Synteza sprawozdania rocznego z działalności Prezesa UODO w 2023 r.

Co Prezes UODO zrobił w 2023 r. i jakie wnioski, wynikające ze stanu przestrzegania przepisów o ochronie danych osobowych, wyciąga na przyszłość.

Wstęp

Dane osobowe są jedną z najcenniejszych wartości współczesnego świata. To dzięki nim rozwija się gospodarka oparta na danych, a państwa tworzą lepsze, bo dostosowane do potrzeb obywateli polityki. Dane osobowe można jednak wykorzystać jako groźną broń i narzędzie manipulacji. Dlatego powinny być traktowane z uwagą i przetwarzane z jak najmniejszym ryzykiem dla osób, których dotyczą.

Organem, który w Polsce zajmuje się ochroną danych osobowych i prawa do prywatności jest Prezes Urzędu Ochrony Danych Osobowych (PUODO). Jego zadaniem jest sprawdzanie, jak przestrzegane są polskie i europejskie przepisy o ochronie danych osobowych. Wydaje wytyczne, interpretuje RODO (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, zwane również ogólnym rozporządzeniem) i rozpatruje skargi. Może nakładać kary, a także wskazywać, co należy zmienić w organizacji, by dane osobowe były lepiej chronione, z mniejszym ryzykiem dla osób, których dotyczą.

Prezes UODO prowadzi też działalność edukacyjną w zakresie ochrony danych osobowych i prawa do prywatności. Niniejszy dokument będący syntezą Sprawozdania z działalności organu w roku 2023, i który zgodnie z art. 59 RODO Prezes UODO przedstawia co roku w Sejmie RP – jest elementem tej działalności.

Sprawozdanie PUODO za 2023 r. dostępne jest pod adresem: https://uodo.gov.pl/pl/p/o-nas. Dotyczy ono okresu, kiedy funkcję Prezesa Urzędu pełnił Jan Nowak. Od stycznia 2024 r. Prezesem UODO jest Mirosław Wróblewski wybrany na to stanowisko przez Sejm za zgodą Senatu 17 stycznia 2024 r.

WARTO WIEDZIEĆ:

Każdy ma prawo do ochrony dotyczących go danych osobowych. Prawo to zostało zagwarantowane w Konstytucji Rzeczypospolitej Polskiej (art. 51 w zw. z art. 47), Karcie Praw Podstawowych Unii Europejskiej (art. 8), a także w Traktacie o funkcjonowaniu Unii Europejskiej (art. 16).

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.

RODO jest rozporządzeniem wypracowanym wspólnie i przyjętym przez wszystkie państwa członkowskie Unii Europejskiej. Obowiązuje w całej Unii.

Skarga do Prezesa Urzędu Ochrony Danych Osobowych na przetwarzanie danych osobowych niezgodnie z prawem (art. 50. Ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

1. Osobie, której dane osobowe są przetwarzane niezgodnie z prawem, przysługuje prawo wniesienia skargi do Prezesa Urzędu w terminie 30 dni od powzięcia wiadomości o tym naruszeniu lub otrzymania informacji od administratora.
2. Prezes Urzędu udziela osobie, która wniosła skargę, pomocy prawnej na jej wniosek do czasu rozpatrzenia skargi przez Prezesa Urzędu.
3. Skargę można wnieść za pomocą formularza zamieszczonego w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa Urzędu, pisemnie, faxem, elektronicznie lub za pomocą elektronicznej platformy usług administracji publicznej ePUAP.
4. Prezes Urzędu informuje osobę, która wniosła skargę, o postępach w jej wyjaśnianiu, sposobie jej rozpatrzenia oraz możliwości złożenia skargi do sądu administracyjnego. Do rozpatrywania skarg stosuje się odpowiednio przepisy art. 225 (obowiązek przeciwdziałania ograniczaniu prawa do składania skarg i wniosków), art. 3 (wyłączenie stosowania ustawy_ 231) oraz art. 237–239 Kodeksu postępowania administracyjnego.
5. Prezes Urzędu nie przekazuje osobie, która wniosła skargę, informacji mogących wskazywać na przetwarzanie danych osobowych przez organy właściwe w sytuacjach, o których mowa w art. 26 (niedopuszczalność przekazywania informacji i udostępniania danych osobowych ust. 1).
6. Prawo do zgłoszenia naruszenia przetwarzania danych osobowych przysługuje również osobom innym niż wymienione w ust. 1 w przypadku powzięcia przez nie wiarygodnej wiadomości o tym naruszeniu. Do rozpatrywania zgłoszeń stosuje się odpowiednio art. 225 (obowiązek przeciwdziałania ograniczaniu prawa do składania skarg i wniosków) Kodeksu postępowania administracyjnego.
7. Dane zgłaszającego naruszenie, o którym mowa w ust. 6, Prezes Urzędu zachowuje w poufności na uzasadniony wniosek zgłaszającego.

DZIAŁANIA PREZESA UODO W 2023 R.

Odpowiedzi na pytania obywateli

W przypadku problemów i wątpliwości dotyczących stosowania przepisów o ochronie danych osobowych można zadzwonić do Urzędu Ochrony Danych Osobowych (tel. 606-950-000).

Każdego dnia pracownicy infolinii UODO odbierali kilkadziesiąt telefonów. Takich rozmów było w 2023 r. ponad 14 tys. To średnio 57 rozmów dziennie. Dzwoniły zarówno osoby fizyczne, jak i przedstawiciele podmiotów prawnych i publicznych.

Najczęstsze pytania na infolinii UODO:

- **monitoring wizyjny** (sąsiedzki, prywatny, wspólnot mieszkaniowych, w placówkach edukacyjnych, w miejscach pracy, w aptekach, w szpitalach, na parkingach);
- **przetwarzanie danych osobowych przez spółdzielnie i wspólnoty mieszkaniowe**;
- **przetwarzanie danych osobowych przez pracodawców** (m.in. przechowywanie CV pracownika, dane dotyczące zdrowia, narkotesty i badanie trzeźwości pracownika a RODO, wniosek o pracę zdalną a dane niepełnosprawnego członka rodziny, kontrola pracownika);
- **naruszenia przepisów w sektorze oświaty** (nagrywanie ucznia przez nauczyciela, robienie mu zdjęć, ujawnianie danych szczególnej kategorii);
- **niechciany telemarketing**
- **żądanie przez internetowe platformy sprzedażowe** skanów dokumentów tożsamości w celu odblokowania środków otrzymanych ze sprzedaży (m.in. Allegro, Vinted, Olx);
- **procedury weryfikacyjne** pasażerów wykorzystywane przez linie lotnicze.

Skargi obywateli

Osobie, która uważa, że jej dane osobowe są przetwarzane niezgodnie z prawem, przysługuje prawo wniesienia skargi do Prezesa Urzędu. Skargi kierowane do PUODO dotyczą różnych aspektów życia codziennego – od spraw dotyczących przetwarzania danych przez sąsiada (np. monitoring wizyjny), przez skargi na pracodawców, a na instytucjach administracji rządowej kończąc.

W roku 2023 r. do UODO wpłynęły **6962 skargi od obywateli** (o 33 skargi mniej niż w roku poprzednim). Sprawy prowadzone na podstawie skarg w Urzędzie są coraz bardziej skomplikowane i wielowątkowe i coraz częściej dotyczą zagadnień związanych z nowymi technologiami.

Najbardziej dramatyczne skargi w 2023 r. dotyczyły sytuacji ujawnienia danych osobowych, które mogły doprowadzić do samobójstwa (DOL.023.173.2023, DOL.051.6.2023.).

Pierwsza z tych spraw dotyczyła osoby niepełnoletniej, której dane osobowe ujawniono w informacji medialnej dotyczącej skazania dorosłej osoby za czyn pedofilski. Informacje te ujawniono, by zaatakować matkę dziecka, która jest osobą publiczną. Podane informacje pozwalały na identyfikację skrzywdzonego dziecka. Niedługo po ujawnieniu tych informacji młoda osoba popełniła samobójstwo.

Druga sprawa dotyczyła ujawnienia w mediach społecznościowych danych osoby w kontekście stwierdzenia o rzekomym popełnieniu przez nią czynu nieobyczajnego w miejscu publicznym i zarzucania mu czynu o charakterze pedofilskim. Zakres ujawnionych danych obejmował informacje o fakcie pełnienia przez tę osobę posługi kapłańskiej, nazwę zgromadzenia oraz wizerunek.

W obu sprawach ówczesny Prezes UODO odmówił rozpatrywania tych spraw uznając, że nie ma podstaw prawnych do wszczęcia postępowania.

Obecny Prezes Urzędu Ochrony Danych Osobowych podjął czynności mające na celu wyjaśnienie okoliczności upublicznienia danych osobowych tych osób. Postępowania w tych sprawach są w toku i będą przedstawione w sprawozdaniu z działalności organu za 2024 r.

