SA/Wa 12/22.

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 roku 2022 Prezes UODO wydał 2030 decyzji administracyjnych, co jest liczbą porównywalną do roku 2021, w którym wydanych zostało 2082 decyzje administracyjne i o 164 więcej w stosunku do roku 2020, w którym wydanych było 1866 decyzji.



Wykres 2: Liczba decyzji wydanych przez Prezesa UODO w latach 2020-2022.

4.1. Skargi

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

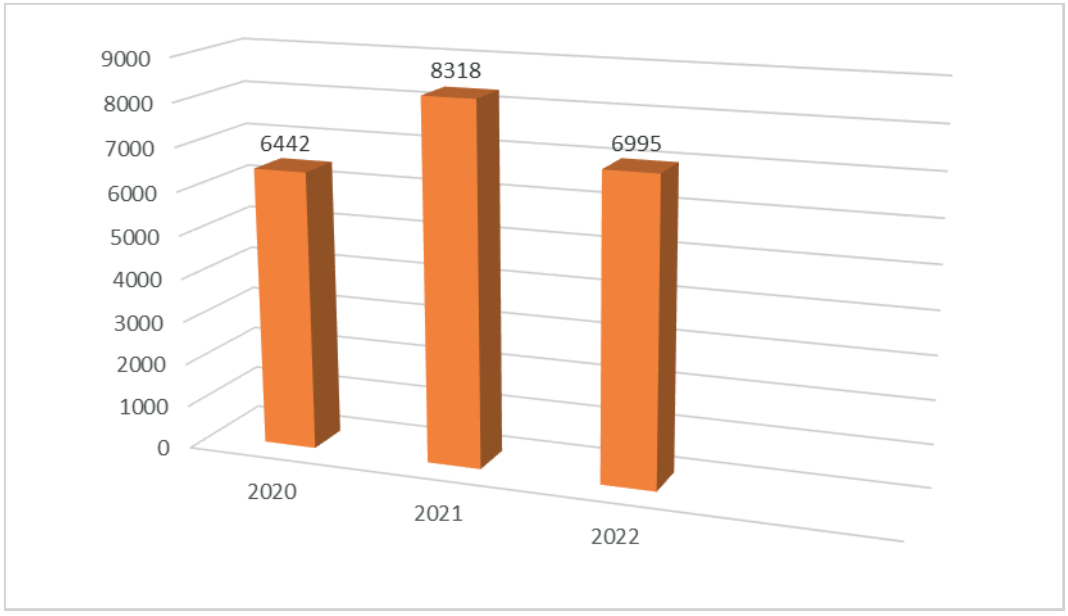
Każda ze skarg analizowana jest na wstępie pod kątem spełnienia warunków formalnych przewidzianych przepisami k.p.a. W sytuacji, gdy skarga nie spełnia warunków wymaganych przez ww. przepisy prawa, organ właściwy do spraw ochrony danych osobowych wzywa wnioskodawcę do uzupełnienia braków formalnych. W sprawach, w których nie uzupełniono braków formalnych, skargi pozostawiano bez rozpoznania.

W toku postępowania administracyjnego organ nadzorczy podejmuje szereg czynności koniecznych do zebrania materiału dowodowego, niezbędnego do wydania rozstrzygnięcia w sprawie, informując jednocześnie strony postępowania, w tym stronę skarżącą, o postępach i wynikach rozpatrzenia skargi. Z obserwacji organu wynika, że kierowane do niego skargi

często nie zawierały precyzyjnego określenia żądania, z jakim skarżący zwracali się do Prezesa UODO. Skarżący wskazywali także na naruszenie ochrony danych osobowych osób trzecich, jak również składali skargi dotyczące przyszłego przetwarzania, które nie zaistniało na dzień złożenia skargi.

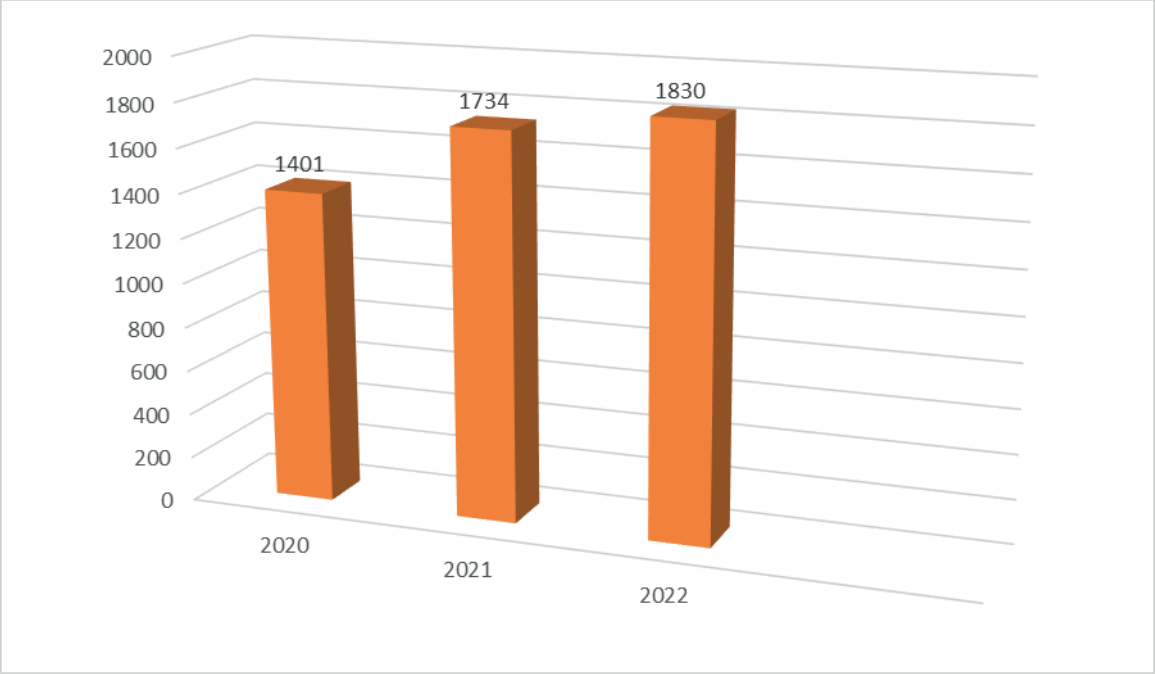
W analizowanym okresie sprawozdawczym Prezes UODO prowadził postępowania administracyjne wszczęte w wyniku skarg wniesionych w roku 2022, jak i w latach poprzednich. Postępowania te toczyły się zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz na podstawie przepisów k.p.a. zgodnie z art. 7 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

W roku 2022 r. do Urzędu Ochrony Danych Osobowych wpłynęło **6995 skarg,** a zatem o 1323 skarg mniej niż w roku poprzednim. Jednakże duży wzrost skarg złożonych w 2021 roku, przełożył się na większą liczbę spraw prowadzonych w UODO także w analizowanym roku sprawozdawczym, które pozostawały w toku, i w których konieczne było podjęcie czynności niezbędnych do zebrania materiału dowodowego i wydania decyzji administracyjnej.



Wykres 3: Liczba skarg, które wpłynęły do UODO w latach 2020-2022.

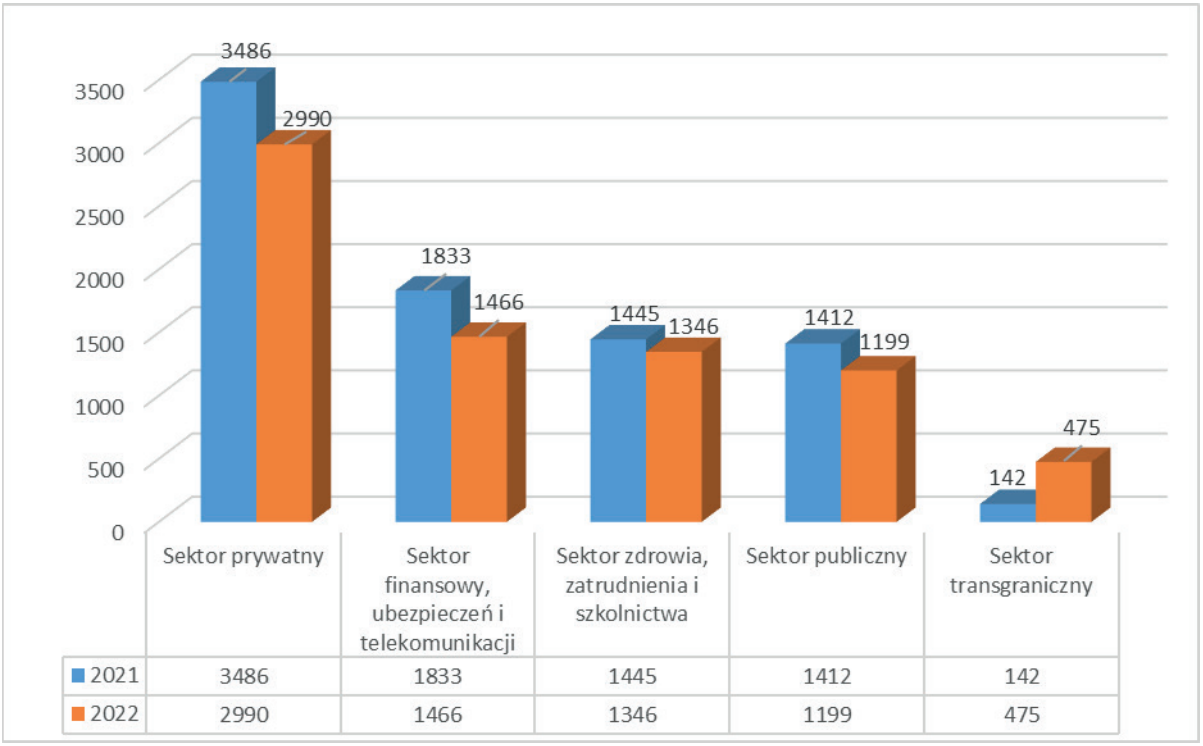
W analizowanym roku 2022 **postępowania zakończono w 6479 sprawach**, spośród których **1830** spraw zakończyło się wydaniem decyzji administracyjnych. Dane porównawcze z lat poprzednich wykazują, że liczba wydawanych przez Prezesa UODO decyzji administracyjnych, w sprawach zainicjowanych skargami osób, których dane dotyczą, stale wzrasta, pomimo utrzymującego się wysokiego poziomu wpływu nowych skarg. W 2021 roku wydaniem decyzji administracyjnej zakończyły się 1734 sprawy, zaś w roku 2020 – było to 1401 spraw.



Wykres 4: Liczba decyzji administracyjnych wydanych w sprawach zainicjowanych indywidualną skargą, wydanych w latach 2020-2022.

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

- 2990 skarg na podmioty sektora prywatnego (3486 skarg w roku 2021),
- 1466 skarg na podmioty sektora finansowego, ubezpieczeń i telekomunikacji (1833 skargi w roku 2021),
- 1346 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa (1445 w roku 2021),
- 1199 skarg na podmioty sektora publicznego (1412 w roku 2021),
- 475 skarg na podmioty sektora transgranicznego (142 w roku 2021).



Wykres 5: Liczba skarg, które wpłynęły do UODO w latach 2021-2022 z podziałem na sektory.

Choć w omawianym roku 2022 zaobserwowano nieznaczny spadek liczby skarg, to liczba ta wciąż pozostaje na bardzo wysokim poziomie. Spadek wpływu skarg odnotowano we wszystkich sektorach, za wyjątkiem skarg zakwalifikowanych jako transgraniczne, których liczba wzrosła. W roku 2022 wpłynęło 475 takich skarg, w roku poprzednim były to 142 skargi.

Spadek liczby skarg na podmioty sektora prywatnego oraz sektora finansowego wiązać należy z sytuacją ekonomiczną i mniejszą skłonnością osób, których dane dotyczą do zawierania umów z podmiotami z tych sektorów. Skargi na te podmioty najczęściej związane były z przetwarzaniem danych osobowych w związku z zawarciem lub wykonywaniem umów. Wśród skarg na podmioty z sektora finansowego niezmiennie – w stosunku do lat ubiegłych – najwięcej dotyczyło umów zawieranych z bankami i instytucjami kredytowymi, zaś spadek liczby skarg z tego sektora wynikać może ze zmniejszonego popytu na oferowane przez te podmioty kredyty.

W każdym spośród wskazanych wyżej sektorów osoby, których dane dotyczyły, często skarżyły się na przetwarzanie ich danych osobowych bez podstawy prawnej, w tym na nieuprawnione udostępnienie ich danych osobowych podmiotom nieuprawnionym oraz nieuprawnione działania marketingowe z wykorzystaniem ich danych. Duża część skarg dotyczyła także niespełnienia obowiązków informacyjnych wynikających z RODO, w tym nieprzekazania kopii danych, zgodnie z art. 15 ust. 3 RODO. Odnotowano także liczne

skargi na nieprawidłowe wykonanie obowiązku sprostowania danych oraz nieprawidłową realizację prawa do usunięcia danych wynikającego z art. 17 RODO i prawa sprzeciwu, o którym mowa w art. 21 RODO.

W okresie od 1 stycznia 2022 r. do 31 grudnia 2022 r. w sprawach skargowych wydanych zostało łącznie **1830 decyzji.** W 974 decyzjach zastosowano środki naprawcze w oparciu o art. 58 RODO, w 637 sprawach – upomnienia za naruszenie przepisów RODO, zaś w 337 przypadkach – środek naprawczy w postaci nakazu.

Do Wojewódzkiego Sądu Administracyjnego w Warszawie zostało zaskarżonych 177 decyzji Prezesa UODO, zaś do NSA wniesiono 55 skarg kasacyjnych od wyroków w sprawach dotyczących decyzji wydanych przez Prezesa UODO.

4.1.1. Sektor publiczny

Skargi wpływające do organu na podmioty z **sektora publicznego (1199 skarg)**, podobnie jak w latach ubiegłych, najczęściej dotyczyły udostępnienia danych osobowych na stronach internetowych Biuletynu Informacji Publicznej.

Udostępnienie danych osobowych w związku z publikacją oświadczenia majątkowego w Biuletynie Informacji Publicznej (BIP)

Przedmiotem skargi na nieprawidłowości w procesie przetwarzania danych osobowych skarżącego przez burmistrza, było udostępnienie danych osobowych skarżącego zawartych w oświadczeniu majątkowym na stronie Biuletynu Informacji Publicznej Urzędu przez okres dłuższy niż 6 lat. Ustalono, że burmistrz w 2014 r. udostępnił na stronie internetowej urzędu oświadczenie majątkowe skarżącego, jako radnego gminy, zgodnie z art. 24i ust. 1 i ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym[33]. Burmistrz uznał, że obowiązujące przepisy prawa nie określają, po jakim czasie oświadczenia majątkowe można usunąć z BIP, ale z ostrożności, biorąc pod uwagę przepis art. 24h ust. 6 tej ustawy, oświadczenie to zostało usunięte. Zebrany w sprawie materiał dowodowy nie potwierdził jednak powyższych wyjaśnień. Na podstawie analizy treści dostępnych na stronie internetowej BIP urzędu ustalono bowiem, że dane osobowe skarżącego zawarte w złożonym przez niego oświadczeniu majątkowym za rok 2014 były nadal upubliczniane. Ustalono jednocześnie, że upublicznione oświadczenie majątkowe nie zawiera danych osobowych skarżącego w zakresie adresu zamieszkania i adresu nieruchomości.

Zgodnie z art. 24h ust. 1 ustawy o samorządzie gminnym, radny, wójt, zastępca wójta, sekretarz gminy, skarbnik gminy, kierownik jednostki organizacyjnej gminy, osoba zarządzająca i członek organu zarządzającego gminną osobą prawną oraz osoba wydająca decyzje administracyjne w imieniu wójta, są obowiązani do złożenia oświadczenia o swoim

33 Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2023 r. poz. 40 z późn. zm.), dalej: „ustawa o samorządzie gminnym”.

stanie majątkowym. Oświadczenie majątkowe dotyczy ich majątku odrębnego oraz majątku objętego małżeńską wspólnością majątkową. Jak stanowi art. 24i ust. 1 ustawy o samorządzie gminnym, informacje zawarte w oświadczeniu majątkowym są jawne, z wyłączeniem informacji o adresie zamieszkania składającego oświadczenie oraz o miejscu położenia nieruchomości. Z uwagi na upływ 6-letniego okresu przechowywania danych zawartych w złożonym przez skarżącego w urzędzie oświadczeniu majątkowym za 2014 r., burmistrz nie posiadał już legitymacji prawnej do upubliczniania na stronie internetowej urzędu danych osobowych skarżącego zawartych w ww. oświadczeniu majątkowym. Powyższe naruszyło art. 6 ust. 1 RODO. W związku z tym Prezes UODO uznał za zasadne skorzystanie w przedmiotowej sprawie z instrumentu o charakterze naprawczym przewidzianym w art. 58 ust. 2 lit. c RODO i nakazał burmistrzowi usunięcie danych osobowych skarżącego zawartych w jego oświadczeniu majątkowym z 2014 r. ze strony internetowej BIP urzędu[34].

Udostępnienie danych osobowych w związku z publikacją w Biuletynie Informacji Publicznej petycji wniesionej przez osobę trzecią

W prowadzonej przez Prezesa UODO sprawie ustalono, że wójt opublikował na stronie internetowej BIP urzędu cyfrowe odwzorowanie wniesionej petycji przez mieszkankę gminy w ramach realizacji obowiązku wynikającego z art. 8 ust. 1 ustawy z dnia 11 lipca 2014 r. o petycjach[35]. Odwzorowanie ww. petycji zawierało dane osobowe skarżącego w zakresie imienia i nazwiska. Skarżący złożył sprzeciw wobec udostępniania na stronie internetowej BIP jego danych osobowych zawartych w petycji osoby trzeciej. Wójt podniósł, że zgodnie z art. 4 ust. 3 ustawy o petycjach, zgoda na publikację danych osobowych wymagana jest wyłącznie od wnioskodawcy, natomiast ustawodawca w ustawie o petycjach nie wnosi wyraźnych zastrzeżeń do zawartości petycji, a za treść petycji odpowiada wnioskodawca, a nie wykonujący dyspozycję prawną wójt. W postępowaniu wyjaśniającym wójt wskazał, że aktualnie nie udostępnia na stronie internetowej BIP danych osobowych skarżącego. Petycja została usunięta ze strony internetowej w związku z prośbą wnoszącego petycję.

Zauważyć należy, że art. 8 ust. 1 ustawy o petycjach reguluje zasady publikowania danych osobowych wnoszącego petycję, nie odnosi się natomiast do publikowania danych osobowych innych osób. W tym zakresie zastosowanie znajdują więc przepisy z zakresu ochrony danych osobowych. Skoro zaś przepis art. 8 ust. 1 w zw. z art. 4 ust. 3 ustawy o petycjach dopuszcza publikację danych wnoszącego skargę tylko pod warunkiem wyrażenia zgody przez osobę, której dane dotyczą, na upublicznienie danych osobowych, to tym bardziej przy przetwarzaniu danych osoby trzeciej, które zawarto w treści petycji, należy uwzględnić prawo do ochrony danych osobowych tej osoby, szczególnie że może ona nie mieć wiedzy o tym, że inny podmiot wskazał w petycji jej dane osobowe. Administrator ma natomiast obowiązek zapewnić, aby dane osobowe przetwarzane były w sposób zgodny z prawem. O powyższym przesądzają ogólne zasady przetwarzania danych

34 DS.523.4358.2020.

35 Ustawa z dnia 11 lipca 2014 r. o petycjach (t.j. Dz. U. z 2018 r. poz. 870), dalej: „ustawa o petycjach".

osobowych określone w art. 5 ust. 1 RODO, m.in. zasada zgodności z prawem, rzetelności i przejrzystości, wyrażona w art. 5 ust. 1 lit. a) RODO, zgodnie z którą dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą, a także zasada minimalizacji danych wyrażona w art. 5 ust. 1 lit. c) RODO, która stanowi, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Wójt, publikując dane osobowe skarżącego na stronie internetowej BIP urzędu, nie legitymował się żadną z przesłanek określonych w art. 6 ust. 1 RODO, która stanowiłaby o legalności tego procesu. Zebrany w sprawie materiał dowodowy nie wykazał, aby wójt uzyskał zgodę skarżącego, na publikację. Nie można było także uznać, uwzględniając zasadę minimalizacji danych, aby udostępnienie ww. danych osobowych skarżącego było niezbędne do wykonania obowiązku wynikającego z przepisu prawa, gdyż w ocenie organu, określony w art. 8 ust. 1 ustawy o petycjach obowiązek opublikowania odwzorowania petycji na stronie internetowej BIP, wójt powinien realizować z poszanowaniem prawa do ochrony danych osobowych osób, których dane zostały zamieszczone w petycji. W ocenie Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z zasadą minimalizacji danych, wójt, jako administrator danych, spełniając obowiązek wynikający z ww. przepisu, przed publikacją petycji powinien był dokonać anonimizacji danych osobowych skarżącego w niej zawartych.

W związku z tym, że wójt naruszył przepisy o ochronie danych osobowych, tj. art. 6 ust. 1 RODO, udostępniając dane osobowe skarżącego w zakresie jego imienia i nazwiska na stronie internetowej BIP urzędu bez podstawy prawnej oraz uwzględniając wagę i charakter stwierdzonego naruszenia, jak również to, że udostępnianie nie było już kontynuowane, Prezes UODO uznał za zasadne skorzystanie w niniejszej sprawie z instrumentu o charakterze naprawczym przewidzianego w art. 58 ust. 2 lit. b) RODO i udzielił wójtowi upomnienia za powyższe naruszenie[36].

Udostępnienie danych osobowych w Biuletynie Informacji Publicznej w związku z publikacją wystąpień pokontrolnych

Kolejne postępowanie administracyjne toczyło się w sprawie publikacji danych osobowych skarżących w zakresie imienia i nazwiska, stopnia pokrewieństwa oraz informacji o pełnieniu przez nich pieczy zastępczej na stronie BIP urzędu wojewódzkiego, w związku z publikacją wystąpień pokontrolnych z kontroli przeprowadzonych przez wojewodę w urzędzie miejskim oraz w ośrodku pomocy społecznej.

Jak wynikało z ustaleń postępowania, wojewoda przeprowadził kontrole w urzędzie miejskim oraz ośrodku pomocy społecznej w celu oceny efektywności udzielonej pomocy jednej z rodzin. Z przeprowadzonych kontroli sporządzono wystąpienia pokontrolne, które następnie zostały opublikowane na stronach internetowych Biuletynu Informacji Publicznej urzędu wojewódzkiego. Wystąpienia te zawierały dane osobowe członków rodziny, której

36 DS.523.6274.2020.

efekty udzielonej pomocy kontrolowano. Jak ustalono, do przedmiotowego udostępnienia danych osobowych doszło na skutek nieprawidłowej anonimizacji wystąpień pokontrolnych.

Zgodnie z brzmieniem art. 6 ust. 1 pkt 4 lit. a tiret drugie ustawy o dostępie do informacji publicznej[37], udostępnieniu podlega informacja publiczna, w szczególności o danych publicznych, w tym dokumentacja przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających, przy czym zgodnie z art. 5 ust. 2 prawo do informacji publicznej podlega ograniczeniu m.in. ze względu na prywatność osoby fizycznej. Wojewoda, publikując na stronie internetowej BIP dane osobowe skarżących w zakresie imienia i nazwiska, stopnia pokrewieństwa oraz informacji o pełnionej przez nich pieczy zastępczej, nie legitymował się żadną z przesłanek legalizujących ten proces, spośród określonych w art. 6 ust. 1 RODO, co przesądziło o naruszeniu tego przepisu. Wystąpienia pokontrolne, w których dane skarżących były niewłaściwie zanonimizowane zostały usunięte ze strony BIP urzędu wojewódzkiego. W opublikowanych ponownie wystąpieniach pokontrolnych nie znajdowały się już te dane, a część z nich została zastąpiona znakami XXX. Tym samym Prezes UODO uznał, że na dzień wydania decyzji wojewoda nie udostępniał już danych osobowych skarżących w sposób zakwestionowany w skardze. Wobec powyższego, korzystając z uprawnienia przewidzianego w art. 58 ust. 2 lit. b) RODO, Prezes Urzędu Ochrony Danych Osobowych udzielił wojewodzie upomnienia za stwierdzone naruszenie przepisów o ochronie danych osobowych[38].

Przetwarzanie danych osobowych przez podmiot publiczny w celu innym, niż ten, dla którego zostały zebrane

Przedmiotem jednej ze skarg rozpoznanych przez Prezesa Urzędu Ochrony Danych Osobowych były nieprawidłowości w procesie przetwarzania danych osobowych przez Samorządowe Kolegium Odwoławcze (SKO). Polegało ono na wykorzystaniu informacji o adresie skarżącego do doręczeń pocztą tradycyjną. Skarżący za pomocą platformy ePUAP wystosował do prezydenta miasta ponaglenie „w sprawie Rzecznika Praw Konsumenta". W piśmie tym zostały wskazane dane osobowe skarżącego w zakresie imienia, nazwiska, numeru PESEL i adresu poczty elektronicznej. W jego treści skarżący wniósł o przesłanie odpowiedzi na adres poczty elektronicznej. Pismo to zostało przekazane przez prezydenta miasta do SKO, na podstawie art. 37 § 4 k.p.a. za pośrednictwem gońca. Następnie SKO pisemnie poinformowało skarżącego, że nie jest właściwe do rozpatrzenia wniesionego przez niego ponaglenia, wysyłając to pismo na adres jego poczty tradycyjnej. Prezes Urzędu Ochrony Danych Osobowych ustalił, że skarżący w piśmie skierowanym do SKO nie wskazał adresu poczty tradycyjnej, jednak w bazach komputerowych repertorium SKO odszukano znaczną ilość spraw, w których stroną był skarżący i gdzie widniał jego adres, a ponadto sprawdzono system, którego ten organ używa do wysyłki poczty i odszukano kolejne sprawy, w których użyto adresu korespondencyjnego skarżącego. Dane z systemu odnośnie adresu

37 Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902), dalej: „u.d.i.p.".
38 DS.523.2010.2021.

poczty tradycyjnej (bez uprzedniego wzywania wnioskodawcy o uzupełnienie wniesionego pisma) wykorzystano, mając na względzie zasadę szybkości, określoną w art. 12 k.p.a.

Art. 39^1 § 1 k.p.a. – w brzmieniu obowiązującym w chwili wystosowania przez SKO pisma do skarżącego – stanowił wprost, że doręczenie pism następuje za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, jeżeli strona lub inny uczestnik postępowania spełni jeden z warunków: (pkt 1) złoży podanie w formie dokumentu elektronicznego przez elektroniczną skrzynkę podawczą organu administracji publicznej. W takim przypadku odstąpienie przez organ administracji publicznej od doręczenia pisma za pomocą środków komunikacji elektronicznej mogło nastąpić jedynie w sytuacji określonej w art. 39^1 § 1d k.p.a. Przepis ten stanowił, że jeżeli strona lub inny uczestnik postępowania zrezygnuje z doręczania pism za pomocą środków komunikacji elektronicznej, organ administracji publicznej doręcza pismo w sposób określony dla pisma w formie innej niż forma dokumentu elektronicznego.

Ponaglenie, do którego odnosiło się pismo Samorządowego Kolegium Odwoławczego, skarżący przesłał za pomocą platformy ePUAP, a zatem w formie dokumentu elektronicznego przez elektroniczną skrzynkę podawczą organu administracji publicznej. Nic nie wskazywało, aby skarżący zrezygnował z doręczania pism za pomocą środków komunikacji elektronicznej. Z powyższych okoliczności wynikało, że na SKO ciążył obowiązek przesyłania skarżącemu korespondencji za pomocą środków komunikacji elektronicznej. Dla doręczenia korespondencji w ten sposób było zaś zbędne przetwarzanie informacji o adresie skarżącego do doręczeń pocztą tradycyjną, którego to adresu skarżący nie podał. Z powyższego wynikało zatem, że wykorzystanie informacji o adresie skarżącego do doręczeń pocztą tradycyjną, do doręczenia mu pisma SKO, nie było niezbędne do wypełnienia obowiązku prawnego ciążącego na tym organie albo do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej mu powierzonej. Zatem po stronie SKO nie wystąpiły przesłanki określone w przepisach art. 6 ust. 1 lit. c) oraz e) RODO.

Kwestionowany przez skarżącego proces przetwarzania jego danych osobowych naruszył przepisy art. 6 ust. 1 RODO, bowiem nie znajdował oparcia w żadnej z przesłanek wskazanych w tym przepisie. Mając to na uwadze, Prezes Urzędu Ochrony Danych Osobowych udzielił SKO upomnienia w związku z zaistniałym naruszeniem art. 6 ust. 1 RODO[39].

4.1.2. Sektor prywatny

Spośród **6995 skarg**, które w 2022 r. wpłynęły do Urzędu, **2990** z nich dotyczyło podmiotów sektora prywatnego. Poniżej omówione zostały przykłady kilku takich skarg.

39 DS.523.5757.2021.

Realizacja prawa dostępu do danych

Jednym z istotnych uprawnień przysługujących osobom, których dane dotyczą, jest prawo dostępu do danych, uregulowane w art. 15 RODO. Prawo to przewiduje możliwość uzyskania od administratora wymienionych w ww. przepisie informacji, w tym kopii danych, o której mowa w art. 15 ust. 3 RODO. W analizowanym roku sprawozdawczym, podobnie jak w latach ubiegłych, do Prezesa UODO wpłynęły liczne skargi na odmowę realizacji tego prawa. Jako powody odmowy administratorzy wskazywali m.in. ewentualne naruszenie prawa do ochrony danych osobowych innych osób (np. w przypadku nagrań wideo) oraz brak środków technicznych umożliwiających realizację tego prawa.

W jednej ze spraw skarżąca złożyła skargę na niezrealizowanie wniosku o udostępnienie kopii jej danych osobowych w postaci treści nagrań rozmów telefonicznych przeprowadzonych przez nią z konsultantami spółki. Skarżąca kilkukrotnie zwracała się do spółki o wydanie kopii treści nagrań rozmów telefonicznych, wskazując numer telefonu i daty dzienne rozmów. Spółka zrealizowała wniosek skarżącej opisując przedmiot tych rozmów, które związane były m.in. z windykacją należności wynikających z zawartej umowy, ale odmówiła przesłania wnioskowanych nagrań z uwagi na bezpieczeństwo danych. W uzasadnieniu spółka wyjaśniła, że nagrania właściwie nie zawierają danych osobowych skarżącej, a powoływany w rozmowach Numer Identyfikacji Podatkowej był jedynie elementem weryfikacyjnym podawanym przez skarżącą w celu weryfikacji rozmówcy.

W ocenie organu sposób realizacji przez spółkę obowiązku informacyjnego z art. 15 ust. 3 RODO nie uwzględniał okoliczności, że w wyniku przechowywania nagrań z rozmów telefonicznych przetwarza ona dane osobowe także w zakresie głosu skarżącej. Spółka uznała, że ujawnienie wnioskowanych nagrań wpłynęłoby niekorzystnie na prawa innych osób[40]. W ocenie organu uznanie, że udostępnienie kopii danych może powodować naruszenie praw i wolności osób trzecich nie skutkuje jednak automatycznym zwolnieniem administratora z obowiązku udostępnienia wnioskującej osobie, której dane dotyczą, informacji określonych w art. 15 RODO. Obowiązkiem administratora jest wówczas wyeliminowanie tych informacji, których udostępnienie w związku z ich przekazaniem wnioskodawcy mogłoby naruszać prawa osób postronnych. Może to nastąpić na przykład poprzez anonimizację głosu osób postronnych. Dodatkowo podkreślić należy istnienie rozwiązań umożliwiających usunięcie fragmentu dźwięku z nagrań audio. Podniesiona przez spółkę kwestia nie powinna zatem powodować odmowy realizacji wniosku skarżącej. Ponadto forma przekazania kopii przetwarzanych danych osobowych nie powinna budzić wątpliwości osoby o nią wnioskującej, czy wszystkie jej dane osobowe zostały tą kopią objęte. Prezes UODO uznał, że w realizacji obowiązku spółka nie uwzględniła kopii wszystkich danych osobowych skarżącej przetwarzanych przez spółkę i nakazał jej spełnienie obowiązku informacyjnego z art. 15 ust. 3 RODO poprzez dostarczenie kopii jej

40 Zgodnie z art. 15 ust. 4 RODO prawo do uzyskania kopii, o której mowa w ust. 3 tego przepisu, nie może niekorzystnie wpływać na prawa i wolności innych.

danych osobowych utrwalonych na nagraniach uwzględniającej również głos skarżącej[41].

Należy zauważyć, że niezwykle istotne jest, aby osoba, której dane dotyczą, wnioskując o realizację swoich uprawnień w zakresie prawa do uzyskania kopii danych osobowych utrwalonych w nagraniu monitoringu wideo, dokładnie wskazała informacje pozwalające na znalezienie fragmentu nagrania, na którym utrwalono te dane. Na podstawie wskazanych przez wnioskodawcę informacji, administrator powinien móc zidentyfikować osobę wnioskującą na nagraniu, zwłaszcza w sytuacji, gdy znajduje się na nim wiele osób. W innym przypadku administrator może nie być w stanie ocenić, czyj głos lub wizerunek udostępnia, a także czy o kopię danych zwraca się osoba, której dane rzeczywiście zostały utrwalone na nagraniu.

Prezes UODO nie zgodził się z zaprezentowanym stanowiskiem spółki, a zwłaszcza z tym, że odmowa wydania kopii danych osobowych skarżącej w postaci jej wizerunku utrwalonego na nagraniu z monitoringu wizyjnego jest przejawem przestrzegania przepisów dotyczących ochrony danych osobowych. Spółka nie wykazała nadmiernego charakteru żądania skarżącej ani też nie udowodniła, że żądanie to jest ewidentnie nieuzasadnione (art. 12 ust. 5 RODO)[42]. Nie wykazała też, że udostępnienie nagrania nie może nastąpić bez naruszenia praw osób trzecich (art. 15 ust. 4 RODO). W ocenie Prezesa UODO, możliwość naruszenia praw i wolności innych osób, wbrew twierdzeniom spółki, obliguje ją do ochrony tych praw i wolności, w tym wypadku poprzez anonimizację danych osobowych – nie może natomiast uniemożliwić realizacji prawa osoby, której dane dotyczą, przysługującego jej zgodnie z RODO. W ocenie Prezesa Urzędu Ochrony Danych Osobowych spółka bezpodstawnie odmówiła skarżącej udostępnienia kopii jej danych, wobec czego skierował do niej stosowny nakaz[43].

Realizacja prawa do usunięcia danych

Obecnie administratorzy najczęściej przetwarzają dane z wykorzystaniem stosownego, często przeznaczonego do tego celu oprogramowania. Ograniczenie funkcjonalności stosowanego oprogramowania nie może jednak negatywnie wpływać na realizację praw osób, których dane dotyczą. To na administratorze ciąży wybór oprogramowania, którego funkcjonalność musi być dostosowana do wymogów RODO. Prezes UODO wskazuje chociażby na obowiązek administratorów danych do szczególnej dbałości o konfigurowanie i przeglądanie prawidłowości działania filtrów spamowych poczty elektronicznej. Zakwalifikowanie wiadomości będącej wnioskiem o realizację uprawnienia wynikającego z przepisów o ochronie danych osobowych do spamu i w następstwie jego nierozpatrzenie – może stanowić naruszenie przepisów RODO. Bardzo istotne jest również zabezpieczenie ciągłości realizacji praw osób, których dane dotyczą, w sytuacji zmian organizacyjnych (np. związanych z przejęciem podmiotu przez inny podmiot), jak i narzędzi służących

41 DS.523.4826.2020.

42 Zgodnie z art. 12 ust. 5 RODO, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

43 DS.523.4194.2022.

przetwarzaniu danych (np. przy ich przenoszeniu).

W jednej ze spraw skarżący zwrócił się do spółki, będącej administratorem jego danych – na specjalnie do tego wskazany przez spółkę adres e-mail – z wnioskiem o usunięcie jego danych osobowych, jednak nie uzyskał odpowiedzi. Spółka wyjaśniła, że wiadomość e-mail została zakwalifikowana przez filtr antyspamowy serwera pocztowego jako wiadomość naruszająca zasady bezpieczeństwa, skutkiem czego było automatyczne przeniesienie wiadomości na listę spam i jej pominięcie. Zgodnie z zasadami bezpieczeństwa wiadomości takie traktowane są jako zagrożenie dla systemu pocztowego. Spółka poinformowała, że podjęła działania mające na celu zapobieżenie takim sytuacjom w przyszłości poprzez zmianę konfiguracji skrzynek pocztowych oraz wprowadziła procedurę obowiązkowego przeglądania folderu spam i usuwania z niego wiadomości dopiero po ich weryfikacji przez pracownika.

W związku ze złożonym żądaniem usunięcia danych osobowych[44] administrator był zobowiązany do udzielenia skarżącemu odpowiedzi. Po złożeniu przez skarżącego wniosku o usunięcie jego danych osobowych zobowiązany był do niezwłocznej weryfikacji przetwarzanych przez siebie danych, a w przypadku ich braku, niezwłocznego poinformowania o tym fakcie skarżącego. Prezes UODO podkreślił, że nawet wiadomości zakwalifikowane przez serwer pocztowy jako rzekomy spam muszą być brane pod uwagę przez administratora danych jako wymagające wykonania działań określonych w RODO. To na administratorze danych ciąży obowiązek zapewnienia osobie, której dane dotyczą, możliwości realizacji przysługujących jej na mocy RODO praw. Sytuacja, w której skarżący nie może zrealizować swojego prawa, pomimo prawidłowo złożonego żądania, jest wynikiem uchybienia spółki. Adresatem do wykonywania praw osób, których dane dotyczą, jest administrator – jeśli administrator otrzyma żądanie, musi ono zostać przetworzone, nawet jeśli wewnętrznie ustalono zróżnicowany podział zadań w spółce. Dotyczy to również zmian organizacyjnych związanych z połączeniem lub przekształceniem spółek.

Prezes UODO udzielił spółce upomnienia za naruszenie art. 12 ust. 3 w zw. z art. 17 ust. 1 RODO, z powodu nieudzielenia skarżącemu odpowiedzi na jego żądanie[45].

W innej sprawie Prezes UODO wydał decyzję, w której skarżącemu odmówiono usunięcia danych osobowych w zakresie numeru telefonu. Spółka odmówiła realizacji żądania skarżącego wskazując, że swoje dane osobowe podał spółce dobrowolnie w celu zawarcia umowy o świadczenie usług elektronicznych, a zaakceptowany przez skarżącego regulamin usługi wymaga podania pełnych i poprawnych danych kontaktowych oraz ich aktualizowania w razie potrzeby, m.in. z uwagi na wykorzystanie tych danych przez kontrahentów podczas finalizacji transakcji zawartych przez skarżącego oraz brak możliwości technologicznych usunięcia danych.

44 Uprawnienie wynikające z art. 17 ust. 1 RODO.
45 ZSPR.440.1055.2019.

Spółka wskazała, że zweryfikowała obowiązującą procedurę i podejście do usuwania danych w przypadku otrzymania żądania usunięcia danych i niezwłocznie uwzględnia wnioski w tym przedmiocie, w związku z czym do skarżącego została skierowana informacja, iż w sytuacji podtrzymywania swojego stanowiska odnośnie usunięcia numeru telefonu, skarżący proszony jest o kontakt ze spółką. Skarżący nie zwracał się do spółki z ponownym żądaniem usunięcia jego danych osobowych w zakresie numeru telefonu, w związku z czym spółka w dalszym ciągu przetwarzała dane w tym zakresie.

W ocenie Prezesa UODO argumentacja spółki, że numer telefonu skarżącego jest niezbędny do realizacji umowy o świadczenie usług elektronicznych ze względu na wskazane przez nią powody, nie stanowi przesłanki do przetwarzania tych danych. Skoro skarżący dobrowolnie podał swój numer telefonu, to w chwili wniesienia przez niego żądania usunięcia tych danych i tym samym odwołania zgody na ich przetwarzanie, spółka nie posiadała przesłanki legalności przetwarzania danych osobowych skarżącego w zakresie numeru telefonu. W przypadku konieczności kontaktu ze skarżącym, spółka dysponowała innymi danymi skarżącego – jego imieniem, nazwiskiem, adresem zamieszkania oraz adresem poczty elektronicznej, w związku z czym w dalszym ciągu pozostawiało to spółce możliwość porozumiewania się ze skarżącym. Wykorzystanie tych danych przez kontrahentów spółki podczas finalizacji transakcji zawartych za jej pośrednictwem przez skarżącego, leży natomiast w zakresie woli i interesu skarżącego, należy więc zachować jego prawo do nieprzetwarzania danych osobowych w zakwestionowanym przez niego zakresie.

Podkreślić należy, że brak możliwości technologicznych usunięcia danych skarżącego, nie stanowi podstawy do odmowy usunięcia danych w zakresie numeru telefonu. Skoro spółka pozyskała numer telefonu i wprowadziła go do bazy danych, to powinna także dysponować narzędziami umożliwiającymi usunięcie danych. Tym bardziej, że spółka sama wskazała, że po zainicjowanej przez skarżącego sytuacji, zweryfikowała obowiązującą procedurę i podejście do usuwania danych w przypadku otrzymania żądania usunięcia danych i niezwłocznie uwzględnia wnioski w tym przedmiocie. W ocenie Prezesa UODO, skoro skarżący nie odwołał swojego oświadczenia, to spółka powinna usunąć dane w zakresie numeru telefonu, nie zaś kierować do niego zapytanie, czy podtrzymuje on swoje stanowisko odnośnie żądania ich usunięcia.

Z uwagi na to, że spółka ostatecznie nie uwzględniła żądania skarżącego i przetwarzała jego dane osobowe w zakresie numeru telefonu bez podstawy prawnej, Prezes UODO nakazał spółce usunięcie tych danych[46].

Realizacja prawa do sprostowania danych

Inna ze spraw dotyczyła zarzutu niezrealizowania prawa do sprostowania danych, wynikającego z art. 16 RODO. W związku ze zmianą adresu poczty elektronicznej, skarżący chciał sprostować używany adres poczty elektronicznej również w serwisie prowadzonym

46 ZSPR.440.963.2019.

przez spółkę. W związku z tym we wrześniu 2019 r. zwrócił się o zmianę adresu e-mail w portalu obsługiwanym przez spółkę. Podmiot ten udzielił skarżącemu odpowiedzi, z której wynikało, że serwis nie umożliwia zmiany adresu e-mail, i że w tym celu należy założyć nowe konto. W czerwcu 2020 r. spółka poinformowała o wprowadzeniu zmian w serwisie, które umożliwiają zmianę identyfikatora konta, którym był adres poczty elektronicznej.

Organ wskazał, że prawo do sprostowania danych osobowych, wynikające z art. 16 RODO, obowiązuje od dnia 25 maja 2018 r. Rozwiązanie techniczne umożliwiające dokonanie przewidzianego w unijnym rozporządzeniu uprawnienia spółka wprowadziła dopiero w kwietniu 2020 r., a więc po prawie 2 latach od rozpoczęcia obowiązywania ww. przepisów. W związku z niedostosowaniem przez spółkę w odpowiednim terminie działania prowadzonego przez nią serwisu internetowego do obowiązujących przepisów, skarżący pozbawiony został możliwości realizacji swojego prawa.

Prezes UODO udzielił spółce upomnienia za naruszenie art. 12 ust. 3 i art. 16 RODO, które polegało na braku możliwości realizacji w terminach przewidzianych we wskazanych przepisach RODO, żądania w zakresie sprostowania danych skarżącego, tj. zmiany adresu e-mail. Ponadto Prezes UODO udzielił upomnienia za naruszenie art. 12 ust. 1, 3 i 4 w zw. z art. 16 RODO, polegające na nieudzieleniu informacji o możliwości wniesienia skargi do organu nadzorczego i skorzystania ze środków ochrony prawnej przed sądem wobec odmowy administratora spełnienia żądania oraz na zaniechaniu dalszej komunikacji ze skarżącym, aż do podjętej po ponad roku – po interwencji organu nadzorczego, a jednocześnie po upływie 6 miesięcy od wprowadzenia technicznych rozwiązań pozwalających na realizację żądania skarżącego[47].

Sąsiedzki monitoring wizyjny

Podobnie jak w latach poprzednich, także w roku 2022 organ nadzorczy rozpatrywał liczne sprawy związane z przetwarzaniem danych osobowych za pomocą monitoringu wizyjnego. Najczęstszym wskazywanym w takich sprawach celem stosowania monitoringu wizyjnego była ochrona własności, zdrowia i życia. Impulsem do zainstalowania monitoringu przez podmioty prywatne był często konflikt sąsiedzki, który dodatkowo nie wpływał korzystnie na przejrzystość przetwarzania danych osobowych. Należy podkreślić, że w związku z rozwojem technologicznym i dostępem nowych funkcjonalności, monitoring może stać się bardzo inwazyjną i nieadekwatną do celów metodą przetwarzania danych osobowych.

Przykładem jest sprawa, w której skarżący podnieśli, że osoby skarżone m.in. przetwarzają ich dane osobowe przy wykorzystaniu monitoringu wizyjnego bez podstawy prawnej. Osoby skarżone wyjaśniły natomiast, że zainstalowane na ich nieruchomości kamery obejmują swoim zasięgiem wyłącznie obszar ich posesji, wobec czego monitoring sprowadza się do przetwarzania danych w ramach czynności o czysto osobistym lub domowym charakterze. Do tego zaś przetwarzania RODO nie ma zastosowania. Osoby

47 DS.523.1783.2020.

te przekonywały, że urządzenia rejestrujące obszar ich posesji nie ingerują w sferę prywatności skarżących, a do miejsc objętych monitoringiem wykraczających poza teren ich nieruchomości została zastosowana tzw. maska prywatności. Zamontowane przez skarżonych kamery obejmowały swoim zasięgiem teren ich posesji oraz drogę publiczną, a monitoring zainstalowano wyłącznie w celu zwiększenia bezpieczeństwa ich mienia. Skarżeni wskazali, że spełnili wobec skarżących obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 RODO[48], zamieszczając na bramie garażu znak informacyjny „obiekt monitorowany". Wskazali również, że skarżący nigdy nie zwracali się do nich z wnioskiem o usunięcie ich danych osobowych.

Prezes UODO w rozstrzygnięciu uwzględnił treść wyroku TSUE w sprawie C-212/13[49]. Zgodnie z tym wyrokiem, jeżeli system monitoringu wizyjnego, o ile obejmuje on ciągłe nagrywanie i przechowywanie danych osobowych i rozciąga się – „choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, o tyle nie powinien on być rozumiany jako czynność o czysto „osobistym lub domowym charakterze".

Prezes UODO uznał, że przetwarzanie danych osobowych pochodzących z nagrań monitoringu wizyjnego przez osobę fizyczną w celu opisanym w art. 2 ust. 2 lit. c) RODO[50], może odbywać się wyłącznie, gdy zasięg monitoringu obejmuje jedynie nieruchomość stanowiącą jej własność. Skierowanie kamer na drogę publiczną powoduje, że dochodzi do ciągłej obserwacji tego terenu, czego skutkiem jest przetwarzanie danych osobowych osób przemieszczających się po tym terenie. Proces konfigurowania sfery prywatności – tzw. maskowania obszaru obrazu, który jest wyłączony z monitoringu – jest procesem odwracalnym i może być w każdym czasie zmieniony przez użytkownika systemu monitoringu, w związku z czym nie może być uznany za skuteczne narzędzie, które w sposób trwały zapewni wyłączenie danego obszaru z monitoringu.

W związku z powyższym Prezes UODO nakazał zaprzestanie przetwarzania danych osobowych skarżących oraz ich usunięcie z dotychczas zebranych nagrań pochodzących z monitoringu wizyjnego obejmującego swoim zasięgiem drogę publiczną. W odniesieniu do kwestii realizacji obowiązku informacyjnego Prezes UODO stwierdził, że skarżeni nie spełnili obowiązku informacyjnego określonego w art. 13 ust. 1 lit. c), d), e) oraz ust. 2 lit. a), b),d) RODO[51]. Prezes UODO udzielił skarżonym upomnienia we wskazanym zakresie[52].

W kolejnej ze spraw skarżący złożył skargę na przetwarzanie jego danych osobowych

48 Zgodnie z art. 13 RODO, jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie przewidziane w niniejszym artykule informacje.

49 Wyrok TSUE z dnia z dnia 11 grudnia 2014 r. w sprawie C-212/13 František Ryneš przeciwko Úřad pro ochranu osobních údajů.

50 Zgodnie z art. 2 ust. 2 lit. c) RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze.

51 W tej sprawie w zakresie wskazania: celów przetwarzania danych osobowych, oraz podstawy prawnej przetwarzania; prawnie uzasadnionych interesów realizowanych przez administratora, informacji o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriów ustalania tego okresu; informacji o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia, ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; informacji o prawie wniesienia skargi do organu nadzorczego.

52 DS.523.399.2021.

bez podstawy prawnej za pomocą monitoringu wizyjnego oraz bezprawnym ich udostępnieniu podmiotom nieuprawnionym.

Skarżeni wyjaśnili, że skarżący nękał ich, co zostało stwierdzone wyrokami sądowymi. W efekcie zamontowali monitoring z funkcją rejestracji obrazu i dźwięku, w celu zapewnienia bezpieczeństwa. Kamera została tak skierowana, aby swoim zasięgiem obejmowała przede wszystkim wejście do ich domu oraz teren wspólny. Zaprzeczyli twierdzeniom skarżącego w zakresie udostępniania nagrań z monitoringu, w tym nagrania z jego wizerunkiem, osobom nieuprawnionym. Skarżeni twierdzili, że wypełnili obowiązek informacyjny, o którym mowa w art. 13 poprzez wielokrotne informowanie o zainstalowaniu kamery, jej zasięgu oraz że umieścili na drzwiach frontowych swojego mieszkania tablicę informacyjną z treścią „obiekt monitorowany". W odniesieniu do monitoringu wizyjnego z wykorzystaniem funkcji nagrywania dźwięku, Prezes UODO odwołał się do wytycznych Europejskiej Rady Ochrony Danych[53]. Zgodnie z nimi administrator przy wybieraniu rozwiązań technicznych odnoszących się do prowadzonego monitoringu powinien wybierać rozwiązania zawierające funkcje, które są niezbędne. Funkcje, które nie są niezbędne, powinny zostać dezaktywowane. Prezes UODO stwierdził, że nagrywanie głosu narusza zasadę wskazaną w art. 5[54] ust. 1 lit. c) RODO. Prowadzony przez skarżonych monitoring przy wykorzystaniu funkcji nagrywania głosu, nie jest odpowiedni i niezbędny do osiągnięcia przez nich celu, jakim jest zapewnienie bezpieczeństwa. W ocenie Prezesa UODO stosowanie funkcji nagrywania w sposób ciągły dźwięku w związku z prowadzonym monitoringiem prowadzi do naruszenia m.in. prawa do prywatności osoby obserwowanej.

W zakresie realizacji obowiązku informacyjnego Prezes UODO uznał, że skarżeni nie wykazali, aby przekazali skarżącemu informacje wynikające z treści art. 13 ust. 1 i 2 RODO, zaś działania przez nich podjęte (umieszczenie tablicy informującej wyłącznie o fakcie objęcia obiektu monitoringiem oraz poinformowanie o zasięgu kamery) nie są wystarczające[55].

4.1.3. Sektor zdrowia, zatrudnienia i szkolnictwa

Spośród **6995 skarg,** które w 2022 r. wpłynęły do Urzędu, **1346** z nich dotyczyło podmiotów działających w obszarze zdrowia, zatrudnienia i szkolnictwa. Poniżej omówione zostały przykłady kilku takich skarg.

Przetwarzanie przez pracodawcę danych osobowych znajdujących się na orzeczeniu lekarskim zwalniającym z obowiązku zakrywania ust i nosa[56]

Przedmiotem postępowania przed Prezesem UODO w jednej ze spraw, były nieprawidłowości w przetwarzaniu danych osobowych skarżącego będącego nauczycielem

53 Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo, wersja 2.1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl_0.pdf (dostęp: 28.02.2023 r.).
54 Zgodnie z art. 5 ust. 1 lit. c dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").
55 DS.523.2332.2021.
56 DS.523.7988.2021.

przez dyrektora placówki. Nieprawidłowości te polegały na przetwarzaniu danych osobowych zawartych w zaświadczeniu lekarskim o przeciwskazaniu do zakrywania ust i nosa w pomieszczeniach zamkniętych bez podstawy prawnej.

Skarżący uzyskał zaświadczenie lekarskie o bezwzględnych przeciwskazaniach do noszenia maseczki lub przyłbicy. W zaświadczeniu znajdowały się jego dane osobowe w zakresie imienia, nazwiska, numeru PESEL, daty urodzenia, adresu zamieszkania oraz informacje o zdrowiu fizycznym i psychicznym wraz z rozpoznaniem choroby. Skarżący poinformował o fakcie posiadania zaświadczenia administratora drogą wiadomości e-mail, zaznaczając jednocześnie, że nie prześle on żadnego potwierdzenia posiadania takiego dokumentu, ze względu na to, że administrator nie jest osobą uprawnioną do wglądu do tego dokumentu. Administrator wezwał skarżącego do przedstawienia dokumentu zwalniającego go z obowiązku zakrywania ust i nosa w pomieszczeniach zamkniętych, przed dopuszczeniem go do pracy. Skarżący okazał administratorowi ten dokument do wglądu, jednak nie zrobił tego dobrowolnie, obawiając się o swoje dalsze zatrudnienie. Administrator wskazał zaś, że skarżący sam zgodził się okazać dokument.

W czasie tego zdarzenia obowiązywało rozporządzenie Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii[57] w wersji obowiązującej od dnia 31 października 2021 r. do 29 listopada 2021 r. Wówczas nakazane było zakrywanie ust i nosa w pomieszczeniach zamkniętych, jednak nakazu tego nie stosowało się m.in. wobec osób dotkniętych zaawansowanymi schorzeniami neurologicznymi, układu oddechowego lub krążenia, przebiegającymi z niewydolnością oddechową lub krążenia. Okazanie dowodu zwolnienia z rzeczonego obowiązku było obowiązkowe jedynie wobec wąskiego zakresu podmiotów, takich jak Policja czy straż gminna, a dyrekcja szkół ani specjalnych ośrodków szkolno-wychowawczych nie znajdowała się na tej liście. Katalog podmiotów uprawnionych do wglądu w tego typu dokumenty został skonstruowany w sposób zamknięty.

W opisywanej sprawie administrator nie wykazał zaistnienia żadnej z przesłanek legalizujących przetwarzanie szczególnych kategorii danych, wymienionych w art. 9 ust. 2 RODO. W ocenie Prezesa UODO, administrator został prawidłowo i wystarczająco poinformowany o przysługującym skarżącemu zwolnieniu z obowiązku zakrywania ust i nosa w miejscu pracy. Dalsze działania administratora zmierzające do uzyskania wglądu do przedmiotowego dokumentu, po zakomunikowaniu przez skarżącego braku woli okazania tego dokumentu, przeczą zaś dobrowolności jego okazania.

W ocenie Prezesa UODO, żądanie skierowane wobec skarżącego stanowiło naruszenie zasad przetwarzania danych osobowych opisanych w art. 5 RODO w postaci zasady zgodności z prawem i rzetelności przetwarzania (art. 5 ust. 1 lit. a RODO) oraz zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO). Prezes UODO zwrócił uwagę, że zgodnie z motywem 43 RODO, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania

57 Dz.U.2021.861 z dnia 06.05.2021 r.

danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą a administratorem. Taki brak równowagi sił występuje w związku z zatrudnieniem i miał on miejsce między administratorem a skarżącym. Odmowa wyrażenia zgody na przetwarzanie przez pracownika wobec pracodawcy nie jest prawdopodobna, zważywszy na występującą między nimi zależność. Dlatego też dobrowolność przetwarzania musi być wyraźnie wykazana, co nie miało miejsca w przedmiotowej sprawie. Zgoda nie jest dobrowolna wówczas, gdy pojawia się jakikolwiek element przymusu lub presji.

Wobec powyższego Prezes UODO stwierdził naruszenie art. 9 ust.1 RODO przez administratora i zastosował wobec niego upomnienie, a w pozostałym zakresie umorzył postępowanie[58].

Publikacja utrwalonego w miejscu pracy wizerunku skarżącego na ogólnodostępnym portalu internetowym przez przedsiębiorcę dostarczającego sprzęt wykorzystywany w miejscu pracy

Kolejna sprawa dotyczyła nieprawidłowości w przetwarzaniu danych osobowych skarżącego polegającej na publikacji utrwalonego w miejscu pracy wizerunku na ogólnodostępnym portalu internetowym przez przedsiębiorcę dostarczającego sprzęt wykorzystywany w tym miejscu pracy. Prezes UODO w wydanej decyzji dokonał oceny przetwarzania danych osobowych zawartych na ww. portalu, biorąc pod uwagę występujące w sprawie okoliczności dotyczące formy i sposobu udostępnienia takich danych oraz twierdzeń przedsiębiorcy (niebędącego pracodawcą skarżącego), że upubliczniony materiał filmowy nie zawiera wizerunku osobowego, a jedynie wygląd dostarczonego do pracodawcy skarżącego urządzenia (wózka widłowego).

W decyzji nakazującej usunięcie danych osobowych skarżącego wskazano, że na kwestionowanej stronie internetowej był prezentowany przez przedsiębiorcę wizerunek skarżącego, obsługującego wózek widłowy w miejscu pracy. Przetwarzanie wizerunku skarżącego realizowane było na kanale przedsiębiorcy prowadzonym w związku z jego działalnością zawodową. Prezes UODO podkreślił, że skutkiem upubliczniania wizerunku skarżącego na ogólnodostępnym szeroko znanym portalu internetowym był nieograniczony dostęp do nagrania video przez szerokie grono odbiorców oglądających, którzy nie tylko mogli, ale również w dalszym ciągu mogą, zapoznać się z jego wizerunkiem widniejącym na nagraniu, na co skarżący nie wyrażał zgody. W wydanej decyzji organ właściwy do spraw ochrony danych osobowych wskazał, że rozpowszechnianie w ten sposób nagrania zawierającego wizerunek nie znajduje podstaw prawnych, a przedsiębiorca, który zarejestrował nagranie i je upublicznił na portalu, nie legitymował się żadną z przesłanek przetwarzania danych osobowych określonych w art. 6 ust. 1 RODO. Wobec tego Prezes Urzędu, korzystając z uprawnienia z art. 58 ust. 2 lit. c) RODO, nakazał przedsiębiorcy

58 DS.523.7988.2021.

usunięcie danych osobowych skarżącego publikowanych na stronie internetowej[59].

Przetwarzanie przez pracodawcę danych osobowych pracownika w zakresie prywatnego numeru telefonu dla celów służbowych

W analizowanym roku sprawozdawczym Prezes UODO rozstrzygał także w sprawie skargi, której przedmiot dotyczył między innymi nieprawidłowości, polegających na przetwarzaniu przez pracodawcę prywatnego numeru telefonu komórkowego pracownika bez podstawy prawnej. Pracownik administratora nie wyraził zgody na przetwarzanie jego danych osobowych w zakresie numeru telefonu dla celów służbowych, polegających na zapewnieniu bezpieczeństwa mienia administratora w ramach procesu aktywacji lub dezaktywacji systemu zabezpieczeń. W związku z powyższym skarżący zwrócił się do Prezesa UODO z żądaniem nakazania administratorowi usunięcia danych osobowych skarżącego w zakresie jego numeru telefonu komórkowego. Prezes UODO, po przeprowadzeniu postępowania administracyjnego wydał decyzję, mocą której m.in. udzielił administratorowi upomnienia za naruszenie artykułu 5 ust. 2 RODO oraz artykułu 6 ust. 1 RODO, poprzez przetwarzanie danych osobowych w zakresie numeru telefonu komórkowego bez podstawy prawnej.

Prezes UODO wskazał, że na administratorze spoczywa obowiązek przetwarzania danych osobowych zgodnie z prawem, z zachowaniem przesłanek, określonych w artykule 6 RODO oraz obowiązek wykazania, że osoba, której dane dotyczą (tu pracownik), wyraziła zgodę na przetwarzanie jej danych dla celów służbowych. Prezes UODO uznał stanowisko skarżącego jako zasługujące na uwzględnienie, z uwagi na kwestionowany przez niego brak udzielenia na rzecz administratora zgody na przetwarzanie jego prywatnego numeru telefonu komórkowego dla celów służbowych, przy jednoczesnym braku dysponowania przez administratora dowodami na potwierdzenie stanowiska, że uzyskał ustną zgodę od skarżącego na przetwarzanie jego danych osobowych we wskazanym powyżej celu[60].

Przetwarzanie danych osobowych pracownika po zakończeniu zatrudnienia

Przedmiotem oceny Prezesa UODO była skarga byłego pracownika na nieprawidłowości w procesie przetwarzania jego danych osobowych przez pracodawcę. Polegały one na bezprawnym przetwarzaniu jego służbowego adresu e-mail pomimo wypowiedzenia mu umowy o pracę oraz odebrania mu dostępu do jego danych osobowych, w tym danych prywatnych, zgromadzonych w systemach spółki, w tym na skrzynce e-mailowej.

Adres e-mail skarżącego był adresem przetwarzanym w związku z jego zatrudnieniem i wykorzystywany w celu realizacji przez niego obowiązków służbowych oraz w procedurze naliczania mu wynagrodzenia przez dział HR spółki do dnia upływu okresu wypowiedzenia. Po zaprzestaniu pełnienia jakiejkolwiek funkcji przez skarżącego spółka ustawiła automatyczną

59 DS.523.3629.2020.
60 DS.523.6412.2021.

odpowiedź kierowaną do wszystkich osób podejmujących kontakt za pośrednictwem adresu e-mail skarżącego, informującą, że nie pełni już żadnych funkcji w spółce, a w celu uzyskania informacji należy kontaktować się za pośrednictwem nowego adresu. Zablokowania adresu e-mail skarżącego, ustawienia wiadomości automatycznych, przekierowań oraz innych jego dostępów do systemów, dokonali upoważnieni pracownicy, którzy nie zapoznawali się z treścią korespondencji wpływającej na skrzynkę e-mailową.

Organ właściwy do spraw ochrony danych osobowych pozytywnie ocenił działania administratora. Spółka legitymowała się prawnie uzasadnionym interesem uprawniającym ją do przetwarzania adresu e-mail skarżącego w okresie wypowiedzenia i po ustaniu zatrudnienia zgodnie z art. 6 ust. 1 lit. f) RODO. W toku przeprowadzonego postępowania dowodowego organ nie stwierdził, aby przetwarzanie naruszyło zasady przetwarzania danych określone w art. 5 ust. 1 RODO[61].

Pozyskiwanie przez pracodawców informacji o przyczynie zwolnienia lekarskiego

Prezes UODO otrzymywał również skargi dotyczące pozyskiwania przez pracodawców informacji dotyczących specjalizacji lekarza wystawiającego skarżącym zwolnienia lekarskie, a następnie udostępnianie tej informacji osobom nieupoważnionym.

Jak wskazano w jednej ze spraw informacja o specjalizacji lekarza wystawiającego zwolnienie (psychiatria) była łatwa do pozyskania poprzez wyszukanie jej w Internecie w oparciu o nazwisko lekarza.

Skarżący zarzucali przy tym, że pracodawcy przedstawiają ich sytuację zdrowotną w sposób prześmiewczy, ujawniają tego rodzaju dane w sposób celowy, przekazując je innym współpracownikom. W jednej ze spraw skarżąca wskazała, że w konsekwencji udostępnienia jej danych odczuwała brak komfortu pracy w środowisku, które poznało jej problemy chorobowe.

Oceniając postępowanie pracodawców Prezes UODO uznał, że takie działanie stanowiło naruszenie danych osobowych zaliczanych do szczególnych kategorii. Prezes UODO nie znalazł uzasadnienia dla pozyskiwania przez pracodawców informacji w ww. zakresie. Każde działanie pracodawcy związane z przetwarzaniem danych musi mieć bowiem swoje prawne uzasadnienie i odpowiadać istniejącym regulacjom prawnym. Informacje dotyczące pracowników, w tym te odnoszące się do określonych zdarzeń, takich jak wystawienie zwolnienia lekarskiego, powinny być dostępne jedynie dla ograniczonego kręgu osób u danego pracodawcy. Do osób takich należą najczęściej osoby zarządzające zakładem pracy, osoby prowadzące sprawy osobowe, zatrudnienia i płac, radcy prawni świadczący dla pracodawcy pomoc prawną. Osoby te, w ramach wykonywanych obowiązków, są najczęściej upoważnione do przetwarzania danych innych pracowników, ponieważ wiąże się to ściśle z zakresem zadań, jakie wykonują w danym zakładzie pracy. Na administratorze danych spoczywa obowiązek zapewnienia ochrony danych osobowych

61 DS.523.2941.2022.

pracowników i wypracowania odpowiednich rozwiązań w celu zapobieżenia tego rodzaju zdarzeniom. Prezes UODO w tego rodzaju sprawach zdecydował o zastosowaniu wobec pracodawców upomnienia za naruszenie art. 9 ust. 1 oraz art. 5 ust. 1 lit. a) RODO[62].

Bezprawne udostępnienie danych osobowych pracownika osobom trzecim

Z analizy skarg z tego obszaru wynikało, że pracownicy często skarżą się na nieuprawnione udostępnienie ich danych osobowych przez pracodawców osobom trzecim. Zadaniem pracodawców udostępnianie danych osobowych nieuprawnionym podmiotom wynika często z braku odpowiedniego przeszkolenia personelu, chęci szybkiego zarządzania nieobecnościami w pracy, czy wreszcie z braku należytej uwagi dla przestrzegania przepisów RODO przez administratorów. W jednej z prowadzonych spraw ustalono, że pracodawca bez podstawy prawnej poinformował kontrahenta spółki oraz osobę zatrudnioną u pracodawcy o fakcie przebywania skarżącej na zwolnieniu lekarskim. Ponadto pracodawca wykorzystywał do korespondencji służbowej prywatny numer jej telefonu. Pracodawca argumentował, że udostępnienie informacji o przebywaniu przez skarżącą na zwolnieniu lekarskim było podyktowane koniecznością usprawiedliwienia kontrahentowi faktu, że w zastępstwie skarżącej jej obowiązki będzie wykonywać inna osoba oraz usprawiedliwienia faktu długotrwałego braku kontaktu z kontrahentem pracodawcy. Ponadto pracodawca przyznał, że korespondencja być może mogła omyłkowo i niecelowo być prowadzona z kontem użytkownika jednej z aplikacji, przypisanym do jej numeru prywatnego.

Prezes UODO stwierdził naruszenie art. 6 ust. 1 RODO polegające na przetwarzaniu bez podstawy prawnej danych osobowych skarżącej w zakresie prywatnego numeru telefonu oraz naruszenie art. 9 ust. 1 RODO polegające na udostępnieniu na rzecz osób nieuprawnionych danych osobowych dotyczących zdrowia (informacji o fakcie przebywania na zwolnieniu lekarskim) kontrahentowi pracodawcy oraz nieupoważnionej do przetwarzania danych osobowych skarżącej osobie zatrudnionej u pracodawcy[63].

Posługiwanie się danymi osobowymi byłego zleceniobiorcy w kontaktach z kontrahentami

Przedmiotem omawianej sprawy była skarga byłego zleceniobiorcy na działania spółki, będącej zleceniodawcą, która po zakończeniu współpracy posługiwała się imieniem, nazwiskiem i wizerunkiem przypisanym do imiennej skrzynki e-mail zleceniobiorcy w kontaktach z kontrahentami. Spółka rozsyłała wiadomości e-mail opatrzone imieniem, nazwiskiem i wizerunkiem zleceniobiorcy w osobie skarżącej.

Spółka wskazywała na istnienie po swojej stronie prawnie uzasadnionego interesu w przetwarzaniu danych osobowych skarżącej w kwestionowany sposób, tj. art. 6 ust 1 lit. f) RODO. Spółka wyjaśniła, iż z uwagi na nagłą rezygnację skarżącej ze zlecenia zmuszona

62 DS.523.4903.2020, DS.523.5467.2020, DS.523.2985.2022.
63 DS.523.2704.2021.

była do natychmiastowego jej zastąpienia. Spółka swoje działanie uzasadniała chęcią zachowania płynności komunikacji oraz zabezpieczeniem możliwości nawiązania kontaktu z kontrahentami i dotychczasowymi klientami.

Organ właściwy do spraw ochrony danych osobowych negatywnie ocenił działania administratora wskazując, że w celu legalizacji procesu przetwarzania danych w oparciu o art. 6 ust. 1 lit. f) RODO, na pierwszym etapie koniecznym jest kumulatywne spełnienie dwóch przesłanek, tj. istnienia po stronie administratora lub strony trzeciej prawnie uzasadnionego interesu oraz niezbędności przetwarzania do realizacji celu wynikającego z powyższego interesu. W drugim etapie wystąpienie przesłanki o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. Organ zauważył, iż o ile spółka wskazała na istnienie po swojej stronie interesu gospodarczego, to jednak zaniechała wykazania niezbędności przetwarzania danych osobowych skarżącej w celu realizacji tego interesu. Organ wskazał, że zakończenie współpracy ze skarżącą jako zleceniobiorcą spółki, choćby nagłe, w żaden sposób nie wpływa na prawne funkcjonowanie spółki w zakresie prowadzenia jej spraw i reprezentacji na zewnątrz. Spółka posiada organy, w tym zarząd, którego skład jest ujawniony w Krajowym Rejestrze Sądowym, wobec czego każdy z kontrahentów z łatwością mógł zweryfikować uprawnienia osoby kontaktującej się w imieniu spółki. Nie uszło również uwadze organu przy rozpatrywaniu opisywanej sprawy, że spółka miała dostęp do listy kontaktów, z którymi korespondencję e-mail prowadziła skarżąca, a także pełną treść tej korespondencji, co było w zupełności wystarczające do płynnego kontynuowania kontaktów z kontrahentami spółki.

Wobec powyższych ustaleń organ nadzorczy uznał, że administrator naruszył przepisy o ochronie danych osobowych, tj. art. 5 ust. 1 lit. c) oraz art. 6 ust. 1 RODO i upomniał za to naruszenie[64].

Uzyskiwanie przez lekarzy dostępu do danych osobowych zgromadzonych na Platformie Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE ZUS) oraz ich dalsze przetwarzanie

Do często wnoszonych do organu nadzorczego skarg na podmioty z sektora zdrowia należy zaliczyć te związane z dostępem lekarzy do PUE ZUS i danych przetwarzanych na tej platformie. W tego typu sprawach skarżący najczęściej kwestionowali uzyskanie dostępu do danych poprzez PUE ZUS w celach nieuzasadnionych względami medycznymi.

W jednej ze spraw Prezes UODO ustalił, że lekarz odpowiedzialny za zespół, którym kierował, w celu weryfikacji grafików czasu pracy podległego personelu, dokonał przeglądu grafiku czasu pracy osoby wnoszącej skargę. Wykorzystał do tego celu medyczny system teleinformatyczny funkcjonujący w podmiocie medycznym, który zapewnia dostęp do listy

64 DS.523.3215.2022.

zwolnień. Funkcjonalność systemu umożliwiła automatyczne połączenie się z profilem ZUS skarżącego i w konsekwencji osoba ta otrzymywała z ZUS komunikat o tym, że lekarz uzyskał dostęp do jej danych osobowych zawartych na PUE ZUS, a korzystanie z danych osoby skarżącej przez lekarza nie było zakończone wystawieniem zaświadczenia lekarskiego lub jego anulowaniem.

W ocenie Prezesa UODO, ww. działanie stanowiło naruszenie art. 9 ust. 1 w zw. z art. 5 ust. 1 lit. a) oraz lit. b) RODO. Z materiału dowodowego zgromadzonego w przedmiotowej sprawie jednoznacznie wynikało, że dostęp do danych osobowych skarżącego zgromadzonych na PUE ZUS nie był związany ze świadczeniem na jego rzecz usług medycznych. Z kolei nie ma przepisów, które legalizowałyby pozyskiwanie przez lekarzy dostępu do danych osobowych za pośrednictwem systemów medycznych, w celu innym niż wystawienie, anulowanie lub sprostowanie zaświadczenia lekarskiego[65].

Kolejna sprawa dotyczyła skargi w przedmiocie nieuprawnionego dostępu do danych osobowych skarżącego przez lekarza, który uzyskał wgląd do jego konta na PUE ZUS oraz nieuprawnionego udostępnienia lekarzowi numeru PESEL skarżącego przez szpital, w którym lekarz ten był zatrudniony, w celu zalogowania się na koncie PUE ZUS skarżącego. W sprawie ustalono, że lekarz dwukrotnie uzyskał dostęp do danych osobowych skarżącego zawartych w PUE ZUS. Dostęp ten nie był zakończony wystawieniem zaświadczenia lekarskiego lub jego anulowaniem. Skarżący nigdy nie był pacjentem lekarza, jak również nie wyrażał zgody na to, aby lekarz uzyskał wgląd w jego profil na PUE ZUS. Lekarz i szpital wyjaśnili, że lekarz przetwarzał dane osobowe skarżącego w kwestionowany przez niego sposób w związku z pełnieniem obowiązków zastępcy dyrektora ds. lecznictwa w szpitalu i wykonywanymi czynnościami nadzorczymi nad personelem tego szpitala, w tym również nad skarżącym zatrudnionym w szpitalu jako lekarz. W związku z powyższym za administratora danych osobowych skarżącego należało uznać szpital. Zarówno szpital jak i lekarz wyjaśnili ponadto, że do przetwarzania danych skarżącego w kwestionowany sposób doszło w celu sprawdzenia, czy skarżący przebywa na zwolnieniu lekarskim. Skarżący nie odpowiadał na próby kontaktu ze strony szpitala, ani też nie przedstawiał wyjaśnień, co do powodów swojej nieobecności w pracy, wobec czego szpital nie wiedział kiedy i czy w ogóle wróci on do pracy. Zdaniem szpitala sytuacja ta mogła skutkować zagrożeniem życia i zdrowia pacjentów, którzy byli powierzeni opiece skarżącego, bowiem jako osoba pełniąca funkcję kierownika oddziału miał szereg zadań, których wypełnienie warunkowało prawidłowe funkcjonowanie oddziału. Prezes UODO ocenił, że wskazane okoliczności nie mogły stanowić podstawy do uzyskania dostępu do danych skarżącego zgromadzonych w systemie PUE ZUS. Brak było bowiem przepisów, które legalizowałyby takie wykorzystywanie danych, jakie miało miejsce w niniejszej sprawie, tj. celem uzyskania dostępu do PUE ZUS przez lekarza nieuzasadnionego względami medycznymi (w szczególności w zamiarze wystawienia, anulowania bądź sprostowania zaświadczenia lekarskiego lub potwierdzenia prawdziwości zawartych w zaświadczeniu danych). Organ podkreślił, że szpital, w związku

65 DS.523.1436.2022.

z nieobecnością skarżącego, mógł wprowadzić inne procedury mające na celu uchronienie pacjentów przed ewentualnymi negatywnymi skutkami tej nieobecności. Mógł wyznaczyć m.in. inną osobę do pełnienia obowiązków w zastępstwie. Ponadto szpital posiadał inne narzędzia do weryfikacji zwolnień lekarskich, natomiast PUE ZUS pacjenta do tego typu weryfikacji nie służy. W związku z powyższym organ ocenił, że nie została spełniona żadna z przesłanek określonych w art. 9 ust. 2 RODO odnośnie kwestionowanego przez skarżącego nieuprawnionego dostępu do jego danych osobowych przetwarzanych za pośrednictwem PUE ZUS.

4.1.4. Sektor finansów, telekomunikacji i ubezpieczeń

Spośród **6995 skarg,** które w 2022 r. wpłynęły do Urzędu, **1466** z nich dotyczyło podmiotów sektora banków i instytucji finansowych, telekomunikacji i ubezpieczeń. Poniżej omówione zostały wybrane przykłady kilku takich skarg.

W roku 2022 działalność Prezesa UODO w omawianym obszarze skupiała się – podobnie do lat poprzednich – na rozpatrywaniu skarg osób kwestionujących proces przetwarzania ich danych związanych z zawieraniem różnego rodzaju umów, w tym przede wszystkim umów skutkujących powstaniem zobowiązań finansowych po stronie osób skarżących. W swoich decyzjach Prezes UODO podkreślał, że nie posiada kompetencji do rozstrzygania sporów wynikłych na tym tle, gdyż właściwość w tym zakresie mają sądy powszechne, podobnie jak w zakresie uznania zawartej umowy za prawnie nieskuteczną. W przypadku zawartej umowy, Prezes UODO jest natomiast organem właściwym do oceny legalności procesu przetwarzania danych osobowych z tym związanego. UODO często dostrzegał w takich sprawach nieprawidłowości w działaniach administratorów, którzy przedkładali swój własny interes gospodarczy nad prawami osób, których dane dotyczyły. Powyższe było szczególnie widoczne w obszarze działalności podmiotów sektora bankowego, głównie w sprawach dotyczących procesu przetwarzania związanego z obsługą zapytań kredytowych niezakończonych zawarciem umowy pomiędzy bankiem a podmiotem danych. Powoływane przez banki i podmioty działające na podstawie art. 105 ust. 4 Prawa bankowego, podstawy prawne w ww. sprawach często, zdaniem organu, nie mogły uzasadniać procesu przetwarzania danych w sytuacji, w której nie doszło do nawiązania stosunków gospodarczych.

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

Znaczna liczba skarg, które wpłynęły do Prezesa UODO 2022 r., podobnie jak w latach poprzednich, dotyczyła procesów przetwarzania danych osobowych klientów banków w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Osoby wnoszące skargi kierowały się z reguły chęcią poprawy swojej zdolności kredytowej i wyeliminowania, nielegalnego

w ich ocenie, procesu przetwarzania ich danych osobowych, który może im w przyszłości utrudnić lub nawet uniemożliwić uzyskanie kredytu lub pożyczki.

Banki, jako instytucje uprawnione do udzielania kredytów, mają obowiązek przeprowadzania oceny zdolności kredytowej osób ubiegających się o udzielenie kredytu, a także analizy ryzyka kredytowego. Powyższy obowiązek wynika z art. 70 Prawa bankowego, zgodnie z którym bank uzależnia przyznanie kredytu od zdolności kredytowej kredytobiorcy. Przez zdolność kredytową rozumie się zdolność do spłaty zaciągniętego kredytu wraz z odsetkami w terminach określonych w umowie. Regulacje dotyczące uprawnienia do przetwarzania informacji stanowiących tajemnicę bankową w tym celu znajdują się w art. 105a prawa bankowego, w ramach którego ustawodawca przewidział różne sytuacje mogące stanowić podstawę przetwarzania danych osobowych. W ust. 1 ww. przepis reguluje ww. uprawnienie przed oraz w trakcie istnienia zobowiązania, natomiast ust. 2, 3 - po jego wygaśnięciu.

Przetwarzanie danych osobowych w związku ze złożeniem zapytania kredytowego

Znaczną część skarg, które dotyczyły przetwarzania danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, stanowiły skargi dotyczące procesu związanego z obsługą zapytań kredytowych, które nie zakończyły się zawarciem umowy kredytu. Prezes Urzędu Ochrony Danych Osobowych, zarówno w decyzjach wydanych w latach poprzednich jak i w roku ubiegłym, konsekwentnie wyrażał stanowisko, zgodnie z którym w przypadku odmowy udzielenia kredytu, cel przetwarzania w postaci oceny zdolności kredytowej i analizy ryzyka kredytowego, został zrealizowany i brak jest podstaw prawnych do kontynuowania przetwarzania danych osobowych, pozyskanych w związku ze złożeniem wniosku kredytowego[66]. Tym samym przetwarzanie danych osobowych dotyczących zapytań kredytowych niezakończonych zawarciem umowy kredytu w celu oceny zdolności kredytowej i analizy ryzyka kredytowego jest niedopuszczalne i nie znajduje uzasadnienia w żadnej z przesłanek, o których mowa w art. 6 ust. 1 lit. f) RODO.

Przetwarzanie danych osobowych przez bank po wygaśnięciu zobowiązania, wynikającego z zawartej umowy

W omawianym 2022 roku Prezes UODO rozpatrywał liczne sprawy dotyczące przetwarzania przez banki i instytucje kredytowe danych osobowych objętych tajemnicą bankową, w celu oceny zdolności kredytowej i analizy ryzyka kredytowego po wygaśnięciu zobowiązania wynikającego z zawartej przez osobę, której dane dotyczą z ww. instytucją umowy. Zgodnie z art. 105a ust. 2 Prawa bankowego podstawą takiego przetwarzania może być zgoda podmiotu danych, która może zostać w każdym czasie odwołana, zaś w przypadku jej braku – legalność kontynuowania przetwarzania uzależniona jest od spełnienia przez bank

66 DS.523.5080.2021.

przesłanek, o których mowa w art. 105a ust. 3 Prawa bankowego. W decyzjach dotyczących legalności przetwarzania danych osobowych po wygaśnięciu zobowiązania wydanych w 2022 r. organ wielokrotnie stwierdzał, że banki nieprawidłowo realizują obowiązki, których spełnienie warunkuje legalność przetwarzania danych osobowych klientów bez ich zgody po wygaśnięciu zobowiązania.

Zgodnie z art. 105a ust. 3 Prawa bankowego banki, instytucje oraz podmioty, o których mowa w ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową i informacje udostępnione przez instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim[67], 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, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby o zamiarze przetwarzania dotyczących jej tych informacji, bez jej zgody.

Osią sporu w postępowaniach dotyczących legalności przetwarzania danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego był sposób realizacji obowiązku skutecznego poinformowania dłużnika o zamiarze przetwarzania jego danych osobowych na podstawie ww. przepisu. Organ uznawał, że bank winien przedstawić dowód na skuteczne poinformowanie, np. w postaci zwrotnych potwierdzeń odbioru przez dłużnika przesyłek zawierających ww. informację[68]. Niewystarczające natomiast jest ograniczenie się wyłącznie do samego oświadczenia o wysłaniu korespondencji i przedstawienie jej kopii wraz z kopią listy korespondencji bankowej wysłanej listem poleconym i nie stanowi dowodu na jej dostarczenie lub poinformowanie o jej treści adresata[69]. Organ wyrażał przekonanie, że przepisy powszechnie obowiązujące nie formułują obowiązku wysłania informacji, o której mowa w art. 105a ust. 3 Prawa bankowego w szczególnej formie. To od podmiotu informującego, którym jest bank, zależy zatem wybór formy przekazania odbiorcy komunikatu o zamiarze przetwarzania danych osobowych bez jego zgody. Jednocześnie organ dostrzegał, że to podmiot informujący wywodzi z powyższego skutki prawne, zatem to on musi wykazać, że poinformował swojego klienta o zamiarze przetwarzania danych stanowiących tajemnicę bankową, bez jego zgody na podstawie art. 105a ust. 3 Prawa bankowego. Zdaniem Prezesa Urzędu Ochrony Danych Osobowych, brak ustalenia daty, w której doszło do doręczenia korespondencji klientowi, uniemożliwia wykazanie przez bank, iż upłynęło 30 dni od poinformowania dłużnika o zamiarze przetwarzania jego danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego. Ostatecznie zaś to bezskuteczny upływ 30 dni od momentu poinformowania stanowi o wypełnieniu przesłanek

67 Ustawa z dnia 12 maja 2011 r. o kredycie konsumenckim (t.j. Dz. U. z 2023 r. poz. 1028), dalej: „ustawa o kredycie konsumenckim".
68 DS.523.2427.2021.
69 DS.523.6339.2021.

z art. 105a ust. 3 Prawa bankowego[70].

Przetwarzanie danych „na zapas”

Zgodnie z określoną w art. 5 ust. 1 lit. b) RODO zasadą ograniczonego celu, dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. O powyższej zasadzie nie zawsze jednak pamiętają administratorzy. Prezes UODO prowadził sprawy, w których jako główną i często jedyną przesłankę legalizującą przetwarzanie danych osobowych administratorzy wskazywali przesłankę wynikającą z art. 6 ust. 1 lit. f) RODO, powołując się na swój prawnie uzasadniony interes i uznając, że zachodzi on w przypadku, gdy pozostawili oni dane osobowe w swoich zasobach na wypadek, gdyby mogły się one okazać im przydatne w przyszłości. Istotne jest jednak, że legalność przetwarzania danych osobowych w oparciu o tę przesłankę uzależniona jest od wykazania, że 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 – wymaga ona tym samym dokonania ważenia interesów administratora i podmiotu danych. Prezes Urzędu Ochrony Danych Osobowych w wydanych decyzjach konsekwentnie uznawał, że przesłanka określona w art. 6 ust. 1 lit. f) RODO nie jest ukierunkowana na ochronę interesów sektora gospodarczego, tylko na ochronę interesów lub podstawowych prawa i wolności osoby, której dane dotyczą.

W 2022 r. Prezes UODO rozpatrywał sprawy, w których administratorzy jako jedyny cel, lub też jako jeden z celów przetwarzania danych osobowych wskazywali dochodzenie ewentualnych roszczeń lub obronę przed ewentualnymi roszczeniami, które mogą zostać zgłoszone w przyszłości. W takich sprawach Prezes Urzędu Ochrony Danych Osobowych wskazywał, że należy odróżnić sytuację, w której podmiot faktycznie dochodzi roszczeń względem osoby, której dane dotyczą lub gdy osoba ta zwróciła się do tego podmiotu z roszczeniem od sytuacji, gdy dane osobowe pozostawiane są w zasobach administratora na tzw. wszelki wypadek, tj. na wypadek zaistnienia konieczności dochodzenia lub obrony roszczeń w przyszłości, a więc w przypadku, gdy zaistnienie takiej sytuacji ma charakter czysto hipotetyczny. W ocenie organu nadzorczego brak istnienia dochodzonego roszczenia skutkuje uznaniem, że przetwarzanie danych osobowych jest niedopuszczalne w świetle przepisów RODO, bowiem ma charakter przetwarzania „na zapas”[71]. Jako niedopuszczalne przy powyższym Prezes UODO uznawał powoływanie się na terminy dotyczące przedawnienia roszczeń wynikające z przepisów prawa cywilnego. Zdaniem organu, przedawnienie roszczenia nie wywołuje skutków na gruncie ochrony danych osobowych. Nie wpływa bowiem na fakt istnienia roszczenia, a powoduje jedynie zmianę w sferze zarzutów procesowych w postaci możliwości podniesienia okoliczności przedawnienia w sporze sądowym. Podkreślenia wymaga, że okolicznością usprawiedliwiającą przetwarzanie

70 DS.523.2366.2020.
71 ZSPR.440.911.2019, ZSPR.440.280.2018.

danych osobowych w celu dochodzenia roszczeń jest sam fakt istnienia roszczenia oraz zamiar jego dochodzenia, nie jest nią natomiast zmiana w uprawnieniach procesowych podmiotu pozwanego[72].

Prezes Urzędu Ochrony Danych Osobowych wyrażał przekonanie, że przesłanka z art. 6 ust. 1 lit. f) RODO dotyczy sytuacji już istniejącej, w której celem wynikającym z prawnie uzasadnionych interesów realizowanych przez administratora była konieczność udowodnienia, potrzeba dochodzenia lub obrony przed roszczeniem istniejącym, nie zaś sytuacji, gdy dane są przetwarzane w celu zabezpieczenia się przed ewentualnym roszczeniem[73].

Przetwarzanie danych osobowych przez bank, w celu rozpatrzenia reklamacji

Za nieprawidłowe Prezes UODO uznawał także przetwarzanie przez banki danych osobowych na podstawie przepisów o rozpatrywaniu reklamacji[74] w przypadku, gdy do rozpatrzenia reklamacji już doszło, a postępowanie reklamacyjne zostało zakończone przez bank[75]. Dane osobowe mogą być przetwarzane w określonym celu, gdy jest to niezbędne do jego osiągnięcia. Wygaśnięcie (osiągnięcie) celu przetwarzania danych powinno po stronie administratora skutkować zaprzestaniem przetwarzania danych w tym celu.

Przetwarzanie danych osobowych przez dostawcę usług płatniczych w celach przekazywania informacji dotyczących tych usług

Prezes Urzędu Ochrony Danych Osobowych rozpatrywał również skargę osoby, która żądała, aby bank zaprzestał m.in. przesyłania jej wszelkich materiałów informacyjnych i reklamowych. Organ ustalił w tej sprawie, że bank był obowiązany do przesłania osobie skarżącej informacji na podstawie art. 29 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[76], zgodnie z którym dostawca informuje o proponowanych zmianach postanowień umownych nie później niż 2 miesiące przed proponowaną datą ich wejścia w życie, a korespondencja skierowana do osoby skarżącej właśnie takie informacje zawierała[77]. Podobna sytuacja ma miejsce w przypadku wysyłania informacji przez bank dla pełnomocników, którzy dysponują pełnomocnictwem rodzajowym tak szerokim, że mogą zarządzać rachunkiem niemal na równi z właścicielami tego rachunku. W takim przypadku bank może być zobowiązany do wysyłania stosownych informacji zgodnie z art. 27 ustawy o usługach płatniczych, który stanowi, że bank zobowiązany jest do przekazywania użytkownikowi informacji dotyczących prowadzonej obsługi, w tym m.in. dotyczących korzystania z usługi płatniczej, dotyczących opłat, stóp procentowych i kursów walutowych,

72 ZSPR.440.911.2019.
73 ZSPR.440.280.2018.
74 Ustawa z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym (t.j. Dz. U. z 2022 r. poz. 187 z późn. zm.).
75 DS.523.4158.2020.
76 Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2022 r. poz. 2360 z późn. zm.), dalej: „ustawa o usługach płatniczych".
77 ZSPR.440.1887.2019.

dotyczących komunikowania się[78].

Nieprawidłowości w procesie przetwarzania danych osobowych przez banki, powstałe w wyniku błędu pracownika banku lub nieprawidłowego działania systemu

Do częstych nieprawidłowości w procesie przetwarzania danych osobowych przez banki, zgłaszanych do Prezesa UODO w analizowanym okresie sprawozdawczym należały te spowodowane np. przez nieumyślny błąd pracownika administratora lub też nieprawidłowe działanie sytemu banku. Przykładami takich nieprawidłowości były m.in.:

- brak zmiany adresu korespondencyjnego w systemie obsługi kart pomimo zgłoszenia przez osobę, której dane dotyczą takiego wniosku do banku[79];
- wygenerowanie przez system raportu dotyczącego historii podatkowej z nadmiarowymi danymi, skutkujące ujawnieniem danych klienta innym klientom banku[80];
- opóźnienie rozpoznania i odnotowania wypowiedzenia umów i dalsze przetwarzanie danych klienta w celu realizacji tych umów bez podstawy prawnej[81];
- omyłkowe skierowanie korespondencji do osoby trzeciej skutkujące udostępnieniem danych osobowych osobie nieuprawnionej[82];
- omyłkowe prowadzenie czynności windykacyjnych pomimo wcześniejszego wpisania zadłużenia przez bank w straty[83].

Umieszczenie nadmiarowych danych na kopercie przez instytucję pożyczkową

W jednej ze spraw instytucja pożyczkowa skierowała do swojego dłużnika przesyłkę, w której na kopercie znajdowały się jego dane osobowe w zakresie imienia, nazwiska oraz adresu korespondencyjnego. Ponadto na odwrocie zaadresowanej do dłużnika koperty została umieszczona adnotacja: „Dział Windykacji. Wezwanie do zapłaty”. W taki sposób instytucja pożyczkowa udostępniła podmiotom nieuprawnionym dane osobowe dłużnika wskazujące na jego zadłużenie wobec ww. podmiotu. Prezes UODO nie zgodził się z administratorem, że usprawiedliwieniem dla przedmiotowego udostępnienia danych osobowych może być okoliczność, że w ww. sposób oznaczył on na kopercie jednostkę odpowiedzialną za przygotowanie pisma, w celu ułatwienia ewidencjonowania korespondencji. Administrator danych powinien zapewnić, aby dane osobowe przetwarzane były w sposób zgodny z prawem, w tym zgodnie z zasadami minimalizacji i poufności danych, przy użyciu odpowiednich środków organizacyjnych i technicznych. Zatem to administrator odpowiada za to, aby wdrożyć takie rozwiązania organizacyjne i techniczne, które będą

78 DS.440.250.2019.
79 DS.523.889.2021.
80 DS.523.191.2021.
81 ZWOS.440.3951.2019.
82 DS.523.3701.2022.
83 DS.523.2228.2021.

wystarczające dla zapewnienia, żeby dane osobowe przetwarzane były w sposób zgodny z prawem, z zachowaniem poufności i w minimalnym zakresie, jaki jest konieczny dla osiągnięcia celu przetwarzania. Ułatwienia organizacyjne po stronie administratora nie mogą w żadnym stopniu stanowić usprawiedliwienia dla naruszenia ww. przepisów art. 6 ust. 1 i zasad wynikających z RODO[84].

Przetwarzanie danych osobowych członków zarządu w związku z dochodzeniem roszczeń od spółki Prawa handlowego

Prezes Urzędu Ochrony Danych Osobowych rozpoznawał również skargi członków zarządu spółek handlowych na przetwarzanie ich danych osobowych przez podmioty trzecie w związku z pełnieniem przez nich ww. funkcji. W takich sprawach organ rozstrzygał, czy takie dane osobowe podlegają ochronie przewidzianej w przepisach RODO. W zdaniu drugim motywu 14 RODO wyjaśniono, że RODO nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. RODO chroni dane osobowe możliwych do zidentyfikowania osób fizycznych i wyklucza spod tej ochrony dane dotyczące osób prawnych. Istnieją jednak sytuacje, w których dane o charakterze osobowym będą związane z danymi dotyczącymi osób prawnych. Przykładem tego mogą być dane osobowe osób pełniących funkcję organów osoby prawnej. W takich sytuacjach spełnienie przesłanki identyfikowalności przesądzić powinno o objęciu zakresem ochronnym RODO danych osobowych również w takich konfiguracjach. W przypadku osób fizycznych pełniących funkcję członków organów osoby prawnej możliwość ich identyfikacji wynika w szczególności z faktu, iż dane takich osób ujawniane są w rejestrze przedsiębiorców Krajowego Rejestru Sądowego. Oznacza to, że należy odmiennie odnosić się do informacji o osobach prawnych i osobach fizycznych reprezentujących osoby prawne. W konsekwencji należy przyjąć, że dane osób fizycznych pełniących funkcje członków organów osoby prawnej będą stanowiły dane osobowe. Prezes Urzędu Ochrony Danych Osobowych podziela w tym zakresie stanowisko wyrażone w wyroku Trybunału Sprawiedliwości UE, który orzekł, że okoliczność, iż informacje wpisują się w ramy działalności zawodowej, nie oznacza, że nie można ich scharakteryzować jako dane osobowe. Definicja danych osobowych odnosi się zatem do osób fizycznych bez względu na rolę, jaką odgrywają (czy są konsumentami, przedsiębiorcami czy pracownikami). Należy zatem uznać, że dane członków zarządu reprezentujących osobę prawną, dane pełnomocników osób prawnych, a także dane pracowników, którzy są osobami kontaktowymi osoby prawnej, będących możliwymi do zidentyfikowania osobami fizycznymi, będą danymi osobowymi podlegającymi ochronie RODO[85].

84 DS.523.1235.2021.
85 Wyrok TSUE z dnia 9 marca 2017 r. w sprawie C-398/15.

Przetwarzanie danych osobowych przez ubezpieczyciela w związku z zawarciem umowy ubezpieczenia z osobę trzecią

Jedną ze spraw dotyczących przetwarzania danych osobowych przez ubezpieczyciela, była sprawa, w której skarżący kwestionował legalność przetwarzania jego danych osobowych w związku z umową ubezpieczenia zawartą przez osobę trzecią. Podmiot skarżony pozyskał dane osobowe skarżącego pierwotnie bezpośrednio od niego, jednak umowa ubezpieczeniowa obowiązująca w chwili wniesienia skargi do organu nadzorczego została zawarta przez jego matkę. Przedmiotem wskazanej umowy ubezpieczenia było objęcie ochroną ubezpieczeniową skarżącego z tytułu następstw nieszczęśliwych wypadków.

Organ wskazał, że zgodnie z art. 808 k.c., ubezpieczenie może być zawarte na cudzy rachunek. Przy czym ubezpieczony może nie być imiennie wskazany w umowie, chyba że jest to konieczne do określenia przedmiotu ubezpieczenia (ust. 1). Ubezpieczony jest także uprawniony do żądania należnego świadczenia bezpośrednio od ubezpieczyciela, chyba że strony uzgodniły inaczej; jednakże uzgodnienie takie nie może zostać dokonane, jeżeli wypadek już zaszedł (ust. 3). Ubezpieczony może żądać, aby ubezpieczyciel udzielił mu informacji o postanowieniach zawartej umowy oraz ogólnych warunków ubezpieczenia w zakresie, w jakim dotyczą praw i obowiązków ubezpieczonego (ust. 4).

Mając na uwadze powyższe, Prezes Urzędu Ochrony Danych Osobowych uznał, że nie ma podstaw do stwierdzenia, iż w tej sprawie zaistniały nieprawidłowości w przetwarzaniu danych osobowych. Kwestionowane przez osobę skarżącą przetwarzanie przez podmiot skarżony jej danych osobowych w związku z realizacją zawartej z osobą trzecią umowy ubezpieczenia, przedmiotem której było objęcie ochroną ubezpieczeniową skarżącego, znajdowało oparcie m.in. w art. 6 ust. 1 lit. c) RODO w związku z obowiązkami prawnymi wskazanymi przez podmiot skarżony[86].

Udostępnienie danych osobowych podmiotom nieuprawnionym przez ubezpieczyciela

Organ wydawał również decyzje, w których stwierdzał naruszenia polegające na udostępnianiu przez podmioty sektora ubezpieczeniowego danych osobowych na rzecz podmiotów nieuprawnionych. Prezes Urzędu Ochrony Danych Osobowych zwracał w tych sprawach uwagę, że proces przetwarzania danych osobowych musi być zgodny z zasadami ustanowionymi w art. 5 ust. 1 RODO, do których zalicza się między innymi zasadę integralności i poufności (art. 5 ust. 1 lit. f RODO). Zgodnie z motywem 39 RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im bezpieczeństwo i poufność, w tym między innymi ochronę przed nieuprawnionym dostępem do nich, tak przez administratora jak i podmiot działający na podstawie umowy powierzenia danych.

W jednej ze spraw Prezes Urzędu Ochrony Danych Osobowych ustalił, że w związku

86 DS.523.2541.2020.

z procesem likwidowania szkody w ramach umowy ubezpieczenia nieruchomości, doszło do udostępnienia danych osobowych skarżącego znajdujących się w polisie ubezpieczeniowej, osobie trzeciej, której mieszkanie zostało zalane przez skarżącego. Podmiot skarżony powierzył dane osobowe osoby skarżącej na podstawie art. 28 ust. 3 RODO w celu wykonania oględzin w związku ze szkodą zgłoszoną z polisy osoby skarżącej. Pracownik podmiotu z powierzenia, który udostępnił poszkodowanej dane osobowe skarżącej zawarte w polisie ubezpieczenia, działał więc w imieniu podmiotu skarżonego. Powyższe działanie zostało przez organ uznane za nieznajdujące uzasadnienia w żadnej z przesłanek z art. 6 ust. 1 RODO[87].

W kolejnej ze spraw zakończonych upomnieniem podmiotu skarżonego ustalono, że skarżony prowadził postępowanie likwidacyjne dotyczące zgłoszonej przez osobę skarżącą szkody. Skarżony przesłał korespondencję zawierającą akta szkody do nieuprawnionego odbiorcy – do kancelarii zajmującej się pomocą osobom poszkodowanym w wypadkach w uzyskaniu należnego odszkodowania – zamiast do Rzecznika Finansowego, który zwrócił się o udostępnienie akt przedmiotowej sprawy. Ujawnienie danych nastąpiło w zakresie danych, do których odnosi się art. 6 RODO, ale co istotniejsze - również danych szczególnej kategorii uregulowanych w art. 9 RODO. W tej sprawie nie zaistniała żadna przesłanka legalizująca dopuszczalność przetwarzania (udostępnienia) danych osobowych osoby skarżącej, wobec czego w niniejszej sprawie Prezes Urzędu Ochrony Danych Osobowych udzielił upomnienia podmiotowi skarżonemu[88].

Realizacja obowiązku udostępnienia kopii danych w zakresie adresu IP

W roku 2022 organ nadzorczy wydał również wobec podmiotów sektora telekomunikacyjnego szereg decyzji upominających za nieprawidłową realizację żądania wniesionego w trybie art. 15 ust. 3 RODO w zakresie udostępnienia kopii dynamicznego adresu IP.