Sprawy życia codziennego

Zgłoszone skargi Prezes UODO wyjaśnia, może udzielić upomnienia, wydać nakaz. W szczególnych sytuacjach – nałożyć karę finansową.

Wiele skarg, które rozpatruje Prezes UODO dotyczą zagadnień związanych z funkcjonowaniem wspólnot i spółdzielni mieszkaniowych.

Oto przykłady takich skarg:

Udostępnienie na rzecz pozostałych członków wspólnoty mieszkaniowej danych osobowych osoby, która zaskarżyła uchwałę wspólnoty. Prezes UODO w decyzji administracyjnej uznał, że udostępnienie tych danych nie było niezbędne do tego, by poinformować wspólnotę o sporze sądowym z jednym z członków. Sprawa skończyła się upomnieniem.

Prawo dostępu do danych a monitoring wizyjny. Wspólnota mieszkaniowa nie chciała wydać mieszkańcowi nagrań z monitoringu, na których uwidoczniony był jego wizerunek. Tłumaczyła, że na nagraniach są też inne osoby. Tymczasem dostęp do swoich danych jest prawem zagwarantowanym przez RODO. Ta sprawa też skoczyła się upomnieniem i nakazem wydania nagrania.

Udostępnienie danych zadłużonego członka wspólnoty mieszkaniowej w mailu zarządcy do wspólnoty. PUODO wskazał, że dochodzenie roszczenia przez wspólnotę nie wymaga, by wszyscy jej członkowie znali dane dłużnika. Upomniał wspólnotę za naruszenie.

Przykłady spraw z 2023 r., w których PUODO zastosował kary pieniężne:

- Spółdzielnia mieszkaniowa skonfliktowana z jedną z członkiń, złożyła zawiadomienie o podejrzeniu popełnienia przestępstwa przez tę osobę. Kopię zawiadomienia, z danymi osobowymi członkini spółdzielni, spółdzielnia przekazała dziennikarzom. Dane te otrzymała osoba związana z mediami, która o ich udostepnienie w ogóle nie wnioskowała. Spółdzielnia nie zgłosiła jednak zaistniałego naruszenia do PUODO ani nie zawiadomiła o zaistniałym naruszeniu osoby, której dane znalazły się w tym dokumencie. W tym wypadku Prezes UODO nałożył na spółdzielnię (administratora danych) karę pieniężną i nakazał jej, by zawiadomiła o fakcie naruszenia osobę, które dane zostały ujawnione.
- Zarządcy wspólnoty mieszkaniowej (podmiotowi przetwarzającemu) skradziono dokumenty, w tym akt notarialny. Wspólnota mieszkaniowa będąca administratorem tych danych nie zgłosiła naruszenia do PUODO (ten dostał w tej sprawie anonimowo zgłoszenie) i nie powiadomiła osób, których dane były w tym akcie. Ponadto w toku postępowania okazało się, że przetwarzanie danych członków tej wspólnoty powierzono firmie zarządzającej nieruchomościami bez pisemnej umowy oraz bez weryfikacji, czy podmiot ten zapewnia wystarczające gwarancje wdrożenia

odpowiednich środków bezpieczeństwa. Prezes UODO nałożył na wspólnotę karę finansową.

UWAGA! Jeśli ukarany nie zgadza się z decyzją PUODO (o upomnieniu czy karze), może zaskarżyć decyzję administracyjną do Wojewódzkiego Sądu Administracyjnego w Warszawie. Sąd albo podtrzymuje decyzję PUODO, albo ją uchyla.

Przykład:

WSA w Warszawie (II SA/Wa 763/22) podtrzymał w 2023 r. decyzję PUODO, by wspólnota mieszkaniowa usunęła dane osobowe skarżącego (jego wizerunek) z nagrań monitoringu w altanach śmietnikowych i przestała robić takie nagrania. Sąd podzielił stanowisko organu nadzorczego uznając, że wspólnota nie wykazała, aby wystąpiły przesłanki pozwalające na takie przetwarzanie danych osobowych. Wyważanie interesów osoby, której dane dotyczą i administratora ma charakter obowiązkowy. Z jednej strony należy ocenić i z rozwagą wyważyć podstawowe prawa i wolności, a z drugiej strony prawnie uzasadnione interesy administratora.

WSA w Warszawie (II SA/Wa 1340/22) poruszył kwestię monitoringu prowadzonego przez osoby prywatne i związanego z tym obowiązku informacyjnego, o którym mowa w art. 13 RODO. Prezes UODO ustalił, że zasięg monitoringu wizyjnego należącego do skarżonych sąsiadów wykracza poza ich nieruchomość i obejmuje przestrzeń wspólną (współwłasność). Wskazana przez sąsiadów potrzeba zapewnienia bezpieczeństwa swojego oraz dzieci jest uzasadnieniem dla monitoringu ograniczonego do terenu nieruchomości będącej ich wyłączną własnością. PUODO nakazał więc zasięg monitoringu ograniczyć i udzielił upomnienia, co WSA podtrzymał.

Zgłoszenia naruszeń przez samych administratorów

Zgodnie z RODO, administrator danych ma obowiązek zgłosić PUODO incydent, wskutek którego doszło do naruszenia ochrony danych i istnieje prawdopodobieństwo szkodliwego wpływu na osoby, których dane dotyczą (np. tzw. kradzież tożsamości). Administrator powinien przy tym samodzielnie przeanalizować to, jak doszło u niego do naruszenia ochrony danych i przedstawić jakie środki wdrożył lub zamierza wdrożyć w celu uniknięcia podobnej sytuacji w przyszłości. UODO analizuje takie naruszenie i w razie potrzeby podejmuje działania, które uzna za stosowne.

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

Prezes UODO zauważył w 2023 r., że administratorzy robią to coraz częściej, a składając kolejny raz formularze naruszeń umieją trafnie ocenić, czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych oraz stwierdzić po analizie, czy należy powiadomić o naruszeniu osoby, których dane dotyczą. Jednocześnie inspektorzy ochrony danych (IOD) coraz częściej potrafili wskazać środki bezpieczeństwa, jakie powinny zostać wdrożone w celu uniknięcia podobnych zdarzeń.

Co zgłaszano? Przykłady:

- **nieprawidłowe zaadresowanie korespondencji**. Bardzo często zgłaszanym naruszeniem jest udostępnienie danych osobowych niewłaściwym adresatom w masowej korespondencji wysyłanej bez ukrycia adresów e-mail innych osób (UDW);
- **udostępnienie danych niewłaściwej osobie** np. przez wydanie dokumentów, jak zaświadczenia czy deklaracje podatkowe osobom nieposiadającym uprawnień do ich otrzymania albo nieprawidłowo wysłaną korespondencję z danymi;
- **nieprawidłowa anonimizacja danych** lub niezamierzona ich publikacja np. na stronie internetowej lub w odpowiedzi na wniosek o dostęp do informacji publicznej;
- **nieuprawniony dostęp do baz danych.** Tego typu naruszenia były spowodowane najczęściej błędami oprogramowania ujawniającymi się po przeprowadzeniu aktualizacji programu, brakiem regularnych, wewnętrznych testów bezpieczeństwa, a także nieprawidłowościami na etapie nadawania uprawnień w systemach informatycznych;
- **zagubienie, kradzież lub pozostawienie w niezabezpieczonym miejscu dokumentacji papierowej.** Naruszenia tego rodzaju miały charakter jednorazowych incydentów i były konsekwencją niefrasobliwości pracowników;
- **zagubienie lub kradzież nośnika danych (laptopa lub niezaszyfrowanego pendrive'a)**;
- **atak hackerski z wykorzystaniem złośliwego oprogramowania** ingerującego w poufność, integralność lub dostępność danych osobowych;
- **naruszenia spowodowane błędami w aplikacjach** umożliwiającymi nieautoryzowany dostęp do zasobów, poprzez dostęp do identyfikatora wskazanego zasobu (podatności IDOR).

Prezes UODO, w przypadku skarg i zgłoszeń naruszeń, ma prawo wezwać administratora do udzielenia dodatkowych informacji czy wskazać czynności niezbędne po jego stronie. W 2023 r. działania te okazywały się generalnie skuteczne: administratorzy podejmowali kroki zapewniające skuteczną ochronę danych osobowych.

Decyzje PUODO

Dla ochrony osoby, której dane dotyczą, kluczowe jest, by mogła ona złożyć skargę do organu nadzorczego, gdy uzna, że przetwarzanie jej danych narusza przepisy RODO. Rolą Prezesa Urzędu Ochrony Danych Osobowych jest zapewnienie, by skarga została rozpatrzona w sposób niezależny, prawidłowy i zgodny z przepisami. Rozpatrywanie skarg osób, których dane dotyczą jest zadaniem, do którego Prezes Urzędu Ochrony Danych Osobowych przykłada szczególną wagę.