W przedmiotowych sprawach organ zajął stanowisko, zgodnie z którym dynamiczny numer IP stanowi dane osobowe w myśl art. 4 pkt 1 RODO. W związku z tym osoba, której dane dotyczą, jest uprawniona do otrzymania kopii tej danej w trybie art. 15 ust. 3 RODO. Uzasadnienie prawne sentencji przedmiotowych decyzji oparto m.in. na stanowiskach Trybunału Sprawiedliwości Unii Europejskiej i Naczelnego Sądu Administracyjnego oraz Grupy Roboczej Art. 29.

W przedmiotowych sprawach Prezes Urzędu Ochrony Danych Osobowych nie kwestionował legalności przetwarzania danych osobowych przez operatora telekomunikacyjnego w zakresie adresu IP, z którego korzystali skarżący, albowiem obowiązek posiadania tych danych przez operatora wynika wprost z wyżej przytoczonych przepisów prawa, jak również posiadał on możliwość jego ustalenia.

87 ZSPR.440.1339.2019.
88 ZSPR.440.1902.2019.

Zgodnie art. 180a ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[89] przedsiębiorcy telekomunikacyjni są m.in.: 1) zobowiązani na własny koszt zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi; 2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom (którymi w myśl art. 179 ust. 1 pkt 1 lit. a Prawa telekomunikacyjnego, są Policja, Biuro Nadzoru Wewnętrznego, Straż Graniczna, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne i Krajowa Administracja Skarbowa), a także sądowi i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych. Prezes Urzędu Ochrony Danych Osobowych uznał, że przedsiębiorca telekomunikacyjny może je również udostępniać osobom, których dane dotyczą, gdy wniosą o doręczenie kopii ich danych osobowych na podstawie art. 15 ust. 3 RODO.

W żadnym z prowadzonych przed Prezesem Urzędu Ochrony Danych Osobowych postępowań dotyczących powyższego zagadnienia, operatorzy telekomunikacyjni nie zrealizowali w terminie określonym w art. 12 ust. 3 RODO żądań skarżących. Niektóre z podmiotów spełniły powyższy obowiązek dopiero na skutek złożenia skarg do Prezesa UODO, tym samym odpowiedzieli wnioskującym z naruszeniem terminu wskazanego w art. 12 ust. 3 RODO. W pozostałych natomiast przypadkach, wobec upływu okresu retencji danych, który stosownie do treści art. 180a ust. 1 pkt 1 Prawa telekomunikacyjnego, wynosi 12 miesięcy, licząc od dnia połączenia, nie było możliwe wydanie decyzji nakazującej spełnienie żądania w powyższym zakresie. W związku z powyższym UODO udzielił upomnień operatorom telekomunikacyjnym za naruszenie art. 15 ust. 3 w zw. z art. 12 ust. 3 RODO, polegające odpowiednio na spełnieniu żądania z naruszeniem terminu wskazanego w art. 12 ust. 3 RODO lub niezasadnej odmowie spełnienia żądania w tym terminie[90].

4.1.5. Postępowania transgraniczne

Prezes Urzędu Ochrony Danych Osobowych uczestniczy w ramach wzajemnej współpracy w egzekwowaniu przestrzegania i stosowania przepisów wynikających z RODO w Europejskim Obszarze Gospodarczym (EOG). Organy nadzorcze współdziałają poprzez System Wymiany Informacji na Rynku Wewnętrznym Komisji Europejskiej (IMI), z którego wykorzystaniem prowadzone są postępowania o charakterze transgranicznym. Postępowania te różnią się od siebie z uwagi na odmienne proceduralne przepisy krajowe państw członkowskich Unii Europejskiej (UE), niemniej Europejska Rada Ochrony Danych

89 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2022 r. poz. 1648 z późn. zm.), dalej: „prawo telekomunikacyjne".
90 DS.523.5555.2020, DS.523.5798.2020, DS.523.5928.2020, DS.523.5700.2020, DS.523.5790.2020, DS.523.5731.2020, DS.523.5677.2020, DS.523.6133.2020, DS.523.5889.2020, DS.523.6319.2020, DS.523.5455.2020, DS.523.5472.2020, DS.523.5458.2020, DS.523.5499.2020, DS.523.5374.2020, DS.523.5446.2020, DS.523.5621.2020, DS.523.5977.2020.

(dalej także: EROD)[91] wraz z wszystkimi organami nadzorczymi prowadzą prace nad wspólnymi wytycznymi ujednolicania przepisów w tym zakresie, w szczególności w tak kluczowych kwestiach jak np. sposób i forma przyjmowana skarg dla wszystkich organów nadzorczych.

Podkreślić należy, że istnieją wytyczne przyjęte przez EROD odnośnie współpracy pomiędzy organami nadzorczymi oraz prowadzenia postępowań transgranicznych, jednak nie w każdym przypadku (zgodnie z przepisami krajowymi danego organu) jest możliwość zastosowania się do nich w pełni przez każdy z organów nadzorczych.

Dłuższy czas rozpatrzenia skarg transgranicznych wiąże się z ich skomplikowanym charakterem, w tym sposobem ich prowadzenia i komunikacji, a także ich znaczną liczbą.

Znaczna część spraw prowadzonych w 2022 r. w ramach współpracy transgranicznej dotyczyła skarg w przedmiocie nieprawidłowości w procesie przetwarzania danych osobowych przez administratorów, polegających na przetwarzaniu danych osobowych bez podstawy prawnej w związku z odwiedzeniem przez skarżących stron internetowych w zakresie (a) przechowywania informacji lub uzyskania dostępu do informacji w urządzeniu końcowym abonenta lub użytkownika (tzw. umieszczanie plików cookie), jak również (b) tzw. późniejszych czynności przetwarzania.

Prowadzone sprawy dotyczyły również realizacji praw skarżących wobec administratorów oferujących dostęp do portali społecznościowych, takich jak Facebook oraz Twitter, zwłaszcza w zakresie prawa dostępu do danych oraz prawa usunięcia danych.

Kierując żądania podjęcia działań przez organ w sprawach o charakterze transgranicznym, skarżący często nie wskazywali podjęcia jakich czynności domagają się od Prezesa UODO, jak również zwracali się do Prezesa UODO z żądaniami dotyczącymi kompetencji autonomicznych organu nadzorczego, np. nałożenia kary administracyjnej lub przeprowadzenia kontroli w siedzibie administratora. Natomiast administratorzy zazwyczaj udzielali wyczerpujących odpowiedzi na zadane pytania oraz nie ukrywali ewentualnych naruszeń ochrony danych, tłumacząc je często błędem ludzkim.

Poprzez szeroką współpracę i współdziałanie wszystkich organów nadzorczych w zakresie ochrony danych osobowych, rozpatrywanie skarg transgranicznych ma, zdaniem Prezesa UODO, znaczny wpływ na większą świadomość korzystania ze swoich praw przez skarżących. Sprawy dotyczące znanych administratorów, przetwarzających dane osobowe dużej części społeczeństwa, np. na portalach społecznościowych bywają głośno komentowane, zaś taki większy rozdźwięk społeczny przekłada się na świadomość osób, których dane dotyczą w zakresie przysługujących im praw wynikających z RODO. Większość podmiotów skarżonych w sprawach zakwalifikowanych jako transgraniczne zajmuje się dostarczaniem usług mediów społecznościowych, transportem i płatnościami internetowymi.

91 Więcej informacji na temat EROD por. Rozdz. IV pkt 1 sprawozdania „Współpraca w ramach EROD".

Współpraca między organem, do którego wpłynęła skarga, tj. Prezesem UODO a wiodącym organem nadzorczym, tj. NAIH (węgierski organ nadzorczy) w sprawie skargi w przedmiocie naruszenia polegającego na udostępnieniu danych osobowych skarżącego, w tym danych dotyczących zdrowia, osobom trzecim przez podmiot świadczący usługi transportu lotniczego[92]

Skarżący odbył lot zorganizowany przez administratora, ale jego bagaż rejestrowany nie został dostarczony do miejsca przeznaczenia. W skardze stwierdził, że administrator przetwarzał jego dane z naruszeniem zasady minimalizacji danych oraz zasady celowości. Dlatego zażądał (1) usunięcia danych osobowych przetworzonych i przekazanych (ujawnionych) niezgodnie z prawem, włącznie z zobowiązaniem do podjęcia rozsądnych działań i poinformowaniem administratorów o żądaniu usunięcia wszelkich połączeń do tych danych i ich kopii / replikacji oraz (2) ograniczenia przetwarzania danych osobowych zebranych w związku z postępowaniem reklamacyjnym wyłącznie do celu, w jakim powinny być przetwarzane.

Prezes UODO przekazał skargę NAIH jako wiodącemu organowi nadzorczemu, a ten uznał się za wiodący organ nadzorczy w rozumieniu art. 56 ust. 1 RODO oraz podjął się rozpatrzenia skargi.

W ramach wyjaśnień spółka wskazała, że w odpowiedzi na reklamację skarżącego przesłała informację o jej rozpatrzeniu oraz listę dokumentów wymaganych do rozpatrzenia reklamacji. Ale pracownik obsługi klienta nie wysłał tej odpowiedzi na adres e-mail skarżącego, tylko na adres e-mail zarejestrowany na konto, za pośrednictwem którego zakupiono bilet lotniczy. W celu przedstawienia informacji pismo zawierało również samą reklamację, w wyniku której jej treść została przekazana osobie trzeciej.

Pierwsze pismo wysłane przez pracownika na adres e-mail zarejestrowany na konto, za pośrednictwem którego zakupiono bilet lotniczy skarżącego, zostało przekazane wraz z reklamacją, przypuszczalnie przez biuro podróży odpowiedzialne za organizację podróży, do współpracownika skarżącego. Ostatecznie cała korespondencja została przekazana skarżącemu przez współpracownika. Skarżący przekazał spółce pełną korespondencję i zażądał informacji na temat podstawy prawnej, na podstawie której spółka przekazała jego dane osobowe, w tym dane dotyczące zdrowia, osobom trzecim. Skarżący powtórzył ten wniosek kilkukrotnie i poinformował spółkę, że w przypadku braku odpowiedzi skieruje sprawę do polskiego organu ochrony danych.

Spółka stanęła na stanowisku, że ze względu na błąd wynikający z zaniedbania pracownika, poufność danych dotyczących stanu zdrowia skarżącego została naruszona. Spółka podjęła natychmiastowe działania po stwierdzeniu incydentu w celu wysłania odbiorcy danych osobowych, których dotyczy incydent, żądania usunięcia niesłusznie przesłanych danych osobowych oraz podjęcia działań w celu usunięcia danych również w odniesieniu do

92 ZSPR.440.1802.2019.

osób trzecich, którym dane osobowe, których dotyczy incydent, mogły zostać przekazane.

W projekcie decyzji NAIH ustalił, że spółka naruszyła art. 5 ust. 1 lit. f), art. 6 ust. 1, art. 9 ust. 1 i art. 15 ust. 1 RODO. Z powodu powyższych naruszeń NAIH udzielił spółce upomnienia na podstawie art. 58 ust. 2 lit. b) RODO. NAIH stwierdził, że spółka zgodnie z prawem przetwarzała dane osobowe zawarte przez skarżącego w reklamacji, tj. zgodnie z ciążącym na niej obowiązkiem prawnym wynikającym z węgierskiej ustawy o ochronie konsumentów, a zatem nie może ich usunąć zgodnie z art. 17 ust. 3 lit. b) RODO. NAIH zauważył ponadto, że w toku postępowania nie ustalił, jakoby spółka przetwarzała dane osobowe skarżącego zawarte w reklamacji do celów innych niż te, o których mowa w art. 17/A ust. 7 węgierskiej ustawy o ochronie konsumentów, a zatem część skargi nr 1 uznana została za bezzasadną. NAIH zauważył również, że skutek prawny drugiej części skargi (art. 58 ust. 2 lit. g) RODO), tj. uznanie, że NAIH powinien nakazać spółce podjęcie rozsądnych działań, aby poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje – nie miał zastosowania w przedmiotowej sprawie, ponieważ można to zrobić i uznać za istotne tylko wtedy, gdy dane osobowe zostały upublicznione przez administratora danych zgodnie z art. 17 ust. 2 RODO, a takie przetwarzanie danych nie miało miejsca w przedmiotowej sprawie. Jednak informując użytkownika adresu e-mail zarejestrowanego na konto, za pośrednictwem którego zakupiono bilet lotniczy skarżącego o naruszeniu ochrony danych i żądając usunięcia wiadomości e-mail zawierającej dane osobowe skarżącego, w tym jego dane zdrowotne, które zostały mu przekazane bezprawnie, spółka zastosowała się zasadniczo do drugiej części skargi, ponieważ w opinii NAIH było to w rzeczywistości celem wnioskowanego środka. NAIH nie uznał za konieczne nakazanie spółce zastosowania się do żądania dostępu do danych skarżącego na podstawie art. 58 ust. 2 lit. c) RODO, ponieważ z jednej strony skarżący nie złożył takiego żądania w swoim piśmie skierowanym do organu polskiego, a z drugiej strony ustalono w toku postępowania, że dane zostały przekazane bez podstawy prawnej, tj. że nie otrzyma od spółki nowych merytorycznych informacji dotyczących przetwarzania jego danych osobowych.

NAIH rozpatrzył wszystkie okoliczności sprawy na podstawie art. 83 ust. 2 RODO oraz art. 75/A ustawy o ochronie prywatności i stwierdził, że nie ma potrzeby nakładania administracyjnej kary pieniężnej za naruszenie stwierdzone w niniejszym postępowaniu, wystarczy upomnieć spółkę za popełnione przez nią naruszenia.

Węgierski organ nadzorczy projekt decyzji przekazał najpierw za pomocą notyfikacji 60IC (nieformalne konsultacje). Mając na uwadze procedurę przewidzianą w art. 60 RODO, polski organ nadzorczy nie zgłosił mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, zgłaszając jedynie komentarz odnośnie braku spójności między naruszeniami stwierdzonymi w sentencji decyzji oraz w jej uzasadnieniu. Węgierski organ nadzorczy zgodził się z komentarzem Prezesa UODO i przekazał nowy projekt decyzji z naniesioną zmianą. Prezes UODO zgodził się z treścią projektu decyzji, w związku z czym NAIH przekazał następnie ostateczną decyzję. Wypełniając dyspozycję art. 60 ust. 7 RODO, Prezes UODO

poinformował skarżącego o decyzji.

Procedowanie powyższej sprawy obrazuje efektywną współpracę wiodącego organu nadzorczego oraz organu, którego sprawa dotyczy. Węgierski organ nadzorczy przekazał projekt decyzji najpierw w ramach dobrowolnej notyfikacji 60IC, tak aby umożliwić Prezesowi UODO przedstawienie uwag przed rozpoczęciem właściwej procedury wynikającej z art. 60 RODO. Po otrzymaniu komentarza Prezesa UODO, NAIH uwzględnił komentarz i dopiero wtedy uruchomił oficjalną procedurę art. 60 oraz wynikające z niego limity czasowe.

Udział Prezesa UODO w procedurze rozwiązywania sporów między organami nadzorczymi przez Europejską Radę Ochrony Danych[93]

Prezes UODO brał udział w charakterze organu, którego sprawa dotyczy, w wydawaniu decyzji przez irlandzki organ nadzorczy (Data Protection Commission - DPC) w trzech sprawach, które dotyczyły spółki Meta Platforms Ireland Limited i jej platform: Facebook i Instagram oraz spółki WhatsApp Ireland Limited. DPC wydał w tych sprawach projekty decyzji, do których szereg organów nadzorczych państw Unii Europejskiej zgłosiło mające znaczenie dla sprawy i uzasadnione sprzeciwy. Na skutek braku możliwości osiągnięcia porozumienia między organami zainicjowano procedurę rozstrzygania sporów przez Europejską Radę Ochrony Danych (EROD), w której brał również udział Prezes UODO.

Wskazane wyżej sprawy dotyczyły żądania przez platformy Facebook, Instagram i WhatsApp wyrażenia przez ich użytkowników zgody na nowe warunki świadczenia ich usług, zaś bez wyrażenia zgody użytkownicy nie mieli możliwości korzystania z oferowanych usług. Zdaniem skarżących zgoda na nowe warunki nie była dobrowolna, warunki te były sprzecznie z postanowieniami RODO, a sposób i zakres przetwarzania danych w nich przedstawiony był niejasny. Administrator wskazywał w każdej ze spraw, że nie opierał on swojego przetwarzania danych na podstawie zgody osób, których dane dotyczą - art. 6 ust. 1 lit. a) RODO, lecz na podstawie art. 6 ust. 1 lit. b) RODO, a więc w celu wykonania umowy, której stronami byli użytkownicy wyżej wskazanych aplikacji.

DPC w przypadku Facebooka uznał, że administrator ten może powoływać się na umowę jako podstawę prawną przetwarzania danych użytkowników, która jest niezbędna dla świadczenia usługi, w tym do funkcjonowania kluczowego elementu serwisu administratora, czyli wyświetlania reklam (w tym reklam behawioralnych), w zamian za oferowanie darmowej usługi mediów społecznościowych. DPC uznał, że w odniesieniu do przetwarzania danych w oparciu o art. 6 ust. 1 lit. b) RODO, doszło do naruszenia art. 5 ust. 1 lit. a), 12 ust. 1 oraz 13 ust. 1 lit. c) RODO. DPC zastosował wobec administratora nakaz dostosowania operacji przetwarzania do przepisów RODO oraz zaproponował nałożenie dwóch kar administracyjnych: w wysokości 18-22 milionów EUR za naruszenie art. 6 ust .1 lit. b) RODO w związku z art. 5 ust. 1 lit. a) oraz art. 13 ust. 1 lit. c) RODO oraz kary w granicach 10-14 milionów EUR za naruszenie 6 ust .1 lit. b) RODO w związku z naruszeniem art. 5 ust. 1 lit.

93 DS.612.381.2021 (dot. Facebook), DS.612.43.2021 (dot. Instagram), DS.612.73.2021 (dot. WhatsApp).

a) oraz art. 12 ust. 1 RODO.

EROD w swojej decyzji nakazał DPC stwierdzenie naruszenia art. 6 ust. 1 RODO i przeprowadzenie dalszego postępowania wyjaśniającego w sprawie przetwarzania szczególnej kategorii danych osobowych. EROD nakazał DPC stwierdzenie naruszenia przez administratora art. 5 ust. 1 lit. a) RODO w postaci zasady rzetelności. EROD polecił DPC włączenie do ostatecznej decyzji nakazu dostosowania operacji przetwarzania danych w celach reklamy behawioralnej do art. 6 ust. 1 RODO oraz zmodyfikowanie nakazu dostosowania polityki i warunków świadczenia usług Meta do zgodności z art. 5 ust. 1 lit. a), art. 12 ust. 1 i art. 13 ust. 1 lit. c) RODO, aby nie odnosiły się wyłącznie do art. 6 ust. 1 lit. b) RODO, ale również do danych przetwarzanych do celów reklamy behawioralnej w kontekście usług administratora, aby odzwierciedlić ustalenie, że w przypadku tego przetwarzania administrator nie może powoływać się skutecznie na art. 6 ust. 1 lit. b) RODO. EROD uznał, że zaproponowana przez DPC wysokość administracyjnej kary pieniężnej nie odzwierciedla charakteru i wagi naruszenia i powinna ona zostać podwyższona, aby była skuteczna proporcjonalna i odstraszająca, biorąc pod uwagę stwierdzenie dodatkowych naruszeń.

DPC w przypadku Instagrama stwierdził, że administrator ten nie musiał opierać przetwarzania na zgodzie i nie chciał korzystać z takiej podstawy prawnej, lecz przetwarzał on dane na podstawie umowy – art. 6 ust. 1 lit. b) RODO. DPC uznał, że doszło do naruszenia art. 5 ust. 1 lit. a), art. 12 ust. 1 oraz art. 13 ust. 1 lit. c) RODO, ze względu na to, że administrator nie przekazał swoim użytkownikom niezbędnych informacji dotyczących podstawy prawnej przetwarzania oraz informacje te nie zostały zaprezentowane w sposób transparentny. DPC zaproponował wobec tego nałożenie kary pieniężnej.

EROD nakazał DPC przeprowadzenie dalszego postępowania wyjaśniającego w celu stwierdzenia, czy doszło do przetwarzania danych szczególnej kategorii i czy przetwarzano je zgodnie z prawem. EROD uznał, że brak jasnych i pełnych informacji przekazywanych przez administratora w odniesieniu do użytkowników jego usług, w połączeniu z sytuacją, w której użytkownicy usług na mogą jedynie zgodzić się na warunki stawiane przez administratora, albo muszą przestać z nich korzystać, z powodu braku alternatywnych usług na rynku oraz braku możliwości modyfikowania umowy, systematycznie stawia użytkowników tych usług w niekorzystnej sytuacji, ogranicza ich kontrolę nad przetwarzaniem ich danych osobowych i podważa możliwość wykonywania ich praw na mocy rozdziału III RODO. EROD nakazał DPC stwierdzenie naruszenia zasady przejrzystości oraz dodanie nakazu dostosowania operacji przetwarzania dokonywanych w celu wykorzystania reklam behawioralnych w kontekście świadczenia usług, do wymogów art. 6 ust. 1 RODO. EROD nakazał DPC również zmianę nakazu dostosowania polityki i warunków świadczenia usług administratora do zgodności z art. 5 ust. 1 lit. a), art. 12 ust. 1 i art. 13 ust. 1 lit. c) RODO, aby nie odnosiły się one wyłącznie do informacji na temat danych przetwarzanych na podstawie art. 6 ust. 1 lit. b) RODO, ale również do danych przetwarzanych do celów reklamy behawioralnej. EROD nakazał również DPC nałożenie na administratora dodatkowej kary za naruszenie

art. 6 ust. 1 RODO i uwzględnienie naruszenia art. 5 ust. 1 lit. a) RODO.

DPC w przypadku WhatsAppa uznał, że administrator nie dążył do przetwarzania danych osobowych użytkowników w oparciu o zgodę na warunki świadczenia usługi jak i nie był zobowiązany do oparcia takiego przetwarzania na zgodzie. DPC wskazał, że co do zasady przetwarzanie w celu dostarczania nowych usług lub zapobiegania oszustwom nie byłoby konieczne do wykonania umowy o usługi online, jednakże w tym konkretnym przypadku, biorąc pod uwagę szczególne warunki umowy oraz charakter usługi świadczonej i uzgodnionej przez strony, administrator może opierać się na art. 6 ust. 1 lit. b) RODO. W odniesieniu do zgodności z art. 12 ust. 1 i art. 13 ust. 1 lit. c) RODO w kontekście przetwarzania prowadzonego na podstawie art. 6 ust. 1 lit. b) RODO, DPC stwierdził już w przeprowadzonym wcześniej postępowaniu z urzędu, że administrator naruszył w tym względzie przepisy RODO.

EROD uznał, że przetwarzanie danych przez administratora w celu ulepszenia usługi i zwiększenia bezpieczeństwa nie jest obiektywnie niezbędne dla świadczenia jego usług i nie może zostać ono uznane za niezbędny element domniemanej umowy łączącej administratora z jego użytkownikami, bez którego umowa ta nie może zostać wykonana. EROD nakazał DPC stwierdzenie, że administrator niesłusznie opierał się na art. 6 ust. 1 lit. b) RODO dla przetwarzania objętego skargą i zobligował DPC do dodania do decyzji nakazu dostosowania operacji przetwarzania danych objętych skargą do art. 6 ust. 1 RODO. EROD nakazał również DPC stwierdzenie naruszenia zasady przejrzystości i zastosowanie wobec tego odpowiednich uprawnień naprawczych. EROD nakazał również DPC przeprowadzenie postępowania wyjaśniającego dotyczącego możliwego przetwarzania danych wrażliwych przez administratora w celach reklamy behawioralnej, celach marketingowych oraz przekazywania danych metrycznych podmiotom trzecim. EROD nakazał również DPC nałożenie na administratora administracyjnej kary pieniężnej za naruszenie art. 6 ust. 1 RODO oraz art. 5 ust. 1 lit. a) RODO.

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

Współpraca z innymi europejskimi organami ochrony danych i EROD w sprawie praktyk spółki Vinted UAB

Grupa robocza składająca się z organów nadzorczych z Francji, Holandii, Litwy i Polski, wspierana przez Europejską Radę Ochrony Danych (EROD), rozpatrzyła szereg skarg dotyczących potencjalnych naruszeń ogólnego rozporządzenia o ochronie danych przez Vinted UAB, operatora serwisu sprzedażowego odzieży Vinted.com.

Organy nadzorcze z Francji, Holandii, Litwy i Polski badali kwestie związane m.in.

z przejrzystym informowaniem, przechowywaniem danych związanych z wypłatą środków czy realizacją praw osób, których dane dotyczą. Praca koncentrowała się również na ochronie danych osobowych w kontekście przetwarzania związanego z blokowaniem kont użytkowników.

W związku z otrzymaniem znacznej liczby skarg dotyczących serwisu sprzedażowego ubrań on-line vinted.com prowadzonego przez litewską spółkę Vinted UAB, organy nadzorcze z Francji, Litwy i Polski podjęły współpracę w celu zbadania zgodności tej strony z przepisami RODO. Po utworzeniu grupy roboczej w jej prace zaangażował się również holenderski organ nadzorczy.

Zaangażowanie i ścisła współpraca organów nadzorczych w toczących się postępowaniach w związku z działalnością Vinted UAB, zaowocowały dokumentem roboczym, który jest w trakcie harmonizacji i posłuży do oceny skarg przeciwko Vinted UAB. Zaangażowanie organów nadzorczych w prace grupy roboczej do spraw Vinted jest przykładem ścisłej współpracy w zakresie egzekwowania prawa – strategicznego priorytetu dla EROD. Członkowie EROD, na spotkaniu, które odbyło się w Wiedniu 27–28 kwietnia 2022 r., uzgodnili dalsze zacieśnianie współpracy w sprawach strategicznych oraz zróżnicowanie zakresu stosowanych metod współpracy. Dzięki zaangażowaniu innych organów, litewski organ nadzorczy uzyskał wsparcie merytoryczne i zasoby ludzkie. Organy pracują nieformalnie, aby pomóc litewskiemu organowi nadzorczemu w wydaniu projektów decyzji dotyczącej zarówno zasad, jak i konkretnych przypadków w oficjalnej procedurze *one-stop-shop*[94]. Mając za przykład grupę roboczą powołaną do spraw Vinted, EROD zgodziła się na częstsze korzystanie z tej formy współpracy w przyszłości.

Wiążąca decyzja EROD w sprawie sporu dotyczącego projektu decyzji CNIL (Commission Nationale de l'Informatique et des Libertés – francuski organ nadzorczy) w sprawie Accor SA[95]

Na posiedzeniu plenarnym 15 czerwca 2022 r. Europejska Rada Ochrony Danych przyjęła wiążącą decyzję w sprawie rozstrzygnięcia sporu dotyczącego projektu decyzji francuskiego organu nadzorczego w sprawie Accor SA na podstawie art. 65 RODO. Konieczność przyjęcia przez EROD wiążącej decyzji wynikała z faktu nieprzychylenia się przez CNIL do mającego znaczenie dla sprawy i uzasadnionego sprzeciwu zgłoszonego przez Prezesa UODO wobec projektu decyzji przedłożonego przez CNIL.

Sprawa dotyczyła spółki Accor SA, specjalizującej się w sektorze hotelarskim, której główna jednostka organizacyjna znajduje się we Francji. Wiodący organ nadzorczy – CNIL – przedłożył projekt decyzji, po przeprowadzeniu postępowania skargowego w sprawie Accor SA, dotyczącego nieuwzględnienia prawa do sprzeciwu wobec otrzymywania wiadomości marketingowych drogą pocztową i/lub trudności napotkanych podczas wykonywania prawa

94 więcej informacji na temat mechanizmu kompleksowej współpracy (one-stop-shop) dostępnych jest na stronie EROD pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/one-stop-shop-leaflet_pl
95 ZSPR.440.1627.2019.

dostępu. Jedna ze skarg, których to postępowanie dotyczyło, pochodziła z Polski.

Pod koniec kwietnia 2021 r. CNIL udostępnił swój projekt decyzji innym organom nadzorczym, których sprawa dotyczyła, zgodnie z mechanizmem współpracy wynikającym z RODO. Prezes UODO, działając w charakterze organu nadzorczego, którego sprawa dotyczyła, zgłosił sprzeciwy, zgodnie z art. 60 ust. 4 RODO, dotyczące m.in. wysokości administracyjnej kary pieniężnej. Organy nadzorcze nie były w stanie osiągnąć porozumienia w sprawie jednego ze sprzeciwów, który następnie został przekazany przez CNIL do EROD w celu jego rozpatrzenia zgodnie z procedurą rozstrzygania sporów na podstawie art. 65 ust. 1 lit. a RODO.

EROD przyjęła w tej sprawie wiążącą decyzję odnoszącą się do meritum tej części sprzeciwu, którą uznano za mającą znaczenie dla sprawy i uzasadnioną, zgodnie z wymogami art. 4 pkt 24 RODO. EROD zdecydowała, że CNIL musi wziąć pod uwagę obrót Accor SA z poprzedniego roku (2021), fakt, że sprawa dotyczy „istotnych" naruszeń, a kara administracyjna nie ma charakteru odstraszającego zgodnie z art. 83 ust. 1 RODO. Z tego powodu EROD poleciła CNIL-owi ponowną ocenę tych elementów przy ustalaniu wysokości kary pieniężnej.

EROD zauważyła, że CNIL nie musi wykazywać wpływu kary na rentowność Accor SA i nie ma potrzeby uznawania spadku obrotów za okoliczność łagodzącą w rozumieniu art. 83 ust. 2 lit. k) RODO. Dzięki temu okoliczności uwzględnione przy obliczaniu kary administracyjnej nie będą liczone podwójnie.

Po dokonaniu oceny EROD poleciła CNIL-owi ponowne oszacowanie przewidywanej kary Accor zgodnie z wnioskami Rady. CNIL w ostatecznej decyzji nałożył na Accor SA administracyjną karę pieniężną w wysokości 5-krotnie wyższej od zaproponowanej pierwotnie w projekcie decyzji.

4.2. Zawiadomienie o podejrzeniu popełnienia przestępstwa

W omawianym okresie sprawozdawczym skierowano, na podstawie art. 304 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego[96], zawiadomienie o podejrzeniu popełnienia przestępstwa polegającego na znieważeniu Prezesa UODO jako funkcjonariusza publicznego z powodu wykonywanego przez niego zawodu lub zajmowanego stanowiska, tj. przestępstwa określonego w art. 226 § 1 w związku z art. 231a ustawy z dnia 6 czerwca 1997 r. Kodeks karny[97].

W zawiadomieniu wskazano, że do Urzędu Ochrony Danych Osobowych, wpłynęło pismo, w którym jego autor, odnosząc się do Prezesa UODO za pomocą słów uznawanych powszechnie za obraźliwe, wyraził swoje niezadowolenie z obowiązywania i przestrzegania RODO w Polsce, funkcjonowania UODO oraz pracy inspektorów ochrony danych osobowych i nadzoru nad nimi. Ponadto w treści ww. pisma autor zarzucił

96 Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2022 r. poz. 1375 z późn. zm.), dalej: „k.p.k."
97 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2022 r. poz. 1138 z późn. zm.), dalej: „k.k.".

Prezesowi UODO nadużywanie władzy poprzez „[…] brak nadzoru nad inspektorami odo i ślepe posłuszeństwo niepisanym zasadom i wadliwym ustawom/rozporządzeniom […]". W uzasadnieniu zawiadomienia wskazano, że działanie autora pisma niewątpliwie wypełnia stronę przedmiotową przestępstwa znieważenia funkcjonariusza publicznego, którym jest Prezes UODO, określonego w art. 226 § 1 k.k. w związku z art. 231a k.k. Zgodnie bowiem z art. 226 § 1 k.k., kto znieważa funkcjonariusza publicznego lub osobę do pomocy mu przybraną, podczas i w związku z pełnieniem obowiązków służbowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Z kolei zgodnie z art. 231a k.k., z ochrony prawnej przewidzianej dla funkcjonariuszy publicznych podczas lub w związku z pełnieniem obowiązków służbowych, funkcjonariusz publiczny korzysta również wtedy, jeżeli bezprawny zamach na jego osobę został podjęty z powodu wykonywanego przez niego zawodu lub zajmowanego stanowiska. Art. 231a rozszerza ochronę funkcjonariuszy publicznych na sytuacje, kiedy zamach na nich nie miał miejsca podczas lub w związku z pełnieniem obowiązków służbowych, tj. nastąpił bez związku z konkretnymi czynnościami lub sprawą, lecz motywacją dla zamachu był wykonywany przez funkcjonariusza zawód[98]. Komentowany przepis – materialnie rzecz ujmując – zawiera wyciągnięte przed nawias znamiona modalizujące „z powodu wykonywanego przez niego zawodu lub zajmowanego stanowiska", o które należy uzupełnić każdy typ czynu zabronionego penalizujący zachowanie skierowane przeciwko funkcjonariuszowi publicznemu „podczas lub w związku z pełnieniem obowiązków służbowych". Są to znamiona określające motywy działania sprawcy (strona podmiotowa)[99].

Wskazano, że obecnie judykatura jednolicie przyjmuje, że znieważenie funkcjonariusza publicznego może nastąpić zarówno publicznie, jak i niepublicznie, bowiem do znamion przestępstwa określonego w art. 226 § 1 k.k. nie należy publiczne działanie sprawcy. Dobrem chronionym na gruncie tego przepisu jest przede wszystkim autorytet organów władzy publicznej oraz porządek publiczny[100]. Przedmiotem czynności wykonawczej jest „funkcjonariusz publiczny". Zgodnie z art. 115 § 13 k.k., funkcjonariuszem publicznym jest osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych (pkt 4), a także osoba zajmująca kierownicze stanowisko w innej instytucji państwowej (pkt 6). Zważywszy na definicję z art. 115 § 13 k.k., stwierdzić należy, iż Prezes UODO w kontekście powołanego wyżej art. 43 ust. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz art. 45 ust. 1 i 3 tej ustawy, niewątpliwie jest funkcjonariuszem publicznym. Działanie zaś autora pisma, który przy użyciu słów powszechnie uznawanych za obelżywe i wulgarne w sposób agresywny zarzuca Prezesowi UODO niewłaściwe wykonywanie obowiązków służbowych, niewłaściwe stosowanie przepisów i przekraczanie uprawnień (nadużywanie władzy), a także pomawia o popełnienie przestępstw, niewątpliwie godzi w powagę UODO oraz zakłóca porządek

98 A. Lach [w:] *Kodeks karny. Komentarz, wyd. III*, red. V. Konarska-Wrzosek, Warszawa 2020, art. 231(a), LEX/el. 2020.
99 A. Barczak-Oplustil [w:] *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k., wyd. IV*, red. A. Zoll, Warszawa 2013, art. 231(a), LEX/el. 2013.
100 por. Czarny-Drożdżejko Elżbieta, *Przestępstwa prasowe*, LEX/el. 2013.

publiczny i tym samym wypełnia dyspozycję przepisu art. 226 § 1 k.k.w. związku z art. 231a k.k.

Z uwagi na to, iż ww. pismo skierowane zostało bezpośrednio do UODO i odnosi się w nim do wykonywanych przez Prezesa UODO obowiązków oraz sposobu nadanej przez niego statutem organizacji UODO, nie budzi wątpliwości, iż zamach na funkcjonariusza publicznego pozostawał w ścisłej korelacji z zajmowanym przez niego stanowiskiem. Podkreślenia bowiem wymaga, iż Prezes UODO wykonuje swoje funkcje przy pomocy zorganizowanego zespołu osób oraz środków rzeczowych i finansowych w postaci UODO w sposób całkowicie niezależny. Zgodnie z art. 52 ust. 5 RODO, każde państwo członkowskie zapewnia, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego. Działanie autora pisma godzi w autorytet i prestiż Prezesa UODO jako jedynego w kraju organu do spraw ochrony danych osobowych, mającego umocowanie do działania w prawie krajowym i unijnym oraz kwestionuje jego niezależność, znieważając go jako osobę kierującą tą instytucją. Brak reakcji Prezesa UODO na opisane zachowanie sprawcze mógłby skutkować intensyfikacją podobnych działań ze strony ww. osoby, a także wywołać u niej poczucie bezkarności, jak i niejako przyzwolenia na takie zachowanie, co w demokratycznym państwie prawa nie może mieć miejsca.

Zgodnie z art. 304 § 2 k.p.a., instytucje państwowe i samorządowe, które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa.

4.3. Skargi na działanie UODO

W 2022 r. do Urzędu Ochrony Danych Osobowych wpłynęło **28** skarg na działanie Urzędu. Przeważnie skargi składane były w toku prowadzonych postępowań i dotyczyły przewlekłego załatwiania spraw lub domniemanej bezczynności Prezesa UODO.

5. Kontrola przestrzegania przepisów o ochronie danych osobowych

Celem czynności kontrolnych jest ustalenie, czy jednostka kontrolowana przetwarza dane zgodnie z przepisami o ochronie danych osobowych. Szerokie uprawnienia kontrolerów UODO zostały odrębnie uregulowane w rozdziale 9 ustawy z 10 maja 2018 r. o ochronie danych osobowych. Kontrolę prowadzi się zgodnie z zatwierdzonym przez Prezesa UODO planem kontroli lub na podstawie uzyskanych przez niego informacji lub w ramach monitorowania przestrzegania stosowania przepisów RODO.

W okresie od 1 stycznia do 31 grudnia 2022 r. Prezes UODO przeprowadzał czynności kontrolne w zakresie przestrzegania przepisów dotyczących ochrony danych

osobowych **w czterdziestu podmiotach.** Wymienione działania były realizowane na podstawie art. 58 RODO. Kontrole były przeprowadzane zarówno w oparciu o przyjęty plan kontroli, jak i w rezultacie powzięcia przez Prezesa UODO informacji o występujących nieprawidłowościach w związku z przetwarzaniem danych osobowych, a także w wyniku zgłoszenia naruszeń ochrony danych.

Zgodnie z planem kontroli sektorowych UODO na 2022 r. czynnościami kontrolnymi zostały objęte:

- podmioty, które przetwarzają dane osobowe przy użyciu mobilnych aplikacji;
- banki – w zakresie profilowania danych osobowych klientów i potencjalnych klientów oraz sposobu informowania osób ubiegających się o kredyt o dokonanej ocenie kredytowej[101];
- organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym – w zakresie przetwarzania danych osobowych SIS/VIS dostępnych poprzez KSI (Krajowy System Informatyczny) lub bezpośrednio w SISII/VIS na podstawie przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym[102].

W 2022 r. UODO przeprowadził kontrole przestrzegania przepisów dotyczących ochrony danych osobowych w takich podmiotach, jak: organy administracji rządowej i administracji samorządowej, uczelniach wyższych, stowarzyszeniu, w bankach i placówkach medycznych oraz w konsulacie RP.

5.1. Aplikacje mobilne

Zgodnie z przyjętym planem kontroli sektorowych na 2022 r., który zakładał kontrolę przetwarzania danych osobowych przy użyciu mobilnych aplikacji, czynnościami kontrolnymi objęto **trzynaście podmiotów**. Jednostki, w których UODO przeprowadził kontrole, reprezentowały różne branże, tj.: medyczną, bankową, handlową, gastronomiczną, turystyczną, transportową, a także administrację rządową. Kontrole aplikacji mobilnych będą kontynuowane w kolejnym roku.

5.2. Profilowanie

Kontrole sektorowe obejmowały sprawdzenie procesu przetwarzania przez banki danych osobowych klientów i potencjalnych klientów w związku z profilowaniem danych. Kontrole miały na celu zweryfikowanie zgodności przetwarzania danych osobowych

101 W związku z art. 70a Prawa a bankowego.
102 Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (t.j. Dz. U. z 2021 r. poz. 1041 z późn. zm.), dalej: „ustawa o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym".

z przepisami o ochronie danych osobowych. Wyniki kontroli wykazały, że banki w celu oceny zdolności kredytowej i analizy ryzyka kredytowego wielokrotnie podejmowały decyzje oparte na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Jak ustalono, w bankach, w których dokonywano profilowania klientów, działanie to odbywało się z zachowaniem wymogów wskazanych w art. 105a ust.1a-1c Prawa bankowego. Zgodnie z tym przepisem, banki mogą w celu oceny zdolności kredytowej i analizy ryzyka kredytowego podejmować decyzje, opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, danych osobowych – również stanowiących tajemnicę bankową – pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień, co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska. Decyzje te mogą być podejmowane wyłącznie na podstawie danych niezbędnych z uwagi na cel i rodzaj kredytu, w szczególności w oparciu o kategorie danych wskazane w art. 105a ust. 1b prawa bankowego.

W wyniku przeprowadzonych w bankach kontroli stwierdzono również, że niektóre z nich nie dokonywały zautomatyzowanego podejmowania decyzji, o których mowa w art. 22 RODO.

Podsumowując, w omawianym okresie sprawozdawczym przeprowadzono **siedem kontroli** w powyższym zakresie i na podstawie dokonanych ustaleń nie stwierdzono naruszenia przepisów o ochronie danych osobowych, które stanowiłyby podstawę do zastosowania art. 90 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, tj. wszczęcia postępowania w sprawie naruszenia, o którym mowa w art. 60 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

5.3. System Informacyjny Schengen, Wizowy System Informacyjny

Kontrolami przetwarzania danych osobowych przez organy przetwarzające w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym, objęto dokonywane przez Służbę Ochrony Państwa operacje przetwarzania danych, prowadzone w związku z bezpośrednim oraz pośrednim dostępem do Krajowego Systemu Informatycznego w celu wglądu do wpisów w SIS oraz VIS. Zakres tych informacji uległ zmianie po nowelizacji z grudnia 2022 r. ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, która zmieniła upoważnienia tej formacji i zakres danych do wskazanych systemów.

Druga kontrola dotyczyła danych osobowych przetwarzanych w Konsulacie Generalnym Rzeczypospolitej Polskiej w Stambule w związku z dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów danych VIS oraz wglądu do danych VIS i danych SIS. Konsulom przysługuje uprawnienie do bezpośredniego wglądu do Wizowego Systemu Informacyjnego w celu dokonania wglądu do danych VIS w związku z rozpatrywaniem złożonych przez cudzoziemców wniosków wizowych i wydawaniem decyzji dotyczących tych wniosków.

Dodatkowo konsulom przysługuje:

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

W trakcie kontroli szczególną uwagę poświęcono operacjom przetwarzania danych osób ubiegających się o wydanie wizy w punktach przyjmowania wniosków wizowych prowadzonych przez podmiot zewnętrzny, z którym Konsulat Generalny RP w Stambule współpracuje na podstawie umowy.

W związku z pracami Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS) Prezes Urzędu skierował do Wojewody Mazowieckiego, Wojewody Małopolskiego, Wojewody Dolnośląskiego oraz Ministerstwa Spraw Zagranicznych pisma z zapytaniem dotyczącym wcześniejszego usuwania danych z Wizowego Systemu Informacyjnego w związku z uzyskaniem obywatelstwa państwa członkowskiego Unii Europejskiej przez osobę, która wnioskowała o wizę, na podstawie art. 25 rozporządzenia 767/2008.

W efekcie pozyskanych informacji została przeprowadzona kontrola w Mazowieckim Urzędzie Wojewódzkim obejmująca swym zakresem przetwarzanie danych osobowych w związku z bezpośrednim dostępem do Krajowego Systemu Informatycznego w celu dokonywania wpisów do Wizowego Systemu Informacyjnego. W wyniku kontroli Prezes Urzędu Ochrony Danych Osobowych skierował do Ministra Spraw Wewnętrznych i Administracji pismo z wnioskiem o zbadanie tego zagadnienia w ramach nadzoru nad wojewodami celem zapewnienia skutecznej realizacji obowiązków nałożonych na mocy rozporządzenia w sprawie VIS na państwa członkowskie.

5.4. Inspektor Ochrony Danych

W 2022 r. Prezes Urzędu Ochrony Danych Osobowych podjął działania mające na celu sprawdzenie prawidłowości powołania i funkcjonowania inspektorów ochrony danych (IOD) i w tym celu kontrolą objęto **cztery podmioty**. Ponadto skierowano dwadzieścia cztery pisma do administratorów danych, którzy wyznaczyli IOD, w sprawie pozyskania informacji dot. realizacji obowiązku publikowania informacji o wyznaczonym IOD, w jaki sposób zapewniony jest kontakt z taką osobą, komu podlega w strukturze administracyjnej, jakie ma kompetencje i czy ta osoba ma zapewnione zasoby do utrzymania fachowej wiedzy. Ponadto kontrolerzy UODO sprawdzali, w jaki sposób administratorzy angażują IOD we wszystkie

sprawy dotyczące ochrony danych osobowych, jak zapewniane są gwarancje niezależności i możliwość prawidłowego realizowania obowiązków IOD-a, jak wygląda w danej organizacji współpraca administratora z IOD-em i czy jego praca jest w jakiś sposób kontrolowana.

W trakcie postępowań stwierdzono szereg nieprawidłowości dotyczących powołania i funkcjonowania inspektorów ochrony danych u administratorów, wobec których były prowadzone czynności kontrolne. Wspomniane uchybienia dotyczyły takich kwestii jak np. niewłaściwe włączanie inspektora ochrony danych w sprawy dotyczące ochrony danych osobowych, niepodejmowanie działań mających na celu zapewnienie inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej, brak procedur zapewniających niezależność inspektora ochrony danych, w szczególności dotyczących zakazu otrzymywania instrukcji, wydawania poleceń, jak również zapewnienia, że w ramach wykonywania zadań inspektora ochrony danych nie będzie on odwoływany ani karany, jak również wykonywanie przez inspektorów ochrony danych zadań, które z mocy prawa należą do wyłącznych zadań administratorów, jak np. prowadzenie rejestru czynności przetwarzania, czy rejestru naruszeń ochrony danych osobowych.

5.5. Kontrole w wyniku zgłoszonego naruszenia

W 2022 r. Prezes UODO przeprowadził **osiem postępowań kontrolnych w związku ze zgłoszonym przez administratora naruszeniem ochrony danych.**

W związku ze zgłoszeniem naruszenia przepisów ochrony danych osobowych dokonanym przez administratora danych **spółki świadczącej usługi marketingowe,** przeprowadzona została kontrola tego podmiotu. Zgłoszone naruszenie polegało na nieuprawnionym przesyłaniu przez podmiot przetwarzający baz danych do innych podmiotów w grupie kapitałowej (o czym administrator nie został poinformowany) i handlu tymi bazami danych. Materiał dowodowy zebrany w toku przedmiotowej kontroli nie potwierdził, żeby kontrolowany podmiot przekazywał bazy danych innym podmiotom w grupie kapitałowej oraz podmiotom za granicą.

Prezes UODO postanowił o skontrolowaniu dwóch podmiotów z uwagi na zgłoszone przez administratora danych naruszenie ochrony danych osobowych, którego wystąpienie miało związek z **usługą informatyczną**, polegającą na realizacji działań wymaganych do uruchomienia sklepu internetowego świadczoną na jego rzecz przez podmiot przetwarzający. Celem kontroli była weryfikacja, czy ww. podmioty wdrożyły odpowiednie środki techniczne i organizacyjne dotyczące funkcjonowania systemu informatycznego związanego z naruszeniem, aby przetwarzanie danych osobowych odbywało się zgodnie z przepisami RODO oraz z uwzględnieniem charakteru, zakresu, kontekstu, celów przetwarzania i ryzyka naruszenia praw i wolności osób fizycznych, a także czy środki te są w razie potrzeby poddawane przeglądom i uaktualniane[103]. W toku czynności kontrolnych wykazano szereg naruszeń przepisów RODO, związanych głównie z brakami w dokumentacji wymaganej od

103 Art. 32 i art. 24 RODO.

administratora oraz podmiotu przetwarzającego. U obu podmiotów stwierdzono przypadki nieopracowania i niewdrożenia kluczowych dla ochrony danych osobowych środków organizacyjnych, takich jak: polityka ochrony danych, rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania, dokument z opisem oceny skutków przetwarzania danych oraz analizy ryzyka, itp. W związku z powyższym wszczęto wobec obu kontrolowanych podmiotów postępowania administracyjne, w przedmiocie naruszenia przepisów RODO.

Kontrolą wszczętą w związku ze zgłoszeniem naruszenia ochrony danych osobowych objęto również przetwarzanie danych osobowych przez spółkę prowadzącą **sklep internetowy.** Naruszenie, którego dotyczyło przedmiotowe zgłoszenie, polegało na przełamaniu zabezpieczeń tego sklepu. W toku kontroli ustalono, że naruszenie powstało na skutek ataku hakerskiego, którego celem było wyłudzenie od administratora danych określonych korzyści (tj. uzyskania określonej kwoty) i że na skutek naruszenia przełamane zostały zabezpieczenia techniczne, a nie organizacyjne. Zaszyfrowanie danych dotyczyło jednego serwera, a nie całej infrastruktury informatycznej spółki. Baza danych klientów objętych naruszeniem została przywrócona z kopii zapasowej. Do spółki nie wpłynęły żadne sygnały (zarówno od samych klientów, kontrahentów, pracowników, jak i od osób trzecich), z których wynikałoby, że dane osobowe objęte naruszeniem zostały ujawnione. Ocena materiału pozyskanego w toku kontroli pozwoliła na stwierdzenie, że administrator danych podjął działania mające na celu zminimalizowanie ryzyka ponownego wystąpienia naruszenia m.in. poprzez zidentyfikowanie miejsca, przez które osoba nieupoważniona zdobyła dostęp, wymuszenie zmiany haseł dostępu do panelu dla wszystkich użytkowników, zastosowanie dodatkowej podwójnej autoryzacji przy logowaniu do panelu użytkownika, wpisanie adresów IP, z których nastąpił atak na tzw. czarną listę oraz wdrożenie dodatkowych zabezpieczeń przed atakami mającymi na celu złamanie zabezpieczeń. Ponadto administrator zawiadomił w sposób prawidłowy osoby, których dane dotyczą, o naruszeniu ich danych osobowych. W świetle dokonanych ustaleń brak było podstaw do wszczęcia postępowania administracyjnego.

Prezes UODO przeprowadził postępowanie wyjaśniające, a następnie czynności kontrolne w komendzie miejskiej policji (dalej jako KMP) w związku z otrzymanym zgłoszeniem naruszenia ochrony danych osobowych, które polegało na przekazaniu osobom nieuprawnionym danych osobowych przetwarzanych w systemach informatycznych policji. Przedmiotem kontroli było dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Kontrolą zostało objęte zabezpieczanie przez komendanta miejskiego policji danych osobowych w związku z ustawową realizacją zadań policji (z wyłączeniem danych pracowników oraz funkcjonariuszy).

W wyniku czynności kontrolnych w KMP został zgromadzony materiał dowodowy, który następnie Prezes Urzędu ocenił w zakresie zgodności z przepisami o ochronie danych osobowych. W rezultacie organ nadzorczy zdecydował o wszczęciu postępowania administracyjnego z urzędu w związku z szeregiem stwierdzonych naruszeń.

Prezes Urzędu stwierdził uchybienia, m.in. w zakresie:

1) **konfliktu interesów,** który wynikał:

   a) z nadmiaru obowiązków osoby pełniącej funkcję IOD i funkcję Naczelnika Wydziału ds. Ochrony Informacji Niejawnych – OIN;

   b) z uwagi na łączenie funkcji dochodziło do sytuacji, w której IOD uczestniczył w procesie nadawania upoważnień, a nie tylko monitorował ten proces;

   c) łączeniu funkcji IOD z funkcją Naczelnika Wydziału i tym samym monitorowaniu przez IOD sposobów i celów przetwarzania danych, o których decydował Naczelnik Wydziału ds. Ochrony Informacji Niejawnych, przez jedną osobę. Dochodziło do sytuacji, w której sam nadzorował swoje działania (co prowadzi do naruszenia przepisów prawa);

2) **braku realizacji zadań administratora danych:**

   a) niewłączanie przez administratora danych IOD we wszystkie zachodzące w jednostce procesy przetwarzania danych osobowych;

   b) administrator danych nie udzielał właściwego wsparcia dla IDO, które przejawiało się brakiem:

   ✓ włączania IOD we wszystkie procesy dotyczące przetwarzania danych osobowych;

   ✓ przydzielenia osoby wspierającej IOD w realizacji jego zadań – pomimo takiego wniosku IOD;

   ✓ szkoleń IOD z zakresu ochrony danych osobowych w szczególności z zakresu identyfikowania naruszeń, postępowania z nimi, przeprowadzania analizy ryzyka, a także analizy ryzyka naruszenia praw lub wolności osób fizycznych objętych naruszeniem;

   ✓ wsparcia IOD ze strony administratora danych osobowych, co spowodowało, iż wielokrotnie monitował konieczność nadania upoważnień do przetwarzania danych – po upływie 11 miesięcy od pierwszego pisma informującego o takiej konieczności otrzymał od jednego z Naczelników wykaz upoważnień, a po 8 miesiącach od terminu wskazanego w art. 103 ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;

   c) niedopełnienie obowiązków administratora w związku z naruszeniem ochrony danych:

   ✓ niezgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu;

   ✓ brak wykonania analizy ryzyka naruszenia praw lub wolności osób objętych tym naruszeniem;

- ✓ niezawiadomienie osób fizycznych w związku z przedmiotowym naruszeniem, ani nie wykazanie, iż z tego obowiązku jest administrator zwolniony;

d) niewypełnienie analizy ryzyka w związku z naruszeniem polegającym na pozyskiwaniu danych osobowych z policyjnej bazy danych – w związku z tym naruszeniem organ stwierdził także brak kontroli administratora danych nad procesem pozyskiwania danych osobowych z baz policyjnych;

e) brak kontroli nad sposobem korzystania z nośników danych;

f) nieprawidłowości w zakresie prowadzonej dokumentacji przez administratora danych:

- ✓ brak udokumentowania wykonania analizy ryzyka;
- ✓ braku konfliktu interesów IOD a innymi jego funkcjami w KMP;
- ✓ brak przejrzystości w prowadzonych u administratora danych szacowaniach ryzyka,
- ✓ brak polityki ochrony danych osobowych;
- ✓ brak procedury dot. identyfikacji i zgłaszania naruszeń ochrony danych osobowych;

g) nieprawidłowości w zakresie upoważnień do przetwarzania danych osobowych.

5.6. Decyzje administracyjne w postępowaniach kontrolnych

W 2022 r. Prezes UODO, po przeprowadzeniu postępowań administracyjnych dotyczących przetwarzania danych osobowych, wydał trzy (3) decyzje, w których nałożył na administratorów danych osobowych administracyjne kary pieniężne.

Przykłady decyzji nakładających administracyjną karę pieniężną administratorowi danych po przeprowadzeniu postępowania kontrolnego w przedmiocie przetwarzania danych osobowych, zostały przedstawione w rozdz. 9 niniejszego Sprawozdania.

6. Egzekucja administracyjna – zapewnienie wykonania decyzji

Prezes Urzędu Ochrony Danych Osobowych, na podstawie art. 1a pkt 13 w zw. z art. 2 § 1 pkt 12 oraz art. 20 § 2 ustawy o postępowaniu egzekucyjnym w administracji[104], jest wierzycielem i organem egzekucyjnym w odniesieniu do egzekucji obowiązków o charakterze niepieniężnym z zakresu ochrony danych osobowych. Dzięki temu Prezes UODO może prowadzić czynności mające na celu zapewnienie wykonania przez zobowiązanych obowiązków z zakresu ochrony danych osobowych nakładanych w drodze decyzji administracyjnych. Ponadto Prezes UODO jest wierzycielem w zakresie egzekucji należności pieniężnych (w szczególności administracyjnych kar pieniężnych, grzywien,

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

kosztów upomnienia, kosztów egzekucyjnych, grzywien w celu przymuszenia, opłat za certyfikację oraz naliczonych od tych należności odsetek za zwłokę). Organem egzekucyjnym w zakresie egzekucji pieniężnych jest naczelnik właściwego urzędu skarbowego.

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

a) **ostateczne decyzje** nakładające na administratora lub podmiot przetwarzający (zobowiązanego) **obowiązek z zakresu ochrony danych osobowych mający charakter niepieniężny** (decyzje zawierające tzw. nakaz). Decyzje te co do zasady stają się wykonalne z dniem ich doręczenia stronie (niezależnie od ich ewentualnego zaskarżenia do sądu administracyjnego)[105]. Jeżeli decyzja administracyjna zawiera postanowienia dodatkowe określające termin jej wykonania, to obowiązek z niej wynikający podlega wykonaniu i w razie potrzeby egzekucji administracyjnej dopiero po upływie tego terminu. Obowiązek niepieniężny nakładany na zobowiązanego może polegać w szczególności na: usunięciu uchybień w procesie przetwarzania danych osobowych, spełnieniu żądania osoby, której dane dotyczą (odnoszącego się do jej praw wynikających z przepisów o ochronie danych osobowych), wprowadzeniu czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania danych, zawieszeniu przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej, czy wreszcie zawiadomieniu osoby, której dane dotyczą o naruszeniu ochrony jej danych osobowych;

b) **prawomocne decyzje nakładające administracyjne kary pieniężne**. Zaskarżenie do sądu administracyjnego takiej decyzji wstrzymuje jej wykonanie i tym samym możliwość wszczęcia egzekucji administracyjnej[106]. Prezes UODO ma prawo nałożyć na podmiot prywatny administracyjną karę pieniężną w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego obrotu, w zależności od tego, która kwota jest wyższa. Natomiast na jednostki sektora finansów publicznych (z wyjątkiem państwowych i samorządowych instytucji kultury), instytuty badawcze i Narodowy Bank Polski, Prezes UODO może nałożyć karę w wysokości do 100 000 zł. Wspomniane wyżej instytucje kultury mogą być ukarane karą do 10 000 zł.

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

Postępowanie prowadzone w Urzędzie, którego ostatecznym efektem ma być stwierdzenie wykonania decyzji Prezesa UODO lub – w razie potrzeby – wyegzekwowanie

105 Art. 61 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi, Dz. U. z 2023 r. poz. 259.
106 Art. 74 ustawy z 10 maja 2018 r. o ochronie danych osobowych, Dz. U. z 2019 r. poz. 1781.

jej wykonania od zobowiązanego podmiotu, jest kilkuetapowe i odmienne w zależności od tego czy egzekwowany obowiązek ma charakter pieniężny (administracyjna kara pieniężna, grzywna w celu przymuszenia, itp.) czy niepieniężny (nakaz).

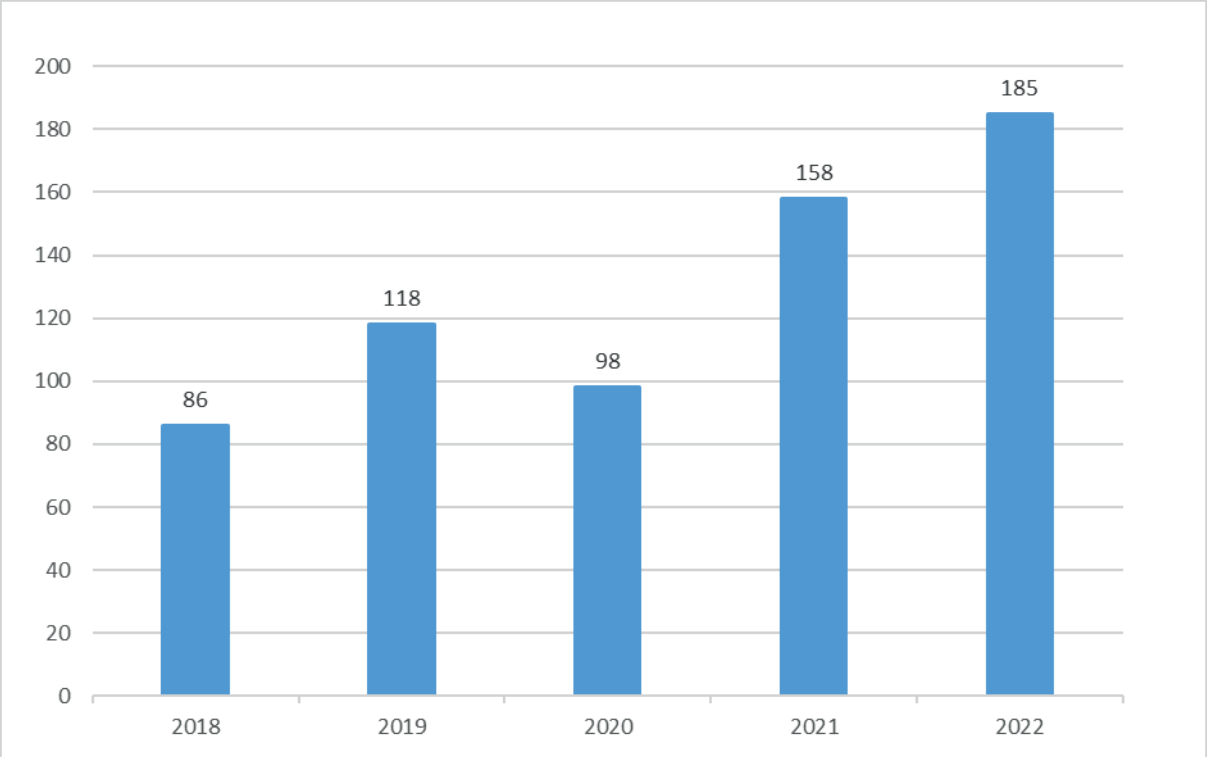
Pierwszym etapem postępowania prowadzonego w UODO, wspólnym dla postępowań dotyczących decyzji nakładających oba rodzaje obowiązków, jest **postępowanie sprawdzające** wykonanie przez zobowiązanego decyzji (i dające też możliwość zobowiązanemu dobrowolnego jej wykonania na tym jeszcze etapie sprawy).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

Jeżeli zobowiązany, mimo otrzymania upomnienia, nadal nie wykonuje nakazu decyzji Prezesa UODO (obowiązku o charakterze niepieniężnym), sporządzone zostają tytuł wykonawczy (dokument urzędowy stwierdzający istnienie oraz wymagalność obciążającego zobowiązanego obowiązku) oraz postanowienie o nałożeniu na zobowiązanego grzywny w celu przymuszenia – środka egzekucyjnego przewidzianego przepisami ustawy o postępowaniu egzekucyjnym w administracji. Doręczenie zobowiązanemu obu tych dokumentów wszczyna wobec niego **egzekucję obowiązku o charakterze niepieniężnym**. Jak wskazane zostało 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 innych niż grzywna w celu przymuszenia, należności pieniężnych – 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.

W 2022 r. wszczętych zostało **185 postępowań sprawdzających wykonanie decyzji Prezesa UODO** (wszystkie decyzje podlegające sprawdzeniu były decyzjami zawierającymi nakaz – obowiązek o charakterze niepieniężnym). Oznacza to **wzrost liczby takich postępowań o 17% w stosunku do roku 2021** (w którym wszczęto 158 takich postępowań) i o 115% w odniesieniu do roku, w którym zaczęto stosować przepisy RODO (86 postępowań).

Trend wzrostowy liczby tego rodzaju postępowań obrazuje poniższy wykres.

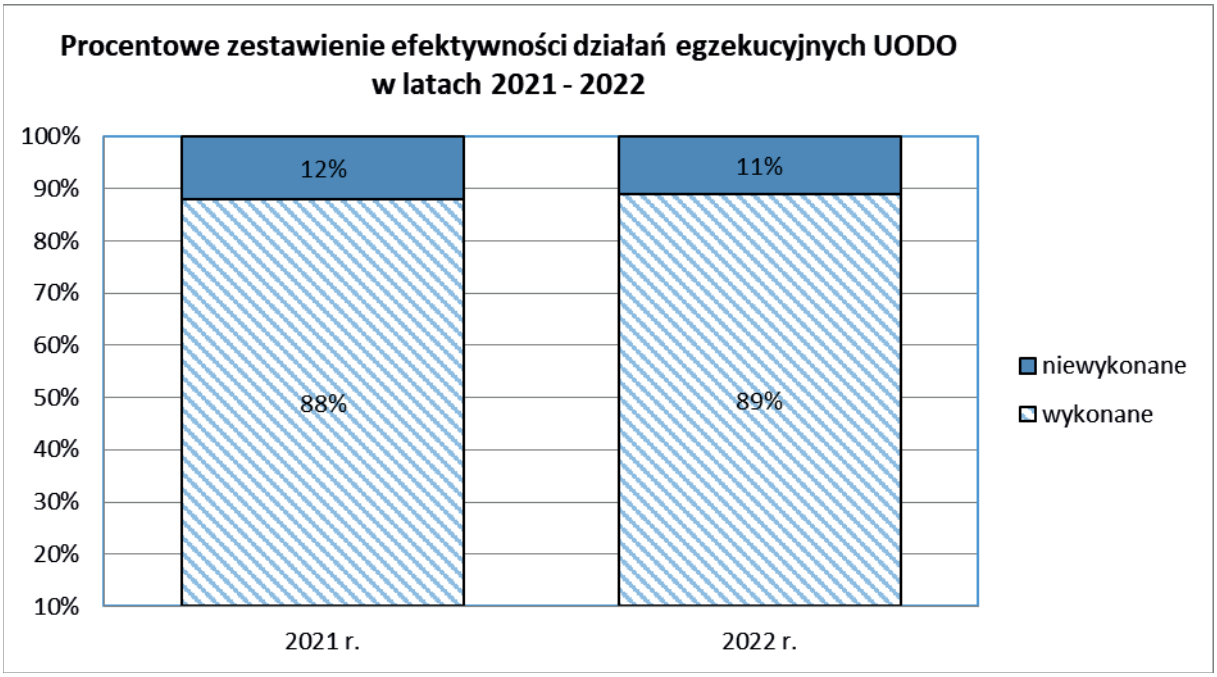


Wykres 6: Zestawienie decyzji Prezesa UODO przekazanych w latach 2018-2022 do sprawdzenia wykonania i ewentualnej egzekucji administracyjnej.

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

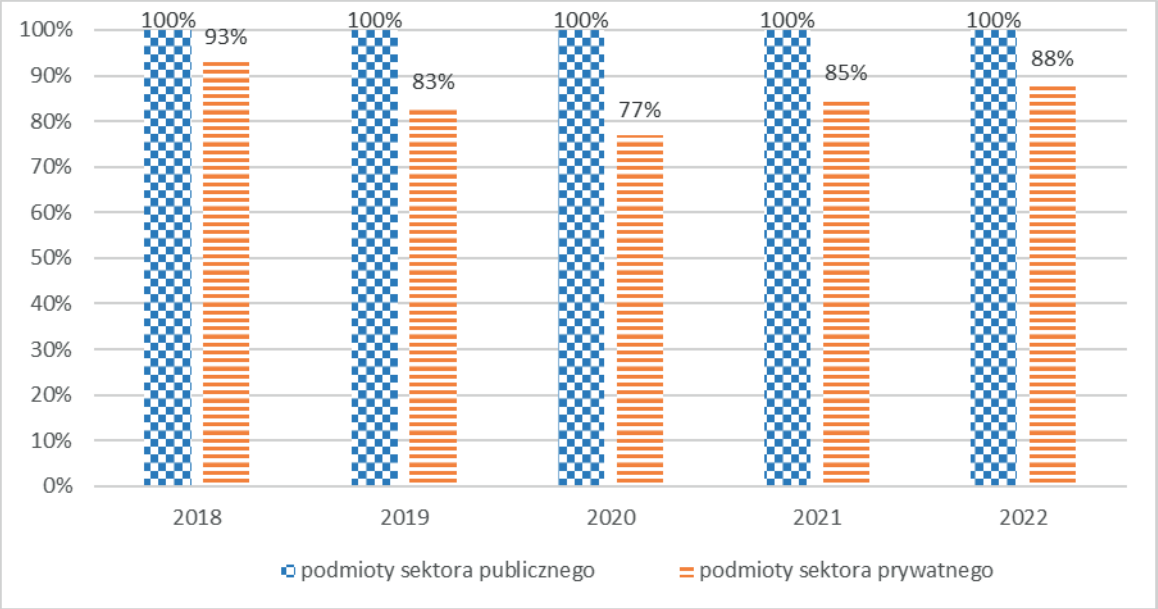
- spośród 185 decyzji, w odniesieniu do których wszczęte zostały postępowania w 2022 r., **wykonanych zostało przez zobowiązanych 165 decyzji**, natomiast
- co do 20 decyzji Prezes UODO nie uzyskał dowodów na ich wykonanie. Decyzje te w dalszym ciągu objęte są działaniami UODO;
- w odniesieniu do dziewięciu z tych 20 decyzji prowadzone są postępowania sprawdzające ich wykonanie; w przypadku pozostałych jedenastu decyzji wszczęta została egzekucja obowiązku o charakterze niepieniężnym, w ramach których na zobowiązanych nałożone zostały grzywny w celu przymuszenia.

Procentowy wskaźnik efektywności działań w odniesieniu do wszystkich decyzji administracyjnych wszczętych w 2022 r., wyniósł **89%.** Oznacza to wzrost o 1% w stosunku do 2022 r., co ilustruje poniższy wykres.



Wykres 7: Procentowe zestawienie efektywności działań egzekucyjnych organu w latach 2021 i 2022.

W 2022 r. działania Prezesa UODO w zakresie sprawdzenia wykonania i egzekucji decyzji administracyjnych dotyczyły w 13% przypadków podmiotów z sektora publicznego (24 podmioty), a w pozostałych 87% przypadkach – podmiotów prywatnych (161 podmiotów). Podobnie jak w roku poprzednim i latach wcześniejszych, wszystkie niewykonane decyzje dotyczyły podmiotów z sektora prywatnego. Analizując na przestrzeni kilku lat efektywność działań egzekucyjnych organu ze względu na przynależność zobowiązanych do sektora publicznego i sektora prywatnego odnotować należy stale utrzymującą się w latach 2018–2022 stuprocentową efektywność w odniesieniu do podmiotów publicznych.



Wykres 8: Zestawienie efektywności prowadzonych działań egzekucyjnych w odniesieniu do podmiotów z sektora publicznego i sektora prywatnego w latach 2018-2022.

Egzekucja obowiązków o charakterze niepieniężnym

Wobec stwierdzenia niewykonania przez zobowiązanych nakazów decyzji Prezesa UODO, w 2022 r. wszczęte zostało **osiem egzekucji obowiązków o charakterze niepieniężnym**. Wystawione w tym okresie tytuły wykonawcze objęły nakazy orzeczone dwunastoma decyzjami administracyjnymi, a łączna kwota grzywien w celu przymuszenia zastosowanych wobec zobowiązanych przez Prezesa UODO w tych postępowaniach wyniosła 35 500 zł. Wszystkie osiem grzywien nałożonych w egzekucjach obowiązków o charakterze niepieniężnym skierowane zostało do dalszego etapu postępowania – egzekucji należności pieniężnych.

Egzekucja należności pieniężnych

W 2022 r. Prezes UODO doprowadził do wszczęcia **piętnastu egzekucji należności pieniężnych**, których łączna wysokość wynosiła 132 381 zł. Porównując liczbę tego rodzaju spraw z rokiem 2021, wskazać należy, że nastąpił jej wzrost o 400% (w poprzednim roku sprawozdawczym wszczęto trzy egzekucje – wszystkie dotyczące administracyjnych kar pieniężnych). W omawianym okresie sprawozdawczym egzekucje należności pieniężnych dotyczyły dwóch rodzajów należności: nałożonych przez Prezesa UODO administracyjnych kar pieniężnych oraz grzywien w celu przymuszenia orzeczonych przez Prezesa UODO jako środków egzekucyjnych w egzekucjach obowiązków o charakterze niepieniężnym. W ujęciu liczbowym postępowania te i ich efekty przedstawiają się następująco:

1. Prezes UODO w bieżącym okresie sprawozdawczym doprowadził do wszczęcia **ośmiu** egzekucji, których przedmiotem były **administracyjne kary pieniężne** o łącznej

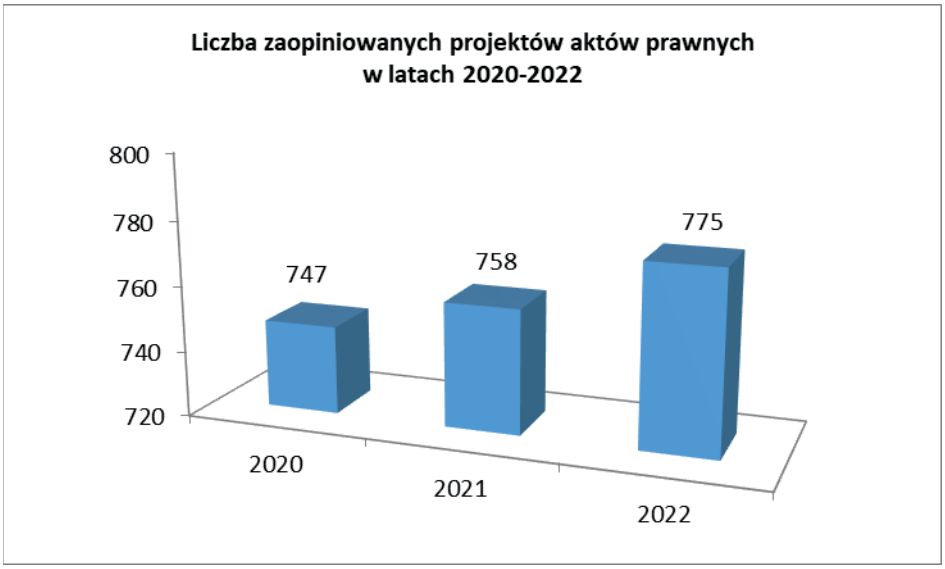
wysokości 101 881 zł. Wszystkie egzekwowane w tych postępowaniach kary pieniężne nałożone zostały na podmioty prywatne – cztery spółki prawa handlowego i cztery osoby fizyczne (w tym trzy osoby fizyczne prowadzące działalność gospodarczą). Spośród tych egzekucji dwie zakończyły się wyegzekwowaniem przez właściwych naczelników urzędów skarbowych orzeczonych kar pieniężnych, na kwotę 17 285 zł. W jednym przypadku, który dotyczył kary w wysokości 22 739 zł, organ egzekucyjny odmówił przystąpienia do egzekucji ze względu na brak majątku lub źródła dochodu, z których możliwa byłaby egzekucja. W pozostałych przypadkach pięciu kar o łącznej kwocie 61 857 zł właściwe organy egzekucyjne prowadzą w dalszym ciągu działania egzekucyjne.

2. Przedmiotem **siedmiu** wszczętych przez Prezesa UODO egzekucji należności pieniężnych były **grzywny w celu przymuszenia**, o łącznej kwocie 30 500 zł. Wszystkie tego rodzaju środki egzekucyjne orzeczone zostały wobec podmiotów prywatnych – sześciu spółek prawa handlowego i jednej osoby fizycznej. W przypadku jednego tytułu wykonawczego wystawionego przez Prezesa UODO na kwotę 5 000 zł właściwy naczelnik urzędu skarbowego odmówił przystąpienia do egzekucji ze względu na brak majątku lub źródła dochodu, z których możliwa byłaby egzekucja. Pozostałe egzekucje - sześć tytułów wykonawczych na łączną kwotę 25 500 zł – nadal były prowadzone przez właściwe organy egzekucyjne.

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

Ważnym zadaniem organu nadzorczego jest opiniowanie projektów aktów prawnych. W 2022 r. zadanie to realizowane było poprzez analizę projektowanych lub nowelizowanych przepisów pod kątem zapewnienia przez projektodawców zgodności treści nowych regulacji z przepisami RODO. Organ nadzorczy opiniował także projekty dotyczące przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

W 2022 r. organ nadzorczy zaopiniował **775 projektów aktów prawnych** (zarówno na poziomie regulacji krajowych, jak i międzynarodowych). Dla porównania w 2021 r. zaopiniowanych zostało 758 projektów, a w 2020 r. 747 – co przedstawia poniższy wykres.



Wykres 9: Liczba zaopiniowanych projektów aktów prawnych, które wpłynęły do Urzędu Ochrony Danych Osobowych w latach 2020–2022.

Do opiniowanych projektów aktów europejskich, np. rozporządzenia Parlamentu Europejskiego i Rady w sprawie przejrzystości i targetowania reklamy politycznej[107], projektu rozporządzenia PE i Rady ws. zharmonizowanych zasad sprawiedliwego dostępu do danych i ich wykorzystania, tzw. akt o danych/Data Act[108], czy dyrektywy Parlamentu Europejskiego i Rady w sprawie poprawy warunków pracy za pośrednictwem platform internetowych (COM(2021) 762)[109], Prezes UODO wydawał do nich stanowiska na takich samych zasadach, jak w przypadku projektów krajowych.

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

Przedmiotem zainteresowania organu nadzorczego były takie zagadnienia, jak:

- ocena skutków dla ochrony danych, w tym przeprowadzenie testu prywatności w procesie tworzenia prawa – tj. projektowanie ochrony danych osobowych przy

107 DOL.401.9.2022.
108 DOL.401.74.2022.
109 DOL.401.606.2021.

określaniu sposobów przetwarzania (art. 25 ust. 1 RODO[110]),

- kwestie związane z wyłączaniem/ograniczaniem stosowania RODO w projektowanych przepisach (art. 23 RODO),
- przetwarzanie danych w zbiorach danych, w rejestrach publicznych,
- wykorzystywanie nowych technologii w procesach przetwarzania danych, m.in. wykorzystujących dane biometryczne, systemy rejestrujące obraz i dźwięk, usługę chmurową oraz różnego rodzaju systemy czy aplikacje,
- określenie ról poszczególnych podmiotów biorących udział w procesie przetwarzania danych osobowych.

Przedkładanie aktów prawnych do zaopiniowania organowi nadzorczemu

Zgodnie z art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[111] w związku z art. 57 ust. 1 lit. c RODO[112], założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi UODO. Obowiązek ten jest realizowany przede wszystkim przez ministrów kierujących poszczególnymi działami administracji rządowej i kierowane przez nich ministerstwa prowadzące konkretny proces legislacyjny. Przedkładają oni projekty aktów normatywnych do organu nadzorczego na etapie prac Rządu nad projektem, odpowiednio do § 38 ust. 1 pkt 3 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów[113].

Zdarzają się przypadki prekonsultacji przez rozpoczęciem procesu legislacyjnego. Przykładami takich aktów są **ustawa o ochronie osób zgłaszających naruszenia prawa**[114] czy też **ustawa o zmianie ustawy o Polskim Instytucie Ekonomicznym oraz niektórych innych ustaw**[115], która wprowadza rozwiązania dotyczące Zintegrowanej Platformy Analitycznej.

W roku 2022 organ nadzorczy brał udział w prekonsultacjach z właściwymi resortami m.in. w związku z ustawą o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw[116] oraz rozporządzeniem Ministra Zdrowia w sprawie badań na obecność alkoholu lub środków działających podobnie do alkoholu w organizmie pracownika[117].

110 Zgodnie z art. 25 ust. 1 RODO – 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 RODO oraz chronić prawa osób, których dane dotyczą.

111 Art. 51 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych stanowi, że założenia i projekty aktów prawnych dotyczące danych osobowych są przedstawiane do zaopiniowania Prezesowi UODO.

112 Art. 57 ust. 1. lit. c RODO stanowi, że bez uszczerbku dla innych zadań określonych na mocy RODO każdy organ nadzorczy na swoim terytorium: doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem.

113 Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (tj. M. P. z 2016 r. poz. 1006).

114 DOL.401.512.2022.

115 DOL.401.443.2022.

116 DOL.401.237.2021.

117 DOL.401.633.2022.

Niektóre organy publiczne poprzez pominięcie procesu uzgodnień i opiniowania nie przekazywały istotnych projektów aktów normatywnych dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie, do oceny organu nadzorczego. Jest to nie tylko działanie wbrew obowiązującym przepisom i obowiązkom, ale także utrata okazji do eksperckiego wsparcia projektodawcy przez organ nadzorczy na jak najwcześniejszym etapie procesu legislacyjnego. W części przypadków projekty te były konsultowane przez Rządowe Centrum Legislacji (na etapie komisji prawniczej) oraz Kancelarię Sejmu, które przekazują część tych projektów do Prezesa UODO, na właściwych dla tych podmiotów etapach procesu legislacyjnego.

Przykładami projektów, które nie zostały przedstawione organowi nadzorczemu do zaopiniowania w toku prowadzonych przez projektodawcę uzgodnień międzyresortowych, a przekazane były dopiero przez Rządowe Centrum Legislacji były m.in.: ustawa o zmianie ustawy o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności oraz niektórych innych ustaw[118], ustawa o zmianie ustawy o ubezpieczeniu społecznym rolników oraz ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[119], ustawa o zmianie niektórych ustaw w celu przeciwdziałania przestępczości środowiskowej[120], rozporządzenie Ministra Rolnictwa i Rozwoju Wsi w sprawie dokonywania zgłoszeń, składania wniosków lub przekazywania informacji do komputerowej bazy danych[121].

Współpraca z jednostką odpowiedzialną w szczególności za opracowywanie i koordynowanie tworzonych ustaw jest niezwykle cenna, jednak przekazanie projektu aktu na tym etapie procesu legislacyjnego było najczęściej zbyt późne, aby organ nadzorczy mógł zgłosić, a projektodawca uwzględnić uwagi merytoryczne.

Zdarzały się także sytuacje, w których projekt aktu normatywnego był przekazany do Urzędu Ochrony Danych Osobowych w tym samym dniu, w którym był rozpatrywany na posiedzeniu plenarnym Sejmu Rzeczypospolitej Polskiej. Tak było np. w przypadku **rządowego projekt ustawy o dodatku węglowym**[122]. Organ nadzorczy nie miał wówczas możliwości jego zaopiniowania w wymaganym czasie. Tego typu praktyki naruszają przepisy RODO oraz ustawy o ochronie danych osobowych.

Na wniosek Kancelarii Sejmu czy Kancelarii Senatu są też opiniowane poselskie (rzadziej senatorskie) projekty ustaw. W ten sposób UODO realizuje zadanie wspomagania i doradztwa na rzecz Parlamentu RP w sprawie projektowanych przez to ciało aktów prawnych. Jako przykłady wskazać można projekty opiniowanych ustaw: o zmianie ustawy o Policji oraz niektórych innych ustaw[123], o zmianie ustawy o wspieraniu rodziny i systemie pieczy zastępczej

118 DOL.401.118.2022.
119 DOL.401.136.2022.
120 DOL.401.186.2022.
121 DOL.401.570.2022.
122 DOL.401.364.2022.
123 DOL.401.24.2022.

oraz niektórych innych ustaw[124], o zmianie ustawy – Kodeks postępowania cywilnego[125].

W 2022 roku organ nadzorczy – w związku rządową z prośbą o dokonanie pilnej analizy przedłożonego aktu prawnego oraz o ocenę ewentualnej konieczności wprowadzenia zmian do krajowego porządku prawnego – opiniował również projekt **rozporządzenia Oceny konieczności dokonania interwencji legislacyjnych w krajowy porządek prawny[126], w związku z publikacją Rozporządzenia (UE) 2022/1925**[127]. Przedmiotowy akt reguluje działalność platform internetowych (strażników dostępu) w obszarze usług, z których na co dzień korzysta większość użytkowników biznesowych i użytkowników końcowych. Kwestia ta stanowiła element szczególnego zainteresowania organu, ponieważ opublikowany 12 października 2022 r. akt o rynkach cyfrowych było jednym z bardziej wyczekiwanych aktów unijnych, z uwagi na to, że wprowadzał liczne zakazy i obowiązki dla tzw. strażników dostępu (cybergigantów). Przyjęte jego mocą rozwiązania w prawie krajowym miały przynieść wiele korzyści zarówno mniejszym platformom internetowym, jak i użytkownikom (konsumentom) m.in. poprzez wzmocnienie ochrony podstawowych praw do prywatności i ochrony danych osobowych.

Rozważając konieczność wprowadzenia zmian do krajowego porządku prawnego w związku z opublikowaniem aktu o rynkach cyfrowych (i koniecznością rozpoczęcia jego stosowania od 2 maja 2023 r.) UODO podkreślił, że główne założenia aktu o rynkach cyfrowych mają zapobiec nieuczciwym praktykom w sektorze cyfrowym. Dlatego w ocenie organu zasadne było, aby ustawodawca krajowy dokonał przede wszystkim przeglądu regulacji obejmujących ten zakres przedmiotowy krajowego porządku prawnego związany z prawem konkurencji i konsumentów. Zgodnie z aktem o rynkach cyfrowych tzw. strażnicy dostępu odpowiadają za to, aby wypełnianie obowiązków na nich nałożonych unijnymi przepisami odbywało się przy jednoczesnym zapewnieniu pełnej zgodności z pozostałymi przepisami prawa UE, w szczególności w zakresie ochrony danych osobowych i prywatności lub ochrony konsumentów. Akt o rynkach cyfrowych, podobnie jak RODO w art. 5 ust. 2[128], przewiduje obowiązek wykazania wypełniania obowiązków przez strażników dostępu, do których zaliczani będą m.in. operatorzy wyszukiwarek internetowych, tacy jak np. Google. Zgodnie z wyrokiem TSUE z 13 maja 2014 r. sygn. C-131/12[129] są oni odpowiedzialni za przetwarzanie danych osobowych, które pojawiają się na stronach internetowych publikowanych przez osoby trzecie, a więc są administratorami tych danych w rozumieniu przepisów RODO. Dlatego w swojej opinii organ nadzorczy wskazał na konieczność analizy zarówno krajowych przepisów, które ograniczyły bądź wyłączyły określone w RODO prawa osób, których dane dotyczą, jak i przepisów dotyczących obowiązków administratorów oraz

124 DOL.401.2.2022.
125 DOL.401.620.2022.
126 DOL.401.507.2022.
127 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych; Dz. U. UE. L. z 2022 r. Nr 265, str. 1), dalej: „akt o rynkach cyfrowych".
128 Art. 5 ust. 2 RODO stanowi o tzw. zasadzie rozliczalności, zgodnie z którą „Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność")".
129 Wyrok TSUE z dnia 13.05.2014 r., w sprawie C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi.

przepisów, które nie zostały przez ustawodawcę dostosowane do przepisów RODO.

7.1. Ocena skutków dla ochrony danych

Okoliczności zawarte w art. 35 RODO – co prawda nie wprost – regulują obowiązek dokonania – m.in. w związku z tworzeniem przepisów regulujących operację lub zestaw operacji przetwarzania – oceny skutków dla ochrony danych, tj. wpływu projektowanych rozwiązań na prawo do prywatności oraz prawo do ochrony danych osobowych (art. 35 ust. 10 RODO). Taka ocena skutków dla ochrony danych powinna być dokonywana ze względu na rodzaj przetwarzania, w szczególności następujący przy użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób. Należy wykazać niezbędność przetwarzania określonych kategorii danych osobowych we wskazanym konkretnie celu i zakresie. Uzasadnione jest, by ocena skutków dla ochrony danych była dokonywana już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych. Z wielu przedkładanych organowi nadzorczemu do zaopiniowania projektów nie wynika, aby ocena taka została przeprowadzona. Co więcej, projektodawcy bardzo często nie dostrzegają potrzeby jej dokonania, jak również powołują argument braku takiego obowiązku, nawet gdy akt prawny w zasadniczej swej części dotyczy przetwarzania danych osobowych, i to z użyciem nowych technologii. Analiza przedstawianych projektów prowadzi do wniosku, że wykonanie testu prywatności w postaci takiej oceny pozwoliłoby na wyeliminowanie wielu niedoskonałości projektowanych przepisów czy uniknięcie ryzyk związanych z proponowanym w przepisach przetwarzaniem danych osobowych w kontekście istoty i celów przyjmowanych rozwiązań oraz stosowanych technik przetwarzania danych, zwłaszcza z użyciem nowych technologii. Poprawnie przeprowadzona ocena skutków powinna wskazywać związek między operacjami wykonywanymi na danych osobowych z konkretnym celem ich przetwarzania. Cel przetwarzania musi być określony w podstawie prawnej, gdy są nią przepisy prawa powszechnie obowiązującego (art. 6 ust. 3 RODO). Podstawa prawna może zawierać również przepisy szczegółowe, które dostosowują projektowane regulacje do przepisów niniejszego rozporządzenia, jak i inne elementy, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX.

7.2. Test prywatności

Wyrażenie „test prywatności” jest pojęciem autonomicznym prawa ochrony danych, występującym w języku prawniczym. Pojęcie to określa minimalny standard (wzorzec)

metodyczny, który projektodawcy (podmioty tworzące prawo) i administratorzy powinni uwzględnić w toku projektowania rozwiązań dotyczących danych osobowych. RODO jest w tym zakresie „neutralne technologicznie”[130], co oznacza, że nie zawiera ono konkretnych wytycznych odnośnie do rozwiązań technologicznych czy organizacyjnych, jakie projektodawca powinien podjąć w celu zabezpieczenia danych osobowych. Jego przeprowadzenie oznacza projektowanie ochrony danych osobowych przy określaniu sposobów przetwarzania (art. 25 ust. 1 RODO[131]). Nie ma jednego wzorca tego testu, lecz istotne jest rozważenie tych ryzyk, które towarzyszą konkretnemu rozwiązaniu (rozwiązaniom) i analiza przyjmowanych przepisów pod kątem uczynienia zadość stosowaniu przepisów rozporządzenia dla zindywidualizowanych mechanizmów wprowadzanych konkretnymi przepisami.

Pozytywnie należy ocenić, że konsekwencją podnoszenia tego istotnego aspektu przez organ nadzorczy w jego eksperckich ocenach projektów aktów prawnych jest to, że niektóre resorty dokonują oceny skutków dla ochrony danych. Dostrzegają jej wagę, choć nadal są to działania podejmowane głównie po zwróceniu uwagi na ten aspekt przez organ nadzorczy, a zatem w toku opiniowania, a nie w czasie koncepcyjnych prac resortowych.

Jako przykład wskazać należy opiniowany projekt **rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie programu pilotażowego opieki nad świadczeniobiorcą w ramach sieci kardiologicznej[132].** Organ nadzorczy z zadowoleniem przyjął dokonanie przez projektodawcę oceny skutków dla ochrony danych. Jednak niezależnie w przedstawionej opinii zwrócił uwagę projektodawcy, że szczegółowe rozwiązania dotyczące wzajemnego przepływu danych powinny zostać uregulowane wprost w przepisach rangi ustawy, a nie w umowach o współpracy zawartych pomiędzy podmiotami leczniczymi realizującymi program pilotażowy. Wskazał również, że projekt rozporządzenia powinien zawierać informacje o tym, jak funkcjonować będzie system teleinformatyczny sieci kardiologicznej, wskazywać przepisy wprowadzające i określające sposoby przetwarzania danych osobowych w związku z dokonywaniem operacji na danych (w tym również danych szczególnych kategorii). Podkreślono także, że przepisy powinny określać, w jakim celu/celach, na jakich zasadach oraz jakie podmioty będą odpowiedzialne za prowadzenie/uzupełnianie systemu teleinformatycznego oraz przetwarzanie danych.

Zdarza się również, i należy to ocenić pozytywnie, że resorty nie opracowują odrębnej oceny skutków dla ochrony danych, ale przedstawiają szczegółowo analizę proponowanych zmian w ramach OSR (oceny skutków regulacji), która również stanowi cenne źródło informacji m.in. dla organu nadzorczego. W 2022 r. UODO z zadowoleniem odnotował

130 Zgodnie z motywem 15 RODO: „Aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik”.

131 Jak stanowi art. 25 ust. 1 RODO: „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”.

132 DOL.401.389.2022.

takie pojawiające się w niektórych przypadkach rozwiązanie. Jednym z przykładów był **projekt ustawy o zmianie ustawy o sposobie ustalania najniższego wynagrodzenia zasadniczego niektórych pracowników zatrudnionych w podmiotach leczniczych oraz niektórych innych ustaw[133].**

Natomiast w wielu przypadkach – i to w odniesieniu do istotnych projektów i regulowanych nimi zagadnień, zwłaszcza nowych rozwiązań związanych z nowymi sposobami przetwarzania danych – ocena taka nie jest niestety dokonywana.

W tym kontekście wskazać należy na **projekt ustawy o aplikacji mObywatel**[134] mający na celu połączenie tej aplikacji z licznymi rejestrami publicznymi oraz wprowadzenie nowych podmiotów publicznych jako współadministratorów w tej aplikacji. Organ wskazał na konieczność przeprowadzenia przez projektodawcę testu prywatności w procesie tworzenia prawa, w tym oceny skutków dla ochrony danych. Odwołując się do art. 25 ust. 1 i art. 35 (w szczególności ust. 1[135] i ust. 10[136]) RODO, podniósł, że zmiany funkcjonalności narzędzi takich jak aplikacja mObywatel, mających charakter innowacyjnych rozwiązań technologicznych – połączonych z rejestrami publicznymi – za których prawidłowe funkcjonowanie odpowiada podmiot publiczny, zawsze powinno być poprzedzone analizą ryzyk i oceną skutków dla ochrony danych. Organ nadzorczy wskazał, że projektowana ustawa wywołuje wiele wątpliwości, zwłaszcza ze względu na blankietowy charakter przyjmowanych regulacji oraz nieprecyzyjne wyznaczenie ról w procesach przetwarzania danych. Część przepisów proponowanych w projektowanej ustawie w ocenie organu była fundamentalnie sprzeczna z zasadami przetwarzania danych określonymi w RODO, co może istotnie, bo negatywnie, wpłynąć na standard przetwarzania danych przez podmioty publiczne w Polsce. Uwagi organu nadzorczego dotyczyły m.in. nowego „dokumentu tożsamości" okazywanego za pomocą aplikacji mObywatel, zawierającego potencjalnie nieograniczony katalog danych osobowych. Wskazano na brak przepisów w zakresie funkcjonowania tego nowego dokumentu, gdyż będzie on kształtowany w oparciu o swobodną decyzję ministra właściwego do spraw informatyzacji, udostępniającego w aplikacji mObywatel daną usługę. Wskazano również, że ustawa umożliwi połączenie aplikacji mObywatel z wszystkimi rejestrami publicznymi funkcjonującymi w Polsce, gdyż jedynym kryterium do przetwarzania tych danych będzie ich niezbędność dla korzystania z usługi udostępnionej w aplikacji mObywatel. Nie będzie miało przy tym znaczenia, kto jest administratorem tych danych, zwłaszcza czy jest to podmiot udostępniający tę usługę. Zaznaczono również, że przepisy projektowanej ustawy – w zakresie ról w procesach przetwarzania – powierzają decyzji ministra właściwego do spraw informatyzacji włączenie dodatkowych współadministratorów

133 DOL.401.218.2021.

134 DOL.401.276.2022.

135 Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

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

do procesów przetwarzania w aplikacji mObywatel, których standard działania będzie określany również w drodze uznaniowej decyzji tego ministra.

Podobnie opiniując **projekt ustawy o badaniach klinicznych stosowanych u ludzi**[137], który będzie nową regulacją w krajowym porządku prawnym dotyczącą badań klinicznych, organ nadzorczy wskazał na konieczność przeprowadzenia oceny skutków dla ochrony danych. Badania kliniczne są uregulowane w rozporządzeniu 563/2014[138], które w zakresie ochrony danych osobowych odwołuje się do nieobowiązującej już dyrektywy 95/46/WE[139]. Dlatego do materii objętej projektowaną ustawą zastosowanie będą miały przepisy RODO. W związku z tym wymogi zarówno wynikające z rozporządzenia 536/2014, jak i z RODO będą musiały zostać – w zakresie wprost nieuregulowanym w tych przepisach – odzwierciedlone w przepisach prawa krajowego. Z tej perspektywy przepisy prawa krajowego muszą zapewniać stosowanie wskazanych wyżej rozporządzeń, zwłaszcza respektować zasady wynikające z ogólnego rozporządzenia o ochronie danych. Natomiast z dokumentów przedstawionych do zaopiniowania przez projektodawcę nie wynikało, by wykonał on taką analizę i ocenę skutków dla ochrony danych, a w konsekwencji wyważył wpływ planowanego przetwarzania danych osobowych na prywatność osób, których dane dotyczą, i zaproponował rozwiązania odpowiadające poszanowaniu zasad przetwarzania danych osobowych. Tymczasem wobec doniosłości i konsekwencji projektowanego przetwarzania danych osobowych w związku z przyjmowanymi w projekcie ustawy rozwiązaniami, organ nadzorczy uznał to za wysoce pożądane. Projektodawca jednak na etapie prac w Rządowym Centrum Legislacji – poddając analizie uwagi zgłoszone przez organ nadzorczy – uwzględnił (bez przeprowadzenia oceny skutków dla ochrony danych) konieczność doprecyzowania tworzonych przepisów m.in. w zakresie wyłączeń stosowania przepisów RODO na rzecz jedynie ich ograniczenia, uwzględniając przy tym poszczególne etapy badania klinicznego. W projekcie pojawiły się rozwiązania, które stanowią przykład godzenia praw z zakresu badań klinicznych i ograniczenia praw osób, których dane mają być przetwarzane. Projekt zakłada bowiem, że wynikające z RODO prawa osób (do dostępu, do sprostowania danych, do ograniczenia przetwarzania, do sprzeciwu) będą mogły być ograniczone, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację celów badania klinicznego, i jeżeli ograniczenia te są konieczne do realizacji tych celów. Ponadto powyższe ograniczenia zostały przez projektodawcę doprecyzowane w zakresie konkretnego etapu badania klinicznego, jak również uwzględnił on dane osobowe, które nie będą podlegały powyższym ograniczeniom. Omawiana regulacja została pozytywnie oceniona przez organ właściwy do spraw ochrony danych osobowych także ze względu na zawarcie w projekcie przepisów dotyczących bezpieczeństwa danych.

137 DOL.401.196.2021.

138 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE (Dz. U. UE. L. z 2014 r. Nr 158, str. 1 z późn. zm.).

139 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. UE. L. z 1995 r. Nr 281, str. 31 z późn. zm.), dalej: „dyrektywa 95/46/WE".

Organ nadzorczy, opiniując **projekt ustawy o zmianie ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy oraz niektórych innych ustaw**[140] zwrócił uwagę, że przepisy dotyczące przetwarzania danych osobowych wprowadzane w projektowanej ustawie determinują zasadność przeprowadzenia testu prywatności – projektowania ochrony danych osobowych w procesie tworzenia prawa, w tym przeprowadzenia oceny skutków dla ochrony danych. Z przekazanej do Urzędu Ochrony Danych Osobowych korespondencji nie wynikało, aby projektodawca wykonał tego rodzaju analizę i ocenę, a w konsekwencji wyważył wpływ planowanego przetwarzania danych osobowych na prywatność osób, których dane dotyczą, i proponował rozwiązania odpowiadające poszanowaniu zasad przetwarzania danych osobowych – zwłaszcza w zakresie podstawy prawnej, rzetelności oraz przejrzystości regulacji dotyczących przetwarzanych danych osobowych. Tymczasem, w związku z przyjmowanymi w projekcie ustawy rozwiązaniami przewidującymi obszerne i istotne zmiany w zakresie funkcjonowania rejestrów publicznych, za których prawidłowe funkcjonowanie odpowiadają podmioty publiczne, zawsze powinny być poprzedzone analizą ryzyka i oceną skutków dla ochrony danych towarzyszących proponowanym rozwiązaniom, oceną ich wpływu na obowiązujące rozwiązania i kompleksowym odzwierciedleniem projektowanych zmian w obowiązującym porządku prawnym. Organ zaznaczył także, że projektowane zmiany mają wpływ na niezwykle ważny aspekt, jakim jest status podmiotów uczestniczących w procesach przetwarzania danych w wyżej wymienionych rejestrach, zwłaszcza zaś na ich status i odpowiedzialność jako administratorów w rozumieniu art. 4 pkt 7 ogólnego rozporządzenia o ochronie danych. Status i rola w procesach przetwarzania danych ministra właściwego do spraw gospodarki (odpowiedzialnego za prowadzenie rejestru CEIDG w systemie teleinformatycznym) oraz innych podmiotów/organów (które będą udostępniać dane z rejestrów publicznych do systemu teleinformatycznego CEIDG) wymagają w ocenie organu nadzorczego pogłębionej analizy dla wyeliminowania propozycji niezgodnych z zasadami przetwarzania danych osobowych, które mogą negatywnie wpłynąć na standard przetwarzania danych w rejestrach publicznych. Jak wskazał, niezbędne jest określenie ról tych podmiotów/organów (czy będzie dochodzić do współadministrowania, odrębnego administrowania). Konieczne jest również przeprowadzanie analizy obowiązujących przepisów szczegółowych celem wypracowania rozwiązań kompleksowych. Ponadto użyte w projektowanych przepisach sformułowania wskazujące, że to CEIDG korzysta/publikuje/wykreśla/dopisuje sugerują, że czynności te odbywają się w sposób zautomatyzowany. Konstrukcja taka jest związana z szeregiem ryzyk, na które projektodawca powinien zwrócić uwagę w przepisach tej ustawy. Omawiany projekt zawierał nieprzejrzyste procedury wymiany danych osobowych pomiędzy organami, nie zapewniając kontroli nad tymi danymi. Nie zostały także określone zasady odpowiedzialności tych podmiotów. Organ nadzorczy podkreślił, że brak zapewnienia zasady rozliczalności (art. 5 ust. 2 RODO) powoduje, że w związku z wymianą danych pomiędzy systemami teleinformatycznymi odpowiedzialność za prawidłowe przetwarzanie danych osobowych zostaje przerzucona

140 DOL.401.460.2022.

z organów na systemy teleinformatyczne. W ocenie organu nadzorczego wszelkie kwestie związane z przekazywaniem czy udostępnianiem danych za pośrednictwem systemów teleinformatycznych powinny być kompleksowo uregulowane w przepisach tej ustawy. Organ nadzorczy zwrócił uwagę na przepisy, które wskazują, że to system (CEiDG) – nie podmiot praw i obowiązków – korzysta z informacji. Przepisy nie określają, na czym korzystanie będzie polegało, w jakim trybie informacje będą udostępniane. Obawy wzbudza zwłaszcza to, czy owo korzystanie dotyczy także udostępniania innym podmiotom danych z różnych rejestrów (w jakim celu i zakresie, na jakich zasadach, w jakim trybie i jakie podmioty będą mieć dostęp do tych danych). Przepisy w tym zakresie powinny być sformułowane w taki sposób, aby czynić zadość zasadom wynikającym z art. 5 RODO. Szczególne znaczenie ma tu zasada rozliczalności (art. 5 ust. 2) – projektodawca nie powinien formułować rozwiązań uniemożliwiających administratorowi przestrzeganie (i wykazanie przestrzegania) zasad dotyczących przetwarzania danych osobowych. Tymczasem projektodawca nie precyzuje, z jakich rejestrów administrator będzie pozyskiwał dane, w jakim celu i zakresie. Organ zwrócił uwagę na motyw 31 RODO, z którego wynika, że ujawnianie danych podmiotom publicznym powinno mieć co do zasady charakter wnioskowy (odbywać się w formie pisemnej, być uzasadnione i 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. Mocą projektowanej ustawy tworzone są kompetencje dla innych organów (określone w odrębnych przepisach) regulujące ich działalność. Projektodawca nie sprecyzował jednocześnie celów takiego rozwiązania.

Jako przykłady innych istotnych projektów, na których potrzeby ocena skutków dla ochrony danych osobowych również nie została przeprowadzona – mimo postulatu organu – wskazać trzeba: **projekt ustawy o polubownej działalności windykacyjnej i zawodzie windykatora**[141], **projekt ustawy o zmianie ustawy o ochronie konkurencji i konsumentów oraz niektórych innych ustaw**[142] oraz **projekt ustawy o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw**[143].

Istotą eksperckiego wsparcia udzielanego w toku opiniowania projektów aktów prawnych jest też tak istotny cel, jak uniknięcie konfuzji i odpowiedzialności po stronie adresatów projektowanych norm, które w swojej treści nie odpowiadają standardom wynikającym z RODO. Tymczasem to właśnie rolą Projektodawcy jest zapewnienie, aby podmioty danych mogły w pełni korzystać ze swoich praw, które wynikają wprost z RODO. Przyjęcie już przez Projektodawcę (ustawodawcę) na etapie tworzenia przepisów prawa rozwiązań zapewniających stosowanie przepisów ogólnego rozporządzenia o ochronie danych pozwoli dobrać rozwiązania optymalne dla realizacji celów projektowanych przepisów i poszanowania zasad przetwarzania danych osobowych, m.in. co do podstawy prawnej przetwarzania danych osobowych, źródła praw i obowiązków z zakresu przetwarzania

141 DOL.401.482.2022.
142 DOL.401.410.2022.
143 DOL.401.371.2021.

danych osobowych. Jest to istotne zarówno dla adresatów tych norm, dla praktyki stosowania tych przepisów, jak i dla ich beneficjentów, tj. osób, których dane będą przetwarzane.

7.3. Wyłączenia bądź ograniczenia praw osób, których dane dotyczą

Zagadnienia związane z wyłączaniem bądź ograniczaniem praw osób, których dane dotyczą, stanowiły w 2022 r. kolejny ważny element w opiniach legislacyjnych organu, który niejednokrotnie podkreślał, że wyłączenia stosowania praw osób są wskazane ściśle w RODO i nie jest dopuszczalne, mocą przepisów prawa krajowego rozszerzanie tych wyłączeń. Ograniczenia stosowania przepisów RODO nie mogą prowadzić do wyłączenia praw oraz mogą następować tylko, gdy ograniczenie jest środkiem niezbędnym i proporcjonalnym do – przewidzianych przepisami RODO – celów, ze względu na które jest wprowadzane. Ograniczenia te mogą więc mieć miejsce tylko i wyłącznie w ściśle wskazanych w przepisach RODO przypadkach, jak stanowi art. 23 tej regulacji, oraz mogą następować jedynie z uwzględnieniem zastosowania odpowiednich gwarancji w treści aktów prawnych ograniczających. Istotny jest tu bowiem aspekt pogodzenia i wyważenia regulacji przyjmowanych w projekcie z prawami i obowiązkami z zakresu realizacji praw osób, których dane będą przetwarzane celem wykonywania przepisów projektowanej ustawy.

Tak wypowiedział się organ w toku opiniowania projektu **ustawy – Prawo o ustroju sądów powszechnych**[144] jak również wymienionej wyżej **ustawy o badaniach klinicznych stosowanych u ludzi** wskazując, że zawarte w projekcie – kierunkowo dopuszczalne przepisami RODO – wyłączenia i ograniczenia praw podmiotów danych powinny zostać poddane ocenie projektodawcy pod kątem ich niezbędności i proporcjonalności. Wskazana ocena projektowanych przepisów jest konieczna w związku z przyjętymi w 2021 r. Wytycznymi Europejskiej Rady Ochrony Danych (Wytyczne 10/2020 w sprawie ograniczeń na mocy art. 23 RODO, Wersja 2.0, przyjęte 13 października 2021 r.)[145], które wprost dotyczą materii uregulowanej w projekcie ustawy i powinny być wzięte pod uwagę przez projektodawcę. Celem Wytycznych 10/2020 jest wskazanie warunków stosowania ograniczeń z art. 23 RODO w świetle przepisów Karty Praw Podstawowych UE i RODO. Dokument zawiera dokładną analizę kryteriów stosowania ograniczeń; ocen, których należy dokonywać, dotyczących tego, jak osoby, których dane dotyczą, mogą wykonywać swoje prawa po zniesieniu ograniczeń oraz konsekwencji naruszeń art. 23 RODO. Ponadto Wytyczne 10/2020 wskazują to, w jaki sposób środki prawne określające ograniczenia muszą spełniać wymóg przewidywalności,

144 DOL.401.179.2022.

145 Zgodnie z wnioskami z wytycznych (zawartymi w pkt. 84-88): 1. Art. 23 RODO zezwala na określonych warunkach krajowemu lub unijnemu prawodawcy na ograniczenie, w drodze środka ustawodawczego, zakresu obowiązków i praw przewidzianych w art. 12-22 i art. 34, a także w art. 5 RODO w zakresie, w jakim jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22, jeżeli takie ograniczenie nie narusza istoty podstawowych praw i wolności oraz jest środkiem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, służącym ochronie, między innymi, ważnych celów leżących w ogólnym interesie publicznym Unii lub państwa członkowskiego. 2. Ograniczenia praw osób, których dane dotyczą, muszą spełniać wymogi określone w art. 23 RODO. Państwa członkowskie lub Unia wydające środki ustawodawcze ustanawiające te ograniczenia, i administratorzy, którzy je stosują, powinni być świadomi wyjątkowego charakteru tych ograniczeń. 3. Test proporcjonalności należy przeprowadzić przed wprowadzeniem do prawa Unii lub prawa państwa członkowskiego ograniczeń praw osób, których dane dotyczą. 4. Przed przyjęciem środków ustawodawczych ustanawiających ograniczenia należy konsultować się z organem nadzorczym i posiadać uprawnienia do egzekwowania jego zgodności z RODO. 5. Po zniesieniu ograniczeń osoba, której dane dotyczą, musi mieć możliwość korzystania ze swoich praw przez administratora.

a także obowiązki i prawa, które mogą zostać ograniczone. Wytyczne 10/2020 zawierają test „niezbędności i proporcjonalności", któremu ograniczenia muszą zostać poddane i go spełnić w oparciu o art. 23 ust. 1 RODO. W opinii do projektu wskazano, że test ten pomoże wypracować rozwiązania odpowiadające celom regulacji, a jednocześnie zgodne z RODO i zapewniające ich stosowanie.

Przykładem aktu, który stanowił balas pomiędzy regulacjami a ograniczeniem praw osób, których dane dotyczą z uwagi na pogodzenie w tworzonych przepisach zarówno kwestii, które wymagają uregulowania (zgłaszanie naruszeń prawa), jak i konieczności zapewnienia prawa do prywatności oraz zgodności z przepisami o ochronie danych osobowych (odnośnie osób zgłaszających te naruszenia) jest **ustawa o ochronie osób zgłaszających naruszenia prawa**[146].

Kwestia dotycząca projektowanych ograniczeń stosowania RODO stanowiła również przedmiot opinii organu nadzorczego w przypadku projektów: **ustawy − Prawo komunikacji elektronicznej (UC45)** oraz **ustawy – Przepisy wprowadzające − Prawo komunikacji elektronicznej (UC46)**[147].

7.4. Precyzyjne określenie ról podmiotów w procesie przetwarzania danych

W 2022 roku, podobnie jak w latach ubiegłych, do Urzędu Ochrony Danych Osobowych wpływała znaczna liczba sygnałów świadczących o wątpliwościach różnych podmiotów, co do ich ról w procesie przetwarzania danych osobowych. Analiza projektów aktów prawnych wskazuje, że przyczyną tych wątpliwości jest nieumiejętne tworzenie regulacji prawnych, tj. takich, które uwzględniałyby przewidziane przepisami RODO możliwości (administrowanie, współadministrowanie, powierzenia przetwarzania). Organ niejednokrotnie wskazywał projektodawcom na konieczność kształtowania przepisów odpowiadających rzeczywistym potrzebom i celom tworzonych regulacji prawnych, odwołując się wprost do przyjętych 7 lipca 2021 r. przez Europejską Radę Ochrony Danych Wytycznych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego. Wskazywał, że na gruncie RODO pojęcie administratora jest pojęciem funkcjonalnym i ma na celu podział odpowiedzialności zgodnie z rzeczywistymi rolami w procesach przetwarzania danych. Oznacza to, że status prawny podmiotu jako administratora musi zasadniczo być określany przez jego rzeczywistą działalność w określonej sytuacji – w tym przypadku projektowaną przepisami i poprzedzoną oceną skutków. Skomplikowane procesy przetwarzania danych mogą też wymagać tworzenia regulacji dotyczących działań więcej niż jednego podmiotu na danych osobowych, podmiotów realizujących różne cele przetwarzania na tych samych danych, jak np. zabezpieczenie procesów przetwarzania danych nierozerwalnie związane z zasilaniem zasobów danymi oraz udostępnianiem danych. Takie sytuacje wymagają, aby przepisy prawa odpowiednio regulowały rolę odrębnych administratorów czy administratorów

146 DOL.401.512.2022.
147 DOL.401.117.2020.

współadministrujących danymi.

Jako przykład opiniowanego przez organ nadzorczy projektu, w którym podział ról podmiotów przetwarzających dane (w powstającym rejestrze) nie został przejrzyście ukształtowany, wymienić można **projekt ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych**[148], który stanowi również przykład chęci odbycia prekonsultacji projektodawcy z organem właściwym do spraw ochrony danych osobowych. W przedstawionej opinii organ nadzorczy wskazał, że projekt – podobnie jak w odniesieniu do Pełnomocnika Rządu do Spraw Osób Niepełnosprawnych – nie precyzuje, na czym miał polegać udział Ministra do spraw zabezpieczenia społecznego w przetwarzaniu danych osobowych w związku z prowadzeniem systemu, tj. jakie cele/zadania/kompetencje miałby ten organ realizować, korzystając z danych zawartych w systemie. Podkreślił, że organy administracji publicznej muszą działać w każdym przypadku na podstawie i w granicach przepisów prawa (konstytucyjna zasada praworządności oraz dotycząca przetwarzania danych osobowych zasada zgodności z prawem, rzetelności i przejrzystości). Niezbędne jest zatem wykazanie oraz wskazanie w przepisach rangi ustawy, jakie konkretne kompetencje (zadania określone, w jakich konkretnie przepisach prawa) realizować będzie minister, korzystając z danych zawartych w tym systemie. Ponieważ planowane przepisy dotyczą kompetencji organów administracji publicznej związanych z przetwarzaniem szczególnych kategorii danych (danych dotyczących zdrowia i niepełnosprawności), należy mieć na uwadze przepisy art. 9 RODO, obligujące do tego, aby przepisy prawa nie tylko regulowały takie przetwarzanie, ale także zapewniały odpowiednie zabezpieczenie praw podstawowych i interesów osoby, której dane dotyczą.

Podobne spostrzeżenia zostały sformułowane w związku z opiniowaniem **projektu ustawy o zmianie ustawy – Prawo budowlane oraz niektórych innych ustaw**[149]**.** Organ zauważył, że w przepisach proponowanego nowego rozdziału Prawa budowlanego nie zostały wystarczająco przewidziane role i sposoby przetwarzania danych osobowych w Systemie do Obsługi Postępowań Administracyjnych w Budownictwie (SOPAB). W konsekwencji nie były w nich wystarczająco zabezpieczone wszelkie prawa i obowiązki organów administracji publicznej prowadzących postępowania administracyjne i będących odrębnymi administratorami w kontekście zapewnienia stosowania przepisów RODO oraz ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[150] dla celów projektowanej regulacji, tj. dla zapewnia prowadzenia postępowań administracyjnych w zakresie procesu inwestycyjno-budowlanego. Nazwanie podmiotu administratorem nie zawsze jest niezbędne, zwłaszcza o ile nie oddaje w pełni ról i sposobów przetwarzania danych osobowych w systemie informatycznym – w tym przykładzie celem wykonania przepisów szczegółowych ustawy Prawo budowlane. Nominalne uczynienie Głównego Inspektora Nadzoru Budowlanego (GINB) administratorem przetwarzanych w SOPAB danych nie może prowadzić do wyłączenia praw i obowiązków wynikających z RODO

148 DOL.401.187.2022.
149 DOL.401.481.2022.
150 Dz.U. z 2021 poz. 2070.

po stronie organów administracji publicznej prowadzących postępowania administracyjne w zakresie procesu inwestycyjno-budowlanego. Nie może też oznaczać, że GINB będzie zastępował te organy w tej roli. Dotyczy to np. realizacji prawa dostępu do danych, prawa do kopii danych, prawa do poprawienia danych – odrębnie jako przetwarzanych w SOPAB i odrębnie jako przetwarzanych dla realizacji celów postepowań prowadzonych przez ww. organy wyspecjalizowanej administracji. W opinii do projektu wskazano, że konieczne jest doprecyzowanie, jakie cele związane z przetwarzaniem danych w ww. systemie będzie realizował GINB[151], a jakie cele będą realizować przetwarzający w ww. systemie dane osobowe inni administratorzy. Będzie to miało zasadnicze znaczenie dla zapewnienia realizacji zasady rozliczalności (art. 5 ust. 2 RODO) przez wszystkich administratorów i wyeliminuje wszelkie wątpliwości na płaszczyźnie proponowanych przepisów w związku chociażby z nadawaniem upoważnień do przetwarzania danych osobowych, odpowiedzialnością za jakość danych, kontrolą procesów udostępniania danych z systemu itd.

Wątpliwości wyrażone przez organ – a dotyczące m.in. konieczności precyzyjnego określenia ról w procesie przetwarzania danych – pojawiły się również w toku opiniowania **ustawy o zmianie ustawy – Kodeks wyborczy oraz niektórych innych ustaw**[152]**.** Dotyczyły one projektowanego przepisu w zakresie funkcjonowania Centralnego Rejestru Wyborców (dalej jako: CRW), który wejdzie w skład Systemu Rejestrów Państwowych, zawierającego: rejestr PESEL, Rejestr Dowodów Osobistych, Rejestr Stanu Cywilnego, Rejestr Danych Kontaktowych, Centralny Rejestr Sprzeciwów, System Odznaczeń Państwowych, Rejestr Dokumentów Paszportowych. Z punktu widzenia ochrony danych osobowych istotne było w ocenie organu określenie ról organów/podmiotów mających dostęp do CRW. Projektowane przepisy wskazywały, że CRW będzie utrzymywany przez ministra właściwego do spraw informatyzacji (przepis ten zawiera otwarty katalog zadań tego organu, co powinno zostać wyeliminowane). Natomiast minister właściwy do spraw wewnętrznych zapewnia funkcjonowanie wydzielonej sieci umożliwiającej dostęp do Centralnego Rejestru Wyborców określonym organom. Projektowane przepisy ustawy nie zawierały definicji pojęcia „sieć" – dlatego w ocenie organu wymagały doprecyzowania w tym zakresie, jak również dookreślenia, czy minister będzie miał dostęp do danych osobowych (a jeśli tak, to na jakich warunkach i w jakim zakresie). Omawiane przepisy nie były również precyzyjne w odniesieniu do organu odpowiedzialnego za aktualizację danych w CRW (projektodawca wskazuje zarówno wójtów, jak i PKW), jak również nie wskazywały sposobu postępowania z danymi osób, które nie mają prawa wybierania. W związku z dostępem tak wielu organów/podmiotów do CRW w opinii do projektu ustawy organ wskazał, że konieczne jest – z punktu widzenia zapewnienia stosowania przepisów RODO, a zwłaszcza zasad wskazanych w art. 5 RODO – precyzyjne przypisanie ról w procesach przetwarzania danych wszystkim mającym dostęp do rejestru. Jak wskazał organ, przypisanie roli administratora

151 Pomocna w tym zakresie co do doprecyzowania celów przetwarzania danych przez GINB może być analiza przepisów ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz.U. z 2022 poz. 1191), rozdział 2: Zakres i zasady rejestracji danych w rejestrze PESEL oraz ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych (Dz.U. z 2022 poz. 197) rozdział 6: Ewidencja wydanych i unieważnionych dokumentów paszportowych i 6a: Udostępnianie danych.

152 DOL.401.512.2022.

ma kluczowe znaczenie w stosowaniu przepisów RODO, ponieważ to administrator jest adresatem licznych obowiązków i praw wynikających z tego aktu prawnego. Przypisanie określonej roli wiąże się z koniecznością wyczerpującego określenia na poziomie ustawy wszystkich celów przetwarzania danych, zadań zobowiązanych lub uprawnionych, praw i obowiązków nierozerwalnie związanych z przetwarzaniem danych osobowych, z którymi przetwarzanie danych wiąże się w sposób bezpośredni lub pośredni. W opinii wskazano, że nie powinno mieć miejsca tworzenie przepisów regulujących odpowiedzialność po stronie stosowanego narzędzia, w tym przypadku systemu, gdyż odpowiedzialność musi być przypisana skonkretyzowanemu podmiotowi praw i obowiązków. Powyższa kwestia jest ciekawym przykładem na rodzaje mankamentów, które w toku opiniowania zauważa organ i które podnosi w pismach kierowanych do projektodawcy.

Przykładem projektu aktu prawnego związanego z koniecznością precyzyjnego określenia ról w procesie przetwarzania danych, jest też **ustawa o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych**[153]. W opinii organ nadzorczy zwrócił uwagę na konieczność dookreślenia w przepisach ról i obowiązków – w odniesieniu do celów przetwarzania, operacji (zestawów operacji) przetwarzania – podmiotów publicznych przetwarzających dane osobowe w związku z powierzeniem realizacji określonych zadań. Na przykładzie tego projektu warto zwrócić uwagę, że przepisy wskazywać powinny w uzasadnionych przypadkach również sposób postępowania z dokumentacją zawierającą dane osobowe (tu: dotyczącą inwestycji), jak i okres (czy okresy) ich przechowywania. W tym kontekście organ zwrócił uwagę, że istotne byłoby określenie okresu przechowywania danych, który uzależniony jest od konieczności realizacji celu, dla jakiego dane osobowe zostały zebrane i mają być przetwarzane. Ponadto zwrócono uwagę na przepisy dotyczące zawiadomienia oraz obwieszczenia, które zawierają numery ksiąg wieczystych, i które mogą zostać zamieszczone w Biuletynie Informacji Publicznej, na stronach internetowych gmin oraz urzędu wojewódzkiego oraz w prasie. Projektodawca nie wskazał okresu, w jakim informacje te mają być upubliczniane, co jest niezgodne z zasadą ograniczenia przechowywania, wynikającą z art. 5 ust. 1 lit. e) RODO. Kluczowym zagadnieniem była też proponowana tym przepisem jawność numerów ksiąg wieczystych, nieprzewidziana w aktualnie obowiązujących przepisach prawa regulujących funkcjonowanie ksiąg wieczystych. Jawne są bowiem – co wynika z przepisów ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece[154] – księgi wieczyste, a dostęp do nich uwarunkowany jest znajomością numeru księgi wieczystej. Projektowany przepis, stanowiąc odstępstwo od zasad dostępu do ksiąg wieczystych wynikających z obowiązujących przepisów, nie precyzuje, czy i jakie dane osób fizycznych będą udostępniane i nie zapewnia tym samym gwarancji związanych z zasadami ochrony danych. W ocenie organu nie powinno mieć miejsca osłabianie ochrony danych osób fizycznych wprowadzane proponowanym przepisem poprzez konstrukcję ujawniania na potrzeby realizacji projektowanej ustawy numerów ksiąg wieczystych jako danych osobowych. Dodatkowo organ nadzorczy zwrócił

153 DOL.401.414.2022.
154 Dz. U. z 2019 r. poz. 2204, z 2021 r. poz. 1177, 1978, z 2022 r. poz. 872, 1374.

uwagę, że projektowane przepisy nie zwierają regulacji odnoszących się do sposobu postępowania z dokumentacją dotyczącą inwestycji ani nie odsyłają do przepisów innych ustaw w tym zakresie. W uzasadnieniu do projektu ustawy projektodawca nie wyjaśnił także przyjętych w tym obszarze rozwiązań. Przepisy tej ustawy, jak wynikało z uzasadnienia, podlegały specjalnej procedurze udzielania zamówień publicznych wyłączającej stosowanie przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych. Wyłączając stosowanie przepisów ww. ustawy (oraz innych ustaw), projektodawca w przepisach ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych powinien takie rozwiązania przede wszystkim szczegółowo uzasadnić, a projektowane przepisy powinny być tak skonstruowane, aby odsyłały do przepisów poszczególnych ustaw. Wątpliwości organu dotyczyły przede wszystkim zgodności przyjmowanych rozwiązań nie tylko z normami konstytucyjnymi, ale również z innymi aktualnie obowiązującymi przepisami krajowymi.

Uwagi dotyczące braku precyzyjnego określenia ról określonych podmiotów w projektowanych przepisach, organ nadzorczy zgłosił również w opinii do **ustawy o zmianie ustawy o Państwowym Ratownictwie Medycznym oraz niektórych innych ustaw**[155]**.** Wątpliwości budziło to, że projektodawca, proponując wprowadzenie nowego podsystemu, nie uwzględnił w nowelizowanych przepisach ustawy o PRM konieczności uregulowania jego funkcjonalności. System ten pełni wiele funkcji, których realizacja oraz cele powinny przekładać się na przepisy materialne ustawy. Dlatego w ocenie organu niezbędna była weryfikacja projektowanych przepisów oraz stosowne uzupełnienia, tak aby zadania i cele administratorów dla przetwarzania danych przy pomocy tego nowo tworzonego podsystemu wynikały wprost z przepisów prawa – biorąc pod uwagę, że system ten będzie przetwarzał dane osobowe, w tym dane szczególnych kategorii (dotyczące zdrowia).

Podobne spostrzeżenia organ wyraził w odniesieniu do **poselskiego projektu ustawy o Państwowej Komisji do spraw badania wpływów rosyjskich na bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej w latach 2007-2022**[156]. Wskazał na niezbędność skorygowania projektu i wprowadzenia zmiany w odpowiednich przepisach, z których jasno będą wynikały zadania określonych w projekcie podmiotów/organów władzy publicznej w zakresie m.in. udostępniania/przekazywania danych na rzecz Komisji, co będzie sprzyjać pełnej realizacji postawionych przed nią zadań. Z tych samych względów w ocenie organu projektodawca powinien dążyć do precyzyjnego i przejrzystego ukształtowania ról podmiotów realizujących poszczególne procesy przetwarzania danych, tak aby w sposób niebudzący wątpliwości z przepisów wynikał zakres realizowanych przez poszczególne podmioty zadań, na których potrzeby przetwarzane są dane osobowe, oraz zakres odpowiedzialności za realizację przypisanych im obowiązków.

W przypadku **projektu rozporządzenia Ministra Zdrowia w sprawie komisji do spraw środka leczniczego dla nieletnich, trybu wykonywania środka leczniczego**

155 DOL.401.532.2022.
156 DOL.401.593.2022.

oraz warunków zabezpieczenia zakładów leczniczych[157] organ z zadowoleniem uznał, że projektodawca zwrócił uwagę na konieczność podejmowania działań mających na celu ochronę danych osobowych zawartych w dokumentacji. Niemniej wskazał, że ze względu na obowiązujące i stosowane bezpośrednio przepisy RODO zamieszczanie klauzul ogólnych w przepisach rozporządzenia, czyli przepisach wykonawczych, jest bezprzedmiotowe, bowiem objęte nimi kwestie dotyczące zasad przetwarzania danych osobowych oraz ról, jakie pełnią określone podmioty w procesie przetwarzania, regulują przepisy o ochronie danych osobowych.

Sformułowane lapidarnie przepisy nie wskazują jasno trybu wyboru oraz powoływania członków komisji, jak również wyboru przewodniczącego oraz jego zastępcy. Obecny kształt przepisów pozwala sądzić, że zgłoszenie kandydata (przedstawiciela) przez określony podmiot polega na wskazaniu konkretnej osoby. Dlatego w ocenie organu nadzorczego wyjaśnienia wymagała kwestia, w jaki sposób i przez kogo dobierani mają być kandydaci do komisji.

7.5. Zbiory danych/łączenie baz danych

Łączenie baz danych, a konkretnie łączenie danych zawartych w zbiorach czy też rejestrach, to również zagadnienie będące przedmiotem szczególnego zainteresowania organu nadzorczego, który w swoich opiniach legislacyjnych zwracał uwagę na związane z tym zagrożenia. Podkreślał, że w tym kontekście istotny jest motyw 31 RODO, zgodnie z którym 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.

Jako przykład należy wskazać na opiniowany projekt **ustawy o przekształceniu Centralnego Ośrodka Informatyki w Agencję Informatyzacji**[158], w którym organ nadzorczy wskazał, że nowo tworzona Agencja Informatyzacji uzyska status organu posiadającego dostęp do rejestrów publicznych: Centralnej Ewidencji Pojazdów, Centralnej Ewidencji Kierowców, Rejestru Danych Kontaktowych, Elektronicznej Platformy Usług Administracji

157 DOL.401.411.2022.
158 DOL.401.444.2022.

Publicznej, Rejestru Dowodów Osobistych, Rejestru PESEL, Rejestru wyborców, Rejestru stanu cywilnego, Rejestru dokumentów paszportowych oraz Rejestru obywateli Ukrainy, którym nadano numer PESEL. Dostęp ten będzie miał również charakter merytoryczny, nie tylko dotyczący spraw związanych z techniczną stroną przetwarzania danych i utrzymaniem systemów. Agencja Informatyzacji przejmie dotychczasowe kompetencje ministra do spraw informatyzacji – minister właściwy do spraw informatyzacji pozostanie jednak nadal wskazany w przepisach regulujących funkcjonowanie ww. rejestrów. W opinii do projektu wskazano, że oprócz kwestii związanych z techniczno-organizacyjną stroną prowadzenia rejestrów publicznych projektowana ustawa zakłada nadanie Agencji Informatyzacji/ Prezesowi Agencji Informatyzacji również licznych uprawnień, które de facto nadają mu status administratora/współadministratora danych. Istotne jest również, że odbywa się to bez stosownych modyfikacji przepisów dotyczących statusu takiego podmiotu.

Organ, analizując projekty aktów prawnych pod kątem łączenia baz danych, wielokrotnie wskazywał na wyrok TSUE C-201/14 w sprawie Smaranda Bara[159], w którym Trybunał orzekł, że odrębne organy w ramach administracji publicznej należy traktować jako odrębnych administratorów z własnymi przesłankami, co w konsekwencji oznacza, że organ, któremu w ramach administracji przekazuje się dane osobowe, jest odbiorcą. Jako przykład wskazać należy na opiniowany w 2022 roku **projekt ustawy o zmianie ustawy – Kodeks spółek handlowych oraz niektórych innych ustaw**[160]. Projektodawca przyjmował w nim – w ocenie organu nadzorczego – rozwiązania, które budziły wątpliwości interpretacyjne, a dotyczyły wykorzystywania przez sąd rejestrowy systemu integracji rejestrów w przypadku, gdy dane identyfikacyjne osoby objętej zapytaniem nie były wystarczające do jednoznacznej jej identyfikacji. W przedstawionej opinii organ podkreślił, że nie jest jasne, czy proponowane rozwiązanie będzie wiązało się z automatycznym przetwarzaniem danych. Analiza obecnego brzmienia tego przepisu dawała podstawę, by sądzić, że projektodawca pozostawił możliwość pozyskiwania informacji ze wszystkich dostępnych rejestrów publicznych, a więc uznać należy, że nie dokonał on oceny projektowanej regulacji pod kątem adekwatności, tj. niezbędności przetwarzanych danych (zasada ograniczenia celu). W ocenie organu pozostawienie przepisu w takim brzmieniu może prowadzić do wielu zagrożeń związanych z łączeniem danych osobowych zawartych w zbiorach danych, w tym będących rejestrami państwowymi. Podkreślono, że niedopuszczalne jest łączenie czy pozyskiwanie przez kolejnego administratora rejestrów administrowanych przez inne podmioty, zwłaszcza dla tak ogólnie sformułowanych celów wykorzystywania zawartych w nich danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

W 2022 r. wznowione zostały, przerwane w 2019 r., prace legislacyjne dotyczące projektu **ustawy o Centralnej Informacji Emerytalnej**[161]. Odnotować należy, że znaczna

159 Wyrok TSUE z dnia 1 października 2015 r. w sprawie C-201/14 Smaranda Bara i in. przeciwko Președintele Casei Națională de Asigurări de Sănătate i in., ZOTSiS 2015, Nr 10, poz. I-638.
160 DOL.401.394.2022.
161 DOL.401.207.2022.

część uwag zgłoszonych przez organ nadzorczy w 2019 r. została uwzględniona w *de facto* nowym projekcie ustawy o Centralnej Informacji Emerytalnej z 2022 r. Jednak wzgląd na rozmiar projektowanej bazy danych, jak i fakt, że w ramach Centralnej Informacji Emerytalnej podlegać będą łączeniu bazy danych wielu podmiotów wypłacających świadczenia z ubezpieczenia społecznego, w opinii organu właściwego w sprawie ochrony danych osobowych obliguje projektodawcę do przeprowadzenia wszechstronnej oceny ryzyk związanych ze stworzeniem i funkcjonowaniem Centralnej Informacji Emerytalnej, wiążących się zarówno z kwestią ochrony praw i wolności osób, których dane osobowe znajdą się w tej megabazie, jak i ochroną tej megabazy przed atakami cybernetycznymi. Organ nadzorczy wskazał przy tym, iż – ze względu na rozmiar i charakter projektowanej megabazy – kwestie dotyczące warunków, sposobu i trybu przekazywania Polskiemu Funduszowi Rozwoju S.A. (administratorowi danych osobowych przetwarzanych w systemie Centralnej Informacji Emerytalnej) danych przez podmioty zobowiązane nie powinny być regulowane w akcie wykonawczym, lecz bezpośrednio w ustawie. Podniósł również zastrzeżenia w odniesieniu do – zaproponowanej w projekcie – konstrukcji powierzenia przez Polski Fundusz Rozwoju S.A. wyspecjalizowanym przedsiębiorcom obsługi technicznej Centralnej Informacji Emerytalnej oraz – także przewidzianej w projekcie – instytucji podpowierzenia, wskazując, że regulujące te instytucje prawne przepisy projektu nie zapewniają należytych gwarancji bezpieczeństwa danych osobowych, które mają być przetwarzane w ramach Centralnej Informacji Emerytalnej. Wątpliwości organu właściwego w sprawie ochrony danych osobowych wzbudziła także szczątkowość unormowań projektu odnoszących się do profilowania.

Innym przykładem ustawy, w toku opiniowania której organ wskazał na wątpliwości w zakresie konstrukcji tworzenia centrów przetwarzania danych osobowych oraz łączenia zbiorów, ze względu na niespełnianie przesłanki przetwarzania danych określonej w art. 6 ust. 1 lit. c) RODO oraz zasady legalizmu z art. 5 ust. 1 lit. a) RODO była **ustawa o zmianie niektórych ustaw w związku z rozwojem e-administracji**[162]. Organ nadzorczy wskazał, że celem uniknięcia ryzyka łączenia zbiorów i baz danych, właściwym rozwiązaniem byłoby wprowadzenie regulacji, które uszczegółowiłyby warunki przetwarzania danych osobowych przez projektowane centra oraz zawierałyby gwarancje dotyczące praw podstawowych i interesów osób, których dane dotyczą. Ponadto organ nadzorczy zwrócił uwagę na przyjęcie w projektowanej ustawie rozwiązań związanych z profilowaniem osoby fizycznej i automatycznym przetwarzaniem danych osobowych. W ocenie organu taka konstrukcja obarczona jest szeregiem ryzyk, które powinny znaleźć odzwierciedlenie w projekcie. Przede wszystkim, zgodnie ze wskazaniem organu, projektodawca powinien jednoznacznie określić, z jakich rejestrów publicznych i systemów teleinformatycznych podmiotów publicznych projektowana w przepisach usługa będzie mogła pozyskiwać dane osobowe w celu profilowania użytkownika korzystającego z usługi. Organ nadzorczy zwrócił także uwagę na rozwiązanie umożliwiające łączenie baz danych i rejestrów w usłudze chmurowej.

162 DOL.401.169.2022.

Szczególne wątpliwości wzbudził ogólnikowy charakter przepisów projektu ustawy w tym zakresie, co podważa zaufanie do przestrzegania zasad dotyczących przetwarzania danych osobowych, zwłaszcza zasad poufności i integralności. W ocenie organu projektodawca powinien ocenić, czy zaproponowane rozwiązania są bezpieczne z punktu widzenia dostępu do danych osobowych szczególnej kategorii, a także do tajemnic prawnie chronionych, a także czy pozwalają na bezpieczne i zgodne z RODO przetwarzanie danych osób fizycznych.

Opiniując projekt **rozporządzenia Rady Ministrów w sprawie zakresu danych i wykazu rejestrów publicznych i systemów teleinformatycznych**, **z których udostępniane są dane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej**[163] organ nadzorczy wskazał, że zawarte w tym projekcie rozwiązania dotyczące przetwarzania danych osobowych na potrzeby analiz w ramach zintegrowanej platformy analitycznej (ZPA) są kluczowe dla systemu ochrony danych osobowych w Polsce i mają istotny wpływ na realizację prawa do prywatności przez osoby, których dane dotyczą. Tymczasem projekt nie tylko nie uzasadniał zmian w fundamentalnych założeniach leżących u podstaw funkcjonowania rejestrów publicznych i zbiorów danych w Polsce, ale wprowadzał rozwiązania sprzeczne z podstawowymi założeniami europejskich przepisów o ochronie danych osobowych. Te europejskie przepisy o ochronie danych osobowych, a zwłaszcza RODO, nakazują podjęcie działań zapobiegających łączeniu zbiorów (zasobów) danych, jak również tworzeniu tzw. megazbiorów, w celu wykorzystywania i nadużywania informacji. Mają też na celu ograniczenie swobody ingerencji państwa w prywatność jednostki i stanowią mechanizmy umożliwiające realizację praw i wolności jednostek w sferze ich życia prywatnego. W tym kontekście organ nadzorczy zarzucił, że przyjęte w projekcie rozwiązania dotyczące przetwarzania danych osobowych na potrzeby analiz w ZPA cechują się ogólnością, niedookreślonością i nieprecyzyjnością, a jednocześnie zakładają przekazywanie ogromnej ilości danych osobowych, na dużą skalę, z bardzo wielu rejestrów i zbiorów (zasobów), w tym danych szczególnej kategorii.

W toku opiniowania projektu **ustawy o zmianie ustawy o Polskim Instytucie Ekonomicznym oraz niektórych innych ustaw**[164] organ nadzorczy wyraził wątpliwości w kwestii poddania danych osobowych jedynie pseudonimizacji, a nie anonimizacji. Przyjęcie takiego rozwiązania, zdaniem organu, nakłada na projektodawcę konieczność obszernego uzasadnienia przyjmowanych rozwiązań, wskazujących w szczególności dlaczego dane poddane anonimizacji nie będą wystarczające do celów analiz. Projektodawca powinien także wskazać szczegółową procedurę pseudonimizacji danych osobowych oraz określić, jakie podmioty będą miały możliwość odwrócenia tego procesu. Wątpliwości organu nadzorczego wzbudziła ponadto konstrukcja łączenia do analiz danych osobowych pozyskiwanych od różnych administratorów, czyli ostatecznie do łączenia informacji z baz danych i rejestrów. Organ nadzorczy zwrócił uwagę na blankietowe sformułowania zawarte w projekcie, które nie dają gwarancji przetwarzania danych osobowych zgodnie z RODO.

163 DOL.401.624.2021.
164 DOL.401.443.2022.

Opiniując powyższy akt organ zwrócił również uwagę na kwestie dotyczące wykorzystanie sztucznej inteligencji do analiz w ZPA. W ocenie organu możliwość gromadzenia i przetwarzania przez narzędzie, jakim jest sztuczna inteligencja, ogromnej ilości informacji będących danymi osobowymi może prowadzić do zwiększonego ryzyka naruszenia prywatności osób. Jak wskazano w opinii temat ten jest przedmiotem szczególnego zainteresowania organów UE z uwagi na ryzyka nie tylko w wymiarze ochrony danych osobowych. Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) 18 kwietnia 2021 r. wydali oświadczenie wzywające do zakazu wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej oraz niektórych innych zastosowań sztucznej inteligencji, które mogą prowadzić do niesprawiedliwej dyskryminacji. Innym istotnym dokumentem dotyczącym omawianego zagadnienia, który wskazano w opinii, jest opublikowana przez Komisję w dniu 19 lutego 2020 r. biała księga w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania. Organ zaznaczył, że wśród innych ważnych aktów, które powinny być brane pod uwagę przez projektodawcę przy tworzeniu założeń funkcjonowania ZPA są również Rezolucja Parlamentu Europejskiego z 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii oraz konkluzje prezydencji z 21 października 2021 r. dotyczące Karty Praw Podstawowych w kontekście sztucznej inteligencji i przemian cyfrowych, w których to dokumentach podkreślano zarówno korzyści, jak i zagrożenia związane ze sztuczną inteligencją, w tym zagrożenia związane z dyskryminacją osób, których dane będą przetwarzane z jej wykorzystaniem.

Zagadnienie związane z tworzeniem baz danych pojawiło się także w toku opiniowania projektu **ustawy o aktywności zawodowej**[165]**.** Organ nadzorczy zwrócił uwagę na problem stworzenia centralnego rejestru danych osobowych osób fizycznych ubiegających się o pomoc określoną w ustawie lub korzystających z tej pomocy oraz innych osób, gdyż, zgodnie z zamysłem projektodawcy, ma ona stanowić scentralizowaną bazę, w której będą przetwarzane w znacznej ilości dane osobowe, w tym dane szczególnych kategorii, przetwarzane dotychczas w odrębnych rejestrach. Opiniując ustawę, organ zwrócił uwagę, że tworzenie tak dużych zbiorów łączących wiele rejestrów w jednej strukturze stoi w sprzeczności z filozofią RODO. Tworzy to również liczne dodatkowe ryzyka w zakresie cyberbezpieczeństwa. Wskazał również, że projektodawca powinien poddać przeglądowi szczegółowe unormowania gwarantujące prawidłowość, integralność i poufność przetwarzanych danych osobowych, a także wyjaśnić i uregulować kwestię ewentualnego automatycznego przetwarzania danych osobowych i profilowania. Podkreślił także konieczność wyjaśnienia i doprecyzowania podziału ról i obowiązków w zakresie administrowania danymi osobowymi. W ocenie organu przepisy projektu nie rozwiewają wątpliwości co do tożsamości i roli administratora. Obawy organu wzbudził również brak doprecyzowania w projekcie ustawy, w jaki sposób starosta będzie weryfikował stan

165 DOL.401.483.2022.

zdrowia bezrobotnego. Kwestia ta, zdaniem organu, wymaga szczegółowego wskazania w przepisach oraz przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych.

Innym przykładem opiniowanego przez organ projektu, który zawierał rozwiązania polegające na łączeniu zbiorów danych jest **ustawa o zmianie niektórych ustaw w związku z rozwojem publicznych systemów teleinformatycznych**[166]**.**

7.6. Korzystanie z nowych technologii przy przetwarzaniu danych osobowych

Zagadnieniem, do którego w 2022 r. najczęściej odnosił się organ nadzorczy w wydawanych opiniach legislacyjnych związanym z bezpieczeństwem przetwarzanych danych, było korzystanie z nowych technologii w procesie przetwarzania danych. Przykładem takiego projektu jest **ustawa o zatrudnianiu cudzoziemców**[167]. W przedstawionej opinii organ nadzorczy zwrócił uwagę na konieczność stworzenia właściwej podstawy prawnej dla „systemu teleinformatycznego pod adresem www.praca.gov.pl". Zwrócono uwagę na konieczność ukształtowania prawidłowych relacji tego systemu z systemem teleinformatycznym umożliwiającym wnoszenie wniosków w postaci elektronicznej do publicznych służb zatrudnienia. Wskazano, że z przepisów rangi ustawy powinny jasno wynikać cele przetwarzania danych osobowych i odpowiednio do tych celów przypisane role w procesach przetwarzania (administratora w przetwarzanych w systemie danych, zakresu jego działań na danych, jak również innych podmiotów uczestniczących w procesach przetwarzania – współadministrowanie, powierzenie). Podkreślono niezbędność wyznaczenia celów przetwarzania, precyzyjnego uregulowania relacji pomiędzy systemami/rejestrami publicznymi, opracowania zamkniętych katalogów danych osobowych przetwarzanych w systemie/systemach, ustalenia okresów przetwarzania w nim/w nich danych oraz stworzenie norm zapewniających adekwatny poziom bezpieczeństwa w systemie teleinformatycznym. Wskazano również, że definiowanie systemów teleinformatycznych przez pryzmat stron internetowych, które umożliwiają do nich dostęp, jest praktyką negatywnie wpływającą na przejrzystość funkcjonowania publicznych systemów teleinformatycznych w Polsce.

Opiniując projekt **rozporządzenia Rady Ministrów w sprawie zintegrowanego systemu informacji o nieruchomościach**[168]**,** organ nadzorczy podniósł, że przy tworzeniu przepisów, które statuują przekazywanie danych osobowych z wykorzystaniem systemów teleinformatycznych, autor takich przepisów powinien mieć świadomość, że ponosi odpowiedzialność za zapewnienie ich zgodności z przepisami RODO. Niepokój organu wzbudziła sytuacja, w której autorem przepisów przewidujących przekazywanie za pośrednictwem rozbudowanego systemu teleinformatycznego znacznej liczby danych osobowych jest podmiot, który nie uznaje stanowisk organu nadzorczego odnoszących się do problematyki ochrony danych osobowych w związku z funkcjonowaniem ksiąg

166 DOL.401.81.2022.
167 DOL.401.484.2022.
168 DOL.401.621.2021.

wieczystych, jak również nie uznaje orzeczeń sądów w tym zakresie. Organ właściwy w sprawie ochrony danych osobowych zwrócił też uwagę na nieprzeprowadzenie przez projektodawcę oceny skutków dla ochrony danych ani oceny ryzyka, jak również naruszenie zasady hierarchiczności systemu aktów prawnych poprzez wprowadzenie do przepisów rozporządzenia unormowań niezgodnych z przepisami ustaw sektorowych kształtujących zasady dostępu do danych zawartych w rejestrze PESEL oraz ewidencji gruntów i budynków. Zastrzeżenia organu nadzorczego wzbudziła też konstrukcja projektu, zgodnie z którą przepisy prawa normujące zasady dostępu do rejestru PESEL czy też ewidencji gruntów i budynków są de facto zastępowane przez rozwiązania stricte informatyczne – „komunikację systemów", co – niezgodnie z zasadą rozliczalności – pozbawia administratorów możliwości kontroli nad danymi osobowymi przekazywanymi z systemów i ewidencji, za które ponoszą odpowiedzialność. Organ właściwy w sprawie ochrony danych osobowych zakwestionował również, użyte w projekcie i niezdefiniowane, pojęcie „certyfikat cyfrowego systemu informatycznego" oraz zażądał doprecyzowania przepisu projektu dotyczącego tworzenia kopii aktualnych zbiorów danych i ich przekazywania Głównemu Geodecie Kraju.

Nowe technologie stanowiły także przedmiot oceny organu w przypadku projektu **rozporządzenia Ministra Klimatu i Środowiska w sprawie infrastruktury sieci domowej**[169]. W toku opiniowania organ zakwestionował brak zachowania odpowiednich gwarancji ochrony danych osobowych, które mogą być wykorzystywane podczas funkcjonowania infrastruktury sieci domowej. Podniósł, że projektowane regulacje nie wskazują, jakie dane będą wykorzystywane do funkcjonowania infrastruktury sieci domowej, jak również, że takich regulacji brakuje w ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne. Tymczasem brak wskazania zakresu danych może spowodować przetwarzanie nadmiernej ilości danych w stosunku do celu, w jakim są one pozyskane. Jako niewłaściwe oceniono także brak wskazania okresu, przez jaki pozyskane dane będą przetwarzane oraz brak przedstawienia informacji, na kogo jest nakładany obowiązek zapewnienia, aby infrastruktura sieci domowej posiadała zabezpieczenia przed nieuprawnioną ingerencją oraz przed nieuprawnionym dostępem do danych pomiarowych i informacji. Podkreślono, że rozwiązanie – korzystanie z infrastruktury sieci domowej, zdalne przekazywanie informacji – może być powiązane również z wykorzystaniem nowych technologii. Jednocześnie wiąże się ono z przetwarzaniem danych osobowych i prowadzi do potencjalnego narażenia na cyberzagrożenia, co generuje ryzyka niekontrolowanego dostępu do danych, niezgodnego z prawem ich przetwarzania w przypadku gdyby doszło np. do ich utraty, zniszczenia, uszkodzenia. Podkreślono, że wprost z przepisów powinno wynikać, jakie ograniczenia/zabezpieczenia powinien zastosować wykonawca tych norm, aby zapewnić odpowiednie zabezpieczenia w kwestii ochrony danych osobowych. Zwrócono też uwagę projektodawcy, że nie przeprowadził testu prywatności w procesie tworzenia prawa – nie uwzględnił kompleksowo ochrony danych w fazie projektowania dla określania sposobów przetwarzania oraz nie wykonał oceny skutków dla ochrony danych w związku z przyjmowaniem podstawy prawnej przetwarzania

169 DOL.401.222.2022.

danych osobowych.

Organ nadzorczy wskazał także na zbyt ogólny charakter przepisu, który dotyczył tworzenia systemu informatycznego w **ustawie o Inspekcji Weterynaryjnej oraz niektórych innych ustaw**[170]**.** Zwrócił uwagę na brak określenia w przepisach zakresu informacji, które mogą być przetwarzane, a także brak informacji o prawach i obowiązkach Głównego Lekarza Weterynarii. Podkreślił, że przepisy dotyczące nowego systemu informatycznego powinny wyczerpująco kształtować prawa i obowiązki osób, których dane będą przetwarzane w tym systemie. Ponadto wskazał, że tworzone przepisy powinny mieć charakter kompleksowy i być prawidłowo umiejscowione w systemie prawa, gdyż związane będą również z przetwarzaniem danych osobowych, w tym potencjalnie danych wrażliwych. W opinii do projektu ustawy zwrócono uwagę, że projektodawca nie przeprowadził testu prywatności w procesie tworzenia prawa oraz nie wykonał oceny skutków dla ochrony danych. Ponadto w stosunku do ustawy o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt zwrócił uwagę na dopuszczenie możliwości przeprowadzenia konsultacji za pomocą środków komunikacji elektronicznej. Wskazał, że minimalne kryteria dla środków i sposobów komunikacji elektronicznej powinny wynikać wprost z ustawy i powinny odpowiadać realizowanym celom regulacji. Określenie wskazanych kwestii w przepisach powszechnie obowiązujących powinno odpowiadać zasadom przetwarzania danych osobowych.

Problematyka dotycząca korzystania z rozwiązań w zakresie nowych technologii w procesie przetwarzania danych pojawiła się także podczas opiniowania projektu **rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie świadczeń gwarantowanych z zakresu ambulatoryjnej opieki specjalistycznej**[171]. Wątpliwości organu nadzorczego wzbudziło niedoprecyzowanie w nim kwestii, w jakich konkretnie systemach teleinformatycznych lub telemedycznych będą przetwarzane dane osobowe pacjentów. Zwrócił uwagę na powinność tworzenia regulacji związanych z realizacją praw i obowiązków dotyczących przetwarzania danych osobowych z wykorzystaniem systemów teleinformatycznych lub telemedycznych w drodze ustawy. Organ zauważył ponadto, że projekt rozporządzenia nie zawiera katalogu danych osobowych, które mogą być przetwarzane w systemie, ani nie wskazuje, jaki podmiot jest odpowiedzialny za przetwarzanie danych. Podkreślił, że konieczne jest określenie ról i obowiązków w odniesieniu do wyraźnie określonych celów przetwarzania i operacji przetwarzania.

Również projekt **ustawy o zmianie ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy oraz niektórych innych ustaw**[172] dotyczył m.in. przetwarzania danych przy wykorzystaniu systemów teleinformatycznych. Organ zwrócił uwagę na konieczność zapewnienia przez projektodawcę zasad przetwarzania, w tym ochrony danych osobowych i prywatności, na każdym etapie tworzenia oraz istnienia technologii obejmującej ich przetwarzanie, a także na wymóg

170 DOL.401.142.2022.
171 DOL.401.234.2022.
172 DOL.401.460.2022.

przeprowadzenia testu prywatności oraz oceny skutków dla ochrony danych. Lakoniczna konstrukcja przepisu, który nie wskazywał na konkretny system ani cel przetwarzania, wymagała wskazania na konieczność doprecyzowania przepisów. Zwłaszcza wszelkie kwestie związane z przekazywaniem lub udostępnianiem danych za pośrednictwem systemów teleinformatycznych powinny być uregulowane w przepisach ustawy. Wątpliwości organu wzbudził także przepis dotyczący Centralnej Informacji Krajowego Rejestru Sądowego oraz udostępniania przez nią danych przy wykorzystaniu systemu teleinformatycznego oraz CEIDG.

W 2022 roku organ właściwy do spraw ochrony danych osobowych kontynuował (prace nad projektem trwały od 2020 r.) opiniowanie projektu **ustawy o Systemie Informacji Finansowej**[173], który zawierał rozwiązania polegające m.in. na wykorzystaniu nowych technologii w procesie przetwarzania danych. Organ podkreślił, że procesy przetwarzania danych dla realizacji zadań wynikających z tej ustawy muszą być także zgodne zarówno z przepisami RODO, jak i dyrektywy 2016/680, implementowanej ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[174]. W ocenie organu, przetwarzanie danych osobowych w ramach Systemu Informacji Finansowej – mimo że wprowadza do porządku krajowego przepisy unijne – będzie nową regulacją w krajowym porządku prawnym (a co za tym idzie, będzie miało do niej zastosowanie RODO). Podkreślono, że aktualność zachowuje zgłaszana wcześniej uwaga organu nadzorczego dotycząca konieczności przeprowadzenia oceny skutków dla ochrony danych ze względu na rodzaj przetwarzania, zwłaszcza następującego przy użyciu nowych technologii, ale także gdy charakter, zakres, kontekst i cele przetwarzania z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób.

Przykładem projektu zawierającego rozwiązania z zakresu nowych technologii, który organ właściwy w sprawie ochrony danych osobowych opiniował w roku 2022 jest **rządowy projekt ustawy o zmianie ustawy o Agencji Restrukturyzacji i Modernizacji Rolnictwa**[175]**.** Prezes UODO wyraził wątpliwości dotyczące tworzenia oprogramowania, aplikacji, dokumentacji systemowej, generowania danych z baz źródłowych na potrzeby zleceniodawców, tworzonego zintegrowanego portalu internetowego – okienka dla rolnika. Wskazał ponadto, że wykonywanie tych działań wiązało się będzie z przetwarzaniem danych osobowych na dużą skalę, pochodzących z różnych źródeł oraz zbiorów (zasobów) danych osobowych, które nie mogą prowadzić do łączenia baz danych. Operacje przeprowadzane na danych osobowych muszą być w pełni zgodne z przepisami RODO. Dlatego organ wnioskował o wskazanie wprost w przepisach rangi ustawy danych osobowych, jakie są przetwarzane w ramach projektowanych systemów, z jakich źródeł (baz) i od jakich administratorów pochodzą, w jakich konkretnie celach są przetwarzane.

173 DOL.401.612.2020.
174 Dz.U. z 2019 r. poz. 125.
175 DOL.401.7.2022.

Opiniując projekt **rozporządzenia Ministra Cyfryzacji w sprawie kontroli korzystania z dostępu do Rejestru Dokumentów Paszportowych**[176]**,** organ nadzorczy zarzucił projektodawcy, że nie objął on ocenianymi regulacjami wszystkich kontroli, do których prowadzenia minister właściwy do spraw informatyzacji jest uprawniony na podstawie ustawy o dokumentach paszportowych.

W następstwie tych uwag projektodawca skorygował projekt w taki sposób, że jego przepisy regulują kwestie wszystkich kontroli przewidzianych w art. 91 ust. 1 ustawy z dnia 27 stycznia 2022 r. o dokumentach paszportowych.

7.7. Przetwarzanie danych szczególnych kategorii

W roku 2022, podobnie jak w latach ubiegłych, organ właściwy do spraw ochrony danych osobowych szczególne zainteresowanie przy opiniowaniu projektowanych przepisów dotyczących przetwarzania danych osobowych skierował na zagadnienia związane z przetwarzaniem danych szczególnych kategorii, w tym m.in. danych dotyczących zdrowia.

Przykładem projektu aktu normatywnego, który przewidywał przetwarzanie danych należących do szczególnych kategorii, jest projekt **ustawy o usprawnieniu procesu inwestycyjnego Centralnego Portu Komunikacyjnego**[177]. Organ zakwestionował propozycję projektodawcy przewidującą, że dla zadania, jakim ma być budowa i utrzymanie Centralnego Portu Komunikacyjnego – miałoby zostać przyznane uprawnienie do przetwarzania nieograniczonego katalogu danych przez nieokreślony okres (również danych sensytywnych, o których mowa w art. 9 ust. 1 RODO), w oparciu o uznaniową decyzję spółki, że są one jej niezbędne do wykonywania zadań, o których mowa w przedmiotowej ustawie. W opinii wskazano, że oparcie przetwarzania na tak blankietowych unormowaniach, bez żadnego ograniczenia katalogu danych osobowych – oprócz wskazanej wcześniej zasady legalizmu – nie może być zaakceptowane ze względu na konieczność poszanowania również zasady minimalizacji danych oraz zasady ograniczenia przetwarzania wynikające z RODO.

Projektodawca jednak – co zostało przez organ pozytywnie ocenione w toku dalszych prac legislacyjnych – uwzględnił większość uwag zgłoszonych do omawianego projektu.

Przetwarzanie danych szczególnych kategorii, dotyczących zdrowia, było przedmiotem projektu **ustawy o wspieraniu i resocjalizacji nieletnich**[178]. Resort sprawiedliwości, który był projektodawcą tych przepisów, dał możliwość pozyskiwania danych szczególnych kategorii małoletnich bez wskazania, jakie konkretnie dane będą pozyskiwane. Organ zwrócił uwagę, że w momencie pozyskiwania danych osobowych, zwłaszcza tych szczególnych kategorii, należy wskazać wprost, jakie dane będą pozyskiwane, w jakim celu, przez jaki okres będą przechowywane oraz w jakim trybie i jakim podmiotom będą ewentualnie udostępniane.

176 DOL.401.55.2022.
177 DOL.401.564.2021.
178 DOL.401.379.2021.

Organ wskazał również, że w projekcie należałoby uwzględnić kwestię dotyczącą obowiązku informacyjnego, który powinien zostać spełniony od razu w momencie pozyskiwania danych, a nie tak, jak przyjął projektodawca, poprzez udostępnienie informacji w Biuletynie Informacji Publicznej lub na stronie internetowej administratora oraz w widocznym miejscu w jego siedzibie. Wskazano również, że należy uwzględnić sytuacje pozyskania danych od osoby trzeciej i spełnienie w tej sytuacji obowiązku informacyjnego wobec osoby, której dane dotyczą, również zgodnie z art. 14 ust. 1 i 2 RODO. Organ zgłaszał uwagi do projektu również na etapie prac sejmowych, jednak nie odniosły one pożądanego rezultatu – projekt pozostawał bez zmian w kwestiach dotyczących danych osobowych i w takim kształcie został uchwalony.

Innym przykładem opiniowanego aktu prawnego odnoszącego się do przetwarzania danych szczególnych kategorii jest projekt **ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych**[179]. Zaproponowano w nim wprowadzenie dużych zmian w zakresie rozszerzenia celu, dla którego realizacji byłyby pozyskiwane dokumenty medyczne zebrane podczas orzekania o niepełnosprawności. W opinii do projektu organ wskazał na konieczność zwiększenia kompetencji lekarzy orzeczników, którzy mieliby dokonywać analizy wydanych orzeczeń. Podkreślono, że projekt nie precyzuje, dla wykonania jakich konkretnie badań zmierzających do podniesienia jakości orzekania (cel ogólny) niezbędne jest wykorzystanie objętych tajemnicą lekarską danych zindywidualizowanych, danych pochodzących z akt konkretnych spraw zakończonych orzeczeniami wydanymi w indywidualnych sprawach. W sytuacji wykorzystania danych, w tym danych szczególnej kategorii, cel ich wykorzystania powinien być wskazany konkretnie, aby nie budził wątpliwości dla wykonawców tych norm oraz dla osób, których dane dotyczą. Użycie ogólnego pojęcia, jakim jest „badanie", w ocenie organu nie było wystarczające. Dodatkowo wskazano, że nie istnieje konieczność przetwarzania wszelkich danych osobowych zgromadzonych podczas orzekania o niepełnosprawności dla realizacji projektowanych przepisów. Ponadto organ zwrócił uwagę, że w projekcie ustawy nie uwzględniono, czy od momentu otrzymania dokumentacji i ewentualnego tworzenia nowych dokumentów – raportów oraz ich przekazania do Pełnomocnika Rządu do Spraw Osób Niepełnosprawnych, wojewódzkie zespoły do spraw orzekania w związku z tą czynnością będą przetwarzać dane osobowe zawarte w przygotowanych przez siebie dokumentach. Projektodawca w ocenie organu nie wykazał niezbędności przetwarzania danych osobowych. W opinii podkreślono, że pozyskanie i dalsze przetwarzanie danych osobowych przez wojewódzkie zespoły do spraw orzekania powoduje, że będą one administratorem tych danych. Organ zwrócił uwagę na kwestię związaną z ustanowieniem obowiązku każdorazowego zasięgania – również bliżej nieokreślonej co do zakresu – opinii Prezesa UODO dla celów przygotowania planu dotyczącego niesprecyzowanych w przepisie analiz, co w ocenie organu wydaje się nadmiarowe. Przepis art. 36 ust. 1 RODO wskazuje możliwość skierowania wniosku o konsultację z organem nadzorczym w sytuacji, kiedy

179 DOL.401.187.2022.

przetwarzanie powodowałoby wysokie ryzyko dla ochrony danych. Wskazano, że nie został określony charakter, jaki miałaby mieć taka opinia i w jakim trybie miałaby być kształtowana w sytuacji, kiedy z przepisów RODO wynika, że zadaniem Prezesa UODO nie jest wydawanie wiążących opinii dla administratorów, chyba że ma to nastąpić w trybie wniosku o uprzednie konsultacje (art. 36 RODO).

Również przypadku projektu **rozporządzenia Ministra Zdrowia w sprawie programu pilotażowego oddziaływań terapeutycznych skierowanych do osób z doświadczeniem traumy oraz ich rodzin**[180], organ nadzorczy zwrócił uwagę projektodawcy m.in. na kwestię dotyczącą nałożenia obowiązków na poszczególne organy lub podmioty przetwarzające szczególne kategorie danych osobowych dotyczących zdrowia z użyciem rozwiązań teleinformatycznych oraz zastosowanie rozwiązania nakładającego prawa i obowiązki na wykonawców norm w drodze rozporządzenia wykonawczego i umów, a nie w drodze ustawy. W projektowanym rozporządzeniu, na co zwrócił uwagę organ nadzorczy, brak było również oceny skutków dla ochrony danych, która jest niezwykle istotna przy przetwarzaniu tak szerokiego zakresu danych i licznego kręgu osób, zwłaszcza z użyciem nowych technologii. W projekcie brak było przepisów dotyczących celu i zasad przetwarzania danych osobowych, a także nie wskazano podmiotów odpowiedzialnych za prowadzenie i uzupełnianie systemu teleinformatycznego.

Warto wskazać, że w 2022 roku resort zdrowia przekazywał organowi nadzorczemu liczne projekty rozporządzeń w sprawie programów pilotażowych, np. **rozporządzenie Ministra Zdrowia w sprawie programu pilotażowego w zakresie świadczeń opieki zdrowotnej zapewnianych przez platformę pierwszego kontaktu oraz centra medycznej pomocy doraźnej**[181]**, rozporządzenie Ministra Zdrowia w sprawie programu pilotażowego w zakresie monitorowania dzieci i młodzieży z pierwotnymi i wtórnymi niedoborami odporności**[182]. W wyniku ich analizy organ wyraził stanowisko, że rozwiązania nakładające prawa i obowiązki związane z realizowaniem programów pilotażowych powinny wynikać z przepisów rangi ustawy, a nie rozporządzeń wykonawczych oraz powinny być zupełne, a tym samym zapewniające stosowanie przepisów, w tym przesłanek legalizujących przetwarzanie szczególnych kategorii danych osobowych, jakimi są dane o stanie zdrowia[183] (art. 9 RODO). Jeżeli poszczególne programy pilotażowe miałyby być kształtowane rozporządzeniami wykonawczymi, to przepisy ustawy powinny określać niezbędne elementy regulacji w odniesieniu do programu pilotażowego w zakresie przetwarzania danych osobowych w ogólności. Organ zaznaczył, że w obecnym stanie prawnym brak

180 DOL.401.278.2022.
181 DOL.401.59.2022.
182 DOL.401.224.2022.
183 Zgodnie z motywem 35 RODO „Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE); numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro”.

jest – wynikającej z przepisów rangi ustawy – podstawy prawnej dla przetwarzania danych osobowych, w tym tych szczególnych kategorii, w toku wykonywania zadań związanych z realizacją programów pilotażowych. Brakuje przepisów ustawowych, które odnosiłby się do praw i obowiązków związanych z przetwarzaniem danych nakładanych na wykonawców i beneficjentów norm – zarówno na świadczeniobiorców, opiekunów świadczeniobiorców, jak i świadczeniodawców, w tym ich pracowników. To w przepisach rangi ustawy w pierwszej kolejności prawodawca powinien wprowadzić odpowiednio (wyczerpująco) skonstruowaną podstawę prawną dla określania przetwarzania szczególnych kategorii danych osobowych, ściśle określając nie tylko cele takiego przetwarzania, ale również wskazując, jakie dane będą gromadzone podczas trwania programu pilotażowego, jak będą przetwarzane na potrzeby leczenia pacjentów i programu pilotażowego, zarówno w czasie jego trwania, jak i po zakończeniu, jak długo będą przechowywane, na jakich zasadach oraz komu i jak ewentualnie udostępniane.

Stanowisko dotyczące przetwarzania danych szczególnych kategorii Prezes UODO zajął również w przypadku poselskiego projektu **ustawy o transparentności finansowania organizacji pozarządowych**[184]. Wskazał, że informacja o darowiźnie dokonanej przez osobę fizyczną na rzecz konkretnej organizacji pozarządowej lub organizacji pożytku publicznego może być uznana za pozwalającą na ustalenie profilu ideologicznego tej osoby, a tym samym może być potraktowana jako dana szczególnej kategorii w rozumieniu art. 9 ust. 1 RODO. Dlatego istnieje konieczność poddania analizie projektowanego w omawianej ustawie modelu upubliczniania danych osobowych, w tym dokonania oceny skutków dla ochrony danych i wykazania zasadności proponowanych rozwiązań. Uwzględnić przy tym należy ryzyka, jakie dla darczyńców będących osobami fizycznymi powstaną w związku z ujawnieniem nieograniczonemu kręgowi podmiotów informacji, że wsparli oni konkretną organizację pozarządową lub organizację pożytku publicznego. Przeanalizować trzeba również konsekwencje, jakie mogą ponieść organizacje, gdyby odmówiły upublicznienia danych swoich darczyńców w sposób i zakresie wskazanym w projekcie.

Przetwarzanie danych szczególnych kategorii stanowiło w 2022 r. również przedmiot analizy i oceny organu nadzorczego w odniesieniu do projektu **rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz przetwarzania danych poprzez Krajowy System Informatyczny (KSI)**[185]**.** W swojej opinii organ nadzorczy podkreślił, że za pośrednictwem Krajowego Systemu Informatycznego będą przetwarzane na dużą skalę dane należące do szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO) oraz dane określone w art. 10 RODO. Obliguje to więc projektodawcę do wprowadzenia wynikających z tych przepisów rozwiązań, gwarantujących odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Cel i specyfika danych osobowych przetwarzanych w KSI generują zaś potrzebę stosowania rozwiązań eliminujących

184 DOL.401.137.2022.
185 DOL.401.452.2022.

zagrożenia nieuprawnionego dostępu do tego systemu. Ponadto wskazano, że ze względu na charakter zaproponowanych zmian prawnych istnieje konieczność przeprowadzenia testu prywatności. Projektodawca powinien wziąć przy tym pod uwagę szereg ryzyk związanych m.in. z możliwością nieautoryzowanego i nieuprawnionego dostępu do danych zawartych w Krajowym Systemie Informatycznym i ewentualną możliwość wytransferowania poza ten system danych, w tym takich, które objęte powinny być szczególną ochroną. Organ w swojej opinii odniósł się również do tworzonych przez projektodawcę ewidencji i wskazał, że uzasadnione byłoby – przez wzgląd na zastosowanie zasady rozliczalności (art. 5 ust. 2 RODO) – doprecyzowanie projektowanego przepisu poprzez wskazanie, że przedmiotowe ewidencje są prowadzone w formie elektronicznej. Powyższa uwaga została przyjęta przez projektodawcę.

Na podwyższony standard ochrony danych osobowych, o których mowa w art. 9 i 10 RODO, organ nadzorczy zwracał uwagę również w toku opiniowania projektu **ustawy o zmianie ustawy o Państwowej Komisji do spraw wyjaśniania przypadków czynności skierowanych przeciwko wolności seksualnej i obyczajności wobec małoletniego poniżej lat 15 oraz niektórych innych ustaw**[186]. Wskazał, że został on wprowadzony dlatego, że przetwarzanie tych danych, jako szczególnie istotnych dla prywatności, wiąże się ze zwiększonym ryzykiem naruszenia praw i wolności osób, których dane dotyczą (podmiotów danych).

7.8. Środki porozumiewania się na odległość

Zagadnieniem, które stanowiło zainteresowanie organu nadzorczego w 2022 roku, było – przez wzgląd na zgodność przyjmowanych rozwiązań z zasadą poufności i integralności – przekazywanie informacji na odległość za pomocą środków komunikacji elektronicznej, zwłaszcza jeśli w ten sposób miałyby być przekazywane dane osobowe.

Opiniując projekt **ustawy o zmianie ustawy o planowaniu i zagospodarowaniu przestrzennym oraz niektórych innych ustaw**[187], organ nadzorczy wskazał, że przyjęcie takiego sposobu przekazywania danych osobowych jest potencjalnie narażone na cyberzagrożenia, wiąże się z ryzykiem niekontrolowanego dostępu w szczególności do danych osobowych, a w konsekwencji niezgodnego z prawem ich przetwarzania. Podkreślił, że przekazywanie danych osobowych powinno odbywać się z zachowaniem zasady integralności i poufności w sposób zapewniający bezpieczeństwo tych danych na odpowiednim poziomie, na zasadach ściśle określonych przepisami ustawy albo z uwzględnieniem wskazanych w przepisach ustawy minimalnych kryteriów zabezpieczających stosowanie wymogów RODO.

Również opiniując projekt **ustawy o Polskiej Agencji Obiektów Sportowych**[188], organ zwrócił uwagę na zapewnienie gwarancji bezpieczeństwa technicznego podczas

186 DOL.401.386.2022.
187 DOL.401.177.2022.
188 DOL.401.406.2022.

posiedzeń Rady Agencji organizowanych z wykorzystaniem środków bezpośredniego porozumiewania się na odległość. Proponowane rozwiązanie w ocenie organu daje możliwość wykorzystywania nowoczesnych technologii pozwalających na odbiór obrazu i dźwięku. Przyjęcie takiego sposobu organizacji posiedzeń Rady Agencji, również z przetwarzaniem danych osobowych, jest potencjalnie narażone na cyberzagrożenia, wiąże się z ryzykiem niekontrolowanego dostępu do danych, niezgodnego z prawem ich przetwarzania, w przypadku gdyby doszło np. do ich utraty, zniszczenia, uszkodzenia. W swojej opinii organ podkreślił, że projektodawca powinien zwrócić uwagę na aspekt kategorii/rodzaju danych, jakie podczas zdalnej organizacji posiedzeń Rady Agencji mogą być przetwarzane (głos, wizerunek, dane osobowe szczególnych kategorii, dla których art. 9 RODO przewiduje szczególny reżim przetwarzania).

Innym przykładem kwestionowanej przez organ regulacji przewidującej wykorzystywania nowych technologii przy przekazywaniu danych na odległość był projekt **rozporządzenia Ministra Zdrowia w sprawie komisji do spraw środka leczniczego dla nieletnich, trybu wykonywania środka leczniczego oraz warunków zabezpieczenia zakładów leczniczych**[189]**.** W swojej opinii organ kwestionował użyte przez projektodawcę pojęcie systemu telewizji wewnętrznej wskazując, że telewizja wewnętrzna nie jest pojęciem tożsamym z systemem urządzeń rejestrujących obraz lub dźwięk (monitoring). Zwrócił też uwagę, że projektowane regulacje nie są spójne z przepisami ustawy, która stawowi delegację ustawową do wydania analizowanego projektu rozporządzenia. Organ podkreślił, że nie można wprowadzać rozwiązań, które w tak bardzo szerokim zakresie ingerują w prywatność, w oderwaniu od przepisów ustawy. Pojawia się więc problem dotyczący różnic w desygnacie zastosowanych pojęć, co może budzić wątpliwości dotyczące niezgodności proponowanego projektu rozporządzenia z przepisami ustawy. Dla organu nie było jasne, czy system telewizji wewnętrznej oznacza przetwarzanie jedynie obrazu, czy też obrazu i dźwięku oraz czy jest to system, który polega na podglądzie w czasie rzeczywistym, a więc bez utrwalania zapisu. Jest to niezwykle istotne także pod względem przetwarzania danych objętych tajemnicą prawnie chronioną, np. tajemnicą lekarską. Jak wskazano w opinii, nie jest również jasny cel, dla którego realizacji zakład leczniczy miałby być wyposażony w system telewizji wewnętrznej.

7.9. Zautomatyzowane przekazywanie danych

Kwestie związane z profilowaniem stanowiły element opinii organu w przypadku projektu **rozporządzenia Ministra Finansów w sprawie korzystania z e-Urzędu Skarbowego**[190]**.** Projekt tworzył ramy prawne dla funkcjonowania systemu teleinformatycznego e-Urzędu Skarbowego, dalej: system e-Urzędu Skarbowego, który będzie służył załatwianiu spraw przez organy Krajowej Administracji Skarbowej (KAS), a także do składania i doręczania pism w sprawach dotyczących wydawania przez organy KAS wiążących informacji

189 DOL.401.411.2022.
190 DOL.401.314.2022.

stawkowych, interpretacji ogólnych i interpretacji indywidualnych oraz innych niż wymienione pism pomiędzy organami KAS a osobami fizycznymi i jednostkami organizacyjnymi. Organ nadzorczy zwrócił uwagę, że zarówno w ustawie o automatyzacji załatwiania niektórych spraw przez KAS, jak i w projekcie analizowanego rozporządzenia nie wskazano, jakie konkretnie podmioty i w jakim zakresie będą użytkownikami konta w e-Urzędzie Skarbowym. Braki takie godzą w zasady dotyczące przetwarzania danych osobowych – legalizmu i przejrzystości (art. 5 ust. 1 lit. a RODO 9) oraz w konstytucyjną zasadę praworządności. Projekt więc w opinii Prezesa UODO powinien zostać rozbudowany o szczegółowe rozwiązania wskazujące, jakie konkretnie podmioty, w jakim zakresie, celu oraz w jaki sposób będą miały dostęp do danych osobowych podatników przetwarzanych w e-Urzędzie Skarbowym. Takimi brakami, wymagającymi uzupełnienia, jest obarczona również ustawa o automatyzacji załatwiania niektórych spraw przez KAS, co w ocenie organu należy przedstawić jako postulat o charakterze *de lege ferenda*. Organ nadzorczy zwrócił również uwagę, że mocą projektowanego aktu w e-Urzędzie Skarbowym mają być załatwiane sprawy polegające na wydawaniu generowanych automatycznie zaświadczeń o niezaleganiu w podatkach lub stwierdzające stan zaległości oraz zaświadczeń o wysokości dochodu osoby fizycznej.

Projektowane w tym zakresie rozwiązania będą się w istocie wiązać z automatycznym przetwarzaniem danych osobowych w systemie e-Urzędu Skarbowego w ramach generowanych automatycznie zaświadczeń. Konstrukcja ta w ocenie organu jest obarczona wieloma ryzykami, na które projektodawca powinien zwrócić uwagę. Podkreślono, że na zagrożenia związane z wykorzystaniem automatycznego przetwarzania danych zwracała też uwagę Grupa Robocza Art. 29 w Wytycznych w sprawie zautomatyzowanego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679 przyjętych 3 października 2017 r. (ostatnio zmienionych i przyjętych 6 lutego 2018 r.). Wytyczne z wyżej wskazanego dokumentu powinny znaleźć – odpowiednie dla realizacji celów przepisów, ale i ryzyk zidentyfikowanych w teście prywatności – odzwierciedlenie w przepisach. Wskazano, że stosowne normy powinny gwarantować właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą zgodnie z art. 22^{191} ust. 2 lit. b RODO. Omawiany projekt powinien zostać rozbudowany o rozwiązania gwarantujące prawidłowość, integralność i poufność przetwarzanych w systemie e-Urzędu Skarbowego informacji zawierających dane osobowe (zapewnienie stosowania zasady poufności i integralności – art. 5 ust. 1 lit. f RODO), a także rozwiązania gwarantujące rozliczalność zastosowanych

191 Zgodnie z art. 22 RODO „1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą."

w systemie e-Urzędu Skarbowego rozwiązań potwierdzających przestrzeganie przepisów ogólnego rozporządzenia o ochronie danych (zapewnienie stosowania zasady rozliczalności – art. 5 ust. 2 RODO[192]).

7.10. Umowy międzynarodowe

Prezes Urzędu Ochrony Danych Osobowych jest też włączany w opiniowanie projektów umów międzynarodowych (są to bowiem źródła prawa dla relacji na poziomie między państwami związane jednocześnie z przetwarzaniem danych osobowych beneficjentów tych relacji). Tak było np. w przypadku **Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Islamskiej Republiki Iranu o współpracy w dziedzinie kultury, edukacji, nauki, sportu, młodzieży i środków masowego przekazu**[193] czy też **projektu Programu współpracy między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Azerbejdżanu w dziedzinie kultury, oświaty i nauki na lata 2022–2026**[194].

Zdarzało się, że przedstawione projekty umów międzynarodowych zawierały już klauzule dotyczące przetwarzania danych osobowych, co organ właściwy do spraw ochrony danych przyjmował z zadowoleniem. Tak było w przypadku projektu **Programu wykonawczego między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Panamy w dziedzinie kultury, edukacji i nauki na lata 2023–2027**[195].

W większości jednak przypadków, opiniując projekty umów międzynarodowych, organ musiał zwracać uwagę projektodawcy na kwestie dotyczące przekazywania danych do państwa trzeciego, wskazując, że może to nastąpić wyłącznie wtedy, gdy są zapewnione odpowiednie zabezpieczenia, i pod warunkiem że zagwarantowane jest egzekwowanie praw osób, których dane dotyczą, i skuteczna realizacja środków ochrony prawnej. Oznacza to, że umowy takie muszą zawierać postanowienia gwarantujące istnienie odpowiednich zabezpieczeń przekazywanych na jej podstawie danych osobowych oraz zabezpieczeń praw osób, których dane te dotyczą. Dodatkowo podkreślał, że jeżeli Umowa nie będzie zawierać odpowiednich klauzul o ochronie danych osobowych, przekazanie do państwa trzeciego będzie musiało odbyć się na podstawie innych przesłanek przewidzianych w przepisach RODO. Najistotniejsze jednak w ocenie organu było poddanie konstruowanych rozwiązań ocenie pod kątem orzeczenia TSUE w sprawie Schrems II [196] w zakresie ważności decyzji KE nr 2010/87, w którym podkreśla się, że podmiot przekazujący dane i podmiot odbierający dane są odpowiedzialni za ocenę, czy w danym państwie trzecim przestrzegany jest stopień ochrony wymagany przez prawo UE, aby ustalić, czy gwarancje udzielone przez standardowe klauzule umowne lub wiążące reguły korporacyjne mogą być przestrzegane

192 Zgodnie z art. 5 ust. 2 RODO administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie.
193 DOL.401.258.2022.
194 DOL.401.12.2022.
195 DOL.401.486.2022.
196 Wyrok TSUE dnia 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi. Sprawa C-311/18 jest kontynuacją wcześniej już rozstrzyganego przez TSUE sporu dot. transferu danych do Stanów Zjednoczonych oraz do innych państw trzecich (por. Wyrok TSUE z dnia 6 października 2015 r. w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner).

w praktyce. Na podstawie wydanego orzeczenia TSUE w sprawie Schrems II, EROD wydała zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych z dnia 10 listopada 2020 r. oraz wytyczne EROD 2/2020 w sprawie art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) RODO dotyczącego przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG z 15 grudnia 2020 r., które mają na celu przedstawienie oczekiwań EROD co do zabezpieczeń, które należy wprowadzić za pomocą prawnie wiążącego i egzekwowalnego instrumentu między podmiotami publicznymi lub pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego za pomocą postanowień administracyjnych między podmiotami publicznymi.

Przykładem umowy międzynarodowej, której projekt nie zawierał klauzul dotyczących przetwarzania danych osobowych, jest **umowa między Rządem Rzeczypospolitej Polskiej a Rządem Ukrainy w sprawie szkół z nauczaniem języka lub w języku polskiej mniejszości narodowej na Ukrainie oraz szkół z nauczaniem języka lub w języku ukraińskiej mniejszości narodowej w Rzeczypospolitej Polskiej**[197].

7.11. Inne projekty aktów prawnych

Blankietowość rozwiązań

Zagadnienia budzące wątpliwości organu nadzorczego pojawiły się na etapie opiniowania **projektu ustawy o zmianie ustawy o ochronie konkurencji i konsumentów oraz niektórych innych ustaw**[198]. Prezes UODO zwrócił uwagę na wprowadzenie instytucji „zakupu towarów i usług z zastosowaniem ukrytej lub przybranej tożsamości". Podkreślono, że rozwiązanie to związane jest z przetwarzaniem danych osobowych kontrolerów Urzędu Ochrony Konkurencji i Konsumentów (UOKiK), czyli szczególnej identyfikacji tych osób na potrzeby przewidywanych czynności. Podkreślono, że projektowane regulacje nie tylko nie mają mieć zastosowania do działań o charakterze operacyjno-rozpoznawczym, ale także w sposób bardzo ogólny odnoszą się do pojęcia „dokumentów publicznych" w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych. W ocenie organu przyjmowane rozwiązania mają charakter blankietowy, ponieważ nie wiadomo, jakim rozwiązaniom podlegać będą dane osobowe zamieszczone w dokumentach, którymi posługiwać się będą kontrolujący z ramienia UOKiK – ustawa o dokumentach publicznych nie reguluje problematyki dokumentów wytwarzanych na potrzeby działań stosowanych z ukrytą lub przybraną tożsamością. Organ podkreślił, że uzasadnione byłoby doprecyzowanie przepisów mających wpływ na prawa i obowiązki wszystkich osób, w związku z przetwarzaniem ich danych osobowych.

Innym przykładem aktów normatywnych zawierających przepisy o charakterze blankietowym są **ustawa o Systemie Informacji Finansowej**[199] oraz **ustawa o zmianie**

197 DOL.401.330.2022.
198 DOL.401.410.2022.
199 DOL.401.612.2020.

ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawy – Prawo telekomunikacyjne[200].

Legalność i celowość rozbudowywania regulacji dotyczących przetwarzania danych osobowych

Uwagę organu nadzorczego wzbudziło – w projekcie **ustawy o zmianie ustawy – Prawo o notariacie oraz niektórych innych ustaw**[201] – rozszerzenie katalogu danych zamieszczonych na liście notariuszy o datę, numer oraz podstawę prawną orzeczenia lub decyzji skutkujących brakiem uprawnień notariusza lub zastępcy notarialnego do wykonywania czynności zawodowych, a także udzielenie Krajowej Radzie Notarialnej kompetencji do udostępniania tych danych publicznie, w tym także za pośrednictwem strony internetowej. W ocenie organu upublicznienie podstaw prawnych zawieszenia notariusza w czynnościach zawodowych będzie jednoznaczne z ujawnieniem, że wobec notariusza prowadzi się postępowanie o umyślne przestępstwo ścigane z oskarżenia publicznego lub umyślne przestępstwo skarbowe albo postępowanie o ubezwłasnowolnienie, lub że toczy się wobec notariusza postępowanie dyscyplinarne. Organ nadzorczy zauważył, że brak jest podstawy prawnej, która umożliwiałaby publiczne informowanie o wszczęciu postępowania karnego toczącego się z urzędu przeciwko funkcjonariuszowi publicznemu. Dodatkowo publikowanie informacji o prowadzeniu postępowania o ubezwłasnowolnienie notariusza, które prowadzić może do wniosku, że u danego notariusza potencjalnie występuje choroba psychiczna lub uzależnienie, podlega szczególnej ochronie, zgodnie z art. 9 RODO. Z tego względu organ nadzorczy wskazał, że upubliczninanie przyczyn, czyli podstaw prawnych zawieszenia, wydaje się nadmiarowe i godzi w zasadę minimalizacji danych. W ocenie organu wystarczające byłoby publiczne wskazywanie wyłącznie informacji o fakcie zawieszenia notariusza w czynnościach zawodowych.

Brak przejrzystości regulacji dotyczących przetwarzania danych osobowych

Opiniując projekt **ustawy o polubownej działalności windykacyjnej i zawodzie windykatora**[202], organ nadzorczy wskazał na brak przejrzystości przepisów dotyczących działalności windykacyjnej. Podniósł m.in., że do wniosku o wszczęcie czynności windykacyjnych dołącza się dokument określający źródło należności mającej być przedmiotem windykacji oraz wyraźne określenie wierzyciela i osoby zobowiązanej. Pojęcie „dokumentu" ma bardzo szeroki charakter i może oznaczać dowolną pisemną informację przekazaną przez domniemanego wierzyciela. Na podstawie takiego „dokumentu" będą mogły być prowadzone daleko ingerujące w prywatność działania windykacyjne wobec osoby, które mogą być ograniczane dopiero następczym sprzeciwem wobec danego przedsiębiorcy windykacyjnego. Zgłoszono postulat, że projektowana ustawa powinna

200 DOL.401.613.2022.
201 DOL.401.514.2022.
202 DOL.401.482.2022.

precyzować, że „dokumentem" są dokumenty urzędowe takie jak tytuły egzekucyjne, które w polskim porządku prawnym dowodzą istnienia danego zobowiązania.

Dane osobowe muszą być przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą, co więc wymaga od projektodawcy tworzenia przepisów, które w sposób jasny będą wskazywały na ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących osobie, której dane będą przetwarzane, organ wskazywał również w opinii do **rozporządzenia w sprawie komisji do spraw środka leczniczego dla nieletnich, trybu wykonywania środka leczniczego oraz warunków zabezpieczenia zakładów leczniczych**[203]. Dla organu ochrony danych z projektowanych przepisów nie wynikał bowiem jasno cel, dla którego realizacji zakład leczniczy miałby być wyposażony w system telewizji wewnętrznej. Nie zostały również przez projektodawcę przewidziane regulacje dotyczące wpływu stosowanych rozwiązań na ochronę prywatności pracowników ww. podmiotów.

Z kolei w projekcie **ustawy o szczególnych rozwiązaniach służących ochronie odbiorców niektórych paliw stałych w związku z sytuacją na rynku paliw**[204] wątpliwości organu nadzorczego wzbudziła baza danych pełnoletnich osób fizycznych zainteresowanych zakupem paliwa stałego na potrzeby własnego gospodarstwa domowego. W swojej opinii wskazał, że jej tworzenie nie spełnia wymogów RODO w zakresie zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO), a przetwarzanie danych osobowych zawartych w tej bazie naruszałoby zasadę ograniczenia celu (art. 5 ust. 1 lit. b RODO). Jednocześnie podkreślił, że skoro – przewidziane w projekcie – rekompensaty mają być wypłacane przedsiębiorcom wykonującym działalność gospodarczą w zakresie wprowadzenia do obrotu paliw, a nie nabywcom paliwa stałego, zaś wypłat tych rekompensat ma dokonywać Zarządca Rozliczeń S.A., a nie minister właściwy do spraw energii, to niejasny jest cel utworzenia i prowadzenia przez ministra właściwego do spraw energii bazy danych pełnoletnich osób fizycznych zainteresowanych zakupem paliwa stałego na potrzeby własnego gospodarstwa domowego.

Ostatecznie, co organ ocenił pozytywnie, projektodawca uwzględnił zgłoszone zastrzeżenia i usunął z projektu przepisy dotyczące bazy danych pełnoletnich osób fizycznych zainteresowanych zakupem paliwa stałego na potrzeby własnego gospodarstwa domowego.

Innym przykładem aktu normatywnego, który zawierał przepisy nieprzejrzyste, jest projekt **ustawy o zmianie ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy oraz niektórych innych ustaw**[205]**.**

Uregulowanie kwestii przetwarzania danych w przepisach wykonawczych, nie zaś w ustawie

203 DOL.401.411.2022.
204 DOL.401.298.2022.
205 DOL.401.460.2022.

Organ właściwy do spraw ochrony danych osobowych, opiniując projekty aktów normatywnych w 2022 roku, zwracał również uwagę na projekty aktów wykonawczych, które regulowały kwestie przetwarzania danych osobowych, a które powinny być zawarte w akcie rangi ustawy.

Przykładem projektu, który w ocenie organu wymagał uregulowania określonych kwestii w ustawie było **rozporządzenie Ministra Sprawiedliwości w sprawie ośrodków kuratorskich**[206]. Projekt aktu nakładał prawa i obowiązki zarówno na sąd, ośrodek kuratorski, kierownika ośrodka jak i osoby związane z osobami przebywającymi w ośrodku rodziców lub opiekunów nieletnich poprzez rozwiązania wskazane w tym akcie m.in. w zakresie posiadania odpowiedniego wykształcenia, (§ 8 ust. 1), dotyczące karalności (§ 8 ust. 2-3), prowadzenia archiwizacji przez sąd (§ 15 ust. 3). Rozwiązania te kształtują funkcjonowanie i działanie ośrodka, niemniej organ poddał pod wątpliwość, czy kwestie te powinny być regulowane przez przepisy wykonawcze, skoro mają być podstawą prawną praw i obowiązków – działań, które wiążą się z przetwarzaniem danych osobowych, zwłaszcza danych szczególnych kategorii i danych z art. 10 RODO.

Błędna terminologia dotycząca administratora

Opiniując projekty aktów normatywnych, organ nadzorczy zwracał uwagę na projekty regulacji, które zawierały błędną terminologię, tj. zamiast pojęcia „administrator danych osobowych" należy konsekwentnie używać pojęcia „administrator" - jako odpowiadającego terminologii RODO i tym samym spełniającemu wymogi zasady zgodności z prawem, rzetelności i przejrzystości. Przykładem projektu, który zawierał w swojej treści ww. błędne odniesienie się do pojęcia „administrator" jest **ustawa – Prawo o ustroju sądów powszechnych**[207] oraz **ustawa o zmianie ustawy o Państwowym Ratownictwie Medycznym oraz niektórych innych ustaw**[208]**.**

Niezamknięte katalogi danych osobowych, rozszerzanie katalogów danych

Proponowany projektem **ustawy o zmianie ustawy – Prawo o ustroju sądów powszechnych oraz ustawy – Prawo o prokuraturze**[209] model przetwarzania danych osobowych dotyczących działalności sądów i pochodzących z wydanych przez nie orzeczeń, oraz dotyczących działalności prokuratury i informacji o sytuacji kadrowej w prokuraturze, jak również konstrukcja przepisów wprowadzająca niezamknięty katalog informacji (potencjalnie danych osobowych), nie spotkał się z aprobatą organu nadzorczego, w którego ocenie treść proponowanych przepisów nie była zgodna z zasadami ochrony danych osobowych wyrażonymi w art. 5 RODO.

206 DOL.401.511.2022.
207 DOL.401.179.2022.
208 DOL.401.532.2022.
209 DOL.401.479.2022.

Wątpliwości organu budził zakres przedmiotowy sprawozdań dotyczących działalności prokuratury oraz to, że projektowane przepisy, także ze względu na to, że potencjalnie dają podstawę przetwarzania danych osobowych, nie stwarzają odpowiednich gwarancji ochronnych, zwłaszcza z punktu widzenia kryterium niezależności prokuratorów (art. 7 ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze) oraz pewności prawa (tego, czy i jakie dane osobowe miałyby być objęte treścią sprawozdań lub informacji, jeśli mają dotyczyć bliżej nieokreślonych kwestii dotyczących funkcjonowania prokuratury i pracy prokuratorów). Przepisy te powinny być skonstruowane tak, by nie stanowiły podstawy do przetwarzania kwestionowanych informacji. W ocenie organu nadzorczego nie znajduje także uzasadnienia rozszerzanie katalogu danych o sędziach, jakie mają się znaleźć w powszechnie dostępnej przestrzeni BIP. Lapidarne jest także uzasadnienie w projekcie zmian w tym zakresie. Decyzja dotycząca zakresu, doboru udostępnianych informacji o charakterze osobowym – ze względu na treść proponowanych regulacji – miałaby charakter wysoce ocenny. Takie dane powinny podlegać ocenie, ale wyłącznie przez organ decydujący o powołaniu sędziego na inne stanowisko. Powyższa zmiana legislacyjna budziła wątpliwości organu z punktu widzenia stosowania wynikających z RODO zasad dotyczących przetwarzania danych osobowych, ze szczególnym uwzględnieniem zasady ograniczenia celu, zasady minimalizacji danych oraz zasady retencji danych/ograniczenia przechowywania. W opinii wskazano, że projektodawca, także w tym zakresie, nie przeprowadził testu prywatności i oceny skutków dla ochrony danych poprzez dokonanie wyważenia między zasadą jawności (wartością jawności życia publicznego) i zasadą prywatności (prawem do prywatności osób pełniących funkcje publiczne). W konsekwencji obowiązek zaprojektowania odpowiednich rozwiązań techniczno-organizacyjnych i ciężar dowodowy wynikający z zasady rozliczalności (art. 5 ust. 2 RODO), polegający na konieczności wykazania przez niego zarówno przed organem nadzorczym, jak i przed podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych, zostałby przerzucony w całości na wykonawców norm (administratorów), a więc właściwych prezesów sądów. Dodatkowo – co organ ocenił negatywnie – projektodawca uznał, że zapewni gwarancje tylko poprzez wyłączenie publikacji (jawności posiedzenia) danych z art. 9 ust. 1 i art. 10 RODO, gdy tymczasem ujawnieniu może podlegać wiele innych danych, tzw. danych zwykłych, także głęboko ingerujących w prywatność osób. Zakres danych ujawnianych na podstawie projektowanych przepisów mógłby być co do zasady nieograniczony. Rozwiązanie to budziło poważne wątpliwości z punktu widzenia standardów zgodności przetwarzania z prawem (art. 6, art. 9 i art. 10 RODO), a także zasad przetwarzania danych osobowych, w tym zwłaszcza: minimalizacji danych, ograniczenia przechowywania/retencji danych, integralności i poufności oraz zasady rozliczalności. Projektodawca ani w treści projektowanych przepisów, ani w uzasadnieniu do projektu ustawy nie zaproponował – odpowiednich do ryzyk towarzyszących transmitowaniu obrad za pośrednictwem Internetu – minimalnych rozwiązań/wymogów (kryteriów, standardów) służących temu, aby realizacja wskazanego rozwiązania regulacyjnego mogła przebiegać w sposób bezpieczny i zgodny z wymienionymi przepisami RODO.

Problem związany z projektowaniem/tworzeniem przepisów prawa zawierających otwarte katalogi danych, które budzą wątpliwości organu ze względu na możliwość przetwarzania na ich podstawie nieograniczonego zakresu danych osobowych, pojawił się również w przypadkach: rządowego projektu **ustawy o zmianie ustawy o przeciwdziałaniu przemocy w rodzinie oraz niektórych innych ustaw**[210], projektu **ustawy o kolejnym w 2022 r. dodatkowym rocznym świadczeniu pieniężnym dla emerytów i rencistów**[211] oraz projektu **ustawy o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych**[212].

W swoich opiniach organ wielokrotnie zatem podkreślał, że tam gdzie jest możliwość stosowania zamkniętych katalogów, projektodawca powinien doprecyzować przepisy tak, aby nie było wątpliwości interpretacyjnych w zakresie praw i obowiązków nakładanych tymi przepisami, zwłaszcza jeżeli katalogi te zawierają dane osobowe (zgodnie z zasadą minimalizacji danych – art. 5 ust. 1 lit. c) RODO).

Przetwarzanie danych osób trzecich

Innym problemem, na który również w 2022 roku zwracał uwagę Prezes UODO, było nadmiarowe przetwarzanie danych osób trzecich. Przez wzgląd na zasadę minimalizacji danych określoną w art. 5 ust. 1 lit. c) RODO i zasadę ograniczenia celu z art. 5 ust. 1 lit. b) RODO wyrażał on swój sprzeciw w projektowaniu takich rozwiązań. Organ podkreślał również, że projektodawca w żaden sposób nie uzasadniał konieczności pozyskiwania takich danych w ocenie skutków regulacji do przedstawianych organowi projektów. Tak było w przypadku nadmiarowego przetwarzania danych: ławnika w projekcie **rozporządzenia Ministra Sprawiedliwości zmieniającego rozporządzenie w sprawie sposobu postępowania z dokumentami złożonymi radom gmin przy zgłaszaniu kandydatów na ławników oraz wzoru karty zgłoszenia**[213], sprawców wykroczeń lub przestępstw stanowiących naruszenia w ruchu drogowym w projekcie **rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie ewidencji kierujących pojazdami naruszających przepisy ruchu drogowego**[214].

Zgoda jako podstawa przetwarzania danych

Odnośnie do tworzenia w przepisach klauzul dotyczących zgody jako podstawy przetwarzania danych organ nadzorczy wypowiedział się, opiniując projekt **rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wniosku o przyznanie świadczenia ratowniczego**[215]. W wydanej opinii wskazał, że stosowanie tego rodzaju klauzul będzie oznaczać, że warunkiem dla realizacji zadania w postaci rozpatrzenia wniosku

210 DOL.401.595.2022.
211 DOL.401.231.2022.
212 DOL.401.414.2022.
213 DOL.401.312.2022.
214 DOL.401.424.2022.
215 DOL.401.96.2022.

i wypłaty, a następnie obsługi świadczenia ratowniczego będzie zgoda osoby, której dane dotyczą, na przetwarzanie danych. Kształtowanie takich rozwiązań narusza art. 7 RODO, z którego wynika jasno, iż cechą zgody jest jej autonomiczność, dobrowolność, a także możliwość swobodnego odwołania w każdym czasie bez negatywnych konsekwencji[216]. 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 (art. 4 pkt 11 RODO). Dlatego organ podkreślił, że wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji[217]. Wskazano również, że o braku dobrowolności świadczy także takie ukształtowanie zgody, jeśli od jej wyrażenia uzależnione będzie wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna[218].

Powierzenie przetwarzania danych na podstawie umowy

Wątpliwości organu budził projektowany przepis **ustawy o zmianie ustawy o finansach publicznych oraz niektórych innych ustaw**[219] pod kątem potencjalnego przetwarzania danych osobowych na podstawie zawartej umowy. W opinii wskazano, że kwestie te powinny być uregulowane w akcie prawa powszechnie obowiązującego rangi ustawy, a nie w umowie (o ile w przedmiotowych umowach zawarte są dane o charakterze osobowym), celem zapewnienia stosowania zasad dotyczących przetwarzania danych osobowych, w tym zasady legalizmu (art. 5 ust. 1 lit. a) RODO), ograniczenia celu (art. 5 ust. 1 lit. b) RODO) oraz zasady minimalizacji danych (art. 5 ust. 1 lit. c) RODO). Ponadto organ podkreślił, że jeżeli miałoby dochodzić do przetwarzania danych osobowych szczególnych kategorii lub o szczególnym charakterze (art. 9 ust. 1 i art. 10 RODO), to dane tego rodzaju poddane muszą być szczególnemu reżimowi przetwarzania, z poszanowaniem warunków wynikających ze wskazanych przepisów, tj. przewidującemu odpowiednie do celu i zakresu regulacji zabezpieczenia praw i wolności osób, których dane dotyczą. Ponadto organ dodał, że wszelkie kluczowe decyzje związane z przetwarzaniem danych osobowych dla realizacji zadań publicznych powinny być określone w przepisach prawa, a nie w aktach pozaustawowych czy umowach.

Przetwarzanie numeru PESEL

Organ nadzorczy w swoich opiniach w 2022 r. zwracał również uwagę na ryzyka, jakie wiążą się z ujawnieniem numeru PESEL w certyfikatach dokumentów podpisywanych

216 Zgodnie z art. 7 ust. 3 RODO „Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie".
217 Motyw 42 RODO.
218 Motyw 43 RODO.
219 DOL.401.202.2022.

elektronicznie. Opiniując projekt **ustawy o aplikacji mObywatel**[220], wyrażał wątpliwości, czy dokument charakteryzujący się unikalnym numerem seryjnym musi zawierać również numer PESEL osoby. Zwracał uwagę, że istotne jest, czy samo imię i nazwisko osoby w połączeniu z numerem seryjnym certyfikatu nie będą wystarczające dla zapewnienia jego funkcjonalności określonych w art. 2 ust.1 pkt 5 projektu ustawy. Wskazywał, że wyjaśnienie tych kwestii jest konieczne dla zapewnienia stosowania zasad dotyczących przetwarzania danych osobowych: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych.

Dalsze obowiązywanie przepisów o charakterze epizodycznym

Organ właściwy do spraw ochrony danych osobowych zwracał uwagę projektodawcy na konieczność wyeliminowania z porządku prawnego rozwiązań, które nie mają charakteru epizodycznego wprowadzonych w czasie pandemii, a które są zbędne/nieadekwatne dla zagwarantowania poszanowania podstawowych praw i wolności osób fizycznych, w tym prawa do ochrony danych osobowych i prawa do prywatności. W swoich opiniach podkreślał, że sytuacja nadzwyczajna jest warunkiem prawnym, który może uzasadniać ograniczenie wolności, pod warunkiem że ograniczenia te są proporcjonalne i ograniczone do okresu nadzwyczajnego. Podnosił także, że dokonanie przeglądu takich aktów będzie zadaniem należącym przede wszystkim do projektodawców i powinno swoim zakresem obejmować nie tylko zagadnienia objęte przepisami **rozporządzenia Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii**[221].