Analizując skargi i zgłoszenia naruszeń ochrony danych w 2023 r. (w tym także skargi i zgłoszenia otrzymane w poprzednim latach) PUODO wydał **1750 decyzji**. Liczba spraw zakończonych wydaniem decyzji administracyjnej jest na stałym poziomie. Decyzje organu nadzorczego zostały zaskarżone do Wojewódzkiego Sądu Administracyjnego w Warszawie w 223 przypadkach (dla porównania: w 2022 r. zaskarżono 177 decyzji). W większości spraw sądy administracyjne podzielały stanowiska zajmowane przez PUODO w sprawach

skargowych. W 2023 r. wzrosła zaskarżalność wyroków wydanych przez WSA w Warszawie do NSA - z 55 w 2022 r. do 66 w 2023 r..

Kiedy postępowanie wyjaśniające, związane ze zgłoszonym naruszeniem ochrony danych, nie prowadzi PUODO do zadawalających rezultatów, wszczyna on postępowanie administracyjne. W 2023 r. Prezes UODO wszczął 24 takich postępowań, zakończył 36 postępowań, które zaczęły się także w poprzednich latach, z czego 17 z nich zakończyło upomnieniami, a 19 – także karami. Siedem decyzji o karach zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie. Sąd utrzymał w mocy 4 i uchylił 2 decyzje. Reszta spraw jest w toku.

Kontrole PUODO

Prezes UODO przeprowadzał czynności kontrolne w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych w **33 podmiotach.** Były to m.in.

- **podmiot branży medycznej,** w którym doszło do wycieku dużej liczby danych osobowych w wyniku ataku hakerskiego i przełamania zabezpieczeń;
- **podmiot branży ubezpieczeniowej** – kontrola wykazała, że pośrednicy ubezpieczeniowi (osoby fizyczne wykonujące czynności agencyjne) mieli dostęp do bazy danych klientów zawierającej takie dane jak: imię i nazwisko, adres, numer PESEL, adres e-mail oraz numer telefonu;
- **placówka medyczna** – kontrola dotyczyła przetwarzania danych osobowych za pomocą środków technicznych umożliwiających rejestrację obrazu lub dźwięku;
- **firma kurierska** - kontrolą objęto przetwarzanie przez spółkę danych osobowych w związku ze świadczeniem usługi w zakresie doręczania przesyłek kurierskich, w szczególności ich odpowiedniego zabezpieczania przed utratą i zniszczeniem.

Szczególną uwagę PUODO zwrócił na aplikacje mobilne i webowe.

Kontrola PUODO objęła tu 15 podmiotów używających aplikacji mobilnych (branże: medyczna, bankowa, handlowa, gastronomiczna, turystyczna, transportowa, a także administracji publicznej).

W 2023 r. zgodnie z planem kontroli sektorowej PUODO skontrolował też pięć podmiotów używających aplikacji internetowych (webowych). Podmioty te działały w branży: ubezpieczeniowej, handlowej, bukmacherskiej i hostingowej.

Kontrole dotyczące w szczególności sposobu zabezpieczenia i udostępniania danych osobowych przetwarzanych przy użyciu aplikacji internetowych nadal trwają i są kontynuowane w 2024 roku.

Wystąpienia PUODO

W 2023 roku Prezes UODO wystosował **5 wystąpień** z określonymi wnioskami do podmiotów administracji publicznej i podmiotów prywatnych działających w różnych sektorach, z czego 2 dotyczyły zagadnień legislacyjnych, zaś impulsem 3 wystąpień były sygnały otrzymane od inspektorów ochrony danych. Dla porównania, w roku sprawozdawczym 2022 odnotowano 16 wystąpień.

Potencjał UODO

W Urzędzie Ochrony Danych Osobowych na koniec 2023 r. pracowało 267 osób. Budżet Urzędu wynosił w 2023 r. 45 mln 367 tys. zł.

Art. 35 RODO. Rewolucja w myśleniu. Szacowanie ryzyka a nie tropienie winnych

Analiza zgłoszeń naruszeń, skarg i wyników kontroli pokazuje, że błędy dotyczące ochrony danych mogą być przypadkowe, np. jako wynik nieszczęśliwego zbiegu okoliczności. Ale mogą też być objawem problemów systemowych - nienależytej wagi przykładanej do ochrony danych osobowych, małej wiedzy osób kierujących organizacjami czy braku procedur zabezpieczających. A przede wszystkim tego, że ciągle nie myślimy w kategoriach **analizy ryzyka**.

Łatwiej nam szukać winnego w przypadku pojawienia się problemu niż z wyprzedzeniem oszacować ryzyko i na podstawie tej analizy podjąć stosowne środki zaradcze, zanim problem się pojawi.

Zasada podejścia opartego na ryzyku (*risk based approach*) jest ważną, perspektywiczną koncepcją. Stanowi trzon RODO. Wynika z niej, że administratorom i podmiotom przetwarzającym nie wskazuje się ściśle określonych środków i procedur w zakresie bezpieczeństwa. Oni sami muszą samodzielnie przeprowadzić szczegółową analizę procesów przetwarzania danych i na tej podstawie ocenić ryzyko, w zależności od ich charakteru zakresu, kontekstu i celów przetwarzania. Oceniają ryzyko naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów administratora.

Przykładowo zatem inne środki ochrony powinny być podjęte w przypadku przetwarzania danych przez sklep prowadzący sprzedaż internetową, a inne - przez sklep prowadzący sprzedaż wyłącznie w lokalu, który nie przetwarza danych swoich klientów przy użyciu systemów teleinformatycznych wykorzystujących sieć Internet.

Mówiąc o ryzyku naruszenia praw i wolności osób fizycznych na gruncie RODO, konieczne jest uwzględnienie:

1) prawdopodobieństwa wystąpienia określonego zdarzenia
2) wagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować

Właśnie o tę analizę ryzyka: jak wygląda i w jaki sposób była aktualizowana, pyta PUODO prowadząc swoje postępowania.

Sposób przeprowadzenia analizy ryzyka opisuje art. 35 RODO.

Przetwarzanie danych osobowych - Problem biznesu

Stosowanie nowoczesnych technologii opartych na przetwarzaniu danych jest dla małych i średnich przedsiębiorstw doskonałym sposobem na rozwój. Problem w tym, że technologia nie tylko usprawnia stare procedury i pozwala wykonać zadania szybciej. Stawia też przedsiębiorcom nowe wyzwania. Dane gromadzone cyfrowo i przetwarzane na coraz większą skalę wymagają analizy ryzyka i ciągłej uwagi. Nie wystarczy zlecić to zadanie

zespołowi informatyków albo inspektorowi ochrony danych. Myślenie o ochronie danych musi być wbudowane w całą organizację.

Aplikacje mobilne

Takim nowym udogodnieniem są dla biznesu aplikacje mobilne.

Na początku 2022 r. było ich na świecie ponad 6 mln. Prawie każda z nich gromadziła informacje o swoich użytkownikach. Wiele aplikacji mobilnych gromadzi dane, które umożliwiają identyfikację konkretnego użytkownika - są to na ogół te aplikacje, które wymagają założenia konta i podania danych osobowych niezbędnych do korzystania z ich funkcjonalności. Niektóre aplikacje mobilne zbierają dane, które pozornie mogą wydawać się anonimowe, ale z prawnego punktu widzenia (i w powiązaniu z innymi przetwarzanymi danymi) mogą „stać się" danymi osobowymi. Takie dane również podlegają ochronie.

Tworzenie aplikacji mobilnych to najlepszy moment, aby zapewnić zgodność tego produktu z zasadami ochrony danych osobowych i dlatego ich twórcy powinni uwzględniać wymogi dotyczące ochrony danych osobowych już na etapie ich projektowania.

Sektorowa kontrola PUODO przeprowadzona w 2023 r. objęła w szczególności:

1) elementy bezpieczeństwa chroniące dane osobowe przetwarzane w aplikacjach mobilnych i w powiązanych z tymi aplikacjami systemach informatycznych,
2) mechanizmy tworzenia i weryfikacji kopii zapasowych,
3) zasady stosowania systemów antywirusowych, antyspamowych i innych systemów wspomagających ochronę aplikacji mobilnych i systemów informatycznych,
4) metody logowania oraz kontrolowania zdarzeń w systemach informatycznych,
5) sposób realizowania dostępu do przetwarzanych danych osobowych (ze szczególnym uwzględnieniem mechanizmów zapewniających poufność, integralność, dostępność danych),
6) kontrolę metod i zakresu informowania użytkowników aplikacji mobilnych o charakterze dostępu tych aplikacji do funkcjonalności wbudowanych w urządzenia mobile.

Co to dało? Kontrola wykazała, że biznes coraz lepiej radzi sobie z aplikacjami mobilnymi, choć jednak nadal pojawiają się problemy, na które należy zwracać uwagę.