Innym przykładem aktu normatywnego, w opinii do którego organ wskazywał na taki charakter przepisów, jest **rozporządzenie Ministra Zdrowia w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu zagrożenia epidemicznego** oraz **rozporządzenie Ministra Zdrowia w sprawie odwołania na obszarze Rzeczypospolitej Polskiej stanu epidemii.**

Wnioski *de lege ferenda* – zmiany w dotychczas obowiązujących przepisach

W roku 2022 również w toku opiniowania projektów aktów normatywnych organ nadzorczy, po dokonanej analizie, często wskazywał projektodawcom na konieczność zmian, jakie powinno się przeprowadzić w dotychczasowym stanie prawnym, tak aby dostosować obowiązujące już przepisy do standardów wynikających z RODO oraz krajowych przepisów o ochronie danych, czyli na konieczność zmian *de lege ferenda*.

Tak było w przypadku opiniowania projektu **ustawy o zmianie ustawy o Państwowym Ratownictwie Medycznym oraz niektórych innych ustaw**[222] w zakresie stosowanego pojęcia „administrator systemu", który występuje aktualnie w ustawie o Państwowym

220 DOL.401.276.2022.
221 Dz.U. z 2022 r. poz. 340.
222 DOL.401.532.2022.

Ratownictwie Medycznym.

Inny przykład to projekt **rozporządzenia w sprawie komisji do spraw środka leczniczego dla nieletnich, trybu wykonywania środka leczniczego oraz warunków zabezpieczenia zakładów leczniczych**[223]*.* W przedstawionej opinii organ wskazał, że obserwacja pacjenta z wykorzystaniem metod monitorowania jego zachowań jest ściśle związana z jego prawem do poszanowania intymności i godności, zwłaszcza w czasie udzielania świadczeń zdrowotnych, dlatego powinna być również uregulowana w przepisach regulujących materię praw pacjenta – ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta[224], a nie jedynie w ustawie o działalności leczniczej.

7.12. Podsumowanie

Wskazane wyżej zagadnienia nie wyczerpują całego katalogu spraw legislacyjnych, którymi w 2022 r. zajmował się organ nadzorczy. Wśród projektów aktów normatywnych, które wpłynęły do zaopiniowania, były także inne akty, zarówno prawa krajowego, jak i prawa wspólnotowego opiniowane w ramach prac na poziomie Unii Europejskiej nieujęte w niniejszym sprawozdaniu. Wśród zagadnień, które od lat znajdują się w kręgu zainteresowań organu nadzorczego, znajdują się sprawy dotyczące sektora bankowego i ubezpieczeniowego, systemu ochrony zdrowia, sądownictwa czy też organów ścigania.

Analiza projektowanych przepisów oraz wnioski z niej płynące wskazują, że nie zawsze odzwierciedlenie w projektowanych przepisach znajdują przepisy ogólnego rozporządzenia o ochronie danych, w tym zasady dotyczące przetwarzania danych osobowych (art. 5 RODO). Dlatego – biorąc pod uwagę liczne zagrożenia i niebezpieczeństwa związane z przetwarzaniem danych w sposób wychodzący poza standardy wyznaczone przez RODO oraz polskie przepisy o ochronie danych – organ podkreślał konieczność analizy wprowadzanych regulacji, tak aby przepisy te były spójne i w kompleksowy sposób regulowały przedmiotową materię.

W swoich opiniach organ wskazywał, że jego wskazówki mają wyłącznie charakter ekspercki dla projektodawcy (ustawodawcy), który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych.

Dlatego – odwołując się w poszczególnych przypadkach do odpowiednich regulacji RODO i wskazując na potrzebę ponownej analizy propozycji pod kątem zapewnienia stosowania RODO – organ w opiniach legislacyjnych wskazywał na:

1. **Test prywatności** – uwzględnienie ochrony danych w fazie projektowania, (sporadycznie domyślną ochronę danych) oraz ocenę skutków dla ochrony danych

223 DOL.401.411.2022.

224 Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2022 r. poz. 1876 z późn. zm.), dalej: „ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta".

(i prywatności) gdy regulacja dotyczy aspektów wskazanych w art. 35 ust. 1 RODO; test prywatności powinien także wiązać się z: inwentaryzacją zasobów, jakimi są dane osobowe, ich zbiory, rejestry; inwentaryzacją procesów przetwarzania, ich przekształcaniem/zmianą, zwłaszcza z metod tradycyjnych na wymagające użycia nowoczesnych technologii; oceną ryzyk wiążących się z planowanymi operacjami przetwarzania danych – wdrożenie zasad w przyjętych procedurach.

2. **Zasady i warunki wynikające z art. 6, art. 9, art. 10, art. 87 RODO** – w zależności od tego, jakie dane osobowe i dla jakich celów/potrzeb mają być przetwarzane.
3. **Zasady dotyczące przetwarzania danych osobowych** (zgodność z prawem, rzetelność i przejrzystość; ograniczenie celu; minimalizacja danych; prawidłowość; ograniczenie przechowywania; integralność i poufność; rozliczalność zwłaszcza w kontekście złożoności systemu przepisów i konieczności wpisania przetwarzania danych osobowych w procesy regulowane przepisami szczegółowymi; niezbędność uwzględniania tych zasad w stanowionych/zmienianych przepisach krajowych; stanowienie przepisów zapewniających stosowanie tych zasad i przetwarzanie danych z poszanowaniem tych zasad; niemożność stanowienia przepisów negujących/wyłączających zasady/prawa oraz stanowienia przepisów nakładających na administratorów prawa/obowiązki sprzecznie z przepisami RODO; niemożność stanowienia na poziomie krajowym przepisów zaprzeczających regulacji na poziomie prawodawstwa unijnego).
4. **Zasadę zgodności z prawem, rzetelności i przejrzystości** – hierarchia przepisów, podstawa praw i obowiązków z zakresu przetwarzania danych osobowych w akcie wykonawczym zamiast w ustawie; niejasność, zawiłość przepisów; nie zawsze regulacja wyczerpująca, zupełna regulacja; niegwarantująca prawa do pewności; niepełna regulacja praw i obowiązków związanych z przetwarzaniem danych osobowych; brak jasności prawa – dla wykonawców norm jak i dla osób, których dane dotyczą; niezupełność regulacji negatywnie wpływająca na działanie na podstawie i w granicach prawa; Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, przyjęte 29 listopada 2017 r., zmienione i przyjęte 11 kwietnia 2018 r.
5. **Zasadę ograniczenia celu** – przepisy wyraźnie wskazujące cel/cele przetwarzania danych, ale i częsty brak ich wskazania lub brak wyczerpującego wskazania wszystkich celów przetwarzania.
6. **Zasadę minimalizacji danych** – przepisy wyznaczające zakres/kategorie przetwarzanych danych, ale i problematyczne otwarte katalogi, dane wykraczające poza cel przetwarzania, ogólne odesłania do art. 9 ust. 1 – przetwarzanie wszystkich, a nie odpowiednio dobranych i wskazanych szczególnych kategorii danych osobowych; wskazywanie przetwarzania danych z art. 10 oraz niewystarczająco szczególnych warunków dotyczących przetwarzania; bez uwzględnienia w przepisach odpowiedniego

zabezpieczenia praw i wolności osób, których dane dotyczą; przetwarzanie krajowego numeru identyfikacyjnego (w RP głównie numeru PESEL) z uwzględnieniem ryzyk związanych z jego unikalnością/niezmienialnością/referencyjnością.

7. **Zasadę ograniczenia przechowywania/przetwarzania** – często pomijana, brak przepisów wyznaczających okresy przechowywania/przetwarzania danych, co prowadziło do braku jakichkolwiek przepisów w tym zakresie.
8. **Zasadę poufności i integralności** – przepisy dotyczące przetwarzania danych w systemach informatycznych; brak bliższego określenia tych systemów; blankietowe odsyłanie do definicji „systemu informatycznego" z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne; nieadekwatne do konkretnej regulacji odnoszenie się do okoliczności wskazanych w definicji „naruszenia ochrony danych osobowych" (art. 4 pkt 12 RODO).
9. W przypadku projektów obejmujących swym zakresem **wyjątki/ograniczenia przepisów RODO**, wskazujemy na prawidłowe rozumienie i rozróżnienie pojęć wyjątku/ograniczenia, o warunkach z art. 23 RODO dotyczących ograniczeń w przypadku ich stanowienia oraz o Wytycznych 10/2020 w sprawie ograniczeń na mocy art. 23 RODO, Wersja 2.0, przyjętych 13 października 2021 r.
10. Konieczność dostrzegania i wskazywania precyzyjnych przepisów odnoszących się do poszczególnych **ról w procesach przetwarzania danych osobowych** poprzez właściwy kształt (administrowanie, współadministrowanie, powierzenie, podmiot przetwarzający – w tym elementy z art. 28 ust. 3, o ile tworzone przepisy mają być instrumentem prawnym regulującym wykonywanie danych na rzecz administratora); niebezpieczeństwo nieprawidłowego przypisania roli administratora poprzez: bezpośrednie go nazwanie, ale niezgodnie ze stanem rzeczywistym; błędne nazywanie „administratorem systemu" oraz uznawanie, że nie pełni roli administratora; wskazywanie rzeczywistego administratora jako „podmiot zapewniający system/ bezpieczeństwo" celem nieprzypisywania mu roli i odpowiedzialności administratora; nazwanie administratorem z pominięciem innego podmiotu pełniącego również rolę administratora.
11. **Konieczność przypisania celu/celów przetwarzania**, zwłaszcza w powiązaniu z rolami w procesach przetwarzania danych osobowych, zwłaszcza przy tworzeniu przepisów dotyczących obowiązków podmiotów/organów publicznych i konieczność poszanowania art. 6 ust. 3 RODO.
12. Opiniowanie przepisów dotyczących procesu udostępnienia danych przez pryzmat: **analizy ryzyka przyjmowanych rozwiązań; analizy obowiązujących przepisów prawa** – jakie przepisy wiążą podmioty uczestniczące w udostępnianiu/wymianie danych; zastosowanych środków bezpieczeństwa – w jaki sposób, na jakich zasadach udostępnianie/wymieniane będą dane, zważywszy na obowiązki administratorów związanych przepisami RODO, przepisami szczegółowymi; zakresu wnioskowanych

danych – określenie zakresów/kategorii danych, które mają podlegać udostępnieniu/wymianie; trybu przewidzianego w regulacjach odrębnych (np. u.d.i.p.); udostępnianie wnioskowe i bezwnioskowe.

13. **Brak rzetelnego ukształtowania celów i sposobów przetwarzania danych przez określone podmioty**, co sprawia, że trudno jest ustalić status administratorów czy też współadministratorów. Brak przejrzystości przepisów przejawia się następnie w problemach ich interpretacji przez przetwarzających, co nie sprzyja budowaniu wysokich standardów ochrony danych.
14. **Centralizację baz danych**, która jest dużym problemem ze względu na niejasne zakresy odpowiedzialności, które próbuje się budować porozumieniami o współpracy zamiast w aktach rangi ustawy.
15. **Pomijanie Prezesa Urzędu Ochrony Danych Osobowych w procesie opiniowania** lub zbyt późne informowanie o toczących się procesach legislacyjnych, w efekcie czego powstają rozwiązania, które nie tylko nie są przeanalizowane pod kątem zgodności z RODO, ale w praktyce powodują powstanie ryzyka naruszenia zasad ochrony danych (nadmiarowe zbieranie danych, udostępnianie bezwnioskowe bez zachowania gwarancji dla ochrony danych, szczególnie danych wrażliwych itd.).

8. Zgłaszanie naruszeń ochrony danych osobowych

Zadaniem Urzędu realizowanym od 25 maja 2018 r. jest przyjmowanie od administratorów zgłoszeń naruszeń o ochronie danych osobowych, które stwarzają ryzyko naruszenia praw lub wolności osób fizycznych. Uzyskanie przez organ nadzorczy informacji o naruszeniu ochrony danych osobowych pozwala mu na reakcję i może doprowadzić do ograniczenia skutków takiego naruszenia, co przekłada się na zwiększenie poziomu ochrony praw i wolności osób, których dane dotyczą.

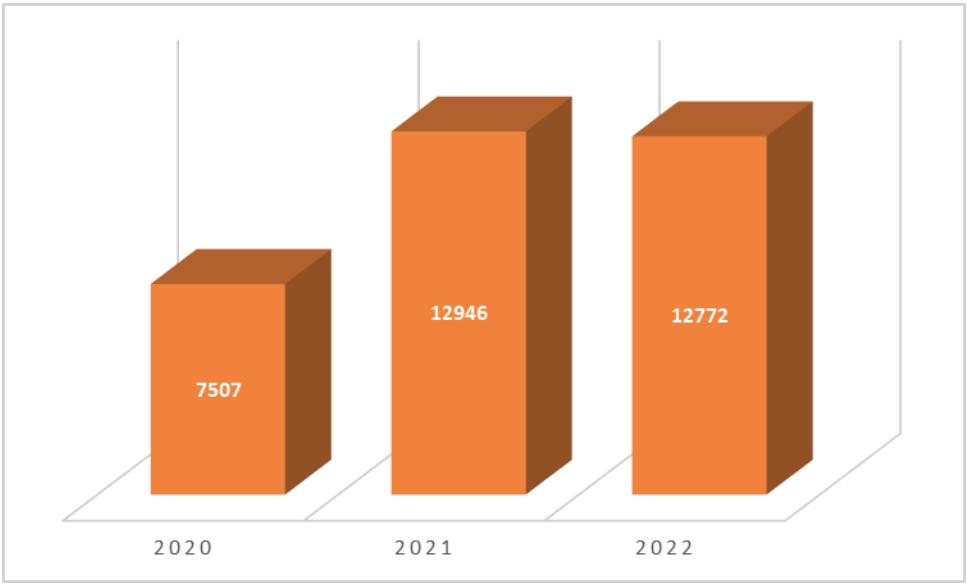
Zgodnie z art. 33 ust. 1 RODO w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości w art. 44 również nakłada na administratorów, w przypadku naruszenia ochrony danych osobowych, obowiązek zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Przepisu nie stosuje się, jeżeli nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych. Natomiast dostawca publicznie dostępnych usług telekomunikacyjnych zawiadamia Prezesa UODO o naruszeniu

danych osobowych w terminie nie późniejszym niż 24 godziny od wykrycia naruszenia danych osobowych, zgodnie z art. 174a ust. 1 prawa telekomunikacyjnego w zw. z art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej.

W celu zapewnienia należytego wywiązania się z tego obowiązku przez administratorów UODO przygotował formularz zgłoszeniowy, który umożliwia każdemu administratorowi nie tylko przekazanie wszystkich niezbędnych informacji określonych w RODO, ale także podanie dodatkowych danych umożliwiających organowi nadzorczemu dokonanie analizy naruszenia pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Dotychczasowa praktyka wskazuje, że w przypadku administratorów zgłaszających naruszenia na zaproponowanym formularzu, ryzyko przekazania niewystarczających informacji jest mniejsze, niż w przypadku naruszeń przesyłanych przez administratorów bez jego użycia.

Zgłaszanie naruszeń przez administratorów stanowi skuteczne narzędzie przyczyniające się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych. Zgłaszając naruszenie organowi nadzorczemu, administratorzy informują Prezesa UODO, czy w ich ocenie wystąpiło wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą oraz – jeśli takie ryzyko wystąpiło – to czy przekazali stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. W uzasadnionych przypadkach mogą również przekazać informację, że powiadomienie w ich ocenie nie jest konieczne ze względu na spełnienie warunków określonych w art. 34 ust. 3 lit. a) i b) RODO. Prezes UODO dokonuje weryfikacji oceny dokonanej przez administratora i może – jeżeli administrator nie zawiadomił osoby – zażądać od niego takiego zawiadomienia. Zawiadomienie osób fizycznych o naruszeniu zapewnia administratorowi możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie osoby te mogą podjąć, aby uchronić się przed potencjalnymi skutkami naruszenia. Administrator ma obowiązek podjęcia skutecznych działań zapewniającym ochronę osobom fizycznym i ich danym osobowym, które z jednej strony pozwolą na kontrolę skuteczności dotychczasowych rozwiązań, a z drugiej – ocenę modyfikacji i usprawnień służących zapobieżeniu nieprawidłowościom analogicznym do objętych zgłoszeniem.

W 2022 r. do Urzędu Ochrony Danych Osobowych wpłynęły **12 772 zgłoszenia naruszeń.** Porównanie liczby zgłoszeń naruszeń ochrony danych osobowych w latach 2020-2022 przedstawia poniższy wykres:



Wykres 10: Liczba naruszeń ochrony danych osobowych, które wpłynęły do UODO w latach 2020-2022.

8.1. Najczęściej zgłaszane oraz typowe naruszenia w 2022 r.

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

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

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

b) udostępnienie danych niewłaściwej osobie

Tego rodzaju naruszenia miały miejsce najczęściej z powodu wydania dokumentów np. zaświadczeń czy deklaracji podatkowych osobom nieposiadającym uprawnień do ich otrzymania. W celu ograniczenia częstotliwości występowania tego typu naruszeń w przyszłości, administratorzy danych podejmowali działania polegające na dyscyplinowaniu pracowników, organizowaniu dodatkowych szkoleń z zakresu ochrony danych osobowych, przeglądzie obowiązujących procedur, a także zwracali się do osób nieuprawnionych o zwrot dokumentów.

c) nieprawidłowa anonimizacja danych lub niezamierzona ich publikacja

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

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

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

e) nieuprawniony dostęp do baz danych

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

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

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

g) zagubienie lub kradzież nośnika danych

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

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

Powodem tych incydentów bezpieczeństwa było wykorzystanie przez osoby specjalizujące się tego typu działaniach, podatności atakowanych systemów informatycznych. Do przełamania zabezpieczeń często przyczyniał się sam administrator danych poprzez wykorzystywanie 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.

8.2. Wyjaśnienia

Zasadniczym uprawnieniem organu nadzorczego, niezbędnym do prawidłowego prowadzenia czynności w następstwie dokonanego zgłoszenia naruszenia ochrony danych osobowych, jest uprawnienie do nakazania dostarczenia informacji przez zgłaszającego. Prawodawca nadaje te uprawnienia Prezesowi Urzędu w art. 58 ust. 1 lit. a) i e) RODO. Korzystając z uprawnień określonych w ww. przepisie, polegających na nakazaniu administratorom, podmiotom przetwarzającym oraz ich przedstawicielom, zapewnienia dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji jego zadań, Prezes Urzędu wystosował do administratorów danych osobowych dokonujących zgłoszeń naruszeń **637 pisemnych wezwań do złożenia wyjaśnień lub udzielił pisemnych informacji w związku z przypadkami naruszeń ochrony danych osobowych.**

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

Adresaci wezwań w zdecydowanej większości przypadków podejmowali działania służące zagwarantowaniu odpowiedniego poziomu bezpieczeństwa danych osobowych i zminimalizowaniu ryzyka ich przetwarzania w sposób niezgodny z przepisami prawa oraz udzielali organowi nadzorczemu oczekiwanych wyjaśnień i informacji. Z analizy przebiegu obsługi zgłoszeń naruszeń ochrony danych osobowych wynika, że realizacja kompetencji Prezesa UODO w trybie art. 58 ust. 1 lit. a) i e) RODO pozytywnie wpływała na ochronę danych osobowych. Znacznie bowiem skracała proces przywracania stanu zgodnego z prawem, pozwalając organowi nadzorczemu na natychmiastowe działanie bez konieczności prowadzenia sformalizowanego postępowania administracyjnego. Podkreślić należy, że cel, jakiemu służy obowiązek zgłaszania naruszeń ochrony danych osobowych i ich kontroli, wymagał wyposażenia Prezesa Urzędu Ochrony Danych Osobowych w instrumenty prawne umożliwiające szybką reakcję na zgłoszenia naruszenia ochrony danych osobowych, tak aby w jak najkrótszym czasie osoby, których dane dotyczą, mogły podjąć działania mające na celu zabezpieczenie się przed ewentualnymi negatywnymi konsekwencjami naruszenia, zaś administratorzy – niezwłocznie zastosować środki bezpieczeństwa w celu ograniczenia rozmiaru naruszenia i w konsekwencji wyrządzonych szkód.

8.3. Postępowania administracyjne

W 2022 roku Prezes Urzędu **wszczął z urzędu 59 postępowań administracyjnych** w sprawie naruszenia przepisów o ochronie danych osobowych. W niektórych przypadkach podjęta została decyzja o przeprowadzeniu u administratora danych kontroli przestrzegania przepisów o ochronie danych. Zastrzeżenia Prezesa Urzędu w związku ze zgłoszonymi naruszeniami ochrony danych osobowych, które wymagały przeprowadzenia postępowania administracyjnego, dotyczyły w szczególności:

a) przeprowadzonej przez administratorów danych oceny ryzyka naruszenia praw lub wolności osób fizycznych, skutkującej koniecznością zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia osób, których naruszenie to dotyczyło;

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

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

d) sposobu realizacji przez podmiot przetwarzający postanowień umowy powierzenia przetwarzania uwzględniającej kryteria zawarte w art. 28 ust. 3 RODO, w szczególności dotyczące spełniania obowiązku przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, podejmowania wszelkich środków wymaganych na mocy art. 32 RODO oraz – po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych – usuwania lub zwracania administratorowi wszelkich danych osobowych i usuwania wszelkich ich istniejących kopii[225],

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

225 Art. 28 ust. 3 lit. a), c) i g) RODO.

8.4. Decyzje administracyjne

W wyniku prowadzonych przez Prezesa Urzędu postępowań administracyjnych, które zostały zakończone w 2022 roku, wydano dwadzieścia pięć (25) decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych. W szesnastu (16) decyzjach Prezes UODO udzielił upomnienia administratorowi danych, w tym w pięciu (5) decyzjach udzielił upomnienia i nakazał dostosowanie operacji przetwarzania do przepisów RODO poprzez: przeprowadzenie analizy ryzyka w celu oszacowania właściwego poziomu ryzyka wiążącego się z przetwarzaniem danych osobowych, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, uwzględniając stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, w tym zagrożenia związane z zainstalowaniem złośliwego oprogramowania ingerującego w dostępność danych oraz zagrożenia w postaci braku możliwości odtworzenia danych z kopii zapasowej w razie wystąpienia incydentu technicznego lub fizycznego oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania oraz wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. W przypadku dziewięciu (9) naruszeń Prezes Urzędu Ochrony Danych Osobowych, po przeprowadzeniu postępowań administracyjnych w wydanych decyzjach administracyjnych, zdecydował się nałożyć na administratorów danych administracyjne kary pieniężne, których przykłady przedstawione zostały w rozdz. 9 niniejszego Sprawozdania.

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

Prezes Urzędu Ochrony Danych stwierdził naruszenie przez Zakład Ubezpieczeń Społecznych[226] przepisów RODO polegające na niewdrożeniu, w procesie obsługi wysyłki korespondencji zawierającej deklaracje PIT, odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych oraz służących zapewnieniu, aby dane osobowe ubezpieczonych przetwarzane w ramach ww. procesu, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. W związku ze stwierdzonym naruszeniem Prezes UODO udzielił upomnienia i nakazał Zakładowi Ubezpieczeń Społecznych wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych i służących zapewnieniu, aby dane osobowe ubezpieczonych przetwarzane w ramach procesu obsługi wysyłki deklaracji PIT, które są nieprawidłowe w świetle celów ich przetwarzania, zostały

226 Sygn. akt. DKN.5131.19.2021.

niezwłocznie usunięte lub sprostowane. Naruszenie polegało na wysyłaniu korespondencji (zawierającej wypełniony druk PIT) na niewłaściwe (nieaktualne) adresy, przez co osoby nieuprawnione mogły uzyskać dostęp do danych osobowych zawartych w korespondencji. Z analizy naruszeń objętych przedmiotowym postępowaniem wynikało, że do wysyłki druków PIT na błędny adres dochodziło z powodu nieuwzględnienia zgłoszeń aktualizujących adres dokonanych w okresie poprzedzającym wysyłkę druku PIT (najczęściej – lecz nie zawsze – już po wygenerowaniu deklaracji). Administrator nie wprowadził rozwiązań służących zapewnieniu integralności (poprawności) danych adresowych – a w konsekwencji poufności danych objętych drukami i wysyłanych na błędne adresy – na każdym etapie funkcjonowania tego systemu (co wymaga realizowanej na bieżąco i na każdym jego etapie weryfikacji poprawności danych adresowych klientów). Z zebranego w sprawie materiału dowodowego wynikało, że administrator miał świadomość, iż może dochodzić do naruszeń wynikających z tego, że w okresie pomiędzy wygenerowaniem przez administratora druku PIT – z uwzględnieniem adresu korespondencyjnego aktualnego na ten moment (moment generowania druku) a jego wysyłką, realizowany jest w zwykłym trybie proces aktualizacji danych adresowych na podstawie kierowanych różnymi kanałami wniosków, przy czym zmiany te (aktualizacje adresów), nie były uwzględniane w ramach wysyłki wygenerowanych już druków (druki były zatem wysyłane na adresy nieaktualne). Materiał dowodowy przedmiotowej sprawy dawał podstawy do stwierdzenia, że ZUS nie tylko miał świadomość istnienia omawianego ryzyka i godził się na nie, lecz przyjął, że jego wyeliminowanie – z uwagi na skalę procesu – leży poza zakresem jego możliwości. Zatem pomimo zidentyfikowania omawianego zagrożenia, administrator nie podjął działań ukierunkowanych na wyeliminowanie bądź zminimalizowanie ryzyka jego zaistnienia. Tym samym nie została zapewniona odpowiednia ochrona danych osobowych ubezpieczonych. Mimo skali działalności tj. ilości wysyłanej korespondencji zawierającej druk PIT i cyklicznego charakteru tej wysyłki (powtarzanej co roku), stanowiącej istotny czynnik z punktu widzenia oceny ryzyka i oczekiwanych od administratora środków bezpieczeństwa, administrator nie wprowadził ani też nie zaplanował możliwych środków bezpieczeństwa służących zminimalizowaniu ryzyka ponownego wystąpienia naruszenia.

W kolejnej sprawie Prezes Urzędu Ochrony Danych Osobowych stwierdził naruszenie polegające na zgłoszeniu naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych po upływie terminu wynikającego z art. 33 ust. 1 RODO tj. 72 godzin od stwierdzenia naruszenia i udzielił upomnienia pracodawcy[227]. Naruszenie bezpieczeństwa dotyczyło przełamania zabezpieczeń informatycznego systemu obsługi kadrowo – księgowej u podmiotu przetwarzającego. Dokonując zgłoszenia administrator nie wskazał jednakże powodów opóźnienia powiadomienia organu nadzorczego. Nie odpowiedział też na wezwanie Prezesa UODO do złożenia wyjaśnień w tej kwestii. Dopiero kolejne wezwanie spowodowało, iż administrator wskazał, z jakiego powodu nie dokonał zgłoszenia naruszenia w obowiązującym terminie. Uzasadniając dokonanie ww. zgłoszenia

227 Sygn. akt. DKN.5131.46.2021.

naruszenia ochrony danych osobowych po upływie terminu wynikającego z ww. przepisu RODO, administrator podał, że podmiot przetwarzający zgłosił naruszenie ochrony danych osobowych Prezesowi UODO, w związku z czym uznano za wystarczające zgłoszenie naruszenia przez podmiot, w systemie którego doszło do naruszenia. Prezes UODO w uzasadnieniu decyzji stwierdził, że wynikający z art. 33 ust. 1 RODO obowiązek dokonania zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu spoczywa wyłącznie na administratorze. Powyższe oznacza, że to pracodawca, jako administrator danych osobowych swoich pracowników, po stwierdzeniu wystąpienia naruszenia ochrony danych osobowych, był zobligowany do dokonania jego zgłoszenia z zachowaniem terminu określonego w RODO. Ponadto administrator wskazał także, że nie zgłosił naruszenia w wymaganym terminie, ponieważ nie miał jeszcze wszystkich informacji niezbędnych do wypełnienia zgłoszenia od podmiotu, w którego systemie nastąpiło naruszenie. Stosownie do art. 33 ust. 4 RODO, jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki. Zatem wyjaśnienia administratora o braku posiadania wszystkich informacji nie mogą uzasadniać zgłoszenia naruszenia organowi nadzorczemu po upływie ponad miesiąca od jego stwierdzenia, tym bardziej że takie zgłoszenie może być dokonywane etapami, w miarę jak administrator uzyskuje kolejne informacje dotyczące zaistniałego naruszenia. W tym miejscu podkreślić również należy, że formularz zgłoszenia naruszenia ochrony danych osobowych opracowany przez Prezesa UODO przewiduje sytuacje, w których administrator może nie posiadać pełnych informacji dotyczących zaistniałego zdarzenia. We wspomnianym formularzu istnieje bowiem możliwość wskazania, iż administrator dokonuje wstępnego zgłoszenia naruszenia, które zostanie przez niego uzupełnione po ustaleniu brakujących informacji.

W związku z przeprowadzonym postępowaniem wyjaśniającym w sprawie zgłoszonego przez komendanta miejskiego policji naruszenia ochrony danych, polegającego na przesłaniu za pośrednictwem wewnętrznej poczty służbowej nieprawidłowo zanonimizowanego wyroku WSA do wszystkich komórek i jednostek organizacyjnych komendy miejskiej policji (KMP), Prezes UODO zdecydował o wszczęciu postępowania administracyjnego. Nieprawidłowa anonimizacja umożliwiła odczytanie danych osobowych funkcjonariusza, którego wyrok dotyczył, w zakresie jego imienia, nazwiska, stopnia służbowego, zajmowanego stanowiska, adresu zamieszkania lub pobytu oraz okresu przebywania na zwolnieniu lekarskim z powodu choroby. Przedmiotem postępowania organ uczynił możliwość naruszenia przez administratora danych przepisów art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1 i 2, art. 32 ust. 1 i ust. 2, art. 34 oraz art. 38 ust. 1 RODO, w związku z naruszeniem ochrony danych osobowych funkcjonariusza Policji. Z uwagi na fakt, iż naruszenie polegało na udostępnieniu danych osobowych funkcjonariusza policji w nieprawidłowo zanonimizowanym wyroku przesłanym do załogi KMP, a nie z zadań własnych Policji, sprawa została rozstrzygnięta w oparciu o przepisy RODO, a nie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Zdaniem Prezesa UODO administrator danych nie testował, nie mierzył i nie oceniał skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych. Tym samym dopuścił się także naruszenia art. 32 ust. 1 lit. d) RODO, a w konsekwencji art. 5 ust. 2 RODO. Administrator nie wykazał bowiem, pomimo iż został do tego zobowiązany pismem organu, aby w KMP miało miejsce regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, których naruszenie dotyczy. Podnieść należy, że wskazane testowanie, mierzenie i ocenianie, aby stanowiło realizację wymogu wynikającego z art. 32 ust. 1 lit. d) RODO, musi być dokonywane w sposób regularny, co oznacza świadome zaplanowanie i zorganizowanie, a także dokumentowanie (w związku z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO) tego typu działań w określonych przedziałach czasowych, niezależnie od zmian w organizacji i przebiegu procesów przetwarzania danych.

Prezes UODO ponadto zarzucił administratorowi brak domyślnej ochrony danych osobowych już na etapie projektowania, tj. od momentu, gdy podjęto decyzję o zastosowaniu środka techniczno-organizacyjnego w postaci anonimizacji, jak również w fazie procesu polegającego na udostępnieniu wyroku z nieprawidłowo zanonimizowanymi danymi funkcjonariusza KMP. Natomiast anonimizacja wyroku sądowego za pomocą markera, naświetlonego następnie podczas skanowania (umożliwiająca odczytanie zamazanych danych) oraz brak weryfikacji poprawności wykonanej anonimizacji zeskanowanego wyroku przed jego dalszym udostępnieniem, świadczy o niezastosowaniu przez administratora danych domyślnej ochrony danych – na żadnym etapie ww. procesu. Powyższe działanie stanowi naruszenie art. 25 ust. 2 RODO w związku z art. 5 ust. 1 lit. f) oraz art. 5 ust. 2 RODO. Administrator danych nie był w stanie bowiem wykazać zastosowania domyślnej ochrony w ww. procesie.

Prezes UODO, zarzucił administratorowi również błędy w przeprowadzanej analizie ryzyka naruszenia praw lub wolności osoby objętej naruszeniem. Nieprawidłowo przeprowadzona analiza tego ryzyka spowodowała, że administrator zaniżył wartości, a to doprowadziło do tego, że nie zawiadomił, stosownie do art. 34 RODO, osoby, której dane zostały objęte naruszeniem. Takie postępowanie administratora spowodowało konieczność podjęcia przez Prezesa UODO, na podstawie art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz art. 34 ust. 4 RODO, działań polegających na dwukrotnym skierowaniu do Komendanta wystąpienia w sprawie zawiadomienia osoby fizycznej o przedmiotowym naruszeniu. Administrator danych zawiadomił osobę fizyczną o naruszeniu, stosownie do art. 34 ust. 1 i 2 RODO, w sposób prawidłowy dopiero za drugim razem.

9. Administracyjne kary pieniężne

Stosownie do art. 58 ust. 2 lit. i) RODO, Prezesowi UODO przysługuje uprawnienie do zastosowania administracyjnej kary pieniężnej, oprócz lub zamiast innych środków naprawczych, zależnie od okoliczności konkretnej sprawy. W oparciu o art. 210a Prawa telekomunikacyjnego[228], Prezes UODO uprawniony jest do nakładania administracyjnych kar pieniężnych za naruszenie niektórych obowiązków przewidzianych przepisami tego aktu prawnego.

W 2022 r. Prezes UODO skorzystał z uprawnienia do zastosowania administracyjnej kary pieniężnej w dziewiętnastu sprawach, nakładając na **dwadzieścia podmiotów** administracyjne kary pieniężne w łącznej kwocie **7 850 861 zł**. W porównaniu z rokiem poprzednim oznacza to wzrost ilościowy o dwie kary i blisko 3,5-krotny wzrost wartości nałożonych kar. Dla porównania, w 2021 r. orzeczonych zostało osiemnaście administracyjnych kar pieniężnych na łączną kwotę 2 288 007,50 zł.

Podobnie jak w roku 2021, jedna kara nałożona została na podstawie przepisów Prawa Telekomunikacyjnego, pozostałe orzeczone zostały za naruszenie przepisów RODO. Spośród dwudziestu ukaranych podmiotów pięć należało do sektora finansów publicznych, natomiast wśród pozostałych piętnastu podmiotów prywatnych, jedenaście to spółki prawa handlowego, a cztery to osoby fizyczne (w tym prowadzące działalność gospodarczą i wspólnicy spółki cywilnej).

Przedstawiając w ujęciu statystycznym działania podmiotów ukaranych z jednej strony, a z drugiej – działania Prezesa UODO w odniesieniu do orzeczonych w omawianym okresie 2022 roku administracyjnych kar pieniężnych, wskazać należy, że:

1) **dziewięć** administracyjnych kar pieniężnych o łącznej wysokości **7 665 259 zł** zaskarżonych zostało przez ukarane podmioty do Wojewódzkiego Sądu Administracyjnego w Warszawie, z czego:
   a) w dwóch przypadkach skargi zostały oddalone przez Wojewódzki Sąd Administracyjny w Warszawie[229];
   b) dwie kary zostały uchylone przez sąd; w obu przypadkach skargę do Naczelnego Sądu Administracyjnego złożył Prezes UODO[230];
   c) w odniesieniu do pięciu administracyjnych kar pieniężnych trwa postępowanie[231].
2) **dziesięć** decyzji nakładających administracyjne kary pieniężne w łącznej kwocie **158 184 zł** uprawomocniło się w związku z niezaskarżeniem ich przez strony do sądu administracyjnego. Spośród tych kar:
   a) pięć kar zapłaconych zostało dobrowolnie przez ukarane podmioty[232];

228 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2022 r. poz. 1648 z późn. zm.).
229 DKN.5131.33.2021, DKN.5131.51.2021.
230 DKN.5130.2215.2020 (dwie administracyjne kary pieniężne nałożone w jednym postępowaniu).
231 DKN.5110.12.2021, DKN.5131.18.2022, DKN.5112.1.2020, DKN.5112.5.2021, DKE.561.30.2022.
232 DKN.5131.27.2022, DKN.5131.34.2021, DKE.561.5.2022, DKN.5131.29.2022, DKN.5131.8.2022.

b) jedna kara wyegzekwowana została w efekcie wszczęcia egzekucji należności pieniężnych[233];

c) w odniesieniu do dwóch kar wszczęta została i jest kontynuowana egzekucja należności pieniężnych[234];

d) dwie kary na koniec okresu sprawozdawczego oczekiwały na wszczęcie egzekucji należności pieniężnych[235].

3) **jedna** kara w wysokości **27 418 zł** była na koniec okresu sprawozdawczego nieprawomocna – nie upłynął termin na wniesienie przez ukarany podmiot skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie[236].

Jak już była o tym mowa w rozdziale 6 dotyczącym egzekucji administracyjnej, zadania związane z zapewnieniem wykonania przez zobowiązanych obowiązków wynikających z decyzji administracyjnych Prezesa UODO, są w Urzędzie Ochrony Danych Osobowych realizowane w Departamencie Kar i Egzekucji. W odniesieniu do wszystkich administracyjnych kar pieniężnych nakładanych przez Prezesa UODO, departament ten pełni funkcję koordynującą i monitorującą – do jego zadań należy zapewnienie spójności ich orzekania w ramach Urzędu i w ramach systemu europejskich organów nadzorczych, a także zapewnienie ich zgodności z wytycznymi Europejskiej Rady Ochrony Danych.

Do kompetencji Prezesa Urzędu Ochrony Danych Osobowych należy ponadto – w zakresie uprawnień Prezesa UODO do orzekania o sankcjach finansowych – **nakładanie administracyjnych kar pieniężnych o szczególnym 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[237].

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.

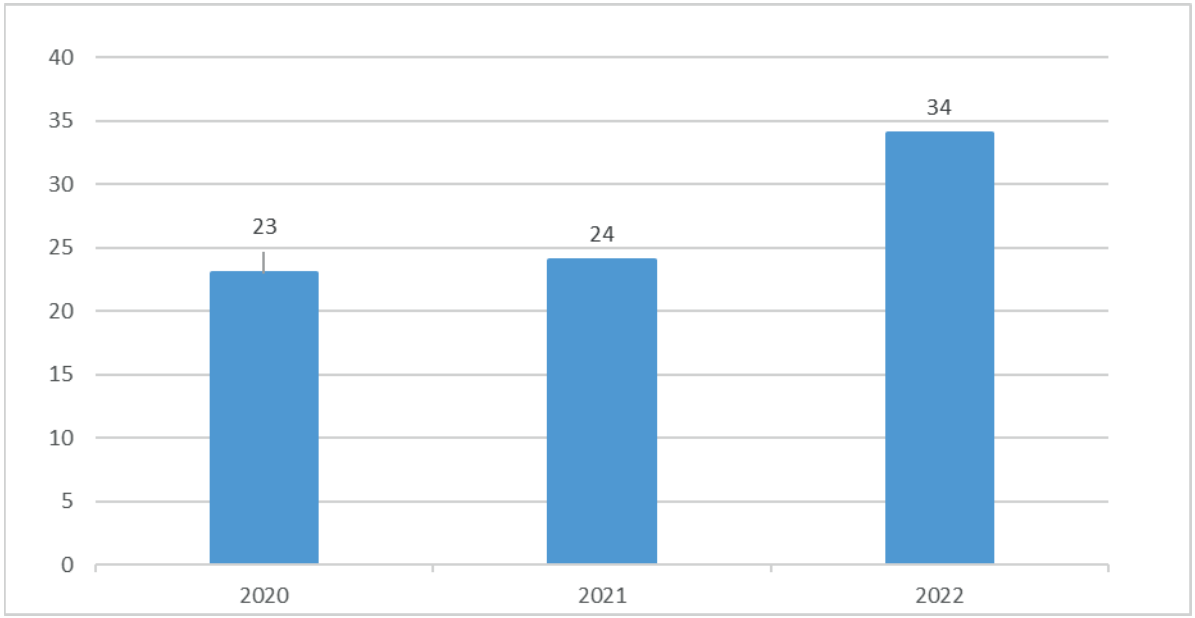
233 DKE.561.18.2021.
234 DKE.561.23.2021, DKE.561.25.2021.
235 DKE.561.6.2021, DKE.561.15.2021.
236 DKE.561.20.2022.
237 Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t.j. Dz. U. z 2022 r. poz. 479 z późn. zm.).

Natomiast na administratorów i podmioty przetwarzające nałożone zostały, skorelowane z uprawnieniami organu nadzorczego, określone obowiązki, w tym obowiązek współpracy z organem nadzorczym (art. 31 RODO) oraz obowiązek zapewnienia organowi nadzorczemu dostępu do informacji niezbędnych do realizacji jego zadań (art. 58 ust. 1 lit a) i e) RODO).

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

W związku z powyższym, w celu zdyscyplinowania stron postępowań do prawidłowego wypełniania obowiązków procesowych, Prezes UODO wszczął w 2022 r. z urzędu **34 postępowania** w przedmiocie nałożenia administracyjnej kary pieniężnej za tego rodzaju naruszenia. Oznacza to wzrost o 42% w stosunku do poprzedniego okresu sprawozdawczego, w którym tego rodzaju postępowań wszczętych zostało 24.

Porównanie liczby wszczętych w 2022 r. postępowań w przedmiocie nałożenia kary za brak współpracy z Prezesem UODO i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań, z liczbą tego rodzaju postępowań zainicjowanych w poprzednich okresach sprawozdawczych, przedstawia poniższy wykres.



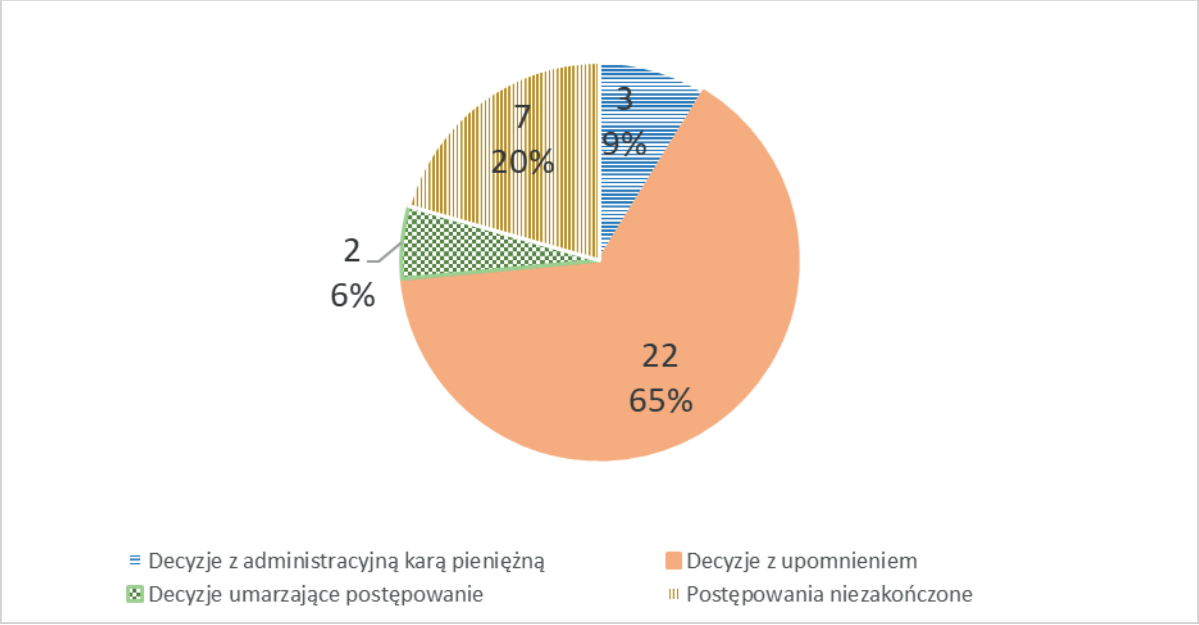
Wykres 11: Zestawienie liczby wszczętych w latach 2020-2022 postępowań w przedmiocie nałożenia kary pieniężnej za brak współpracy z organem i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań.

W 22 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. W dwóch przypadkach Prezes UODO umorzył postępowania ze względu na brak podstaw do zastosowania sankcji finansowej w sprawie. Jedno postępowanie zostało zawieszone ze względów proceduralnych.

Decyzjami nakładającymi administracyjne kary pieniężne zakończyły się trzy postępowania, zaś wysokość nałożonych tymi decyzjami kar wyniosła łącznie 70 830 zł. Pozostałych sześć postępowań nie zostało zakończonych na koniec omawianego okresu sprawozdawczego.

Spośród powyższych trzech decyzji orzekających sankcję w postaci administracyjnej kary pieniężnej, jedna decyzja (kara w wysokości 36 558 zł)[238] zaskarżona została przez stronę do Wojewódzkiego Sądu Administracyjnego w Warszawie, kolejna (kara w wysokości 27 418 zł)[239] – nie uprawomocniła się przed końcem omawianego okresu sprawozdawczego, natomiast w ostatnim przypadku kara pieniężna (w wysokości 6 854 zł)[240] została dobrowolnie zapłacona przez zobowiązanego.

Stan wszczętych w 2022 r. postępowań w przedmiocie nałożenia kary za brak współpracy z Prezesem UODO w związku z nieudzielaniem mu niezbędnych informacji, oraz rozstrzygnięcia tych postępowań, obrazuje poniższy wykres.



Wykres 12: Zestawienie stanu oraz sposobu rozstrzygnięcia wszczętych w 2022 r. postępowań w przedmiocie nałożenia kary za brak współpracy w związku z nieudzielaniem informacji niezbędnych Prezesowi UODO do realizacji jego zadań.

238 DKE.561.30.2022.
239 DKE.561.20.2022.
240 DKE.561.5.2022.

W omawianym okresie sprawozdawczym, poza trzema wskazanymi wyżej sprawami wszczętymi w 2022 r. i zakończonymi w tym samym roku nałożeniem administracyjnych kar pieniężnych, orzeczone zostały dodatkowo **cztery kary pieniężne** za tego samego rodzaju naruszenia w postępowaniach wszczętych jeszcze w 2021 r.[241] Łączna kwota tych kar wyniosła **61 691 zł**.

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 monitorowanie przestrzegania nakazów zawartych w jego decyzjach. Dlatego też Prezes UODO nie może pozwolić na ignorowanie wydawanych przez siebie orzeczeń. Istotnym narzędziem służącym do zapewnienia wykonania nakazów decyzji jest uprawnienie organu nadzorczego do nakładania kar za ich nieprzestrzeganie – zgodnie z art. 83 ust. 6 RODO.

W roku 2022 Prezes UODO wszczął **trzy postępowania** w przedmiocie nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie orzeczonych przez siebie w decyzjach administracyjnych nakazów. W jednym przypadku samo wszczęcie postępowania doprowadziło do stwierdzenia przez Prezesa UODO wykonania przez zobowiązanego nakazu decyzji, w związku z czym Prezes UODO uznał, że wystarczającą sankcją w sprawie będzie udzielenie zobowiązanemu upomnienia zamiast kary pieniężnej. Dwa pozostałe postępowania nie zostały zakończone przed końcem okresu sprawozdawczego. Natomiast w omawianym okresie sprawozdawczym **jedno postępowanie**, wszczęte jeszcze w 2021 r., zakończone zostało nałożeniem na zobowiązanego (spółkę prawa handlowego) **administracyjnej kary pieniężnej w kwocie 9 139 zł** za nieprzestrzeganie nakazu orzeczonego przez Prezesa UODO[242].

9.1. Administracyjne kary pieniężne w postępowaniach kontrolnych

W 2022 r. prezes UODO wydał 3 decyzje nakładające administracyjną karę pieniężną administratorowi danych, po przeprowadzeniu postępowania kontrolnego w przedmiocie przetwarzania danych osobowych.

Po przeprowadzeniu kontroli w spółce cywilnej[243], której działalność polegała na świadczeniu pomocy prawnej w zakresie reprezentowania klientów poszkodowanych głównie

241 DKE.561.6.2021, DKE.561.18.2021, DKE.561.23.2021, DKE.561.25.2021.
242 DKE.561.15.2021.
243 Sygn. akt. DKN.5112.5.2021.

w wypadkach komunikacyjnych w postępowaniach sądowych o roszczenia odszkodowawcze, Prezes UODO wydał decyzję, nakazując wspólnikom dostosowanie operacji przetwarzania do przepisów RODO, poprzez zaprzestanie przetwarzania danych osobowych potencjalnych klientów bez podstawy prawnej, tj. bez uzyskania zgody na przetwarzanie ich danych osobowych oraz nałożył na wspólników administracyjną karę pieniężną w **wysokości 45 697 zł.** Do pozyskania i późniejszego przetwarzania danych potencjalnego klienta przez wspólników dochodziło wskutek pozyskiwania przez nich ustnej zgody od klienta podczas pierwszego kontaktu z nim (telefonicznego lub bezpośredniego). W przypadku potencjalnych klientów wspólnicy pozyskiwali, jeszcze przed zawarciem z nimi umowy, następujące dane: imię, nazwisko, numer telefonu, adres poczty elektronicznej, informację o śmierci innej osoby oraz dane dotyczące stanu zdrowia, w związku ze zdarzeniami wypadkowymi. Zważywszy na przedmiot i okoliczności działalności gospodarczej wykonywanej przez wspólników, przetwarzanie w jej ramach danych osobowych potencjalnych klientów, może się odbywać na podstawie art. 6 ust. 1 lit. a) oraz art. 9 ust. 2 lit. a) w związku z art. 5 ust. 1 lit. a) RODO, tj. wówczas, gdy osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (w odniesieniu do danych, które nie podlegają szczególnej ochronie) oraz gdy ww. osoba udzieliła wyraźnej zgody na przetwarzanie danych podlegających szczególnej ochronie, w tym przypadku danych o stanie zdrowia. W przedmiotowej sprawie wspólnicy, jako administratorzy pozyskiwali i przetwarzali dane potencjalnych klientów w celu utrzymywania z nimi kontaktów dla uzyskania deklaracji co do zawarcia albo niezawarcia umowy o świadczenie usług przez wspólników. W ocenie Prezesa UODO uzyskanie celu, o którym wyżej mowa, nie wymaga pozyskiwania od potencjalnych klientów ich danych osobowych, a w szczególności danych dotyczących zdrowia. Wskazany wyżej cel administratorzy byliby w stanie osiągnąć np. poprzez zostawienie potencjalnemu klientowi ulotki informującej o jego usługach i możliwości zawarcia umowy o świadczenie usług dochodzenia odszkodowania (zadośćuczynienia). Prezes UODO uznał, że przetwarzanie danych potencjalnych klientów przez administratorów było nieproporcjonalne do pożądanego rezultatu, który chcieli oni osiągnąć i nie było do tego celu niezbędne. Zgodnie z treścią art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie przepisów art. 5 ust. 1 RODO i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Z kolei w myśl art. 7 ust. 1 RODO, jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Jednak w sytuacji, gdy zgody na przetwarzanie danych udzielone były przez potencjalnych klientów wyłącznie w formie ustnej, wykazanie tego faktu było niemożliwe, zaś oświadczenia wspólników i osób przez nich zatrudnionych są w tym względzie niewystarczającym dowodem. Powyższe stwierdzenie w szczególności odnosi się do zgody na przetwarzanie danych dotyczących zdrowia, która musi mieć, w myśl art. 9 ust. 1 lit. a) RODO, wyraźny charakter. Prezes UODO uznał w wydanej decyzji, że ustne oświadczenie w przedmiocie zgody na przetwarzanie danych, zarówno w przypadku danych „zwykłych", jak i tym bardziej „szczególnych", nie jest

formą dostatecznie gwarantującą wykazanie jednoznaczności, a tym bardziej wyraźności wyrażonej zgody. Forma taka, w przypadku danych „zwykłych", mogłaby być uznana za wystarczającą wyjątkowo w przypadku, gdy w ślad za nią podążałyby inne, dodatkowe działania administratora, np. polegające na sporządzeniu stosownego rejestru zgód lub rejestrowaniu dźwiękowym rozmów z osobami, których dane dotyczą. Działania takie, w przypadku wspólników, nie były jednak podejmowane.

Prezes UODO wydał w roku 2022 decyzję, w której stwierdził naruszenie ochrony danych przez spółkę prawa handlowego prowadzącą działalność w zakresie produkcji przyczep samochodowych[244]. Naruszenie to polegało na niezgłoszeniu organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Prezes UODO nałożył na spółkę administracyjną karę pieniężną w **wysokości 15 994 zł** oraz umorzył postępowanie w pozostałym zakresie. W przedmiotowej sprawie doszło do naruszenia ochrony danych osobowych polegającego na utracie przez spółkę dokumentu w postaci świadectwa pracy jej pracownika. Spółka nie zgłosiła przedmiotowego naruszenia Prezesowi UODO, ponieważ w jej opinii nie wiązało się ono z ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą. Pracownik, którego świadectwo pracy zagubiono, został powiadomiony o tym fakcie, ale nie zgłaszał z tego tytułu roszczeń wobec spółki. Tymczasem informacje zawarte w treści świadectwa pracy – obok danych zwykłych, jak imię, nazwisko, data urodzenia, nazwa pracodawcy, itd. – mogą być istotne z punktu widzenia praw lub wolności osoby, której dane dotyczą, np. w zakresie wskazania podstawy prawnej rozwiązania/wygaśnięcia stosunku pracy, ew. zajęcia wynagrodzenia za pracę w myśl przepisów o postępowaniu egzekucyjnym, itp. Dane te mogą bowiem bezpośrednio lub pośrednio ujawniać informacje o życiu osobistym osoby, której dane dotyczą, o jej problemach natury prawnej oraz statusie majątkowym. Uznanie przez spółkę, że incydent nie stanowił naruszenia ochrony danych osobowych, nie miało podstaw prawnych. Spółka nie przeanalizowała okoliczności utraty tego dokumentu, nie oszacowała skali oraz wysokości ryzyka naruszenia dla praw lub wolności podmiotu danych. W konsekwencji Prezes UODO stwierdził, że spółka, nie dokonując zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych, nie wykonała obowiązku z art. 33 ust. 1 RODO. Uznał ponadto, że w przedmiotowej sprawie nie wystąpiło wysokie ryzyko naruszenia praw lub wolności ww. osoby, przede wszystkim z uwagi na zakres danych objętych naruszeniem, przewidzianych w świadectwie pracy i dlatego postępowanie w części dotyczącej ww. kwestii stało się bezprzedmiotowe i zostało przez Prezesa UODO umorzone.

Prezes UODO, po uchyleniu przez Wojewódzki Sąd Administracyjny w Warszawie[245] decyzji z 3 grudnia 2020 r. nakładającej na operatora komunikacyjnego[246] administracyjną karę pieniężną w wysokości **1 968 524 zł,** ponownie zajmował się sprawą naruszenia przez tego administratora przepisów RODO. Postępowanie administracyjne było

244 Sygn. akt. DKN.5110.12.2021.
245 Wyrok z 21 października 2021 r. (sygn. akt: II SA/Wa 272/21).
246 Sygn. akt. DKN.5112.1.2020.

wynikiem przeprowadzonej przez organ nadzorczy kontroli zgodności przetwarzania danych osobowych z przepisami ogólnego rozporządzenia o ochronie danych osobowych oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, w związku wystąpieniem naruszenia ochrony danych osobowych. Wskutek tego incydentu nieuprawniona osoba uzyskała dostęp do dużej ilości danych abonentów usług przedpłaconych, obejmujących m.in. imię i nazwisko, numer PESEL, serię i numeru dowodu tożsamości. Kontrola wykazała, że w procesie przetwarzania danych abonentów usług przedpłaconych, administrator naruszył przepisy o ochronie danych osobowych. Postępowanie zakończyło się wydaniem decyzji, w której organ nadzorczy po raz kolejny stwierdził naruszenie przepisów RODO polegające na niewdrożeniu przez administratora odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych. Systemy te służyły do rejestracji danych osobowych abonentów usług przedpłaconych, a brak zastosowanych w nich odpowiednich środków technicznych i organizacyjnych doprowadził do uzyskania przez osobę nieuprawnioną dostępu do tych danych, co stanowiło również naruszenie zasady integralności i poufności. Za naruszenie art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1, art. 32 ust. 1 lit. b) i lit. d) oraz art. 32 ust. 2 RODO, Prezes UODO nałożył na następcę prawnego operatora telekomunikacyjnego administracyjną karę pieniężną **w kwocie 1 599 395 zł.** W wydanej decyzji organ stwierdził, że u administratora nie były dokonywane regularne testy pomiarów i oceny skuteczności stosowanych przez niego środków technicznych oraz organizacyjnych, mające zapewnić bezpieczeństwo przetwarzanych danych osobowych. Podejmowane przez administratora przeglądy zastosowanych środków bezpieczeństwa w sytuacji wystąpienia zmiany organizacyjnej lub prawnej, jak również podejmowane działania dopiero w przypadku podejrzenia zaistnienia podatności, nie mogły zostać uznane za regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych. Prezes Urzędu w uzasadnieniu decyzji podkreślił, że wskazane testowanie, mierzenie i ocenianie, aby stanowiło realizację wymogu wynikającego z art. 32 ust. 1 lit. d) RODO, musi być dokonywane w sposób regularny, co oznacza świadome zaplanowanie i zorganizowanie, a także dokumentowanie (w związku z zasadą rozliczalności) tych działań w określonych przedziałach czasowych, niezależnie od zmian w organizacji i przebiegu procesów przetwarzania danych spowodowanych np. zmianą organizacyjną u administratora danych. Administrator zobowiązany jest do weryfikacji zarówno doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania. Kompleksowość tej weryfikacji powinna być oceniana przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania. Przeprowadzona kontrola wykazała, że administrator nie przeprowadził testów weryfikujących stosowanych przez niego zabezpieczeń dotyczących przekazywania danych pomiędzy aplikacjami, które służą do rejestracji usług przedpłaconych. Takie działania zostały podjęte dopiero po wystąpieniu zgłoszonego przez administratora naruszenia ochrony danych osobowych. Istniejąca od

czasu stworzenia aplikacji luka w systemach informatycznych została wykorzystana przez osobę nieuprawnioną.

9.2. Administracyjne kary pieniężne w związku z naruszeniem

Wybrane przykłady decyzji Prezesa UODO nakładających na administratorów danych administracyjne kary pieniężne w związku ze stwierdzonym naruszeniem ochrony danych osobowych

Prezes UODO w związku ze stwierdzeniem naruszenia ochrony danych osobowych przez ośrodek dla osób nietrzeźwych[247] wydał decyzję nakładającą administracyjną karę pieniężną w wysokości **10 000 zł** na wspomniany podmiot. Naruszenie polegało na nagrywaniu i utrwalaniu dźwięku (głosu) w zainstalowanym w ww. ośrodku systemie monitoringu, tj. przetwarzaniu bez podstawy prawnej danych osobowych w tym zakresie. Naruszenie przepisów o ochronie danych osobowych w tym przypadku wydaje się szczególnie rażące, jako że w placówkach tego typu przebywają osoby często niepanujące nad wydawanymi przez siebie dźwiękami i wypowiadanymi słowami. Z uwagi na specyfikę działalności tego typu placówek i fakt, że znajdują się w nich również osoby doprowadzone do nich pod przymusem, decyzja ta ma istotne znaczenie ze względu na ochronę osób fizycznych przed nieuprawnionym przetwarzaniem danych.

Prezes UODO wobec stwierdzenia naruszenia ochrony danych osobowych polegającego na niezapewnieniu odpowiedniego bezpieczeństwa danych osobowych oraz braku wdrożenia odpowiednich środków technicznych i organizacyjnych, nałożył administracyjną karę pieniężną w kwocie **8 000 zł na wójta gminy**[248]. Administrator zgłosił do UODO naruszenie ochrony danych osobowych członków ochotniczej straży pożarnej, do którego doszło na skutek włamania do mieszkania pracownika i kradzieży laptopa, zawierającego plik z danymi osobowymi. W konsekwencji doszło do utraty poufności danych osobowych ww. osób. Co należy podkreślić, administrator opracował odpowiednie procedury i polityki dotyczące bezpieczeństwa przetwarzania danych osobowych oraz przeprowadził analizę ryzyka, w której odniósł się m.in. do zagrożenia w postaci kradzieży sprzętu komputerowego wykorzystywanego do przetwarzania danych osobowych. Administrator miał świadomość ryzyka związanego z utratą sprzętu komputerowego wynoszonego poza jego organizację. Ryzyko to ocenił jako nieakceptowalne i określił, w ramach sposobu postępowania z ryzykiem, zabezpieczenia, jakie należy wdrożyć w celu jego ograniczenia. Wśród wymienionych zabezpieczeń mających obniżyć poziom ryzyka wskazano m.in. szyfrowanie. Jednak, jak wykazało postępowanie, skradziony komputer był zabezpieczony przed nieautoryzowanym dostępem jedynie za pomocą hasła, a przyjęte w procedurach zabezpieczenia nie zostały zastosowane, przynajmniej na tym komputerze. Pomimo że administrator miał świadomość konieczności zastosowania

247 Sygn. akt. DKN.5131/51/2021.
248 Sygn. akt. DKN.5131/8/2022.

odpowiednich środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych osobowych przetwarzanych przy użyciu przenośnego sprzętu komputerowego, dopiero po naruszeniu ochrony danych osobowych podjął działania mające na celu uniknięcie podobnych zdarzeń w przyszłości poprzez szyfrowanie dysków twardych komputerów przenośnych. Zatem administrator dopiero po wystąpieniu naruszenia zastosował się do wyników własnej analizy ryzyka i określonego w niej sposobu postępowania z tym ryzykiem. Przy nakładaniu administracyjnej kary pieniężnej uwzględniono również fakt, że skradziony komputer został odnaleziony, a przeprowadzona przez administratora analiza wykazała, że od dnia kradzieży system operacyjny komputera nie był uruchamiany. Tym samym, pomimo że administrator utracił kontrolę nad danymi osobowymi, a nieuprawniona osoba uzyskała do nich bezprawny dostęp, nie było podstaw do uznania, że na dzień wydania przedmiotowej decyzji administracyjnej, osoby, których dane dotyczą, poniosły jakąkolwiek szkodę na skutek tego naruszenia.

W kolejnej sprawie Prezes UODO stwierdził naruszenie przez ośrodek kultury[249] przepisów RODO, polegające na powierzeniu innemu podmiotowi przetwarzania danych osobowych bez zawartej na piśmie umowy powierzenia oraz bez przeprowadzenia weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Decyzją Prezesa UODO została nałożona na ośrodek kultury administracyjna kara pieniężna **w wysokości 2 500 zł.** W decyzji tej bardzo szeroko opisano status i rolę podmiotu przetwarzającego oraz warunki, jakie należy spełnić przy jego wyznaczaniu.

Kolejną decyzją Prezesa UODO została nałożona administracyjna kara pieniężna w wysokości ponad **4 900 000 zł** na spółkę akcyjną[250] za niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych oraz brak weryfikacji podmiotu przetwarzającego. Z kolei podmiot przetwarzający otrzymał karę w wysokości **ponad 250 000 zł**. Naruszenie ochrony danych polegało na pozostawieniu w ogólnodostępnej lokalizacji bazy danych klientów administratora, przez co dostęp do niej uzyskały nieuprawnione osoby. Doszło do tego w momencie wprowadzania zmiany w środowisku teleinformatycznym. Zmiany tej dokonał podmiot przetwarzający, z którym administrator współpracował na podstawie zawartych umów, w tym umowy powierzenia przetwarzania danych osobowych. W trakcie dokonywanych zmian utworzona została dodatkowa baza danych klientów spółki, która nie została zabezpieczona przed dostępem osób trzecich. Administrator dowiedział się o incydencie nie od podmiotu przetwarzającego, a od dwóch niezależnych użytkowników Internetu, którzy powiadomili go, że mają nieuprawniony dostęp do bazy. W trakcie procesu dokonywania zmian w systemie zostały użyte rzeczywiste dane osobowe klientów administratora, a skuteczność zastosowanych zabezpieczeń nie została zweryfikowana przed przekazaniem do spółki nowego rozwiązania. Ponadto funkcje

249 Sygn. akt. DKN.5131.29.2022.
250 Sygn. akt. DKN.5130.2215.2020.

bezpieczeństwa nie były testowane w trakcie prowadzonych w tym celu prac. Zaistniałe naruszenie wynikało z niezastosowania przez podmiot przetwarzający podstawowych zasad bezpieczeństwa polegających na zabezpieczeniu danych osobowych przed dostępem osób nieuprawnionych. Administrator, pomimo wdrożonych procedur oraz posiadanej wiedzy, jak zgodnie z powszechnie stosowanymi praktykami powinno przebiegać wprowadzanie zmian w systemach informatycznych, na żadnym etapie wdrożenia nie prowadził nadzoru nad tym, czy wdrożenie faktycznie przebiega zgodnie z powszechnie obowiązującymi standardami. Spółka nie egzekwowała od podmiotu przetwarzającego realizacji umów, nie stosowała się do własnej praktyki wdrażania zmian w środowisku IT opartej o wewnętrzne regulacje oraz nie weryfikowała podmiotu przetwarzającego w zakresie prowadzonych działań mających na celu usprawnienie funkcjonowania usługi. Mając na względzie ustalone okoliczności, organ nadzorczy stwierdził, iż zaistniały przesłanki uzasadniające nałożenie na administratora oraz na podmiot przetwarzający administracyjnych kar pieniężnych.

Decyzją Prezesa UODO została nałożona kolejna administracyjna kara pieniężna na Głównego Geodetę Kraju (GGK)[251]. Jej wysokość to **60 000 zł.** Powodem nałożenia kary było niezgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu oraz niepowiadomienie o nim osób, których dane osobowe zostały ujawnione. Decyzja nakazywała też powiadomienie o naruszeniu osoby, których ono dotyczyło. Naruszenie ochrony danych osobowych polegało na ujawnieniu numerów ksiąg wieczystych w serwisie prowadzonym przez Głównego Geodetę Kraju, czyli www.geoportal.gov.pl. W toku postępowania GGK utrzymywał, że numery ksiąg wieczystych nie są danymi osobowymi. Ponadto GGK utrzymywał, że numery ksiąg są też widoczne w innych serwisach i krótkotrwałe pojawienie się numerów w serwisie www.geoportal.gov.pl nie spowodowało żadnego ryzyka naruszenia praw i wolności osób, których dane dotyczą. W przedmiotowej decyzji Prezes UODO uzasadnił, że numery ksiąg wieczystych są danymi osobowymi i przytoczył wyrok WSA w Warszawie[252], w którym sąd potwierdził stanowisko UODO, że numery ksiąg wieczystych są danymi osobowymi. Prezes UODO zwrócił uwagę na możliwość szeregu negatywnych konsekwencji dla osoby fizycznej. Podkreślił przy tym kluczową rolę numeru PESEL, który powinien być szczególnie chroniony. UODO wskazując niebezpieczeństwa związane z wykorzystaniem PESEL, przypomniał sprawę sądową, w której oskarżonym udało się wyłudzić pożyczkę, posiadając jedynie prawdziwy numer PESEL ofiary, gdyż pozostałe dane, jak adres czy numer dokumentu tożsamości były już fikcyjne.

Prezes UODO nałożył na jeden z banków administracyjną karę pieniężną w **wysokości 363 832 zł** za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki oraz niepowiadomienie w sposób prawidłowy o naruszeniu osób, których dane dotyczyły[253]. Podstawą powzięcia przez Prezesa UODO wiedzy o naruszeniu była skarga osób na nieprawidłowości w procesie przetwarzania ich danych osobowych przez bank. Naruszenie polegało na zgubieniu przez firmę kurierską

251 Sygn. akt. DKN.5131.27.2022.
252 Sygn. akt. II Sa/Wa 2222/20.
253 Sygn. akt. DKN.5131.16.2021.

korespondencji z danymi osobowymi skarżących. Bank nieprawidłowo określił stopień ryzyka dla osób, których dane dotyczą, przyjmując jego poziom jako średni. W następstwie powyższego nie zgłosił naruszenia do organu nadzorczego. Podkreślić należy, że zgłoszeniu podlegają te z incydentów, w przypadku których istnieje prawdopodobieństwo (wyższe niż małe) szkodliwego (niekorzystnego) wpływu na prawa lub wolności osób, których dane dotyczą. Gdy to ryzyko jest wysokie, to o naruszeniu trzeba także powiadomić osoby, których dane dotyczą. Prezes UODO podkreślił w uzasadnieniu przedmiotowej decyzji, że nie jest istotne to, czy nieuprawniony odbiorca faktycznie wszedł w posiadanie i zapoznał się z danymi osobowymi innych osób, lecz to, że wystąpiło takie ryzyko.

Administrator w swoich wyjaśnieniach podkreślał, że z posiadanych przez niego informacji wynikało, że dane nie zostały wykorzystane na szkodę osób, których dane dotyczą, ale przewidział, że naruszenie może wiązać się z takim ryzykiem. Świadczy o tym fakt zaproponowania dodatkowej usługi BIK Alert w ramach środków w celu zaradzenia naruszeniu. Zdaniem banku miałoby to umożliwić podjęcie stosownej reakcji w przypadku, gdyby doszło, jak sam wskazuje, „pomimo niskiego prawdopodobieństwa, do wykorzystania danych skarżących w systemie bankowym w sposób nieuprawniony". Powyższa decyzja została zaskarżona przez bank do Wojewódzkiego Sądu Administracyjnego w Warszawie, który po rozpoznaniu sprawy wydał wyrok oddalający skargę[254]. W uzasadnieniu orzeczenia sąd wskazał, że przy wydawaniu przedmiotowej decyzji Prezes UODO nie naruszył przepisów prawa materialnego oraz postępowania administracyjnego w stopniu mogącym mieć wpływ na wynik sprawy. Od powyższego wyroku Wojewódzkiego Sądu Administracyjnego bank złożył skargę kasacyjną.

Prezes UODO stwierdził naruszenie przepisów RODO i nałożył administracyjną karę pieniężną w **wysokości 545 748 zł** na bank[255] za niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki, osób, których dane dotyczyły.

Naruszenie polegało na posiadaniu dostępu do Platformy Usług Elektronicznych ZUS przez byłego pracownika banku, któremu nie odebrano uprawnień po zakończeniu stosunku pracy. Osoba ta mogła przeglądać znajdujące się na profilu płatnika dane pracowników banku. Administrator nieprawidłowo określił poziom ryzyka uznając, że były pracownik w okresie zatrudnienia miał dostęp do znacznie szerszego zakresu danych osobowych pracowników, a więc jest odbiorcą zaufanym, co skutkowało rezygnacją z zawiadomienia o naruszeniu ochrony danych pracowników. W związku z powyższym Prezes UODO wszczął wobec banku postępowanie administracyjne. Prezes UODO podkreślił w uzasadnieniu decyzji, że w przedmiotowej sprawie nie występował odbiorca zaufany. Były pracownik logował się do systemu w momencie kiedy nie był związany z bankiem żadnym stosunkiem prawnym, wobec czego bank powinien był zachować się w sposób bardziej ostrożny w przypadku ujawnienia danych osobie nieuprawnionej, a więc zawiadomić o naruszeniu ochrony danych osobowych osoby, których dane dotyczą, zakładając, że naruszenie może wywołać szersze skutki. Administrator w swoich

254 Wyrok WSA w Warszawie z dnia 8 sierpnia 2022 r. sygn. akt II SA/Wa 4143/21.
255 Sygn. akt DKN.5131.33.2021.

wyjaśnieniach podkreślał, że może ufać odbiorcy na tyle, aby móc racjonalnie oczekiwać, że strona ta nie odczyta omyłkowo wysłanych danych lub nie uzyska do nich wglądu, oraz że wypełni polecenie ich odesłania. Bank podkreślał, że nawet jeżeli do danych uzyskano wgląd, nadal może mieć zaufanie do odbiorcy, że nie podejmie on żadnych dalszych działań w kwestii tych danych.

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

10. Uprzednie konsultacje

Do zadań Urzędu Ochrony Danych Osobowych należy udzielanie zaleceń na wniosek o uprzednie konsultacje złożony przez administratora. Uprzednie konsultacje z UODO to procedura służąca wsparciu administratorów w sytuacji stwierdzenia przez nich wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, którego sami nie są w stanie zminimalizować. Procedura ta uregulowana jest w art. 36 RODO oraz w art. 57 ustawy o ochronie danych osobowych. Celem uprzednich konsultacji jest wypracowanie rozwiązań, które pozwolą administratorowi prawidłowo chronić dane osobowe. Z wnioskiem o uprzednie konsultacje należy wystąpić w sytuacji, w której w wyniku przeprowadzonej oceny skutków dla ochrony danych na liście badanych operacji przetwarzania znajdą się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i gdy administrator nie może znaleźć środków wystarczających do zmniejszenia (zminimalizowania) tego ryzyka do dopuszczalnego poziomu.

W omawianym okresie sprawozdawczym administratorzy, częściej niż w poprzednich latach, korzystali z rozwiązania przewidzianego w art. 36 RODO i art. 38 DODO[256]. W 2022 roku do Urzędu wpłynęło **siedem (7) wniosków o przeprowadzenie uprzednich konsultacji**. W poprzednim roku sprawozdawczym wpłynęły 3 takie wnioski, w 2020 roku – 3, w 2019 roku – 5, a w 2018 roku – 2. Niemniej żaden z wniesionych w 2022 roku wniosków nie mógł zainicjować postępowania w sprawie uprzednich konsultacji, gdyż wnioski te obarczone były brakami.

W większości przypadków zagadnienia w nich przedstawione budziły wątpliwości w zakresie podstawy prawej udostępnienia danych osobowych, które powinny być rozstrzygane na podstawie obowiązujących przepisów regulujących opisane w tych wnioskach kwestie, nie zaś w trybie określonym w art. 36 RODO czy też art. 38 DODO.

Procedura uprzednich konsultacji ma zastosowanie wówczas, gdy planowana operacja przetwarzania danych, tj. planowany proces, w którym przetwarzane są dane osobowe (np. wprowadzenie w organizacji 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

256 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r. poz. 1206), zwana dalej „DODO".

może mieć miejsce podczas takiego przetwarzania.

W takim przypadku warunkiem koniecznym do wystąpienia z wnioskiem o uprzednie konsultacje do organu nadzorczego jest wcześniejsze dokonanie przez administratora oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi ryzyka naruszenia praw i wolności osób fizycznych. Ocena taka powinna zawierać ponadto wskazanie konkretnych środków planowanych przez administratora w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie przepisów o ochronie danych osobowych, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

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 wyrazi opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym (motyw 94 RODO).

Efektem takich konsultacji jest udzielenie administratorowi pomocy w znalezieniu środków wystarczających do zmniejszenia, do dopuszczalnego poziomu, ryzyka zdiagnozowanego podczas oceny skutków dla ochrony danych jako wysokie.

Natomiast zagadnienie istnienia podstawy prawnej do prowadzenia określonych operacji przetwarzania powinno być rozstrzygane jako zagadnienie pierwotne wobec oceny skutków dla ochrony danych, a tym samy również wobec uprzednich konsultacji.

W jednym z wniosków o uprzednie konsultacje, oprócz braku podstawy prawnej do przetwarzania danych, administrator rozpoczął proces przetwarzania danych przed udzieleniem konsultacji przez organ nadzorczy. Warto przypomnieć, że zgodnie z treścią art. 36 ust. 1 RODO procedura uprzednich konsultacji może nastąpić jedynie przed rozpoczęciem przetwarzania danych osobowych. Na uprzedni, a więc dokonywany przed rozpoczęciem przetwarzania, charakter tych konsultacji prawodawca unijny zwraca uwagę w motywach 84 i 94 RODO. Zgodnie z motywem 84 RODO, jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym. Ponadto z motywu 94 RODO wynika, że 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, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym.

W jednym z wniosków organ nadzorczy nie udzielił konsultacji ze względu na brak spełnienia wymogów określonych w przepisach prawa, zwłaszcza w art. 36 ust. 3 RODO oraz w art. 63 § 1-3 k.p.a. Do wniosku o uprzednie konsultacje nie załączono bowiem oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Ponadto wniosek został wniesiony na adres poczty e-mail, a nie na adres do doręczeń elektronicznych lub za pośrednictwem konta w systemie teleinformatycznym organu administracji publicznej (art. 63 § 1 k.p.a.), nie wskazywał osoby, od której pochodzi (art. 63 § 2 k.p.a.), a także nie był podpisany przez wnoszącego (art. 63 § 3 k.p.a.) – podpisy na wniosku przesłanym elektronicznie zostały negatywnie zweryfikowane (nie spełniały wymogu określonego w art. 63 § 3 k.p.a. w zw. art. 14 § 1d w zw. z art. 14 § 1a k.p.a.).

Inny ze złożonych w 2022 roku wniosków o uprzednie konsultacje dotyczył operacji przetwarzania informacji o osobach zmarłych. Wniosek ten nie mógł inicjować postępowania w sprawie uprzednich konsultacji, ponieważ przepisy o ochronie danych osobowych nie mają zastosowania do przetwarzania informacji o osobach zmarłych. Potwierdzają to m.in. motywy 27 i 160 preambuły RODO.

W doktrynie wskazuje się, że po śmierci osoby informacje jej dotyczące tracą status danych osobowych, co oznacza kres ochrony opartej na prawnych mechanizmach ochrony danych osobowych. Wynika to z faktu, iż prawo do ochrony danych osobowych jest prawem o czysto osobistym charakterze, ściśle powiązanym z osobą, której przysługuje. Z chwilą śmierci ustaje możliwość bycia podmiotem praw i obowiązków, a co za tym idzie – kończy się przewidziana prawem ochrona osoby, której dane dotyczą[257]. Nie oznacza to, że informacje o osobach zmarłych nie podlegają żadnej ochronie. Podkreślić bowiem należy, że nie tylko przepisy dotyczące ochrony danych osobowych regulują dostęp do prywatnej sfery życia człowieka. Oprócz nich istnieje wiele innych aktów prawa, które gwarantują prawo do poszanowania godności, czci, dobrego imienia czy wizerunku (np. przepisy k.c., k.k., prawa prasowego[258], itd.).

W odniesieniu do poprzednich okresów sprawozdawczych można zaobserwować, że administratorzy częściej sięgają po instytucję uprzednich konsultacji, jednak nadal stwierdzić można brak zrozumienia, jakich sytuacji mogą dotyczyć uprzednie konsultacje oraz jakie działania należy podjąć przed skorzystaniem z nich.

Podsumowując, należy stwierdzić, że złożone w 2022 roku wnioski o dokonanie uprzednich konsultacji nie doprowadziły do udzielenia zaleceń Prezesa Urzędu w tym zakresie, gdyż administratorzy nie do końca jednak rozumieli, jak prawidłowo skorzystać z tego narzędzia celem uzyskania pomocy ze strony organu nadzorczego.

Przede wszystkim złożone wnioski o uprzednie konsultacje dotyczyły w istocie wątpliwości związanych z przetwarzaniem danych osobowych w konkretnych opisanych

257 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. 4, LEX/el. 2022.

258 Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (t.j. Dz. U. z 2018 r. poz. 1914), dalej: „prawo prasowe"

sytuacjach. Świadczyć to może o tym, że administratorzy nie dokonali uprzedniej analizy podstaw prawnych dla realizacji określonych procesów przetwarzania z udziałem nowych technologii. Powyższe może prowadzać do wniosku, że administratorzy często mylą instytucję uprzednich konsultacji z sytuacją, gdy chcą jedynie uzyskać od Prezesa UODO stanowisko w konkretnej sprawie związane z przetwarzaniem danych osobowych. Należy jednak podkreślić, że kwestie dotyczące podstaw procesów przetwarzania danych opisanych we wnioskach powinny być rozstrzygane na podstawie obowiązujących, regulujących je przepisów, nie zaś na podstawie art. 36 RODO. Procedura uprzednich konsultacji ustanowiona została bowiem w innym celu.

Ponadto administratorzy, mimo podejmowanych w tym zakresie działań informacyjnych Urzędu (dedykowana uprzednim konsultacjom zakładka na stronie internetowej Urzędu), nie do końca potrafili stosować właściwe przepisy dotyczące możliwości skorzystania z tej formy wsparcia. Instytucja uprzednich konsultacji jest dość sformalizowana, tzn. oprócz wymogów określonych w art. 63 k.p.a., wniosek taki musi zawierać co najmniej informacje wymienione w art. 36 ust. 3 RODO. Jeżeli wniosek nie będzie spełniał tych wymogów, Prezes Urzędu informuje o nieudzieleniu konsultacji, wskazując tego przyczyny (zgodnie z art. 57 ust. 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych).

11. Kodeksy postępowania

Na mocy art. 40 RODO wprowadzony został instrument prawny w postaci kodeksu postępowania, którego celem jest doprecyzowanie i pomoc we właściwym stosowaniu przepisów RODO w danej branży. Organ nadzorczy nieustannie zachęca do podjęcia prac w tym zakresie. Kodeksy postępowania mogą być sporządzone, a następnie przedkładane Prezesowi UODO do zatwierdzenia, przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Po otrzymaniu wniosku o zatwierdzenie kodeksu postępowania, organ nadzorczy przeprowadza postępowanie administracyjne w tym zakresie. W jego toku wydaje opinię o zgodności przedłożonego projektu z przepisami o ochronie danych osobowych, a następnie zatwierdza kodeks postępowania w formie decyzji administracyjnej, o ile uzna, że stanowi on odpowiednie zabezpieczenie właściwego stosowania RODO.

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

Kodeksy postępowania zatwierdzone przez organ nadzorczy

W roku sprawozdawczym 2022 organ nadzorczy zatwierdził pierwszy kodeks postępowania – „Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych"[259] (14 grudnia 2022 r.). Tego samego dnia odbyło się uroczyste wręczenie decyzji przedstawicielom wnioskodawcy – Federacji Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie". Kodeks został opublikowany na stronie internetowej Urzędu Ochrony Danych Osobowych[260]. Była to także okazja do przedstawienia stanu prac nad pozostałymi wnioskami i przypomnienia zasad tworzenia kodeksów oraz najczęstszych błędów popełnianych przez wnioskodawców[261].

Nowe wnioski o zaopiniowanie kodeksów postępowania

W maju 2022 r. do organu nadzorczego wpłynął wniosek o zatwierdzenie „Kodeksu postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego" (KODO)[262]. Wnioskodawcą w tej sprawie jest Polskie Stowarzyszenie Marketingu SMB. Organ nadzorczy poinformował wnioskodawcę o spełnieniu warunków formalnych procedowania kodeksu. Obecnie trwa ocena merytoryczna tego kodeksu.

Postępowania prowadzone w 2022 r. w sprawie wniosków o zatwierdzenie kodeksów postępowania, które zostały złożone we wcześniejszych latach:

- Na zaawansowanym etapie postępowania znajduje się projekt „Kodeksu postępowania dla sektora ochrony zdrowia" zgłoszony przez Polską Federację Szpitali[263]. W lutym 2021 r. organ nadzorczy pozytywnie zaopiniował projekt ww. kodeksu z zastrzeżeniem, że kwestia monitorowania podmiotów publicznych musi zostać doprecyzowana – opinia ta jest dostępna na stronie internetowej Urzędu Ochrony Danych Osobowych[264]. W 2022 r. organ nadzorczy dwukrotnie wzywał wnioskodawcę do uzupełnienia projektu kodeksu o stosowne mechanizmy monitorowania;
- W 2022 r. kontynuowano prace nad zatwierdzeniem projektu „Kodeksu postępowania w sprawie przetwarzania danych osobowych dla celów badań naukowych przez biobanki w Polsce"[265]. Wnioskodawcą w tej sprawie jest Sieć Badawcza Łukasiewicz – PORT, Polski Ośrodek Rozwoju Technologii z siedzibą we Wrocławiu. Po zweryfikowaniu wniosku i projektu kodeksu pod względem formalnym organ nadzorczy przedstawił wnioskodawcy w sierpniu 2022 r. pełną merytoryczną ocenę projektu kodeksu. Obecnie zaś oczekuje na wyjaśnienia i doprecyzowania wskazanych kwestii przez przedstawicieli twórców kodeksu;

259 ZAS.070.2.2018.
260 https://uodo.gov.pl/pl/426/1110
261 https://archiwum.uodo.gov.pl/pl/138/2520; https://archiwum.uodo.gov.pl/pl/138/2519
262 DOL.4421.1.2022.
263 ZAS.070.4.2018.
264 https://uodo.gov.pl/pl/426/1110
265 DOL.4421.1.2021.

- W okresie objętym sprawozdaniem prowadzona była korespondencja z twórcami projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez spółdzielnie mieszkaniowe zrzeszone w Związku Rewizyjnym Spółdzielni Mieszkaniowych RP”, czyli przedstawicielem Związku Rewizyjnego Spółdzielni Mieszkaniowych RP[266];
- Kontynuowano prace związane z zatwierdzeniem projektu „Kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencja badawcze”[267]. Wnioskodawca, tj. Organizacja Firm Badania Opinii i Rynku, przedstawił poprawioną wersję projektu tego dokumentu. Po dokonaniu kompleksowej oceny merytorycznej projektu pod kątem jego zgodności z przepisami o ochronie danych osobowych, organ nadzorczy przedstawił wnioskodawcy liczne uwagi i wezwał do ich uwzględnienia w projekcie;
- Krajowa Izba Doradców Podatkowych przedłożyła nową wersję projektu „Kodeksu postępowania Krajowej Izby Doradców Podatkowych w zakresie ochrony danych osobowych”[268]. Po jego weryfikacji pod względem formalnym, organ nadzorczy wezwał wnioskodawcę (KIDP) do uzupełnienia braków. Kodeks jest na etapie kompleksowej oceny merytorycznej pod kątem zgodności z przepisami o ochronie danych osobowych.

Współpraca organu nadzorczego z inicjatywami opracowania kodeksów postępowań:

W 2022 r. organ nadzorczy pozostawał również w kontakcie z inicjatywami przygotowującymi projekty kodeksów postępowania, które nie złożyły jeszcze wniosków o ich zatwierdzenie:

- przedstawiciele organu nadzorczego spotkali się dwukrotnie z reprezentacją Inspektorów Ochrony Danych w sądach powszechnych. Podczas spotkań uczestnicy zostali zaznajomieni z podstawowymi wymogami związanymi z tworzeniem kodeksu postępowania i przedkładania go do zatwierdzenia. Uczestnicy zapowiedzieli chęć stworzenia kodeksu postępowania w sądach powszechnych w sprawach niezwiązanych z wymiarem sprawiedliwości;
- organ nadzorczy został poinformowany przez Związek Województw RP o rozpoczęciu prac nad projektem „Kodeksu postępowania z danymi osobowymi w jednostkach samorządu terytorialnego”[269] i udzielił przedstawicielom tej inicjatywy wstępnych wskazówek dotyczących pracy nad kodeksami postępowania;
- Izba Gospodarcza Hotelarstwa Polskiego zwróciła się z prośbą o zorganizowanie

266 ZAS.070.5.2019.
267 DOL.4421.2.2020.
268 DOL.4421.1.2020.
269 DOL.023.799.2022.

spotkania w związku z planowanym złożeniem, celem zatwierdzenia przez organ nadzorczy, projektu kodeksu postępowania dla reprezentowanej branży[270].

Z dotychczasowych doświadczeń organu nadzorczego zebranych w czasie prac nad projektami kodeksów postępowania wynika, że środowiska inicjujące prace nad tymi dokumentami popełniają błędy, które często wpływają na wydłużenie procedury zatwierdzenia kodeksu, zawieszenie prac nad projektem, a nawet całkowite zaniechanie przygotowania takiego dokumentu. Należą do nich:

- brak jasnego i zwięzłego uzasadnienia, w którym przedstawia się szczegółowe informacje o celu kodeksu, zakresie jego stosowania oraz sposobie, w jaki ułatwi on skuteczne stosowanie RODO,
- wnioskowanie o zatwierdzenie kodeksu przez podmiot, który nie reprezentuje większości sektora,
- brak podmiotu, który podjąłby się roli wnioskodawcy w postępowaniu o zatwierdzenie kodeksu,
- zbyt wąski zakres przeprowadzonych konsultacji (np. nieobejmujący w ogóle osób, których dane dotyczą – użytkowników albo klientów czy organizacji działających na ich rzecz) oraz przedstawianie zbyt szczegółowego sprawozdania z konsultacji,
- zbyt kompleksowe/szerokie podejście do zagadnień przetwarzania danych zamiast rozstrzygnięcia najważniejszych problemów sektora, co powoduje niemożność zatwierdzenia kodeksu ze względu na istnienie zbyt wielu kwestii spornych, które trudno jest rozstrzygnąć w jednym dokumencie (warto w tym miejscu zwrócić uwagę na brzmienie ustępu 2 art. 40 RODO – wymieniono w nim zagadnienia, jakie mogą obejmować kodeksy postępowania, ale wyliczenie to ma charakter przykładowy i nie jest wyliczeniem wyczerpującym, tzn. nie wszystkie wskazane w nim zagadnienia muszą być uregulowane w kodeksie),
- przepisanie w kodeksie przepisów RODO lub ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych bez praktycznego wyjaśnienia ich stosowania,
- niewskazanie w kodeksie przepisów sektorowych oraz wytycznych, opinii i stanowisk EROD w odniesieniu do konkretnego sektora lub konkretnej czynności przetwarzania lub tylko ogólne ich wskazanie bez odniesienia się do konkretnych przepisów związanych z przetwarzaniem danych osobowych w sektorze, dla którego powstał kodeks,
- niepowoływanie się przez twórców na istniejące orzecznictwo rozstrzygające zagadnienia regulowane w kodeksie,
- brak wypracowania odpowiednich mechanizmów umożliwiających monitorowanie kodeksu.

270 ZAS.071.9.2018.

Przyczyn powyższych błędów jest kilka. Z doświadczeń organu nadzorczego wynika, że nie wszystkie środowiska przystępujące do prac nad kodeksami postępowania wystarczająco dokładnie przeanalizowały procesy przetwarzania danych osobowych, których dokonują w związku z realizowanymi zadaniami czy prowadzoną działalnością. Tymczasem pozwoliłoby im to zdiagnozować problemy, których sposób rozwiązania mógłby być przedmiotem regulacji kodeksu postępowania. Stąd zapewne ogólny charakter zaproponowanych przez nich rozwiązań czy wręcz „przepisanie RODO", co nie jest celem kodeksu postępowania. Wydaje się, że mimo iż prowadzenie rejestrów, o których mowa w art. 30 RODO, nie zawsze stanowi obowiązek administratorów czy podmiotów przetwarzających, to wykorzystanie tych dokumentów (oczywiście nie przez ich wzajemne udostępnianie) w pracach nad kodeksem postępowania mogłoby stanowić punkt wyjścia do dyskusji nad zakresem regulacji i celem kodeksu postępowania. Warto przypomnieć, iż organ nadzorczy zaproponował sposób prowadzenia tych rejestrów w formule rozszerzonej w stosunku do tego, czego wymaga art. 30 RODO, m.in. przez wpisywanie do nich informacji o podstawie prawnej przetwarzania, źródle danych osobowych, systemie informatycznym wykorzystywanym do przetwarzania czy o konieczności przeprowadzenia oceny skutków dla ochrony danych – dla rejestru czynności przetwarzania oraz przez określanie czasu trwania przetwarzania, kategorii podpowierzonych przetwarzań – dla rejestrów wszystkich kategorii czynności przetwarzania[271].

Innym problemem jest zbyt małe zaangażowanie w prace nad kodeksem postępowania administratorów/podmiotów przetwarzających, którzy będą wykorzystywali kodeks w swojej działalności. Należy podkreślić, że scedowanie w całości przygotowania projektu kodeksu podmiotom zewnętrznym (np. kancelariom prawnym, firmom szkoleniowym czy audytowym) może nie być dobrym rozwiązaniem z uwagi na ich niewystarczającą wiedzę co do specyfiki działalności danej branży (sektora).

Doświadczenia organu nadzorczego wskazują również, że czasem konkretne środowisko, najczęściej reprezentowane przez inspektorów ochrony danych danego sektora, widzi potrzebę opracowania kodeksu postępowania, ale brak jest podmiotu, który mógłby ich reprezentować i być stroną postępowania przed organem nadzorczym.

Niezależnie od wskazanych wyżej trudności i błędów popełnianych podczas prac nad tworzeniem kodeksów, wpływ na czas trwania postępowania o zatwierdzenie kodeksu ma też oczekiwanie przez środowiska pracujące nad takim dokumentem na zmianę przepisów sektorowych (gdy ich projekt jest przygotowywany przez rząd lub spodziewane jest implementowanie przepisów unijnych). Rozsądnym rozwiązaniem w takiej sytuacji jest wstrzymanie się z konsultacjami, albo ze złożeniem wniosku o zatwierdzenie kodeksu, jeżeli regulowane operacje przetwarzania mogą po nowelizacji ulec zmianie. Inicjatywy kodeksowe powinny swoje wątpliwości i postulaty sygnalizować w procesie legislacyjnym, w którym najczęściej bierze także udział organ nadzorczy.

271 https://archiwum.uodo.gov.pl/pl/126/214

Należy zatem podkreślić, że organ nadzorczy chętnie wspiera każdą zgłoszoną mu inicjatywę dotyczącą kodeksów postępowania, m.in. poprzez spotkania z ich twórcami, podczas których wskazuje, jak powinny przebiegać prace nad kodeksem (z uwzględnieniem wydanych przez EROD „Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679") i jak przebiega procedura jego zatwierdzania, wynikająca z RODO i doprecyzowana w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

12. Akredytacja podmiotów monitorujących kodeksy postępowania

Za monitorowanie przestrzegania kodeksu postępowania odpowiada niezależny podmiot monitorujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu. Podmiot ten musi zostać akredytowany w tym celu przez organ nadzorczy jeszcze przed zatwierdzeniem kodeksu postępowania.

Jeszcze w 2020 roku Prezes UODO – działając na podstawie art. 41 ust. 3 RODO oraz art. 29 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, jak również Wytycznych Europejskiej Rady Ochrony Danych nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679[272] - przygotował projekt wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Dokument ten został przetłumaczony przez organ nadzorczy na język angielski, a następnie przekazany do EROD w trybie art. 64 RODO[273]. Po otrzymaniu opinii EROD w tej sprawie, Wymogi akredytacji zostały przyjęte i opublikowane w 2021 roku na stronie internetowej UODO[274].

Wnioski o udzielenie akredytacji do monitorowania kodeksów postępowania

W 2022 r. do UODO nie wpłynął żaden nowy wniosek o udzielenie akredytacji do monitorowania kodeksów postępowania. Może to być spowodowane tym, że opiniowanie przez Prezesa UODO projektów kodeksów postępowania wymaga od ich twórców odnoszenia się do uwag organu nadzorczego w ramach toczącego się postępowania, w tym korygowania zgłoszonych zastrzeżeń i proponowania nowych rozwiązań zgodnych z RODO, a jest to czasochłonne ze względu na wielość i obszerność zagadnień, których dotyczą kodeksy. Z kolei niezatwierdzenie kodeksu postępowania wyklucza możliwość udzielenia akredytacji podmiotowi monitorującemu. Akredytacja uprawnia bowiem do monitorowania przestrzegania konkretnego kodeksu postępowania.

Przyczyną problemów ze wskazaniem w projektach kodeksów postępowania podmiotu/podmiotów monitorujących kodeks lub zasad jego/ich wyłonienia można upatrywać w szczególności w braku takich wyspecjalizowanych jednostek na rynku, dysponujących

272 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pl.pdf
273 DOL.602.4.2020
274 https://archiwum.uodo.gov.pl/pl/138/1861

zasobami kadrowymi. Nie można zapominać, że uzyskanie akredytacji uprawniającej do monitorowania konkretnego kodeksu postępowania jest uzależnione od wyniku postępowania przed organem nadzorczym, podczas którego ocenia on, czy kandydat do pełnienia roli podmiotu monitorującego posiada m.in.:

- niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu;
- możliwości kadrowe (dostęp do fachowców/specjalistów);
- dysponuje procedurami, które pozwolą mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania;
- dysponuje procedurami i strukturami, które pozwolą mu rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwolą zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej;
- wiedzę fachową w dziedzinie będącej przedmiotem kodeksu.

Powyższe wynika z RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz przywołanych powyżej Wymogów akredytacji podmiotów monitorujących kodeksy postępowania, które stanowią doprecyzowanie.

W przypadku kodeksów postępowania, które mogłyby być stosowane przez organy i podmioty publiczne, wciąż nierozstrzygniętą kwestią jest sposób monitorowania przestrzegania tych kodeksów. Ze względu na konstytucyjną zasadę praworządności, zgodnie z którą organy władzy publicznej działają na podstawie i w granicach prawa, kwestie te niejednokrotnie powinny być rozstrzygnięte na poziomie legislacyjnym. W przepisach prawa powinny być również określone zasady dostępu do tajemnic prawnie chronionych w procesie monitorowania przestrzegania kodeksów postępowań.

Akredytacje udzielone przez organ nadzorczy

W 2022 r. po przeprowadzeniu pełnej oceny nowego wniosku RS JAMANO Sp. z o.o. sp.k.[275] o udzielenie akredytacji do monitorowania „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych" (poprzedni wniosek został pozostawiony bez rozpoznania w związku z nieuzupełnieniem braków formalnych) oraz załączonych dokumentów, organ nadzorczy udzielił akredytacji tej spółce. 14 grudnia 2022 r. odbyło się uroczyste wręczenie certyfikatu akredytacyjnego przedstawicielom spółki RS JAMANO Sp. z o.o. sp.k., która jest pierwszym podmiotem monitorującym kodeks postępowania, który został akredytowany przez organ nadzorczy.

275 DOL.420.9.2021.

Prowadzone postępowania o udzielenie akredytacji

W 2022 r. organ nadzorczy prowadził również postępowania o udzielenie akredytacji do monitorowania kodeksów postępowania wszczęte w 2021 r. na wniosek:

- KPMG Advisory Sp. z o.o. sp.k.[276] – wniosek o udzielenie akredytacji do monitorowania przestrzegania „Kodeksu postępowania dla sektora ochrony zdrowia".
  Jest to ponowny wniosek spółki (poprzedni został pozostawiony bez rozpoznania, w związku z nieuzupełnieniem braków formalnych). Organ nadzorczy dokonał pełnej oceny wniosku oraz załączonych dokumentów. W 2022 r. postępowanie w tej sprawie nie mogło być zakończone w związku z faktem, że Polska Federacja Szpitali, tj. wnioskodawca w sprawie dotyczącej zatwierdzenia ww. kodeksu, wciąż nie przedłożył organowi nadzorczemu odpowiednich propozycji monitorowania przestrzegania kodeksu przez podmioty publiczne, do czego był wzywany przez organ nadzorczy w postępowaniu dot. zatwierdzenia kodeksu;
- Prometriq Akademia Zarządzania Sp. z o.o.[277] – wniosek o udzielenie akredytacji do monitorowania przestrzegania „Kodeksu postępowania dla sektora ochrony zdrowia". Wniosek został poddany ocenie pod kątem formalnym. Wobec nieuzupełnienia braków formalnych przez spółkę, organ nadzorczy pozostawił wniosek bez rozpoznania;
- Krajowa Izba Doradców Podatkowych (KIDP)[278] – wniosek o udzielenie akredytacji podmiotowi monitorującemu „Kodeks postępowania Krajowej Izby Doradców Podatkowych w zakresie ochrony danych osobowych".

  Organ nadzorczy odmówił wszczęcia postępowania w ww. sprawie, gdyż projekt kodeksu nie został jeszcze pozytywnie zaopiniowany przez organ nadzorczy. Wcześniejsza opinia w sprawie kodeksu jest niezbędna, gdyż podmiot monitorujący może być akredytowany tylko do konkretnego kodeksu.