Np. kontrola przeprowadzona w jednej z **placówek medycznych** wykazała**,** że użytkownik w celu uruchomienia aplikacji mobilnej wprowadzał swój numer PESEL jako login. Kont było kilkanaście tysięcy. Zatem proces logowania się do aplikacji był przetwarzaniem danych osobowych na dużą skalę. Prawidłowo przeprowadzona ocena skutków dla ochrony danych od razu wskazywałaby ryzyka wiążące się z ustanowieniem numeru PESEL jako loginu.

Kontrola **w spółce zajmującej się obsługą platformy do zamawiania jedzenia online** i korzystającej z aplikacji mobilnej wykazała, że od klientów pobierane były nadmiarowe dane. Spółka domagała się od klientów skanów dowodów osobistych lub paszportów, co jest sprzeczne z zasadą minimalizacji danych.

Generalnie należy stwierdzić, że kontrolowane podmioty wdrożyły wymagane środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych. Przygotowały i wdrożyły polityki bezpieczeństwa, dotyczące haseł i środków kryptograficznych. Ciągle też monitorowały bezpieczeństwo systemów, stosowały systemy antyspamowe i antywirusowe, przeprowadzały okresowe testy bezpieczeństwa, szyfrowały pliki i nośniki, monitorowały przepływ danych z i na nośniki, stosowały dwuskładnikowe uwierzytelnienia. Do ochrony przed atakami z sieci publicznej stosowały systemy bezpieczeństwa (np. system zapór sieciowych, system wykrywania oraz reagowania na zagrożenia) oraz systemy zapewniające rozliczalność operacji wykonywanych na danych osobowych. Dużą wagę podmioty kontrolowane przykładały do dostępności swoich usług dla użytkowników.

Korzystanie z pośredników przetwarzających dane.

Wielu przedsiębiorców korzysta z platform internetowych. Mogą np. powierzać dane klientów firmom marketingowym. Istotne jest tu, że nadal są administratorami danych i mają z tego powodu obowiązki.

Przykładem problemów, jakie wynikają z zaniedbań i niedopilnowania obowiązków i kończą się interwencją PUODO, jest sprawa obywatela, który dostawał od firmy marketingowej SMS-y i domagał się usunięcia swoich danych z bazy – tymczasem to inna firma była ich administratorem i powierzyła je do kampanii marketingowej. Przekazała je nie mając zgody osób, których dane dotyczą. Nie myślała w kategoriach ochrony danych, a tylko – usprawnienia swojej działalności. Skończyło się wyjaśnieniami przed PUODO i upomnieniem.

Rutyna w dokumentach kadrowych i w postępowaniu

Ten typ błędów w czasach przedcyfrowych mógł być niezauważony: dokument z danymi jednej osoby traktowano jako wzór dla innych. Wzór był papierowy, więc dane nie krążyły po świecie. Teraz jest inaczej. Do PUODO poskarżył się człowiek, który odkrył, że jego dane z prawdziwej umowy zawartej na czas określony z pewną firmą są nadal używane we wzorze umowy. I krążą w sieci – z imieniem, nazwiskiem, adresem, wysokością wynagrodzenia, stanowiskiem pracy i numerem konta bankowego.

Można wskazać jeszcze inne złe praktyki – np. informowanie całego zespołu na zebraniu o szczegółowych powodach rozwiązania umowy o pracę z pracownikiem. W czasach cyfrowych takie praktyki stają się poważnym problemem. Tak było w przypadku obywatelki, która poskarżyła się do PUODO, że szczegółowy opis zakończenia z nią współpracy znalazł się w mailu do wszystkich pracowników. Kodeks pracy nie daje pracodawcy podstaw do przekazywania takich informacji. Komunikacja cyfrowa pogłębia problem.

GPS w samochodzie służbowym

To nowa i popularna forma kontrolowania, czy sprzęt służbowy wykorzystywany jest zgodnie z przeznaczeniem, a nie np. do celów prywatnych pracownika. Rzecz w tym, że zasady każdego monitoringu powinny być uregulowane, a pracownicy powinni wiedzieć, na jakich zasadach przetwarzane są ich dane osobowe. Wymaga tego od 2018 r. Kodeks pracy, ale nadal wiele podmiotów nie uregulowało na piśmie celów, zakresu oraz sposobów zastosowania tego monitoringu w organizacji.

Także przetwarzanie wizerunku pracowników w związku z prowadzonym monitoringiem wizyjnym oraz niezapewnienie dostępu do danych osobowych przetwarzanych w jego ramach jest powodem częstych skarg do PUODO.

Ponadto w każdym spośród wskazanych wyżej sektorów, podobnie jak w latach ubiegłych, osoby, których dane dotyczyły, skarżyły się na przetwarzanie ich danych osobowych bez podstawy prawnej, w tym na nieuprawnione udostępnienie ich danych innym podmiotom.

Dane osobowe pracowników

Realizacja prawa dostępu do danych przez pracodawcę.

Były pracownik zwrócił się do spółki z pytaniem, jak przetwarza ona jego dane osobowe. Po 11 dniach spółka odpowiedziała, że dane są przetwarzane zgodnie z prawem, w związku z czym nie ma powodu do zmartwień. Odpowiedzi nie było jednak także po miesiącu, stąd skarga do UODO. Spółka wyjaśniła Prezesowi UODO, że kompletowanie odpowiedzi przeciągnęło się z przyczyn niezależnych i nie wynikało ze złej woli. O takich trudnościach spółka nie poinformowała jednak byłego pracownika, a terminy wynikające z prawa zlekceważyła. Skończyło się to upomnieniem ze strony PUODO.

Sprawa ta pokazuje stosunek wielu podmiotów przetwarzających dane osobowe, dla których ochrona danych oraz działanie zgodne z wymogami RODO jest zagadnieniem drugorzędnym i dopiero świadomość konsekwencji, jakie może nieść za sobą prowadzone wobec takich podmiotów postępowanie administracyjne w sprawie naruszenia przepisów stanowi czynnik motywujący do dostosowania operacji przetwarzania danych do obowiązującego prawa.

PUODO w 2023 r. zwrócił uwagę, że 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.

Część z takich spraw kończyła się decyzją PUODO o nałożeniu administracyjnej kary pieniężnej oraz nakazem zmiany sposobu przetwarzania danych osobowych

Dane osobowe pracowników pewnej firmy zostały zaszyfrowane w wyniku ataku ransomware. Firma ta (administrator danych) nie była w stanie przywrócić do nich dostępu. Co więcej, administrator nie zgłosił naruszenia ochrony danych osobowych Prezesowi UODO i nie powiadomił o tym fakcie osób, których dane dotyczyły. PUODO nałożył na firmę karę pieniężną. Powodem było nie to, że straciła dostęp do danych, ale to, że nie wdrożyła odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych. Takie środki powinna nie tylko mieć, ale też regularnie je testować i oceniać ich skuteczność.

Utrata pendrive'a. Prawnik w toku postępowania dyscyplinarnego wysłał pocztą nagranie z rozprawy, zawierające dane osobowe ośmiu osób i szczegóły z ich życia na niezaszyfrowanym pendrive'ie. Koperta rozerwała się i nośnik z danymi zaginął. PUODO nałożył karę za brak analizy ryzyka dla danych. Ukarany złożył skargę do WSA w Warszawie i tam oczekuje ona na rozpatrzenie.

Wojewódzki Sąd Administracyjny analizował sprawy dotyczące przetwarzania danych osobowych w firmach i wydał m.in. następujące rozstrzygnięcia:

WSA w Warszawie (II SA/Wa 714/23) podtrzymał decyzję PUODO o upomnieniu spółki za to, że **informację pozyskaną ze zwolnienia lekarskiego o tym, że skarżąca jest w ciąży, udostępnił innym pracownikom**. Sąd podzielił stanowisko PUODO, że spółka nie miała podstaw do przetwarzania takich danych. Nie można przyjąć, że informowanie o przyczynach zwolnienia lekarskiego jest niezbędne. Pracodawca może przetwarzać szczególne kategorie danych osobowych swoich pracowników, jednak dane w zakresie zdrowia podlegają rygorom z art. 9 ust. 2 RODO.

W wyroku (II SA/Wa 2256/22) sąd podzielił stanowisko Prezesa UODO, że **numer telefonu to dana osobowa** niezależnie od tego, czy podmiot posiada dodatkowe dane lub informacje identyfikujące konkretną osobę. Jest to kolejne orzeczenie potwierdzające to stanowisko. Spółka wykorzystywała numer telefonu, aby oferować usługi i produkty. PUODO uznał, że skarżący nie mógł spodziewać się przetwarzania jego danych do celów marketingowych. Nie miał bowiem żadnych związków z tą firmą. Spółka dane usunęła, a PUODO udzielił jej upomnienia. Spółka zaskarżyła tę decyzję twierdząc, że numer telefonu nie stanowi danych osobowych, a zatem do przetwarzania tych informacji nie stosuje się przepisów RODO. Sąd podzielił zdanie PUODO, że spółka przetwarzała dane osobowe w postaci numeru telefonu skarżącego bez podstawy prawnej.

WSA w Warszawie (II SA/Wa 355/22) podtrzymał decyzję Prezesa UODO, że **komornik mógł przetwarzać dane skarżącego zawiadamiając jego byłego pracodawcę o zajęciu wierzytelności.** Sąd podzielił stanowisko organu nadzorczego, uznając że komornik przetwarzał dane osobowe skarżącego zgodnie z art. 6 ust. 1 lit. c) RODO, tj. dla potrzeb prowadzonej egzekucji - w celu wypełnienia ciążącego na nim obowiązku prawnego.

Sektor finansowy

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

W 2023 r., tak jak w latach poprzednich, ludzie skarżyli się do PUODO na proces przetwarzania ich danych związanych z zawieraniem różnego rodzaju umów, przede wszystkim kredytowych. Banki swoje roszczenia wobec klientów przekazywały firmom windykacyjnym, a także funduszom inwestycyjnym. Zasadności tych roszczeń PUODO nie może oceniać, ale sprawdza, czy przy przetwarzaniu danych nie doszło do naruszenia praw osób, których dane dotyczą.

W roku 2023 Prezes UODO rozpoznawał także skargi na proces przetwarzania danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego, dokonywany przez instytucje pożyczkowe. Problem polegał na tym, że instytucje finansowe przetwarzały dane osobowe powołując się na tajemnicę bankową (art. 105a ust. 3 Prawa bankowego), choć nie łączyła ich z podmiotami danych żadna umowa. Powinny więc mieć zgodę na przetwarzanie danych.

Przetwarzanie przez bank danych osobowych ze skanu dowodu osobistego. Klient banku spłacił kredyt i poprosił o potwierdzenie tego faktu. Bank uzależnił wydanie zaświadczenia od uzyskania skanu dowodu osobistego. W ocenie Prezesa UODO, bank powinien w pierwszej kolejności rozważyć, czy do realizacji celu, jakim było udzielenie osobie, której dane dotyczą informacji o spłaconym kredycie, niezbędne było pozyskanie skanu jej dowodu. Zdaniem PUODO nie było takiej potrzeby. Zatem dane były przetwarzane w sposób nieuprawniony. Ostatecznie skan ten został usunięty.

Przetwarzanie danych osobowych przez firmy windykacyjne w celu dochodzenia wierzytelności nabytych w wyniku cesji wierzytelności. Wiele postępowań dotyczyło przetwarzania danych w związku z dochodzeniem roszczeń. W tego rodzaju postępowaniach poruszana była często kwestia udostępniania danych przez wierzyciela pierwotnego na rzecz innego podmiotu w oparciu o zawierane na podstawie art. 509 K.c. umowy cesji wierzytelności. Wiąże się ona z uprawnieniem do przekazania danych osobowych dłużnika umożliwiających podjęcie działań zmierzających do odzyskania należności. Prezes UODO w postępowaniach tych stwierdzał najczęściej, że takie udostępnienie danych osobowych przez wierzycieli nie może być oceniane jako naruszające prawa i wolności osoby, której dane dotyczą, będącej dłużnikiem. Osoba ta - jako dłużnik - musi liczyć się z tym, że kiedy zwleka w spełnieniu zobowiązania, jej prawo do prywatności może zostać ograniczone ze względu na dochodzenie przez wierzyciela należnych mu zobowiązań finansowych.

Przetwarzanie danych osobowych przez zakład ubezpieczeń w związku z zawarciem umowy ubezpieczenia cywilnego. Skarżący w trakcie trwania ubezpieczenia OC zbył ubezpieczony pojazd, nie informując zakładu ubezpieczeń o sprzedaży, choć taki obowiązek wynika z ustawy o ubezpieczeniach obowiązkowych (art. 32 ust. 1). Ubezpieczyciel powiadomił skarżącego, że wznowił umowę, bo taki ma obowiązek. Prezes UODO nie dopatrzył się nieprawidłowości w procesie przetwarzania danych osobowych przez zakład ubezpieczeniowy. Dane osobowe osoby, która złożyła skargę, były przetwarzane w celu wykonywania umowy ubezpieczenia, zaś korespondencja została do niej skierowana w związku z obowiązkiem wynikającym z ustawy o ubezpieczeniach obowiązkowych (art. 28).

Przykłady spraw, które zakończyły się decyzją PUODO o nałożeniu administracyjnej kary pieniężnej oraz nakazem zmiany sposobu przetwarzania danych osobowych

Ujawnienie danych osobowych przez brokera ubezpieczeniowego. Broker ubezpieczeniowy (administrator danych), chcąc umożliwić swoim pracownikom pracę zdalną, zlecił podmiotowi przetwarzającemu (wykonującemu na jego rzecz usługi informatyczne) wdrożenie takiego rozwiązania. W wyniku zmian wprowadzonych w systemie informatycznym doszło do niezamierzonej publikacji danych osobowych obejmującej szeroki zakres danych. Sprawa ta skończyła się decyzją PUODO o nałożeniu administracyjnej kary pieniężnej za naruszenie polegające na niewdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych, co doprowadziło do naruszenia ich poufności i rozliczalności.

Wojewódzki Sąd Administracyjny analizował sprawy dotyczące przetwarzania danych osobowych przez instytucje finansowe i wydał m.in. przytoczone poniżej rozstrzygnięcia

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

WSA (II SA/Wa 2198/22) uznał, że interpretowanie obowiązku poinformowania podmiotu danych wyłącznie w oparciu o przepisy Kodeksu cywilnego jest nieprawidłowe. Zdaniem sądu prawidłowa wykładnia zawartego w art. 105a ust. 3 Prawa bankowego zwrotu „poinformowania tej osoby" winna uwzględnić nie tylko treść normy zawartej w art. 61 § 1 K.c., ale także tę część normy zawartej w art. 105a ust. 3 ustawy — Prawo bankowe, która ustanawia dodatkowy trzydziestodniowy termin na wykonanie zobowiązania. Skoro to bank wywodzi skutki prawne z powiadomienia uczestnika o zamiarze przetwarzania jego danych osobowych stanowiących tajemnicę bankową bez jego zgody, to musi wykazać, że bezskutecznie upłynęło 30 dni od daty poinformowania go o tym zamiarze. Wykazanie tej okoliczności wymaga jednak wskazania początku biegu owego trzydziestodniowego terminu.

WSA (II SA/Wa 1554/22) oddalając skargę na decyzję Prezesa UODO WSA wskazał, że możliwość zapoznania się z treścią oświadczenia przez adresata nie może być utożsamiana z rzeczywistym zapoznaniem się przez niego z tym oświadczeniem (faktem zapoznania się). Sąd uznał, że skany (pliki pdf) oświadczenia z podanym numerem przesyłki i datą nadania oraz fragmentem elektronicznej książki nadawczej nie pozwalały stwierdzić, że bank poinformował (umożliwił zapoznanie się z informacją w zwykłym biegu zdarzeń) podmiot danych o zamiarze przetwarzania jego danych osobowych na podstawie art. 105a ust. 3 Prawa bankowego.

Problem instytucji świadczących usługi publiczne

Instytucje publiczne na wielką skalę przetwarzają cyfrowo dane, które wcześniej przetwarzały w sposób tradycyjny. Z uwagi na rozmiar tego zjawiska rosną ryzyka dla osób, których dane dotyczą.

Niepokojącym trendem jest w Polsce tworzenie przepisów przewidujących przetwarzanie danych osobowych na wielką skalę lub prowadzących do łączenia różnych baz i rejestrów, bez wnikliwej analizy wszystkich aspektów przetwarzania. W tym bez oceny wiążących się z tym ryzyk.

Konieczny jest przegląd przepisów dotyczących wykorzystywania i upubliczniania numeru PESEL, który jest krajowym numerem identyfikacyjnym w rozumieniu RODO.

W 2023 r. PUODO wskazał na ten problem m.in. opiniując projekt ustawy o zmianie ustawy o statystyce publicznej czy w wystąpieniu do Prezesa Zarządu Krajowej Rady Izb Rolniczych (PESEL jest ujawniany w siedzibie gminy w spisie członków izby rolniczej uprawnionych do głosowania w wyborach do walnych zgromadzeń izb rolniczych).

Przykłady z działania UODO pokazują, z jakim wyzwaniem się mierzymy.