13. Certyfikacja

Certyfikacja jest nową instytucją prawną, nieznaną w uchylonych w 2018 r. przepisach o ochronie danych osobowych. Zgodnie z RODO, państwa członkowskie, organy nadzorcze, EROD oraz Komisja Europejska zachęcają do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, z uwzględnieniem szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Narzędzia te mają na celu nie tylko zapewnienie dodatkowych gwarancji dla osób, których dane dotyczą, ale również pozwolą tzw. podmiotom zobowiązanym na wdrożenie odpowiednich środków technicznych i organizacyjnych w rozumieniu RODO. Stosownie do art. 12 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, w Polsce certyfikacja będzie dokonywana przez podmioty certyfikujące, które będą posiadać stosowną

276 DOL.420.11.2021.
277 DOL.420.10.2021.
278 DOL.420.8.2021.

akredytację udzieloną przez Polskie Centrum Akredytacji (PCA). Akredytacja ta będzie dokonywana m.in. w oparciu o wymogi akredytacji podmiotów certyfikujących, o których mowa w art. 43 ust. 3 RODO, które – stosownie do przepisów RODO i ustawy o ochronie danych osobowych – opracowuje, zatwierdza i podaje do publicznej wiadomości Prezes UODO. W związku z przyjętym w Polsce modelem certyfikacji, zadaniem Prezesa UODO będzie również zatwierdzanie kryteriów certyfikacji, o których mowa w art. 42 ust. 5 RODO.

W styczniu 2022 r. polski organ nadzorczy przedłożył EROD do zaopiniowania – w trybie art. 64 RODO – **projekt dodatkowych wymogów akredytacji podmiotów certyfikujących**[279]. Projekt ten został przygotowany w oparciu m.in. o wytyczne EROD 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679).

4 lipca 2022 r. EROD wydała Opinię 11/2022 w sprawie projektu decyzji właściwego organu nadzorczego w Polsce w sprawie zatwierdzenia wymogów dotyczących akredytacji podmiotów certyfikujących zgodnie z art. 43 ust. 3 (RODO)[280], którą polski organ nadzorczy przyjął w całości. Uwagi EROD spowodowały konieczność wprowadzenia zmian do ww. projektu dodatkowych wymogów akredytacji podmiotów certyfikujących.

14. Pytania prawne, wnioski o dostęp do informacji i wystąpienia Prezesa UODO

Inicjowanie i podejmowanie działań w zakresie doskonalenia ochrony danych osobowych obejmuje w szczególności udzielanie odpowiedzi na pytania dotyczące interpretacji oraz stosowania przepisów prawa o ochronie danych osobowych, a także kierowanie wystąpień do właściwych podmiotów, w celu zapewnienia skutecznej ochrony danych osobowych. Zgodnie z art. 57 ust. 1 RODO, Prezes Urzędu Ochrony Danych Osobowych, w ramach swoich kompetencji, m.in. upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz udziela osobie, której dane dotyczą, na jej żądanie informacji o jej prawach wynikających z RODO. Ponadto zgodnie z art. 57 ust. 3 RODO, zadaniem organu nadzorczego jest bezpłatne wypełnianie zadań na rzecz osoby, której dane dotyczą, i – gdy ma to zastosowanie – inspektora ochrony danych.

14.1. Pytania prawne

Mimo że udzielanie odpowiedzi na pytania prawne nie zostało wprost ujęte wśród kompetencji organu właściwego w sprawach ochrony danych osobowych, to stanowi ważny wyraz jego troski o upowszechnianie i doskonalenie wiedzy w tym zakresie. Jednocześnie problemy podnoszone w pismach z pytaniami stanowią często impuls do podjęcia określonych

279 DOL.602.1.2022.
280 https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112022-draft-decision-competent_pl

działań z urzędu (takich jak np. komunikaty, poradniki, wystąpienia). Niejednokrotnie bowiem organowi nadzorczemu w tego typu korespondencji sygnalizowane są problemy wspólne dla różnych grup podmiotów.

W roku 2022 administratorzy oraz osoby fizyczne skierowali do Urzędu Ochrony Danych Osobowych 1784 pisma z pytaniami prawnymi, zaś 274 pisma wpłynęły od inspektorów ochrony danych.

W sumie, w 2022 r. do UODO wpłynęło 2058 pytań prawnych. To znacznie mniej niż w latach ubiegłych, kiedy wpłynęło ich odpowiednio 2774 w roku 2022 i 2141 w roku 2021. Spadek liczby wpływających pytań może być spowodowany tym, że wiele kwestii zostało już przez organ nadzorczy wyjaśnionych, np. w komunikatach zamieszczonych na stronie internetowej Urzędu czy w Newsletterze UODO dla IOD.

W roku 2022 **rozpatrzonych** zostało **1766 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 szczególną rolę, jaką osoby wykonujące tę funkcję mają pełnić w systemie ochrony danych osobowych – podchodzi ze szczególną uwagą. W 2022 roku do UODO wpłynęły **274 pytania od inspektorów ochrony danych** (IOD). Udzielono zaś **294 odpowiedzi** na pytania od IOD.

14.1.1. Pytania prawne od administratorów i osób fizycznych

Kwestie, o które pytali administratorzy i osoby fizyczne, dotyczyły różnych aspektów przetwarzania danych osobowych oraz stosowania nie tylko RODO, ale także innych, szczególnych przepisów prawa.

Wśród najczęściej poruszanych lub szczególnie interesujących zagadnień, na które zwrócili uwagę administratorzy i osoby fizyczne w przesłanych do Urzędu pytaniach, a które stały się przedmiotem analiz organu, były takie kwestie, jak:

1) określenie statusu podmiotów w procesie przetwarzania danych osobowych,
2) przetwarzanie danych osobowych w związku z zatrudnieniem,
3) stosowanie monitoringu wizyjnego,
4) przetwarzanie danych osobowych przez podmioty publiczne,
5) udostępnianie danych osobowych.

Na plan dalszy zeszła kwestia przetwarzania danych osobowych w związku z pandemią COVID-19. UODO stanął zaś przed nowymi wyzwaniami. Zajmował się – zwłaszcza na początku roku - m.in. kwestiami przetwarzania danych osobowych obywateli Ukrainy licznie przybywających do Polski w związku z aktualną sytuacją w ich kraju[281] czy interpretacją

281 Zob. https://www.uodo.gov.pl/pl/138/2436

przepisów w związku z obowiązkiem prowadzenia rejestru umów[282] przez jednostki sektora finansów publicznych[283].

Wątpliwości co do statusu administratora

Choć organ nadzorczy wielokrotnie zajmował stanowisko w kwestii statusu administratora[284], to w roku 2022 wciąż wpływały pytania – głównie od podmiotów publicznych – dotyczące tej kwestii.

Wątpliwości co do statusu administratora w odniesieniu do administracji samorządowej zespolonej w województwie miał jeden z sejmików województwa[285]. W odpowiedzi wskazano, że w tym zakresie kluczowe znaczenie mają definicja administratora[286] oraz Wytyczne Europejskiej Rady Ochrony Danych nr 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. Organ nadzorczy wyjaśniał, że w przypadku szeroko rozumianego sektora publicznego podmiot będący administratorem może być wprost wskazany w konkretnym przepisie prawa, jednak najczęściej ma miejsce sytuacja, w której wskazanie podmiotu pełniącego tę rolę wymaga analizy przepisów stanowiących podstawę przetwarzania danych osobowych. O tym, czy dany podmiot publiczny jest administratorem, decydują wówczas przede wszystkim rodzaj i charakter nadanych mu przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania. Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ocena będzie zależała od tego, o jakie dane osobowe oraz o jakie zadania chodzi w określonym przypadku.

Organ podkreślał, że istnieją przypadki, w których administrator lub kryteria jego wyznaczania są wprost określone w przepisie prawa, jednak bardziej powszechne są sytuacje, w których status ten wynika z tego, że ustawa nakłada na dany podmiot zadanie lub obowiązek gromadzenia i przetwarzania określonych danych. Wówczas administratorem jest zwykle organ wyznaczony na mocy prawa do realizacji tego zadania publicznego. W takim przypadku prawo, choć pośrednio, określa, kto jest administratorem. Innymi słowy, prawo może nakładać na podmioty publiczne lub prywatne obowiązek przetwarzania określonych danych, a podmioty te uznawane są zazwyczaj za administratorów w odniesieniu do przetwarzania, które jest niezbędne do wykonania tego obowiązku.

Biorąc pod uwagę powyższe, stwierdzono, że w zależności od konkretnego procesu przetwarzania danych osobowych w ramach struktur samorządu województwa, w tym

282 Obowiązek ten został wprowadzony przepisami ustawy z dnia 14 października 2021 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 2054 z późn. zm.).
283 Np. DOL.023.47.2022, DOL.023.402.2022.
284 Zob. https://archiwum.uodo.gov.pl/pl/225/2018 lub w tekście: „Komendant straży w strukturach gminy jako niezależny administrator" umieszczonym w Newsletterze UODO dla IOD nr 4/2019.
285 DOL.023.521.2022.
286 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.

w zależności od celów przetwarzania oraz podstawy prawnej przetwarzania i kompetencji poszczególnych podmiotów (organów), administratorem może być np. marszałek województwa, urząd marszałkowski, sejmik województwa czy radny tego sejmiku. Uprawnienia organów jednostek samorządu – jako administratorów – podlegają dekoncentracji, w ślad za merytoryczną kompetencją, z którą związane jest przetwarzanie danych osobowych. Realizacja koncepcji jednego administratora w samorządzie województwa – o co wnioskował sejmik – nie jest możliwa do wprowadzenia bez zmian w obowiązujących przepisach prawa, gdyż to z nich wynikają określone zadania dla określonych podmiotów, które faktycznie, a nie jedynie formalnie podejmują decyzje o celu i sposobie przetwarzania danych. Rola administratora czy też współadministratora jest kształtowana na podstawie obowiązujących przepisów prawa materialnego regulującego zadania i cele funkcjonowania danego podmiotu. Tylko taki podmiot, który ma faktyczny wpływ na proces przetwarzania danych, jest też w stanie ponieść odpowiedzialność za ten proces.

Jeden z ośrodków pomocy społecznej miał podobne wątpliwości przy określeniu administratora w przypadku udziału ośrodka w programach realizowanych przez gminę, takich jak Program „Asystent osobisty osoby niepełnosprawnej" oraz Program „Opieka wytchnieniowa"[287]. Organ nadzorczy podkreślił, że prawidłowe ustalenie statusu administratora nie jest możliwe bez analizy zróżnicowanych form prawnych oraz organizacyjnych podmiotów, które faktycznie decydują o celach i sposobach przetwarzania, a przede wszystkim posiadają przypisane im prawnie autonomiczne cele przetwarzania. Nawet jeśli gmina jest wskazana jako administrator, ale zadanie jest scedowane na jednostkę gminną, np. ośrodek pomocy społecznej i to ta jednostka faktycznie je realizuje na podstawie także odrębnych przepisów, to nie można takiej jednostki pominąć przy ostatecznym kształtowaniu jej statusu i odpowiedzialności jako administratora. Nie oznacza to, że gmina/powiat nie będą realizować autonomicznie – jako administrator – celów, np. związanych z kontrolą sposobu realizacji zadania przez rzeczoną jednostkę organizacyjną.

Przetwarzanie danych osobowych w związku z zatrudnieniem

W 2022 r. – podobnie jak w latach ubiegłych – do UODO wpłynęło wiele pytań dotyczących przetwarzania danych osobowych w związku z zatrudnieniem od pracodawców, pracowników, związków zawodowych czy społecznych inspektorów pracy. Dotyczyły one głównie przechowywania oraz udostępniania danych osobowych innym podmiotom, ale także wykorzystywania nowych technologii takich jak czytniki danych biometrycznych.

287 DOL.023.194.2022.

1. Praktyki pracodawców

Weryfikacja informacji o zaszczepieniu przez pracodawcę będącego podmiotem leczniczym.

Na początku 2022 roku – w związku z jeszcze panującym w kraju stanem epidemii – częste były pytania odnośnie do pozyskiwania od pracowników pracujących w podmiotach leczniczych informacji o zaszczepieniu przeciwko COVID-19[288]. Organ nadzorczy wskazywał, że nie zostały wdrożone przepisy prawa, które uprawniałyby pracodawców do żądania od pracowników informacji o odbyciu szczepienia ochronnego i kształtujące po stronie pracowników obowiązek ich ujawnienia. Z przepisów prawa pracy takie uprawnienia nie wynikają, nie zostały one również wyjątkowo (jako epizodyczne) przyznane pracodawcom mocą przepisów specustawy na szczególny czas pandemii, co pozwalałoby im na pozyskiwanie od pracowników informacji o odbyciu szczepienia ochronnego przeciwko COVID-19 – uprawnienia takie przyznano jedynie określonym służbom i ich organom. § 12a rozporządzenia Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii[289] nakładał obowiązek szczepień przeciw COVID-19 na osoby wykonujące zawód medyczny, osoby świadczące usługi farmaceutyczne i studentów kształcących się na kierunkach przygotowujących do wykonywania zawodu medycznego, jeśli osoby te nie mają przeciwwskazań do szczepienia w zakresie stanu ich zdrowia. Przepis nie precyzował jednak, w jaki sposób powinna odbywać się weryfikacja wypełnienia przez wskazane podmioty nałożonego obowiązku – co powinno także wynikać z przepisów prawa.

Organ nadzorczy podkreślał, że informacje dotyczące szczepienia przeciw COVID–19 stanowią dane dotyczące zdrowia, których przetwarzanie jest – zgodnie z art. 9 ust. 1 RODO – co do zasady zabronione, chyba że spełni się jeden z wymogów wskazanych w art. 9 ust. 2 RODO. Zgodnie z art. 22^{1b} ustawy z dnia 26 czerwca 1974 r. Kodeks pracy[290] zgoda może stanowić podstawę przetwarzania przez pracodawcę danych wrażliwych, w tym danych dotyczących zdrowia, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Warunki pozyskania zgody muszą być ściśle zachowane (art. 4 pkt 11 i art. 7 RODO), a więc musi być ona dobrowolna, świadoma, konkretna – wyrażona w formie jednoznacznego okazania woli i możliwa do odwołania w każdym czasie. Skoro zatem brak jest regulacji, które określałyby zarówno szczególne warunki dla zobowiązywania osób wykonujących zawody medyczne do udostępniania danych o szczepieniach bez ich zgody, jak i formy dokumentowania zaistnienia tej okoliczności, np. poprzez przedstawienie certyfikatów poświadczających odbycie szczepienia, to w tym przypadku nie znajduje uzasadnienia eliminowanie przesłanki zgody.

288 Np.: DOL.023.212.2022, DOL.023.213.2022, DOL.023.246.2022.
289 Dz.U. z 2022 r. poz. 340; akt utracił moc z dniem 16 maja 2022 r.
290 Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2022 r. poz. 1510 z późn. zm.), dalej: „kodeks pracy".

Tworzenie tzw. czarnych list lub szarych list w procesie rekrutacji

Do UODO wpłynęło też pytanie, czy pracodawca może tworzyć i wymieniać się z innymi pracodawcami listami pracowników, którzy nie pasują do zespołu ze względu na posiadane cechy osobowościowe sprzeczne z zasadami i standardami firmy, np. ze względu na to, że wykazuje cechy homofobiczne czy ksenofobiczne bądź jego metody zarządzania opierają się na przemocy psychicznej w stosunku do podwładnych (tworzenie tzw. czarnych lub szarych list)[291]. Organ nadzorczy jednoznacznie wskazał, że za niedopuszczalne uznaje się tworzenie takich list osób ubiegających się o zatrudnienie. Tworzenie zbiorów danych o charakterze negatywnym może prowadzić do dyskryminacji i podejmowania niekorzystnych dla danej osoby decyzji na podstawie często nierzetelnych, bezpodstawnie pozyskanych informacji. Tworzenie tzw. czarnych/szarych list, zwłaszcza przy braku jasnych, obiektywnych i uzasadnionych kryteriów w tym zakresie, nie jest zasadne jako praktyka np. firmy rekrutacyjnej służąca przeciwdziałaniu mobbingowi w rozumieniu art. 943 Kodeksu pracy, ponieważ może ona budzić wątpliwości m.in. z punktu widzenia zasady zgodności z prawem i rzetelności (art. 5 ust. 1 lit. a RODO). Podkreślono także, że podstawy prawnej w przepisach obowiązującego prawa nie znajduje wymienianie się informacjami pomiędzy pracodawcami o kandydatach do pracy, których zatrudniać nie chcą.

Wykorzystywanie przez pracodawcę czytnika danych biometrycznych lub linii papilarnych do ewidencjonowania czasu pracy

Jedno z pytań skierowanych do UODO dotyczyło legalności wykorzystywania przez pracodawcę czytnika danych biometrycznych w celu ewidencjonowania czasu pracy[292]. Jak wskazano w odpowiedzi pracodawca, wykorzystując dane biometryczne pracownika do rejestracji czasu pracy, naruszyłby zasady określone w RODO (art. 5 ust. 1), ponieważ nie byłby w stanie wykazać, dlaczego i na jakiej podstawie prawnej przetwarza dane biometryczne pracowników do celów związanych z weryfikowaniem ich obecności w pracy. Każdy administrator, czyli również pracodawca, w zakresie danych osobowych pracowników zobowiązany jest bowiem przetwarzać je zgodnie z zasadami, o których mowa w art. 5 ust. 1 RODO, w tym zgodności z prawem, ograniczenia celu oraz minimalizacji. Ponadto w tej sytuacji zastosowanie mają przepisy prawa pracy, które szczegółowo wskazują, jakie dane pracownika może przetwarzać pracodawca.

Stosownie do art. 4 pkt 14 RODO linie papilarne należy zaliczyć do danych biometrycznych[293]. Z treści art. 9 ust. 1 RODO wynika, że dane biometryczne należą do szczególnych kategorii danych osobowych, których przetwarzanie jest co do zasady zabronione, chyba że administrator spełnia jeden z warunków, o których mowa w ust. 2 tego przepisu. Jeśli chodzi o sektor zatrudnienia, to warunki dopuszczalności przetwarzania

291 DOL.023.590.2022.
292 DOL.023.803.2022.
293 Art. 4 pkt 14 RODO: „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

danych biometrycznych zostały określone w przepisach prawa pracy. Nie dają one podstawy prawnej do przetwarzania przez pracodawcę danych biometrycznych pracowników w celu rejestracji czasu pracy. Zgodnie bowiem z art. 22^{1b} Kodeksu pracy szczególne kategorie danych, w tym dane biometryczne, mogą być przetwarzane przez pracodawcę w dwóch sytuacjach: 1) za zgodą pracownika wyłącznie w przypadku, gdy ich przekazanie następuje z inicjatywy tych osób, przy czym pracodawca musi pamiętać, że – zgodnie z art. 22^{1a} § 2 Kodeksu pracy – brak zgody lub jej wycofanie nie może być podstawą niekorzystnego traktowania pracownika, a także nie może powodować wobec niego żadnych negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny wypowiedzenia umowy o pracę lub jej rozwiązania bez wypowiedzenia przez pracodawcę; ponadto zgoda musi spełniać warunki określone w art. 4 pkt 11, art. 7 i art. 9 ust. 2 lit. a) RODO lub 2) wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

Kontrola i weryfikacja absencji chorobowej pracowników

Od jednego z pracowników organ nadzorczy otrzymał pytanie dotyczące wdrożenia przez pracodawcę usługi kontroli i weryfikacji absencji chorobowej pracowników[294]. Temat ten został także później opisany w Newsletterze dla IOD[295]. W przygotowanym materiale wskazano, że kwestię kontroli przez pracodawcę nieobecności pracowników w pracy z powodu choroby lub konieczności sprawowania opieki nad chorym dzieckiem lub innym chorym członkiem rodziny regulują: ustawa z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa[296] oraz rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich[297]. Stosownie do art. 68 ust. 1 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa Zakład Ubezpieczeń Społecznych oraz płatnicy składek, o których mowa w art. 61 ust. 1 pkt 1 tej ustawy (tj. tacy, którzy zgłaszają do ubezpieczenia chorobowego powyżej 20 ubezpieczonych), są uprawnieni do kontrolowania ubezpieczonych co do prawidłowości wykorzystywania zwolnień od pracy zgodnie z ich celem oraz są upoważnieni do formalnej kontroli zaświadczeń lekarskich.

Pracodawca uprawniony do kontroli prawidłowości wykorzystywania zwolnień lekarskich może taką kontrolę przeprowadzić sam lub upoważnić do tego swoich pracowników bądź

294 DOL.023.374.2022.
295 Newsletter UODO dla IOD 5/2022.
296 Ustawa z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (t.j. Dz. U. z 2022 r. poz. 1732 z późn. zm.), dalej: „ustawa o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa".
297 Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 27 lipca 1999 r. w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich (Dz. U. Nr 65, poz. 743), dalej: „rozporządzenie w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich".

zlecić jej przeprowadzenie podmiotowi zewnętrznemu. Jeśli korzysta z tego ostatniego rozwiązania, ważne jest, by z podmiotem, któremu zleca takie zadanie, zawarł umowę powierzenia przetwarzania danych osobowych. Pamiętać przy tym trzeba o poszanowaniu zasady minimalizacji danych w rozumieniu art. 5 ust. 1 lit. c) RODO. W praktyce oznacza to m.in., że osobie kontrolującej nie można przekazać informacji o przyczynie wydania zwolnienia lekarskiego, a także nie ma ona prawa wymagać od osoby kontrolowanej podania informacji na temat swojego stanu zdrowia.

Co ważne, pracodawca, który zlecił podmiotowi zewnętrznemu przeprowadzenie kontroli, nadal pozostaje administratorem danych osobowych swoich pracowników i jest odpowiedzialny za to, by były one przetwarzane zgodnie z przepisami o ochronie danych osobowych.

Organ nadzorczy zaznaczył też, że zgodnie z § 8 rozporządzenia w sprawie szczegółowych zasad i trybu kontroli prawidłowości wykorzystywania zwolnień lekarskich od pracy oraz formalnej kontroli zaświadczeń lekarskich osobie kontrolującej prawidłowość wykorzystywania zwolnień lekarskich od pracy płatnik składek wystawia imienne upoważnienie według wzoru stanowiącego załącznik nr 1 do rozporządzenia. Upoważnienie jest ważne łącznie z legitymacją pracowniczą albo dokumentem tożsamości, których numery powinny być podane w upoważnieniu. Uprawnia ono do wykonywania kontroli w miejscu zamieszkania, miejscu czasowego pobytu lub miejscu zatrudnienia osoby kontrolowanej[298].

Przechowywania aktu urodzenia dziecka w aktach osobowych pracownika

Inne ze skierowanych do Urzędu pytań dotyczyło kwestii przechowywania aktu urodzenia dziecka w aktach osobowych pracownika. W udzielonej na nie odpowiedzi[299] wskazano, że urlop rodzicielski to jedno z określonych przepisami kodeksu pracy uprawnień przysługujących ojcu i matce dziecka, a także rodzicom adopcyjnym oraz że to przepisy prawa pracy są podstawą uprawniającą pracodawcę do przechowywania aktu urodzenia dziecka w aktach osobowych pracownika, który chce skorzystać z urlopu rodzicielskiego.

Zgodnie bowiem z § 2 ust. 2 oraz § 4 ust. 2 rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 8 grudnia 2015 r. w sprawie wniosków dotyczących uprawnień pracowników związanych z rodzicielstwem oraz dokumentów dołączanych do takich wniosków[300] do wniosku, o którym mowa w art. 179^1 § 1 Kodeksu pracy, tj. do wniosku o udzielenie pracownicy lub pracownikowi, bezpośrednio po urlopie macierzyńskim, urlopu rodzicielskiego w pełnym wymiarze, dołącza się skrócony odpis aktu urodzenia dziecka (dzieci) lub zagraniczny akt urodzenia dziecka (dzieci) albo kopie tych dokumentów, albo kopię zaświadczenia lekarskiego wystawionego na zwykłym druku, określającego przewidywaną datę porodu. Stosownie zaś do § 4 ust. 4 ww. rozporządzenia, przepisy ust.

298 Dopuszczalność takiego postępowania została potwierdzona w decyzji Prezesa UODO, sygn.: ZSZZS.440.727.2018.
299 DOL.023.442.2022; omówionej także w Newsletterze UODO dla IOD 6/2022.
300 Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 8 grudnia 2015 r. w sprawie wniosków dotyczących uprawnień pracowników związanych z rodzicielstwem oraz dokumentów dołączanych do takich wniosków (Dz. U. poz. 2243).

1–3 stosuje się odpowiednio do wniosku o udzielenie urlopu rodzicielskiego złożonego przez pracownika, który przyjął dziecko na wychowanie i wystąpił do sądu opiekuńczego z wnioskiem o wszczęcie postępowania w sprawie przysposobienia dziecka lub przyjął dziecko na wychowanie jako rodzina zastępcza.

Zakres, sposób i warunki prowadzenia oraz przechowywania dokumentacji pracowniczej są z kolei określone w rozporządzeniu Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej[301]. Stanowi ono, że akta osobowe pracownika składają się z czterech części[302] i wskazuje, jaki rodzaj oświadczeń i dokumentów znajduje się w każdej z nich. Zgodnie z § 3 pkt 2 lit. m tego rozporządzenia, w części B akt osobowych pracownika gromadzone są dokumenty związane z ubieganiem się i korzystaniem przez pracownika z urlopu macierzyńskiego, urlopu na warunkach urlopu macierzyńskiego, urlopu rodzicielskiego, urlopu ojcowskiego lub urlopu wychowawczego. Zatem to powołane wyżej przepisy uprawniają pracodawcę do przechowywania w części B akt osobowych pracownika zarówno wniosku o urlop rodzicielski, jak i dołączanego do niego skróconego odpisu aktu urodzenia dziecka (dzieci) lub zagranicznego aktu urodzenia dziecka (dzieci) albo kopii tych dokumentów.

Wykorzystywanie służbowego adresu e-mail byłego pracownika

W 2022 r. do UODO wpłynęło też pytanie, czy pracodawca może używać służbowego adresu e-mail byłego pracownika[303]. Odpowiadając na nie, organ nadzorczy wskazał, że imienny adres e-mail zawiera dane z zakresu tzw. danych zwykłych, których przetwarzanie regulowane jest przepisami RODO i musi być zgodne z zasadami zawartymi w jego art. 5. Jeśli pracodawca nadal posiada aktywny adres poczty elektronicznej byłego pracownika, który był przypisany do niego w czasie pełnienia obowiązków, to pozostaje administratorem tych danych. W omawianym przypadku podstawą przetwarzania danych byłego pracownika zawartych w adresie e-mailowym może być realizacja prawnie uzasadnionego interesu administratora. Ważne jednak, aby administrator miał świadomość, że prawnie uzasadnione interesy administratora mogą stanowić podstawę do przetwarzania tylko w sytuacji, w której mają one nadrzędny charakter w stosunku do interesów lub podstawowych praw i wolności osób, których dane dotyczą. Zdaniem organu nadzorczego dane byłego pracownika mogą być używane przez pracodawcę jedynie w sytuacjach, gdy klient podejmuje próbę kontaktu i jedynie w celu wskazania aktualnych danych kontaktowych. Adres e-mailowy zawierający imię i nazwisko byłego pracownika nie może być aktywnie wykorzystywany przez administratora przez czas nieokreślony i w dowolnych dalszych celach, np. do pozyskiwania nowych klientów. Jednocześnie organ przypomniał, że szerzej zagadnienie to zostało omówione na stronie internetowej Urzędu[304].

301 Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej (Dz. U. poz. 2369 z późn. zm.).

302 Nowelizacja rozporządzenia – będąca w 2022 r. na etapie uzgodnień – wprowadziła piątą część akt osobowych pracownika – część E.

303 DOL.023.511.2022.

304 M.in. w materiale: *Czy pracodawca może używać imiennego adresu e-mail byłego pracownika?* dostępnym na stronie internetowej

2. Związki zawodowe, społeczni inspektorzy pracy

Pozyskiwanie przez związek zawodowy informacji o wysokości wynagrodzenia na poszczególnych stanowiskach pracy

Jeden ze związków zawodowych zwrócił się do Prezesa UODO z prośbą o ocenę legalności pozyskiwania informacji o wysokości wynagrodzeń na poszczególnych stanowiskach pracy[305]. W odpowiedzi organ nadzorczy wskazał, że ponieważ informacja o wysokości wynagrodzenia pracownika należy do kategorii danych osobowych w rozumieniu art. 4 pkt 1 RODO, to związek zawodowy, który chciałby pozyskiwać od pracodawcy dane o wynagrodzeniu pracowników, powinien wykazać, że jego żądanie znajduje uzasadnienie w jednej z przesłanek przewidzianych w art. 6 ust. 1 RODO.

Zgodnie z art. 28 ust. 1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych[306], pracodawca jest obowiązany udzielić na wniosek zakładowej 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, przewidywanych zmian zatrudnienia oraz działań mających na celu utrzymanie poziomu zatrudnienia; 4) działań, które mogą powodować istotne zmiany w organizacji pracy lub podstawach zatrudnienia.

UODO wskazał, że przy wątpliwościach co do interpretacji powyższego przepisu warto odwołać się do orzecznictwa sądowego. Zgodnie z wyrokiem Sądu Apelacyjnego w Białymstoku z 25 czerwca 2014 r. (sygn. akt III AUa 2078/13) pojęcia „informacji o zasadach wynagradzania" nie można rozumieć tylko jako 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 wystarczające jest pozyskanie informacji przetworzonych w postaci danych statystycznych dotyczących zasad wynagradzania poszczególnych grup pracowników. Z kolei w wyroku WSA w Warszawie z 2 listopada 2005 r. (sygn. akt VI SA/Wa 1080/2005) wskazano, że zgodnie z art. 51 ust. 1 Konstytucji RP nikt nie może być obowiązany inaczej, niż na podstawie ustawy, do ujawniania informacji dotyczących jego osoby. Prawo do wynagrodzenia może być dobrem osobistym, które co do zasady zgodnie z przepisem art. 24 k.c. pozostaje pod ochroną prawa cywilnego.

UODO pod linkiem: https://archiwum.uodo.gov.pl/pl/138/1312

305 DOL.023.368.2022.

306 Ustawa z dnia 23 maja 1991 r. o związkach zawodowych (t.j. Dz. U. z 2022 r. poz. 854), dalej: „ustawa o związkach zawodowych".

Udostępnianie danych osobowych pracowników związkowi zawodowemu w celu przeprowadzenia referendum strajkowego

Przedmiotem rozważań UODO było także zagadnienie udostępniania związkowi zawodowemu danych osobowych pracowników w celu przeprowadzenia referendum strajkowego[307]. W ocenie organu właściwego w sprawach ochrony danych osobowych (wyrażanej konsekwentnie od wielu lat[308]) obowiązujące przepisy prawa dają podstawę do udostępnienia określonych danych osobowych na rzecz organizacji związkowych w celu organizacji i przeprowadzenia referendum strajkowego. Wynika to zarówno z art. 20 ustawy z dnia 23 maja 1991 r. o rozwiązywaniu sporów zbiorowych[309], jak i z art. 28 ustawy o związkach zawodowych. Wprawdzie ustawa o związkach zawodowych nie precyzuje, jakiego rodzaju informacje są niezbędne do prowadzenia działalności związkowej i wprost nie stanowi o czynności udostępnienia danych osobowych pracowników przez pracodawcę, niemniej z wielu jej przepisów wynika obowiązek podjęcia przez organizację związkową jako odrębnego administratora określonych działań z udziałem określonej liczby pracowników zatrudnionych u danego pracodawcy, a także nakładane są na nią określone reguły szczególnej staranności w procesie przeprowadzenia referendum strajkowego, włącznie z odpowiedzialnością karną za przeprowadzenie referendum niezgodnie z przepisami prawa[310]. Odpowiedzialność ta jest także szczególnie podkreślana w judykaturze[311].

Organizując referendum strajkowe, organizacja związkowa musi zatem zapewnić, aby udział w referendum wzięły wyłącznie uprawnione osoby. Nie dysponując jednak listą osób zatrudnionych w danym zakładzie pracy, organizacja nie będzie w stanie rzetelnie zweryfikować, czy głosujący są osobami uprawnionymi do głosowania, a tym samym – zapewnić zgodnego z prawem przeprowadzenia referendum. W związku z tym udostępnienie przez pracodawcę związkowi zawodowemu – na jego wniosek – listy pracowników obejmującej np. imię, nazwisko i służbowe dane do kontaktu (jako dane związane z zatrudnieniem pracowników) na potrzeby przeprowadzenia referendum strajkowego nie będzie naruszać zasad ochrony danych osobowych, gdyż w ten sposób będzie dochodziło do przetwarzania niezbędnego dla realizacji obowiązków wskazanych w wymienionych przepisach prawa. Pracodawca – jako administrator danych pracowników – rozpatrując wniosek organizacji związkowej, powinien ocenić przede wszystkim, czy jest on należycie uzasadniony, a także czy zakres żądanych danych osobowych jest adekwatny do celu, w jakim dane mają być przetwarzane. Odpowiada bowiem za realizację zasad ochrony danych osobowych i musi być w stanie wykazać, że ich przestrzega (art. 5 RODO).

307 DOL.023.797.2022.

308 M.in. w materiale: *RODO pozwala pozyskać dane pracowników na potrzeby referendum strajkowego* zamieszczonym na stronie UODO pod linkiem: https://archiwum.uodo.gov.pl/pl/138/756

309 Ustawa z dnia 23 maja 1991 r. o rozwiązywaniu sporów zbiorowych (t.j. Dz. U. z 2020 r. poz. 123), dalej: „ustawa o rozwiązywaniu sporów zbiorowych".

310 Zgodnie z art. 26 ustawy o rozwiązywaniu sporów zbiorowych: 1. Kto w związku z zajmowanym stanowiskiem lub pełnioną funkcją 1) przeszkadza we wszczęciu lub w prowadzeniu w sposób zgodny z prawem sporu zbiorowego, 2) nie dopełnia obowiązków określonych w tej ustawie – podlega grzywnie albo karze ograniczenia wolności 2. Tej samej karze podlega ten, kto kieruje strajkiem lub inną akcją protestacyjną zorganizowaną wbrew przepisom ustawy. 3. Za szkody wyrządzone strajkiem lub inną akcją protestacyjną zorganizowaną wbrew przepisom ustawy organizator ponosi odpowiedzialność na zasadach określonych w Kodeksie cywilnym.

311 Np. w wyroku Sądu Najwyższego z 24 września 2013 r. sygn. akt III PK 90/12.

Pozyskiwanie danych osobowych pracowników w związku z wyborami społecznego inspektora pracy

Jeden ze związków zawodowych zwrócił się do UODO z pytaniem o legalność udostępnienia przez pracodawcę danych osobowych pracowników w celu przeprowadzenia wyborów społecznego inspektora pracy[312]. Organ nadzorczy wskazał, że pracodawca (jako administrator) ma prawo przetwarzać dane osobowe pracowników w taki sposób i w takim zakresie, który wynika z przepisów prawa pracy. Nie ulega przy tym wątpliwości, że obowiązkiem każdego administratora jest przestrzeganie zasad przetwarzania danych określonych w RODO, w tym zasady zgodności z prawem, która stanowi, że dane osobowe muszą być przetwarzane na podstawie przynajmniej jednej z przesłanek określonych w art. 6 ust. 1 RODO (w przypadku danych zwykłych) albo w art. 9 ust. 2 RODO (w przypadku danych szczególnej kategorii). Jednocześnie – stosownie do art. 88 RODO – państwa członkowskie mogą zawrzeć w przepisach krajowych bardziej szczegółowe regulacje mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników.

W świetle art. 6 ust. 6 ustawy z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy[313], wybory społecznego inspektora pracy przeprowadza zakładowa organizacja związkowa na podstawie uchwalonego przez siebie regulaminu. W pierwszej kolejności to on powinien określać sposób przeprowadzenia takich wyborów, a organizacja chcąca je zorganizować powinna mieć status organizacji związkowej. Jak zaznaczono, kodeks pracy nie określa kwestii udostępniania danych pracownika (w tym służbowego adresu e-mail) na rzecz organizacji związkowej celem przeprowadzenia wyboru społecznego inspektora pracy. Zdaniem organu nadzorczego jeżeli jednak organizacja ma swoich członków, to powinna pozyskać ich dane kontaktowe bezpośrednio od nich.

Pozyskiwanie dokumentacji zawierającej dane osobowe pracowników przez społecznego inspektora pracy

Jeden ze społecznych inspektorów pracy zapytał UODO o możliwość pozyskiwania przez niego od pracodawcy dokumentacji zawierającej dane osobowe pracowników[314]. W odpowiedzi UODO wskazał, że zgodnie z art. 8 ust. 2 ustawy o społecznej inspekcji pracy 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. UODO zaznaczył jednak, że na podstawie wyroku Trybunału Konstytucyjnego z dnia 26 kwietnia 2018 r., przepis ten utracił moc z dniem 2 maja 2018 r. w zakresie, w jakim nie uzależnia obowiązku udzielenia społecznemu inspektorowi pracy informacji oraz okazania mu dokumentów od uzyskania zgody pracownika w przypadkach, w których realizacja tego obowiązku wiązałaby się z udostępnianiem danych osobowych

312 DOL.023.192.2022.
313 Ustawa z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy (t.j. Dz. U. z 2015 r. poz. 567 z późn. zm.), dalej: „ustawa o społecznej inspekcji pracy".
314 DOL.023.410.2022.

tego pracownika. Trybunał podkreślił, że ochrona życia prywatnego w sposób konieczny obejmuje bowiem także autonomię informacyjną, która oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących siebie, jak również prawo do kontrolowania tych informacji, jeżeli znajdują się w dyspozycji innych podmiotów[315]. Powyższe rozstrzygnięcie stawia zatem prymat autonomii informacyjnej pracownika nad prawem do pozyskiwania bez wiedzy i zgody pracownika informacji na jego temat i dostępu do jego danych przez społecznego inspektora pracy[316].

3. Inne pytania

Stosowanie monitoringu wizyjnego, w tym pozyskiwanie i udostępnianie nagrań, to temat częstych pytań kierowanych do UODO. Nie zabrakło ich również w roku 2022.

Monitoring zainstalowany przez lokatora a czynności o domowym (osobistym) charakterze

Jedno z pytań dotyczyło tego, czy zainstalowanie monitoringu przez jednego z lokatorów budynku można uznać za czynność o czysto osobistym lub domowym charakterze, w przypadku której RODO nie ma zastosowania[317]. Organ nadzorczy przypomniał, że w sytuacji zainstalowania przez osobę fizyczną kamer monitorujących – prócz prywatnej przestrzeni – również przestrzeń publiczną nie można zastosować wyłączenia przewidzianego w art. 2 ust. 2 lit. c) RODO. Tym samym jego przepisy mają wówczas zastosowanie. Potwierdza to wyrok TSUE z 11 grudnia 2014 r. w sprawie C-212/13, przesądzający, że art. 3 ust. 2 tiret drugie dyrektywy 95/46 należy interpretować w ten sposób, że wykorzystywanie systemu kamer przechowującego zapis obrazu osób na sprzęcie nagrywającym w sposób ciągły, takim jak dysk twardy, zainstalowanego przez osobę fizyczną na jej domu rodzinnym w celu ochrony własności, zdrowia i życia właścicieli domu, który to system monitoruje również przestrzeń publiczną, nie stanowi przetwarzania danych w trakcie czynności o czysto osobistym lub domowym charakterze w rozumieniu tego przepisu[318]. W związku z tym – zgodnie z wytycznymi EROD 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo – administratorzy muszą wdrożyć środki techniczne i organizacyjne, aby zapewnić stosowanie wszelkich zasad dotyczących ochrony danych w czasie ich przetwarzania i ustanowić środki dla osób, których dane dotyczą, umożliwiające wykonywanie ich praw, o których mowa w art. 15-22 RODO.

315 Wyrok Trybunału Konstytucyjnego z dnia 26 kwietnia 2018 r. sygn. akt K 6/15 (Dz. U. poz. 830).
316 Kwestia ta jest obecnie przedmiotem dodatkowej analizy UODO.
317 DOL.023.489.2022.
318 Wyrok TSUE z dnia z dnia 11 grudnia 2014 r. w sprawie C-212/13 František Ryneš przeciwko Úřad pro ochranu osobních údajů.

Publikowanie w mediach społecznościowych nagrań z monitoringu dotyczących aktów wandalizmu „ku przestrodze"

Jeden z administratorów zapytał UODO, czy mógłby publikować w mediach społecznościowych nagrania dotyczące aktów wandalizmu, by odstraszyć potencjalnych innych naruszających przepisy[319]. W odpowiedzi UODO wskazał, że każdy administrator, który przetwarza wizerunki osób za pomocą monitoringu wizyjnego, ma obowiązek zapewnić zgodność z zasadami, o których mowa w art. 5 ust. 1 RODO, w tym przetwarzać dane osobowe zgodnie z prawem, czyli na podstawie jednej z przesłanek, o których mowa odpowiednio w art. 6 ust. 1, art. 9 ust. 2 i art. 10 RODO, oraz zagwarantować ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem za pomocą odpowiednich środków technicznych lub organizacyjnych. Powyższe zasady mają również zastosowanie w przypadku udostępniania danych osobowych, w tym wizerunków osób, w mediach społecznościowych w Internecie. Deklarowany cel takiego upublicznienia danych, dotyczący „odstraszenia" innych osób mogących potencjalnie naruszać przepisy, nie wydaje się uzasadniony w świetle którejkolwiek ze wspomnianych wyżej przesłanek.

Wykorzystywanie przez zakłady karne monitoringu w celu kontrolowania pracowników i funkcjonariuszy służby więziennej

Z kolei Rzecznik Praw Obywatelskich zwrócił się do Prezesa UODO o zajęcie stanowiska odnośnie wykorzystywania przez zakłady karne monitoringu, w tym monitoringu audiowizualnego, w celu kontrolowania pracowników i funkcjonariuszy służby więziennej[320]. W odpowiedzi organ właściwy w zakresie ochrony danych osobowych wskazał, że stosowanie monitoringu, w ramach którego przetwarzane są dane osobowe, od dawna jest przedmiotem szczególnego zainteresowania organu nadzorczego. Niewątpliwie zastosowanie tej technologii jest inwazyjną formą ingerencji w prywatność osób fizycznych i z tego względu powinno mieć miejsce wyłącznie po spełnieniu określonych warunków. Pod szczególną rozwagę należy poddać technologię monitoringu audiowizualnego. Jej zastosowanie powinno być poprzedzone analizą ryzyka, tak aby wyeliminować zagrożenia związane m.in. z nadmiarowym i nieproporcjonalnym do realizowanego celu przetwarzaniem danych. Powyższe zyskuje na znaczeniu w przypadku zastosowania monitoringu w środowisku zatrudnienia. Szczególne bowiem wymogi i gwarancje prawne dla przetwarzania danych pracowników kreuje zarówno art. 88 RODO, jak i przepisy prawa pracy.

W kontekście zatrudnienia w zakładach karnych zastosowanie mają przede wszystkim przepisy ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej[321]. Powyższa ustawa nie reguluje jednak kwestii związanych z wykorzystywaniem w zakładach karnych monitoringu wobec osób zatrudnionych. Zastosowania w tym przypadku nie będą miały także przepisy

319 DOL.023.393.2022.
320 DOL.023.418.2022.
321 Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej (t.j. Dz. U. z 2022 r. poz. 2470 z późn. zm.).

.

Kodeksu pracy. W wyroku NSA z 28 października 2008 r.[322] sąd wskazał bowiem, iż funkcjonariusz więzienny nie jest pracownikiem w rozumieniu kodeksu pracy. Nie ma do niego zatem zastosowania zasada subsydiarnego stosowania przepisów kodeksu pracy zawarta w art. 5 tego aktu. Podobne stanowisko zajął Sąd Najwyższy w wyroku z 16 grudnia 2009 r.[323] wskazując, iż stosunek służbowy funkcjonariusza służby celnej jest stosunkiem administracyjnoprawnym.

Organ nadzorczy wskazał zatem, że powyższe okoliczności powinny być wzięte pod rozwagę przy dokonywaniu ostatecznej oceny zgodności przepisów o służbie więziennej ze standardami konstytucyjnymi w zakresie ochrony prywatności funkcjonariuszy służby więziennej. W przypadku bowiem monitoringu wizyjnego w zakładach pracy wobec pracowników niebędących funkcjonariuszami więziennymi zastosowanie znajdą ogólne zasady określone w Kodeksie pracy i gwarancje wynikające z przepisów prawa pracy. Art. 73a § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy[324] stanowi jedynie o monitoringu skazanego i zgodnie z jego treścią: monitorowanie, zapewniające możliwość obserwowania zachowania skazanego, można stosować w szczególności w celach mieszkalnych wraz z częścią przeznaczoną do celów sanitarno-higienicznych, w łaźniach, w pomieszczeniach wyznaczonych do widzeń, w miejscach zatrudnienia osadzonych, w ciągach komunikacyjnych, na placach spacerowych, a także do obserwacji terenu zakładu karnego na zewnątrz budynków, w tym linii ogrodzenia zewnętrznego. Potwierdzają to także inne przepisy (np. art. 73a § 1 k.k.w.). Treść przepisu art. 73a § 15 k.k.w. nie pozostawia wątpliwości co do tego, że istota monitoringu może polegać na używaniu urządzeń rejestrujących obraz lub dźwięk. Oznacza to, że na mocy powyższego przepisu dozwolone jest utrwalanie zarówno obrazu, jak i dźwięku albo tylko obrazu, albo dźwięku. Zakres przedmiotowy tego przepisu uzasadnia stosowanie monitoringu w zakładach karnych, ale wobec skazanych.

Wykorzystywanie monitoringu wobec pracowników zakładów karnych może odbywać się natomiast wyłącznie na podstawie przepisów Kodeksu pracy. Brak jest jednocześnie szczególnych regulacji prawnych, które pozwalałyby na objęcie monitoringiem funkcjonariuszy Służby Więziennej. Wobec braku przepisów szczególnych każdy administrator, w myśl zasady rozliczalności, jest zobowiązany do wykazania podstaw prawnych dla pozyskiwania danych osobowych za pomocą tej technologii, w tym danych z art. 9 ust. 1 i art. 10 RODO oraz jest obowiązany wykazać spełnienie wszystkich zasad określonych w art. 5 ust. 1 RODO. Przed wdrożeniem technologii audio monitoringu konieczne będzie także przeprowadzenie testu prywatności i dokonanie oceny skutków dla ochrony danych.

Podsumowując, celem stosowania na terenie jednostek penitencjarnych środków technicznych umożliwiających rejestrację obrazu lub dźwięku powinno być zapewnienie wyłącznie bezpieczeństwa osobistego osób osadzonych, a także zapewnienie humanitarnego wykonywania kary pozbawienia wolności.

322 Wyrok NSA z dnia 28 października.2008 r., I OSK 1721/07, LEX nr 499777.
323 Wyrok SN z dnia 16. grudnia 2009 r., II PK 152/09, OSNP 2011, nr 13-14, poz. 172.
324 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (t.j. Dz. U. z 2023 r. poz. 127), dalej: „k.k.w.”.

Udostępnianie sołtysowi listy osób uprawnionych do głosowania podczas zebrań sołeckich

Jedna z rozpatrywanych przez organ nadzorczy spraw dotyczyła legalności udostępnienia sołtysowi przez urząd gminy listy osób uprawnionych do głosowania podczas zebrań sołeckich[325]. W przesłanych pytającemu wyjaśnieniach podkreślono, że kwestia udostępnienia dokumentów, które mogą zawierać informacje o konkretnych osobach, powinna być rozpatrywana w każdym przypadku indywidualnie oraz poprzedzona dokonaniem oceny ryzyka dla ochrony danych osobowych i zapewnieniem odpowiedniego zabezpieczenia tych danych, m.in. poprzez anonimizację. Sołtys jest organem wykonawczym sołectwa, które z kolei jest jednostką pomocniczą gminy tworzoną przez radę gminy w drodze uchwały. Zgodnie z art. 35 ustawy o samorządzie gminnym, rada gminy w odrębnym statucie określa organizację i zakres działania jednostki pomocniczej. To, co bezwzględnie musi być uregulowane w statucie sołectwa, wynika z przepisów art. 35 ust. 3 ustawy o samorządzie gminnym (nazwa i obszar jednostki pomocniczej, zasady i tryb wyborów organów jednostki pomocniczej, organizację i zadania jednostki pomocniczej, zakres zadań przekazywanych jednostce przez gminę oraz sposób ich realizacji, zakres i formy kontroli oraz nadzoru organów gminy nad działalnością organów jednostki pomocniczej). Dokument ten – będący aktem prawa miejscowego – poprzez wskazanie sposobu realizacji zadań jednostki pomocniczej, w tym również określenie regulacji dotyczących organizacji zebrań wiejskich, w szczególności konkretyzacji, kto może w nich uczestniczyć z prawem głosu i jak prawo to weryfikować – może okazać się zatem pomocny w omawianej sprawie. Ważne jest, że – o ile statut gminy nie przewiduje inaczej – to gmina, za pośrednictwem uprawnionych osób i organów, powinna weryfikować prawo mieszkańców do oddania głosu na zebraniu sołeckim, nie zaś sam sołtys.

Udostępnianie danych osobowych na żądanie sądu

Do UODO wpływały także pytania dotyczące legalności udostępniania dokumentów zawierających dane osobowe na żądanie sądu[326]. Organ nadzorczy konsekwentnie wskazywał, że w procedurze karnej zgodnie z art. 15 § 2 k.p.k. wszystkie instytucje państwowe i samorządowe są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne w terminie wyznaczonym przez te organy. Tak samo – na mocy art. 15 § 3 – obowiązkowi temu podlegają osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej oraz osoby fizyczne, jeżeli bez tej pomocy przeprowadzenie czynności procesowej jest niemożliwe albo znacznie utrudnione. W postępowaniu cywilnym natomiast udostępnienie danych na żądanie sądu jest konieczne w świetle art. 248 § 1 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[327], zgodnie z którym każdy obowiązany jest przedstawić na zarządzenie sądu

325 DOL.023.129.2022.
326 Np.: DOL.023.162.2022, DOL.023.637.2022.
327 Ustawa z dnia 17 listopada 1964 r. cywilnego (t.j. Dz. U. z 2021 r. poz. 1805 z późn. zm.), dalej: „k.p.c.”.

w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera informacje niejawne. Biorąc powyższe pod uwagę w każdym z tych przypadków udostępnienie danych osobowych jest realizacją obowiązku prawnego ciążącego na administratorze. Podstawę prawną udostępnienia stanowi tu zatem art. 6 ust. 1 lit. c) RODO.

Przetwarzanie danych osobowych dziecka (ucznia szkoły) i jego rodziców przez publiczną poradnię psychologiczno-pedagogiczną.

W 2022 r. UODO odniósł się także do podstaw prawnych przetwarzania danych osobowych dziecka (ucznia szkoły) i jego rodziców przez publiczną poradnię psychologiczno-pedagogiczną w ramach świadczonych przez nią usług wynikających z przepisów prawa[328]. Jak wskazał, poradnie psychologiczno-pedagogiczne, zgodnie z art. 2 pkt 6 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe[329], są częścią systemu oświaty i realizują zadania określone w przepisach prawa, w tym m.in. w rozporządzeniu Ministra Edukacji Narodowej z dnia 1 lutego 2013 r. w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych[330]. Z treści motywu 45 RODO wynika, że jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii Europejskiej lub prawo państwa członkowskiego. Zatem w przypadku realizacji przez poradnie psychologiczno-pedagogiczne zadań ustawowych podstawę prawną przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. c) i/lub e) RODO, a w przypadku szczególnych kategorii danych osobowych – art. 9 ust. 2 lit. g) RODO w powiązaniu z odpowiednimi przepisami prawa, z których wynika to zadanie.

Organ nadzorczy podkreślił także, że jeżeli przetwarzanie danych osobowych ma swoje uzasadnienie w obowiązujących przepisach prawa, odbieranie zgody na takie przetwarzanie danych osobowych nie jest prawidłowe, nawet w przypadku gdy zgodnie z art. 13 ww. rozporządzenia Ministra Edukacji Narodowej korzystanie z pomocy udzielanej przez poradnie psychologiczno-pedagogiczne jest dobrowolne i nieodpłatne. Na podstawie § 6 ust. 8 pkt 1 rozporządzenia Ministra Edukacji Narodowej z dnia 9 sierpnia 2017 r. w sprawie warunków organizowania kształcenia, wychowania i opieki dla dzieci i młodzieży niepełnosprawnych, niedostosowanych społecznie i zagrożonych niedostosowaniem społecznym[331] do kompetencji dyrektora szkoły należy wnioskowanie o udział w posiedzeniach zespołu opracowującego program edukacyjno-terapeutyczny m.in. przedstawiciela poradni psychologiczno-pedagogicznej. Zgodnie z § 6 ust. 9 tego rozporządzenia zespół,

328 DOL.023.423.2022.
329 Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe (t.j. Dz. U. z 2023 r. poz. 900).
330 Rozporządzenie Ministra Edukacji Narodowej z dnia 1 lutego 2013 r. w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych (Dz. U. poz. 199 z późn. zm.).
331 Rozporządzenie Ministra Edukacji Narodowej z dnia 9 sierpnia 2017 r. w sprawie warunków organizowania kształcenia, wychowania i opieki dla dzieci i młodzieży niepełnosprawnych, niedostosowanych społecznie i zagrożonych niedostosowaniem społecznym (t.j. Dz. U. z 2020 r. poz. 1309).

co najmniej dwa razy w roku szkolnym, dokonuje okresowej wielospecjalistycznej oceny poziomu funkcjonowania ucznia, uwzględniając ocenę efektywności programu oraz, w miarę potrzeb, dokonuje modyfikacji programu. Okresowej wielospecjalistycznej oceny poziomu funkcjonowania ucznia i modyfikacji programu dokonuje się, w zależności od potrzeb, we współpracy z poradnią psychologiczno-pedagogiczną, w tym poradnią specjalistyczną, a także – za zgodą rodziców ucznia – z innymi podmiotami. Zatem nie ma potrzeby uzyskiwania zgody rodziców na udostępnienie danych osobowych ucznia dla pracownika poradni psychologiczno-pedagogicznej biorącego udziału w pracach tego zespołu, gdyż podstawą tego udostępnienia są ww. przepisy prawa.

Współpraca placówki wsparcia dziennego z placówkami oświatowymi

Do UODO wpłynęło też pytanie dotyczące współpracy pomiędzy placówką wsparcia dziennego a placówkami oświatowymi[332], które było podstawą do przygotowania materiału do Newslettera UODO dla IOD[333]. Urząd Ochrony Danych Osobowych wyjaśnił, że wymiana między szkołą a placówką wsparcia dziennego takich informacji o dziecku, jak m.in. wyniki w nauce, frekwencja, potrzeby rozwojowe i edukacyjne, zachowanie oraz funkcjonowanie społeczne, jest możliwa bez zgody jego rodziców lub opiekunów. Podstawą uprawniającą do takiego działania są przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej.

Placówki wsparcia dziennego to jedne z podmiotów, które wspierają rodziny przeżywające trudności w wypełnianiu funkcji opiekuńczo wychowawczych. Są one prowadzone na podstawie ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej[334] przez gminę lub powiat, podmiot, któremu gmina lub powiat zleciły realizację tego zadania na podstawie art. 190, albo przez podmiot, który uzyskał zezwolenie wójta bądź starosty. Placówki wsparcia dziennego, realizując zadania wynikające z powołanej ustawy, mają – zgodnie z art. 23 ust. 1 – współpracować z rodzicami lub opiekunami dziecka, a także z placówkami oświatowymi i podmiotami leczniczymi. W związku z tym konieczne bywa wzajemne przekazywanie informacji dotyczących m.in. wyników w nauce, zachowania czy potrzeb rozwojowych i edukacyjnych oraz funkcjonowania społecznego dziecka.

Ponadto przepisy powołanej ustawy stanowią (art. 8 ust. 3), że wspieranie rodziny jest prowadzone za jej zgodą i aktywnym udziałem. U podstaw owej współpracy leży wartość, jaką jest dobro dziecka w rozumieniu art. 72 Konstytucji RP, zaś współdziałanie określonych podmiotów podejmowane w jej ramach ma służyć poprawie realizacji funkcji opiekuńczo-wychowawczej przez rodzinę lub opiekunów dziecka, a w konsekwencji poprawie sytuacji samego dziecka. Zdaniem UODO odczytując przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej przez pryzmat standardów wykładni funkcjonalnej i systemowej, uznać należy, że zgoda rodziców lub opiekunów dziecka na określone działania podejmowane przez

332 DOL.023.394.2022.
333 Tekst „Wymiana informacji między szkołą a placówką wsparcia dziennego" opublikowany w Newsletterze UODO dla IOD 6/2022.
334 Ustawa z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej (t.j. Dz. U. z 2022 r. poz. 447 z późn. zm.).

.

określone podmioty jest wymagana jedynie w szczególnych (nadzwyczajnych) sytuacjach, w których dochodzi do istotnej ingerencji w sferę władzy rodzicielskiej w rozumieniu ustawy z dnia 25 lutego 1964 r. – Kodeks rodzinny i opiekuńczy[335]. Wydaje się, że w kontekście omawianej ustawy brak konieczności pozyskiwania zgody rodziców lub opiekunów prawnych na działania nieingerujące w sferę władzy rodzicielskiej jest uzasadniony zwłaszcza wówczas, gdy rodzina przyjmuje pozycję bierną w procesie współpracy z placówką wsparcia dziennego. Natomiast podstawę prawną wymiany informacji dotyczących m.in. wyników w nauce, frekwencji, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, zachowania w szkole lub placówce wsparcia dziennego oraz funkcjonowania społecznego dziecka, dokonywanej między placówką wsparcia dziennego a placówką oświatową, stanowi art. 18 ustawy o wspieraniu rodziny i systemie pieczy zastępczej w zw. z art. 23 ust. 1 tej ustawy. Przepisy te i wynikające z nich obowiązki powinny być interpretowane ze szczególnym uwzględnieniem zasad ogólnych zawartych w art. 5 RODO oraz w świetle art. 7 ust. 1-4 ustawy o wspieraniu rodziny i systemie pieczy zastępczej dotyczącego przetwarzania danych osobowych. Przy ocenie omawianego zagadnienia należy brać pod uwagę również konkretne okoliczności faktyczne danego przypadku oraz szczegółowe postanowienia zawarte m.in. w regulaminie organizacyjnym i korzystania z usług danej placówki wsparcia dziennego oraz we wniosku o przyjęcie dziecka do placówki wsparcia dziennego.

Przetwarzanie danych osobowych przedsiębiorców wpisanych do Centralnej Ewidencji i Informacji o Działalności Gospodarczej przez osoby trzecie

Organ nadzorczy zajmował się również sprawą podstaw prawnych przetwarzania danych przedsiębiorców wpisanych do CEIDG[336]. W przesłanych pytającemu wyjaśnieniach wskazano, że biorąc pod uwagę przesłanki legalizujące przetwarzanie danych osobowych, wymienione w art. 6 ust. 1 RODO, przetwarzanie przez inne podmioty danych osobowych dostępnych publicznie, a zawartych w CEIDG, znajduje oparcie w art. 6 ust. 1 lit. f) RODO, stanowiącym o dopuszczalności przetwarzania, gdy jest ono niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

Korzystając z ww. przesłanki, należy ocenić, czy po stronie administratora lub strony trzeciej występuje prawnie uzasadniony interes – może to być interes faktyczny, gospodarczy lub prawny, ale taki, który jest zgodny z prawem. Przetwarzanie musi być również m.in. niezbędne dla realizacji celu wynikającego z tak rozumianego interesu administratora. Przetwarzanie takie należy ściśle powiązać z celem, w ramach realizacji którego jedynie

335 Ustawa z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (t.j. Dz. U. z 2020 r. poz. 1359 z późn. zm.).
336 DOL.023.618.2022.

niezbędne dane będą podlegały np. udostępnieniu. Tak więc każdy administrator pozyskujący dane z tej ewidencji będzie musiał wykazać podstawę prawną dla realizacji konkretnych zakładanych przez siebie celów, zgodnie ze wszystkimi zasadami ochrony danych osobowych.

Mając na uwadze kwestię ewentualnej zgody osoby, której dane dotyczą, należy zaznaczyć, że zgoda może być podstawą przetwarzania danych tylko wtedy, gdy nie występują inne przesłanki legalizujące określone w art. 6 ust. 1 RODO. Co ważne są one równoprawne i niezależne, co oznacza, że spełnienie jednej z nich jest wystarczające, aby uznać, że dane osobowe są przetwarzane zgodnie z prawem. Zatem zgoda osoby, której dane dotyczą, w omawianej sprawie byłaby bezprzedmiotowa. Przepisy prawa w sposób jasny i klarowny kształtują zasady prowadzenia Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punktu Informacji dla Przedsiębiorcy (ustawy o CEIDG i PIP), a także tryb dostępu do informacji, w tym danych osobowych się w niej znajdujących. Z przepisów tych nie wynika, aby podstawą prawną dla udostępnienia danych osobowych z CEIDG dla osób trzecich czy też innych przedsiębiorców dla realizacji ich celów przetwarzania (w tym komercyjnych) była zgoda osoby, której dane dotyczą. Zasadą wynikającą z powyższych przepisów jest jawność informacji zawartych w tym rejestrze publicznym i zapewnienie poprzez stronę internetową każdemu prawa dostępu do jego zasobów (art. 45) z wyjątkiem numeru PESEL, daty urodzenia oraz danych kontaktowych w przypadku gdy, podając je, osoba uprawniona sprzeciwiła się ich udostępnianiu w CEIDG (art. 43). Także TSUE w wyroku z 9 marca 2017 r. w sprawie C-398/15[337] wskazał, że celem jawności rejestrów spółek jest zagwarantowanie pewności prawa w stosunkach między spółkami a osobami trzecimi. Ocena aspektu jawności danych osobowych przetwarzanych w rejestrach publicznych była także przedmiotem licznych rozstrzygnięć sądów krajowych[338].

Wskazano ponadto, że dane osób fizycznych prowadzących samodzielną działalność gospodarczą (czyli indywidualnych przedsiębiorców wpisanych do CEIDG) podlegają ochronie na gruncie unormowań RODO. Komisja Europejska stwierdziła bowiem, że jeżeli w polskim porządku prawnym osoby fizyczne prowadzące indywidualną działalność gospodarczą nie są osobami prawnymi, lecz fizycznymi, czyli nie mają charakteru spółek, to znaczy, że w pełni podlegają przepisom RODO. Z motywu 14 RODO wynika także, że ochrona zapewniana RODO powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. RODO nie dotyczy zaś przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi (czyli tych wpisanych do KRS, np. spółek prawa handlowego), w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. Powyższe dotyczy także reprezentantów osób prawnych. Oznacza to, że od 25 maja 2018 r. – czyli od dnia rozpoczęcia stosowania RODO w polskim porządku prawnym podmioty, które wykorzystują dane osobowe osób

337 Wyrok TSUE z dnia 9 marca 2017 r. w sprawie C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, ZOTSiS 2017, nr 3, poz. I-197.
338 Por. np. Wyrok NSA z dnia 3 grudnia 2015 3, I OSK 1166/14, LEX nr 2094277.

fizycznych prowadzących działalność gospodarczą na podstawie wpisu do CEIDG, stały się administratorami tych danych osobowych. Pociąga to za sobą konieczność realizacji wszystkich obowiązków narzuconych na administratorów przez RODO – przede wszystkim obowiązków informacyjnych, o których mowa w art. 13 czy art. 14 RODO.

Odrębny administrator, pozyskując dane osobowe, nie będzie mógł ich przetwarzać z pominięciem zasady przejrzystości i z wyłączeniem praw – w tym prawa do informacji – osób, których dane z tej ewidencji są pozyskiwane. Przedsiębiorca prowadzący działalność gospodarczą polegającą na pozyskiwaniu informacji, w tym danych osobowych osób prowadzących działalność gospodarczą, z ogólnodostępnych rejestrów publicznych (np. CEIDG) oraz analizowaniu, interpretowaniu, a następnie udostępnianiu tych informacji zainteresowanym klientom, musi spełnić obowiązek informacyjny wobec tych osób określony w art. 14 RODO poprzez bezpośrednie przekazanie informacji osobie, której dane dotyczą, oraz realizować wiele innych praw na rzecz podmiotów danych (np. określone w Sekcji III RODO prawo do usunięcia danych, sprostowania danych, itd.). Wobec tego, jeżeli nie zaistnieją okoliczności uzasadniające skorzystanie z wyłączeń, o których mowa w art. 14 ust. 5 RODO lub art. 4 ustawy z dnia z dnia 10 maja 2018 r. o ochronie danych osobowych, administrator pozyskujący dane osobowe nie od osoby, której one dotyczą, musi taki obowiązek wypełnić.

Podsumowując, w roku 2022 zakres tematyczny pytań prawnych kierowanych do Urzędu był bardzo szeroki i dotyczył różnych aspektów przetwarzania danych osobowych. Wątpliwości dotyczyły nie tylko stosowania RODO, ale także innych, szczególnych przepisów prawa.

Podobnie jak w ubiegłych latach pojawiły się pytania dotyczące dostępu do informacji publicznej[339]. W swoich odpowiedziach organ nadzorczy konsekwentnie podkreślał, że granice prawa do informacji publicznej wyznacza art. 5 u.d.i.p. Zgodnie z art. 5 ust. 2 u.d.i.p., prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Ocena spełnienia przesłanki ograniczenia dostępu do informacji publicznej ze względu na prywatność osoby fizycznej należy natomiast do autonomicznej sfery decyzyjnej organu rozpatrującego wniosek o udostępnienie takiej informacji.

Wiele pytań dotyczyło kwestii dopuszczalności kopiowania dowodów osobistych przez instytucje finansowe, co skłoniło organ nadzorczy do odświeżenia komunikatu na ten temat na stronie internetowej UODO[340]. Pojawiły się także pytania o dowody osobiste z odciskiem palców. Organ właściwy w zakresie ochrony danych osobowych podkreślał, że

339 Np.: DOL.023.516.2022, DOL.023.572.2022.
340 Materiał: *Czy instytucje finansowe mogą kopiować dowody osobiste?* umieszczony na stronie internetowej UODO pod linkiem: https://www.uodo.gov.pl/pl/138/2476

jest to konsekwencją wprowadzenia nowej procedury wydawania dokumentów tożsamości wprowadzonej ustawą z dnia 14 kwietnia 2021 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw[341]. Wprowadzenie dowodów osobistych wydawanych na nowych zasadach jest natomiast wynikiem implementacji przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1157 z 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się[342].

Jak co roku wpływały też pytania dotyczące praw, które przysługują osobom na gruncie przepisów o ochronie danych osobowych, w tym dzieci. W odpowiedziach wskazywano w szczególności na art. 15 oraz art. 77 RODO.

Podmioty publiczne pytały o możliwość weryfikacji tzw. deklaracji śmieciowych[343] po wejściu w życie art. 6o ust. 1a ustawy o utrzymaniu i czystości w gminach[344]. W odpowiedziach organ nadzorczy wskazywał, że zgodnie z art. 6o ust. 1a ustawy o utrzymaniu i czystości w gminach wójt, burmistrz lub prezydent miasta w celu weryfikacji złożonych deklaracji może wykorzystać informacje i dane znajdujące się w jego posiadaniu oraz posiadaniu gminnych jednostek organizacyjnych, w tym przedsiębiorstw wodociągowo-kanalizacyjnych. Skoro powyższy przepis może stanowić dla wójta, burmistrza lub prezydenta podstawę do pozyskiwania danych z gminnych jednostek organizacyjnych w celu weryfikacji złożonych deklaracji, to za prawidłowe należy przyjąć takie postępowanie, zgodnie z którym dane osobowe zawarte w tych deklaracjach w celu sprawdzenia ich prawdziwości i rzetelności nie będą pozyskiwane w sposób automatyczny z baz, do których dostęp został przyznany mocą przepisu art. 6o ust. 1a tej ustawy. W ocenie organu nadzorczego przy weryfikacji deklaracji administrator powinien bowiem respektować także zasadę celowości, z której wynika, że przetwarzane dane mają być stosowne i ograniczone to tego, co niezbędne dla realizacji celu (art. 5 ust. 1 lit. c RODO). Zasadne jest zatem przyjęcie, że weryfikacja danych osobowych zawartych w deklaracji powinna dotyczyć tylko sytuacji, w których zachodzą uzasadnione wątpliwości co do prawdziwości ich treści. Brak jest natomiast podstaw prawnych do przyjęcia takiej weryfikacji względem wszystkich osób, które złożyły przedmiotowe deklaracje.

341 Ustawa z dnia 14 kwietnia 2021 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw (Dz. U. poz. 1000 z późn. zm.).

342 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1157 z dnia 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii i dokumentów pobytowych wydawanych obywatelom Unii i członkom ich rodzin korzystającym z prawa do swobodnego przemieszczania się (Dz. U. UE. L. z 2019 r. Nr 188, str. 67).

343 Np.: DOL.023.405.2022, DOL.023.734.2022.

344 Artykuł ten wprowadzono przepisami ustawy z dnia 11 sierpnia 2021 r. o zmianie ustawy o utrzymaniu czystości i porządku w gminach, ustawy – Prawo ochrony środowiska oraz ustawy o odpadach, Dz. U. 2022 r. poz. 1648.

14.1.2. Pytania prawne od inspektorów ochrony danych

Rola inspektorów ochrony danych ma fundamentalne znaczenie dla budowy systemu skutecznej ochrony danych osobowych. Przejawia się ona m.in. w pełnieniu obowiązków punktu kontaktowego oraz pośrednika pomiędzy administratorem i organem nadzorczym. IOD z jednej strony udziela bowiem fachowego wsparcia administratorowi co do sposobu wykonania ciążących na nim obowiązków nałożonych przepisami RODO, z drugiej strony – wspomaga go przed organem nadzorczym w wykazaniu zasadności wybranych rozwiązań, np. udzielając określonych informacji na żądanie organu nadzorczego. Jednocześnie IOD ma prawo zwrócić się do organu nadzorczego o udzielenie mu konsultacji nie tylko w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, ale również we wszelkich innych sprawach, co ma istotne znaczenie dla doskonalenia systemu ochrony danych osobowych.

Z tego względu UODO od wielu lat przykłada dużą wagę do współpracy z inspektorami ochrony danych, m.in. udzielając im konsultacji i porad.

W 2022 roku do UODO wpłynęły **274 pytania od inspektorów ochrony danych** (IOD). Udzielono zaś **294 odpowiedzi** na pytania od IOD, w tym część na pytania, które wpłynęły jeszcze 2021 r.

Nieznaczny spadek liczby pytań, podobnie jak w roku 2021, mógł być spowodowany tym, że wiele kwestii związanych z właściwym stosowaniem przepisów dotyczących ochrony danych osobowych zostało wyjaśnionych m.in. w materiałach zamieszczonych na stronie internetowej UODO – w specjalnej zakładce adresowanej inspektorom, która była przygotowywana na podstawie wpływających do UODO pytań od inspektorów ochrony danych. Stanowiska zamieszczane w tej zakładce wskazywały nie tylko, jak postąpić w podobnej sprawie, ale również wyznaczały kierunek i zasady interpretacji przepisów pomocne przy rozstrzyganiu nowych wątpliwości z zakresu ochrony danych osobowych.

Podobnie jak w latach ubiegłych pytania przesyłane przez inspektorów były dla organu nadzorczego ważnym źródłem informacji na temat aktualnych problemów w stosowaniu przez administratora, podmiot przetwarzający i wspierających ich inspektorów ochrony danych prawa ochrony danych osobowych. Informacje o aktualnych problemach w stosowaniu przepisów RODO pozwalały podejmować organowi również działania zmierzające do podnoszenia poziomu ochrony danych osobowych, w tym w zakresie legislacji czy edukacji.

W 2022 roku wśród najczęściej poruszanych lub szczególnie interesujących zagadnień, na które zwrócili uwagę inspektorzy w przesłanych do Urzędu pytaniach, a które stały się przedmiotem analiz organu, były takie kwestie, jak:

1) określenie statusu podmiotów w procesie przetwarzania danych osobowych,
2) udostępnianie danych osobowych,

3) zasady ochrony danych osobowych,
4) obowiązki administratora określone w RODO w zakresie realizowania przez administratora praw osób, których dane dotyczą,
5) wyznaczanie IOD, status i zadania inspektora ochrony danych.

Określenie statusu podmiotów w procesie przetwarzania danych osobowych

W 2022 roku – podobnie jak w latach poprzednich – wiele wątpliwości przysparzało inspektorom ochrony danych właściwe określenie statusu podmiotów biorących udział w procesie przetwarzania danych osobowych. Pytania o to, jak ustalić, czy mamy do czynienia z administratorem, współadministratorem czy podmiotem przetwarzającym pochodziły zarówno od IOD z sektora publicznego, jak i z sektora prywatnego. Tymczasem właściwe określenie roli podmiotu w procesie przetwarzania danych osobowych jest kluczowe dla wskazania, kto ponosi odpowiedzialność za przestrzeganie przepisów o ochronie danych oraz do kogo osoby, których dane dotyczą, mogą zwracać się z żądaniem realizacji swoich praw.

Odpowiadając na zgłaszane wątpliwości, UODO wskazywał kryteria pomocne w ocenie statusu podmiotów biorących udział w przetwarzaniu danych oraz powoływał się na wskazówki zawarte m.in. w wytycznych 7/2020 Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego. Za szczególnie przydatny uznał schemat zamieszczony w załączniku nr 1 zawierający pytania ułatwiające dokonywanie tej oceny.

Jednocześnie UODO podkreślał, że dla dokonania właściwej oceny, jaką rolę pełni dany podmiot uczestniczący w przetwarzaniu danych, niezbędne jest rzetelne przeanalizowanie przez niego nie tylko stanu faktycznego, ale również przepisów, które mają zastosowanie do jego działalności.

Przykładowo, w pytaniu **„Czy należy podpisać umowę powierzenia z firmą sprzątającą?”**[345] UODO zwrócił uwagę, iż ocena statusu firmy sprzątającej będzie zależała przede wszystkim od tego, jaki jest zakres jej usług, tj. czy obejmują one – obok usług porządkowych – również np. niszczenie dokumentów lub inne działania, które nie mogą być realizowane bez dostępu do dokumentów lub innych nośników danych osobowych.

Konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator w celu realizacji swoich celów (zadań) związanych z przetwarzaniem danych osobowych posługuje się innym, zewnętrznym podmiotem. Jak wynika z art. 28 ust. 1 RODO, z powierzeniem przetwarzania danych osobowych mamy do czynienia, gdy przetwarzanie danych osobowych jest dokonywane przez zewnętrzny podmiot w imieniu administratora, w celach określonych przez administratora i zgodnie z jego poleceniami i instrukcjami. Natomiast usługi sprzątania powierzchni danego obiektu (np.

345 https://archiwum.uodo.gov.pl/pl/225/2245

uczelni, biura) trudno zaliczyć do usług związanych z przetwarzaniem danych osobowych. Należy zatem przyjąć, że co do zasady usługi takie nie wymagają powierzenia przetwarzania danych osobowych. Niemniej w przypadku korzystania przez administratora z takich usług (jak i innych usług wymagających dostępu do pomieszczeń administratora, w których przetwarzane są dane osobowe) – konieczne może się okazać zastosowanie odpowiednich środków technicznych i organizacyjnych, których celem będzie zapewnienie odpowiedniej ochrony danych osobowych, w tym przed nieuprawnionym ujawnieniem danych osobowych.

Administrator powinien bowiem analizować ryzyko związane z przetwarzaniem danych i podejmować środki, które będą je minimalizować. Działania te powinny dotyczyć zarówno pracowników administratora, jak i podmiotu zewnętrznego. Powinny one polegać m.in. na wprowadzeniu odpowiednich procedur i zadbanie o ich skuteczne wdrożenie i realizowanie przez cały cykl przetwarzania danych (art. 24 RODO, art. 32 RODO). W procedurach tych warto też przewidzieć, iż mogą zdarzyć się sytuacje, w których pracownicy firmy sprzątającej znajdą określony dokument lub inny nośnik zawierający dane osobowe. Jednocześnie w umowie z firmą sprzątającą należy określić sposób postępowania w takiej sytuacji oraz obowiązki pracownika, który uzyskał przypadkowy dostęp do danych osobowych.

W Wytycznych Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO (pkt 79) wskazuje się, że przetwarzanie danych osobowych w imieniu administratora wymaga przede wszystkim, aby odrębny podmiot przetwarzał dane osobowe na rzecz administratora. Art. 4 pkt 2 RODO ujmuje „przetwarzanie" jako szeroki zakres operacji, począwszy od gromadzenia, przechowywania i przeglądania, a skończywszy na wykorzystaniu, rozpowszechnianiu lub udostępnianiu w inny sposób i niszczeniu. W rozdziale dotyczącym pojęcia „osoby trzeciej" podany jest następujący przykład związany z usługami sprzątania (pkt 89): „Przedsiębiorstwo A zawiera umowę z przedsiębiorstwem świadczącym usługi sprzątania, aby sprzątało ich biura. Osoby sprzątające nie powinny mieć dostępu do danych osobowych ani w inny sposób przetwarzać tych danych. Nawet jeśli mogą oni sporadycznie natknąć się na takie dane podczas poruszania się po biurze, mogą wykonywać swoje zadania bez dostępu do danych i mają umowny zakaz dostępu do danych osobowych lub przetwarzania w inny sposób danych osobowych, które Przedsiębiorstwo A przechowuje jako administrator. Osoby sprzątające nie są zatrudnione przez Przedsiębiorstwo A ani nie są postrzegane jako podlegające bezpośrednio temu przedsiębiorstwu. Przedsiębiorstwo nie ma zamiaru angażować podmiotu świadczącego usługi sprzątania ani jego pracowników w przetwarzanie danych osobowych w imieniu Przedsiębiorstwa A. Przedsiębiorstwo świadczące usługi sprzątania i jego pracownicy powinni być zatem postrzegani jako strona trzecia, a administrator musi upewnić się, że istnieją odpowiednie środki bezpieczeństwa uniemożliwiające im dostęp do danych i wprowadzić obowiązek zachowania poufności w przypadku przypadkowego ujawnienia danych osobowych".

Problemy w zakresie określenia statusu podmiotu w procesie przetwarzania danych osobowych zgłaszali również inspektorowie ochrony danych z sektora medycznego. Ich

wątpliwości dotyczyły nie tylko tego, czy i kiedy należy zawierać umowy powierzenia przetwarzania danych osobowych, ale czy przy ich zawieraniu powinny być spełnione dodatkowe warunki poza tymi wskazanymi w RODO. Wskazówki w tym zakresie organ nadzorczy zawarł w odpowiedzi na pytanie: „Na co zwrócić szczególną uwagę przy powierzeniu danych osobowych w sektorze medycznym?"346. Wyjaśnił, iż powierzenie przetwarzania danych osobowych powinno mieć miejsce wówczas, gdy zewnętrzny podmiot przetwarza dane w imieniu administratora, w celach określonych przez administratora i zgodnie z jego poleceniami i instrukcjami. W przypadku powierzenia przetwarzania danych to administrator musi legitymować się podstawą prawną do przetwarzania wynikającą z art. 6 lub art. 9 RODO oraz ponosi odpowiedzialność za zgodność tego przetwarzania z przepisami o ochronie danych osobowych, również w zakresie przetwarzania, które powierzył innemu podmiotowi. W motywie 79 RODO wskazano, że ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach RODO jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

To, czy w danej sytuacji należy skorzystać z powierzenia przetwarzania danych, wymaga przeprowadzenia analizy uwzględniającej przepisy prawa regulujące działalność podmiotów leczniczych oraz stan faktyczny, w którym funkcjonują podmioty, pomiędzy którymi dochodzić będzie do przepływu danych. Na tej podstawie należy ustalić, jakie dane osobowe są przetwarzane, jakie zadania/cele są realizowane, do którego z podmiotów one należą, a w związku z tym, który podmiot decyduje o celach przetwarzania, a także, czy któryś z nich działa na zlecenie administratora i realizuje jego cele, czy też wspólnie ustalają cele i sposoby przetwarzania.

Jednym z warunków kwalifikowania danej relacji jako relacji administrator – podmiot przetwarzający jest posiadanie przez podmiot przetwarzający statusu odrębnego (zewnętrznego) podmiotu od administratora. Między innymi dlatego pracownicy i inne osoby, które działają pod bezpośrednim zwierzchnictwem administratora (na przykład tymczasowo zatrudnieni pracownicy), nie są podmiotami przetwarzającymi, ponieważ przetwarzają dane, będąc częścią organizacji administratora. Zgodnie z art. 29 RODO są one również związane instrukcjami administratora.

Gdy działalność jest wykonywana przez lekarza w siedzibie podmiotu leczniczego, na warunkach techniczno-organizacyjnych określonych przez ten podmiot i w związku z przetwarzaniem danych osobowych klientów podmiotu leczniczego jako świadczeniodawcy, dochodzi do quasi-zatrudnienia. Ponieważ działalność ta może być wykonywana wyłącznie w zakładzie leczniczym na podstawie kontraktu umowy z podmiotem leczniczym, stanowi ona substytut zatrudnienia. Inny słowy w sytuacji lekarza zatrudnionego na kontrakcie, tj.

346 https://archiwum.uodo.gov.pl/pl/225/2378

na podstawie umowy cywilnej, mamy do czynienia z relacją podobną do tej, jaka występuje w przypadku pracodawcy i pracownika. Lekarz nie ma wówczas statusu podmiotu odrębnego od administratora i nie należy go traktować ani jako osobnego administratora, ani jako podmiotu przetwarzającego. Niemniej w praktyce podmiotów leczniczych mogą występować również inne modele współpracy. Dlatego ustalenie wzajemnych relacji pomiędzy podmiotami zawierającymi kontrakt powinno następować na podstawie analizy danego przypadku. Umowy cywilnoprawne, w zależności od uregulowań, mogą różnić się od siebie zarówno zakresem obowiązków, jak i stopniem zależności od podmiotu leczniczego.

W przypadku zawarcia przez podmiot udzielający świadczeń zdrowotnych umowy powierzenia przetwarzania danych osobowych, poza warunkami przewidzianymi w art. 28 ust. 3 RODO muszą być spełnione dodatkowe wymagania wskazane w ustawie o prawach pacjenta i Rzecznik Praw Pacjenta (art. 24 ust. 5-7):

- realizacja tej umowy nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej,
- podmiot, któremu powierzono przetwarzanie danych osobowych w związku z realizacją umowy o powierzeniu przetwarzania danych osobowych jest obowiązany do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją tej umowy. Podmiot ten jest związany tajemnicą także po śmierci pacjenta,
- w przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, o którym mowa w ust. 1, który powierzył przetwarzanie danych osobowych.

W uzasadnieniu do wprowadzenia powyższych przepisów do ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta wskazano: „w art. 24 ust. 4-6 wprowadzone zostały przepisy umożliwiające podmiotom udzielającym świadczeń zdrowotnych zawieranie umów z podmiotami zajmującymi się przechowywaniem i archiwizacją dokumentacji medycznej. W wielu przypadkach przechowywanie i archiwizowanie elektronicznej dokumentacji medycznej będzie wiązało się z dużymi nakładami inwestycyjnymi i technicznymi. W przypadku małych podmiotów wykonujących działalność leczniczą zlecenie ww. usług może być uzasadnione względami bezpieczeństwa i efektywności finansowej. Przechowywanie dokumentacji przez podmiot zewnętrzny nie będzie mogło wpływać na ograniczenie prawa pacjenta do dostępu do jego dokumentacji. Ponadto wprowadzono przepis regulujący postępowanie w przypadku zaprzestania, w tym także nagłego, działalności przez podmiot, który przetwarzał dane osobowe zawarte w dokumentacji medycznej, na podstawie umowy zawartej z podmiotem udzielającym świadczeń zdrowotnych”.

Udostępnianie danych osobowych

Wiele pytań inspektorów – kierowanych do UODO − dotyczyło kwestii udostępniania danych osobowych. Zgodnie z przepisami RODO, podmiot może przetwarzać (w tym udostępniać) dane osobowe wyłącznie wtedy, gdy istnieje podstawa prawna uprawniająca dany podmiot do przetwarzania (w tym pozyskiwania) danych. Co ważne, każdy wniosek o udostępnienie danych wymaga indywidualnej analizy. Rozpatrujący go administrator, który podejmuje ostateczną decyzję w tej sprawie, musi wziąć pod uwagę konkretne okoliczności faktyczne i prawne, w tym obowiązujące przepisy prawa, rodzaj danych osobowych, cel oraz uzasadnienie potrzeby posiadania danych przez podmiot, który występuje o ich udostępnienie. Administrator za każdym razem powinien zweryfikować, czy faktycznie ze wskazanego przepisu prawa wynika uprawnienie wnioskodawcy do ich pozyskania. Administrator ponosi bowiem odpowiedzialność za wykazanie właściwej staranności w zapewnieniu, aby dane nie były udostępniane nieuprawnionym odbiorcom.

Przykładowym pytaniem dotyczącym kwestii udostępniania danych osobowych (na które odpowiedź została opublikowana na stronie internetowej UODO), było pytanie **„W jakim zakresie należy ujawniać dane przedsiębiorców prowadzących ośrodki szkolenia kierowców?”**[347]. Przedstawione w pytaniu wątpliwości dotyczyły tego, czy w celu realizacji obowiązku określonego w art. 43 ust. 1 pkt 6 lit. a ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami[348] starosta może udostępnić informacje o firmie przedsiębiorcy zawierającej imię i nazwisko osoby prowadzącej jednoosobową działalność, np. „Krzysztof Kowalski Ośrodek Szkolenia Kierowców Krzysztof”.

W odpowiedzi na to pytanie organ nadzorczy zwrócił uwagę, iż dane osobowe osób fizycznych prowadzących jednoosobową działalność gospodarczą podlegają ochronie na mocy RODO, a podmioty, które chcą je przetwarzać, muszą spełnić wszystkie obowiązki wynikające z przepisów o ochronie danych osobowych, w tym legitymować się podstawą prawną do ich przetwarzania.

Administrator będący podmiotem publicznym, oceniając, czy przetwarzanie (w tym udostępnianie) danych jest w określonej sytuacji dopuszczalne, powinien w pierwszej kolejności kierować się przepisami prawa odnoszącymi się do jego działalności. Podmioty publiczne co do zasady przetwarzają dane na podstawie i w granicach określonych przez przepisy.

Zgodnie z art. 43 ust. 1 pkt 6 lit. a ustawy o kierujących pojazdami, starosta sprawuje nadzór w zakresie zgodności prowadzenia szkolenia osób ubiegających się o uzyskanie uprawnień do kierowania, w ramach którego w szczególności sporządza analizę, przetwarza oraz podaje do publicznej wiadomości wyniki analizy statystycznej, w zakresie średniej zdawalności osób szkolonych w danym ośrodku szkolenia kierowców oraz liczby uwzględnionych skarg złożonych na dany ośrodek. Przepis ten − zobowiązując starostę

347 https://archiwum.uodo.gov.pl/pl/225/2246

348 Ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami (t.j. Dz. U. z 2023 r. poz. 622 z późn. zm.), dalej: „ustawa o kierujących pojazdami”.

do podawania do publicznej wiadomości wyników analizy statystycznej − nie precyzuje, w jaki sposób powinien zostać oznaczony taki ośrodek. Art. 28 ust. 7 w związku z art. 28 ust. 4 ustawy o kierujących pojazdami stanowi, że w prowadzonym przez starostę rejestrze przedsiębiorców prowadzących ośrodek szkolenia kierowców (który jest jawny zgodnie z art. 43 ust. 4 ustawy Prawo przedsiębiorców) umieszcza się w szczególności firmę przedsiębiorcy oraz oznaczenie jego adresu i siedziby albo miejsca zamieszkania, a ponadto oznaczenie i adres ośrodka szkolenia kierowców. Aby zrealizować powyższy obowiązek starosta może zatem podać do wiadomości publicznej takie informacje dotyczące „danego" ośrodka, które go jednoznacznie identyfikują, łącznie z oznaczeniem i adresem ośrodka szkolenia kierowców nawet w przypadku, gdy oznaczenie to obejmuje firmę przedsiębiorcy[349], czyli w przypadku przedsiębiorcy będącego osobą fizyczną – jego imię i nazwisko.

Zatem podstawę do przetwarzania danych osobowych w tym celu stanowi ww. przepis ustawy o kierujących pojazdami, nie zaś zgoda osoby, której dane dotyczą.

Inne z pytań IOD dotyczące kwestii udostępniania danych osobowych, do którego organ odniósł się w materiale zamieszczonym na stronie internetowej, brzmiało: **„Czy przekazanie członkom wspólnoty mieszkaniowej treści uchwał z podpisami członków wspólnoty stanowi naruszenie przepisów o ochronie danych osobowych?"**[350].

W odpowiedzi UODO wskazał, że przepisy prawa nie określają szczegółowo elementów treści uchwały. Niemniej zgodnie z art. 23 ust. 2 ustawy z dnia 24 czerwca 1994 r. o własności lokali[351], uchwały zapadają większością głosów właścicieli lokali, liczoną według wielkości udziałów, chyba że w umowie lub w uchwale podjętej w tym trybie postanowiono, że w określonej sprawie na każdego właściciela przypada jeden głos. Na podstawie zaś art. 23 ust. 3 ustawy o własności lokali, o treści uchwały, która została podjęta z udziałem głosów zebranych indywidualnie, każdy właściciel lokalu powinien zostać powiadomiony na piśmie. Należy mieć na uwadze, iż zgodnie z art. 25 ust. 1 ustawy o własności lokali właściciel lokalu może zaskarżyć uchwałę do sądu z powodu jej niezgodności z przepisami prawa lub z umową właścicieli lokali albo jeśli narusza ona zasady prawidłowego zarządzania nieruchomością wspólną lub w inny sposób narusza jego interesy. Powództwo w tym zakresie może być wytoczone przeciwko wspólnocie mieszkaniowej, w terminie 6 tygodni od dnia podjęcia uchwały na zebraniu ogółu właścicieli lokali albo od dnia powiadomienia wytaczającego powództwo o treści uchwały podjętej w trybie indywidualnego zbierania głosów (ust. 1a tego przepisu).

Sąd Okręgowy w Świdnicy w wyroku z 27 listopada 2018 r. w sprawie I C 1465/18[352] wyjaśnił, że niezgodność z przepisami prawa to przede wszystkim kolizja treści uchwały z przepisami ustawy oraz z przepisami k.c. w zakresie, w jakim ma on zastosowanie do

349 Zgodnie z art. 43^4 k.c. firmą osoby fizycznej jest jej imię i nazwisko. Nie wyklucza to włączenia do firmy pseudonimu lub określeń wskazujących na przedmiot działalności przedsiębiorcy, miejsce jej prowadzenia oraz innych określeń dowolnie obranych.
350 https://archiwum.uodo.gov.pl/pl/225/2323
351 Ustawa z dnia 24 czerwca 1994 r. o własności lokali (t.j. Dz. U. z 2021 r. poz. 1048), dalej: „ustawa o własności lokali".
352 Wyrok Sądu Okręgowego w Świdnicy z dnia 27 listopada 2018 r. I C 1465/18, LEX nr 2629046.

odrębnej własności lokali. Niezgodność uchwały z prawem może wynikać nie tylko z treści uchwały, ale także z powodu wadliwości postępowania prowadzącego do podjęcia uchwały. Oznacza to, że właściciel lokalu może podnosić obok zarzutów merytorycznych, również i zarzuty formalne, jeżeli uważa, że zostały naruszone przepisy postępowania określające tryb podejmowania uchwał we wspólnocie mieszkaniowej. Uchybienia mogą dotyczyć np. zasad głosowania. Jak pokazuje orzecznictwo, błędy dotyczące zasad głosowania mogą dotyczyć przykładowo: oddania głosu przez osobę inną niż właściciel, oddania głosu tylko przez jednego ze współwłaścicieli czy też nieprawidłowej reprezentacji podmiotu będącego członkiem wspólnoty. Błędy te z kolei mogą mieć wpływ przy ustalaniu ważności oddanego głosu i skuteczności podjęcia uchwały większością głosów.

W świetle wyżej wskazanego uprawnienia przekazanie członkowi wspólnoty mieszkaniowej treści uchwały wspólnoty mieszkaniowej wraz z podpisami jej członków nie może być zatem traktowane jako naruszenie przepisów o ochronie danych osobowych.

Jednocześnie należy pamiętać, że udostępnianie danych osobowych członków wspólnoty w zakresie szerszym niż konieczny do sprawowania zarządu nieruchomością wspólną może stanowić naruszenie przepisów o ochronie danych osobowych (zob. Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2017, str. 44). W świetle przepisów RODO administrator jest zobowiązany do przetwarzania danych osobowych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Przetwarzanie danych osobowych musi być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których te dane są przetwarzane (art. 5 ust. 1 lit. c RODO).

Zasady ochrony danych osobowych

Kolejnym analizowanym przez organ zagadnieniem była kwestia danych nadmiarowych. Inspektor ochrony danych pełniący swoją funkcję w ośrodku pomocy społecznej w przesłanym do UODO piśmie wskazywał, iż zdarzają się sytuacje, gdy do ośrodka pomocy społecznej kierowana jest dokumentacja, o którą nie wnioskował i która nie jest mu potrzebna do prowadzenia postępowania (np. karty leczenia szpitalnego z ośrodków zdrowia czy innych instytucji). Zbędne dane – dotyczące osób trzecich albo niemające związku ze sprawą, która jest rozpatrywana – przekazywane bywają też przez klientów. Pytał, co robić z takimi niechcianymi danymi (danymi nadmiarowymi), jakie działania rekomendować pracownikom.

Urząd Ochrony Danych Osobowych w odpowiedzi na powyższe zagadnienie (w zamieszczonym na stronie internetowej materiale „**Jak postępować w przypadku otrzymywania tzw. niechcianych danych?”**[353]) wskazywał, iż rozstrzygając tego typu wątpliwości, należy uwzględnić zarówno przytoczone w pytaniu zasady RODO, jak i przepisy prawa regulujące zasady i sposób realizacji określonych zadań przez ośrodki pomocy

353 https://archiwum.uodo.gov.pl/pl/225/2247

społecznej, np. k.p.a.

Rzeczywiście RODO wymaga, aby pozyskiwane (przetwarzane) dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – tzw. zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO). Ponadto dane osobowe powinny być zbierane w wyraźnie określonym i prawnie uzasadnionym celu (art. 5 ust. 1 lit. c RODO). Niemniej kwestia ta powinna być rozstrzygana indywidualnie w każdej sprawie. Jest to spowodowane chociażby tym, że strona postępowania administracyjnego ma prawo przedstawienia wszelkich dowodów, np. dokumentów mających wpływ na jej sytuację, a w konsekwencji na treść wydanego przez organ rozstrzygnięcia. Organ dokonuje oceny tych dowodów, a następnie w uzasadnieniu decyzji wskazuje okoliczności, które uznał za udowodnione, dowody, na których się oparł oraz przyczyny, z powodu których innym odmówił mocy dowodowej. Wszelkie pisma strony składane w postępowaniu powinny zostać załączone do akt sprawy i ocenione w toku postępowania.

Mając na uwadze wskazane wyżej zasady RODO oraz przepisy prawa regulujące realizację określonych zadań przez ośrodki pomocy społecznej, np. k.p.a., administrator powinien dokonywać analizy, czy określony dokument zawierający dane osobowe istotnie został przesłany nadmiarowo lub pomyłkowo i w zależności od wyników takiej analizy np. pozostawić dokument w aktach sprawy, zwrócić lub przekazać zgodnie z właściwością do innego organu.

Realizowanie przez administratora praw osób, których dane dotyczą

Administratorzy w związku z przetwarzaniem danych osobowych obywateli Ukrainy zastanawiali się, w jakim języku powinny być formułowane kierowane do nich klauzule informacyjne (np. w związku z przyjęciem do szkoły). Ponadto wątpliwości budziło to, czy wszystkie klauzule informacyjne funkcjonujące w szkole należy przetłumaczyć na język ukraiński (np. klauzula dot. monitoringu wizyjnego, ogólna klauzula informacyjna, klauzula dot. udostępniania danych na podstawie zgody). W jaki sposób i przez kogo klauzule te powinny zostać przetłumaczone, czy konieczne jest tłumaczenie przysięgłe.

Te kwestie organ nadzorczy przedstawił w odpowiedzi na pytanie: „**W jakim języku należy wypełnić obowiązek informacyjny?”**[354]. Przypominał, iż wypełniając obowiązek informacyjny, należy przede wszystkim wziąć pod uwagę zasadę przejrzystości. Została ona wyrażona w art. 5 ust. 1 lit. a) RODO, a rozwinięta w art. 12 ust. 1 RODO. Zgodnie z drugim z wymienionych przepisów administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności, gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi

354 https://archiwum.uodo.gov.pl/pl/225/2346

sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Powyższa zasada wraz z zasadami zgodnego z prawem i rzetelnego przetwarzania (art. 5 ust. 1 lit. a RODO) nie bez powodu zajmuje pierwszą pozycję w katalogu zasad dotyczących przetwarzania danych osobowych. W praktyce oznacza ona, że osoba, której dane dotyczą, powinna zostać poinformowana o podjęciu operacji przetwarzania i jej celach, a także o ryzyku, zasadach, zabezpieczeniach i prawach związanych z przetwarzaniem jej danych osobowych.

Dlatego jeżeli administrator przetwarza dane osób nieposługujących się językiem polskim, powinien zapewnić, aby klauzule informacyjne były dla nich zrozumiałe, czyli sporządzone w języku, jakiego zwykle używa w komunikacji z tymi osobami. Grupa Robocza Art. 29 w Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev. 01 wskazała, że „jeżeli administrator kieruje informacje do osób, których dane dotyczą i które posługują się innym językiem lub innymi językami, należy zapewnić tłumaczenie w tym języku lub tych językach". W przypadku, gdy administrator przetwarza dane wielu osób posługujących się różnymi językami, możliwym rozwiązaniem jest stworzenie – oprócz klauzuli informacyjnej w języku polskim – klauzuli informacyjnej w języku uniwersalnym, takim jak np. język angielski. W sytuacji, gdy administrator będzie przetwarzał dane obywateli jednego kraju, np. Ukrainy, powinien zapewnić, aby informacje, o których mowa w art. 13 lub 14 RODO, były przekazywane tym osobom w języku dla nich zrozumiałym.

Brak jest przepisów prawa, które wskazywałyby, w jaki sposób powinny zostać przetłumaczone klauzule informacyjne. Jednakże – jak wskazała Grupa Robocza Art. 29 we ww. Wytycznych w sprawie przejrzystości – jeżeli informacje są tłumaczone na język obcy, administrator danych powinien zapewnić, by wszystkie tłumaczenia były wierne oraz by frazeologia i składnia tekstów w języku obcym były zrozumiałe. Administrator jest zobowiązany podejmować odpowiednie decyzje co do szczegółowych, przyjmowanych w konkretnej organizacji rozwiązań.

Analogicznie należy się odnieść do pytania, które klauzule powinny być przetłumaczone, ponieważ zależy to od tego, w jakich rzeczywistych celach dane osobowe Ukraińców będą przetwarzane. Również i w tym zakresie administrator musi dokonać analizy i oceny, uwzględniając konkretne okoliczności przetwarzania danych oraz wyżej wskazane zasady rzetelności, zgodności z prawem i przejrzystości. W dużej mierze zależy to od tego, jakie zadania administrator realizuje i jakie dane oraz jakiej kategorii osób w związku z tymi zadaniami przetwarza.

Inne z pytań IOD dotyczyło tego, czy osoby, których dane dotyczą, mogą wyznaczyć pełnomocników, którzy w ich imieniu będą realizować prawa przysługujące im na mocy RODO.

Wyjaśnienie tej kwestii zawarte zostało w tekście „**Czy prawo dostępu do danych**

osobowych można realizować przez pełnomocnika?”[355]. Urząd Ochrony Danych Osobowych wskazał w nim, że RODO nie odnosi się do kwestii wykonywania prawa dostępu do danych osobowych określonego w art. 15 RODO przez inną osobę niż ta, której dotyczy wniosek kierowany do administratora. Nie oznacza to jednak, by możliwość realizacji prawa dostępu do danych osobowych przez pełnomocnika była wyłączona.

Rozpatrując przedstawione zagadnienie, należy przede wszystkim wziąć pod uwagę treść art. 12 ust. 1 i 2 RODO wskazującego na konieczność łatwej dostępności do informacji na temat przetwarzania danych (zasada przejrzystości) oraz ułatwiania wykonywania praw osoby, której dane dotyczą, w tym prawa określonego w art. 15 RODO. Zgodnie z motywem 63 RODO: „Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem”. Z powyższego wnioskować można, że „możliwość łatwego wykonywania prawa dostępu do danych osobowych” oznacza również wykonywanie tego prawa przez pełnomocnika.

Z tych samych powodów należy przyjąć, że nie jest tu wymagane pełnomocnictwo (upoważnienie) mające szczególną formę. Niemniej treść pełnomocnictwa powinna pozwolić na weryfikację, kto złożył oświadczenie uprawniające inną osobę do działania w jej imieniu.