Służba zdrowia

System ochrony zdrowia gromadzi szczegółowe dane osobowe na nasz temat, które stanowią dane szczególnych kategorii (np. dane o stanie zdrowia). Ze skarg napływających do Prezesa UODO widać, że dane te są wykorzystywane przez osoby nieuprawnione albo są przetwarzane do niewłaściwych celów. Upowszechnienie wiedzy, że jest to działanie sprzeczne z prawem, wymagać będzie dużo wysiłku.

Przykładem są skargi na lekarzy i pracowników ich gabinetów, którzy w różnych niemedycznych sytuacjach życiowych bezprawnie pozyskiwali potrzebne im dane osobowe z Platformy Usług Elektronicznych Zakładu Ubezpieczeń Społecznych (PUE ZUS).

Lekarz pozyskał dane świadka w sporze cywilnym z PUE ZUS. W procesie o zniesławienie, które pewien lekarz wytoczył dziennikarzowi (i sprawę wygrał) jako świadek obrony zeznawała kobieta, która twierdziła, że była pacjentką tego lekarza. Lekarz złożył zawiadomienie o składaniu fałszywych zeznań: kobieta nigdy się u niego nie leczyła. Lekarz dane tej kobiety pozyskał z PUE ZUS. Stał na stanowisku, że działa na potrzeby toczącego się postępowania karnego, a więc ze względu na swój prawnie uzasadniony interes. PUODO zauważył, że uzasadnionym interesem lekarza może być cel zawodowy lub związany z działalnością zawodową. W ocenie PUODO lekarz nie miał prawa używać danych osobowych z PUE ZUS do celów sporu sądowego. Sprawa zakończyła się upomnieniem.

Lekarz sprawdzał w PUE ZUS dane matki swojego dziecka, z którą jest w konflikcie. Sprawdzał, czy rzeczywiście ma ona zwolnienie lekarskie na opiekę nad ich dzieckiem. Tłumaczył, że półtora roku temu matka dziecka odcięła go od informacji o dziecku, w tym o stanie jego zdrowia. PUE ZUS było jedynym sposobem, by dowiedzieć się czy dziecko choruje. Niestety, żadne przepisy nie pozwalają na takie przetwarzanie danych osobowych. Sprawa skończyła się upomnieniem

Pracownik gabinetu lekarskiego potwierdzał w PUE ZUS, czy ma poprawne dane adresowe znajomego. Administrator danych uznał, że postępowanie to tłumaczy „sytuacja rodzinna". W ocenie Prezesa UODO było to jednak naruszenie RODO. Dostęp do danych zgormadzonych na profilu PUE ZUS nie był związany ze świadczeniem na rzecz osoby wnoszącej skargę usług medycznych.

Asystent medyczny wszedł na PUE ZUS z konta lekarza w przychodni i sprawdzał, czy nieobecny pracownik ma zwolnienie lekarskie. Osoba, której dane sprawdzano, poskarżyła się do PUODO, że nie było żadnych podstaw do zaglądania na jej konto. Tego dnia nie miała wizyty lekarskiej. Prezes UODO zauważył, że do korzystania z PUE ZUS trzeba mieć swoje konto i mieć w nim zdefiniowaną rolę, w jakiej się występuje. Uznał za niedopuszczalne używanie konta lekarza w celu sprawdzenia danych pracownika. PUODO udzielił przychodni upomnienia.

Lekarz sprawdzał dane w PUE ZUS w sprawach związanych ze sprawami pracowniczymi innej osoby. Oboje pracowali w jednej spółce, nie wiązały ich relacje lekarz-pacjent. Lekarz nie był też faktycznym pracodawcą skarżącej – była nim spółka, która go do takiego działania nie upoważniła. Jak się okazało, do sytuacji doszło dlatego, że osoba upoważniona do

czynności w imieniu płatnika składek na ZUS, była nieobecna. Prezes UODO upomniał lekarza, że wykorzystywanie możliwości lekarza w sytuacji, gdy wykonuje zadania dla pracodawcy, i to bez upoważnienia, nie jest właściwe.

Recepty i skierowania na badania wystawiane przez nieznanych lekarzy. Ludzie skarżyli się, że na ich Internetowym Koncie Pacjenta (IKP) pojawiały się informacje o wystawieniu im recept albo skierowań przez lekarzy, których nie znali. Zlecenia te miały status zrealizowanych, zaś błędne wpisy i wystawiane recepty zniekształcały ich historie choroby. W toku postępowań administratorzy (placówki medyczne, lekarze) wskazywali, że do wystawienia recept/skierowań dochodziło m.in. w wyniku omyłki i błędnej weryfikacji pacjenta. Zdaniem PUODO nie był to jednak drobny błąd. Dochodziło do niego w wyniku zaniedbania obowiązków ciążących na administratorze danych. Sprawy te zakończyły się upomnieniami.

Szkoły i uczelnie

Szkoły i placówki oświatowe dysponują danymi osobowymi dzieci i młodzieży, a także ich opiekunów. Jeśli nie myśli się w kategoriach ryzyka dla tych danych – i dla osób, których te dane dotyczą – łatwo o problemy.

Skalę problemu pokazują skargi i pytania do PUODO. W 2023 r. dotyczyły one m.in. takich zagadnień, jak: legalność zawierania umów powierzenia pomiędzy ubezpieczającym a szkołą jako ubezpieczonym, przetwarzanie danych osobowych ucznia w ramach medycyny pracy, przechowywanie przez szkoły oryginałów świadectw uczniów potwierdzających ukończenie danego etapu edukacji, przetwarzanie wizerunku ucznia, przetwarzanie danych absolwentów czy wycofanie przez ucznia zgody na przetwarzanie jego danych osobowych przez szkołę.

Skutki nieprawidłowej anonimizacji danych osobowych przy udostępnianiu informacji publicznej
Matka ucznia poskarżyła się do kuratorium na nieprawidłowości w szkole. Kurator przeprowadził kontrolę doraźną, a protokół z niej został udostępniony na BIP szkoły. Były w nim dane skarżącej: jej imię, początek nazwiska i informacja, w której klasie uczy się jej dziecko. Anonimizacja była więc nieskuteczna – łatwo można było ustalić dane tej osoby. Prezes UODO ocenił, że szkoła udostępniając protokół w wersji spseudonimizowanej, naruszyła zasadę minimalizacji danych określoną w art. 5 ust. 1 lit. c) RODO. Ujawnienie tych danych nie było adekwatne, stosowne ani ograniczone do celu, w którym były przetwarzane (w tym wypadku – udostępnieniu informacji o wynikach kontroli).

Udostępnienie danych osobowych małoletniego na grupie internetowej osobom nieuprawnionym. Przedszkole podało na grupie internetowej listę przyjętych dzieci. Jedno dziecko miało przy nazwisku dopisek „o”. Zdaniem jego opiekunki przedszkole ujawniło w ten sposób, że dziecko ma orzeczenie o niepełnosprawności i potrzebie kształcenia specjalnego. Przedszkole tłumaczyło, że listę opublikował sam nauczyciel, nie była ona opatrzona legendą, więc „o” mogło na niej znaczyć wiele różnych rzeczy (obserwację, opinię, orzeczenie czy konieczność dodatkowego odpoczynku). Prezes UODO wskazał, że za

publikację listy odpowiada przedszkole, a publikacja jej w zamkniętej grupie internetowej nie wypełnia obowiązku publicznego ogłoszenia listy przyjętych dzieci. Natomiast literka „o" nie dawała się połączyć jednoznacznie z konkretną kategorią danych osobowych. Ze względu na fakt, że lista dzieci przyjętych do przedszkola została usunięta tego samego dnia co dzień jej publikacji, Prezes UODO zadecydował, że wystarczające będzie zastosowanie wobec przedszkola upomnienia.

Młodzieżowy ośrodek wychowawczy (MOW) dochodzi należności za wyżywienie od osoby, która przywiozła małoletniego. MOW postanowił dochodzić należności za wyżywienie wychowanka od osoby, która przywiozła go do ośrodka. Ta osoba nie była jednak prawnym opiekunem młodocianego. Prezes UODO nie stwierdził tu nieprawidłowości, bo dane osobowe zostały przekazane tylko sądowi, który mógł w tej sytuacji ocenić, kto odpowiada za młodocianego. Sąd uznał stanowisko MOW. Skarżący mógł skorzystać z przysługujących mu uprawnień i złożyć sprzeciw wobec wydanego przez sąd rejonowy nakazu zapłaty. Przepisy o ochronie danych osobowych nie mają w tej sprawie zastosowania.

Przykłady spraw, które zakończyły się decyzją PUODO o nałożeniu administracyjnej kary pieniężnej oraz nakazem zmiany sposobu przetwarzania danych osobowych.