EROD w wytycznych nr 1/2022 w sprawie praw osób, których dane dotyczą – prawo dostępu w rozdziale 3.4 pt. „Requests made via third parties/proxies”[356] wskazała, że z prawa dostępu do danych osobowych najczęściej korzystają osoby, których dane dotyczą, jednak dopuścić należy również możliwość złożenia wniosku w imieniu osoby, której dane dotyczą np. przez pełnomocnika. Zgodnie ze wskazówkami znajdującymi się w powyższym projekcie wytycznych w przypadku gdy wniosek nie jest składany przez osobę, której dane dotyczą, należy wziąć pod uwagę przepisy krajowe dotyczące działania przez pełnomocnika/przedstawiciela ustawowego — w celu sprawdzenia, czy osoba ta jest prawidłowo umocowana i czy może występować w imieniu osoby, której dane dotyczą.

W przypadku rozpatrywania wniosku na podstawie art. 15 RODO przez podmioty z sektora medycznego (np. szpitale) należy zwrócić uwagę, iż dostęp do danych osobowych będzie obejmował również dane dotyczące zdrowia, a więc dane szczególnej kategorii. Jak wyjaśnia się w motywie 63 RODO, prawo określone w art. 15 RODO obejmuje „prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych

355 https://archiwum.uodo.gov.pl/pl/225/2344
356 https://uodo.gov.pl/pl/537/2517

oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania".

Z treści pełnomocnictwa dotyczącego wykonania prawa dostępu do danych osobowych w imieniu innej osoby powinno wynikać, iż obejmuje ono realizację prawa dostępu do danych osobowych przetwarzanych przez konkretnego administratora bądź kategorię administratorów przetwarzających dane o stanie zdrowia (np. szpitale, przychodnie).

Ważne jest też ustalenie, czy pełnomocnictwo (upoważnienie) obejmuje działanie do realizacji praw przysługujących podmiotowi danych na mocy RODO czy innej ustawy (np. ustawa z o prawach pacjenta i Rzeczniku Praw Pacjenta). Należy odróżnić sytuację, gdy wniosek o realizację prawa określonego w art. 15 RODO jest składany przez osobę, która została umocowana do takiego działania w imieniu innej osoby, od sytuacji, gdy osoba działa na podstawie upoważnienia, o którym mowa w art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. W myśl tego przepisu podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta.

Kolejną ważną kwestią, na którą zwrócił organ, jest weryfikacja tożsamości zarówno osoby, która składa pełnomocnictwo, jak i osoby, której danych dotyczy wniosek. EROD we ww. projekcie wytycznych zwróciła uwagę, że udostępnienie danych osobowych osobie, która nie jest uprawniona do dostępu do nich, może stanowić naruszenie ochrony danych osobowych. RODO w motywie 64 wskazuje, że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Zasadę tę należy odnieść również do weryfikacji tożsamości pełnomocnika osoby, której dane dotyczą.

Jak wynika z brzmienia motywu 59 RODO, administrator powinien przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy RODO, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych. Wobec powyższego administrator powinien zastanowić się, w jaki sposób będzie obsługiwał wnioski osób, których dane dotyczą, w tym, jak będzie weryfikować, czy osoba, która składa wniosek w imieniu innej osoby, jest umocowana do złożenia wniosku o dostęp do danych na podstawie art. 15 RODO (np. jakie dane będą niezbędne do ustalenia tożsamości osoby, której dane dotyczą, jak również jej pełnomocnika).

W ww. projekcie wytycznych EROD zwróciła uwagę na jeszcze jedną istotną kwestię. Celem prawa dostępu do danych osób, których dane dotyczą, jest zapewnienie osobom fizycznym wystarczających, przejrzystych i łatwo dostępnych informacji o przetwarzaniu ich danych osobowych, tak aby osoby te mogły być świadome i weryfikować zgodność z prawem przetwarzania oraz dokładność przetwarzanych danych. Realizowanie prawa określonego w art. 15 RODO przez pełnomocnika stanowić może gwarancję, że prawa tego nie zostaną pozbawione osoby, które nie mogą go wykonać ze względu na swój stan

zdrowia. Natomiast uznanie, iż prawo dostępu do danych może być realizowane wyłącznie osobiście, byłoby dla podmiotu danych nieuzasadnionym ograniczeniem, w szczególności w sytuacji, gdy z przyczyn obiektywnych nie mógłby tego prawa zrealizować (m.in. z uwagi na stan zdrowia albo brak umiejętności i z tego powodu potrzebne byłoby działanie przez pełnomocnika).

Wyznaczanie IOD, status i zadania inspektora ochrony danych

Kolejną grupą zagadnień, która była przedmiotem analiz organu w związku ze zgłoszonymi do niego wątpliwościami w zakresie stosowania przepisów RODO, była kwestia dotycząca wyznaczania, statusu i zadań IOD. Inspektorzy ochrony danych zwracali się z prośbą o przekazanie wskazówek co do tego: **„Czy administrator może przerzucać swoje obowiązki na IOD?”**[357].

Organ nadzorczy − udzielając odpowiedzi na to pytanie − podkreślił, iż inspektor ochrony danych to funkcja szczególna. Znajduje to odzwierciedlenie w brzmieniu przepisów RODO, określających zarówno status IOD (art. 38), jak i jego obowiązki (art. 39). UODO konsekwentnie przypominał, że do zadań inspektora ochrony danych należy m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk danego administratora, a także nadzorowanie prawidłowego wykonywania wynikających z nich obowiązków, doradzanie i podnoszenie świadomości w tym zakresie. Co istotne, IOD nie powinien być osobą, która wyręcza administratora w realizacji należących do niego zadań. Mogłoby to prowadzić do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do inspektorów art. 38 ust. 6 RODO.

Potwierdzeniem powyższego jest jedna z decyzji, w której organ nadzorczy udzielił upomnienia podmiotowi, który zobowiązał IOD do nadawania pracownikom upoważnień do przetwarzania danych osobowych[358]. W decyzji tej wskazano, że: „Podstawowy zakres zadań IOD, wśród których na próżno szukać jednak tych związanych z nadawaniem pracownikom administratora upoważnień do przetwarzania danych osobowych, określony został przez unijnego ustawodawcę w art. 39 ust. 1 RODO, niemniej zgodnie z art. 38 ust. 6 RODO IOD może wykonywać też inne zadania i obowiązki, o ile administrator lub podmiot przetwarzający zapewni, aby te zadania i obowiązki nie powodowały konfliktu interesów. Należy jednak przyjąć, że z uwagi na specyfikę zadań IOD ogniskujących się na doradzaniu oraz kontrolowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, administrator nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych, pozostawiając IOD w procedurze wydawania upoważnień do przetwarzania danych osobowych, sprawowanie funkcji doradczej i nadzorczej. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny

357 https://archiwum.uodo.gov.pl/pl/225/2374
358 sygn. sprawy ZWAD.405.31.331.2019.

za przeprowadzenie tej procedury, a jednocześnie miałby monitorować jej zgodność z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b) RODO, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 RODO. Wyraźnego podkreślenia wymaga fakt, iż IOD, cechujący się szczególnym statusem w dziedzinie zapewniania właściwego przestrzegania przepisów o ochronie danych osobowych, musi mieć dla tego celu zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację obowiązków wynikających z przepisów prawa, co wynika z art. 38 ust. 2 i 3 RODO. W tym kontekście za słuszny uznać należy pogląd, w którym nakładanie na IOD obowiązków prowadzących do powstania konfliktu interesów, stawia pod znakiem zapytania nie tylko możliwość efektywnego wypełniania przez niego zadań, do których realizacji zobowiązuje go dyspozycja normy art. 39 RODO, ale godzi w same fundamenty instytucji IOD, opartej w pierwszym rzędzie na niezależności jego funkcjonowania. […] IOD nie powinien być osobą, która realizuje obowiązki określone w art. 29 i art. 32 ust. 1 i 4 RODO, tym bardziej że adresatem norm zawartych w przytoczonych przepisach jest administrator danych lub podmiot przetwarzający. Jak już wyżej wskazano, przyjęcie odmiennego poglądu powodowałoby konflikt interesów, którego występowania zakazuje w odniesieniu do IOD art. 38 ust. 6 RODO. Zatem uprawniony jest pogląd, zgodnie z którym dla celów zapewnienia właściwej skuteczności systemowi ochrony danych osobowych [...] najkorzystniejszym rozwiązaniem jest to, w którym upoważnienia do przetwarzania danych osobowych wydawane są przez osobę pełniącą funkcję kierowniczą w ww. podmiocie, w tym np. kierownika działu kadr lub kierowników innych komórek organizacyjnych, a więc osoby będące w stanie w sposób najbardziej precyzyjny określać, komu oraz w jakim zakresie upoważnienie powinno zostać nadane oraz na bieżąco je aktualizować".

14.1.3. Działania informacyjno-edukacyjne podejmowane przez IOD

Oprócz zamieszczania na stronie internetowej Urzędu odpowiedzi na zagadnienia zgłaszane przez IOD, kolejnym i**stotnym działaniem edukacyjnym** organu nadzorczego – wspierającym IOD − **było opublikowanie 30 marca 2022 r. na www.uodo.gov.pl materiału pt. „**Weryfikacja przestrzegania przepisów dotyczących inspektora ochrony danych[359] oraz zamieszczenie w nr 4/2022 Newslettera UODO dla IOD tematu: „Ocena przestrzegania przepisów dotyczących funkcjonowania IOD"[360].

UODO w komunikacie z 30 marca 2022 r. poinformował, że korzystając ze swoich uprawnień wynikających z art. 58 ust. 1 lit. a) i e) RODO, przesłał do ponad 20 administratorów z sektora publicznego i prywatnego 27 pytań o następującej treści:

1) Czy u administratora został wyznaczony inspektor ochrony danych (IOD)?

359 https://archiwum.uodo.gov.pl/pl/138/2336
360 Archiwum Newslettera UODO dla IOD nr 4/2022: https://archiwum.uodo.gov.pl/pl/file/4030

2) Czy na administratorze ciąży obowiązek wyznaczenia IOD (jeżeli tak, to na jakiej podstawie prawnej), czy też IOD został wyznaczony mimo braku takiego obowiązku?

3) Czy administrator opublikował imię i nazwisko oraz kontakt do IOD na swojej stronie internetowej lub - jeżeli nie prowadzi swojej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia swojej działalności?

4) Czy ww. informacje znajdują się w ogólnie dostępnym miejscu (proszę wskazać to miejsce, w przypadku strony internetowej proszę wskazać jej adres oraz link do tej informacji)?

5) Czy Inspektor Ochrony Danych jest pracownikiem administratora, a jeśli nie, to na jakiej podstawie prawnej wykonuje swoje obowiązki?

6) Czy IOD został powołany na wyłączność u administratora, czy wykonuje swoje obowiązki również u innych administratorów?

7) Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza)?

8) Jakie niezbędne zasoby, o których mowa w art. 38 ust. 2 rozporządzenia 2016/679 administrator zapewnia IOD?

9) W jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?

10) Jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?

11) Czy administrator powołał zastępcę IOD, jeżeli tak, to kiedy?

12) Czy u administratora funkcjonuje zespół IOD lub inna forma stałego wsparcia IOD w zakresie wykonywania jego zadań?

13) W jaki sposób administrator zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (np. czy zostały opracowane zasady dotyczące tego, jakie sprawy mają być konsultowane z IOD, kto i w jakich sytuacjach powinien zgłaszać się w celu uzyskania konsultacji IOD, czy i na jakich zasadach IOD bierze udział w naradach kierownictwa)?

14) W jaki sposób administrator zapewnia IOD dostęp do danych osobowych i operacji przetwarzania?

15) Czy administrator przyjął jakiekolwiek regulacje wewnętrzne dotyczące funkcjonowania IOD (w szczególności w celu zapewnienia poszanowania gwarancji jego niezależności oraz jego uprawnień w zakresie dostępu do danych osobowych i operacji przetwarzania, włączania we wszystkie sprawy dotyczące ochrony danych osobowych, unikania konfliktu interesów), a jeżeli tak, to w jakim akcie wewnętrznym zostały one przewidziane?

16) W jaki sposób administrator zapewnia, aby IOD nie były wydawane instrukcje co do

wykonywania zdań przez IOD?

17) W jaki sposób administrator zapewnia, aby IOD nie był karany i odwoływany za wykonywanie swoich zadań?

18) W jaki sposób ADO postępuje w przypadku, gdy nie uwzględnia wskazówek lub rekomendacji IOD, np. czy dokumentuje powody niezastosowania tych wskazówek?

19) W jaki sposób osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych zgodnie z art. 38 ust. 4 rozporządzenia 2016/679?

20) Czy inspektor ochrony danych wykonuje również inne obowiązki lub sprawuje inną funkcję poza obowiązkami związanymi z ochroną danych osobowych, jeżeli tak to:

    a) jakie oraz w jakim wymiarze czasu pełni funkcję IOD, a w jakim inne zadania,

    b) w jaki sposób administrator ocenił, że w przypadku każdego z tych zadań nie występuje konflikt interesów, o którym mowa w art. 38 ust 6 rozporządzenia 2016/679?

    c) Czy w zakresie wykonywania innych zadań IOD podlega innym osobom niż najwyższe kierownictwo administratora?

21) Czy administrator opracował politykę zarządzania konfliktem interesów lub wprowadził inny mechanizm zapewniający niewystępowanie konfliktu interesów?

22) Czy IOD wykonuje swoje zadania jedynie w siedzibie administratora, a jeżeli nie, to w jakim miejscu i w jaki sposób zapewniona jest stała dostępność IOD dla kierownictwa i pracowników administratora?

23) Czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń, audytów?

24) Czy taki plan był prezentowany administratorowi w celu umożliwienia dokonania oceny, czy IOD dysponuje wystarczającymi zasobami i uprawnieniami w obszarach, które IOD obejmuje swoimi zadaniami?

25) Jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów?

26) Czy administrator występował do IOD o udzielenie zaleceń co do oceny skutków dla ochrony danych, a jeśli tak, to w jakich sytuacjach?

27) Czy administrator kontroluje pracę inspektora, jeżeli tak, to w jaki sposób?

Pytania te obejmują kluczowe obowiązki administratorów odnoszące się do zagwarantowania IOD prawidłowego statusu i wykonywania zadań (art. 37 – 39 RODO). Podmioty, do których zostały skierowane wezwania, zobowiązane były – zgodnie z zasadą rozliczalności – złożyć szczegółowe wyjaśnienia dotyczące przyjętych przez nich rozwiązań

w zakresie każdego obowiązku wynikającego z art. 37-39 RODO wraz z przedstawieniem odpowiednich dowodów.

Wraz z podaniem treści pytań UODO poinformował, że od początku stosowania przepisów RODO, zarówno w ramach prowadzonych postępowań, jak i w reakcji na zgłaszane mu przypadki nieprzestrzegania przepisów dotyczących inspektorów ochrony danych, podejmował działania wynikające z jego uprawnień, określone w art. 58 RODO. Dotychczasowe doświadczenia organu nadzorczego w tym zakresie posłużyły do sformułowania powyższej listy zagadnień, do których – wraz z przedstawieniem odpowiednich dowodów **–** będą musieli odnieść się wezwani administratorzy i podmioty przetwarzające.

Działania organu nadzorczego miały i mają na celu weryfikację przestrzegania przepisów dotyczących IOD jako niezwykle ważnych dla prawidłowego funkcjonowania systemu ochrony danych w każdej organizacji, która inspektora wyznaczyła. Spotkały się one z pozytywnym odbiorem nie tylko IOD, ale również administratorów, dla których lista 27 pytań była istotną wskazówką, w jakich obszarach i z jakich działań muszą się oni rozliczyć. Z drugiej strony była jasnym sygnałem dla administratorów, że organ nadzorczy od momentu wejścia do stosowania RODO ma obowiązek egzekwować standardy wynikające wprost z jego przepisów i będzie wymagał od administratorów, aby w tym zakresie wykazali się starannie przemyślanymi i sprawdzonymi pod względem skuteczności rozwiązaniami.

Jednocześnie o tej akcji UODO poinformował w newsleterze nr 4/2022. Przy tej okazji organ zwrócił uwagę, iż sukcesywnie podejmował działania edukacyjne i zamieszczał wyjaśnienia i stanowiska odnoszące się do wielu kwestii związanych z wyznaczeniem inspektora, jego właściwym funkcjonowaniem oraz prawidłowym wykonywaniem przez niego zadań. W tym numerze newslettera zaprezentowane zostało również zestawienie wyjaśnień i stanowisk − związanych z wyznaczeniem inspektora, jego właściwym funkcjonowaniem oraz prawidłowym wykonywaniem przez niego zadań zamieszczonych − na stronie internetowej UODO oraz w „Newsletterze UODO dla IOD".

Zagadnienia związane z obowiązkiem wyznaczania IOD, zapewnienia mu niezależności i gwarancji prawidłowego funkcjonowania zostały szczegółowo omówione na stronie internetowej Urzędu w zakładce Inspektor Ochrony Danych[361]. Znaleźć tu można liczne wskazówki, jak prawidłowo zawiadamiać Prezesa UODO o wyznaczeniu IOD lub jego zastępcy, a także jak przesyłać inne zawiadomienia dotyczące IOD. Dodatkowo informacje te można znaleźć również w Newsletter dla IOD:

- Zawiadomienie o wyznaczeniu IOD lub jego zastępcy trzeba przesłać na właściwym formularzu (Newsletter nr 3/2022)[362],
- Zawiadomienie dotyczące IOD lub jego zastępcy należy przesyłać tylko w postaci

361 https://uodo.gov.pl/pl/p/dla-iod
362 Archiwum Newslettera UODO dla IOD nr 3/2022: https://archiwum.uodo.gov.pl/pl/file/4010

elektronicznej (Newsletter nr 7/2022)[363].

Podjęcie powyższych działań edukacyjnych UODO uznał za niezbędne i konieczne, ponieważ nadal do Urzędu wpływają nieprawidłowe zawiadomienia dotyczące IOD (zastępców IOD). Administratorzy nadal mają trudności we właściwym wypełnieniu tego obowiązku, o czym świadczą liczne pytania kierowane do Urzędu w tym zakresie.

Przykłady działań podjętych w efekcie sygnałów od IOD

Tak jak w latach poprzednich sygnały i pytania od IOD dotyczyły wadliwie skonstruowanych przepisów prawa lub luk w przepisach prawa. W takich przypadkach Prezes UODO korzystał ze swoich uprawnień dotyczących sygnalizowania właściwym resortom konieczności dokonania stosownych zmian, które będą uwzględniały zasady ochrony danych osobowych.

Przykładem takiego działania jest wystąpienie Prezesa UODO do Ministra Spraw Wewnętrznych i Administracji, w którym wskazano, iż niektóre z przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Wystąpienie to zostało opisane w newsletterze UODO dla IOD nr 89 /2022 r. w materiale pt. „Niektóre z przepisów ustawy implementującej dyrektywę policyjną dot. IOD wymagają zmian”[364].

Innym przykładem działań podjętych w rezultacie przedstawienia problemu przez IOD było wystąpienie UODO do Ministerstwa Zdrowia sygnalizujące potrzebę dokonania zmian w „Kwestionariuszu wstępnego wywiadu przesiewowego przed szczepieniem dziecka w wieku 5-11 lat przeciw COVID-19”[365]. Organ wskazywał w nim, że nie ma podstawy uprawniającej do pozyskiwania na te potrzeby takich danych osobowych przedstawiciela ustawowego dziecka, jak: jego imię i nazwisko, numer PESEL oraz rodzaj, seria i numer dokumentu tożsamości (ewentualnie seria i numer paszportu).

W wyniku tego wystąpienia Ministerstwo Zdrowia poinformowało, że dokonało zmian w „Kwestionariuszu wstępnego wywiadu przesiewowego przed szczepieniem dziecka w wieku 5-11 lat przeciw COVID-19” oraz w „Kwestionariuszu wstępnego wywiadu przesiewowego przed szczepieniem osoby małoletniej przeciw COVID-19”[366], dostosowując je do regulacji zawartych w art. 25 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Usunięto z nich rubryki umożliwiające pozyskiwanie numer PESEL oraz serii i numeru dokumentu tożsamości przedstawiciela ustawowego, a dodano te, które służą zbieraniu informacji o jego adresie zamieszkania.

Podsumowując część sprawozdania dotyczącą pytań od inspektorów ochrony danych, można zauważyć, że zagadnienia przedstawione w pytaniach są bardzo zróżnicowane.

363 Archiwum Newslettera UODO dla IOD nr 7/2022: https://archiwum.uodo.gov.pl/pl/file/4122
364 Archiwum Newslettera UODO dla IOD nr 8-9/2022 r. https://archiwum.uodo.gov.pl/pl/file/4120
365 DOL.413.10.2022.
366 Archiwum Newslettera UODO dla IOD nr 11/2022: https://archiwum.uodo.gov.pl/pl/file/4214

Dotyczą zarówno spraw związanych z zapewnieniem prawidłowego wykonywania swojej funkcji przez IOD, jak i zagadnień, z którymi inspektorzy spotykają się, wypełniając swoje zadania, a które pochodzą z różnych sektorów gospodarki i dotyczą różnych problemów, w tym podstaw prawnych, zakresu przetwarzanych danych, statusu podmiotów, praw osób, środków organizacyjnych, które powinny być stosowane w celu zapewniania bezpieczeństwa danych.

Przedstawiane przez IOD zagadnienia i wątpliwości dotyczące stosowania przepisów prawa ochrony danych osobowych są dla organu nadzorczego niezmiernie ważne i istotne. Inspektorzy często identyfikują ważne problemy nie tylko z punktu widzenia administratora, u którego zostali wyznaczeni, ale również całego systemu ochrony danych osobowych.

Analizując treść przesyłanych do UODO pytań, można zauważyć, że w wielu przypadkach inspektorzy w swoich pismach przedstawiają rzetelnie przeprowadzoną przez siebie analizę problemu, zawierającą opis zagadnienia budzącego wątpliwości, przepisy prawa mające zastosowanie w danej sprawie oraz wyniki tej analizy. Dzięki temu organ nadzorczy może szybciej i dokładniej zidentyfikować problem i udzielić inspektorowi bardziej precyzyjnych wskazówek pomocnych w rozstrzygnięciu wątpliwości lub też podjąć inne działania, np. skierować wystąpienie.

Zdarzają się też sytuacje, gdy pytania kierowane przez inspektorów są bardzo ogólne czy wręcz lakoniczne i nie zawierają wyników analizy przeprowadzonej przez inspektora. Takie przedstawienie zagadnienia powoduje, że trudno odnieść się do pytania, zaś odpowiedź organu często ogranicza się do kierunkowego wskazania, jakie aspekty należy przeanalizować (np., że należy ustalić, jakie dane osobowe, w jakim celu i w jaki sposób będą przetwarzane, przez które podmioty, czy realizowane zadania są uregulowane przepisami prawa, jaka jest rola poszczególnych podmiotów w przetwarzaniu).

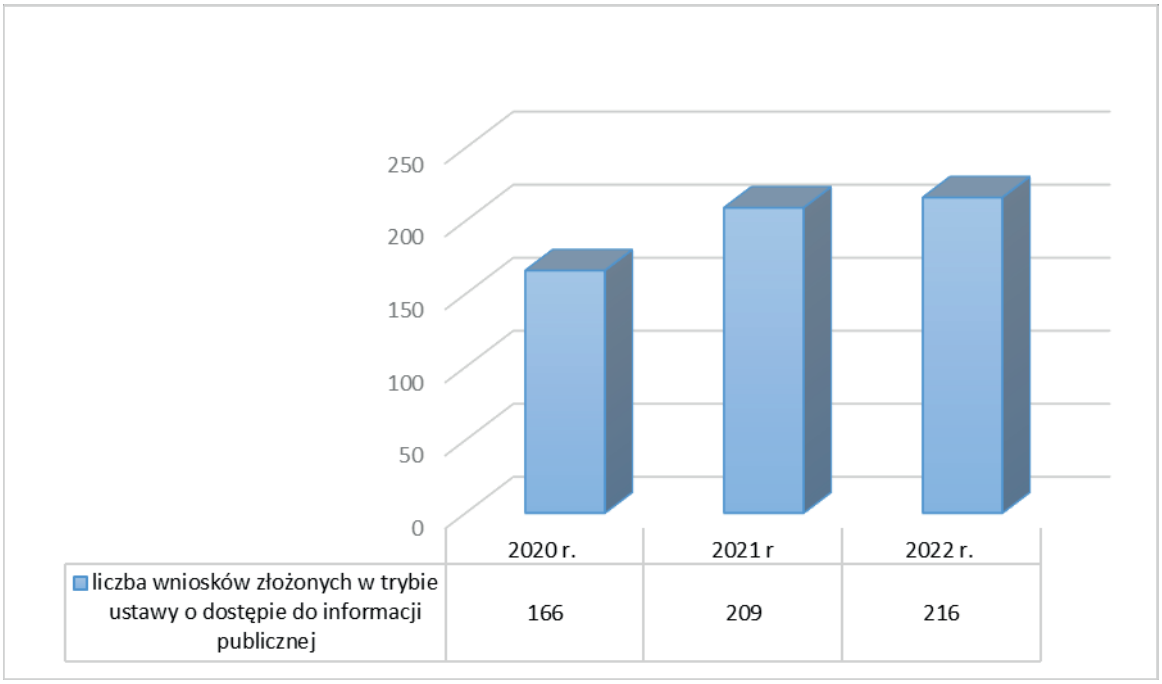
14.2. Wnioski o dostęp do informacji publicznej

Podstawy oraz ogólne zasady dostępu do informacji publicznej określone zostały w art. 61 Konstytucji RP. Zgodnie z jego treścią prawo do informacji publicznej obejmuje możliwość uzyskiwania informacji o działalności organów władzy publicznej, osób pełniących funkcje publiczne w zakresie, w jakim podmioty te wykonują zadania władzy publicznej, bądź odpowiednio gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Przepis art. 61 Konstytucji umieszczony został w Rozdziale II, zatytułowanym „Wolności, prawa i obowiązki człowieka i obywatela", w podrozdziale „Wolności i prawa polityczne". Usytuowanie prawa do informacji publicznej w grupie wolności i praw politycznych znajduje uzasadnienie w tym, że wiąże się ono ściśle z innymi prawami obywatelskimi, jak czynne prawo równego dostępu do służby publicznej, czy z fundamentalnymi zasadami ustroju politycznego państwa. Szczegółowe zasady i tryb udzielania informacji określony został w u.d.i.p.

W roku 2022 UODO odnotował wzrost zainteresowania obywateli problematyką ochrony danych osobowych oraz działalnością organu nadzorczego. Świadczy o tym większa niż w roku 2021, liczba wniosków skierowanych do UODO w trybie u.d.i.p.

W analizowanym 2022 r. do Urzędu Ochrony Danych Osobowych wpłynęło **216 wniosków o dostęp do informacji publicznej** oraz 39 pytań poza ww. trybem.

Poniższy wykres wskazuje przyrost liczby wniosków składanych w trybie ustawy o dostępie do informacji publicznej w stosunku do poprzednich lat.



Wykres 13: Liczba wniosków o dostęp do informacji publicznej, które wpłynęły do UODO w latach 2020-2022.

Pytania wnioskodawców dotyczyły zarówno realizacji ustawowych kompetencji Prezesa UODO, jak też działalności UODO w sferze organizacyjnej, finansowej czy kadrowej.

Wnioski o informację dotyczyły danych statystycznych, takich jak: liczba postępowań, skarg i naruszeń ochrony danych osobowych, liczba wydanych decyzji, przeprowadzonych kontroli, wysokości nałożonych kar pieniężnych, rodzaju i liczby zastosowanych uprawnień naprawczych, a także konkretnych rozwiązań merytorycznych. Wiele pytań dotyczyło decyzji administracyjnych, liczby zgłoszonych Inspektorów Ochrony Danych, planu kontroli sektorowych, kontroli podmiotów przetwarzających dane osobowe przy użyciu aplikacji mobilnych oraz informacji, w jakich podmiotach Prezes Urzędu przeprowadził kontrolę.

Zdarzały się również wnioski o udostępnienie treści decyzji wydanych przez Prezesa UODO, umów zawieranych przez UODO z podmiotami zewnętrznymi, statystyk dotyczących spraw kadrowych, treści opinii Prezesa UODO w sprawie zgodności projektu ustawy o szczególnych rozwiązaniach zapewniających możliwość prowadzenia działalności

gospodarczej w czasie epidemii COVID-19.

Niektóre pytania dotyczyły spraw prowadzonych przez kilka komórek organizacyjnych Urzędu, które rozpatrywane były przez Prezesa UODO czy Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w latach ubiegłych. Nierzadko jeden wniosek zawierał kilka pytań, często niezwiązanych ze sobą tematycznie. W wielu przypadkach zachodziła konieczność zwrócenia się do wnioskodawcy o uzasadnienie interesu publicznego, a dopiero potem dokonywana była analiza jego argumentów, uzupełnianie braków formalnych wniosku w związku z koniecznością wydania decyzji administracyjnej, czy udzielania odpowiedzi na skargę wnioskodawcy skierowaną do sądu.

Prezes UODO wydał w 2022 roku 4 decyzje o odmowie udostępnienia informacji publicznej. Żadna z powyższych decyzji nie została zaskarżona do WSA w Warszawie.

Liczbę wydanych przez Prezesa UODO decyzji w sprawie skierowanych do niego wniosków o dostęp do informacji publicznej w latach 2020-2022, przedstawia poniższy wykres.

Wykres 14: Liczba wydanych decyzji w sprawie wniosków o dostęp do informacji publicznej wydanych w latach 2020-2022.

W analizowanym 2022 roku wszystkie wnioski zostały rozpatrzone w ustawowym terminie.

Poza trybem udostępniania informacji publicznej UODO udzielił odpowiedzi na 39 pism zawierających pytania z zakresu swojej działalności. Tematyka tych pytań dotyczyła takich m.in. zagadnień, jak: współpraca z organami ścigania, byłego już obowiązku rejestracji zbiorów danych osobowych, przedstawienia Związkowi Banków Polskich kwestii, które mogą być istotne dla działalności sektora bankowego i jego klientów w obszarze

przetwarzania danych osobowych, pomoc w zakresie Profilu Zaufanego w serwisie e-PUAP, działań podejmowanych przez Urząd Ochrony Danych Osobowych, w szczególności wobec osób z różnymi niepełnosprawnościami, udostępnianie danych osobowych krewnego czy przewodników po RODO. Łącznie UODO udzielił **255 odpowiedzi na pytania wnioskodawców.**

14.3. Wystąpienia

Jak stanowi art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Prezes UODO może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów, wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych. Zgodnie z ustępem 2 powołanego przepisu, Prezes Urzędu może również występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych. Podmiot, do którego skierowane zostało wystąpienie, jest zaś obowiązany (zgodnie z art. 52 ust. 3) ustosunkować się do niego na piśmie w terminie 30 dni od daty otrzymania.

Wystąpienia są ważnym instrumentem w kształtowaniu i podnoszeniu poziomu ochrony danych osobowych. Zawarte w nich wnioski o zmianę obowiązujących regulacji prawnych lub o wprowadzenie nowych norm dotyczących przetwarzania danych osobowych albo wskazujące na konieczność zmodyfikowania praktyk stosowanych w podmiotach, do których są skierowane, wskazują na prawidłowy sposób postępowania i zapewniania zgodności z RODO.

W 2022 roku Prezes UODO wystosował **16 wystąpień** z określonymi wnioskami do podmiotów administracji publicznej i podmiotów prywatnych działających w różnych sektorach, z czego 14 dotyczyło zagadnień legislacyjnych, a impulsem do ich skierowania

były zarówno prowadzone analizy obowiązujących lub projektowanych aktów prawnych, jak i wpływające do Prezesa UODO sygnały czy pytania prawne, a także doniesienia medialne.

Szczególnie istotne były zaś te sprawy, które wpływały na ochronę danych osobowych lub prywatność dużych grup osób, odnosiły się do wykorzystania nowoczesnych technologii, w tym zautomatyzowanego przetwarzania oraz monitorowania osób, a także przetwarzania szczególnych kategorii danych osobowych, np. o stanie zdrowia.

Poniżej przedstawione zostały wybrane przykłady wystąpień.

Jednym z istotnych wystąpień Prezesa UODO, bo dotyczącym odpowiedniego kształtowania **przepisów legalizujących pozyskiwanie szczególnych kategorii danych osobowych**, było **wystąpienie** skierowane **do Ministra Spraw Wewnętrznych**

i Administracji[367], w związku z wpływającymi od administratorów oraz inspektorów ochrony danych (IOD) z ośrodków pomocy społecznej i gmin licznymi sygnałami dotyczącymi problemów ze stosowaniem przepisów ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz wydanych na jej podstawie aktów wykonawczych. Ich wątpliwości dotyczyły podstawy prawnej pozyskiwania danych osobowych szczególnych kategorii (np. informacji o niepełnosprawności) przez podmiot, który decyduje o przedłużeniu okresu przyznania świadczenia pieniężnego przysługującego z tytułu zapewnienia zakwaterowania i wyżywienia obywatelom Ukrainy.

Organ nadzorczy, podzielając te opinie, zwrócił się więc do Ministra Spraw Wewnętrznych i Administracji z wnioskiem o zmianę obowiązujących przepisów. Wskazał, że kwestie dotyczące przyznawania świadczenia pieniężnego przysługującego każdemu podmiotowi, który zapewni, na własny koszt, zakwaterowanie i wyżywienie obywatelom Ukrainy, zostały uregulowane w ustawie. Natomiast warunki przedłużenia przyznania tego świadczenia określone zostały w rozporządzeniu Rady Ministrów z dnia 4 maja 2022 r. w sprawie maksymalnej wysokości świadczenia pieniężnego przysługującego z tytułu zapewnienia zakwaterowania i wyżywienia obywatelom Ukrainy oraz warunków przyznawania tego świadczenia i przedłużania jego wypłaty.

Zgodnie z jego § 4 ust. 1, gmina może przedłużyć okres wypłaty wymienionego świadczenia w przypadku zapewnienia zakwaterowania i wyżywienia obywatelowi Ukrainy, który spełnia jedno z określonych w tym przepisie kryteriów, np.: posiada orzeczenie o niepełnosprawności lub stopniu niepełnosprawności lub orzeczenie, o którym mowa w art. 5 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych; posiada dokument potwierdzający I lub II stopień niepełnosprawności wydany w ramach ukraińskiego systemu orzekania o niepełnosprawności lub też jest kobietą w ciąży lub osobą wychowującą dziecko do 12 miesiąca życia. Jednocześnie przepisy te nie wskazują, w jaki sposób gminy mogą weryfikować oświadczenia składane przez wnioskodawców w zakresie spełnienia kryteriów do wydłużenia terminu wypłaty świadczeń.

Organ nadzorczy podniósł, że zgodnie z zasadą legalności określoną w art. 5 ust. 1 lit. a) RODO, podmiot może przetwarzać dane osobowe wyłącznie wtedy, gdy istnieje uprawniająca go do tego podstawa. Przy czym warunki dla przetwarzania danych szczególnych kategorii są bardziej restrykcyjne, co wynika z art. 9 ust. 1 RODO kształtującego generalny zakaz ich przetwarzania i art. 9 ust. 2, który określa odstępstwa od tego zakazu. Ma to istotne znaczenie w sytuacji przetwarzania danych osobowych przez podmioty publiczne, które jako administratorzy nie mogą pozyskiwać więcej danych, niż wynika wprost z przepisów prawa i w zakresie adekwatnym do realizowanych na podstawie ustawy celów. Aby taki podmiot mógł legalnie przetwarzać szczególne kategorie danych osobowych, takie uprawnienie musi wynikać z przepisu prawa w randze ustawy zawierającego określone gwarancje praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. b RODO).

367 DOL.413.18.2022.

W związku z tym Prezes UODO zwrócił się do Ministra Spraw Wewnętrznych i Administracji o przeanalizowanie obowiązujących regulacji pod kątem dokonania w nich stosownych zmian tak, aby nakładanie obowiązku przekazywania szczególnych kategorii danych osobowych wynikało z przepisów rangi ustawy przewidujących stosowne gwarancje dla osób, których dane te dotyczą. W odpowiedzi resort wyraził gotowość uzupełnienia lub korekty przepisów wymienionej ustawy przy okazji najbliższych prac legislacyjnych.

Z kolei z wnioskiem o **zmianę przepisów ustawy implementującej dyrektywę policyjną w zakresie przepisów dotyczących inspektora ochrony danych Prezes UODO zwrócił się do Ministra Spraw Wewnętrznych i Administracji**[368]. Wskazał, że zmiany wymagają art. 37 ust. 3 i art. 38 ust. 6 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, gdyż są one sprzeczne z przepisami tzw. dyrektywy policyjnej. Z przepisów tych wynika, że zarówno przeprowadzenie oceny skutków dla ochrony danych, jak i uprzednich konsultacji administrator może powierzyć inspektorowi ochrony danych (IOD). Tymczasem przeprowadzenie oceny skutków dla ochrony danych oraz i wystąpienie z wnioskiem o uprzednie konsultacje do organu nadzorczego to zadania administratora i to właśnie jemu są one przypisane w dyrektywie. Ich realizacja przez IOD prowadziłaby zaś do powstania konfliktu interesów. Błędna i wymagająca zmiany jest również redakcja art. 38 ust. 6. Artykuł ten stanowi, że realizację obowiązków, o których mowa w ust. 1-4 tego artykułu, administrator lub podmiot przetwarzający może powierzyć inspektorowi ochrony danych. Tymczasem ust. 2 i 4 tego przepisu odnoszą się do zadań Prezesa UODO, wobec tego przypisanie ich IOD oznacza błędne sformułowanie przepisu. Brakuje też precyzyjnych przepisów określających, jakie dane administratora powinny być przekazane przez niego do Prezesa UODO w związku z dokonywaniem zawiadomienia dotyczącego inspektora ochrony danych (wyznaczenia, odwołania, zmiany danych IOD). Ponadto potrzebne są regulacje, na mocy których administrator byłby zobowiązany do powiadomienia Prezesa UODO o każdej zmianie danych odnoszących się do administratora. Tymczasem ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych takie przepisy zawiera.

MSWiA nie w pełni podzieliło tę opinię. W ocenie resortu nie ma potrzeby doprecyzowania przepisów odnoszących się do przesyłania do Prezesa UODO zawiadomień dotyczących IOD. Pozytywnie odniesiono się natomiast do zmiany art. 37 ust. 3 i art. 38 ust. 6 ustawy w zakresie możliwości powierzenia IOD przeprowadzenia oceny skutków planowanych operacji przetwarzania danych dla ochrony danych osobowych, jak również wystąpienia do organu nadzorczego z wnioskiem o przeprowadzenie uprzednich konsultacji. W odpowiedzi na wystąpienie wskazano jednak, 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". Odnosząc się do tych informacji i dziękując za deklarację wprowadzenia zmian, organ nadzorczy wskazał, że w toku

368 DOL.413.11.2022.

ewentualnych przyszłych prac legislacyjnych należy ponownie rozważyć kwestię dokonywania zawiadomień dotyczących IOD oraz wprowadzenia przepisów, na mocy których administrator byłby zobowiązany do powiadomienia Prezesa UODO o danych administratora oraz o każdej zmianie tych danych.

W roku 2022 organ nadzorczy **wystąpił** też **do Ministra Edukacji Narodowej z wnioskiem o podjęcie inicjatywy ustawodawczej w sprawie dotyczącej dopuszczalności ujawniania list kandydatów na studia wyższe lub do szkoły doktorskiej, zawierających dane tych osób w miejscach publicznie dostępnych lub w inny sposób** (np. na własnych stronach internetowych)[369]. W przesłanej korespondencji zwrócił uwagę, że obecnie obowiązujące przepisy ustawy – Prawo o szkolnictwie wyższym i nauce nie odpowiadają w pełni zasadom ochrony danych osobowych. Stanowią bowiem jedynie o jawności wyników postępowania w sprawie przyjęcia na studia wyższe i do szkół doktorskich, bez doprecyzowania, o jaką jawność wyników chodzi. Organ nadzorczy wskazał, iż jawność wewnętrzna list kandydatów (np. przez udostępnienie w siedzibie uczelni) zasadniczo różni się od powszechnej dostępności (np. udostępnienia na stronie internetowej). Zaznaczył, że jawność wyników postępowania rekrutacyjnego nie powinna być rozumiana jako równoznaczna z pojęciem powszechnej dostępności. Organ wskazał także na konieczność przeprowadzenia analizy ryzyka oraz brak określenia okresu upowszechnienia danych. W odpowiedzi Minister Edukacji i Nauki wskazał, że to uczelnie ustalają warunki wstępu na studia i do szkoły doktorskiej, przy czym kryterium kwalifikacji stanowić może jedynie obiektywna ocena wiedzy lub umiejętności kandydatów. Żeby dochować przejrzystości procesu rekrutacji, ustawodawca określił, że wyniki postępowania w sprawie przyjęcia na studia oraz wyniki konkursu do szkoły doktorskiej będą jawne. Minister wskazał także, że każdy uczestnik rekrutacji/konkursu powinien otrzymać informację o wynikach rekrutacji, aby uczynić zadość zasadzie transparentności. Minister zapewnił jednak, że kwestie wskazane przez organ nadzorczy zostaną rozważone w toku prac przy ewentualnej nowelizacji ustawy – Prawo o szkolnictwie wyższym i nauce.

Z kolei **do Ministra Infrastruktury** organ nadzorczy **wystąpił z wątpliwościami dotyczącymi konstrukcji podstawy prawnej do przetwarzania danych osobowych osób, które nie naruszyły przepisów ruchu drogowego, przetwarzanych w ramach odcinkowych pomiarów prędkości w ruchu drogowym**[370]. Wskazał, że specyfika urządzeń służących do rejestracji odcinkowego pomiaru prędkości nie odpowiada w pełni definicji urządzenia rejestrującego z art. 2 pkt 59 ustawy – Prawo o ruchu drogowym. Zwrócił również uwagę na niezgodność art. 129h ust. 2 Prawa o ruchu drogowym ze stanem faktycznym. Przepis wskazuje bowiem, że urządzenia rejestrujące stosowane w ramach odcinkowego pomiaru prędkości rejestrują tylko dane osób, które przekroczyły prędkość dozwoloną na danym odcinku. Urządzenie rejestrujące zbiera natomiast dane osób prowadzących pojazd z dozwoloną prędkością oraz ją przekraczających. Zwrócono uwagę, że taki sposób

369 DOL.413.3.2022.
370 DOL.413.7.2022.

przetwarzania danych osobowych, których wymaga specyfika działania urządzeń służących do rejestracji odcinkowego pomiaru prędkości, aby był legalny, powinien odbywać się na podstawie stosownych norm prawnych, których obecnie brak w polskim porządku prawnym.

Minister Infrastruktury w odpowiedzi na wystąpienie nie zgodził się ze stanowiskiem organu nadzorczego, wskazując, że urządzenie rejestrujące stosowane w ramach odcinkowego pomiaru prędkości wypełnia definicję urządzenia rejestrującego zawartą w art. 2 pkt 59 ustawy – Prawo o ruchu drogowym. Wskazał także, że w przypadku braku przekroczenia dopuszczalnej prędkości, urządzenie rejestrujące nie ujawnia naruszenia, a zebrane dane są automatycznie usuwane przez to urządzenie. Nie ma także możliwości wywarcia żadnego wpływu na urządzenie przy pomocy elementów sterowania.

W wystąpieniu do Ministra Spraw Wewnętrznych i Administracji organ nadzorczy wyraził z kolei wątpliwości co do klauzuli zawartej w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wniosku o przyznanie świadczenia ratowniczego[371]. Wskazano, że klauzula ta narusza zasadę legalizmu i rzetelności z art. 5 ust. 1 lit. a) RODO, gdyż warunkuje realizację zadania wskazanego w rozporządzeniu od wyrażenia zgody osoby, której dane dotyczą, na przetwarzanie danych. Wyrażenie zgody nie może być uznane za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji. Wskazano także, że nie można stosować zgody jako przesłanki przetwarzania danych, jeżeli podstawą ich przetwarzania jest przepis prawa. W związku z tym wystarczające z punktu widzenia zapewnienia poszanowania zasady legalizmu i celowości są przepisy ustawy o ochotniczych strażach pożarnych. Wprowadzenie rozwiązania w postaci pozyskiwania dodatkowej zgody na przetwarzanie danych obarczone jest wadą wpływającą na jego skuteczność i prowadzi do konfliktu informacyjnego. Organ nadzorczy wskazał, że z powyższych względów niezbędne jest usunięcie klauzuli zgody z przepisów rozporządzenia.

W odpowiedzi Ministerstwo Spraw Wewnętrznych i Administracji zwróciło się z prośbą o opinię dotyczącą stanowiska przekazanego przez Komendę Główną Państwowej Straży Pożarnej zawierającego propozycję rozwiązania kwestii klauzuli zamieszczonej w załączniku do rozporządzenia, a także poinformowało, że wszczęte zostaną prace legislacyjne zmierzające do wyeliminowania klauzuli. Ostatecznie omawiane przepisy zostały skorygowane zgodnie z sugestiami organu nadzorczego i zaczęły obowiązywać od 27 grudnia 2022 r.

Kolejne z **wystąpień** organu nadzorczego skierowane **do Ministra Rodziny i Polityki Społecznej związane było z wątpliwościami w zakresie zgodności procesów przetwarzania danych pozyskiwanych w ramach naboru wniosków na 2022 r., w takich programach, jak „Asystent osobisty osoby niepełnosprawnej" oraz „Opieka wytchnieniowa", z przepisami RODO**[372]. Z informacji podanych w opisach powyższych

371 DOL.413.9.2022.
372 DOL.413.6.2022.

programów wynikało, że jeżeli w związku z realizacją przedmiotu umowy zaistnieje potrzeba przetwarzania przez gminę/powiat danych osobowych osób fizycznych, to gmina/powiat oświadcza, że obowiązki administratora będzie wykonywać zgodnie z przepisami prawa powszechnie obowiązującego, w tym RODO. Wskazano, że istnieją przypadki, w których administrator określony jest wprost w przepisie prawa, jednak częściej status administratora wskazany jest przez ustawę, która nakłada na dany podmiot zadanie lub obowiązek gromadzenia i przetwarzania określonych danych. Zwrócono uwagę, że na podstawie art. 110 ust. 1 ustawy o pomocy społecznej gminny ośrodek pomocy społecznej jest uprawniony do realizacji ww. programów. W konsekwencji więc to on, a nie gmina, ma status administratora. Zamieszczenie w treści klauzul informacyjnych gminy jako administratora narusza zasadę przejrzystości i rzetelności. Wskazano ponadto na potrzebę przeprowadzenia oceny skutków dla ochrony danych, ze względu na przetwarzanie danych różnych kategorii na szeroką skalę.

W odpowiedzi na wystąpienie Ministerstwo Rodziny i Polityki Społecznej przychyliło się do uwag zgłoszonych przez organ nadzorczy i po dokonaniu analizy stwierdziło, że dotychczas obowiązujące klauzule mogą nieprawidłowo wskazywać podmiot, będący realizatorem programu, który faktycznie przetwarza dane osobowe. W związku z tym Ministerstwo poinformowało, że podjęte zostaną działania mające na celu usunięcie zdiagnozowanych nieprawidłowości.

Impulsem do skierowania wystąpień do Krajowej Rady Komorniczej[373] i Ministra Sprawiedliwości[374] **w sprawie zapewnienia przetwarzania danych osobowych zawartych w publicznych obwieszczeniach komorniczych o terminie opisu i oszacowania nieruchomośc**i (art. 945 § 2 k.p.c.) zgodnie z zasadami, o których mowa w art. 5 ust. 1 RODO, były napływające do Urzędu Ochrony Danych Osobowych sygnały, przede wszystkim co do nieodpowiedniego (nadmiarowego) zakresu tych danych. Wobec braku przejrzystych norm prawnych dotyczących treści wskazanych obwieszczeń komorniczych organ nadzorczy zwrócił się do Krajowej Rady Komorniczej (KRK) o dokonanie analizy przedstawionego problemu, która mogłaby doprowadzić do wypracowania określonego standardu działania komorników w tym zakresie. W wystąpieniu do Ministra Sprawiedliwości organ nadzorczy zasugerował podjęcie niezbędnych działań legislacyjnych polegających na określeniu w przepisach prawa niezbędnego zakresu informacji, w tym danych osobowych, które powinny być zamieszczane w publicznych obwieszczeniach komorniczych o terminie opisu i oszacowania zajętej nieruchomości w rozumieniu art. 945 § 2 k.p.c. oraz określenia w nich okresu publikacji. Inicjatywa Prezesa Urzędu spotkała się z przychylnością obydwu podmiotów.

W 2022 r. organ nadzorczy zwrócił się również z prośbą do Prezesów Sądów Apelacyjnych o **zasygnalizowanie sądom okręgowym, działającym w obszarze kompetencji kierowanego przez nich sądu apelacyjnego, konieczności uwzględniania**

373 DOL.413.15.2022.
374 DOL.413.16.2022.

w ich działalności obowiązku wynikającego z art. 94 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[375] .Wystąpienie to spotkało się z pozytywnym przyjęciem, a jeden z sądów apelacyjnych zaproponował nawet wzór formularza, który mógłby być wykorzystywany przez sądy okręgowe działające w obszarze apelacji do realizacji obowiązku wynikającego z przywołanego we wcześniejszym zdaniu przepisu prawa.

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*[376]*;*
- *upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO*[377]*;*
- *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*[378]*.*

Organ właściwy w sprawie ochrony danych osobowych podejmuje szereg działań edukacyjno-informacyjnych, których celem jest zwiększenie świadomości społeczeństwa w zakresie prawa do prywatności i ochrony danych osobowych oraz podnoszenie poziomu wiedzy na temat ochrony danych osobowych w Polsce.

1. Działalność edukacyjna

Wychodząc naprzeciw zapotrzebowaniu na edukację, w analizowanym 2022 roku UODO zorganizował szereg inicjatyw w celu wyjaśnienia bieżących problemów związanych ze stosowaniem przepisów RODO w różnych obszarach życia zawodowego i prywatnego obywateli. Były to nieodpłatne szkolenia, warsztaty czy webinaria z zakresu ochrony danych osobowych, skierowane do instytucji publicznych oraz innych podmiotów zainteresowanych podnoszeniem swoich kwalifikacji w tym obszarze. Urząd Ochrony Danych Osobowych współpracuje ze szkołami wyższymi, a jego eksperci wspierają swoją wiedzą wiele wydarzeń krajowych i międzynarodowych.

375 DOL.413.12.2021.
376 Art. 57.1.b RODO.
377 Art. 57.1.d RODO.
378 Art. 57.1.e RODO.

1.1. Szkolenia zewnętrzne

Cyklicznymi szkoleniami od 13 lat organizowanym przez UODO są szkolenia realizowane w ramach ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli". Uczestnikami dwudniowych szkoleń, które każdego roku odbywają się w październiku, są koordynatorzy bieżącej edycji tego programu. Następnie koordynatorzy ci przekazują zdobytą podczas szkolenia wiedzę innym nauczycielom i w ramach lekcji z uczniami. 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 tego Programu, dzięki któremu kadra pedagogiczna szkół i placówek doskonalenia nauczycieli zdobywa wiedzę na temat zasad ochrony danych osobowych i prywatności. Szkolenia są również okazją do odpowiedzi na wiele nurtujących pytań oraz wymiany doświadczeń i dobrych praktyk dotyczących organizacji zajęć tematycznych z uczniami.

Odprawa szkoleniowa Biura Nadzoru Wewnętrznego MSWiA. Otwock, 21.06.2022 r.

Tematem spotkania było omówienie wyników czynności realizowanych przez Wydział I Biura Nadzoru Wewnętrznego MSWiA w kontekście naruszeń zgłaszanych organowi nadzorczemu przez służby nadzorowane przez MSWiA. Celem szkolenia było przedstawienie zagadnień ochrony danych osobowych w związku z sygnalizowanymi przez te podmioty potrzebami i oczekiwaniami wsparcia w zakresie interpretacji przepisów RODO i ich stosowania. Szkolenie przeprowadzili przedstawiciele Departamentu Kontroli i Naruszeń UODO.

1.2. Szkolenia wewnętrzne

Szkolenie z archiwizacji dokumentacji w systemie EZD PUW, 19.05.2022 r.

19 maja 2022 r. odbyło się szkolenie online pracowników UODO w zakresie archiwizacji dokumentacji w systemie EZD PUW, autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku. Szkolenie było skierowane do pracowników archiwum zakładowego UODO i osób odpowiedzialnych za przeprowadzenie archiwizacji w tym systemie. Zespół EZD PUW działa w ramach Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) i realizuje zadanie zlecone przez Ministra Cyfryzacji w zakresie upowszechniania, utrzymania i rozwoju systemu EZD w działalności administracji publicznej.

Szkolenia z zakresu obsługi systemu EZD PUW, 9 i 14.06.2022 r.

W związku z realizacją projektu „Upowszechnianie elektronicznego zarządzania dokumentacją w administracji publicznej", zespół EZD PUW, działający w ramach Naukowej

i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, zorganizował 2 szkolenia dla pracowników UODO. Pierwsze z nich dotyczyło **weryfikacji metadanych i przygotowania dokumentacji do archiwizacji w systemie EZD PUW** (9.06.2022 r.), drugie – **instrukcji kancelaryjnej**, a także zasad związanych z nadawaniem numeracji prowadzonym sprawom oraz przechowywania zarchiwizowanej dokumentacji (14.06.2022 r.). W trakcie tych spotkań omówiono kluczowe zagadnienia dotyczące elektronicznego zarządzania dokumentacją w obecnym otoczeniu prawnym, koncepcję udostępniania nowego systemu EZD RP oraz integracji EZD PUW z systemami zewnętrznymi.

Szkolenie z zakresu cyberbezpieczeństwa, 2.12.2022 r.

Celem szkolenia było podniesienie świadomości pracowników UODO w dziedzinie ochrony informacji w systemach IT i wskazanie sposobów reakcji na zagrożenia. Przedstawiona została procedura wdrażania rozwiązań podnoszących poziom bezpieczeństwa systemów informacyjnych będących w dyspozycji podmiotów krajowego systemu bezpieczeństwa.

1.3. Letnia Akademia Ochrony Danych Osobowych

W analizowanym roku sprawozdawczym 2022 Urząd Ochrony Danych Osobowych zorganizował dla uczniów klas VII i VIII szkół podstawowych oraz uczniów szkół ponadpodstawowych, cykl spotkań online z przedstawicielami UODO oraz liderami programu edukacyjnego „Twoje dane – Twoja sprawa".

Codziennie, od 22 do 26 sierpnia 2022 r., za pośrednictwem strony internetowej Urzędu, transmitowane były webinaria o tematyce związanej z ochroną danych osobowych.

Podczas tych spotkań słuchacze dowiedzieli się o mechanizmach cyfrowej sztuki manipulacji, zwodniczych wzorcach projektowych, poznali zasady ochrony danych osobowych i możliwe konsekwencje wynikające z naruszenia prawa do prywatności, poszerzyli wiedzę na temat wykorzystywania danych biometrycznych jako inwazyjnej metody weryfikacji dostępu do urządzeń, a także poznali praktyczne sposoby anonimizacji zdjęć, usuwania danych lokalizacyjnych oraz inne metody sprzyjające dbaniu o ochronę prywatności za pomocą bezpłatnych narzędzi informatycznych[379]. Ponadto przedstawiono młodzieży cele ogólnopolskiego programu edukacyjnego Prezesa UODO „Twoje dane – Twoja sprawa", aby zachęcić do udziału w tym przedsięwzięciu w nowym roku szkolnym

379 https://uodo.gov.pl/pl/138/2475

2022/2023, w nadchodzącej XIII edycji.

Szczegółowy przebieg letnich webinariów przedstawiał się następująco:

- „Dark patterns, czyli jak łowią w Sieci", 22.08.2022 r. - o mechanizmach cyfrowej sztuki manipulacji;
- „Czy dane osobowe mogą być kolorowe? Czyli kolorowy element na czarno-białym tle", 23.08.2022 r. – poznajemy zasady ochrony danych osobowych oraz możliwe konsekwencje wynikające z naruszenia prawa do prywatności;
- „DODO Agencja – mitologiczna interwencja", 24.08.2022 r. – poszerzamy wiedzę na temat wykorzystywania danych biometrycznych, jako inwazyjnej metody weryfikacji dostępu do urządzeń;
- „Jak chronić swoją prywatność na zdjęciach?", 25.08.2022 r. – praktyczne sposoby anonimizacji zdjęć, usuwania danych lokalizacyjnych i innych metod sprzyjających ochronie prywatności za pomocą bezpłatnych narzędzi informatycznych;
- „Dane biometryczne – bezpieczeństwo czy ryzyko?", 26.08.2022 r. – jak zapewnić skuteczną ochronę swoim danym biometrycznym?

Celem cyklu webinariów było wsparcie młodych ludzi w kształtowaniu świadomych i odpowiedzialnych zachowań związanych z bezpiecznym korzystaniem z Internetu oraz upowszechnianie wiedzy o zasadach posługiwania się danymi osobowymi w świecie nowych technologii. Inicjatywa ta służy podkreślaniu roli wartości ochrony danych osobowych w życiu każdego człowieka, w szczególności młodego pokolenia.

1.4. Ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa"

XII edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa" w roku szkolnym 2021/2022 oraz rozpoczęcie XIII edycji w roku szkolnym 2022/2023.

Zgodnie z art. 57 pkt. 1b RODO jednym z zadań Prezesa Urzędu Ochrony Danych Osobowych jest upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumieniem tych zjawisk, ze szczególnym uwzględnieniem działań skierowanych do dzieci, które są mniej świadome konsekwencji i praw przysługujących im w związku z przetwarzaniem dotyczących ich danych. Wsparciem dla tego zadania jest z powodzeniem realizowany od 2009 r. ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa", który cieszy się

niesłabnącym zainteresowaniem wśród placówek oświatowych.

Podniesienie kompetencji pedagogów i nauczycieli oraz edukowanie dzieci i młodzieży, w jaki sposób mają chronić dane osobowe zarówno w realnym, jak i cyfrowym świecie, to główne cele tego Programu, prowadzonego od 13 lat przez Prezesa Urzędu Ochrony Danych Osobowych. Program realizowany jest pod honorowym patronatem Ministra Edukacji i Nauki oraz Rzecznika Praw Dziecka, przy wsparciu patronów medialnych oraz Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie (partnera wspierającego).

Program stanowi doskonałe źródło wiedzy i dobrych praktyk dla nauczycieli w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty. Rezultatem podejmowanych działań edukacyjnych jest odpowiednia wiedza i umiejętności uczniów w zakresie ochrony swojej prywatności i danych osobowych oraz świadomość swoich praw i obowiązków wynikających z przepisów prawa. Ochrona danych osobowych jest sednem umiejętności cyfrowych, dlatego też kształtowanie odpowiedzialnych postaw i nawyków wśród dzieci i młodzieży, popularyzacja wiedzy na temat skutecznej ochrony danych osobowych wśród uczniów i nauczycieli, nabrała kluczowego znaczenia zwłaszcza w okresie edukacji zdalnej.

Program „Twoje dane – Twoja sprawa” – skierowany do szkół podstawowych, ponadpodstawowych oraz placówek doskonalenia nauczycieli – jest największym systemowym projektem edukacyjnym Prezesa Urzędu Ochrony Danych Osobowych realizowanym na skalę ogólnopolską. Działania w ramach Programu są realizowane w dwóch etapach. Po pierwsze, UODO dociera z wiedzą o ochronie danych osobowych do dyrektorów szkół i nauczycieli. W drugim etapie edukowani są uczniowie i ich środowisko. Atutem Programu jest profesjonalne wsparcie merytoryczne ekspertów Urzędu Ochrony Danych Osobowych i organizacja szkoleń oraz webinariów.

Program „Twoje dane – Twoja sprawa” od wielu lat cieszy się popularnością i na trwałe wpisał się w kalendarz wydarzeń w wielu szkołach, o czym świadczy m.in. liczny udział szkół i placówek w minionych edycjach.

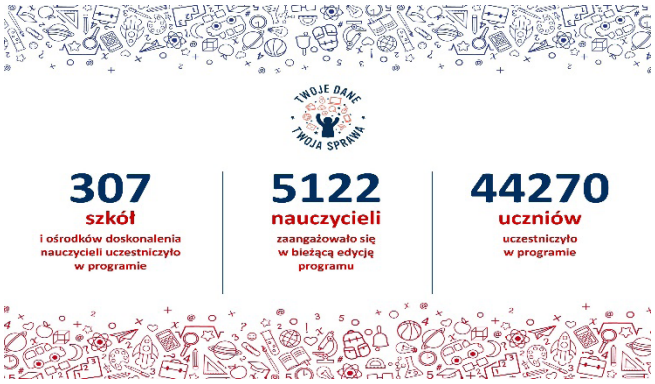
Rocznie w Programie bierze udział ponad 45 000 uczniów i ponad 4 000 nauczycieli, którzy podejmują różnorodne działania edukacyjne na rzecz upowszechniania wiedzy o ochronie danych osobowych i prawa do prywatności wśród uczniów. Co roku odbywa się ponad 1 000 inicjatyw edukacyjnych skierowanych do uczniów, nauczycieli, rodziców, seniorów i środowiska lokalnego.

Jednym z etapów Programu jest przeszkolenie i wyposażenie kadry pedagogicznej szkół i placówek doskonalenia nauczycieli w materiały edukacyjne zawierające m.in. informacje dotyczące zasad ochrony danych osobowych i scenariusze lekcji, jak również przygotowanie nauczycieli do zadania, jakim jest kształtowanie świadomych i odpowiedzialnych postaw wśród uczniów w obszarze ochrony danych osobowych, poprzez realizowane różnorodne zajęcia przystosowane do wieku uczniów. Praktyczny aspekt edukacji jest bardzo ważny. Kluczowe jest budowanie świadomości i rozumienie

pewnych zjawisk związanych z ochroną prywatności, aby umiejętnie stosować nabytą wiedzę w codziennym życiu. Umiejętności te uczniowie nabywają podczas zajęć lekcyjnych, pozalekcyjnych oraz innych wydarzeń tematycznych organizowanych lokalnie – w szkołach i placówkach doskonalenia nauczycieli.

XII edycja programu „Twoje dane – Twoja sprawa" – rok szkolny 2021/2022

W roku szkolnym 2021/2022, w XII edycji programu „Twoje dane – Twoja sprawa" udział wzięło 307 placówek oświatowych z całej Polski – wśród nich było 195 szkół podstawowych (63%), 103 szkół ponadpodstawowych (34%), a także 9 placówek doskonalenia nauczycieli (3%). Do udziału w Programie najwięcej zgłoszeń wpłynęło z województw: mazowieckiego, łódzkiego i wielkopolskiego. W zajęciach lekcyjnych, pozalekcyjnych oraz wydarzeniach tematycznych uczestniczyło 44 270 uczniów. Ze szkoleń oferowanych w ramach Programu skorzystało 5 122 nauczycieli, którzy następnie zaangażowali się w działania popularyzujące ideę ochrony danych osobowych i prywatności.



O ochronie danych osobowych nauczyciele mówili podczas godzin wychowawczych, lekcji informatyki, w ramach edukacji wczesnoszkolnej oraz innych lekcji przedmiotowych.

W XII edycji Programu odbyło się 3 543 lekcji poświęconych ochronie danych osobowych i prywatności oraz podjętych zostało 1 296 inicjatyw edukacyjnych, w tym 463 z okazji Dnia Ochrony Danych Osobowych. Przeszkolono również 5122 nauczycieli.

Dzień Ochrony Danych Osobowych 2022

Ważnym elementem realizacji każdej edycji Programu są obchody Dnia Ochrony Danych Osobowych. W różnych regionach kraju odbyły się 463 inicjatywy edukacyjne w formie lekcji, spotkań, apeli oraz zabaw dla najmłodszych. Wyświetlane były prezentacje i filmy tematyczne przygotowane przez uczniów, a także wystawy plakatów, ulotek, prac konkursowych i komiksów. Dużą popularnością wśród uczniów cieszyły się zajęcia kodowania i szyfrowania z wykorzystaniem różnych aplikacji i platform edukacyjnych, a także gry, spotkania z ekspertami, konkursy czy quizy interaktywne, krzyżówki i rebusy. Uczniowie opracowywali poradniki, kodeksy ochrony danych osobowych, a także prowadzili zajęcia dla swoich kolegów i angażowali się w przygotowanie kampanii informacyjnych, przygotowując prezentacje, ulotki, plakaty, pokazy filmowe i gazetki. Zasadniczym celem tych wydarzeń było podkreślenie istotnej roli tematyki ochrony prywatności i danych osobowych w życiu każdego człowieka.

Wielu uczestników Programu wzięło udział w konferencji „Ochrona danych osobowych

na co dzień", zorganizowanej przez Urząd Ochrony Danych Osobowych 28 stycznia 2022 r., podczas której omówiono problemy szczególnie istotne dla kadry pedagogicznej i rodziców oraz wręczono Nagrodę im. Michała Serzyckiego, Dyrektorce Szkoły Podstawowej nr 9 im. Władysława Jagiełły w Kutnie za szczególne zaangażowanie w działania edukacyjne podejmowanie na rzecz ochrony danych osobowych młodych ludzi.

Dodatkowe inicjatywy edukacyjne

Ogólnopolski program edukacyjny „Twoje dane – Twoja sprawa" od wielu lat jest szansą dla uczniów na zdobywanie i rozwijanie praktycznych umiejętności oraz kompetencji cyfrowych, niezbędnych we współczesnym świecie.

Szkolenia, materiały edukacyjne, webinaria oraz wsparcie ekspertów przyczyniają się również do wzrostu wiedzy oraz podniesienia kompetencji nauczycieli i pedagogów. W ramach XII edycji Programu odbyło się webinarium dla uczniów pt. „Twoje dane i sztuczna inteligencja" (10.01.2022 r.) oraz dla nauczycieli pt. „Jak przygotować interesujące zajęcia z uczniami w różnym wieku na temat kluczowych zasad ochrony danych osobowych?" (31.01.2022 r.).

Uczestnicy Programu brali również udział w seminarium dla nauczycieli pt. „Wpływ aktywności w Internecie na wizerunek ucznia w realnym świecie", które odbyło się 24 marca 2022 r.

Urząd Ochrony Danych Osobowych włączył się w obchody IV Dnia Nowych Technologii w Edukacji, zorganizowane przez Ministerstwo Edukacji i Nauki oraz kuratorów oświaty. Z tej okazji przygotowany został materiał dla nauczycieli i uczniów z cyklu „Warto wiedzieć… Nowe technologie a prywatność. Jak zadbać o bezpieczeństwo w Internecie?"

Konkursy i podsumowanie XII edycji programu „Twoje dane – Twoja sprawa"

Uroczystość wręczenia nagród w konkursach, prezentacja prac konkursowych oraz podsumowanie XII edycji Programu odbyło się 21 czerwca 2022 r. w Warszawie.

Na zwycięskie prace w konkursie dla uczniów złożyły się porady dla seniorów w postaci podcastów na temat zasad ochrony danych osobowych i bezpiecznego korzystania z sieci, pod hasłem „Ochrona danych osobowych na co dzień".

W konkursie dla szkół i placówek oświatowych zwyciężyły wymienione poniżej najciekawsze inicjatywy edukacyjne:

I miejsce – zdobywcą „Złotego Pióra" – statuetki specjalnego wyróżnienia Prezesa UODO – została Szkoła Podstawowa nr 360 w Warszawie za „Udany Oficjalny Debiut Oryginalny – 360 minut o ochronie danych osobowych, czyli dane osobowe na okrągło". Inicjatywa ta obejmuje osiem scenariuszy zajęć lekcyjnych w formie publikacji opracowanych przez uczniów i nauczycieli.

II miejsce zdobyła Szkoła Podstawowa nr 9 im. Władysława Jagiełły w Kutnie za lekcję integracyjną w formie zabawy w podchody, pod nazwą „8 przygód z RODO, czyli wspólna grywalizacja wieczorową porą w SP9. Szkolną dróżką do wiedzy o ochronie danych osobowych".

III miejsce zdobyła Szkoła Podstawowa nr 5 z Oddziałami Integracyjnymi im. Powstańców Śląskich w Wieluniu, za zorganizowanie happeningu pod hasłem „Twoje dane – Twoja sprawa" według autorskiego scenariusza.

Nagrodę w postaci wyróżnienia otrzymał Specjalny Ośrodek Szkolno-Wychowawczy Nr 2 w Kielcach za terenową grę edukacyjną z wykorzystaniem kodów QR.

Sieć współpracy placówek doskonalenia nauczycieli

W realizację Programu co roku włączają się placówki doskonalenia nauczycieli. Ich zaangażowanie i aktywność została doceniona podczas spotkania 21 czerwca 2022 r. podsumowującego XII edycję programu „Twoje dane – Twoja sprawa". Przedstawiciele placówek odebrali specjalne podziękowania za wkład włożony w rozwijanie kompetencji nauczycieli w zakresie ochrony danych osobowych. Koordynatorem cyklicznych spotkań online był Radomski Ośrodek Doskonalenia Nauczycieli. Udział w tych spotkaniach pozwalał nie tylko na wymianę doświadczeń, ale stanowił również inspirację do podejmowania nowych inicjatyw w ramach Programu.

XIII edycja programu „Twoje dane – Twoja sprawa", rok szkolny 2022/2023

Jak co roku, również XIII edycja programu „Twoje dane – Twoja sprawa" przyciągnęła uwagę wielu szkół i placówek oświatowych z całego kraju. 1 września 2022 r. rozpoczęła się rekrutacja uczestników tej edycji w roku szkolnym 2022/2023. Na koniec 2022 r. do udziału w XIII edycji Programu zarejestrowało się 269 placówek oświatowych, z czego 84 placówki przystąpiły do Programu po raz pierwszy, zaś 185 kontynuowało współpracę z UODO. Najliczniej reprezentowane były placówki oświatowe z województw: mazowieckiego, łódzkiego, śląskiego i wielkopolskiego.

Szkolenie online, które odbyło się 20-21 października 2022 r., zainaugurowało XIII edycję Programu. Miało na celu przygotowanie szkolnych koordynatorów Programu do jego realizacji. Podczas pierwszego dnia szkolenia eksperci UODO przekazali niezbędną wiedzę w zakresie przetwarzania danych osobowych w placówkach oświatowych oraz omówili szczegóły realizacji Programu. Drugi dzień szkolenia stanowił blok wymiany doświadczeń i dobrych praktykach, a także innowacyjnych pomysłów nauczycieli na realizację przedsięwzięć edukacyjnych.

W listopadzie 2023 roku rozpoczęto realizację ogólnopolskich lekcji dla uczniów szkół podstawowych i ponadpodstawowych pod hasłem „#ODOlekcje": Lekcje były realizowane

z udziałem liderów Programu oraz ekspertów UODO. Inicjatywa służyła zwróceniu uwagi młodych ludzi na kwestie bezpiecznego korzystania z nowych technologii oraz podkreśleniu wartości ochrony prywatności i danych osobowych w życiu każdego człowieka. Cykl comiesięcznych spotkań online rozpoczęły zajęcia pt. „Pozwólcie, że się przedstawię. Moja nowa koleżanka Prywatność – co warto i dlaczego zachować dla siebie?" (21.11.2022 r.) oraz kolejne pt. „Prawo do prywatności – czyli sposób na anonimizację zdjęć i usuwanie metadanych?" (9.12.2022 r.). Atutami zajęć była możliwość uczestniczenia w wydarzeniu w formule online, różnorodność tematów podkreślających rolę i znaczenie różnych aspektów ochrony prywatności i danych osobowych dla młodego pokolenia, a także dostosowanie tematyki i sposobu realizacji lekcji do potrzeb uczniów z niepełnosprawnościami.

W ramach XIII edycji Programu 8 grudnia 2022 r. odbyło się kolejne webinarium dla nauczycieli w ramach cyklu *RODO w szkolnej ławce* pt. „Przetwarzanie danych osobowych przez poradnie psychologiczno-pedagogiczne i rady rodziców". Podczas wykładu ekspertka UODO wyjaśniła, kto jest administratorem danych przetwarzanych przez poradnie psychologiczno-pedagogiczne w ramach kompetencji własnych oraz przez szkolnych psychologów i pedagogów. Wiele uwagi poświęciła na omówienie obowiązków administratorów wynikających z RODO, zasad, jakimi pedagodzy i psycholodzy szkolni powinni się kierować podczas udzielania odpowiedzi na wnioski o udostępnienie informacji o charakterze osobowym oraz wyjaśnieniu roli rady rodziców w procesie przetwarzania danych osobowych w szkole.

Podsumowanie

Realizacja Programu przez tysiące szkół, nauczycieli i uczniów pokazuje, jak dużo już zostało zrobione w obszarze ochrony danych osobowych dzieci w Polsce. Niemniej jednak pozostaje wiele wyzwań w tym zakresie, aby kwestia ochrony prywatności stała się szczególnie ważnym tematem w edukacji szkolnej. Współpraca ze szkołami ma bardzo duże znaczenie w realizacji tego zadania. Dzieci i młodzież są coraz bardziej świadomi swoich praw i obowiązków wynikających z przepisów prawa, a stopień spełnienia oczekiwań uczestników Programu jest bardzo wysoki, o czym świadczą, co roku wysokie oceny Programu przez jego realizatorów – uczniów i nauczycieli. Ponad połowa uczestników XII edycji Programu, kontynuowała współpracę z Urzędem Ochrony Danych Osobowych również w XIII edycji Programu. Nauczyciele wskazywali na adekwatność tematyki Programu do realiów społeczeństwa informacyjnego, uniwersalny zakres merytoryczny zajęć oraz duże zainteresowanie uczniów i nauczycieli jego realizacją. Podkreślali konieczność stałego organizowania zajęć lekcyjnych dla uczniów i wykładów dla nauczycieli w tym obszarze tematycznym, uznając je za niezbędny element zapewnienia bezpieczeństwa w środowisku szkolnym i poza nim.

Dzięki uczestnictwu w Programie dyrektorzy, nauczyciele i inspektorzy ochrony danych poszerzają swoją wiedzę na temat tego, jak bezpiecznie i zgodnie z prawem przetwarzać

dane osobowe, skutecznie przeciwdziałać naruszeniom ochrony danych osobowych oraz potrafią sprawniej identyfikować ryzyka związane z zadaniami dotyczącymi ochrony danych osobowych w placówce oświatowej.

Z kolei uczniom Program pomaga pozyskiwać wiedzę, a przez to również nabywać umiejętności, które ułatwią im funkcjonowanie nie tylko w społeczności szkolnej, ale także w środowisku lokalnym, a w przyszłości – zawodowym.

1.5. Konferencje, seminaria, spotkania

W analizowanym roku sprawozdawczym organ nadzorczy organizował konferencje i seminaria, jak również brał aktywny udział w różnych wydarzeniach organizowanych przez inne podmioty. Patronował także wielu przedsięwzięciom, których wykaz znajduje się w załączniku nr 2.

Poniżej przedstawione zostały wybrane przykłady wydarzeń krajowych lub międzynarodowych z udziałem Prezesa UODO bądź jego przedstawicieli, które odbyły się w Polsce w 2022 roku. Ich pełny wykaz zawiera załącznik nr 3.

1) XVI Dzień Ochrony Danych Osobowych – 28 stycznia 2022 r.

Przypadające co roku **28 stycznia** święto, jakim jest Dzień Ochrony Danych Osobowych, zostało ustanowione dla upamiętnienia rocznicy otwarcia do podpisu Konwencji 108 Rady Europy w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych – najstarszego aktu prawnego o zasięgu międzynarodowym, kompleksowo regulującego zagadnienia związane z ochroną danych osobowych. Z tej okazji w całej Europie organizowane są różne wydarzenia poświęcone aktualnym zagadnieniom związanym z prawem do prywatności i ochrony danych osobowych, informujące obywateli w zakresie ich praw i obowiązków oraz zagrożeń związanych z przetwarzaniem dotyczących ich danych osobowych.

Z okazji Dnia Ochrony Danych Osobowych Prezes UODO zorganizował konferencję online *„Ochrona danych osobowych na co dzień”,* która transmitowana była 28 stycznia 2022 r. za pośrednictwem strony internetowej Urzędu - www.uodo.gov.pl. Podczas tego wydarzenia poruszono zagadnienia związane z praktycznym wymiarem stosowania RODO w dwóch obszarach – w środowisku pracy oraz w sektorze oświaty, a także temat transformacji cyfrowej i powszechnego dostępu do nowych technologii. Wydarzenie to było również okazją do omówienia wyzwań związanych z budowaniem kompetencji w zakresie prawa do prywatności i ochrony danych osobowych wśród dzieci, a także zagadnień związanych z prawidłowym stosowaniem RODO w relacjach pracownik – pracodawca.

Jak co roku, Dniu Ochrony Danych Osobowych towarzyszyły wydarzenia upowszechniające wiedzę o ochronie danych osobowych, zorganizowane przez podmioty współpracujące z UODO oraz takie, które swoimi działaniami chciały zaakcentować wagę tej tematyki. Wśród nich znalazły się też uczelnie wyższe, z którymi UODO ma zawarte porozumienie o współpracy. Wśród zaplanowanych na ten dzień wydarzeń z udziałem ekspertów Urzędu, znalazły się:

- **Konferencja online „Wyzwania i standardy dla inspektorów ochrony danych", 26.01.2022 r.**

W programie Konferencji przewidziano wystąpienia przedstawicieli różnych organizacji, którzy omówili aktualne problemy związane z wykonywaniem funkcji IOD. Podczas debaty przedstawiciel Urzędu Ochrony Danych Osobowych odniósł się do zagadnień związanych z realizacją przepisów wynikających z RODO w związku z wykonywaniem zadań przez IOD. Organizatorem Konferencji było SABI – Stowarzyszenie Inspektorów Ochrony Danych[380].

- **Konferencja Rzeczowo o Prawie, pt. „Ochrona danych osobowych – wyzwania 2022", 26.01.2022 r.**

Celem konferencji było upowszechnienie wiedzy na temat aktualnych zagadnień związanych z ochroną danych osobowych, w związku z obchodami XVI Dnia Ochrony Danych Osobowych. Wydarzenie to zorganizowane zostało w Dniu Inspektorów Ochrony Danych, które przypada 26 stycznia. W trakcie konferencji poruszono zagadnienia na styku prawa ochrony danych osobowych z prawem pracy, ochroną sygnalistów, compliance, sztucznej inteligencji, nowych technologii i mediów, a także transferów danych osobowych do państw trzecich, wpływu projektów rozporządzenia ePrivacy oraz ustawy – Prawo komunikacji elektronicznej na ochronę danych osobowych. Celem tego wydarzenia było stworzenie warunków do wymiany informacji i myśli pomiędzy ekspertami i praktykami, którzy przedstawili tematykę ochrony danych osobowych przez pryzmat różnych branż. Konferencja Rzeczowo o Prawie objęta została patronatem Prezesa UODO. Przedstawiciel UODO wystąpił w sesji poświęconej wyzwaniom w zakresie stosowania przepisów RODO w świetle projektowanych przepisów ustawy o ochronie osób zgłaszających naruszenie prawa.

- **Warsztaty dla nauczycieli pt. „Warto wiedzieć… jak wykorzystać TIK w szkole, by chronić dane osobowe", 31.01.2022 r**.

Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie wraz z Urzędem Ochrony Danych Osobowych przeprowadził 31 stycznia 2022 r. warsztaty online dla nauczycieli na temat wykorzystania TIK w działaniach wspomagających nauczanie

380 https://sabi.org.pl/iii-dzien-iod/

o ochronie danych osobowych. Warsztaty zorganizowane zostały w ramach programu edukacyjnego „Twoje dane – Twoja sprawa”.

- **VIII Dzień Otwarty Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej, 7.02.2022 r.**

W związku z obchodami XVI Dnia Ochrony Danych Osobowych 28 stycznia, Akademia Wyższej Szkoły Biznesu w Dąbrowie Górniczej po raz kolejny aktywnie zaangażowała się w obchody tego święta, przygotowując konferencję tematyczną połączoną z promocją dobrych praktyk w zakresie ochrony danych osobowych. Prezes Urzędu Ochrony Danych Osobowych objął to wydarzenie patronatem honorowym oraz udzielił wsparcia merytorycznego w postaci udziału ekspertów UODO w sesjach tematycznych Konferencji.

Ceremonia wręczenia nagród im. Michała Serzyckiego

Nagroda im. Michała Serzyckiego jest wyróżnieniem Prezesa Urzędu Ochrony Danych Osobowych dla tych, którzy przyczyniają się do poszerzania świadomości na temat prywatności i roli ochrony danych osobowych w wielu dziedzinach i środowiskach. Od 2018 roku nagroda ta jest wręczana co roku podczas obchodów Dnia Ochrony Danych Osobowych. Termin ten ma wymiar symboliczny, gdyż Polska włączyła się w obchody tego święta w 2007 roku, a więc w czasie, gdy patron nagrody – Michał Serzycki – zajmował stanowisko Generalnego Inspektora Ochrony Danych Osobowych III kadencji. Jednym z rezultatów jego działań było zainicjowanie na szeroką skalę działalności informacyjnej i edukacyjnej organu ds. ochrony danych osobowych.

W 2022 roku po raz piąty przyznano nagrodę im. Michała Serzyckiego. Wyróżnieni nagrodą zostali: Pani Małgorzata Margulska-Haczyk, dyrektor Szkoły Podstawowej nr 9 im. Władysława Jagiełły w Kutnie i Pan mec. Xawery Konarski – ekspert prawny w dziedzinie prawa nowych technologii, współzałożyciel kancelarii prawnej nadzorującej prace zespołów związanych z prawem do prywatności i ochroną danych osobowych. Nagrodzonych wyróżniono za działania na rzecz edukacji w dziedzinie ochrony danych osobowych. Uroczystość wręczenia nagród odbyła się w Warszawie 27 stycznia 2022 r., w przeddzień obchodów XVI Dnia Ochrony Danych Osobowych.

XVI Dzień Ochrony Danych Osobowych w szkołach

Na coroczne obchody Dnia Ochrony Danych Osobowych składają się także liczne wydarzenia lokalne, podejmowane głównie przez szkoły i placówki doskonalenia nauczycieli uczestniczące w programie edukacyjnym UODO „Twoje dane – Twoja sprawa”.

W analizowanym 2022 roku uczniowie i nauczyciele przygotowali wiele propozycji, w tym głównie pogadanki na temat ochrony danych osobowych i prywatności podczas lekcji

wychowawczych, lekcji tematycznych z języka polskiego, informatyki, języka angielskiego i przedmiotów zawodowych, wystawy plakatów, ulotek, prac konkursowych oraz komiksów wykonanych przy użyciu nowych technik i narzędzi graficznych. Quizy, krzyżówki, rebusy, gry i zabawy z wykorzystaniem wirtualnych platform, zajęcia z kodowania, szyfrowania, kąciki informacyjne, gazetki i plakaty były przykładami najpopularniejszych sposobów upowszechniania wiedzy o ochronie danych podejmowanych w społecznościach szkolnych w związku z przypadającymi 28 stycznia obchodami XVI Dnia Ochrony Danych Osobowych. Przygotowano także zabawy o tematyce ochrony danych osobowych i prywatności adresowane specjalnie dla przedszkolaków.

Na ten Dzień szkoły zaplanowały projekcje prezentacji oraz filmów tematycznych przygotowanych przez uczniów. Przykładem takiego działania była inicjatywa uczniów Technikum Reklamy z Zespołu Szkół Usługowych w Ostrowie Wielkopolskim, którzy przygotowali prezentacje multimedialne o tematyce cyberzagrożeń, cyfrowych śladów, reputacji w sieci oraz cyberprzemocy. Podczas tego święta odbyły się też spotkania z ekspertami, m.in. z inspektorami ochrony danych oraz przedstawicielami policji.

Również placówki doskonalenia nauczycieli przygotowały na ten Dzień własne inicjatywy. Przykładowo, Radomski Ośrodek Doskonalenia Nauczycieli zorganizował grę dydaktyczną w ramach swojej sieci współpracy ze szkołami. Natomiast Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie, wraz z Urzędem Ochrony Danych Osobowych, przeprowadził 31 stycznia 2022 r. warsztaty online dla nauczycieli. Tematyka warsztatów dotyczyła wykorzystania TIK w działaniach wspomagających nauczanie o ochronie danych osobowych[381]. Celem warsztatów było wprowadzenie do tematyki planowanych przez UODO konkursów dla szkół i uczniów poprzez przygotowanie nauczycieli do organizacji zajęć z uczniami w różnym wieku na temat kluczowych zasad ochrony danych osobowych. Tematyka przewodnia warsztatów była realizowana przy wykorzystaniu TIK w oparciu o opracowany przez UODO cykl porad „Warto wiedzieć…", które zawierają praktyczne wskazówki dotyczące ochrony danych osobowych i bezpiecznego korzystania z narzędzi cyfrowych. Wśród zagadnień omówionych podczas tego warsztatu znalazły się następujące tematy:

- Warto wiedzieć... o ochronie danych osobowych – cykl porad i planowane konkursy dla uczestników programu;
- Chronimy swój wizerunek w sieci – tworzymy własne awatary;
- Narzędzia TIK do łatwej prezentacji treści związanych z ochroną danych osobowych i bezpieczeństwem w sieci;
- W stronę podcastu – uczymy się tworzyć komunikaty głosowe na temat bezpieczeństwa w sieci.

381 https://archiwum.uodo.gov.pl/pl/480/2296

2) Forum IOD, 31.03.2022 r.

Głównym tematem Forum IOD zorganizowanym przez Wielkopolski Ośrodek Kształcenia i Studiów Podyplomowych, były zagadnienia związane ze stosowaniem przepisów RODO w praktyce jednostek samorządowych. Wybuch wojny na Ukrainie zintensyfikował rozważania dotyczące udzielania pomocy humanitarnej przy zachowaniu zasad ochrony danych osobowych i prawa do prywatności osób objętych pomocą. Forum odbyło się w formule szkolenia, podczas którego przedstawiciel UODO, po prezentacji pt. „Zagadnienia dotyczące przepisów RODO w sytuacji napływających uchodźców z Ukrainy", odpowiadał na pytania inspektorów ochrony danych pracujących w gminach i powiatach województwa wielkopolskiego.

3) Konferencja pt. „Rozliczalność to podstawa RODO", 24.05.2022

Grono ekspertów i praktyków podzieliło się swoimi doświadczeniami oraz spostrzeżeniami, jak po 4 latach obowiązywania RODO przedstawia się porządek prawny w organizacji, widziany z różnych perspektyw w temacie rozliczalności. Podczas Konferencji omówiono przepisy o inspektorze ochrony danych skierowane do administratora (obowiązki, odpowiedzialność, rozliczalność), realizację zasady rozliczalności w marketingu online oraz w obszarze naruszeń ochrony danych osobowych. Poruszone zostały także zagadnienia związane z edukacją, jako gwarantem prawidłowej realizacji zasady rozliczalności w organizacji. Zastępca Prezesa UODO w swoim wystąpieniu przedstawił 27 pytań UODO, czyli o rozliczalności Inspektora Ochrony Danych. Organizatorem tego wydarzenia był DAPR sp. z o.o. skupiająca ekspertów prawa, IT oraz cyberbezpieczeństwa.

4) Konferencja „RODO i cyberbezpieczeństwo w Zdrowiu", 24.05.2022 r.

Polska Federacja Szpitali, Zespół Ekspertów w Zdrowiu oraz Kancelaria Domański Zakrzewski Palinka sp. k., byli organizatorami tego wydarzenia, podczas którego poruszone były tematy związane z bezpieczeństwem danych medycznych w środowisku cyfrowym. Przedstawiciel UODO wystąpił w sesji poświęconej kodeksom postępowania zgodnym z RODO i wyjaśnił, co w praktyce oznacza pozytywna opinia dla kodeksu i akceptacja podmiotów monitorujących.

5) Konferencja „Przeszłość, teraźniejszość i przyszłość RODO", 25.05.2022 r.

Celem Konferencji była wymiana informacji dotyczących bieżących zagadnień z zakresu RODO, w szczególności obowiązków administratorów i podmiotów przetwarzających wynikających z RODO, w świetle rozwiązań legal-tech. Temat ten poruszany był z trzech perspektyw czasu w stosunku do funkcjonowania RODO. Przedstawiciel UODO wystąpił w sesji I PRZESZŁOŚĆ, podczas której przedstawił prezentację zawierającą podsumowanie

obowiązywania przepisów RODO. Konferencja odbywała się w czwartą rocznicę obowiązywania RODO.

6) VI Kongres Sekretarzy, 19.04.2022 r.

Jednym z głównych tematów Kongresu były zagadnienia związane z informatyzacją i cyfryzacją urzędów, cyberbezpieczeństwem oraz wyzwaniami stojącymi przed jednostkami samorządu terytorialnego w zakresie przetwarzania i ochrony danych osobowych w ich pracy. Przedstawiciel UODO przedstawił prezentację, pt. „Dane osobowe. Granice swobody decyzyjnej w przedmiocie upublicznienia danych osobowych, jako informacji publicznej", w której omówiony został temat dostępu do informacji publicznej w świetle przepisów o ochronie danych osobowych. VI Kongres Sekretarzy objęty został patronatem Prezesa Urzędu Ochrony Danych Osobowych.

7) Coroczne Forum Prywatności, 23-24.06.2022 r.

Podczas Corocznego Forum Prywatności dyskutowano nad zagadnieniami związanymi z dostosowaniem prawa ochrony danych osobowych do dynamicznie zmieniającego się świata innowacji technologicznych w obszarze życia społecznego i ekonomicznego. Przedstawiciel UODO poruszył temat dotyczący nowych regulacji przyjętych w ramach strategii europejskiej i ich konsekwencji dla ochrony danych. Organizatorzy: Akademia Leona Koźmińskiego w Warszawie, Uniwersytet Karola Stefana Wyszyńskiego w Warszawie we współpracy z The European Union for Cybersecurity, DG for Communication Networks.

8) Konferencja pt. „Legal FinTech 2022". Warszawa, 21.09.2022 r.

„Wyzwania prawne w sektorze technologii finansowych" to tytuł konferencji z cyklu „Legal FinTech 2022" zorganizowanej w Warszawie przez Stowarzyszenie Prawników Nowoczesnych Technologii we współpracy z Wydawnictwem C.H.Beck. Przedstawiciel UODO wystąpił w panelu dyskusyjnym dot. procedury Know Your Customer (KYC) w kontekście nowych regulacji i wytycznych w obszarze AML, w tym zagadnień dotyczących ochrony danych osobowych.

9) Forum Inspektorów Ochrony Danych, online 23.09.2022 r.

Organizatorem Forum, który z udziałem online przedstawiciela UODO odbył się w Poznaniu, był Wielkopolski Ośrodek Kształcenia i Studiów Samorządowych. Podczas tego cyklicznego wydarzenia adresowanego do Inspektorów Ochrony Danych w gminach i powiatach poruszone były tematy związane z zapewnieniem bezpieczeństwa danym osobowym przetwarzanym w chmurze obliczeniowej i wynikających z tego obowiązków i odpowiedzialności. Przedstawiciel Urzędu wygłosił prelekcję „Usługi chmurowe a RODO –

jak je połączyć?” oraz udzielał odpowiedzi na pytania uczestników Forum.

10) Konferencja „Człowiek w postkwantowej rzeczywistości”, 28.09.2022 r.

Konferencja poruszyła tematy związane z wpływem technologii postkwantowej na życie człowieka. Z jednej strony analizowano w szczególności zagrożenia, jakie ona niesie dla cyberbezpieczeństwa i podstawowych praw człowieka. Z drugiej zaś – szukano wskazówek, jak zapewnić bezpieczeństwo i poufność przetwarzanych danych przy wykorzystaniu tej technologii. Organizatorem Konferencji, która w formule hybrydowej odbyła się w siedzibie KPRM, był UODO we współpracy z Kancelarią Premiera Rady Ministrów.

11) Webinarium „Zabezpieczenia techniczne przetwarzanych danych osobowych”, 30.09.2022 r.

Tematyka webinarium obejmowała zagadnienia będące odpowiedzią na pytania administratorów i inspektorów ochrony danych osobowych skierowane do UODO. W wystąpieniu eksperta Urzędu podkreślone zostało, aby stosowanie zabezpieczeń miało charakter ciągłego procesu, a nie jednorazowego wdrożenia. Takie działania pozwolą na bieżącą identyfikację nowych podatności w systemach i wykrycie luk w zabezpieczeniach, które nie były znane w momencie uruchamiania danych rozwiązań. Wykorzystanie takich podatności przez cyberprzestępców może nie tylko zakłócić funkcjonowanie danego systemu, ale doprowadzić do incydentu bądź naruszenia ochrony danych osobowych. Podczas tego wydarzenia kontynuowany był temat poruszony podczas webinarium, które online odbyło się 9.06.2021 r. pt. „Zgłoszenia naruszeń ochrony danych osobowych w praktyce”, gdzie omówiono praktyczne aspekty zgłaszania naruszeń ochrony danych osobowych, w oparciu o przypadek zaszyfrowania danych złośliwym oprogramowaniem typu *ransomware.*

12) VI Krajowy Kongres Sekretarzy. Warszawa, 19-20.10.2022 r.

O tym, że nie istnieje sprzeczność pomiędzy prawem dostępu do informacji publicznej a prawem do ochrony danych osobowych, przedstawiciel UODO przekonywał w swoim wystąpieniu pt. „Granice swobody decyzyjnej w przedmiocie upublicznienia danych osobowych jako informacji publicznej”. Zakres i cele regulacji w prawie do informacji publicznej i prawie do ochrony danych osobowych dają możliwość pogodzenia tych z pozoru sprzecznych celów. Organizatorem tego wydarzenia była Krajowa Rada Forów Sekretarzy działająca przy Fundacji Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego.

13) Szczyt Cyfrowy IGF Polska 2022. Lublin, 20.10.2022 r.

Przedstawiciel UODO wystąpił w jednej z trzech ścieżek tematycznych Szczytu, pod nazwą Forum Legislacji Cyfrowej, w sesji „Wpływanie na unijne środowisko legislacyjne

oraz budowanie skutecznych koalicji wspierających interesy polskiego przemysłu i nauki w Brukseli". Podczas wystąpienia przybliżył zagadnienia związane z prawnymi aspektami cyfryzacji oraz unijny proces legislacyjny. Organizatorem tej sesji była organizacja pozarządowa Business & Science Poland we współpracy z Kancelarią Prezesa Rady Ministrów – KPRM.

14) Zajęcia online dla uczniów klas 4-6 szkoły podstawowej, 21.11.2022 r.

„Pozwólcie, że przedstawię. Moja nowa koleżanka PRYWATNOŚĆ – co warto i dlaczego zachować dla siebie?" – to temat lekcji zorganizowanej przez UODO w ramach XIII edycji programu edukacyjnego „Twoje dane – Twoja sprawa". Podczas lekcji szukano odpowiedzi na pytania, czym jest sekret i tajemnica, co warto i dlaczego zachować dla siebie, czym jest prywatność i dlaczego warto o nią dbać we współczesnym świecie oraz jakie są skutki jej naruszenia. Lekcja nawiązywała do Międzynarodowego Dnia Praw Dziecka, rocznicy uchwalenia Konwencji o prawach dziecka i prawie do prywatności. Prelegentami tego wydarzenia byli: koordynatorka programu „Twoje dane – Twoja sprawa" (UODO) oraz nauczycielka ze Szkoły Podstawowej z Rzeszowa.

15) Webinarium „Projektowanie systemów SI zgodnych z RODO", 25.11.2022 r.

Wydarzenie to zainaugurowało cykl spotkań zorganizowanych przez UODO na temat sztucznej inteligencji we współpracy z Kancelarią Prezesa Rady Ministrów oraz Grupą Roboczą ds. Sztucznej Inteligencji. Celem tych spotkań miało być zwiększenie wiedzy i świadomości na temat zarządzania systemami sztucznej inteligencji i przetwarzaniem przez nie danych osobowych w sposób bezpieczny i zgodny z RODO. Eksperci przedstawili ogólne ramy unijnego rozporządzenia ws. sztucznej inteligencji, obowiązki producentów w kontekście wymogów RODO, a także kwestie wykorzystania tych systemów w celu wykrywania, zapobiegania i przeciwdziałania przestępstwom oraz identyfikowania i lokalizowania ich sprawców. Nie zabrakło również omówienia kluczowych zasad wynikających z unijnego projektu ws. sztucznej inteligencji w odniesieniu do RODO – m.in. w kontekście podejścia opartego na ryzyku czy zasad etycznych dotyczących SI z zasadami przetwarzania danych osobowych.

16) Spotkanie pt. „Stan prac nad kodeksami postępowania", 14.12.2022 r. online

Głównym tematem spotkania było przedstawienie stanu prac organu nadzorczego nad kodeksami postępowania, o których mowa w art. 40 RODO. Eksperci UODO wskazywali na korzyści dla podmiotu, który opracuje taki dokument. Podkreślano przy tym ważną rolę kodeksów postępowania zgodnych z RODO w zapewnieniu wysokich standardów ochrony danych osobowych w branży przyjmującej kodeks. Aspekt ten omawiany był na przykładzie kodeksu dla Federacji Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie.

2. Działalność informacyjna

Działalność informacyjna UODO opiera się na informowaniu społeczeństwa o zadaniach organu nadzorczego, takich jak monitorowanie i przestrzegania przepisów RODO, edukowanie społeczeństwa, współpraca z innymi organami nadzorczymi oraz na informowaniu o bieżącej działalności UODO. Działania informacyjne dotyczyły również innych zagadnień odnoszących się do ochrony danych osobowych, takich jak realizacja praw wynikających z RODO czy wskazanie praktycznych aspektów realizacji obowiązków administratorów. W analizowanym roku opinia publiczna z dużą uwagą śledziła też informacje dotyczące administracyjnych kar pieniężnych.

Wzorem lat poprzednich w 2022 roku działania informacyjne obejmowały:

prowadzenie działań informacyjno-edukacyjnych poprzez media własne, w tym inicjowanie i redagowanie komunikatów oraz tekstów problemowych czy poradnikowych udostępnianych na stronie www.uodo.gov.pl,

- obecność i obsługę profili UODO w mediach społecznościowych (Twitter),
- współpracę z przedstawicielami mediów m.in. poprzez udzielanie odpowiedzi na bieżące zapytania dziennikarzy mediów tradycyjnych i elektronicznych, aranżowanie wywiadów z ekspertami UODO i ich wystąpień medialnych,
- promocję w mediach programu edukacyjnego „Twoje dane – Twoja sprawa”,
- opracowywanie i cykliczną publikację „Newsletter UODO dla IOD”.

2.1. Strona internetowa i media społecznościowe

Rok sprawozdawczy 2022 był kolejnym, w którym UODO za pośrednictwem strony internetowej www.uodo.gov.pl komunikowało się ze społeczeństwem, stawiając na rozwój tzw. mediów własnych. Publikowane materiały kierowane były do szerokiego grona odbiorców, popularyzując w ten sposób wiedzę o ochronie danych osobowych wśród różnych grup społecznych i zawodowych. Na stronie internetowej Urzędu zamieszczono **81 komunikatów**, wśród których znalazły się również informacje o konferencjach, webinariach oraz seminariach.

Strona internetowa organu nadzorczego – www.uodo.gov.pl - odgrywa ogromną rolę informacyjną i edukacyjną.

Wśród publikowanych na niej treści dużym zainteresowaniem opinii publicznej cieszyły się informacje o administracyjnych karach pieniężnych nakładanych na administratorów w drodze decyzji administracyjnej, a także materiały związane z ewentualnymi późniejszymi postępowaniami przed sądami administracyjnymi i wydawanymi przez nie wyrokami.

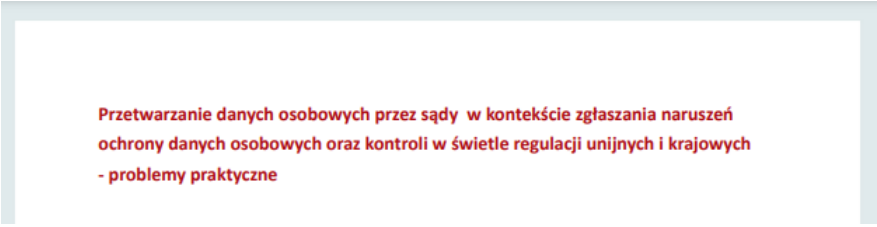
Powyższa ilustracja przedstawia grafikę wykorzystywaną w komunikatach UODO dotyczących nakładania administracyjnych kar pieniężnych.

Dużą popularnością cieszyły się również komunikaty o charakterze edukacyjnym, które UODO przygotowało i opublikowało na swojej stronie internetowej, aby wspierać uczestników systemu ochrony danych. Opracowania takie dostarczyły wielu wskazówek dla osób fizycznych oraz administratorów. Przykładem takiego działania była m.in. akcja informacyjna z okazji Dnia Bezpiecznego Internetu na temat wpływu nowych technologii na prywatność skierowaną do internautów (luty 2022 r.)[382]. UODO przedstawiło osiem dobrych praktyk, propagujących wśród internautów sposoby bezpiecznego poruszania się w internecie.

Inny przykład to aktywny udział UODO w obchodach Dnia Nowych Technologii w Edukacji (kwiecień 2022 r.)[383] - inicjatywie MEiN zorganizowanej wspólnie z kuratorami oświaty. Głównym zadaniem tego wydarzenia była popularyzowanie technologii informacyjno-komunikacyjnych wykorzystywanych w pracy z uczniami w szkole i poza nią.

UODO przygotowało interaktywną poradę dla nauczycieli i uczniów z cyklu „Warto wiedzieć... pt. Nowe technologie a prywatność. Jak zadbać o bezpieczeństwo w internecie?”[384]. W materiale przedstawiono zagrożenia dla prywatności, jakie niesie za sobą nieświadome korzystanie z nowych technologii. Eksperci UODO zaprezentowali także kilka praktycznych wskazówek, co zrobić, aby młodzi użytkownicy nowych technologii bezpiecznie posługiwali się swoimi danymi osobowymi i w ten sposób świadomie zadbali o swoją prywatność. Uzupełnieniem porady była fiszka zawierająca wyjaśnienie najważniejszych pojęć oraz quiz, dzięki któremu uczniowie mogli sprawdzić swoją wiedzę.

Kolejnym przykładem komunikatu o charakterze edukacyjnym było opracowanie poświęcone zgłaszaniu naruszeń ochrony danych osobowych przez sądy[385].



Na potrzeby tego komunikatu UODO przygotował publikację „Przetwarzanie danych osobowych przez sądy w kontekście zgłaszania naruszeń ochrony danych osobowych”. Opracowanie to stanowi odpowiedź na pytanie, czy Prezes UODO jest organem właściwym do przyjmowania zgłoszeń naruszeń ochrony danych osobowych oraz prowadzenia kontroli

382 https://archiwum.uodo.gov.pl/pl/138/2300
383 https://archiwum.uodo.gov.pl/pl/480/2362
384 https://archiwum.uodo.gov.pl/nt-2022/
385 https://archiwum.uodo.gov.pl/pl/138/2454

w przypadku sądów – i w jakim ewentualnie zakresie może takie działania podejmować.

UODO wskazywał osobom fizycznym i administratorom, jak należy zadbać o ochronę danych osobowych poprzez udzielanie odpowiedzi na pytania dotyczące interpretacji przepisów RODO w świetle obowiązujących w Polsce przepisów innych aktów prawa.

Przykładem takich wskazówek było udzielenie odpowiedzi na pytanie „Czy instytucje finansowe mogą kopiować dowody osobiste?”[386]. W materiale tym wskazano niezmienne stanowisko organu nadzorczego, że sporządzanie kopii dowodów tożsamości przez instytucje finansowe jest legalne jedynie wtedy, kiedy konieczne jest zastosowanie środków bezpieczeństwa mających na celu przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu.

Będąc aktywnym członkiem EROD, polski organ nadzorczy systematycznie informuje o działaniach EROD zmierzających do pełnej harmonizacji przepisów związanych z ochroną danych osobowych. Dzięki tej wiedzy obywatele Unii dowiadują się, jak skutecznie dochodzić przysługujących im praw. Dlatego też UODO szeroko informuje o wytycznych, decyzjach, czy opiniach przyjmowanych przez EROD. Oprócz prezentowania podsumowań posiedzeń plenarnych Rady, na stronie internetowej UODO na bieżąco publikowane są informacje o ważnych sprawach zarówno dla obywatela, jak i administratora.

W tym miejscu warto odnotować przykład sprawy dotyczącej kopiowania dokumentów tożsamości przez operatora portalu sprzedażowego, która wywołała tak ogromne zainteresowanie opinii publicznej, że przyczyniła się do zacieśnienia współpracy między organami ochrony danych i w konsekwencji – do powstania grupy roboczej składającej się z organów nadzorczych Francji, Holandii, Litwy i Polski. Nowopowstała grupa robocza do spraw Vinted, wspierana przez Europejską Radę Ochrony Danych, rozpatrzyła szereg skarg dotyczących potencjalnych naruszeń RODO przez operatora serwisu sprzedażowego odzieży[387].

Jak co roku z dużym zainteresowaniem mediów spotkała się informacja o Dniu Ochrony Danych Osobowych, zorganizowanym w 2022 roku po raz szesnasty[388], co ilustruje poniższa grafika zapowiadająca obchody tego corocznego święta.

Strona internetowa UODO była na bieżąco poddawana modyfikacjom w zakresie sposobu redagowania prezentowanych na niej treści. Przede wszystkim dopracowano ją pod kątem dostępności cyfrowej, ułatwiając korzystanie z niej przez osoby ze szczególnymi

386 https://archiwum.uodo.gov.pl/pl/138/2435
387 https://archiwum.uodo.gov.pl/pl/138/2392
388 https://archiwum.uodo.gov.pl/pl/484/2243

potrzebami. Materiały dostępne na stronie w postaci wideo były wzbogacane o dodatkową transkrypcję, co uczyniło je atrakcyjniejszymi w odbiorze i bardziej odpowiadającymi aktualnym potrzebom komunikacyjnym odbiorców. Łącznie UODO przygotowało **8 materiałów filmowych**.

Równolegle do prezentowania w Internecie bieżącej działalności informacyjno-komunikacyjnej Urzędu, trwały prace nad nową odsłoną strony WWW w celu dostosowana jej do zróżnicowanych potrzeb odbiorców.

Istotnym wzmocnieniem działań informacyjnych prowadzonych przez UODO było systematyczne **komunikowanie za pośrednictwem mediów społecznościowych**. Chodzi przede wszystkim o działania informacyjne UODO prowadzone w serwisie Twitter – @UODOgov_pl.

W analizowanym 2022 roku na Twitterze UODO opublikowano 536 wpisów. Dla porównania w 2021 r. zamieszczono 493 tweetów. Liczba wyświetleń publikacji w perspektywie całego roku przekroczyła 380 tys. – wygenerowały one średni miesięczny zasięg na poziomie niemal 32 tys. W 2022 roku profil @UODOgov_pl liczył prawie 178 tys. odsłon. Liczba osób śledzących profil na koniec grudnia 2022 roku wynosiła 5 653.

Natomiast w publikacjach na Twitterze pojawiło się 1 651 wzmianek profilu @ UODOgov_pl.

Na Twitterze zamieszczane były wypowiedzi eksperckie pracowników UODO, a także komunikowane były inicjatywy i wydarzenia (szkolenia, debaty, wykłady, webinaria, konferencjach, czy seminaria naukowe) zorganizowane przez UODO, bądź nad którymi UODO objął patronat honorowy. Wydarzenia te były relacjonowane na żywo, ale udostępniane też były zapisy nagrań. Nie zabrakło także wpisów wzbogaconych o grafiki lub animacje, które uatrakcyjniały prezentowane posty.

Poniżej zaprezentowany został przykładowy post wzbogacony grafiką.

Równie istotną rolę pełnił wymiar edukacyjny – w serwisie Twitter publikowane były wskazówki i porady dotyczące ochrony danych osobowych oraz ostrzeżenia przed zagrożeniami. Prowadzono także działania promocyjne ogólnopolskiego programu edukacyjnego „Twoje Dane – Twoja Sprawa", informowano o wydaniu najnowszego numeru „Newsletter UODO dla Inspektorów Ochrony Danych" oraz o zredagowaniu nowych odpowiedzi na pytania IOD. W roku 2022 opublikowano także posty zawierające informacje o ofertach pracy i aktualnie trwających rekrutacjach.

Przykładowy post informujący o wydaniu „Newsletter UODO dla Inspektorów Ochrony Danych", przedstawia się następująco:

Profil UODO na Twitterze służy jako dodatkowy kanał komunikacji do promocji wydarzeń organizowanych przez UODO i zachęcający do udziału w nich. Warto podkreślić, że prowadzenie oficjalnego profilu nie wymaga dodatkowych nakładów finansowych. Publikowane na nim treści mają charakter głównie informacyjny i merytoryczny, rzadziej wizerunkowy. Zaletą Twittera jest możliwość bezpośredniej komunikacji z obywatelem i budowania zaufania do UODO. Informacje zamieszczane na Twitterze są przekazywane w sposób skuteczny i szybki. Pozwala to UODO aktywnie i na bieżąco reagować na pojawiające się wątpliwości czy problemy oraz jeszcze lepiej dostosowywać treści przekazów do potrzeb użytkowników. Niemal wszystkie treści zamieszczane na oficjalnym profilu na Twitterze odsyłały na stronę www.uodo.gov.pl, która jest podstawowym źródłem informacji o działalności Urzędu.

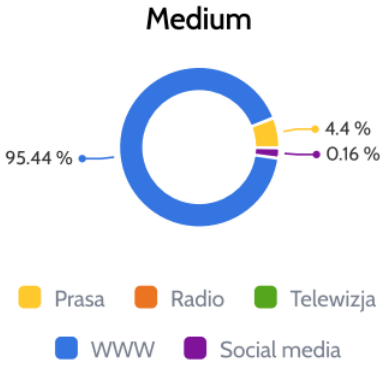
UODO prowadzi również anglojęzyczną stronę internetową – www.uodo.gov.pl/en, oraz anglojęzyczny profil na Twitterze – @PDPO_Poland, które są wykorzystywane jako kanały komunikacji w ramach współpracy międzynarodowej prowadzonej przez UODO. Aktywność kanału na Twitterze – @PDPO_Poland obejmowała informowanie o najważniejszych aktualnościach oraz udostępnianie tweetów zamieszczonych na profilu Europejskiej Rady Ochrony Danych (@EU_EDPB). W okresie sprawozdawczym opublikowano 55 wpisów, które dotarły do ponad 5,5 tys. użytkowników. W 2022 r. profil anglojęzyczny został wyświetlony ponad 19,6 tys. razy i zyskał 52 nowych obserwujących. Na koniec grudnia 2022 r. liczba obserwujących profil @PDPO_Poland wynosiła 368 osób.

2.2. Współpraca z mediami

W 2022 roku UODO współpracował z mediami o zasięgu ogólnopolskim, regionalnymi oraz z ogólnopolskimi pismami branżowymi. Tematyką ochrony danych osobowych i prywatności interesowały się również media lokalne. Współpraca z mediami objęła także portale internetowe, w tym serwisy tematyczne.

W ramach stałej współpracy UODO z mediami opracowanych zostało 78 informacji prasowych o tematyce ochrony danych i prywatności oraz udzielono blisko **30** wypowiedzi radiowo-telewizyjnych. Dotyczyły one tematów związanych z bieżącą działalnością organu nadzorczego lub były reakcją na zdarzenia wzbudzające zainteresowanie opinii publicznej.

W roku sprawozdawczym 2022 w mediach tradycyjnych i na portalach internetowych ukazało się ok. **19,1 tys. informacji** w postaci artykułów, notek lub wzmianek, najczęściej odnoszących się do działalności Urzędu Ochrony Danych Osobowych[389]. Jeśli chodzi o wskaźnik zasięgu informacji[390], to wyniósł on 6,5 mld potencjalnych kontaktów, zaś dotarcie informacji wyniosło 145,7 mln realnych kontaktów.

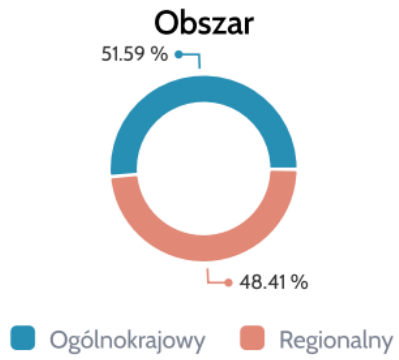


Wykres 15: Procentowy udział publikacji nt. UODO, które ukazały się w 2022 roku, w podziale na media.

389 Tak wynika z danych zebranych przez PSSM Monitoring & More

390 Zasięg publikacji jest miarą określającą liczbę potencjalnych kontaktów odbiorców z przekazem medialnym. W prasie obliczany jest na podstawie sumy nakładów pisma, w Internecie wyrażany jest przez sumę liczby unikatowych użytkowników danego portalu. Natomiast w radiu i telewizji zasięgiem jest suma oglądalności bądź słuchalności danej stacji. Zasięg wyraża liczbę potencjalnych kontaktów z informacją, a nie liczbę osób, które mogły zetknąć się z nią. Zasięg wyższy niż liczba mieszkańców Polski oznacza, iż każda osoba mogła spotkać się z daną informacją kilkukrotnie.

Dotarcie publikacji jest miarą określającą liczbę realnych kontaktów odbiorców z przekazem medialnym. Dotarcie jest przypisane do konkretnej publikacji. Różni się od zasięgu wprowadzeniem zmiennych odnoszących się do realnych zachowań odbiorców – sposobów i częstotliwości korzystania z kanałów przekazu.



Wykres 16: Procentowy podział aktywności mediów ogólnopolskich i regionalnych na temat UODO w 2022 r.

Dominującym środkiem przekazu nt. działalności UODO niezmiennie pozostaje Internet. Znajduje to odzwierciedlenie w liczbie opublikowanych informacji za pośrednictwem mediów internetowych lub internetowych wydań mediów tradycyjnych. Za ich pośrednictwem dziennikarze przekazywali informacje dotyczące różnorodnych działań związanych z zadaniami i decyzjami Prezesa UODO, relacjonowali wydarzenia z udziałem ekspertów Urzędu, informowali o wielu przedsięwzięciach informacyjno-edukacyjnych podejmowanych przez UODO, a także zwracali się z pytaniami odnoszącymi się do różnych, nierzadko złożonych stanów faktycznych.

Kontynuowana była również współpraca z ogólnopolskimi stacjami telewizyjnymi i radiowymi o profilu informacyjnym i społeczno-gospodarczym oraz z redakcjami czasopism branżowych, we współpracy z którymi publikowano cykliczne materiały eksperckie. Natomiast regularna współpraca z czołowymi agencjami informacyjnymi zaowocowała realizacją wielu materiałów informacyjnych.

W roku sprawozdawczym uwagę mediów zwróciły opublikowane na stronie www.uodo.gov.pl m.in. teksty problemowe i poradnikowe. Szczególnym zainteresowaniem dziennikarzy cieszyły się porady dla inspektorów ochrony danych dostępne na stronie internetowej Urzędu oraz artykuły publikowane w „Newsletterze UODO dla Inspektorów Ochrony Danych".

Tematyka, która budziła szczególne zainteresowanie dziennikarzy, była bardzo zróżnicowana. Dużą uwagą cieszył się wątek wpływu RODO na prewencyjne badania przez pracodawców stanu trzeźwości pracowników. Miało to niewątpliwie związek z trwającymi w 2022 roku pracami legislacyjnymi, które zakończyły się w grudniu 2022 roku uchwaleniem nowelizacji kodeksu pracy, umożliwiającej pracodawcom przeprowadzanie takich badań. Wiele uwagi dziennikarze poświęcili także takim zagadnieniem jak: naruszenia ochrony danych osobowych, ochrona wizerunku, monitoring wizyjny czy praca zdalna. Dziennikarze wykorzystywali także komunikaty UODO poświęcone bieżącej działalności EROD, zwłaszcza w obszarze współpracy transgranicznej oraz spraw dotyczących największych

firm technologicznych.

Dziennikarze zarówno mediów ogólnopolskich, jak i regionalnych i lokalnych, byli szczególnie zainteresowani wątkami kradzieży tożsamości, wycieków danych czy dopuszczalności kopiowania dokumentów tożsamości. W wielu takich sprawach zwracali się do UODO w celu potwierdzenia tych zdarzeń. Równie chętnie korzystali z opracowań UODO, udzielając obywatelom na ich podstawie wskazówek, jak przeciwdziałać negatywnym skutkom utraty kontroli nad danymi osobowymi.

Współpraca z mediami zaowocowała także patronatami medialnymi nad np. XVI Dniem Ochrony Danych Osobowych oraz XII i XIII edycją programu edukacyjnego „Twoje dane – Twoja sprawa".

2.3. Odpowiedzi na indywidualne pytania dziennikarzy

Szczególne miejsce w realizacji działań informacyjnych UODO zajmuje udzielanie odpowiedzi na indywidualne pytania dziennikarzy. W roku sprawozdawczym 2022 odnotowano **241 pytań** skierowanych do rzecznika prasowego Urzędu.

Pytania dziennikarzy charakteryzowały dużą szczegółowością. Do rzadkości należały pytania o podstawowe i ogólne kwestie związane z przepisami RODO, jak np. czym są dane osobowe, jakie prawa mają osoby, których dane dotyczą, jakie obowiązki mają administratorzy danych, itp.

Odpowiedzi dla mediów często wymagały odwołania się nie tylko do przepisów o ochronie danych osobowych, ale i do przepisów szczególnych lub też wymagały ustaleń z innymi przedstawicielami EROD. Takie sytuacje miały miejsce szczególnie w przypadku zagadnień dotyczących praw i obowiązków pracodawców w zakresie ochrony danych osobowych, przechowywania przez nich danych osobowych pracowników oraz zasad ich zabezpieczania. Pytania dotyczyły w szczególności rodzajów zabezpieczeń technicznych, jakie powinni stosować administratorzy w celu skutecznej ochrony danych i związanej z tym analizy ryzyka. Wiele pytań odnosiło się też do działalności tzw. gigantów technologicznych i oferowanych przez nich usług.

Dziennikarze najczęściej zadawali pytania dotyczące naruszeń ochrony danych osobowych. Stanowiły one ponad jedną trzecią wszystkich pytań i związane były z wyciekami danych, o których nierzadko informowali sami administratorzy, realizując ciążące na nich obowiązki związane z powiadamianiem osób, których dotyczyły te incydenty. Media były wówczas zainteresowane informacjami dot. danego naruszenia, konsekwencjami, jakie grożą administratorowi danych i co mogą zrobić osoby, których dane zostały naruszone.

Zauważalna jest różnica w podejściu do tematu naruszeń ochrony danych osobowych wśród mediów ogólnopolskich i regionalnych. Te pierwsze zazwyczaj interesowały się naruszeniami, które miały miejsce w dużych podmiotach. Natomiast wiele pytań od

przedstawicieli mediów regionalnych dotyczyło przede wszystkim incydentów, które miały miejsce w ich województwie czy mieście – nawet gdy naruszenie dotyczyło jednej bądź kilku osób. W takich przypadkach dziennikarze częściej pytali o podjęte w danej sprawie działania UODO i możliwe decyzje organu nadzorczego.

Kolejnymi tematami, które w roku sprawozdawczym cieszyły się dużym zainteresowaniem dziennikarzy, był monitoring oraz orzecznictwo sądów administracyjnych w sprawach dotyczących decyzji Prezesa UODO. W odniesieniu do monitoringu na pierwszy plan wysunęły się zagadnienia prawne i techniczne monitoringu stosowanego przez pracodawców. Natomiast w kwestiach związanych z orzecznictwem sądów administracyjnych, media zazwyczaj ciekawił komentarz UODO do zapadających wyroków, jak i ewentualne dalsze działania organu nadzorczego w przypadku orzeczeń Wojewódzkiego Sądu Administracyjnego w Warszawie.

Wśród innych tematów, jakie interesowały dziennikarzy w roku sprawozdawczym, znalazły się m.in.:

- zagadnienia związane z telemarketingiem i pozyskiwaniem danych przez firmy świadczące usługi w tej dziedzinie;
- kopiowanie dokumentów tożsamości przez różne instytucje;
- statystyki związane ze skargami, naruszeniami oraz karami.

2.4. Newsletter UODO dla inspektorów ochrony danych – IOD

W 2022 roku kontynuowano wydawanie cyklicznego **„Newslettera UODO dla Inspektorów Ochrony Danych”**[391]. W roku sprawozdawczym 2022 ukazało się 11 wydań. O jego popularności świadczy stale rosnąca liczba subskrybentów. Na koniec grudnia 2022 roku newsletter trafił do **9257 subskrybentów**. Dla porównania, w analogicznym okresie na koniec grudnia w 2021 r. było **8592** subskrybentów.

Na ilustracji poniżej przedstawiony został nagłówek tytułowy „Newslettera UODO dla Inspektorów Ochrony Danych”.

391 https://uodo.gov.pl/p/archiwum-newslettera-dla-iod

„Newsletter UODO dla Inspektorów Ochrony Danych" stanowi cenne źródło informacji o działalności Urzędu. Początkowo powstał z myślą o bieżącym informowaniu głównie inspektorów ochrony danych. Niemniej jednak prezentowane w nim materiały mają na tyle ogólny charakter, że pomagają przybliżyć tematykę ochrony danych osobowych również osobom spoza tego kręgu. Dlatego dużą część subskrybentów stanowią również inne osoby zainteresowane ochroną danych osobowych i prawem do prywatności, w tym dziennikarze oraz przedstawiciele podmiotów prawnych. Zamieszczane w newsletterze materiały zawierają ogólne wskazówki o stosowaniu przepisów RODO oraz wnioski płynące z decyzji administracyjnych. W 2022 roku wprowadzono do periodyku nowy rozdział „Rozmowy z ekspertem", w którym publikowane były najciekawsze rozmowy przeprowadzone z osobami zajmującymi się ochroną danych osobowych.

Treści publikowane w newsletterze wpisują się w działalność informacyjno-edukacyjną Urzędu, co pozwala organowi nadzorczemu nie tylko na budowanie relacji z wszystkimi osobami, którym bliska jest tematyka ochrony danych osobowych, ale także na utrzymanie z nimi stałej, comiesięcznej komunikacji.

2.5. Infolinia UODO

Każdego dnia pracownicy infolinii UODO odbierają kilkadziesiąt telefonów od osób zainteresowanych tematyką dotyczącą ochrony danych osobowych. Z pytaniami zwracają się zarówno osoby fizyczne, jak i podmioty prawne. Pracownicy infolinii przekazują informacje dotyczące działalności UODO, upowszechniając wśród obywateli wiedzę o ochronie danych osobowych oraz o przysługujących im prawach. W szczególności informują o procedurze składania skarg i wniosków, prawidłowym wypełnianiu i przesyłaniu formularzy zgłoszeń naruszeń oraz zgłoszeń powołania, odwołania i innych zmian w odniesieniu do inspektora ochrony danych, a także o wydarzeniach z dziedziny ochrony danych osobowych, w tym o szkoleniach i konferencjach organizowanych lub współorganizowanych przez UODO.

Tematyka przeprowadzonych rozmów w roku sprawozdawczym była bardzo różnorodna. Najczęściej zadawane pytania dotyczyły (oprócz pytań o stan sprawy toczącej się w Urzędzie) następujących zagadnień:

- monitoring wizyjny,
- przetwarzanie danych osobowych przez spółdzielnie i wspólnoty mieszkaniowe,
- przetwarzanie danych osobowych przez pracodawców,
- prawidłowe postępowanie w przypadku naruszeń,
- niechciany telemarketing,
- żądanie przez internetowe platformy sprzedażowe przesyłania skanów dokumentów tożsamości w celu odblokowania środków otrzymanych ze sprzedaży na kontach użytkowników.

Techniczne uwarunkowania infolinii nie pozwalają na przedstawienie dokładnej liczby odebranych połączeń. W przybliżeniu pracownicy infolinii przeprowadzili w 2022 roku **prawie 12,8 tys. rozmów, co w przeliczeniu na dzień roboczy daje wynik ok. 51 rozmów telefonicznych dziennie.** Trzeba mieć też na uwadze, że na jedno połączenie często składało się kilka pytań, dotyczących różnych i nierzadko skomplikowanych prawnie zagadnień.

2.6. Inne

W 2022 roku odbyło się 10 spotkań, w ramach prac sieci komunikacji EROD (Communications Network). Spotkania te odbywały się gównie w formule online i tylko jedno spotkanie odbyło się stacjonarnie w Brukseli.

Grupa ta jest platformą wymiany wiedzy, doświadczeń, działań pomiędzy poszczególnymi członkami EROD. Uczestnicząc w spotkaniach Communications Network, polski organ nadzorczy miał możliwość zapoznania się z działaniami komunikacyjnymi innych organów nadzorczych, z ich interpretacją przepisów oraz z informacjami o karach nakładanych przez te organy. Podczas tych spotkań omawiano plany działania poszczególnych organów ochrony danych osobowych oraz wspólne działania komunikacyjne w ramach EROD. Ponadto omawiano sposoby wzmocnienia i poprawę współpracy w realizacji zadań komunikacyjnych w sprawach transgranicznych. Każdy komunikat wydawany po posiedzeniach plenarnych Rady był przedmiotem zainteresowania sieci komunikacji rzeczników prasowych.

Podczas spotkań omawiane były przede wszystkim bieżące komunikaty publikowane na stronie EROD, projekty koordynowane przez Radę, działania prasowe poszczególnych organów krajowych, a także sposoby wzmocnienia współpracy w realizacji zadań komunikacyjnych w sprawach transgranicznych.

W roku 2022 w ramach spotkań sieci rzeczników podjęto m.in. pracę nad przygotowaniem wkładu do rocznego raportu EROD. Dokument ten zawierał:

- przegląd najważniejszych decyzji karowych wydanych przez organy nadzorcze, w tym Prezesa UODO;
- informację o zaangażowaniu rzeczników w działania na rzecz optymalizacji skutecznego sposobu wzajemnego informowania się jednostek organizacyjnych urzędów w sprawach o transgranicznym charakterze w ramach mechanizmu kompleksowej współpracy.

Wśród działań informacyjnych UODO znalazły się też takie, które UODO zrealizował we współpracy z innymi podmiotami. Przykładem było ogólnopolskie badanie opinii publicznej pt. „Ochrona danych osobowych w 2022 r.” na temat świadomości Polaków w kwestii zagrożeń ochrony danych osobowych związanych z postępem technologicznym, sposobów

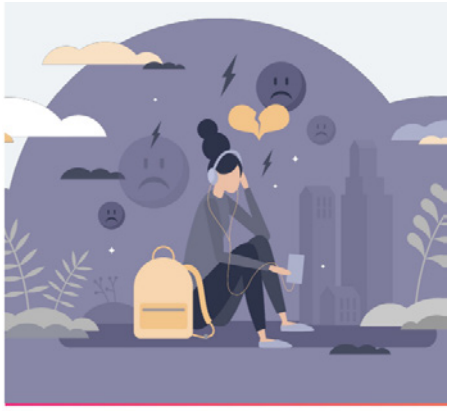
przeciwdziałania tym zagrożeniom oraz minimalizowania skutków zdarzeń niepożądanych. Wyniki tego badania pozwoliły ocenić, jak dotychczasowe stosowanie RODO wpłynęło na zmianę świadomości Polaków w kwestii ochrony dotyczących ich danych osobowych[392].

W rezultacie tej współpracy powstał trzyczęściowy raport poświęcony kluczowym wnioskom wynikającym z tego badania.

Wiedza na temat bezpieczeństwa danych osobowych w Polsce[393] to temat przewodni pierwszej części raportu, który opublikowano w maju 2022 roku[394]. Z badań wynikało, że **90% Polaków wie, jak zadbać o bezpieczeństwo swoich danych osobowych.** Najpewniej czują się ludzie młodzi. Pomimo przekonania o swojej wiedzy, to oni są jednak grupą, która najczęściej podejmuje działania stwarzające ryzyko dla ochrony danych osobowych – np. publikuje w sieci zdjęcia swoich dokumentów lub udostępnia osobom trzecim swoje loginy i hasła.

Wiedza na temat bezpieczeństwa danych osobowych w Polsce

Raport z badania
maj 2022 r.



Cyberzagrożenia –
czego boją się Polacy?

Raport z badania
czerwiec 2022 r.

Co trzeci badany uważa, że najbardziej musimy się obawiać wycieków z baz danych różnych instytucji lub firm. Jako najgroźniejszych wskazaliśmy jednak oszustów wyłudzających dane. Na pierwszym miejscu umieściło ich blisko 43% ankietowanych**.** Z kolei prawie 23% badanych obawiało się kradzieży swoich danych przez hakerów. Tylko ponad połowa (55%) z badanych wiedziała, co należy zrobić w przypadku wyłudzenia dotyczących ich danych osobowych. Największą wiedzę w tym zakresie posiadały młode osoby w wieku 18-34 lata (65%). Ponad 80% ankietowanych sprawę wyłudzenia danych osobowych zgłosiłoby na policję lub poinformowało o zdarzeniu swój bank, 68% zmieniłoby hasła do logowania, ponad 45% badanych zgłosiłoby sprawę do UODO, a blisko co czwarty sprawdziłby w biurze informacji gospodarczej, czy ktoś nie próbował już wykorzystać skradzionych danych.

Druga część raportu pt. „Cyberzagrożenia – czego boją się Polacy?", który opublikowano w czerwcu 2022 r.[395], dostarczyła wiele wniosków nt. poczucia zagrożenia Polaków o ich własne dane. Jak wynika z tego raportu, **co trzeci Polak boi się wycieków danych osobowych**. Równocześnie mniej niż połowa zadeklarowała, że wie, co należy w takiej sytuacji zrobić. Największe problemy

392 Badanie zrealizowały serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem UODO. Przeprowadzono je w marcu 2022 roku metodą CAWI na reprezentatywnej grupie 1007 respondentów przez IMAS International.
393 https://archiwum.uodo.gov.pl/pl/138/2389
394 Badanie jest kontynuacją badania zrealizowanego w 2021 roku.
395 https://archiwum.uodo.gov.pl/pl/138/2404

mieliby seniorzy, którzy nie mają wystarczającej wiedzy na temat tego, kto i w jaki sposób przetwarza ich dane osobowe. Niewiele ponad 30% ankietowanych wie, kto odpowiada za skutki wycieku danych, zaś co trzeci badany uważa, że odpowiedzialność spoczywa wyłącznie na ofierze.

Odnosząc się do wyników badań płynących z pierwszej i drugiej części raportu, UODO zorganizował webinarium, aby w gronie ekspertów skomentować zaprezentowane w raporcie wyniki. W większości eksperci potwierdzili ujawnione w raporcie postawy i zachowania Polaków, jednocześnie wskazując obszary, w których mogą one się utrwalać. Wiedza ta pozwoli w przyszłości na wyznaczenie kierunków potencjalnych działań, które mogłyby zminimalizować negatywne efekty tych zachowań.

Z trzeciej części raportu pt. „Zadania administratorów i IOD w kontekście bezpiecznego przetwarzania danych osobowych", opublikowanego we wrześniu 2022 roku[396] wynika, że **70% Polaków deklaruje, że nie wie, kto powinien zająć się konsekwencjami wycieku danych osobowych, a 10% z tych, którzy mają świadomość na ten temat uważa, że musi to zrobić sam poszkodowany**. Pozostali wskazują m.in. na policję, UODO oraz inspektorów ochrony danych i oczekują od nich szczegółowej informacji na temat zdarzenia oraz rekomendacji dalszych działań.

ınia administratorów i inspektorów ochrony danych w kontekście bezpiecznego przetwarzania danych osobowych"

Podsumowaniem tej części badania było webinarium[397] pt. „Zadania administratorów i inspektorów ochrony danych w kontekście bezpiecznego przetwarzania danych osobowych". Podczas tego wydarzenia eksperci odnieśli się do wyników przedstawionych wyżej badań, jednocześnie udzielając odpowiedzi na pytania: Czy Polacy wiedzą, jaką rolę w procesie przetwarzania danych odgrywa administrator? Czy orientują się, w jakich sprawach mogą zwracać się do inspektora ochrony danych? Czy rozumieją na czym polega ochrona danych osobowych w miejscu pracy?

Współpraca UODO z innymi instytucjami w 2022 roku nabrała nowego wymiaru ze względu na sytuację związaną z atakiem Federacji Rosyjskiej na Ukrainę. Jednym z wyzwań okazała się konieczność wsparcia przybywających do Polski Ukraińców w bezpiecznym przetwarzaniu ich danych osobowych w tak szczególnych okolicznościach. Urząd Ochrony Danych Osobowych wywiązał się z tego zadania udostępniając specjalny adres e-mail: forUkraine@uodo.gov.pl w celu umożliwienia im pozyskania informacji o prawach z zakresu ochrony danych osobowych i prywatności.

Ponadto Urząd Ochrony Danych Osobowych włączył się w obchody Światowego Dnia Konsumenta, który co roku przypada 15 marca[398]. Z myślą o konsumentach z Ukrainy UODO, wspólnie z UOKiK oraz innymi instytucjami, przygotował przydatne informacje, które

396 https://archiwum.uodo.gov.pl/pl/138/2449
397 https://archiwum.uodo.gov.pl/pl/138/2449
398 https://archiwum.uodo.gov.pl/pl/489/2318

ułatwią im zakupy, podróżowanie i korzystanie z usług w Polsce. Z okazji tego święta UODO przygotował także specjalny materiał poradnikowy, który przybliżył uchodźcom z Ukrainy prawa, jakie przysługują im na gruncie RODO. Wskazówki te zostały przygotowane w języku ukraińskim i angielskim, co przedstawia poniższa ilustracja:

W działalności informacyjno-edukacyjnej UODO na dużą skalę wykorzystywano webinaria, jako efektywną formę przekazu w komunikacji z ekspertami oraz młodzieżą. Uwagę mediów skupiały webinaria tematyczne, np. te, zrealizowane na potrzeby programu edukacyjnego „Twoje dane – Twoja sprawa", poświęcone zabezpieczeniom technicznym przetwarzanych danych osobowych[399] czy kodeksom postępowania zgodnym z RODO. Podczas webinarium „Stan prac nad kodeksami postępowania w Polsce"[400] eksperci przedstawili korzyści z przystąpienia do kodeksów postępowania oraz omówili aspekt monitorowania ich przestrzegania. Spotkanie to odbyło się tuż po zatwierdzeniu przez Prezesa UODO pierwszego kodeksu postępowania, o którym mowa w art. 40 RODO - „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych". Kodeks ten przygotowała Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie, po udzieleniu akredytacji podmiotu monitorującego stosowanie kodeksu.

W analizowanym roku sprawozdawczym przedstawiciel UODO uczestniczył w badaniu nad wykorzystaniem bezzałogowych statków powietrznych (BSP) w pracy Policji, m.in. w zakresie zapewnienia skutecznej ochrony danych osobowych. Badanie to realizowane było w ramach międzynarodowego projektu finansowanego przez Narodowe Centrum Nauki w zakresie prawno-porównawczej analizy regulacji określających warunki wykonywania lotów BSP w Polsce, Niemczech, Wielkiej Brytanii i Hiszpanii. Wymienione kraje wyróżniają się pod względem poziomu regulacji w tym zakresie na tle innych krajów

399 https://archiwum.uodo.gov.pl/pl/138/2451
400 https://archiwum.uodo.gov.pl/pl/138/2519

Unii Europejskiej. Celem projektu była identyfikacja czynników umożliwiających skuteczne i efektywne wykorzystanie BSP w pracy Policji dla zapewnienia bezpieczeństwa obywateli, z uwzględnieniem zasad ochrony danych osobowych i prawa do prywatności.

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

1. Współpraca w ramach EROD

Jednym z ustawowych zadań organu właściwego w sprawach ochrony danych osobowych jest uczestnictwo w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych. Do zadań Prezesa UODO należy współpraca z organami nadzorczymi innych państw członkowskich UE w szczególności w ramach działań Europejskiej Rady Ochrony Danych RODO, ustanowionej przepisami RODO, do której należy Prezes UODO.

EROD jest organem UE posiadającym osobowość prawną, który wykonuje swoje zadania i korzysta z uprawnień z zachowaniem pełnej niezależności. Zgodnie z tą zasadą zapisaną w art. 69 RODO, w toku wypełniania swoich zadań lub wykonywania uprawnień Rada działa w sposób bezstronny i całkowicie niezależny. Rada ma siedzibę w Brukseli, która jest głównym miejscem prowadzenia jej działalności.

EROD działa na rzecz spójnego stosowania zasad ochrony danych w całej Unii Europejskiej, a także promuje współpracę pomiędzy organami nadzorczymi do spraw ochrony danych z UE oraz Europejskiego Obszaru Gospodarczego (EOG). EROD zapewnia spójne stosowanie RODO, a także realizację zadań wymienionych w dyrektywie 2016/680 oraz w innych właściwych instrumentach prawodawczych zgodnie z prawem UE.

W skład EROD wchodzą przewodniczący jednego organu nadzorczego każdego państwa członkowskiego i państw EOG-EFTA lub wspólny przedstawiciel organów nadzorczych, zgodnie z treścią art. 68 ust. 4 RODO, a także Europejski Inspektor Ochrony Danych („EIOD") lub ich przedstawiciele. W odniesieniu do działań Rady związanych z RODO, organy nadzorcze państw EOG-EFTA mają takie same prawa i obowiązki jak organy nadzorcze państw członkowskich UE, z wyjątkiem prawa do głosowania i do kandydowania w wyborach na przewodniczącego lub wiceprzewodniczących, o ile nie określono inaczej w regulaminie wewnętrznym EROD. Organy te mają prawo wyrażenia swojego stanowiska na temat wszystkich omawianych lub poddanych pod głosowanie kwestii.

Komisja Europejska ma prawo uczestniczyć w pracach Rady bez prawa głosu i wyznacza swojego przedstawiciela w Radzie. Urząd Nadzoru EFTA ma prawo uczestniczyć w działaniach Rady dotyczących RODO bez prawa do głosowania oraz wyznacza swojego przedstawiciela.

Jeżeli w państwie członkowskim za monitorowanie stosowania przepisów RODO i dyrektywy 2016/680 odpowiada więcej niż jeden organ nadzorczy, to zgodnie z przepisami prawa krajowego wyznaczony zostaje wspólny przedstawiciel. To samo dotyczy organów nadzorczych państw EOG-EFTA odpowiedzialnych za monitorowanie stosowania przepisów zgodnie z RODO.

EROD działa na podstawie regulaminu wewnętrznego, który określa najważniejsze zasady działania Europejskiej Rady Ochrony Danych[401]. Zasady te dotyczą organizacji Europejskiej Rady Ochrony Danych, wspólnej pracy jej członków, wyboru przewodniczącego i wiceprzewodniczących i metod pracy.

Protokół ustaleń jest porozumieniem, które określa warunki współpracy pomiędzy EROD i EIOD. Ma on również zastosowanie do personelu sekretariatu, którego obsługę zapewnia EIOD w celu wsparcia Europejskiej Rady Ochrony Danych[402].

2. Podgrupy ekspertów EROD

Zgodnie z art. 25 regulaminu wewnętrznego EROD, działa ona poprzez wewnętrzne podgrupy ekspertów, w skład których wchodzą przedstawiciele organów nadzorczych, EIOD i Komisji Europejskiej. Podgrupy ekspertów wspierają EROD w wykonywaniu jej zadań i dążą do osiągnięcia porozumienia w sprawie każdego wniosku przedłożonego Radzie. EROD, działając przez podgrupy ekspertów, realizuje zadania zgodnie z dwuletnim programem prac. Wstępny plan roczny powinien być przygotowany na początku każdego roku przez koordynatora, ze wskazaniem liczby posiedzeń oraz, w miarę możliwości, harmonogramu i zagadnień, które zostaną omówione. Na podstawie art. 70 ust. 1 lit. u) RODO, EROD powołuje również dedykowane grupy zadaniowe, które służą koordynacji działań organów nadzorczych.

W ramach prac podgrup i grup zadaniowych przedstawiciele polskiego organu nadzorczego, wraz z reprezentantami pozostałych organów, opracowują dokumenty EROD, w tym opinie, wytyczne, zalecenia i najlepsze praktyki w celu promowania wspólnego zrozumienia RODO i dyrektywy 2016/680, a także biorą udział w doradzaniu Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych w UE. Dokumenty te są następnie przedmiotem dyskusji i zostają przyjmowane na comiesięcznych posiedzeniach plenarnych EROD, podczas których polski organ nadzorczy reprezentowany jest przez Prezesa UODO lub jego zastępców.

Poszczególne podgrupy ekspertów koncentrują się na konkretnych obszarach ochrony danych i wspierają EROD w wykonywaniu jej zadań. Poniżej zamieszczony jest wykaz podgrup eksperckich i opis zakresów ich zadań. W 2022 r. pracownicy UODO czynnie reprezentowali polski organ nadzorczy, uczestnicząc w pracach wszystkich podgrup

401 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/rules-procedure_pl
402 Protokół ustaleń dostępny jest na stronie EROD, pod adresem:
https://edpb.europa.eu/our-work-tools/our-documents/memorandum-understanding/memorandum-understanding_pl

ekspertów EROD.

1) Podgrupa Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Borders, Travel and Law Enforcement Expert Subgroup)

Podgrupa właściwa w sprawach dotyczących dyrektywy 2016/680, transgranicznych wniosków o udostępnienie elektronicznego materiału dowodowego, decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony danych w państwach trzecich, dostępu do danych przez organy ścigania i krajowych organów wywiadowczych w państwach trzecich (np. działania podjęte w związku z wyrokiem TSUE w sprawie Schrems II), kontroli nad danymi o przelocie pasażera (PNR) i kontroli granicznych.

2) Podgrupa Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health Expert Subgroup)

Podgrupa właściwa do spraw m.in. kodeksów postępowania, certyfikacji i akredytacji, oceny skutków dla ochrony danych, uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, zgodności z prawem publicznym, administracji elektronicznej, zdrowia i przetwarzania danych osobowych do celów badań naukowych, aktu o zarządzaniu danymi, aktu ws. danych;.

3) Podgrupa Ekspertów ds. Współpracy (Cooperation Expert Subgroup)

Podgrupa właściwa do spraw m.in. ogólnych aspektów mechanizmu współpracy i spójności w ramach RODO; kwestii proceduralnych dotyczących art. 56 RODO i rozdziału VII (sekcja 1 i 2) RODO; przypadków współpracy, w których administrator nie ma jednostki organizacyjnej w UE; międzynarodowej wzajemnej pomocy i innych narzędzi współpracy w celu egzekwowania RODO poza UE (art. 50 RODO) (we współpracy z podgrupą ekspertów ds. Międzynarodowego Przekazywania Danych).

4) Podgrupa Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup)

Podgrupa zajmuje się analizą zapotrzebowania na dodatkowe wyjaśnienia lub wytyczne w oparciu o praktyczne doświadczenia związane ze stosowaniem rozdziałów VI, VII i VIII RODO, oceną konieczności aktualizowania narzędzi podgrupy Cooperation, monitorowania postępowań, wytycznych dotyczących praktycznego stosowania rozdziału VII i VIII RODO, wytycznymi dotyczącymi praktycznego stosowania rozdziału VII i VIII RODO; wiążącymi decyzjami EROD, opracowywaniem strategii EROD w zakresie egzekwowania prawa.

5) Podgrupa Ekspertów ds. Finansowych (Financial Matters Expert Subgroup)

Podgrupa jest właściwa do spraw m.in. stosowania zasad ochrony danych w sektorze finansowym, np. opodatkowaniem, zwalczaniem przestępczości finansowej, walutą cyfrową, usługami płatniczymi, kredytami, ubezpieczeniami, tożsamością cyfrową itp.; w indywidualnych przypadkach dostarczaniem informacji międzynarodowym lub europejskim instytucjom, organom lub organizacjom finansowym (np. EBC, ESMA, EBA,

EIOPA, FATF itp.)

6) Podgrupa Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup)

Podgrupa właściwa do spraw m.in. wytycznych dotyczących rozdziału V RODO, w szczególności przeglądu decyzji Komisji Europejskiej stwierdzających odpowiedni stopień ochrony danych w państwach trzecich, przeglądu uzgodnień administracyjnych między władzami i organami publicznymi, kodeksów postępowania i certyfikacji, jako narzędzi do przekazywania danych, wiążących reguł korporacyjnych i klauzul umownych dla międzynarodowego przekazywania danych.

7) Podgrupa Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup)

Podgrupa opracowuje i testuje narzędzia informatyczne wykorzystywane przez EROD, z naciskiem na kwestie praktyczne, tj. zbieranie informacji zwrotnych na temat systemów informatycznych od użytkowników, w tym przede wszystkim IMI – narzędzia wymiany informacji na rynku wewnętrznym, a także innych potrzeb IT, w tym systemów tele- i wideokonferencyjnych.

8) Podgrupa Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup)

Podgrupa opracowująca wytyczne dotyczące podstawowych pojęć i zasad RODO, w tym rozdziału I (np. zakres, definicje pojęć takich jak wiodący organ nadzorczy i przetwarzanie na dużą skalę), II (główne zasady), III (np. prawa osób fizycznych, przejrzystość), IV (np. inspektor ochrony danych – we współpracy z Podgrupą ekspertów ds. Zgodności, e-Administracji i Zdrowia, Podgrupą ekspertów ds. Egzekwowania Prawa i Podgrupą ekspertów ds. Technologii) oraz IX RODO.

9) Podgrupa Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup)

Podgrupa właściwa do analizy usług mediów społecznościowych, rozumianych jako platformy internetowe, które koncentrują się na umożliwieniu rozwoju sieci i społeczności użytkowników, między którymi udostępniane są informacje i treści, przy czym dodatkowe funkcje zapewniane przez usługi mediów społecznościowych obejmują targetowanie, personalizację, integrację aplikacji, wtyczki społecznościowe, uwierzytelnianie użytkowników, analitykę i publikowanie. Do zadań tej podgrupy należą także: analiza istniejących i powstających funkcji oferowanych przez media społecznościowe, w tym leżących u ich podstaw czynności przetwarzania danych i związanych z nimi zagrożeń dla praw i wolności osób fizycznych; opracowywanie wytycznych, zaleceń i najlepszych praktyk w odniesieniu do oferowania i korzystania z funkcji mediów społecznościowych, w szczególności do celów gospodarczych i politycznych, oraz akt o usługach cyfrowych.

10) **Podgrupa Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup)**

Podgrupa zajmuje się kwestiami strategicznymi, które mają wpływ na całą EROD (w tym omawianiem planów prac podgrup ekspertów) i wyjaśnianiem kwestii, które nie zostały jednoznacznie rozstrzygnięte w ramach podgrup ekspertów. Podgrupa ta prowadzi również prace nad wkładem do oceny RODO;

11) **Podgrupa Ekspertów ds. Technologii (Technology Expert Subgroup),**

Podgrupa, która jest właściwa do spraw związanych z technologiami, innowacjami, bezpieczeństwem informacji, poufnością komunikacji, łącznością elektroniczną i prywatnością, szyfrowaniem, oceną skutków dla ochrony danych, zgłaszaniem naruszeń ochrony danych, nowymi technologiami, innowacjami i innymi wyzwaniami związanymi z prywatnością: refleksją nad zagrożeniami dla ochrony danych i możliwościami związanymi z przyszłym rozwojem technologicznym, a także aktem w sprawie sztucznej inteligencji.

3. Grupy zadaniowe EROD

W 2022 r. pracownicy UODO reprezentowali polski organ nadzorczy także w grupach zadaniowych i sieciach EROD, o których mowa poniżej:

1) **Grupie zadaniowej ds. bannerów cookie,** której celem jest koordynowanie działań organów nadzorczych EOG w odpowiedzi na skargi dotyczące bannerów cookie złożonych przez NOYB;

2) **Grupie zadaniowej ds. administracyjnych kar pieniężnych,** której zadaniem jest opracowanie wytycznych w sprawie harmonizacji obliczania przez krajowe organy nadzorcze administracyjnych kar pieniężnych;

3) **Grupie zadaniowej ds. 101 skarg,** która zajmuje się rozpatrywaniem skarg wniesionych przez organizację NOYB, reprezentującą skarżących. Skargi dotyczą spółek w 30 państwach członkowskich UE i EOG, w związku z korzystaniem przez administratorów z narzędzi, za pomocą których dane przekazywane są do państw trzecich w sposób niezgodny z wyrokiem TSUE w sprawie C-311/18 (Schrems II), który rozstrzygnął, kiedy przekazywanie danych do państw trzecich jest legalne.

4. Sieć Inspektorów Ochrony Danych

Inspektor Ochrony Danych UODO jest członkiem Sieci Inspektorów Ochrony Danych (DPO Network). Sieć IOD została powołana podczas posiedzenia plenarnego EROD w lipcu 2019 roku w celu umożliwienia wymiany najlepszych praktyk pomiędzy inspektorami ochrony danych organów nadzorczych i stworzenia bardziej zharmonizowanego podejścia między nimi. Opracowywane w jej ramach zalecenia są rekomendacjami nieformalnymi, wewnętrznymi i dotyczą wyłącznie organów nadzorczych.

Sieć Inspektorów Ochrony Danych ma charakter nieformalnej sieci, niezależnej w udzielaniu opinii i porad. W jej skład wchodzą wszyscy inspektorzy ochrony danych organów nadzorczych, inspektor ochrony danych EROD oraz inspektor ochrony danych EIOD. Działania niezależnej Sieci IOD pozwalają na lepszą koordynację między EROD, organami i EIOD w zakresie korzystania z narzędzi związanych z ich wspólnymi działaniami (np. IMI).

5. Nadzór nad wielkoskalowymi systemami

Istotnym obszarem działalności Prezesa UODO w 2022 r. pozostawała także współpraca międzynarodowa w ramach art. 62 rozporządzenia 2018/1725, która przewiduje zharmonizowany model skoordynowanego nadzoru, mający zastosowanie w przypadku, gdy odpowiednie prawo Unii Europejskiej odnosi się do tego artykułu.

Zgodnie z tym przepisem EIOD i krajowe organy nadzorcze czynnie współpracują w ramach swoich obowiązków, aby zapewnić skuteczny nadzór nad wielkoskalowymi systemami informatycznymi oraz organami i jednostkami organizacyjnymi Unii. Skoordynowane działania obejmują m.in. wspólne kontrole i dochodzenia oraz prace nad wspólną metodologią.

W analizowanym 2022 r. przedstawiciele UODO uczestniczyli w posiedzeniach wymienionych poniżej wyspecjalizowanych grup:

- Grupy ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen (SIS II), z którego korzystają organy z całej UE, by wprowadzać do niego lub odnajdywać w nim wpisy o poszukiwanych lub zaginionych osobach i przedmiotach;
- Grupy ds. Koordynacji Nadzoru nad Systemem Informacji Celnej (CIS), który pomaga w zapobieganiu naruszeniom przepisów prawa celnego i rolnego, ich dochodzeniu i ściganiu;
- Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS), który jest bazą danych mającą ułatwić procedurę rozpatrywania wniosków o wydanie wiz krótkoterminowych;
- Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac, który zawiera odciski palców wszystkich osób ubiegających się o azyl zarejestrowanych w państwach członkowskich UE i krajach współpracujących.

Przedstawiciele UODO uczestniczyli także w skoordynowanych działaniach nadzorczych nad systemem informacyjnym rynku wewnętrznego (IMI), Eurojust i Europol w ramach Komitetu Skoordynowanego Nadzoru (CSC)[403]. W przyszłości Komitet obejmie nadzór również nad unijnymi systemami informatycznymi, organami, biurami i agencjami w dziedzinie granic, azylu i migracji (SIS, EES, ETIAS i VIS), współpracy policyjnej i sądowej

403 Więcej informacji o Komitecie dostępnych jest na stronie EIOD: https://edpb.europa.eu/csc/about-csc/who-we-are-coordinated-supervision-committee_pl

(SIS, ECRIS-TCN) oraz Prüm nowej generacji.

Wielkoskalowe systemy i sieci informacyjne UE, takie jak IMI i Eurojust, które łączą organy unijne i krajowe, mają charakter hybrydowy: zarówno krajowy – unijny, jak i transeuropejski. Dane mogą być przekazywane i przechowywane w wielu miejscach oraz przetwarzane przez różne podmioty. Osoby, których dane dotyczą, mogą nie posiadać informacji, czy ich dane są przetwarzane na szczeblu unijnym lub krajowym. W związku z tym mogą nie wiedzieć, do kogo powinni kierować swoje wnioski o realizację uprawnień wynikających z art. 15 RODO. Dlatego w 2022 r. jednym z głównych zadań Komitetu Skoordynowanego Nadzoru było zbadanie problemów związanych ze sprawowaniem niezależnego nadzoru lub wykonywaniem praw osób, których dane dotyczą oraz proponowanie rozwiązań tych problemów.

Kolejnym zadaniem Komitetu było badanie trudności w interpretacji lub stosowaniu rozporządzenia 2018/1725 i innych przepisów prawa UE w odniesieniu do wielkoskalowych systemów i organów informacyjnych. Stosowanie niektórych z tych systemów musi być pogodzone ze stosowaniem prawa krajowego, które może mieć zastosowanie, np. do przetwarzania danych z zakresu ochrony porządku publicznego.

Innym kluczowym zadaniem Komitetu było umożliwienie organom nadzorczym wymiany istotnych informacji oraz wzajemnej pomocy w przeprowadzaniu audytów i inspekcji. Komitet rozpoczął także przygotowania do sprawowania skoordynowanego nadzoru nad Europolem, który w dniu 28 czerwca 2022 r. został objęty zakresem jego kompetencji. Komitet zaangażował się w przygotowanie tego przejścia wraz z Radą Współpracy Europolu.

Ponadto przedstawiciel UODO uczestniczył w charakterze eksperta w zespołach prowadzących kontrole w zakresie oceny i monitorowania stosowania dorobku Schengen w obszarze ochrony danych osobowych, zgodnie z rozporządzeniem 1053/2013. W ocenach tych dokonuje się ewaluacji, w jaki sposób państwa członkowskie wdrażają i stosują dorobek Schengen, w szczególności w odniesieniu do SIS i VIS w kontekście wymogów ochrony danych. Badają one również rolę organów ochrony danych w odniesieniu do nadzoru nad organami zarządzającymi i korzystającymi z SIS i VIS. Ocena jest gwarancją tego, że państwa członkowskie stosują przepisy Schengen skutecznie i zgodnie z podstawowymi zasadami i normami. Za wdrożenie mechanizmu oceny i monitorowania odpowiadają wspólnie państwa członkowskie i Komisja przy wsparciu organów i jednostek organizacyjnych Unii uczestniczących we wdrażaniu dorobku Schengen.

6. Prace EROD w 2022 r.

W 2022 roku, tak jak w roku poprzednim, EROD funkcjonowała w oparciu o przyjęty w 2021 roku *Program prac na lata 2021/2022*[404]. Program ten opiera się na czterech filarach:

404 https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf

- Filar I: Wspieranie harmonizacji i ułatwianie zgodności.
- Filar II: Wspieranie skutecznego egzekwowania i efektywnej współpracy między krajowymi organami nadzorczymi.
- Filar III: Podejście do nowych technologii oparte na prawach podstawowych.
- Filar IV: Wymiar globalny.

W 2022 roku Sekretariat EROD zorganizował 347 posiedzeń EROD, w tym 15 posiedzeń plenarnych, 160 posiedzeń podgrup ekspertów lub grup zadaniowych oraz 172 posiedzenia zespołów redakcyjnych. W 2022 r. EROD po raz pierwszy zwołała posiedzenia hybrydowe. Spośród 347 posiedzeń 34 miały charakter hybrydowy, podczas gdy 308 odbyło się zdalnie, a 5 osobiście.

Działając zgodnie z art. 24 Regulaminu wewnętrznego, EROD podejmowała niektóre decyzje i przyjmowała wybrane, niewymagające dodatkowej dyskusji, dokumenty w trybie procedury pisemnej.

Porządki obrad i protokoły z sesji plenarnych są publikowane na stronie internetowej EROD[405]. Podczas tych posiedzeń EROD przyjmuje wytyczne, opinie i inne dokumenty, będące ogólnymi wskazówkami w zakresie interpretacji RODO i tzw. dyrektywy policyjnej, a także inne dokumenty w ramach konsultacji prawodawczych, skierowane do Komisji Europejskiej, instytucji UE lub organów krajowych, w kwestiach związanych z RODO.

Zgodnie z ustalonym planem oraz w wyniku potrzeby działania *ad hoc*, w 2022 r. EROD przyjęła m.in. niżej wymienione dokumenty[406].

6.1. Wytyczne

1) Wytyczne 1/2022 w sprawie praw osób, których dane dotyczą – prawo dostępu;
2) Wytyczne 2/2022 w sprawie stosowania art. 60 RODO;
3) Wytyczne 3/2022 w sprawie tzw. zwodniczych wzorców w interfejsach platform społecznościowych;
4) Wytyczne 4/2022 w sprawie obliczania administracyjnych kar pieniężnych na mocy RODO;
5) Wytyczne 5/2022 w sprawie stosowania technologii rozpoznawania twarzy w dziedzinie egzekwowania prawa;
6) Wytyczne 6/2022 w sprawie praktycznego wdrażania polubownego rozwiązywania spraw;
7) Wytyczne 7/2022 w sprawie certyfikacji jako narzędzia do przekazywania danych;

405 https://edpb.europa.eu/our-work-tools/agenda_en
https://edpb.europa.eu/our-work-tools/our-documents/publication-type/minutes_pl
406 Wszystkie dokumenty EROD o charakterze publicznym znajdują się na jej stronie:
https://edpb.europa.eu/our-work-tools_pl

8) Wytyczne 8/2022 w sprawie identyfikacji organu wiodącego dla administratora i podmiotu przetwarzającego;

9) Wytyczne 9/2022 w sprawie zgłaszania naruszeń ochrony danych zgodne z RODO.

6.2. Konsultacje prawodawcze i dokumenty skierowane do instytucji UE lub organów krajowych

1) Wspólna Opinia EROD i EIOD 1/2022 w sprawie wniosku Rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2021/953 w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID) w celu ułatwienia swobodnego przemieszczania się w czasie pandemii COVID-19;

2) Wspólna Opinia EROD i EIOD 2/2022 dotycząca wniosku Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych);

3) Wspólna Opinia EROD i EIOD 03/2022 w sprawie Wniosku Komisji Europejskiej w sprawie Europejskiej Przestrzeni Danych Dotyczących Zdrowia;

4) Wspólna Opinia EROD i EIOD 04/2022 w sprawie Wniosku Komisji Europejskiej dotyczącego rozporządzenia w sprawie zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczania;

5) Oświadczenie 01/2022 w sprawie ogłoszenia porozumienia zasadniczego w sprawie nowych Transatlantyckich Ram Ochrony Prywatności Danych;

6) Oświadczenie 04/2022 w sprawie wariantów konstrukcji cyfrowego euro z perspektywy prywatności i ochrony danych;

7) Odpowiedź EROD na ukierunkowane konsultacje Komisji Europejskiej w sprawie cyfrowego euro;

8) Oświadczenie w sprawie wpływu wyroku TSUE C-817/19 na korzystanie z danych PNR w państwach członkowskich.

6.3. Inne wskazówki i oświadczenia

Oświadczenie 02/2022 w sprawie przekazywania danych osobowych do Federacji Rosyjskiej.

6.4. Opinie dotyczące spójności[407]

1) Opinie w sprawie projektów decyzji dotyczących wiążących reguł korporacyjnych

Organy nadzorcze mogą zatwierdzać wiążące reguły korporacyjne w rozumieniu art. 47 RODO. Wiążące reguły korporacyjne to polityki ochrony danych wdrożone i przestrzegane w ramach grupy przedsiębiorstw mających siedzibę w EOG w odniesieniu do przekazywania danych osobowych poza EOG w ramach tej samej grupy. W 2022 r. kilka organów nadzorczych przedłożyło EROD swoje projekty decyzji dotyczących wiążących reguł korporacyjnych administratora lub podmiotu przetwarzającego różnych przedsiębiorstw, zwracając się o wydanie opinii na podstawie art. 64 ust. 1 lit. f). W 2022 r. EROD wydała dwadzieścia trzy opinie w sprawie wiążących reguł korporacyjnych.

2) Opinie w sprawie projektu wymogów dotyczących akredytacji podmiotów certyfikujących

Trzy organy nadzorcze, w tym Urząd Ochrony Danych Osobowych, przedłożyły swoje projekty decyzji w sprawie wymogów akredytacji dla jednostek certyfikujących na podstawie art. 43 ust. 1 lit. b) RODO do EROD z wnioskiem o wydanie opinii na podstawie art. 64 ust. 1 lit. c) RODO. Wymogi te umożliwiają akredytację jednostek certyfikujących odpowiedzialnych za wydawanie i odnawianie certyfikacji zgodnie z art. 42 RODO. Opinie te mają na celu ustanowienie spójnego i zharmonizowanego podejścia w odniesieniu do wymogów, które organy nadzorcze i krajowe jednostki akredytujące stosują podczas akredytacji jednostek certyfikujących na mocy RODO. W tym celu EROD przedstawiła odpowiednim organom zalecenia dotyczące zmian, które należy wprowadzić do projektów opinii. Następnie organy nadzorcze zmieniły swoje projekty zgodnie z art. 64 ust. 7 RODO, uwzględniając w jak największym stopniu opinie EROD. Opinia 11/2022, przyjęta 4 lipca 2022 r., w sprawie projektu decyzji właściwego organu nadzorczego Polski w sprawie zatwierdzenia wymogów dotyczących akredytacji podmiotu certyfikującego zgodnie z art. 43 ust. 3 (RODO) dostępna jest na stronie EROD[408].

3) Opinie w sprawie kryteriów certyfikacji

Jeżeli organ nadzorczy zamierza zatwierdzić certyfikację zgodnie z art. 42 ust. 5 RODO, rolą EROD jest zapewnienie spójnego stosowania RODO poprzez mechanizm spójności, o którym mowa w art. 63, 64 i 65 RODO. W tych ramach, zgodnie z art. 64 ust. 1 lit. c RODO, EROD jest zobowiązana do wydania opinii na temat projektu decyzji organu nadzorczego zatwierdzającej kryteria certyfikacji. W 2022 r. EROD wydała trzy opinie w sprawie kryteriów certyfikacji, mające na celu zapewnienie spójnego stosowania RODO, w tym przez organy nadzorcze, administratorów i podmioty przetwarzające.

4) Opinie w sprawie zatwierdzenia przez organy nadzorcze wymogów akredytacji dla podmiotów monitorujących kodeksy postępowania

407 Opinie dotyczące spójności dostępne są na stronie EROD pod adresem: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_pl

408 Opinia dostępna pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112022-draft-decision-competent_pl

Celem opinii w sprawie zatwierdzenia przez organy nadzorcze wymogów akredytacji dla podmiotów monitorujących kodeksy postępowania jest zapewnienie spójności i prawidłowego stosowania wymogów wśród organów nadzorczych. W tym celu EROD przedstawiła organom szereg zaleceń dotyczących zmian, jakie należy wprowadzić do projektu wymogów akredytacji. Na tej podstawie organy nadzorcze zmieniły swoje projekty zgodnie z art. 64 ust. 7 RODO, uwzględniając w jak największym stopniu opinie EROD.

W 2022 r. EROD wydała trzy opinie w sprawie projektów wymogów akredytacji dla podmiotów monitorujących kodeksy postępowania, o które zwróciły się organy nadzorcze, zgodnie z art. 64 ust. 1 lit. c) RODO.

6.5. Wiążące decyzje

EROD jest uprawniona do wydawania wiążących decyzji na mocy art. 65 RODO w celu zagwarantowania spójnego stosowania RODO przez organy nadzorcze. W 2022 r. EROD wydała 5 wiążących decyzji dotyczących kwestii takich jak: prawo dostępu do danych, prawo do sprzeciwu wobec marketingu bezpośredniego, czy też podstawy prawne przetwarzania danych osobowych.

1) Decyzja 01/2022 w sprawie sporu dotyczącego projektu decyzji francuskiego organu nadzorczego w sprawie Accor SA na podstawie art. 65 ust. 1 lit. a RODO;
2) Wiążąca decyzja 2/2022 w sprawie sporu dotyczącego projektu decyzji irlandzkiego organu nadzorczego w sprawie Meta Platforms Ireland Limited (Instagram) na podstawie art. 65 ust. 1 lit. a RODO;
3) Wiążąca decyzja 3/2022 w sprawie sporu wszczętego przez irlandzki organ nadzorczy dotyczącego Meta Platforms Ireland Limited i jej serwisu Facebook (art. 65 RODO);
4) Wiążąca decyzja 4/2022 w sprawie sporu wszczętego przez irlandzki organ nadzorczy dotyczącego Meta Platforms Ireland Limited i jej serwisu Instagram (art. 65 RODO);
5) Wiążąca decyzja 5/2022 w sprawie sporu wszczętego przez irlandzki organ nadzorczy dotyczącego WhatsApp Ireland Limited (art. 65 RODO).

6.6. Współpraca organów i egzekwowanie prawa

1) Oświadczenie w sprawie współpracy e zakresie egzekwowania prawa

W dniu 28 kwietnia 2022 r. EROD przyjęła oświadczenie w sprawie współpracy w zakresie egzekwowania prawa[409] w następstwie spotkania wysokiego szczebla w Wiedniu, podczas którego członkowie EROD zgodzili się zacieśnić współpracę w sprawach strategicznych i zdywersyfikować zakres stosowanych metod współpracy.

409 Oświadczenie dostępne jest pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-enforcement-cooperation_pl

W oświadczeniu podkreślono zobowiązanie organów nadzorczych do ścisłej współpracy transgranicznej. Organy uzgodniły, że regularnie będą wspólnie identyfikować sprawy transgraniczne o strategicznym znaczeniu, przy wsparciu EROD. Ponadto organy nadzorcze zobowiązały się do dalszej wymiany informacji na temat krajowych strategii egzekwowania prawa w celu osiągnięcia porozumienia w sprawie rocznych priorytetów na szczeblu EROD. Oświadczenie potwierdziło również rolę EROD w zapewnianiu spójnej interpretacji RODO.

Co istotne, w celu zmaksymalizowania pozytywnego wpływu współpracy w zakresie RODO, EROD postanowiła określić listę aspektów proceduralnych, które można dalej zharmonizować w UE[410]. Lista dotyczy, między innymi, statusu i praw stron postępowań administracyjnych; terminów proceduralnych; wymogów dopuszczalności lub odrzucenia skarg, uprawnień do prowadzenia postępowań wyjaśniających przez organy ochrony danych; czy też praktycznego wdrożenia procedury współpracy. Lista została przedłożona Komisji Europejskiej do rozważenia.

2) Dokument EROD dotyczący wyboru spraw o znaczeniu strategicznym

Po spotkaniu wysokiego szczebla w Wiedniu w kwietniu 2022 r., EROD przyjęła także dokument, w którym ustanowiono kryteria określania, czy dana sprawa ma znaczenie strategiczne[411].

EROD uznaje sprawy za mające strategiczne znaczenie, jeżeli istnieje wysokie ryzyko naruszenia praw i wolności osób fizycznych w kilku państwach członkowskich, jeżeli dotyczy strukturalnego lub powtarzającego się problemu w kilku państwach członkowskich, jest związana z krzyżowaniem się ochrony danych z innymi dziedzinami prawa lub dotyczy dużej liczby osób, których dane dotyczą w kilku państwach członkowskich. Sprawy, które obejmują dużą liczbę skarg w kilku państwach członkowskich, podstawową kwestię wchodzącą w zakres strategii EROD lub sprawy, w przypadku których RODO sugeruje, że mogą stanowić wysokie ryzyko, również kwalifikują się jako sprawy o znaczeniu strategicznym.

3) Wsparcie puli ekspertów (Support Pool of Experts)

W ramach strategii na lata 2021-2023 EROD w 2020 r. ustanowiła pulę wsparcia ekspertów (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. Ponadto SPE ma za zadanie zaspokajanie ewentualnych potrzeb operacyjnych organów. W wyniku naboru na ekspertów zewnętrznych, przeprowadzonego

410 Dokument dostępny pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_pl

411 https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-selection-cases-strategic-importance_pl

przez Sekretariat EROD w ramach SPE, pod na koniec 2022 r. w skład SPE wchodziło 409 ekspertów zewnętrznych.

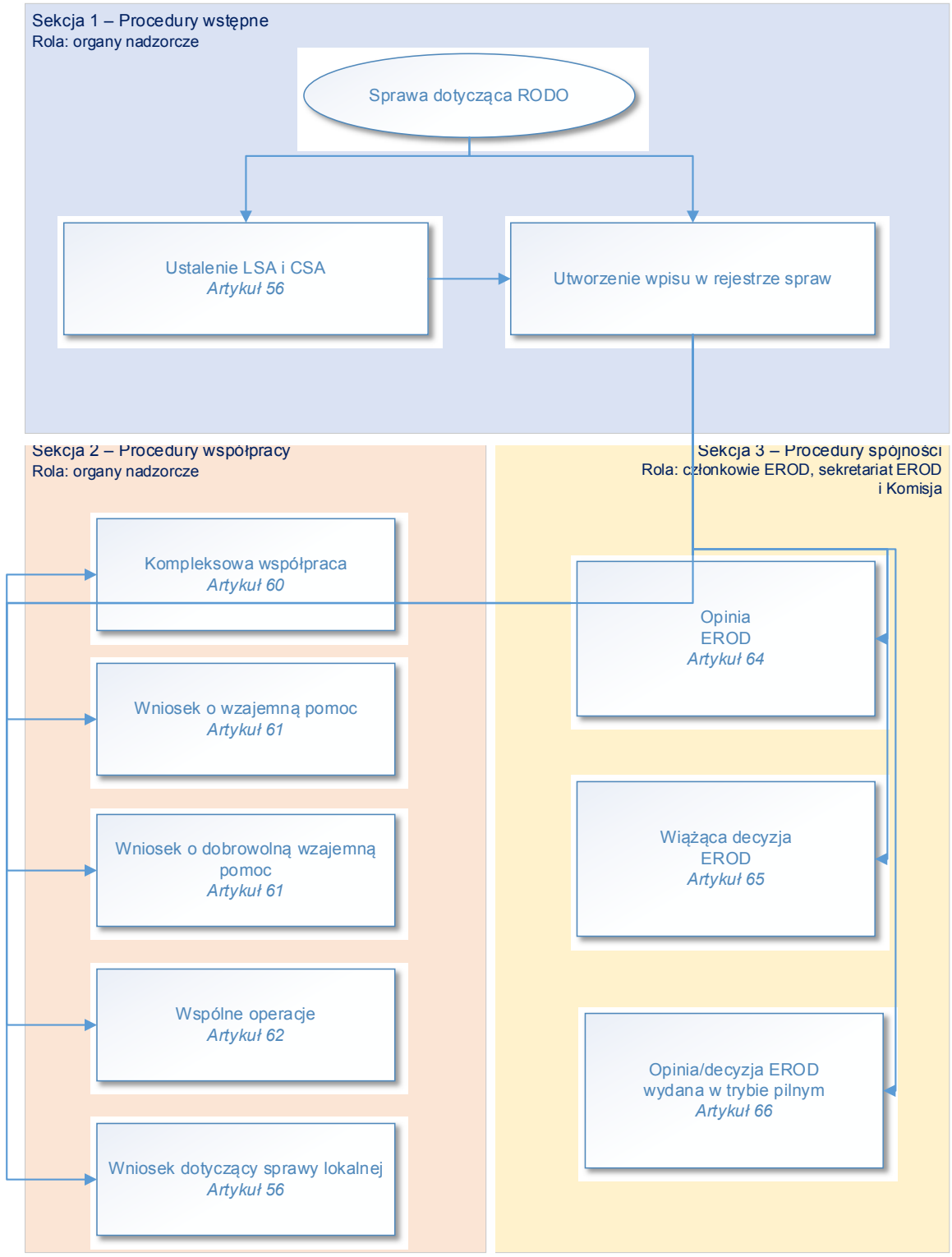
7. Współpraca w ramach IMI

Od 25 maja 2018 r. organy nadzorcze korzystają z systemu wymiany informacji na rynku wewnętrznym[412], 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[413].

System IMI został opracowany przez Dyrekcję Generalną Komisji Europejskiej ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MŚP (DG GROW). Został on dostosowany do potrzeb RODO w ścisłej współpracy z Sekretariatem EROD i organami nadzorczymi. W celu zapewnienia dostosowania systemu do zmieniających się potrzeb organów nadzorczych, w ramach EROD działa podgrupa ekspertów IT Users, która omawia i zatwierdza wszelkie niezbędne zmiany.

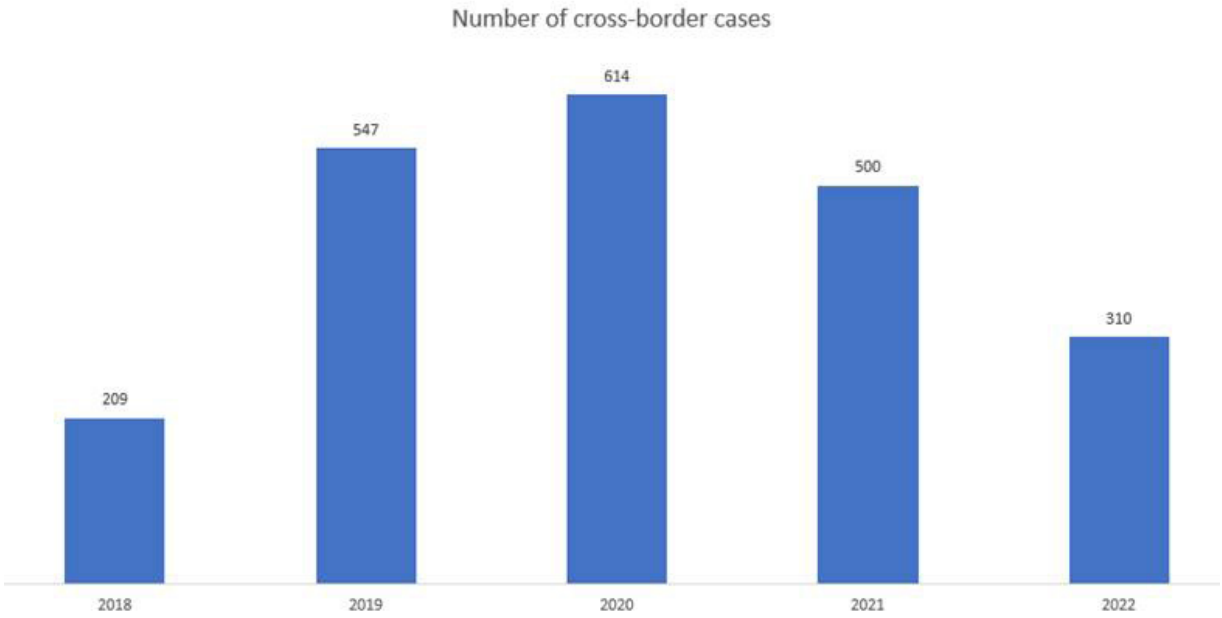
W ramach systemu IMI organy współpracują, korzystając z procedur współpracy i spójności, na podstawie przepisów RODO: art. 56 – ustalenie wiodącego organu nadzorczego i organów, których sprawa dotyczy (wniosek dotyczący sprawy lokalnej); art. 60 – kompleksowa współpraca; art. 61 – wniosek o wzajemną pomoc i dobrowolną wzajemną pomoc; art. 62 – wspólne operacje organów nadzorczych; art. 64 – opinia EROD; art. 65 – wiążąca decyzja EROD; art. 66 – opinia/decyzja EROD wydana w trybie pilnym.

412 Ang. *Internal Market Information System* , dalej: „system IMI" lub „IMI".
413 Szczegółowe informacje na temat prowadzonych przez Prezesa UODO postępowań transgranicznych znajdują się w części niniejszego Sprawozdania dotyczącej postępowań transgranicznych.



Źródło: wewnętrzny podręcznik IMI dla organów nadzorczych, opracowany przez Sekretariat EROD.

Zgodnie ze statystykami przygotowanymi przez EROD[414], od momentu rozpoczęcia obowiązywania RODO do 31 grudnia 2022 r. w rejestrze spraw IMI[415] utworzono **2180** spraw o charakterze transgranicznym[416].



Wykres 17: Liczba spraw o charakterze transgranicznym utworzonych w rejestrze IMI w okresie 25.05.2018 r.-31.12.2022 r..

- **1608** spraw zostało zainicjowanych w następstwie wniesionych skarg;
- **572** pochodziło z innych źródeł, takich jak postępowania, inicjatywy organów nadzorczych, zobowiązania prawne, doniesienia medialne itd.

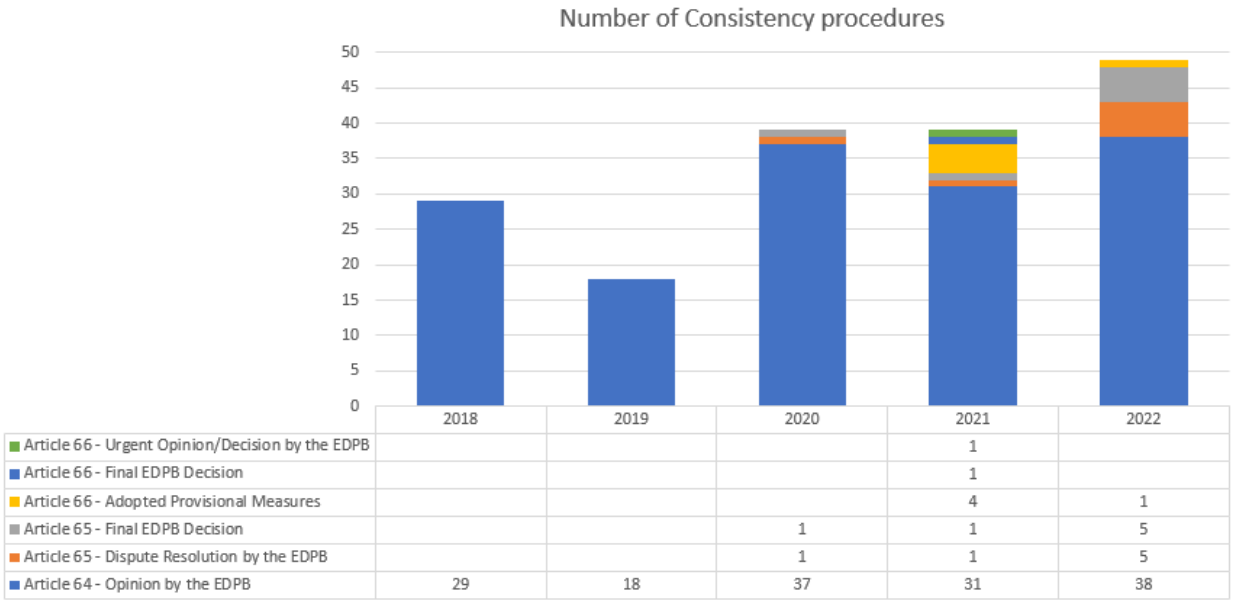
Z powyższych spraw uruchomiono następujące procedury:

- **850** procedur wzajemnej pomocy (art. 61); oprócz tego organy uruchomiły **10138** procedur w celu świadczenia sobie dobrowolnej wzajemnej pomocy;
- **1575** procedury w ramach mechanizmu kompleksowej współpracy – One-stop-shop (art. 60), z których **639** zakończyło przyjęcie ostatecznej decyzji;
- **103** sprawy o charakterze lokalnym (art. 56 ust. 2);
- **1** wspólną operację organów nadzorczych (art. 62);

414 Stan spraw zgodny ze statystykami na dzień 31 grudnia 2022 r. sporządzonymi dla organów nadzorczych przez Sekretariat EROD.
415 Wpis w rejestrze spraw IMI odnosi się do wpisu w systemie IMI, który umożliwia zarządzanie procedurami współpracy lub spójności od początku do końca. Wpis w rejestrze spraw może polegać na zarządzaniu jedną lub wieloma procedurami związanymi z wpisem do rejestru. Jest to centralny punkt, w którym organy mogą wymieniać się informacjami na temat konkretnych kwestii i wyszukiwać je. Informacje i procedury dotyczące wielu skarg związanych z tym samym przetwarzaniem mogą być połączone w jeden wpis dotyczący jednej sprawy, aby ułatwić wyszukiwanie informacji i spójne stosowanie RODO.
416 Należy pamiętać, że statystyki te obejmują jedynie sprawy rozpatrywane w ramach mechanizmu One-Stop-Shop z art. 60 RODO. W związku z tym należy wziąć pod uwagę, że: (1) odniesienia do wpisów do rejestru spraw w tych statystykach nie mają korelacji 1 do 1 z liczbą spraw transgranicznych rozpatrywanych w danym kraju, ponieważ wiele spraw może być połączonych w jednym wpisie do rejestru spraw, który w związku z tym może odnosić się do wielu spraw transgranicznych; (2) w zależności od ustawodawstwa państwa członkowskiego, organy nadzorcze mogły rozpatrywać sprawy poza procedurą przewidzianą w art. 60 zgodnie z prawem krajowym.

Wykres 18: Liczba procedur w ramach mechanizmu kompleksowej współpracy utworzonych w rejestrze IMI w okresie 25.05.2018 r.-31.12.2022 r.[417].

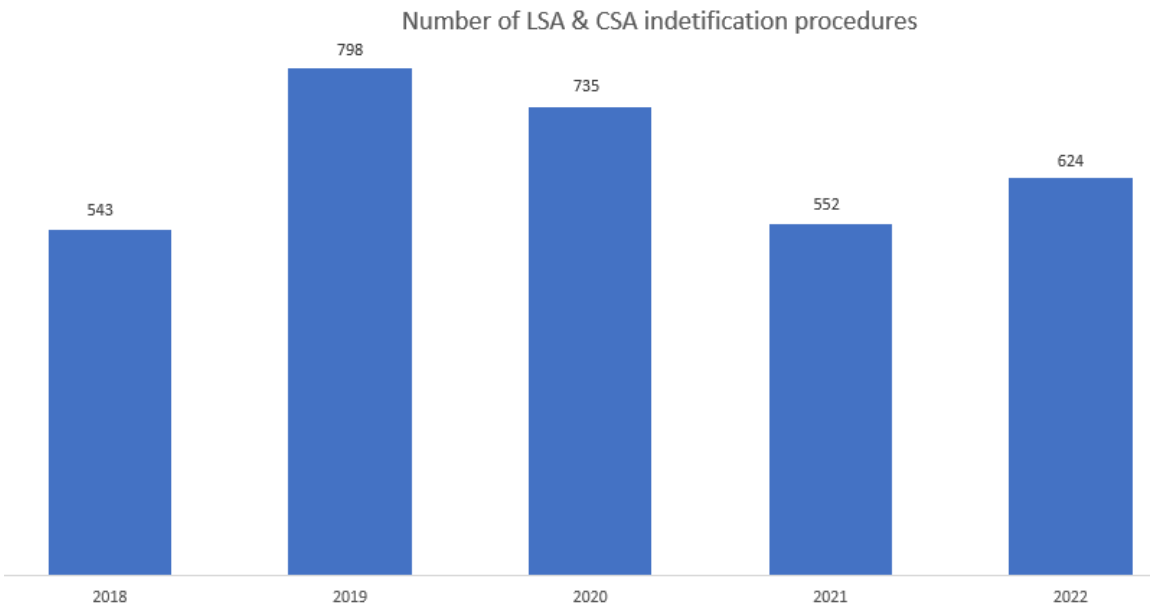
- **Procedury spójności**, w tym:
  - **153** procedury z art. 64 zakończone wydaniem **136** ostatecznych opinii z art. 64;
  - **7** procedur z art. 65 zakończonych wydaniem **7** decyzji ostatecznych z art. 65;
  - **5** środków tymczasowych z art. 66;
  - **1** ostateczną decyzję EROD z art. 66;
  - **1** ostateczną decyzję EROD w trybie pilnym z art. 66.



Wykres 19: Liczba procedur w ramach mechanizmu spójności utworzonych w rejestrze IMI w okresie 25.05.2018 r.-31.12.2022 r..

417 Źródłem grafik do wykresów w podrozdziale 8. były wewnętrzne statystyki EROD przygotowywane dla organów nadzorczych przez Sekretariat EROD.

Dodatkowo uruchomiono **3252** procedury wszczęte w celu zidentyfikowania organów wiodących i organów, których sprawa dotyczy, na podstawie art. 56 ust. 1 (**109** procedur w toku, **3143** zakończone).



Wykres 20: Liczba procedur wszczętych w celu zidentyfikowania organów wiodących i organów, których sprawa dotyczy (art. 56 ust. 1) utworzonych w rejestrze IMI w okresie 25.05.2018 r.–31.12.2022 r..

Zgodnie ze statystykami IMI na dzień 31 grudnia 2022 r. Urząd Ochrony Danych Osobowych:

- był organem wiodącym w **32** sprawach w rejestrze spraw IMI;
- zainicjował łącznie **769** powiadomień, w tym **149** z art. 56 (identyfikacja organu wiodącego i organu, którego sprawa dotyczy), **48** z art. 60 (**6** – projekt decyzji, **9** – ostateczna decyzja; **33** – nieformalne konsultacje), **569** z art. 61 (dobrowolna wzajemna pomoc) i **3** z art. 64 (opinia EROD);
- przesłał łącznie **260** wniosków, w tym: **4** z art. 56 (sprawa lokalna), **118** z art. 61 (wzajemna pomoc), **138** z art. 61 (dobrowolna wzajemna pomoc);
- otrzymał łącznie **80** wniosków, w tym: **1** z art. 56 (sprawa lokalna), **22** z art. 61 (wzajemna pomoc), **54** z art. 61 (dobrowolna wzajemna pomoc), **3** z art. 64 (ostateczna opinia EROD).

Pytania od innych organów nadzorczych

Prezes UODO jest zobowiązany na podstawie przepisów RODO do udzielania odpowiedzi na pytania zadane mu przez inne organy nadzorcze z państw Unii Europejskiej. Obowiązki te realizowane są w oparciu o mechanizmy spójności i współpracy uregulowane

w rozdz. VII RODO. Zapytania od innych organów nadzorczych kierowane są do polskiego organu za pośrednictwem Systemu IMI, w ramach procedury z art. 61 RODO. Tą samą drogą przekazywane są odpowiedzi na przedłożone zapytania.

W 2022 r. do Prezesa UODO wpłynęło 41 zapytań organów nadzorczych z innych państw, w tym m.in. z: Słowenii, Słowacji, Holandii, Francji. Włoch, Lichtensteinu, Finlandii, Norwegii, Irlandii, Malty, Niemiec, Danii, Cypru.

Dla porównania, w 2021 roku takich pytań wpłynęło 25, zaś w 2020 roku – 14.

Organy nadzorcze zwracały się do Prezesa UODO z różnymi zagadnieniami. Pytania dotyczyły m.in. opinii polskiego organu nadzorczego w zakresie:

- przetwarzania numeru telefonu w celach marketingowych,
- wprowadzania aplikacji covidowych w Polsce,
- kodeksów postępowania dla małych i średnich przedsiębiorstw,
- zainstalowanych w samochodach i dronach kamer,
- stosowania przez uniwersytety lub szkoły wyższe „rozwiązań egzaminacyjnych na odległość" w kontekście kryzysu zdrowotnego i poza nim,
- ram prawnych marketingu bezpośredniego B2B skierowanego do osób prywatnych za pośrednictwem ich adresu zawodowego,
- instalacji kamer w przedszkolach i żłobkach,
- listy sankcyjnej,
- aktualizacji do sprawy TikTok; aktualizacji do sprawy Google – Mój Ad Center,
- e-paragonu,
- kodeksu postępowania w zakresie gier hazardowych w Internecie na podstawie art. 40 RODO, opublikowanego przez Europejskie Stowarzyszenie Gier i Zakładów Online; organów nadzorczych przy DGA,
- wprowadzenia informacji behawioralnych do codziennej praktyki egzekwowania RODO,
- kwestii interpretacji art. 15 RODO, w tym w zakresie ewentualnego dostępu do danych medycznych przez współmałżonka oskarżonego o stosowanie przemocy fizycznej,
- interpretacji Dyrektywy NIS i RODO pod kątem wzajemnej relacji tych przepisów i kompetencji organów nadzorczych,
- interpretacji Dyrektywy 2019/944 w zakresie przetwarzania danych osobowych za pośrednictwem inteligentnych liczników energii elektrycznej,
- transferu danych do Rosji po 24 lutego 2022 r.,
- tworzenia czarnych list pasażerów przez linie lotnicze i przekazywania sobie wzajemnie

danych osobowych pasażerów znajdujących się na takiej liście,

- łączenia danych między instytucjami bankowymi jako środka przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML/CFT),
- spersonalizowanych ubezpieczeń OC pojazdów tzw. usage-based insurance (UBI) oraz przekazywania danych osobowych wewnątrz grupy (holdingu) podmiotów – administratorów tych danych.

Polski organ ochrony danych dokonał wnikliwej analizy przedłożonych pytań, a następnie przygotował stosowne odpowiedzi w języku angielskim i przekazał je do właściwych organów nadzorczych.

8. Wnioski prejudycjalne

W ramach współpracy międzynarodowej z organami nadzorczymi innych państw członkowskich UE oraz wykonywania obowiązków wynikających z członkostwa Polski w Unii Europejskiej, Prezes UODO dokonuje analizy wniosków w sprawach prejudycjalnych wniesionych do TSUE, przekazanych przez KPRM. Wnioski te dotyczą zagadnień z zakresu ochrony danych osobowych. Organ nadzorczy przygotowuje obszerne stanowiska, których przedmiotem jest rekomendacja w zakresie zasadności udziału Polski w poszczególnych postępowaniach przed TSUE. Stanowiska te przekazywane są do KPRM i służą do przygotowania stanowiska Polski w sprawach postępowań prowadzonych przez TSUE. Prezes UODO przedstawia swoje rekomendacje także na późniejszych etapach postępowań prowadzonych przed TSUE. Po wydaniu wyroku TSUE organ nadzorczy przedstawia swoje stanowisko w sprawie zasadności zmiany polskiego prawa w świetle treści danego orzeczenia.

Organ nadzorczy dokonuje – niezależnie od powyższego – regularnego przeglądu wszystkich postępowań inicjowanych przez TSUE, na podstawie wykazów otrzymanych od KPRM. Organ bada, czy wszystkie sprawy, których przedmiotem jest ochrona danych osobowych, trafiły do organu nadzorczego i czy zajął on stanowisko co do zasadności udziału Polski w postępowaniu.

W 2022 r. do polskiego organu nadzorczego wpłynęło **28 nowych wniosków prejudycjalnych skierowanych do TSUE** przez sądy z różnych państw Unii Europejskiej – dla porównania należy wskazać, że w 2021 r. było ich 27, a w 2020 r. – 13. Organ nadzorczy dokonał wnikliwej analizy przekazanych przez KPRM wniosków prejudycjalnych, a następnie przedstawił swoje stanowisko, co do zasadności udziału Polski w tych postępowaniach z punktu widzenia przepisów o ochronie danych osobowych. W poszczególnych postępowaniach przedstawiał on również dalsze rekomendacje, w tym co do zasadności wnioskowania przez Polskę o przeprowadzenie rozprawy przed TSUE. Jako przykłady można wskazać następujące sprawy:

- C-162/22 Lietuvos Respublikos generalinė prokuratura (sprawa dotyczyła ochrony

danych osobowych w sektorze łączności elektronicznej i wykorzystania danych retencyjnych przez dostawców usług łączności elektronicznej, w ocenie organu nadzorczego udział w postępowaniu był zasadny)[418];

- C-178/22 Procura della Repubblica presso il Tribunale di Bolzano (sprawa dotyczyła również ochrony danych osobowych w sektorze łączności elektronicznej, dostępu organów ścigania do wyciągów telefonicznych, w ocenie organu nadzorczego udział w postępowaniu był zasadny)[419];
- C-241/22 DX (sprawa dotyczyła także ochrony danych w sektorze łączności elektronicznej – dostępu organów publicznych do danych o ruchu i lokalizacji użytkowników w celu zwalczania przestępczości, pojęcia poważnej przestępczości, w ocenie organu udział w postepowaniu był zasadny)[420];
- C-26/22 i C-64/22 SCHUFA Holding i in. (sprawa dotyczyła sądowej kontroli decyzji organu nadzorczego, wykładni art. 77 ust. 1 w zw. z art. 78 ust. 1 RODO, przechowywania danych osobowych przez prywatne biuro informacji kredytowej, w którym są dane z rejestru publicznego, istnienia równoległych baz danych, które są tworzone obok państwowych baz danych, organ nadzorczy odniósł się do uwag uczestników postępowania, organ wskazał na zasadność udziału w rozprawie)[421];
- C-604/22, IAB Europe (sprawa dotyczyła wykładni podstawowych pojęć RODO, w tym m.in. administratora i danych osobowych, ciąg znaków zawierających preferencje użytkownika Internetu jako dane osobowe, może ona mieć duże znaczenie dla wykładni RODO w przyszłości, organ nadzorczy przedstawił obszerne stanowisko dotyczące zasadności udziału Polski w postępowaniu przed TSUE);
- C-280/22 Kinderrechtencoalitie Vlaanderen et Liga voor Mensenrechten (sprawa dotyczyła obowiązku umieszczania i przechowywania odcisków palców w dowodach osobistych, polski organ nadzorczy wskazał, że udział w postępowaniu w sprawie jest zasadny, ponieważ sprawa ta, w zakresie wskazanym w pytaniu prejudycjalnym, może mieć istotny wpływ na polskie prawo, w przypadku stwierdzenia przez TSUE niezgodności obowiązku umieszczania i przechowywania odcisków palców w dowodach osobistych z prawem pierwotnym Unii Europejskiej konieczne będzie bowiem dokonanie zmiany prawa polskiego)[422].

W 2022 r. Prezes UODO przedstawiał również swoje stanowiska w ramach postępowań TSUE – na różnych ich etapie – w których wnioski prejudycjalne wpłynęły do organu nadzorczego w poprzednich latach. Przykładowo, organ nadzorczy dokonał analizy wpływu wyroków wydanych przez TSUE w sprawach:

- C-793/19 i C-794/19 SpaceNet i in. (w ocenie organu nadzorczego wyrok będzie

418 DOL.0623.12.2022.
419 DOL.0623.11.2022.
420 DOL.0623.17.2022.
421 DOL.0623.5.2022.
422 DOL.0623.19.2022.

skutkował koniecznością zmian w polskim porządku prawnym. Sprawa dotyczyła retencji danych osobowych przez dostawców sieci łączności elektronicznej, zdaniem organu nadzorczego zmiany powinny dotyczyć art. 180a w zw. z art. 180c prawa telekomunikacyjnego z uwagi na art.15 ust. 1 dyrektywy 2002/58/WE. Prawodawca polski ponadto nie precyzuje warunków dostępu do danych telekomunikacyjnych. Oprócz wskazanych regulacji prawa telekomunikacyjnego, zmiany legislacyjne powinny objąć poszczególne ustawy przyznające właściwym organom dostęp do danych o ruchu i lokalizacji, a także powinny regulować sposób pozyskania danych)[423];

- C-339/20 i C397/20 VD i in. (w ocenie organu nadzorczego wyrok będzie skutkował koniecznością zmiany prawa polskiego, sprawa dotyczyła dostępu organów nadzoru finansowego do danych telekomunikacyjnych)[424];
- C-140/20 G.D. vs. Commissioner of An Garda Síochána i in. (orzeczenie będzie istotne z uwagi na retencję danych telekomunikacyjnych z art. 180a prawa telekomunikacyjnego)[425];
- C-534/20 Leistritz (sprawa dotyczyła statusu IOD, zakazu wypowiedzenia stosunku pracy IOD przez administratora będącego jego pracodawcą, w ocenie organu nadzorczego w świetle orzeczenia celowe jest rozważenie zmiany przepisów prawa pod kątem doprecyzowania w polskim porządku prawnym regulacji z art. 38 ust. 3 zdanie drugie RODO, a tym samym wzmocnienia pozycji IOD)[426];
- C-601/20 Sovim (organ nadzorczy przedstawił obszerne stanowisko dotyczące zasadności zmiany przepisów polskiego prawa dotyczące publicznego udostępniania informacji o beneficjentach rzeczywistych w świetle wyroku TSUE w tej sprawie, z 22 listopada 2022 r.)[427].

W 2022 r. organ nadzorczy wydawał także rekomendacje w innych postępowaniach – wszczętych przed 2022 rokiem – prowadzonych przez TSUE:

- C-132/21 Nemzeti Adatvédelmi és Információszabadság Hatóság (sprawa dotyczyła zbiegu postepowań przed organem nadzorczym i przed sądem, organ nadzorczy nie dostrzegł zasadności udziału Pełnomocnika RP w rozprawie)[428];
- C-548/21 Bezirkshauptmannschaft Landeck (ochrona danych osobowych w sektorze łączności elektronicznej – dostęp organów ścigania do danych zapisanych na telefonach komórkowych bez zezwolenia sądu, organ nadzorczy dostrzegł zasadność udziału RP w postępowaniu jako zasadny, bowiem wyrok Trybunału może mieć wpływ

423 DOL.070.2.2019.
424 DOL.0623.30.2020.
425 DOL.0623.14.2020.
426 DOL.0623.33.2020.
427 DOL.0623.1.2021.
428 DOL.0623.6.2021.

na obowiązujące w Polsce przepisy prawa regulujące kontrolę operacyjną Policji)[429].

9. Przekazywanie danych osobowych poza EOG

W 2022 r. do Prezesa UODO wpływały informacje i zapytania od organów nadzorczych z Europejskiego Obszaru Gospodarczego („EOG") dotyczące wiążących reguł korporacyjnych („WRK") w ponad 50 grupach kapitałowych. Współpraca organów nadzorczych z EOG w toku procedury zatwierdzania WRK odbywa się z uwzględnieniem mechanizmu spójności przewidzianego w art. 63 RODO, po zasięgnięciu opinii Europejskiej Rady Ochrony Danych.

Informacje i zapytania od organów nadzorczych z EOG dotyczyły przede wszystkim:

- zgłoszenia ewentualnych zastrzeżeń odnośnie do ustanowienia organu wiodącego w ramach danej procedury zatwierdzania WRK,
- ewentualnych komentarzy do projektu konkretnych wiążących reguł korporacyjnych (ich skonsolidowanego projektu, będącego rezultatem współpracy organu wiodącego i współrecenzentów),
- ewentualnych komentarzy do zaktualizowanych wersji już zatwierdzonych WRK.

W przypadku projektów niektórych WRK komentarze do nich były również dyskutowane podczas dedykowanych sesji podgrupy ekspertów EROD ds. Międzynarodowego Przekazywania Danych dotyczących WRK, w których uczestniczyły inne organy z EOG.

W 2022 r. polski organ nadzorczy podjął się działania w charakterze współrecenzenta w procedurze zatwierdzania wiążących reguł korporacyjnych prowadzonej przez organ wiodący z EOG i została w tym zakresie sporządzona stosowna analiza.[430] Ponadto polski organ nadzorczy uczestniczył w ramach EROD w procedurze przyjmowania opinii odnoszących się projektów decyzji dotyczących projektów WRK.

W 2022 r. polski organ nadzorczy otrzymał dwa zapytania odnośnie do wystąpienia, jako wiodący organ nadzorczy, przy tworzeniu Wiążących Reguł Korporacyjnych dla administratorów danych osobowych i podmiotów przetwarzających.

W jednej ze spraw, która rozpoczęła się jeszcze w 2021 r.[431], pewna grupa kapitałowa rozważała „przeniesienie" swoich wiążących reguł korporacyjnych do polskiego organu nadzorczego, który miałby działać w charakterze organu wiodącego. W 2022 r., w związku z pismem wspomnianej grupy kapitałowej zostało wszczęte formalne postępowanie[432] w tej sprawie.

W 2022 r. została wydana przez polski organ nadzorczy decyzja o umorzeniu postępowania w sprawie dotyczącej zatwierdzenia wiążących reguł korporacyjnych[433]. Postępowanie w tej sprawie zostało wszczęte w 2018 r., po rozpoczęciu stosowania RODO.

429 DOL.0623.29.2021.
430 DOL.4413.11.2022.
431 DOL.023.768.2021.
432 DOL.4413.9.2022.
433 ZWME.46.1.2018.

Zgodnie z procedurą określoną w przyjętym przez Grupę Roboczą Art. 29 dokumencie WP 263 rev. 01 „Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR” ustalono, że to polski organ ochrony danych będzie organem wiodącym w przedmiotowej procedurze zatwierdzania wiążących reguł. W 2022 r. do Urzędu Ochrony Danych Osobowych wpłynęło pismo pełnomocnika spółki wnioskującej o zatwierdzenie wiążących reguł korporacyjnych, który działając w jej imieniu, poinformował o cofnięciu wniosku, co do przyjęcia wiążących reguł korporacyjnych i wniósł o umorzenie postępowania w tym zakresie.

W 2022 r., w związku z otrzymanym przez jeden z organów nadzorczych z EOG wnioskiem dotyczącym tzw. klauzul umownych ad-hoc przewidzianych w art. 46 RODO, poinformował on inne organy nadzorcze z EOG o tym, że jest gotowy podjąć się działania w roli organu wiodącego dla tej aplikacji, wyznaczając jednocześnie termin na przesłanie ewentualnych zastrzeżeń w tym zakresie. Polski organ nadzorczy nie zgłaszał w tym zakresie zastrzeżeń[434].