Publiczna uczelnia przypadkowo ujawniła w internecie dane kandydatów na wyjazdy organizowane w ramach studenckiej wymiany międzynarodowej. Stało się tak, bo aplikacja do rejestracji nie była odpowiednio zabezpieczona, nie mówiąc już o braku regularnego testowania skuteczności tych zabezpieczeń. Naruszenie zgłosił administrator (uczelnia). Do incydentu doszło w następstwie błędu w ramach prac programistycznych mających na celu przeniesienie aplikacji na nowy serwer produkcyjny. Incydent doprowadził do zaindeksowania niezabezpieczonych danych przez jedną z wyszukiwarek internetowych.

Prezes UODO podkreślił w uzasadnieniu decyzji, że administrator nie był zdolny wykazać w toku postępowania, iż wdrożone przez niego środki bezpieczeństwa danych były adekwatne wobec potencjalnych zagrożeń. PUODO nałożył na uczelnię karę finansową. Ta złożyła na to skargę, która oczekuje na rozpatrzenie przed WSA w Warszawie.

Problem instytucji publicznych i polityk państwowych

W 2023 do UODO wpłynęło **1328 skarg na sektor publiczny**. Przykładem problemów, z jakim mierzą się instytucje publiczne, jest ujawnianie danych osobowych na stronach Biuletynów Informacji Publicznej. Rozgraniczenie prawa dostępu do informacji publicznej i prawa do prywatności jest rzeczą wymagającą od instytucji publicznej więcej uważności.

Innym poważnym zagadnieniem jest odpowiedź na pytanie, ile i jakie dane państwo może zbierać. Nie ma wątpliwości, że polityki publiczne oparte na danych są lepsze i bardziej skuteczne. Niemniej przetwarzanie danych zawsze wiąże się z ryzykiem dla osób, których dane dotyczą – pytanie więc, czy jest to zasadne.

Prawo do informacji publicznej i prawo do prywatności

Udostępnienie danych osobowych w uchwale opublikowanej na BIP. Gmina udostępniła na BIP dane skarżącej wraz z informacją, że jej oferta nie spełnia wymogów formalnych na

stanowisko zastępcy głównego księgowego. Władze gminy uważały, że musiały tak postąpić, bo radni przyjmując uchwałę w sprawie naboru na to stanowisko z danymi skarżącej postanowili też, że informacja ta będzie podana do publicznej wiadomości.
Prezes UODO udzielając wójtowi upomnienia przypomniał, że prawo do informacji publicznej podlega ograniczeniu m.in. ze względu na prywatność osoby fizycznej. Uchwałę można było opublikować anonimizując dane osobowe.
Udostępnienie danych osobowych w BIP w związku z publikacją protokołu z sesji rady powiatu. Obywatelka poskarżyła się starostwu, że dyrektor szkoły nie chce jej wypłacić świadczenia emerytalnego i odprawy. Rada powiatu zajęła się skargą podczas sesji, a w protokole z obrad znalazły się dane skarżącej. Dokument ten został ujawniony na podstawie przepisów o dostępie do informacji publicznej. Upominając starostę PUODO podkreślił, że nie było żadnego powodu, by dane skarżącej publikować na BIP. Doszło więc do naruszenia RODO. Ważne w tej sprawie było to, że zanim Prezes UODO wydał decyzję, starostwo usunęło dane skarżącej ze strony BIP.

Udostępnienie stronom postępowania administracyjnego danych osoby zgłaszającej naruszenie. Skarżąca poinformowała burmistrza o naruszeniu przepisów ustawy o ochronie przyrody w związku z wycinką drzew. Burmistrz wszczął postępowanie i wydał decyzję administracyjną. Poinformował w niej, że dostał skargę i podał dane skarżącej, choć nie była ona stroną postępowania administracyjnego. Prezes UODO wskazał, że działanie takie nie znajdowało podstaw w przepisach K.p.a., które pozwalają na zbadanie sygnalizowanych przez obywateli nieprawidłowości poprzez wszczęcie postępowania z urzędu, bez konieczności ujawniania źródła pozyskanych informacji. PUODO udzielił burmistrzowi upomnienia.

Przykłady kolejnych spraw, które zakończyły się decyzją PUODO o nałożeniu administracyjnej kary pieniężnej oraz nakazem zmiany sposobu przetwarzania danych osobowych.

Ujawnienie danych osobowych lekarza przez ministra zdrowia. Minister zdrowia w 2023 r. ujawnił na platformie X dane lekarza wraz z informacją, że wystawił on na siebie receptę na leki z grupy psychotropowych i przeciwbólowych. Dane pochodziły z Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych i były przekazywane komunikatorem WhatsApp. Prezes UODO nałożył na Ministra Zdrowia karę finansową m.in. za bezprawne ujawnienie danych lekarza.

Zgubione pendrive'y z sądu. Pracownik sądu rejonowego zgubił trzy pendrive'y (jeden służbowy – szyfrowany i dwa nieszyfrowane - prywatne) z danymi nieustalonej liczby osób. Prezes UODO wykazał w postępowaniu naruszenie, za które nałożył karę pieniężną. Naruszenie polegało na niewdrożeniu przez sąd odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu przenośnych pamięci. Z analizy ryzyka przeprowadzonej przez sąd przed powstaniem naruszenia wynika, że administrator danych przewidział zagrożenie utraty poufności poprzez utratę danych na niezabezpieczonych nośnikach i wprowadził odpowiednie zabezpieczenia. Nie przewidział jednak, że dane zostaną przegrane na prywatny, niezabezpieczony nośnik, a potem utracone. PUODO wskazał, że warto

wprowadzić blokadę dla prywatnych pendrive'ów lub wprowadzić obowiązek ich szyfrowania. WSA w Warszawie, po skardze sądu utrzymał decyzję PUODO w mocy.

MSZ zawiadomił Sąd Okręgowy w Krakowie, że konsul w Wielkiej Brytanii otrzymał uszkodzoną przesyłkę z danymi osobowymi kilku osób. Koperta była rozdarta i każdy mógł te dane podejrzeć. Dokumenty zostały wysłane na wniosek sądu, który był ich administratorem. Sąd tego naruszenia ochrony danych nie zgłosił PUODO i nie zawiadomił osób, których dane znajdowały się w dokumentach. PUODO wskazał, że inspektor ochrony danych sądu błędnie ocenił, że ryzyko dla danych nie jest wysokie, bo koperta rozdarła się w Wielkiej Brytanii, a dokumenty były po polsku. Prezes UODO zauważył, że dziś dostępne są narzędzia do szybkiego tłumaczenia tekstów, a Polonia na Wyspach jest liczna, więc nie można tak tłumaczyć tej sprawy. PUODO wydał decyzję o nałożeniu kary finansowej. Decyzja jest nieprawomocna i czeka na ocenę WSA w Warszawie.

Prokuratura rejonowa na wniosek dziennikarza przekazała mu niezanonimizowane dokumenty. Naruszenie dotyczyło danych trzech osób, w tym dziecka, zaś administrator nie zgłosił go do PUODO i nie zawiadomił zainteresowanych. Następnie administrator (czyli prokuratura) odmówił wszczęcia śledztwa w sprawie naruszenia ochrony danych uznając, że do niego nie doszło. W toku postępowania administracyjnego PUODO ustalił, że prokuratura nie przeprowadziła analizy ryzyka w zakresie ochrony danych, więc jej twierdzenie, że do naruszenia nie doszło, nie było uprawdopodobnione. Sama odmowa wszczęcia postępowania nie jest wystarczającą podstawą do takiego wniosku w świetle RODO. WSA w Warszawie utrzymał w mocy decyzję PUODO o nałożeniu kary finansowej.

Przykłady spraw dotyczących instytucji publicznych, w których w 2023 r. wypowiedział się WSA w Warszawie

WSA w Warszawie (II SA/Wa 1944/21), a następnie Naczelny Sad Administracyjny (III OSK 595/22) podtrzymał decyzję Prezesa UODO nakazującą burmistrzowi usunięcie z nagrania z sesji rady miejskiej na stronie internetowej, danych osobowych skarżącego w zakresie nazwiska. WSA podzielił stanowisko PUODO, że w niniejszej sprawie wyłączenia z ustawy o dostępie do informacji publicznej nie występują, albowiem dane osobowe ujawnione w nagraniu nie dotyczą osoby pełniącej funkcję publiczną, jak również skarżący nie zrezygnował z przysługującego mu prawa do prywatności. NSA doprecyzował, że ustawa o dostępie do informacji publicznej wyklucza uznanie za osoby pełniące funkcje publiczne takie osoby, które są znane publicznie (w skali całego kraju lub określonej wspólnoty regionalnej lub lokalnej), lecz pozostające poza strukturami aparatu państwa.

WSA w Warszawie (III OSK 595/22) podtrzymał decyzję Prezesa UODO w sprawie upomnienia administratora, który naruszył zasadę minimalizacji danych, poprzez gromadzenie w aktach osobowych skarżącego dokumentów, które w istocie są zbędne do osiągnięcia celu przetwarzania (na kopercie pocztowej oprócz imienia, nazwiska i adresu skarżącego było też jego stanowisko służbowe i miejsce pracy).