Przedstawiciele polskiego organu nadzorczego uczestniczyli również w comiesięcznych spotkaniach podgrupy ekspertów EROD ds. Międzynarodowego Przekazywania Danych. W omawianym okresie sprawozdawczym polski organ nadzorczy przedstawił swoje stanowisko odnośnie do propozycji Europejskiej Rady Ochrony Danych dotyczącej usprawnień procedur, współpracy transgranicznej i harmonizacji działań krajowych organów ochrony danych osobowych na poziomie unijnym[435]. Ponadto pracownicy UODO przygotowywali informacje na posiedzenie plenarne w związku z dokumentami, które były przyjmowane przez EROD (w tym w procedurze pisemnej). Kwestie te były także przedmiotem spotkań wewnętrznych, organizowanych w UODO. UODO udzielał również odpowiedzi na zapytania innych organów nadzorczych lub Sekretariatu EROD dotyczące np. propozycji odpowiedzi na zapytanie o dostęp do dokumentów czy ewentualnych działań podejmowanych przez inne organy nadzorcze[436].

W dniach 17-18 maja 2022 r. dwóch pracowników Urzędu Ochrony Danych Osobowych uczestniczyło w warsztatach dotyczących wiążących reguł korporacyjnych zorganizowanych przez chorwacki organ nadzorczy ds. ochrony danych.

10. Inne sprawy

W 2022 roku organ właściwy w sprawie ochrony danych osobowych zajmował się również innymi sprawami – zarówno o zasięgu krajowym, jak i międzynarodowym – dotyczącymi innych kwestii niż te wskazane powyżej.

W 2022 roku UODO otrzymywał regularnie różnego rodzaju informacje z ministerstw

434 DOL.601.2.2022.
435 DOL.4413.29.2022.
436 DOL.614.12.2022.

dotyczące udziału RP w pracach organizacji i organów współpracy międzynarodowej, negocjacji umów wielostronnych itp., mających związek z przetwarzaniem danych osobowych. W dniach 10-14 października 2022 r. w ramach wizyty studyjnej gościł przedstawicieli organu ochrony danych z Macedonii Północnej, podczas której m.in. przedstawiona została prezentacja, której tematem było „Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych".

Prezes Urzędu zajmował również stanowiska w sprawie wystąpień przedstawiciela RP w Grupie ekspertów Komisji Europejskiej ds. rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680 w 2022 r.[437]

W 2022 r. polski organ nadzorczy, jako członek Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych, uczestniczył w opiniowaniu dwóch dokumentów roboczych *Draft guidelines on data protection in the context of mechanisms for inter-state exchanges of data for Anti-Money Laundering/Countering Financing of Terrorism, and tax purposes* (Projekt wytycznych w sprawie ochrony danych w kontekście mechanizmów międzypaństwowej wymiany danych do celów przeciwdziałania praniu pieniędzy/przeciwdziałania finansowaniu terroryzmu oraz do celów podatkowych) oraz *Model Contractual Clauses for Transborder Data Flows of Personal Data* (Standardowe klauzule umowne dotyczące transgranicznych przepływów danych osobowych)[438].

11. Międzynarodowe Warsztaty

Warsztaty Internet Privacy Engineering Network. Warszawa, 22.06.2022 r.

Warsztaty Internet Privacy Engineering Network (IPEN Workshop 2022) odbyły się pod hasłem „Digital Identity in data protection by design – current developments and future trents" na Uniwersytecie Stefana Wyszyńskiego w Warszawie (UKSW). Wydarzenie to, w całości poświęcone tożsamości cyfrowej, zorganizowane zostało przez Europejskiego Inspektora Ochrony Danych Osobowych i UKSW w Warszawie. Warsztaty IPEN miały na celu zapoznanie uczestników z zagadnieniami związanymi z rozwojem systemów tożsamości cyfrowej w Unii Europejskiej i określenie aktualnego stanu wiedzy na temat możliwych rozwiązań pozwalających na pełne wdrożenie w ramach takich inicjatyw, przewidzianej przez RODO zasady zapewnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

12. Porozumienie o współpracy

6 lipca 2022 r. zostało zawarte Porozumienie o współpracy pomiędzy Urzędem Ochrony Danych Osobowych a Krajowym Centrum Ochrony Danych Osobowych Republiki Mołdawii.

437 DOL.401.560.2021.
438 DWME.IK.367468.

W Porozumieniu strony wyraziły zainteresowanie dalszym rozwojem i umacnianiem stosunków dwustronnych między Urzędem Ochrony Danych Osobowych Rzeczypospolitej Polskiej a Krajowym Centrum Ochrony Danych Osobowych Republiki Mołdawii oraz dążeniem do wspólnego celu, jakim jest promowanie swojej roli na poziomie europejskim w dziedzinie ochrony praw podstawowych, wolności i ochrony danych osobowych. Porozumienie to było bardzo istotną inicjatywą zapewniającą wzmocnienie oraz intensyfikację współpracy w zakresie ochrony danych osobowych pomiędzy mołdawskim i polskim organem ochrony danych osobowych, w świetle niedawnego przyznania Republice Mołdawii statusu państwa kandydującego do przystąpienia do Unii Europejskiej.

13. Wizyta studyjna, 10-14.10.2022 r.

W dniach 10-14 października 2022 r. siedzibę UODO odwiedziła 8-osobowa reprezentacja przedstawicieli Agencji Ochrony Danych Osobowych z Północnej Macedonii. Wizyta odbyła się w ramach finansowanego przez UE projektu twinningowego „Support to the implementation of the Modernised Data Protection Legal Framework" („Wsparcie dla wdrażania zmodernizowanych ram prawnych w zakresie ochrony danych"), realizowanego na rzecz Agencji Ochrony Danych Osobowych z Macedonii Północnej przez Chorwacką Agencję Ochrony Danych Osobowych we współpracy z Niemiecką Fundacją na rzecz Międzynarodowej Współpracy Prawnej. Pięciodniowy cykl spotkań miał na celu wymianę wspólnych doświadczeń oraz podzielnie się dobrymi praktykami i czerpanie z wypracowanej już wiedzy. Przedstawiciele UODO zaprezentowali doświadczenia polskiego organu związane z unijną reformą ochrony danych osobowych, strukturę i zadania polskiego organu nadzorczego oraz praktyczne aspekty jego działalności. Delegacja organu ochrony danych z Macedonii Północnej przedstawiła prezentację pt. „Ramy instytucjonalne i prawne", w której dokonała analizy porównawczej stosowania prawa ochrony danych osobowych w Macedonii Północnej w odniesieniu do RODO. Współpraca UODO z Agencją Ochrony Danych Osobowych w Macedonii Północnej, trwa już od wielu lat. W 2011 roku podczas wizyty studyjnej w ramach projektu „Wsparcie dla organu ochrony danych osobowych" przedstawiciele organów nadzorczych podpisali porozumienie o współpracy i wzajemnej wymianie doświadczeń.

14. Międzynarodowe konferencje, seminaria i spotkania

W okresie sprawozdawczym 2022 r. Prezes UODO i jego przedstawiciele uczestniczyli w konferencjach, seminariach i spotkaniach o charakterze międzynarodowym organizowanych przez UODO oraz inne podmioty krajowe i zagraniczne. Wykaz tych wszystkich wydarzeń znajduje się w załączniku nr 4.

Poniżej przedstawione zostały wybrane przykłady najważniejszych z nich.

1) Spotkania Sieci Inspektorów Ochrony Danych (DPO Network) – online 27.01.2022 r., 27.04.2022 r., 21.09.2022 r., 30.11.2022 r.

Niezależna sieć inspektorów ochrony danych, której prace koordynuje EROD, składa się z IOD każdego z organów nadzorczych, inspektora ochrony danych EROD I inspektora ochrony danych EIOD. W 2022 roku Sieć IOD spotkała się 4 razy w formule online. W spotkaniach tych uczestniczył IOD Urzędu Ochrony Danych Osobowych.

2) I Posiedzenie Komitetu ekspertów ds. Integralności informacji online (MSI-INF), 15-16.03.2022 r.

W dniach 15-16 marca 2022 r. odbyło się pierwsze posiedzenie Komitetu Ekspertów ds. integralności informacji w sieci (Committee of experts on the integrity of online information MSI-INF), w którym brał udział przedstawiciel UODO. W skład Komitetu wchodzi 13 członków, w tym siedmiu przedstawicieli państw członkowskich, wyznaczonych przez Komitet Sterujący ds. Mediów i Społeczeństwa Informacyjnego (CDMSI) oraz sześciu niezależnych ekspertów wyznaczonych przez Sekretarza Generalnego Rady Europy, posiadających uznaną wiedzę specjalistyczną związaną z wolnością słowa i informacji, środowiskiem informacyjnym online oraz gospodarką i projektowaniem platform cyfrowych. W pracach komitetu biorą udział także inne państwa członkowskie, które mogą desygnować swoich reprezentantów. Wśród uczestników i obserwatorów znajdują się m.in. odpowiednie organy i struktury Rady Europy (np. Komitet Konsultacyjny Konwencji 108, z ramienia którego w pracach MSI-INF uczestniczy przedstawiciel UODO). Zadaniem MSI-INF jest przygotowanie do końca 2023 roku projektu wytycznych dotyczących przeciwdziałania rozpowszechnianiu błędnych informacji i dezinformacji poprzez sprawdzanie wiarygodności danych i projektowanie platform w sposób zgodny z prawami człowieka. Celem projektu wytycznych jest sformułowanie podejścia zgodnego z prawami człowieka i zestawu konkretnych wytycznych dla państw członkowskich, określających istotne potrzeby, wyzwania, kwestie i warunki skutecznego przeciwdziałania dezinformacji. Dokument ma być narzędziem „miękkiego prawa", niewiążący prawnie. Przeznaczony będzie głównie dla państw członkowskich, tj. decydentów politycznych i osób zaangażowanych we wdrażanie. Ostatecznie przyjęty ma być przez przez Steering Committee od Media and Information Society (CDMSI) oraz zostanie zgłoszony przez Komitet Ministrów. Rozważane jest także sporządzenie uzasadnienia, jako pomocniczego narzędzia interpretacyjnego.

3) 55. Posiedzenie Biura Komitetu Konsultacyjnego Konwencji 108 Rady Europy. Paryż, 23-25.03.2022 r.

Biuro Komitetu Konwencji 108 odbyło 55. posiedzenie w formacie hybrydowym w Paryżu. Przy udziale ekspertów-konsultantów zajmujących się różnymi tematami kontynuowało dyskusje nad wytycznymi w sprawie tożsamości cyfrowych w perspektywie ich przyjęcia na następnym posiedzeniu plenarnym, międzypaństwową wymianą danych do celów przeciwdziałania praniu pieniędzy, zwalczania finansowania terroryzmu i celów podatkowych, interpretacją art. 11 zmodernizowanej Konwencji nr 108 i klauzulami umownymi w kontekście transgranicznych przepływów danych, a także nad elementami projektu regulacji wewnętrznej przyszłego mechanizmu oceny i monitorowania w ramach Konwencji nr 108+. Biuro przyjęło również wniosek administracji organizacji o wydanie opinii na temat projektu nowych przepisów Rady Europy dotyczących ochrony danych osobowych[439].

4) Privacy Symposium – Międzynarodowe Sympozjum nt. ochrony prywatności. Wenecja, 5-7.04.2022 r.

Międzynarodowa konferencja Privacy Symposium, poświęcona była zagadnieniom ochrony prywatności w związku z rozwojem nowych technologii, takich jak sztuczna inteligencja, 5G i obliczenia kwantowe. W wydarzeniu tym uczestniczyła przedstawicielka UODO, która wygłosiła wystąpienie, pt. „Jak zapewnić ochronę prywatności dzieci – perspektywa polskiego organu nadzorczego" podczas panelu dotyczącego praw osób małoletnich („Data Subject Rights with Minors of Age"). W swojej prezentacji skupiła się na zagadnieniach związanych z rozwojem sztucznej inteligencji w obszarze edukacji najmłodszych[440].

5) Spotkanie Rzeczników organów ochrony danych. Wiedeń, 27-28.04.2022 r.

W dniach 27-28 kwietnia 2022 r. w Wiedniu odbyło się spotkanie Rzeczników organów ochrony danych w sprawie funkcjonowania mechanizmu kompleksowej współpracy i wdrażania RODO, w którym wzięła udział również przedstawicielka UODO. Organizatorem wydarzenia był austriacki organ ochrony danych. Podczas tego spotkania na wysokim szczeblu członkowie Europejskiej Rady Ochrony Danych osiągnęli porozumienie w sprawie dalszego wzmacniania współpracy w zakresie spraw strategicznych oraz w sprawie dywersyfikacji zakresu wykorzystywanych metod współpracy. Podjęto m.in. decyzję, że członkowie EROD będą regularnie wspólnie identyfikowali sprawy transgraniczne o znaczeniu strategicznym w różnych

439 Pełny raport z posiedzenia znajduje się tutaj: https://rm.coe.int/t-pd-bur-2022-55rapabr-abridged-report-en/1680a5f460
440 Więcej informacji na temat Sympozjum dostępnych jest na stronie internetowej wydarzenia: www.privacysymposium.org

państwach członkowskich, a następnie nadawali współpracy w ramach takich spraw status priorytetowy, zapewniający wsparcie EROD. Grupy organów ochrony danych mogą zdecydować o połączeniu sił w zakresie działań związanych z postępowaniami i egzekwowaniem prawa, a organy ochrony danych mogą dzielić się pracą w ramach tych grup. W razie potrzeby można utworzyć grupę zadaniową EROD[441].

6) Wiosenna Konferencja Europejskich Organów Ochrony Danych. Cavtat w Chorwacji, 19-29.05.2022 r.[442]

W Cavtat, w Chorwacji, odbyła się 30. Wiosenna Konferencja Europejskich Organów Ochrony Danych, zorganizowana przez chorwacką Agencję Ochrony Danych Osobowych (AZOP) w celu wsparcia współpracy i wymiany najlepszych praktyk między członkami. W wydarzeniu udział wzięli również przedstawiciele Urzędu Ochrony Danych Osobowych. Warto podkreślić znaczenie uczestnictwa 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. Podczas 30. Konferencji Europejskich Organów Ochrony Danych członkowie przyjęli Rezolucję w sprawie potrzeby szybkiej ratyfikacji „Konwencji 108+", zmodernizowanej Konwencji 108. Rezolucja wzywa rządy państw członkowskich Rady Europy, rządy państw trzecich do Rady Europy, Unii Europejskiej i organizacji międzynarodowych do przyspieszenia procesu podpisania i ratyfikacji Konwencji 108+.

Konferencja była dla organów okazją do omówienia różnych zagadnień, przykładów najlepszych praktyk i strategii, w szczególności dotyczących ich własnej funkcji prognozowania, przekazywania danych i egzekwowania w zakresie spraw transgranicznych. Podczas wydarzenia ogłoszono, że w 2023 r. gospodarzem Wiosennej Konferencji będzie węgierski organ ochrony danych w Budapeszcie.

7) Roundtable on Children's Privacy in Europe. Londyn, 15.06.2022 r.

W ramach okrągłego Stołu odbyły się warsztaty CIPL (Centre for International Policy Leadership) pod nazwą *Taking stock of law, policy, regulatory qiudance and best practices on children's data protection in Europe.* Podczas tego wydarzenia przeanalizowane zostały inicjatywy regulacyjne dotyczące ochrony danych osobowych

441 Więcej informacji znajduje się w wydanej przez EROD deklaracji w sprawie współpracy w zakresie egzekwowania prawa.
442 Więcej informacji można znaleźć na stronie: springconference2022.hr

dzieci, sposoby maksymalnego zwiększenia ich bezpieczeństwa w świecie cyfrowym oraz relacji pomiędzy prawem do prywatności a interesami biznesu w środowisku cyfrowym. Uczestnicy zapoznali się z metodami weryfikacji wieku oraz normami bezpieczeństwa w zakresie przetwarzania danych osobowych dzieci. Przedstawiciel UODO wystąpił w sesji Regulatory Priorities and Policy Initiatives, podczas której dyskutowano na temat zapewnienia dzieciom szerokiego zakresu ochrony prywatności, zarządzania ryzykiem oraz umożliwienia dzieciom bezpiecznego uczestnictwa w gospodarce cyfrowej, przy jednoczesnym wspieraniu innowacji.

8) Konferencja EIOD pt. „Przyszłość ochrony danych. Skuteczne egzekwowanie prawa w cyfrowym świecie" (EDPS Conference „The Future of data protection. Effective enforcement in the digital world"). Bruksela, 16-17.06.2022 r.

Europejski Inspektor Ochrony Danych Osobowych zorganizował Konferencję pt. „Przyszłość ochrony danych. Skuteczne egzekwowanie prawa w cyfrowym świecie" w celu omówienia różnych podejść i modeli egzekwowania prawa. EIOD uznał, że niemal cztery lata po tym, jak zaczęło obowiązywać RODO, nadszedł czas, aby zastanowić się nad funkcjonowaniem i skutecznością rozporządzenia. Głównym zadaniem konferencji była wymiana poglądów, pomysłów i wizji dotyczących przyszłości ochrony danych. Program wydarzenia oparto na czterech głównych blokach tematycznych: (1) modele zarządzania i egzekwowania prawa UE, (2) mechanizm egzekwowania RODO, (3) identyfikacja najlepszych praktyk w zakresie egzekwowania przepisów i mechanizmu współpracy, (4) identyfikacja potencjalnych scenariuszy, ze szczególnym uwzględnieniem skutecznej ochrony podstawowych praw człowieka – prawa do prywatności i ochrony danych osobowych.

9) 56. posiedzenie Biura Komitetu Konsultacyjnego Konwencji 108 Rady Europy. Strasburg, 21-22.09.2022 r.

Podczas 56. Posiedzenia plenarnego, Biuro kontynuowało prace nad wytycznymi w sprawie tożsamości cyfrowej z myślą o ich przyjęciu na kolejnym posiedzeniu plenarnym, nad międzypaństwową wymianą danych do celów przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu oraz do celów podatkowych, itd. We współpracy z sekretariatem Moneyval uczestnicy tego spotkania debatowali nad interpretacją art. 11 zmodernizowanej konwencji nr 108 oraz nad klauzulami umownymi w kontekście transgranicznych przepływów danych. Biuro odnotowało również pozytywne postępy w pracach Kostaryki nad jej przepisami o ochronie danych[443].

443 Pełny raport z posiedzenia znajduje się tutaj: https://rm.coe.int/t-pd-bur-2022-56rapabr-abridged-report-en/1680a837b2

10) II Posiedzenie Komitetu ekspertów ds. Integralności informacji online (MSI-INF), 5-6.10.2022 r.

Drugie Posiedzenie Komitetu Ekspertów ds. Integralności Informacji Online (MSI-INF) odbyło się w formacie hybrydowym. Komitet Ekspertów i uczestnicy przeprowadzili konstruktywne dyskusje na temat pierwszego projektu Wytycznych w sprawie przeciwdziałania rozprzestrzenianiu się w sieci błędnych informacji i dezinformacji, poprzez sprawdzanie faktów i rozwiązania w zakresie projektowania platform w sposób zgodny z prawami człowieka, które mają być gotowe pod koniec 2023 roku.

11) 44. Międzynarodowa Konferencja Global Privacy Assembly. Stambuł, 25-28.10.2022 r.

Gospodarzem 44. Międzynarodowej Konferencji Global Privacy Assembly (GPA) zatytułowanej „A Matter of Balance. Privacy in The Era of Rapid Technological Advancement" („Kwestia równowagi. Prywatność w dobie szybkiego postępu technologicznego") był organ ochrony danych osobowych Turcji (KVKK). **W tej najważniejszej corocznej międzynarodowej konferencji poświęconej ochronie danych osobowych, która zrzesza organy ochrony danych i prywatności z całego świata, uczestniczyła przedstawicielka Urzędu Ochrony Danych Osobowych.** Konferencja została podzielona na dwie sesje: otwartą, która odbywała się 25-26 października 2022 r., oraz zamkniętą - 27-28 października 2022 r. Przemówienia przewodnie i panele sesji otwartej koncentrowały się na postępującym rozwoju technologicznym w dziedzinie rozpoznawania twarzy, sztucznej inteligencji i blockchain oraz związanych z tym wyzwaniach dla ochrony danych, na transgranicznym przekazywaniu danych, na zagrożeniach dla prywatności w obszarze pomocy humanitarnej i w odniesieniu do grup szczególnie wrażliwych, takich jak dzieci. Podczas sesji zamkniętej Konferencji, Grupy robocze GPA, Podkomitet GPA ds. Kierunków Strategicznych, różni członkowie i obserwatorzy GPA, a także Grupa Berlińska i inne organizacje partnerskie przedstawiły swoje sprawozdania. Przemówienia przewodnie i dyskusje panelowe prowadzone podczas sesji zamkniętej koncentrowały się głównie na poprawie efektywności i wzmocnieniu współpracy pomiędzy organami nadzorczymi.

Podczas sesji zamkniętej 44. Międzynarodowej Konferencji Global Privacy Assembly przyjęto następujące rezolucje:

- Rezolucję w sprawie zmiany planu działania i harmonogramu Sekretariatu,
- Rezolucję w sprawie budowania potencjału współpracy międzynarodowej w celu poprawy bezpieczeństwa cybernetycznego oraz identyfikacji szkód związanych z incydentami cybernetycznymi,
- Rezolucję w sprawie zasad i oczekiwań dotyczących właściwego wykorzystywania danych osobowych w technologii rozpoznawania twarzy.

Podczas wydarzenia ogłoszono, że organ nadzorczy Bermudów będzie gospodarzem Międzynarodowej Konferencji Global Privacy Assembly w 2023 r.[444]

12) 43. Posiedzenie plenarne Komitetu Konsultacyjnego Konwencji 108 Rady Europy. Strasburg, 16-18.11.2022 r.

43. posiedzenie plenarne Komitetu Konwencji 108 było pierwszym od trzech lat spotkaniem w formule stacjonarnej. Zgromadziło przedstawicieli ponad 70 państw i instytucji międzynarodowych, aby kontynuować prace rozpoczęte w ramach przyjętego programu pracy na lata 2022-2025. Komitet kontynuował prace nad wzorcowymi klauzulami umownymi w kontekście transgranicznych przepływów danych, nad międzypaństwową wymianą danych na potrzeby przeciwdziałania praniu pieniędzy i walce z finansowaniem terroryzmu, a także nad interpretacją art. 11 Konwencji 108+. Komitet zaprosił do udziału w swoich pracach dwie organizacje: Organizację Państw Amerykańskich (OAS) oraz Commission de l'Informatique et des Libertés (CIL) z Burkina Faso. Zajmował się także warunkami udziału Federacji Rosyjskiej w jego pracach, w odpowiedzi na wniosek Komitetu Ministrów Rady Europy z czerwca 2022 r. dotyczący konsekwencji jej agresji na Ukrainę. Podczas tego spotania, dwie laureatki Nagrody im. Stefano Rodoty 2022, Teresa Quintel i Sabrina Nucciotti, mogły zaprezentować swoje nagrodzone prace i odebrać nagrody[445]. Podczas 43. posiedzenia plenarnego Komitet Konwencji 108 przyjął Wytyczne dotyczące systemów tożsamości cyfrowej, które obok niewątpliwych korzyści mogą także przynieść negatywne konsekwencje dla praw człowieka osób fizycznych, społeczności i grup osób. Konsekwencje te mogą obejmować dyskryminację i wykluczenie, marginalizację, nieuzasadnione profilowanie i nadzór, utratę kontroli nad tożsamością lub nawet jej nadużycie lub kradzież. Wytyczne promują obiektywną ocenę wszystkich wchodzących w grę interesów, w tym korzyści płynących z tych systemów w porównaniu z ingerencją, jaką mogą one stanowić w prawa człowieka i podstawowe wolności. Wytyczne zawierają również zalecenia dla każdego rodzaju podmiotów w zakresie opracowywania i wdrażania takich systemów[446].

13) 57. posiedzenie Biura Komitetu Konsultacyjnego Konwencji nr 108. Strasburg, 15-16.12.2022 r.

Posiedzenie było okazją dla niedawno wybranego nowego Biura Komitetu do podsumowania roku 2022 i przygotowań do realizacji działań w roku 2023, zwłaszcza w odniesieniu do trwających prac nad interpretacją art. 11 zmodernizowanej konwencji, nad ochroną danych w zakresie przetwarzania danych osobowych do celów przeciwdziałania praniu pieniędzy i przeciwdziałania finansowaniu terroryzmu oraz

444 Dokumenty przyjęte podczas 44. Międzynarodowej Konferencji Global Privacy Assembly opublikowane są na stronie GPA: https://globalprivacyassembly.org/document-archive/

445 Pełny raport z posiedzenia znajduje się tutaj: https://rm.coe.int/tpd-43-abriged-report-en-final-2756-4125-3382-1/1680a91b70

446 Wytyczne dostępne są w języku angielskim: https://rm.coe.int/t-pd-2021-2rev9-guidelines-digital-identity-2761-5846-6310-2/1680a95e1e

nad aktualizacją wzorcowych klauzul umownych dotyczących przekazywania danych osobowych. Komitet przeprowadził również dyskusję na temat swojego programu prac na lata 2022-2025 i postanowił kontynuować prace normatywne nad ochroną danych osobowych w kontekście wyborów oraz skupić się na gwarancjach i zabezpieczeniach związanych z danymi biometrycznymi i innymi danymi szczególnie chronionymi w tym zakresie[447].

447 Pełny raport z posiedzenia znajduje się tutaj: https://rm.coe.int/t-pd-bureau-57-abridged-report-en-2762-9261-8246-3/1680a96b46

V. Podsumowanie

Na przestrzeni ostatnich lat obserwowany jest utrzymujący się wysoki wskaźnik liczby **skarg** wnoszonych do UODO przez osoby, których dane dotyczą. Taka tendencja z jednej strony wskazuje na problemy z przestrzeganiem przez administratorów prawa tych osób do ochrony danych, z drugiej jednak strony oznacza wzrost świadomości osób, których dane dotyczą, co do przysługujących im praw. Odnotowany w niniejszym Sprawozdaniu za 2022 rok prawie 7-tysięczny wpływ do Urzędu skarg osób, których dane dotyczą, należy oceniać właśnie w ten sposób.

Utrzymująca się tak duża liczba wpływających skarg stanowiła w roku 2022 duże wyzwanie dla UODO. Wraz ze wzrostem świadomości podmiotów danych, a także postępem technicznym, sprawy prowadzone w UODO są coraz bardziej skomplikowane i wielowątkowe. Wymagają ciągłego poszerzania przez pracowników UODO wiedzy, zarówno z zakresu prawa jak i innych dziedzin, co przekłada się na wysoką jakość merytoryczną ich pracy i wydawanych rozstrzygnięć. Pomimo bardzo dużej liczby spraw, którymi zajmował się UODO, w roku 2022 udało się zwiększyć liczbę spraw zakończonych wydaniem decyzji administracyjnej, przy zachowaniu wysokiej jakości merytorycznej rozstrzygnięć organu nadzorczego.

Podkreślenia wymaga, że dla ochrony danych osobowych kluczowe jest zapewnienie, by osoba, której dane są przetwarzane, mogła złożyć skargę do organu nadzorczego, gdy uzna, że dzieje się to z naruszeniem przepisów RODO. Natomiast rolą Prezesa Urzędu Ochrony Danych Osobowych jest zapewnienie, by ta skarga została rozpatrzona w sposób niezależny, prawidłowy i zgodny z przepisami. Rozpatrywanie skarg osób, których dane dotyczą, jest zadaniem, do którego Prezes UODO przykłada szczególną wagę, ponieważ prawidłowa realizacja tego zadania przyczynia się do ochrony tych osób, przed przetwarzaniem ich danych w sposób niezgodny z przepisami RODO.

RODO nadało osobom, których dane są przetwarzane, liczne narzędzia do kontroli przetwarzania ich danych. Wśród nich, jednym z najważniejszych, jest **prawo do uzyskania informacji na temat okoliczności przetwarzania danych osobowych,** o którym mowa w art. 15 RODO. To ono, w pierwszej kolejności, pozwala administratorowi wyjaśnić i usunąć wszelkie wątpliwości klienta dotyczące podstaw prawnych przetwarzania jego danych osobowych. Z kolei osobie, której dane dotyczą, pozwala skontrolować te podstawy, wykryć ewentualne nieprawidłowości lub nieaktualność przetwarzanych danych, a w następstwie podjąć decyzję co do dalszych działań.

Niestety, zarówno po stronie podmiotów danych, jak i administratorów, zauważa się tendencję do ignorowania obowiązków informacyjnych, zwłaszcza tego, który jest realizowany na wniosek. Skarżący często pomijają tę drogę, pomimo że w większości przypadków skorzystanie z niej wyjaśniłoby wszelkie wątpliwości co do okoliczności przetwarzania. Częstym przypadkiem jest sytuacja, w której podmiot danych nie podejmował żadnej próby kontaktu z administratorem, uciekając się wyłącznie do złożenia skargi.

Powodowało to zbędne wszczynanie postępowań w przypadkach, które tego nie wymagały. Często również skargi kierowane były wobec podmiotów, które nie są administratorami, a jedynie prowadzą marketing produktów lub usług tego podmiotu korzystając ze swoich własnych baz danych (marketing na zlecenie). Z kolei administratorzy często ignorują wezwania osób do udzielenia informacji. Jest to materia złożona, gdyż często w takiej korespondencji poruszane są roszczenia i skargi związane z realizacją samych usług (a więc roszczeniami na gruncie prawa cywilnego). Niewątpliwie kwestia ta wymaga uwagi administratorów, zwłaszcza szkoleń personelu w zakresie obsługi takich zgłoszeń.

Warto w tym miejscu zauważyć, że w styczniu 2022 r. opublikowano długo oczekiwane wytyczne Europejskiej Rady Ochrony Danych 01/2022 sprawie praw osób, których dane dotyczą – Prawo dostępu[448]. Wytyczne określają sposób realizacji tego obowiązku, zwłaszcza w kontekście dostępu do kopii danych, oraz wskazują wiele problemów z tym związanych.

W okresie sprawozdawczym 2022 roku, w toku prowadzonych **kontroli przestrzegania przepisów o ochronie danych osobowych,** Prezes UODO zwracał szczególną uwagę na przestrzeganie przez administratorów odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych osobowych, przeprowadzoną ocenę skutków dla ochrony danych osobowych oraz analizę ryzyka naruszenia praw lub wolności osób fizycznych, których dotyczyło naruszenie ochrony danych osobowych. Ocenie podlegały m.in. przesłanki legalności przetwarzania danych osobowych, w szczególności warunki wyrażenia zgody na przetwarzanie tych danych, w tym informacji o stanie zdrowia, umowy powierzenia przetwarzania danych osobowych, zabezpieczenia systemów informatycznych z uwzględnieniem mechanizmu tworzenia i weryfikacji kopii zapasowych, systemów antywirusowych/antyspamowych, jak również zabezpieczenia fizyczne pomieszczeń strategicznych dla bezpieczeństwa danych osobowych. Wątpliwości Prezesa UODO w kontrolowanych podmiotach wzbudziło przetwarzanie biometrycznych danych osobowych pod kątem spełniania jednego z warunków wskazanych w art. 9 ust. 2 RODO oraz w zakresie niezbędności i proporcjonalności identyfikacji do celów uwierzytelniania.

W analizowanym 2022 r. należy odnotować porównywalną do roku 2021 liczbę decyzji administracyjnych nakładających na administratorów **administracyjne kary pieniężne** oraz decyzji, w których udzielił upomnienia administratorom w związku ze stwierdzeniem **naruszenia ochrony danych osobowych.** Natomiast zaobserwować należy wzrost wysokości kar pieniężnych nakładanych przez organ nadzorczy za naruszenia przepisów o ochronie danych osobowych.

W zgłoszonych Prezesowi UODO **naruszeniach** będących przedmiotem postępowania administracyjnego, istotnym problemem był brak weryfikacji doboru i poziomu skuteczności stosowanych środków technicznych ocenianych przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do wiedzy technicznej, kosztów wdrożenia oraz charakteru,

448 Wytyczne dostępne są w języku angielskim pod adresem, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_pl

zakresu i celów przetwarzania, brak działań zmierzających do optymalnej konfiguracji wykorzystywanych systemów operacyjnych poprzez regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych, w postaci testów bezpieczeństwa w zakresie infrastruktury informatycznej oraz aplikacji, które powinny wynikać z przeprowadzonej analizy ryzyka, identyfikującej podatności odnoszące się do wykorzystywanych zasobów oraz wynikające z nich zagrożenia.

W ocenie Prezesa UODO istotnym z punktu widzenia naruszeń ochrony danych osobowych jest wdrożenie odpowiednich procedur pozwalających na wykrycie i zgłoszenie incydentu, dokonanie klasyfikacji i analizy zdarzenia, jego stopnia i rodzaju oraz dokonanie oceny skutków dla praw i wolności osób fizycznych, niezbędnej do podjęcia decyzji w przedmiocie notyfikacji naruszenia organowi nadzorczemu i zawiadomienia osób, których ten incydent dotyczy, a także sprawne podjęcie działań mających na celu m.in. ograniczenie rozmiaru naruszenia i odzyskanie dostępności do baz danych.

Urząd Ochrony Danych Osobowych nieustannie podejmuje szereg **działań edukacyjnych**, które wpisują się w misję organu nadzorczego. Poprzez edukację i informację upowszechnia w społeczeństwie wiedzę o ochronie danych osobowych i ryzyku, a także o przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienia tych zjawisk – poświęcając szczególną uwagę działaniom skierowanym do dzieci. Efektem takiego podejścia jest realizowany od 13 lat wspomniany już wcześniej w niniejszym Sprawozdaniu, ogólnopolski program edukacyjny dla szkół, uczniów i ośrodków doskonalenia nauczycieli „Twoje dane – Twoja sprawa". Dużym zainteresowaniem uczestników Programu cieszą się zwłaszcza materiały opracowane przez UODO – tzw. pigułki wiedzy z cyklu „Warto wiedzieć", które pozwalają zdobyć wiedzę z zakresu ochrony danych osobowych, szczególnie w środowisku cyfrowym oraz webinaria. Spotkania z ekspertami, zajęcia i współpraca z licznymi instytucjami, a także zaangażowanie rodziców czy seniorów w działania edukacyjne szkół miały znaczny wpływ na skuteczność podejmowanych działań w ramach Programu.

Podobnie jak w poprzednich edycjach Programu, stopień spełnienia oczekiwań uczestników był bardzo wysoki, o czym świadczą wysokie oceny tego przedsięwzięcia przez jego realizatorów – uczniów i nauczycieli. Nauczyciele podkreślali konieczność organizowania zajęć w tym obszarze tematycznym – jako niezbędny element zapewnienia bezpieczeństwa nauczania w szkole. Podkreślali też adekwatność tematyki programu do realiów społeczeństwa informacyjnego, uniwersalny zakres merytoryczny oraz duże zainteresowanie uczniów i nauczycieli tematyką prawa do prywatności i ochrony danych osobowych.

Wieloletnia realizacja Programu w szkołach przyczyniła się do kształtowania prawidłowych podstaw i nawyków dzieci i młodzieży w zakresie bezpieczeństwa, wzrostu świadomości w zakresie ochrony prywatności, popularyzacji wiedzy na temat ochrony

danych osobowych wśród uczniów i nauczycieli, a także wzrostu zainteresowania tematem. Program stanowi ważne źródło aktualnej wiedzy i dobrych praktyk w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty.

Warto również podkreślić ogromną rolę podmiotów współpracujących i popierających działania edukacyjne Urzędu Ochrony Danych Osobowych m.in. Rzecznika Praw Dziecka, Ministra Edukacji i Nauki, co jest dowodem na to, że temat ten jest ważny i niezbędny w edukacji dzieci i młodzieży. Coraz więcej dyrektorów szkół widzi również potrzebę podniesienia świadomości nauczycieli w organizacji procesu edukacji oraz współpracę z inspektorem ochrony danych osobowych.

Działania edukacyjne są kluczowe dla budowania świadomości społeczeństwa. Dlatego Urząd Ochrony Danych Osobowych nie ustaje w popularyzowaniu wiedzy o ochronie danych osobowych poprzez organizację szkoleń, konferencji, seminariów, debat naukowych i różnych spotkań dotyczących ochrony danych osobowych. Współpracuje ze szkołami wyższymi, a eksperci UODO wspierają swoją wiedzą ważne wydarzenia przeznaczone również dla inspektorów ochrony danych. Podczas webinariów adresowanych do IOD-ów, prezentowane były oczekiwania społeczeństwa względem nich oraz obowiązki administratora, takie jak np. wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających bezpieczeństwo danych i zgodność ich przetwarzania z przepisami RODO. Ponadto opracowane zostałyśmy poradniki, wytyczne i podręczniki dla IOD w ramach działań prowadzonych wspólnie z organami nadzorczymi innych państw. Jeśli chodzi o efektywność podejmowanych działań, to bardziej niż z narzędziami jest ona związana z otwartością na potrzeby odbiorców, tj. administratorów, inspektorów ochrony danych oraz wszystkich zainteresowanych tematem ochrony danych osobowych i prywatności. Wielokierunkowość tych działań pozwala docierać do różnych grup odbiorców z konkretnym, dopasowanym do ich potrzeb przekazem. Przykładem może być czas pandemii, który pokazał, że UODO potrafi szybko odpowiedzieć na zapotrzebowanie administratorów i IOD w zakresie dostarczenia wiedzy na temat tego, jak bezpiecznie przetwarzać dane osobowe podczas pracy czy nauki zdalnej.

Prowadzone od chwili rozpoczęcia stosowania RODO działania organu nadzorczego, zapewniają wielu różnym środowiskom wsparcie eksperckie na etapie tworzenia oraz stosowania prawa. Dzięki podejmowanym przez UODO działaniom, takim jak przedstawianie opinii w toku procesów legislacyjnych czy kierowanie wystąpień legislacyjnych, udało się zapobiec wejściu w życie lub wyeliminować z obrotu prawnego przepisy nieprzejrzyste, niezapewniające poszanowania gwarantowanych przez RODO praw osób, których dane są przetwarzane.

W roku 2022 organ nadzorczy brał udział w prekonsultacjach tak istotnych projektów przepisów, jak m.in. ustawa o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw[449] oraz rozporządzenie Ministra Zdrowia w sprawie badań na obecność alkoholu lub środków

449 DOL.401.237.2021.

działających podobnie do alkoholu w organizmie pracownika[450].

Tego typu działania sprzyjają wypracowaniu przepisów zgodnych z zasadami określonymi w RODO, a jednocześnie klarownych, spójnych i niebudzących wątpliwości interpretacyjnych.

Warto podkreślić, że na skutek uwag organu nadzorczego w toku prac legislacyjnych w przyjmowanych przepisach udało się wprowadzić wiele istotnych zmian. Przykładowo w projekcie ustawy o badaniach klinicznych stosowanych u ludzi[451] projektodawca zgodził się z koniecznością doprecyzowania tworzonych przepisów m.in. w zakresie wyłączeń stosowania przepisów RODO na rzecz jedynie ich ograniczenia, uwzględniając przy tym poszczególne etapy badania klinicznego. W projekcie pojawiły się rozwiązania, które stanowią ciekawy przykład godzenia praw z zakresu badań klinicznych i ograniczenia praw osób, których dane mają być przetwarzane. Ponadto powyższe ograniczenia zostały przez projektodawcę doprecyzowane w zakresie konkretnego etapu badania klinicznego, jak również uwzględnił on dane osobowe, które nie będą podlegały powyższym ograniczeniom. Dodatkowo po zgłoszonych uwagach projekt uzupełniono o przepisy dotyczące bezpieczeństwa danych.

Przykładem projektu aktu normatywnego, w którym po zgłoszeniu uwag przez organ nadzorczy uwzględniono przepisy sprzyjające realizacji standardów RODO, był projekt ustawy o usprawnieniu procesu inwestycyjnego Centralnego Portu Komunikacyjnego[452]. Organ kwestionował propozycję projektodawcy przewidującą, że dla realizacji przez spółkę zadania, jakim ma być budowa i utrzymanie Centralnego Portu Komunikacyjnego, miałoby zostać jej przyznane uprawnienie do przetwarzania nieograniczonego katalogu danych przez nieokreślony okres. Projektodawca uwzględnił większość uwag zgłoszonych do omawianego projektu.

Również w projekcie ustawy o szczególnych rozwiązaniach służących ochronie odbiorców niektórych paliw stałych w związku z sytuacją na rynku paliw[453] projektodawca uwzględnił zgłoszone zastrzeżenia i usunął z projektu przepisy przewidujące utworzenie bazy danych pełnoletnich osób fizycznych zainteresowanych zakupem paliwa stałego na potrzeby własnego gospodarstwa domowego.

Także w toku prac legislacyjnych dotyczących projektu ustawy o Centralnej Informacji Emerytalnej[454] znaczna część uwag zgłoszonych przez UODO w 2019 r. została uwzględniona w *de facto* nowym projekcie ustawy o Centralnej Informacji Emerytalnej z 2022 r.

Powyższe działania są przykładem na to, że przy tworzeniu prawa możliwe jest wypracowanie norm, które stanowią pewien balans pomiędzy koniecznością uregulowania określonych zagadnień (celu regulacji) a zachowaniem spójności z przepisami o ochronie danych. Niestety stanowią one niewielką część opiniowanych projektów. Nadal, w opinii organu nadzorczego, jest wiele przepisów oraz kwestii, które wymagają analizy, dyskusji

450 DOL.401.633.2022.
451 DOL.401.196.2021.
452 DOL.401.564.2021.
453 DOL.401.298.2022.
454 DOL.401.207.2022.

oraz wprowadzenia stosownych zmian.

Po stronie sukcesów warto odnotować zatwierdzenie przez Prezesa UODO pod koniec 2022 r. pierwszego w Polsce kodeksu postępowania – **„Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych"** – i udzielenie akredytacji podmiotowi, który będzie monitorował jego przestrzeganie. 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 z uwzględnieniem specyfiki danej branży), przynosi wiele korzyści[455]. Administratorom i podmiotom przetwarzającym będącym członkami kodeksu ułatwia stosowanie przepisów i wypełnianie wielu obowiązków, wskazuje właściwe rozwiązania tam, gdzie istnieją dylematy. Pomaga też odpowiednio organizować system ochrony danych osobowych w danej branży, podnosząc jego poziom. Jego wdrożenie jest korzystne nie tylko dla administratorów i podmiotów przetwarzających, ale również dla osób, których dane są przetwarzane, gdyż dodatkowo będą one mogły liczyć na zbliżony standard ochrony danych oraz obsługę w zakresie realizacji ich praw przez daną branżę.

Odpowiednio przygotowany kodeks jest nie tylko gwarancją pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy. Administratorzy mogą także liczyć na nadzór nad procesami przetwarzania danych osobowych przez niezależny podmiot monitorujący kodeks. Podmioty monitorujące w celu uzyskania akredytacji organu nadzorczego muszą wykazać swoją niezależność w stosunku do twórcy kodeksu oraz posiadanie odpowiednich: zasobów finansowych, personalnych, środków organizacyjnych i materialnych (technicznych). Szczegółowe wymagania w tym zakresie zostały opisane w Wymogach akredytacji podmiotów monitorujących kodeksy postępowania przygotowanych przez Prezesa UODO. Natomiast kodeksy obejmujące podmioty sektora publicznego, choć nie podlegają obowiązkowi wskazania podmiotu monitorującego, to muszą zawierać skuteczny 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 jego projektem, a nawet całkowite

455 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.).

zaniechanie przygotowania takiego dokumentu[456].

Tym bardziej cieszy to, że w Polsce wraz z rozpoczęciem stosowania RODO wiele organizacji zainicjowało prace nad stworzeniem branżowych kodeksów postępowania. Złożone do organu nadzorczego wnioski o zatwierdzenie projektów kodeksów, ale też sygnały od inicjatyw, które rozpoczynają prace związane z opracowaniem tego mechanizmu rozliczalności wskazują, że zarówno podmioty publiczne (np. sądy, jednostki samorządu terytorialnego), jak i prywatne (np. centra handlowe, stowarzyszenie marketingu) dostrzegają potrzebę i zalety korzystania z tego typu narzędzia, które pozwoli im wykazać rozliczalność, o której mowa w art. 5 ust. 2 RODO.

W tym kontekście cenne będą pierwsze doświadczenia związane z funkcjonowaniem zatwierdzonego kodeksu postępowania **dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych.** W 2023 r. organ nadzorczy z uwagą będzie śledził ten proces.

Innym mechanizmem umożliwiającym wykazanie wywiązania się przez administratora lub podmiot przetwarzający z ciążących na nich obowiązków określonych w RODO jest **certyfikacja.** W Polsce, co wynika z ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, został przyjęty następujący model w tym zakresie. Certyfikacja będzie udzielana przez Prezesa UODO lub podmioty certyfikujące. Z treści procedowanego przed EROD projektu dodatkowych wymogów akredytacji podmiotów certyfikujących w rozumieniu art. 43 ust. 3 RODO, opracowanego przez polski organ nadzorczy wynika, że certyfikacji w Polsce będą udzielały wyłącznie podmioty certyfikujące akredytowane przez Polskie Centrum Akredytacji, czyli krajową jednostkę akredytującą w rozumieniu art. 43 ust. 1 lit. b RODO. Administratorzy i podmioty przetwarzające, którzy zamierzają certyfikować swoje procesy przetwarzania, będą w pierwszej kolejności przygotowywać kryteria certyfikacji, które będą podlegały zatwierdzeniu przez Prezesa UODO. W opinii organu nadzorczego indywidualny charakter takiej certyfikacji oraz prace nad europejskimi programami certyfikacji będą miały mniejszy wpływ na poszczególne branże niż przyjmowanie standardów wypracowanych w ramach kodeksów postępowania.

456 Do najczęstszych błędów popełnianych przez środowiska pracujące nad projektami kodeksów postępowania należą:

– brak jasnego i zwięzłego uzasadnienia, w którym przedstawia się szczegółowe informacje o celu kodeksu, zakresie jego stosowania oraz sposobie, w jaki ułatwi on skuteczne stosowanie RODO,

– wnioskowanie o zatwierdzenie kodeksu przez podmiot, który nie reprezentuje większości sektora,

– brak podmiotu, który podjąłby się roli wnioskodawcy w postępowaniu o zatwierdzenie kodeksu,

– zbyt wąski zakres przeprowadzonych konsultacji (np. nieobejmujący w ogóle osób, których dane dotyczą – użytkowników albo klientów czy organizacji działających na ich rzecz) oraz przedstawianie zbyt szczegółowego sprawozdania z konsultacji,

– zbyt kompleksowe/szerokie podejście do zagadnień przetwarzania danych zamiast rozstrzygnięcia najważniejszych problemów sektora, co powoduje niemożność zatwierdzenia kodeksu ze względu na istnienie zbyt wielu kwestii spornych, które trudno jest rozstrzygnąć w jednym dokumencie (warto w tym miejscu zwrócić uwagę na brzmienie ustępu 2 art. 40 RODO – wymieniono w nim zagadnienia, jakie mogą obejmować kodeksy postępowania, ale wyliczenie to ma charakter przykładowy i nie jest wyliczeniem wyczerpującym, tzn. nie wszystkie wskazane w nim zagadnienia muszą być uregulowane w kodeksie),

– przepisanie w kodeksie przepisów RODO lub ustawy o ochronie danych osobowych bez praktycznego wyjaśnienia ich stosowania,

– niewskazanie w kodeksie przepisów sektorowych oraz wytycznych, opinii oraz stanowisk EROD w odniesieniu do konkretnego sektora lub konkretnej czynności przetwarzania lub tylko ogólne ich wskazanie bez odniesienia się do konkretnych przepisów związanych z przetwarzaniem danych osobowych w sektorze, dla którego powstał kodeks,

– niepowoływanie się przez twórców na istniejące orzecznictwo rozstrzygające zagadnienia regulowane w kodeksie,

– brak wypracowania odpowiednich mechanizmów umożliwiających monitorowanie kodeksu.

Niezwykle istotnymi, podjętymi przez organ nadzorczy w roku 2022, działaniami w zakresie doskonalenia kultury ochrony danych osobowych, a mającymi na celu przyczynienie się do zagwarantowania właściwego funkcjonowania IOD, były podjęte kontrole oraz towarzysząca im akcja informacyjno-edukacyjna. Na te potrzeby przygotowana została lista 27 pytań obejmujących kluczowe obowiązki administratorów odnoszące się do zagwarantowania IOD prawidłowego statusu oraz umożliwienie prawidłowego wykonywania zadań. Wezwania do udzielenia na nie odpowiedzi oraz odpowiedniego udokumentowania składanych wyjaśnień zostały przesłane do wybranych administratorów i podmiotów przetwarzających. Jednocześnie informacje na ten temat zostały zamieszczone na stronie internetowej Urzędu, a także w „Newsletterze UODO dla IOD". Dodatkowo w newsletterze organ – zwracając uwagę, iż sukcesywnie podejmował działania edukacyjne w zakresie właściwego postrzegania roli i zadań IOD – przygotował i opublikował zestawienie wyjaśnień i stanowisk w kwestiach objętych kontrolą.

Powyższe działania organu nadzorczego zostały pozytywnie odebrane nie tylko przez inspektorów ochrony danych, ale również przez administratorów i podmioty przetwarzające. Inspektorzy uznali je – zgodnie z intencją organu – za zwracające uwagę na ich szczególną pozycję i rolę, a jednocześnie będące dla nich wsparciem i mające przełożenie na prawidłowe i efektywne wypełnianie przez nich ich funkcji. Natomiast administratorzy i podmioty przetwarzające wspomnianą listę 27 pytań wykorzystywali do autokontroli w tym zakresie.

Dla organu nadzorczego wspieranie IOD we właściwym wypełnianiu przez nich ich funkcji, w tym weryfikowanie przestrzegania przez podmioty powołujące IOD przepisów dotyczących ich funkcjonowania, czy udzielanie konsultacji we wszelkich sprawach, którymi się zajmują, to niezmiernie ważna kwestia. Inspektorzy ochrony danych, którzy dysponują odpowiednią *wiedzą* i umiejętnościami, a także mają odpowiednią pozycję w organizacji, w której funkcjonują, stanowią bowiem fundament skutecznego systemu ochrony danych osobowych. Dla administratora realizują bowiem istotne funkcje: weryfikacyjną i doradczą. Jednocześnie pełnią inną ważną rolę – punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą, oraz między administratorem lub podmiotem przetwarzającym a organem nadzorczym.

Podnoszeniu poziomu ochrony danych osobowych służy też **udzielanie odpowiedzi na pytania.** Dla organu nadzorczego są one jednocześnie ważnym sygnałem wskazującym na istnienie problemów w konkretnym obszarze i umożliwiającym szybkie reagowanie na nie, m.in. w formie komunikatów publikowanych na stronie internetowej UODO lub kierowania do właściwych podmiotów wystąpień postulujących zmianę przepisów prawa bądź stosowanej praktyki.

Przykładem szybkiej reakcji na pojawiające się problemy związane z przetwarzaniem danych osób przybywających z Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, było opublikowanie na stronie internetowej UODO komunikatu[457] wskazującego,

457 https://www.uodo.gov.pl/pl/138/2436

że wszelkie działania podejmowane na rzecz przebywających w Polsce obywateli Ukrainy powinny odbywać się z poszanowaniem prawa do ochrony danych osobowych i prawa do prywatności. Organ nadzorczy przypomniał, że niosąc pomoc z myślą o uchodźcach z Ukrainy, należy odpowiednio wyważyć ingerowanie w prawa podstawowe i weryfikować, czy procesy ułatwiające i koordynujące pobyt Ukraińców w Polsce nie ingerują w sposób nadmiarowy w prywatność uchodźców, czy wynikają z przepisów prawa, czy są z nimi zgodne itp.

Kolejne wskazówki w tym zakresie zawarte zostały w zamieszczonym na stronie internetowej UODO materiale „O ochronie danych osobowych osób przybywających z Ukrainy podczas Forum IOD”[458], który jest relacją ze szkolenia dla inspektorów ochrony danych z jednostek samorządowych z Wielkopolski i zawiera wyjaśnienia dotyczące m.in. podstaw przetwarzania danych osobowych osób przybywających z Ukrainy i dopełniania wobec nich obowiązku informacyjnego.

Z kolei reagując na pytania od administratorów oraz inspektorów ochrony danych z ośrodków pomocy społecznej i gmin dotyczące podstawy prawnej pozyskiwania danych osobowych szczególnych kategorii (np. informacji o niepełnosprawności) przez podmiot, który decyduje o przedłużeniu okresu przyznania świadczenia pieniężnego przysługującego z tytułu zapewnienia zakwaterowania i wyżywienia obywatelom Ukrainy, Prezes UODO skierował do Ministra Spraw Wewnętrznych i Administracji wystąpienie[459] zawierające wniosek o zmianę obowiązujących przepisów, uzyskując zapewnienie, że zostaną one skorygowane możliwie szybko.

W opinii organu nadzorczego wciąż jest jeszcze wiele, niekiedy podstawowych kwestii, które wymagają analizy, dyskusji oraz wprowadzenia stosownych zmian, czego wyrazem są wciąż sygnalizowane przez IOD problematyczne zagadnienia, np. luki w przepisach. Nadal konieczny jest przegląd przepisów dotyczących wykorzystywania i upubliczniania numeru PESEL, który jest krajowym numerem identyfikacyjnym w rozumieniu RODO. Niektóre polskie regulacje budzą wątpliwości, co do zgodności z art. 87 RODO, zgodnie z którym krajowego numeru identyfikacyjnego można używać wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, przewidzianych w RODO. Propozycje projektodawców nie nawiązują do tych zabezpieczeń i ich nie przewidują. Tymczasem ujawnienie numeru PESEL może powodować szereg ryzyk, w tym ryzyko kradzieży tożsamości, gdy trafia on do osoby niepowołanej, jak również gdy jest zestawiany z innymi danymi i wykorzystywany w innych celach niż pierwotnie wskazane, określone przepisami. Na szczególne ryzyka są tym bardziej narażone osoby, których PESEL jest powszechnie dostępny w rejestrach publicznych i to bez określenia żadnych dodatkowych warunków wykorzystania danych. W tej bowiem sytuacji prowadzący taki rejestr, upowszechniając PESEL, traci automatycznie kontrolę nad tym, kto i w jakich celach oraz w jaki sposób będzie dalej dane te wykorzystywał. Z drugiej strony natomiast istnieją ryzyka

458 https://uodo.gov.pl/pl/138/2439
459 DOL.413.18.2022.

związane z dalszym przetwarzaniem numerów PESEL przez kolejnych administratorów w celach innych niż pierwotny cel pozyskania tych identyfikatorów. Powyższy problem jest wielokrotnie i systematycznie poruszany przez organ nadzorczy, przy okazji opiniowania projektów aktów prawnych, jak i w toku realizacji innych zadań organu nadzorczego. W 2022 r. organ wyraził swoje wątpliwości w tym zakresie m.in. opiniując projekt ustawy o aplikacji mObywatel[460].

Niepokojącym trendem, który stale jest i nadal będzie przedmiotem szczególnego zainteresowania i troski organu nadzorczego, jest tworzenie przepisów przewidujących **przetwarzanie danych osobowych, często na wielką skalę lub prowadzących do łączenia różnych baz i rejestrów, bez wnikliwej analizy wszystkich aspektów przetwarzania, bez oceny wiążących się z tym ryzyk, a często regulujących kwestie związane z pozyskiwaniem danych osobowych przepisami rangi rozporządzenia, a nie ustawy.** Przykładem takich budzących zastrzeżenia rozwiązań jest wskazany już projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji[461] czy projekt rozporządzenia Rady Ministrów w sprawie zakresu danych i wykazu rejestrów publicznych i systemów teleinformatycznych, z których udostępniane są dane na potrzeby prowadzenia analiz w ramach zintegrowanej platformy analitycznej[462], do których Prezes UODO zgłosił liczne uwagi na różnych etapach procesu legislacyjnego.

Dla organu nadzorczego wyzwaniem będzie weryfikowanie zapewniania, w tym przez prawodawcę, właściwej **ochrony danych osobowych przetwarzanych przy użyciu chmur, aplikacji, portali, wspólnych systemów czy innych rozwiązań informatycznych**. Są one coraz powszechniej stosowane, lecz najczęściej tworzone z pominięciem określonych w RODO zasad. Jest to niezwykle istotne, gdyż przepisy RODO wymagają, by każde przetwarzanie danych osobowych było planowane z uwzględnieniem koncepcji ochrony danych (i prywatności) w fazie projektowania (*privacy by design*), ale i w czasie samego przetwarzania. W sytuacji, gdy twórca przepisów przewiduje, że przetwarzanie danych osobowych będzie prowadzone z wykorzystaniem określonych rozwiązań informatycznych, to od samego początku, na każdym etapie projektowania ich wykorzystywania, pod uwagę powinien brać wpływ, jaki ich stosowanie będzie wywierało na prywatność osób, których dane dotyczą. Uwzględniać przy tym powinien także stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych, a jednocześnie tak powinien projektować planowane cyfrowe rozwiązania, by były odpowiednie dla konkretnego przypadku, a jednocześnie pozbawione były na jak najwyższym poziomie ryzyk naruszeń praw i wolności podmiotów danych. Pożądane jest, by aspekt ważenia ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze brać pod uwagę już na etapie projektowania rozwiązań prawnych. Oprócz uwzględniania ochrony danych w fazie projektowania (art. 25 ust. 1 RODO) równie istotne jest też wdrożenie mechanizmów zapewniających stosowanie zasady domyślnej ochrony danych

460 DOL.401.276.2022.
461 DOL.401.169.2022.
462 DOL.401.624.2021.

(art. 25 ust. 2 RODO). Zasadę tę należy rozumieć jako postulat uwzględnienia jak najdalej posuniętych gwarancji, środków ochrony praw i wolności, w tym zabezpieczeń prywatności w ustawieniach początkowych każdego systemu. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego mają być zbierane (minimalizacja danych). Rozwiązania prawne powinny być skonstruowane tak, by wypełnianie celów prawodawcy następowało ze spełnieniem wskazanych w RODO funkcjonalności i zasad, a z drugiej strony pozwalało na zachowanie gwarantowanej w RODO neutralności technologicznej. Jeśli zaś w przetwarzaniu danych z wykorzystaniem nowoczesnych rozwiązań informatycznych uczestniczyć będą różne podmioty, ważne jest precyzyjne określenie ich ról oraz praw i obowiązków tak, by w sposób niebudzący wątpliwości wiadomo było, kto, w związku z jakimi etapami operacji na danych osobowych jest odpowiedzialny za to przetwarzanie (w tym m.in. pozyskiwanie czy udostępnianie danych). Nie bez znaczenia w kontekście art. 25 RODO jest też uwzględnianie ochrony danych w czasie samego przetwarzania określonego przepisami prawa, stąd w uzasadnionych przypadkach uwagi organu do projektowanych przepisów przyjmują również charakter *de lege ferenda*. Przykładem takich działań są np. uwagi zgłoszone w czasie prac nad projektem rozporządzenia Ministra Finansów w sprawie korzystania z e-Urzędu Skarbowego[463], w których podniesiono, że zarówno w ustawie o automatyzacji załatwiania niektórych spraw przez KAS, jak i w projekcie analizowanego rozporządzenia nie wskazano, jakie konkretnie podmioty i w jakim zakresie będą użytkownikami konta w e-Urzędzie Skarbowym.

Uwagi o charakterze *de lege ferenda* organ nadzorczy przedstawił, opiniując programy pilotażowe dotyczące zdrowia, których projektodawcą jest minister właściwy do spraw zdrowia (np. projekt rozporządzenia Ministra Zdrowia zmieniającego rozporządzenie w sprawie programu pilotażowego opieki nad świadczeniobiorcą w ramach sieci kardiologicznej[464]). Zwrócił uwagę, że szczegółowe rozwiązania dotyczące wzajemnego przepływu danych powinny zostać uregulowane wprost w przepisach rangi ustawy, a nie w umowach o współpracy zawartych pomiędzy podmiotami leczniczymi realizującymi program pilotażowy.

W najbliższym czasie wyzwaniem dla projektodawców będzie także przegląd prawa tworzonego na potrzeby realizacji zadań mających na celu ograniczenie i złagodzenie skutków pandemii COVID-19. Epidemia COVID-19 wymusiła wprowadzenie do polskiego porządku prawnego nowych, ale jednocześnie mających charakter epizodyczny, rozwiązań normatywnych umożliwiających funkcjonowanie zarówno ludzi i innych podmiotów z sektora prywatnego, jak i publicznego, w tym organów państwa w nadzwyczajnych warunkach. Organ nadzorczy w swoich opiniach legislacyjnych wskazywał wielokrotnie, że rozumie konieczność i cele wprowadzanych rozwiązań, w tym w zakresie dostosowywania różnych instytucji prawnych do sytuacji, w której niemożliwy jest bezpośredni kontakt między osobami (obywatelami) a instytucjami państwa powołanymi do rozpatrywania konkretnych spraw. Przepisy RODO odnoszą się do tego problemu i przewidują tak istotną przesłankę,

463 DOL.401.314.2022.
464 DOL.401.389.2022.

jak „ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi" – art. 6 ust. 1 lit. e[465] oraz art. 9 ust. 2 lit. i[466]. W tej sytuacji istotne jest zachowanie odpowiedniej hierarchii aktów prawnych, tj. regulowanie fundamentalnych kwestii związanych z ochroną danych osobowych ustawą, a nie rozporządzeniem oraz przeprowadzenie w procesie tworzenia i przyjmowania prawa tzw. testu prywatności, zważenia ryzyk dla praw i wolności pomiotów danych, ale i dla wykonawców norm, tj. oceny skutków dla ochrony danych, o której mowa w art. 35 ust. 10 RODO – szczególnie w przypadku innowacyjnych rozwiązań informatycznych oraz w związku z przetwarzaniem danych o szczególnym charakterze, danych sensytywnych. Przy tej okazji organ podkreślał, że zawieranie określonych norm w przepisach wykonawczych, które jednak powinny być zawarte w akcie rangi ustawy, zwłaszcza jeśli kształtują prawa i obowiązki w ogólności albo w części nieobowiązujące jeszcze w porządku prawnym, jest sprzeczne z zasadami wynikającymi z Konstytucji RP. Takie działania powodują stanowienie prawa nieodpowiadającego obowiązującym zasadom, chaos legislacyjny oraz przyczyniają się do zwiększenia niestabilności prawa, gdyż mogą być zmieniane z dnia na dzień, w dodatku poza jakąkolwiek kontrolą parlamentu oraz prezydenta. Dlatego po zakończeniu pandemii COVID-19 konieczny jest przegląd systemu prawa dla wyeliminowania z niego rozwiązań, którym nie nadano charakteru epizodycznego, a które są zbędne/nieadekwatne z punktu widzenia podstawowych praw i wolności osób fizycznych, w tym prawa do prywatności. Będzie to jednak zadanie przede wszystkim dla projektodawców, a organ nadzorczy będzie mógł się włączyć do niego w roli eksperckiej. Dodatkowo podobne działania powinny zostać również podjęte przez administratorów. Powinni oni rozważyć, czy nie przetwarzają danych nadmiarowych, zbędnych, gdyż zamierzony cel został osiągnięty, a nie ma innej podstawy legalizującej takie działanie.

Wyzwań nie brakuje też na poziomie unijnym. Jednym z nich jest prawne uregulowanie kwestii ochrony prywatności i danych osobowych w związku z niezwykle dynamicznym rozwojem nowych technologii, w tym m.in. z coraz powszechniejszym wykorzystywaniem **sztucznej inteligencji, internetu rzeczy, stosowaniem zwodniczych wzorców projektowych** (tzw. *deceptive patterns)*, **tworzeniem szczegółowych profili, na podstawie których dobierany jest przekaz reklamowy czy budową ogólnoeuropejskiego systemu tożsamości cyfrowej.**

Dalsze zacieśnianie współpracy organów nadzorczych, harmonizacja stosowania i egzekwowania RODO to kolejne wyzwania na najbliższy czas. Dostrzega je zarówno Komisja Europejska, jak i Europejska Rada Ochrony Danych (EROD), której Prezes UODO jest członkiem. **Członkowie EROD, na spotkaniu, które odbyło się w Wiedniu 27–28 kwietnia 2022 r., uzgodnili dalsze zacieśnianie współpracy w sprawach strategicznych**

465 Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

466 Przetwarzanie szczególnych kategorii danych osobowych jest dozwolone prawem gdy: i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

oraz zróżnicowanie zakresu stosowanych metod współpracy[467].

W tym kontekście warto podnieść inne ważne zagadnienie, jakim jest spójność orzecznictwa sądowego. Ważnym, sprzyjającym temu działaniem Prezesa UODO jest analiza wniosków w sprawach prejudycjalnych wniesionych do TSUE. Prezes UODO – na podstawie informacji przesłanych przez Pełnomocnika RP przed TSUE– przygotowuje stanowiska w kwestiach dotyczących zasadności udziału RP w tych postępowaniach, opracowuje pisemne analizy skutków orzeczeń TSUE na ustawodawstwo krajowe, a także przygotowuje odpowiedzi na pytania TSUE na rozprawę czy zasadności udziału w rozprawach, oczywiście w zakresie spraw, których przedmiotem jest ochrona danych osobowych. Realizacja tego zadania jest pracochłonna i wymaga analizy wielu aktów prawa krajowego i unijnego. Co jednak ważne, stanowiska organu nadzorczego prezentowane w tym obszarze opierają się również na wytycznych EROD i orzecznictwie, co może sprzyjać harmonizacji podejścia do kwestii będących przedmiotem postępowań.

Jednocześnie warto zauważyć rosnącą liczbę **postępowań prejudycjalnych dotyczących ochrony danych osobowych.** Wskazuje to, z jednej strony, na wzrost świadomości osób, których dane dotyczą, co do ich praw, ale z drugiej dla ustawodawcy unijnego i krajowego jest jednocześnie sygnałem, że mimo iż zasady ochrony danych osobowych zostały uregulowane dla Unii Europejskiej i Europejskiego Obszaru Gospodarczego w rozporządzeniu, to jednak pojawiają się rozbieżności, których sądy krajowe nie mogły samodzielnie rozstrzygnąć[468].

Prezes UODO z uwagą śledzi też orzecznictwo sądów krajowych, które w niektórych przypadkach niepokojąco zaczyna odbiegać od rozstrzygnięć sądowych zapadających w pozostałych państwach UE. Przykładem takich wyroków są m.in. wyroki Naczelnego Sądu Administracyjnego uznające, że numery rejestracyjne pojazdów nie są danymi osobowymi[469].

Zupełnie odosobnione poglądy polska judykatura zaprezentowała też w wyroku z 19 kwietnia 2022 r. dotyczącym Mircosoftu[470], w którym sąd orzekł, że renoma dostawcy usługi jest wystarczająca, aby uznać, że daje on wystarczające gwarancje bezpieczeństwa w rozumieniu art. 28 ust. 1 RODO[471].

Biorąc pod uwagę powyższe niepokojące tendencje i sygnały, Prezes UODO za

467 Więcej informacji na ten temat dostępnych jest na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/2549

468 W tym kontekście warto wspomnieć o pierwszej polskiej sprawie przed TSUE dotyczącej ochrony danych osobowych. Sąd odsyłający zadał pytanie, czy art. 5 ust. 1 lit. a) w zw. z art. 6 ust. 1 lit. a), c), e) w zw. z art. 6 ust. 3 RODO należy wykładać w ten sposób, że stoi na przeszkodzie takiemu unormowaniu prawa krajowego, które pozwala na sprzedaż w postępowaniu egzekucyjnym bazy danych w rozumieniu art. 1 ust. 2 dyrektywy 96/9/WE 2 Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych, składającej się z danych osobowych, jeśli osoby, których te dane dotyczą, nie wyraziły zgody na taką sprzedaż. Polski organ nadzorczy w opinii przygotowanej dla Pełnomocnika RP (DOL.0623.28.2022) wskazał m.in., iż w obowiązującym porządku prawnym nadal brak jest przepisów regulujących postępowanie komorników w przypadku sprzedaży zbiorów danych w toku postępowania egzekucyjnego. Komornik nie jest też w świetle aktualnie obowiązujących przepisów egzekucyjnych zobowiązany do weryfikacji danych w bazach. Brak jest także regulacji wskazujących, kto będzie odpowiedzialny za respektowanie praw osób, których dane dotyczą. Zarówno w obecnej, jak i w przyszłej regulacji tej kwestii prawa osób muszą być zagwarantowane niezależnie od tego, czy postępowanie egzekucyjne jest w toku, czy też zostało zakończone.

469 Por. sygn. akt I OSK 2063/17, III OSK 1522/21, III OSK 1466/21.

470 Sygn. akt II SA/Wa 2259/21.

471 Art. 28 ust. 1 RODO: „Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą".

potrzebne uznaje stałe upowszechnianie wiedzy na temat orzecznictwa TSUE, ETS, sądów krajowych z państw członkowskich UE oraz wytycznych EROD, co powinno przyczynić się do spójności wykładni RODO.

ZAŁĄCZNIKI

Załącznik nr 1

Wykaz administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2022 r.

L.p.	Data decyzji	Departament UODO prowadzący postępowanie	Sygnatura	Wysokość kary w zł
1.	19.01.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.33.2021	545 748,00
2.	19.01.2022 r.	Departament Kontroli i Naruszeń	DKN.5130.2215.2020	4 911 732,00
3.	19.01.2022 r.	Departament Kontroli i Naruszeń	DKN.5130.2215.2020	250 135,00
4.	23.03.2022 r.	Departament Kar i Egzekucji	DKE.561.18.2021	2 285,00
5.	18.05.2022 r.	Departament Kontroli i Naruszeń	DKN.5110.12.2021	15 994,00
6.	31.05.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.51.2021	10 000,00
7.	06.07.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.27.2022	60 000,00
8.	06.07.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.34.2021	10.000,00
9.	18.08.2022 r.	Departament Kar i Egzekucji	DKE.561.23.2021	4 569,00
10.	30.08.2022 r.	Departament Kar i Egzekucji	DKE.561.25.2021	31 988,00
11.	31.08.2022 r.	Departament Kar i Egzekucji	DKE.561.5.2022	6 854,00
12.	07.09.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.29.2022	2 500,00
13.	05.10.2022 r.	Departament Kar i Egzekucji	DKE.561.15.2021	9 139,00
14.	02.11.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.8.2022	8 000,00
15.	03.11.2022 r.	Departament Kontroli i Naruszeń	DKN.5131.18.2022	250 000,00
16.	16.11.2022 r.	Departament Kontroli i Naruszeń	DKN.5112.1.2020	1 599 395,00
17.	23.11.2022 r.	Departament Kar i Egzekucji	DKE.561.6.2021	22 849,00
18.	30.11.2022 r.	Departament Kontroli i Naruszeń	DKN.5112.5.2021	45 697,00
19.	29.12.2022 r.	Departament Kar i Egzekucji	DKE.561.30.2022	36 558,00
20.	30.12.2022 r.	Departament Kar i Egzekucji	DKE.561.20.2022	27 418,00

Załącznik nr 2

Wykaz wydarzeń objętych patronatem Prezesa UODO w 2022 r.

1. Konferencja Rzeczowo o Prawie, pt. „Ochrona Danych Osobowych – wyzwania 2022". Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp.k., 26.01.2022 r.

2. Konferencja z okazji VII Dnia IOD pt. „Wyzwania i standardy dla Inspektorów Ochrony Danych w 2022 r.". Organizator: SABI – Stowarzyszenie Inspektorów Ochrony Danych, 26.01.2022 r.

3. VIII Dzień Otwarty Ochrony Danych Osobowych w Dąbrowie Górniczej. Organizator: Akademia WSB w Dąbrowie Górniczej, 7.02.2022 r.

4. Konferencja pt. „Przeszłość, teraźniejszość i przyszłość RODO". Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp. k., 25.05.2022 r.

5. Konferencja online pt. „RODO i cyberbezpieczeństwo w Zdrowiu". Organizatorzy: Polska Federacja Szpitali, Zespół Ekspertów „w Zdrowiu", Kancelaria DZP, 24.05.2022 r.

6. III Konferencja z cyklu „RODO w zakładzie pracy" pt. „Inspektor ds. zgodności a przetwarzanie danych osobowych w związku ze zgłoszeniem wewnętrznym sygnalisty". Organizator: Wydział Prawa i Administracji UJ, 10.06.2022 r.

7. VI Krajowy Kongres Sekretarzy. Organizator: Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego, 19-20.10.2022 r.

Załącznik nr 3

Wykaz konferencji, seminariów, spotkań i innych wydarzeń krajowych i międzynarodowych z udziałem Prezesa UODO lub jego przedstawicieli, zorganizowanych w 2022 r. w Polsce przez UODO lub inne podmioty.

L. p.	Data	Wydarzenie	Miejsce
1.	10.01.2022 r.	Webinarium nt. sztucznej inteligencji i ochrony danych osobowych, pt. „Twoje dane i sztuczna inteligencja". Organizatorzy: UODO i firma Intel.	online
2.	18.01.2022 r.	Wywiad z Profesorem Paul'em de Hert'em na temat wyzwań, trendów i możliwych zagrożeń związanych z ochroną danych osobowych w 2022 roku.	online
3.	20.01.2022 r.	Uroczyste wręczenie Nagrody im. Michała Serzyckiego dwóm laureatom: Pani M. Margulskiej-Haczyk i Panu mec. Xaweremu Konarskiemu, 20.01.2022 r.	Warszawa
4.	26.01.2022 r.	Konferencja „Dzień IOD. IOD wobec nowych wyzwań w ochronie danych". Organizator: SABI – Stowarzyszenie Inspektorów Ochrony Danych.	online
5.	26.01.2022 r.	Konferencja Rzeczowo o Prawie: „Ochrona Danych Osobowych – Wyzwania 2022". Organizator: Lubasz i Wspólnicy Kancelaria Radców Prawnych.	online
6.	28.01.2022 r.	Konferencja „Ochrona danych osobowych na co dzień" w ramach obchodów XVI Dnia Ochrony Danych Osobowych. Organizator: UODO.	online
7.	31.01.2022 r.	Warsztaty dla nauczycieli „Warto wiedzieć… jak wykorzystać TIK w szkole, by chronić dane osobowe". Organizator: UODO we współpracy z Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.	online
8.	7.02.2022 r.	VIII Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej.	online
9.	11.03.2022 r.	Konferencja Państwowej Inspekcji Pracy pt. „Pierwszy rok – podsumowanie i wyzwania'.	Warszawa
10.	19.03.2022 r.	Inauguracja 23. edycji Podyplomowego Studium Ochrony Danych Osobowych w Akademii Leona Koźmińskiego.	Warszawa
11.	24.03.2022 r.	Seminarium „Wpływ aktywności w Internecie na wizerunek ucznia w realnym świecie". Organizator: Radomski Ośrodek Doskonalenia Nauczycieli.	online
12.	31.03.2022 r.	Konferencja inaugurująca projekt pn. „Inteligentnie w energetyce. Wsparcie budowy inteligentnej sieci energetycznej w Polsce". Organizator: Ministerstwo Klimatu i Środowiska.	online
13.	31.03.2022 r.	Forum Inspektorów Ochrony Danych Osobowych. Organizator: Stowarzyszenie Wielkopolski Ośrodek Kształcenia i Studiów Samorządowych.	online

14.	31.03.2022 r.	Spotkanie sieci współpracy placówek doskonalenia zawodowego nauczycieli w ramach programu edukacyjnego „Twoje dane – Twoja sprawa”.	online
15.	29.04.2022 r.	IV Dzień Nowych Technologii w Edukacji. Organizatorzy: MEiN oraz kuratorzy oświaty.	Warszawa
16.	24.05.2022 r.	Konferencja pt. „RODO i cyberbezpieczeństwo w Zdrowiu”. Organizatorzy: Polska Federacja Szpitali, Zespół Ekspertów w Zdrowiu oraz Kancelaria Domański Zakrzewski Palinka sp. k.	online
17.	24.05.2022 r.	Konferencja „Rozliczalność to podstawa RODO”. Organizator: DAPR Data Protection.	online
18.	25.05.2022 r.	Konferencja „Przeszłość, teraźniejszość i przyszłość RODO”. Organizator: Lubasz i Wspólnicy – Kancelaria Radców Prawnych sp. k.	online
19.	27.05.2022 r.	Święto UKSW – uroczysta sesja Senatu UKSW.	Warszawa
20.	28.05.2022 r.	Gala Jubileuszowa 30-lecia Uczelni Techniczno-Handlowej w Warszawie.	Warszawa
21.	30-31.05.2022 r.	Ogólnopolska Konferencja Naukowa pt. „Procedury prawodawcze – znaczenie, zmiany, wyzwania”.	Lublin
22.	7-9.06.2022 r.	Forum IAB „Transformacja na sterydach. Digital w czasach kryzysów”. Organizator: Zespół IAB Polska.	Warszawa
23.	10.06.2022 r.	Konferencja pt. „RODO w zakładzie pracy. Inspektor ds. zgodności a przetwarzanie danych osobowych w związku ze głoszeniem wewnętrznym sygnalisty”.	online
24.	21.06.2022 r.	Spotkanie podsumowujące XII edycję ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa”. Organizator: UODO.	Warszawa
25.	21.06.2022 r.	Odprawa szkoleniowa Biura Nadzoru Wewnętrznego MSWiA – ocena naruszeń zgłaszanych organowi nadzorczemu przez służby nadzorowane przez MSWiA.	Otwock
26.	23-24.06.2022 r.	Coroczne Forum Prywatności (Annual Privacy Forum – APF) 2022. Organizatorzy: ALK w Warszawie, UKSW w Warszawie, The European Union Agency for Cybersecurity.	Warszawa
27.	25.06.2022 r.	XIV konferencja z cyklu „Bezpieczeństwo w Internecie” pt. „Hacking”. Organizatorzy: UKSW w Warszawie, NASK-PIB, ALK w Warszawie, Naukowe Centrum Prawno-Informatyczne.	Warszawa
28.	28.06.2022 r.	Posiedzenie Komisji do spraw Międzynarodowego Prawa Humanitarnego.	Warszawa
29.	1.07.2022 r.	Uroczystość zakończenia roku akademickiego 2021/2022 na Uniwersytecie Warszawskim.	Warszawa
30.	12.07.2022 r.	Webinarium pt. „Cyberzagrożenia – czego boją się Polacy?”. Organizator: UODO.	online
31.	14.07.2022 r.	Posiedzenie Komitetu Konsultacyjnego UODO ds. Administracyjnych Kar Pieniężnych.	Warszawa

32.	13.09.2022 r.	Konferencja KPRM pt. „GRAI – rekomendacje ekspertów, raporty, projekty, regulacje”.	Warszawa
33.	21.09.2022 r.	Konferencja „Legal FinTech 2022. Wyzwania prawne w sektorze technologii finansowych”. Organizatorzy Stowarzyszenie Prawników Nowoczesnych Technologii we współpracy z Wydawnictwem CH. Beck	Warszawa
34.	23.09.2022 r.	Forum Inspektorów Ochrony Danych. Organizator: Wielkopolski Ośrodek Kształcenia i Studiów Samorządowych	online
35.	27-30.09.2022 r.	16. Międzynarodowa Konferencja pt. „Bezpieczeństwo dzieci i młodzieży w Internecie”. Organizator: Polskie Centrum Programu Safer Internet (PCPSI).	Warszawa
36.	28.09.2022 r.	Konferencja pt. „Człowiek w postkwantowej rzeczywistości”. Organizator: UODO we współpracy z KPRM.	online / Warszawa
37.	30.09.2022 r.	Webinarium pt. „Zabezpieczenia techniczne przetwarzanych danych osobowych”. Organizator: UODO.	online
38.	3.10.2022 r.	Inauguracja roku akademickiego 2022/2023 w Akademii Leona Koźmińskiego w Warszawie.	Warszawa
39.	7.10.2022 r.	Inauguracja roku akademickiego 2022/2023 na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie.	Warszawa
40.	10-17.10.2022 r.	Pobyt delegacji organu nadzorczego Republiki Północnej Macedonii w UODO w ramach projektu twinningowego „Support to the implementation of the Modernised Data Protection Legal Framework.	Warszawa
41.	19.10.2022 r.	VI Krajowy Kongres Sekretarzy. Organizator: Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego – FDRL oraz Krajowa Rada Forów Sekretarzy.	Warszawa
42.	19-20.10.2022 r.	Konferencja Cybersecurity Forum 2022. Organizator: Evention Sp. z o.o.	Warszawa
43.	20.10.2022 r.	Szczyt Cyfrowy IGF Polska. Organizatorzy: Business & Science Poland we współpracy z KPRM.	Lublin
44.	20-21.10.2022 r.	Inauguracja XIII edycji ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa”. Organizator: UODO.	Online
45.	22-23.10.2023 r.	Konferencja Szkoleniowa „E-zdrowie, E-medycyna, E-bezpieczeństwo”. Organizator: Federacja Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie”.	Jelenia Góra
46.	27.10.2022 r.	Posiedzenie Komitetu Konsultacyjnego UODO ds. Administracyjnych Kar Pieniężnych.	online
47.	29.10.2022 r.	Inauguracja 24. edycji Podyplomowego Studium Ochrony Danych Osobowych w Akademii Leona Koźmińskiego w roku akademickim 2022/2023.	Warszawa
48.	15-16.11.2022 r.	VII Forum Edukacji Dorosłych. Organizator: Fundacja Rozwoju Systemu Edukacji w ramach Krajowego Biura EPALE.	Warszawa

49.	25.11.2022 r.	Webinarium „Projektowanie systemów SI zgodnych z RODO”. Organizator: UODO.	online / Warszawa
50.	2.12.2022 r.	Szkolenie z zakresu cyberbezpieczeństwa dla pracowników UODO.	online / Warszawa
51.	8.12.2022 r.	Wykład „Przetwarzanie danych osobowych przez poradnie psychologiczno-pedagogiczne i rady rodziców” Organizator: UODO w ramach cyklu „RODO w szkolnej ławce”.	online
52.	9.12.2022 r.	Webinarium z cyklu ogólnopolskich lekcji pod hasłem „#ODOlekcje” w ramach XIII edycji programu „Twoje dane – Twoja sprawa”	online
53.	14.12.2022 r.	Spotkanie nt. „Stanu prac nad kodeksami postępowania zgodnymi z RODO”. Organizator: UODO.	online
54.	14.12.2022 r.	Uroczystość wręczenia certyfikatu akredytacyjnego dla Federacji Porozumienia Zielonogórskiego.	Warszawa

Załącznik nr 4

Wykaz wydarzeń międzynarodowych i europejskich, w tym posiedzeń plenarnych EROD i podgrup, z udziałem Prezesa UODO lub jego przedstawicieli, które odbyły się w 2022 r.

L. p.	Data	Konferencja/Seminarium/Spotkanie	Miejsce
1.	10.01.2022 r.	Posiedzenie Komisji ds. Międzynarodowego Prawa Humanitarnego (MPH)	online
2.	10.01.2022 r.	Spotkanie punktów kontaktowych ds. Grupy Wsparcia Ekspertów Wspierających EROD (SPE)	online
3.	11.01.2022 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101)	online
4.	11.02.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych	online
5.	12.01.2022 r.	Posiedzenie Grupy Zadaniowej ds. banerów cookie (FT Cookie Banner)	online
6.	12.01.2022 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network)	online
7.	17.01.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych	online
8.	18.01.2022 r.	posiedzenie plenarne Europejskiej Rady Ochrony Danych	online
9.	20.01.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych	online
10.	25.01.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych	online
11.	25-26.01.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych	online
12.	26.01.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych	online
13.	27.01.2022 r.	Sieć Inspektorów Ochrony Danych – posiedzenie podgrupy DPO Network	online

14.	27.01.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych	online
15.	1.02.2022 r.	60. posiedzenie plenarne Europejskiej Rady Ochrony Danych	online
16.	2.02.2022 r.	Posiedzenie Grupy Zadaniowej ds. banerów cookie (TF Cookie Banner)	online
17.	4.02.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych	online
18.	9.02.2022 r.	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych	online
19.	10.02.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
20.	14.02.2022 r.	Spotkanie sprawozdawców wytycznych dot. art. 60 RODO.	online
21.	15.02.2022 r.	Wspólne spotkanie ekspertów podgrup: ITS – COOP.	online
22.	15-16.02.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
23.	17.02.2022 r.	Posiedzenie Grupy zadaniowej ds. Nakładania Kar (Fining Task Force) Europejskiej Rady Ochrony Danych.	online
24.	21.02.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
25.	22.02.2022 r.	61. posiedzenie plenarne EROD.	online
26.	25.02.2022 r.	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
27.	3.03.2022 r.	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
28.	3.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
29.	8.03.2022 r.	Posiedzenie Grupy zadaniowej ds. banerów cookie (TF Cookie Banner) Europejskiej Rady Ochrony Danych.	online
30.	9.03.2022 r.	Posiedzenie Grupy zadaniowej ds. Nakładania Kar (Fining Task Force) Europejskiej Rady Ochrony Danych.	online

31.	9.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
32.	10.03.2022 r.	Spotkanie Sieci Komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
33.	10.03.2022 r.	I Spotkanie dot. call-a Artificial intelligence, big data and democracy z przedstawicielami Uniwersytetu Segedyńskiego z Węgier.	online
34.	10.03.2022 r.	11. spotkanie EROD-podgrupy dot. agendy 62. Posiedzenia plenarnego EROD oraz omówieniu wkładów do instrukcji dla przedstawiciela UODO.	Warszawa
35.	10.03.2022 r.	Spotkanie organów nadzorczych w sprawie Vinted.	online
36.	10.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
37.	10.03.2022 r.	I Spotkanie z przedstawicielem Uniwersytetu Segedyńskiego w związku z projektem Horizon Artificial intelligence, big data and democracy.	online
38.	14.03.2022 r.	62. posiedzenie plenarne EROD.	online
39.	15.03.2022 r.	Połączone Spotkanie Podgrup Ekspertów ITS i CEH (Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych – ITS i Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia – CEH) Europejskiej Rady Ochrony Danych.	online
40.	15-16.03.2022 r.	Spotkanie Komitetu Ekspertów RE ds. Integralności Informacji Online w Internecie (Committee of Experts on the Integrity of Online Information MSI-INF).	online
41.	15-16.03.2022 r.	I Spotkanie Komitetu Ekspertów ds. Integralności Informacji Online (Committee of Experts on the Integrity of Online Information MSI-INF).	online
42.	16.03.2022 r.	II Spotkanie z przedstawicielem Uniwersytetu Segedyńskiego w związku z projektem Horizon Artificial intelligence, big data and democracy.	online
43.	16.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup TECH) Europejskiej Rady Ochrony Danych.	online
44.	16.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
45.	17.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health - CEH) Europejskiej Rady Ochrony Danych.	online
46.	23.03.2022 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101).	online

47.	23.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
48.	23-25.03.2022 r.	55. Posiedzenie Biura Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (T-PD Bureau).	Paryż/online
49.	28.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
50.	29.03.2022 r.	Posiedzenie Grupy Zadaniowej ds. banerów cookie (FT Cookie Banner)	online
51.	29.03.2022 r.	Posiedzenie Podgrupy IT Users Europejskiej Rady Ochrony Danych.	online
52.	30.03.2022 r.	Posiedzenie Podgrupy Ekspertów ITS-BCR Workshop.	online
53.	30.03.2022 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
54.	31.03.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
55.	1.04.2022 r.	Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory – SAESG) Europejskiej Rady Ochrony Danych	online
56.	4-7.04.2022 r.	Privacy Symposium.	Wenecja
57.	6.04.2022 r.	63. posiedzenie plenarne EROD.	online
58.	7.04.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup TECH) Europejskiej Rady Ochrony Danych.	online
59.	7.04.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE).	online
60.	8.04.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
61.	12.04.2022 r.	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
62.	19.04.2022 r.	Spotkanie grupy Mobile apps expert exchange.	online
63.	20.04.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	Bruksela
64.	20.04.2022 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101).	online

65.	21.04.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
66.	21.04.2022 r.	Posiedzenie Podgrupy Ekspertów ITS-BCR Workshop.	online
67.	25.04.2022 r.	Posiedzenie Podgrupy Ekspertów ITS-BCR Workshop.	online
68.	27.04.2022 r.	Sieć Inspektorów Ochrony Danych – posiedzenie podgrupy DPO Network.	
69.	27-28.04.2022 r.	Spotkanie Rzeczników Ochrony Danych w sprawie funkcjonowania mechanizmu kompleksowej współpracy i wdrażania RODO.	Wiedeń
70.	29.04.2022 r.	Spotkanie organów nadzorczych w sprawie Vinted.	online
71.	2.05.2022 r.	Posiedzenie Podgrupy Ekspertów ITS-BCR Workshop.	online
72.	2-3.05.2022 r.	Spotkanie sprawozdawców Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health - CEH) Europejskiej Rady Ochrony Danych.	online
73.	4.05.2022 r.	64. posiedzenie plenarne EROD.	online
74.	5.05.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
75.	5.05.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
76.	6.05.2022 r.	Spotkanie sieci komunikacyjnej rzeczników prasowych organów ochrony danych osobowych (The EDPB Communications Network).	online
77.	11.05.2022 r.	Posiedzenie Grupy Zadaniowej ds. banerów cookie (FT Cookie Banner).	online
78.	12.05.2022 r.	65. posiedzenie plenarne EROD.	online
79.	16-19.05.2022 r.	Warsztaty dot. wiążących reguł korporacyjnych.	Cavtat k. Dubrownika
80.	17-18.05.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
81.	18-20.05.2022 r.	Wiosenna Konferencja Europejskich Organów Ochrony Danych. Organizator: chorwacki organ nadzorczy (Spring Conference of European Data Protection Authorities).	Cavtat k. Dubrownika
82.	19.05.2022 r.	Posiedzenie Podgrupy Ekspertow ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE).	online
83.	19.05.2022 r.	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online

84.	20.05.2022 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101).	online
85.	24.05.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
86.	31.05.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
87.	31.05.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
88.	1.06.2022 r.	Posiedzenie grupy ds. koordynacji nadzoru nad CIS.	online
89.	1.06.2022 r.	Posiedzenie grupy ds. koordynacji nadzoru nad SIS.	online
90.	1.06.2022 r.	Posiedzenie Rady Współpracy Europolu.	online
91.	2.06.2022 r.	Posiedzenie grupy ds. koordynacji nadzoru nad VIS.	online
92.	2.06.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
93.	2.06.2022 r.	Posiedzenie grupy ds. koordynacji nadzoru nad Systemem Eurodac.	online
94.	3.06.2022 r.	Posiedzenie Zespołu ds. Ewaluacji Schengen w Szwecji.	online
95.	7.06.2022 r.	Wspólne Posiedzenie Podgrupy Doradczej ds. Strategii (Strategic Advisory – SAESG) i Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
96.	7.06.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfer Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
97.	8.06.2022 r.	Spotkanie sprawozdawców wytycznych w sprawie prawa dostępu do danych.	online
98.	8.06.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
99.	10.06.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	online
100.	10.06.2022 r.	Posiedzenie Grupy roboczej ds. Nakładania Kar (Fining Taskforce) Europejskiej Rady Ochrony Danych.	online
101.	12-17.06.2022 r.	Konferencja pt. „Realizacja obowiązku prowadzenia kontroli na miejscu z zakresu oceny stosowania dorobku Schengen, na podstawie Rozporządzenia 1053/2013”.	Sztokholm
102.	14-15.06.2022 r.	66. posiedzenie plenarne EROD.	Bruksela

103.	15.06.2022 r.	Konferencja CIPL „Roundtable on Children's Privacy in Europe" oraz warsztaty *Taking stock of law, policy, regulatory qiudance and best practices on children's data protection in Europe.*	online
104.	15-17.06.2022 r.	43. Posiedzenie plenarne T-PD.	online
105.	16-17.06.2022 r.	Konferencja EIOD "The Future of Data Protection. Effective enforcement in the digital world".	Bruksela
106.	20.06.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
107.	22.06.2022 r.	Warsztaty Internet Privacy Engineering Network (IPEN Workshop 2022) „Digital Identity in data protection by design – current developments and future trends".	Warszawa
108.	23-24.06.2022 r.	10th Annual Privacy Forum.	Warszawa
109.	24.06.2022 r.	Posiedzenie Podgrupy Ekspertów Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
110.	27.06.2022 r.	Spotkanie sprawozdawców wytycznych dot. prawa dostępu.	online
111.	28.06.2022 r.	Posiedzenie Komisji do spraw Międzynarodowego Prawa Humanitarnego	Warszawa
112.	28.06.2022 r.	Międzynarodowa Konferencja Privacy Research Day. Organizator: CNIL.	online
113.	29.06.2022 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee) Europejskiej Rady Ochrony Danych.	online
114.	29-30.06.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Government and Health – CEH) Europejskiej Rady Ochrony Danych.	Bruksela
115.	1.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych – w sprawie terminów przygotowania projektu oświadczenia o przekazywaniu danych do Rosji.	online
116.	4.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup FMES) Europejskiej Rady Ochrony Danych.	online
117.	5.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
118.	6.07.2022 r.	Posiedzenie Komitetu ds. Skoordynowanego Nadzoru (Coordinated Supervision Committee) Europejskiej Rady Ochrony Danych.	online
119.	6.07.2022 r.	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online

120.	6.07.2022 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101) Europejskiej Rady Ochrony Danych.	online
121.	7.07.2022 r.	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych.	online
122.	7.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
123.	8.07.2022 r.	Spotkanie sieci komunikacyjnej (Communications network) Europejskiej Rady Ochrony Danych.	online
124.	11.07.2022 r.	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych	online
125.	12.07.2022 r.	67. Posiedzenie plenarne EROD.	online
126.	13.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
127.	15.07.2022 r.	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych	online
128.	19.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
129.	19.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
130.	22.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
131.	22.07.2022 r.	Spotkanie Grupy zadaniowej ds. 101 skarg NOYB (Taskforce 101) Europejskiej Rady Ochrony Danych.	online
132.	25.07.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
133.	28.07.2022 r.	68. posiedzenie plenarne EROD.	online
134.	5.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych	online
135.	6.09.2022 r.	Spotkanie sprawozdawców wytycznych dot. prawa dostępu do danych.	online
136.	8.09.2022 r.	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela

137.	8.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
138.	9.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Finansowych (Financial Matters Expert Subgroup FMES) Europejskiej Rady Ochrony Danych.	online
139.	12.09.2022 r.	Spotkanie sprawozdawców wytycznych dot. prawa dostępu do danych.	online
140.	12-13.09.2022 r.	69. posiedzenie plenarne EROD.	Bruksela
141.	14-15.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
142.	15.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych	online
143.	20.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
144.	20.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	Bruksela
145.	21-22.09.2022 r.	Szkolenie dla uczestników wymian EDPS-EDPB biur/ urzędów organów nadzorczych.	Bruksela
146.	22.09.2022 r.	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
147.	27.09.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
148.	29.09.2022 r.	Spotkanie w ramach projektu STeP – Surveillance Toward Ensuring Privacy Horizon, z udziałem Fondazzione Basso oraz Bułgarską Komisją Ochrony Danych.	online
149.	30.09.2022 r.	Spotkanie Grupy roboczej DEWG w sprawie ankiety dla nauczycieli „Teachers and digital citizenship”.	online
150.	3-7.10.2022 r.	Realizacja obowiązku prowadzenia kontroli na miejscu z zakresu oceny stosowania dorobku Schengen.	Dania
151.	5.10.2022 r.	Spotkanie Grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB (Taskforce 101).	online
152.	5-6.10.2022 r.	II posiedzenie Committee of Experts on the Integrity of Online Information (MSI-INF).	online
153.	10.10.2022 r.	70. posiedzenie plenarne EROD.	online

154.	18-19.10.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online
155.	20.10.2022 r.	Posiedzenie Podgrupy Ekspertów ITS-BCR Workshop.	online
156.	20.10.2022 r.	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
157.	21.10.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
158.	21.10.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych	online
159.	21.10.2022 r.	Spotkanie koordynacyjne przed 44. Posiedzeniem plenarnym Komitetu T-PD.	online
160.	21.10.2022 r.	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network) Europejskiej Rady Ochrony Danych.	online
161.	24.10.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych	online
162.	25-28.10.2022 r.	44. Międzynarodowa Konferencja Global Privacy Assembly – GPA: „A Matter of Balance: Privacy in the Era of Rapid Technological Advancement”.	Stambuł
163.	26.10.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych	online
164.	27.10.2022 r.	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
165.	28.10.2022 r.	Spotkanie sprawozdawców wytycznych w sprawie prawa dostępu do danych.	online
166.	7.11.2022 r.	Skoordynowane działanie EROD w zakresie egzekwowania prawa – wyznaczenie i pozycja IOD.	online
167.	7.11.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
168.	9.11.2022 r.	Posiedzenie Podgrupy ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych	online
169.	10.11.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online

170.	10.11.2022 r.	Posiedzenie Podgrupy ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
171.	11.11.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
172.	14.11.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Doradztwa Strategicznego (Strategic Advisory Expert Subgroup– SAESG) Europejskiej Rady Ochrony Danych	online
173.	14.11.2022 r.	71. posiedzenie plenarne EROD.	online
174.	15-17.11.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Egzekwowania Prawa (Enforcement Expert Subgroup – ENF) Europejskiej Rady Ochrony Danych.	online
175.	16.11.2022 r.	Posiedzenie Sieci Komunikacyjnej (Communications network) Europejskiej Rady Ochrony Danych.	online
176.	16-18.11.2022 r.	44. Posiedzenie plenarne Komitetu T-PD.	Strasburg
177.	21.11.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
178.	21.11.2022 r.	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Systemem Informacyjnym Schengen II – SIS.	online
179.	21-22.11.2022 r.	Posiedzenie Podgrupy ds. Egzekwowania Prawa (Enforcement – ENF) Europejskiej Rady Ochrony Danych.	online
180.	22.11.2022 r.	Posiedzenie Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS) oraz Systemem Eurodac.	online
181.	22.11.2022 r.	Posiedzenie Podgrupy ds. Finansowych (Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
182.	23.11.2022 r.	Spotkanie grupy zadaniowej Europejskiej Rady Ochrony Danych ds. 101 skarg NOYB w kontekście wyroku TSUE Schrems II (Taskforce 101).	online
183.	24.11.2022 r.	Posiedzenie Podgrupy ds. Granic, Podróży i Egzekwowania Prawa (Boarders, Travel & Law Enforcement Expert Subgroup – BTLE) Europejskiej Rady Ochrony Danych.	online
184.	30.11.2022 r.	Spotkanie Sieci Inspektorów Ochrony Danych (DPO Network) Europejskiej Rady Ochrony Danych.	online
185.	1.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Użytkowników IT (IT Users Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
186.	5.12.2022 r.	72. posiedzenie plenarne EROD.	online
187.	6-7.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Międzynarodowego Przekazywania Danych (International Transfers Expert Subgroup – ITS) Europejskiej Rady Ochrony Danych.	online

188.	8.12.2022 r.	Posiedzenie Podgrupy ds. Mediów Społecznościowych (Social Media Expert Subgroup) Europejskiej Rady Ochrony Danych.	online
189.	8.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Technologii (Technology Expert Subgroup – TECH) Europejskiej Rady Ochrony Danych – spotkanie ekspertów ds. audytu aplikacji mobilnych.	online
190.	9.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Kluczowych Przepisów (Key Provisions Expert Subgroup – KEYP) Europejskiej Rady Ochrony Danych.	online
191.	9.12.2022 r.	Posiedzenie Sieci Komunikacyjnej (Communications network) Europejskiej Rady Ochrony Danych.	online
192.	12.12.2022 r.	Spotkanie Grupy zadaniowej ds. bannerów cookie (TF Cookie Banner).	online
193.	13.12.2022 r.	73. posiedzenie plenarne EROD.	online
194.	13.12.2022 r.	Polsko-Serbskie Forum Nowych Technologii.	online
195.	13-14.12.2022 r.	73. Posiedzenie plenarne EROD.	online
196.	15.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Współpracy (Cooperation Expert Subgroup – COOP) Europejskiej Rady Ochrony Danych.	online
197.	19.12.2022 r.	Posiedzenie Podgrupy ds. Finansowych (Financial Matters (FMES) Europejskiej Rady Ochrony Danych.	online
198.	19.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
199.	20.12.2022 r.	Posiedzenie Podgrupy Ekspertów ds. Zgodności, e-Administracji i Zdrowia (Compliance, e-Governmen and Health – CEH) Europejskiej Rady Ochrony Danych.	online
200.	20.12.2022 r.	Spotkanie organów nadzorczych w sprawie Vinted.	online
201.	20.12.2022 r.	Spotkanie grupy sprawozdawców wytycznych dot. art. 60 – prawo do bycia wysłuchanym.	online

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
www.uodo.gov.pl