WSA w Warszawie (II SA/Wa 446/23) utrzymał upomnienie PUODO dla prezydenta miasta za udostępnienie numeru tablicy rejestracyjnej pojazdu skarżącego (osoby pełniącej funkcję publiczną) podczas obrad sesji rady miasta. Sąd podzielił stanowisko PUODO, że numer

tablicy rejestracyjnej skarżącego stanowi w niniejszym postępowaniu jego dane osobowe, ponieważ równocześnie zostały ujawnione jego imię i nazwisko.

Służby graniczne

System Informacyjny Schengen (SIS) to najskuteczniejsze narzędzie zapewniające efektywną współpracę między organami imigracyjnymi, policją, organami celnymi i organami sądowymi w UE i państwach stowarzyszonych w ramach Schengen. Umożliwia wprowadzanie i przeglądanie danych dotyczących osób poszukiwanych, osób, które mogą nie mieć prawa do wjazdu lub pobytu na terytorium UE oraz osób zaginionych – w szczególności dzieci. Po zmianie prawa można w nim wprowadzać tzw. „wpisy prewencyjne" – władze w państwach członkowskich mogą wskazywać dzieci, w przypadku których ryzyko uprowadzenia jest szczególnie duże. Zmiany te oznaczają, że funkcjonariusze straży granicznej i służby wymiaru sprawiedliwości zostaną powiadomieni w przypadku występowania dużego ryzyka rychłego uprowadzenia dziecka przez jednego z rodziców i będą w stanie dokładniej zbadać okoliczności podróży takiego dziecka, w razie potrzeby stosując wobec niego pieczę ochronną. Po zmianie tych przepisów PUODO przeprowadził kontrolę sektorową, jak zbierane i przetwarzane są dane o dzieciach.

Policja i służby mundurowe

W 2023 r. w sprawach dotyczących działalności Policji, PUODO przychylał się do jej argumentacji i nie interweniował w sprawach z zakresu ochrony danych osobowych, choć sprawdzał zakres ich przetwarzania przez policję i analizował skargi na mundurowych.

Przetwarzanie danych osobowych w Krajowym Systemie Informacyjnym Policji (KSIP). W systemie tym Policja zbiera wszystkie dane o osobach będących w jej zainteresowaniu. Baza zawiera informacje o osobach skazanych za różne przestępstwa i zachowuje wiedzę o tym nawet wtedy, kiedy samo przestępstwo uległo zatarciu. PUODO dostaje więc wiele skarg od osób, których danych Policja nie chciała z KSIP usunąć, mimo że o to wnosiły. Choć Policja zbiera dane osobowe do KSIP zgodnie z prawem, PUODO zauważył, że nie oznacza to możliwości nieograniczonego w czasie przetwarzania tych danych. Na gruncie przepisów obowiązującej ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przetwarzane dane osobowe podlegają okresowej weryfikacji i usunięciu w przypadku uznania za niecelowe dalsze ich przetwarzanie. Komendant Główny Policji ma obowiązek dokonywania weryfikacji danych osobowych nie rzadziej niż co 10 lat. Ma sprawdzać, czy istnieją dane, których dalsze przechowywanie jest zbędne. Jednocześnie w 2023 r. Prezes UODO uznawał argumenty Policji, że nadal potrzebuje ona konkretnych danych „w związku z naruszeniem norm prawnokarnych przez skarżącego oraz rodzajem norm naruszonych".

Udostępnienie przez Policję sanepidowi danych osobowych osoby, która nie zakryła ust i nosa maseczką. Chodziło tu o sytuacje z czasów pandemii koronawirusa: policjanci legitymowali osoby bez maseczek, a następnie przekazywały ich dane sanepidowi. Inspekcja sanitarna mogła ukarać takie osoby w postępowaniu administracyjnym karą do 30 tys. zł. Pytanie jednak, czy Policja miała prawo przekazywać te dane sanepidowi.

Rzecznik Praw Obywatelskich (RPO) stanął na stanowisku, że nie, gdyż policyjna notatka nie jest dokumentem wydanym przez organ, a tylko taki dokument może być używany w postępowaniu administracyjnym. Dlatego RPO zaskarżał przed sądami administracyjnymi kary administracyjne nakładane na obywateli na podstawie notatek policyjnych.
Prezes UODO zajął podobne stanowisko: Policja nie ma podstaw do przekazywania danych osobowych sanepidowi. Uznał jednak, że udostępnienie danych osobowych sanepidowi już nastąpiło i jest procesem nieodwracalnym, wobec tego w 2023 r. odmówił uwzględnienia wniosku skarżącego.

Inspektorzy ochrony danych i ich rola

Inspektorzy ochrony danych pełnią kluczową rolę w tworzeniu skutecznego systemu ochrony danych osobowych w Polsce i w całej Unii Europejskiej. To oni wspierają administratorów w realizacji obowiązków dotyczących ochrony danych osobowych. Pełnią też funkcję punktu kontaktowego dla osób, których dane dotyczą oraz dla organu nadzorczego.

Jednocześnie IOD mają prawo zwrócić się do Prezesa UODO o konsultację. Dlatego współpraca z inspektorami ochrony danych jest dla PUODO niezmiernie istotna. Pytania inspektorów są ważnym źródłem wiedzy na temat problemów, z jakimi się oni mierzą. Inspektorzy trafnie identyfikują problemy prawne wynikające np. z luk w przepisach lub ich nieodpowiedniej interpretacji W takich sytuacjach IOD oczekują od UODO wskazówek lub podjęcia stosownych działań, np. skierowania wystąpienia legislacyjnego.

W 2023 roku do Urzędu Ochrony Danych wpłynęły **253 pytania od inspektorów ochrony danych**. Prezes UODO udzielił **246 odpowiedzi**. Nieznaczny spadek liczby pytań (w 2022 r. były 274 pytania, w 2021 r. 301) wynikać może z tego, że wiele kwestii zostało wyjaśnionych w poprzednich latach.

Z każdym rokiem pytania IOD coraz rzadziej dotyczą kwestii podstawowych, a raczej bardziej złożonych problemów obejmujących nieprawidłowości i zagrożenia, które mogą wpływać na niezależność inspektora i skuteczne wykonywanie jego funkcji (np. pełnienie przez IOD funkcji pełnomocnika administratora). Inspektorzy z dużym wyczuciem identyfikują zagrożenia dla ochrony danych osobowych wnikające z luk prawnych lub nieprecyzyjnie skonstruowanych przepisów prawa albo też nieprawidłowej ich interpretacji.

Pierwsza grupa pytań IOD obejmowała zagadnienia, które pojawiają się niezmiennie od kilku lat. Chodzi tu o występowanie konfliktu interesów w związku z pełnieniem funkcji IOD, określenie statusu podmiotów biorących udział w procesie przetwarzania danych osobowych, udostępnianie danych osobowych czy problemy ze stosowaniem w praktyce zarówno przepisów prawa dotyczących ochrony danych osobowych, jak i przepisów sektorowych.

Druga grupa pytań dotyczyła w 2023 r. wydarzeń i problemów bieżących, takich jak kwestie statusu podmiotów przetwarzających dane osobowe na potrzeby organizacji wyborów do parlamentu, czy zagadnienia związane z przetwarzaniem danych osobowych w związku ze stosowaniem przepisów ustawy o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli, która weszła w życie w 2023 r.

Prezes UODO udzielał na nie odpowiedzi na stronie internetowej UODO lub w Newsletterze UODO dla IOD, późniejszym Biuletynie UODO. Sygnalizował też właściwym podmiotom zaobserwowane nieprawidłowości lub potrzeby zmian legislacyjnych.

Ważnym problemem jest to, że administratorzy danych (pracodawcy) nakładają na IOD dodatkowe obowiązki, które mogą utrudniać im wykonywanie zadań dotyczących ochrony danych osobowych. IOD nie może być odpowiedzialny za wykonanie zadania administratora, np. za zgłaszanie naruszeń i jednocześnie monitorować, czy to zadanie wykonywane jest prawidłowo. Taka sytuacja może mieć miejsce, np. w przypadku udzielania inspektorowi pełnomocnictwa do reprezentowania administratora w sprawach dotyczących ochrony danych osobowych. Zadaniem IOD jest bowiem informowanie administratora o obowiązkach spoczywających na nim na mocy RODO oraz monitorowanie wykonania tych obowiązków (art. 39 ust. 1 lit. a i b RODO). Występowanie w roli pełnomocnika administratora w zakresie obowiązków nałożonych na administratora może istotnie utrudniać lub uniemożliwiać inspektorowi niezależną ocenę, czy obowiązki administratora są w ogóle realizowane i czy są wykonywane prawidłowo.

Warto wiedzieć, że w 2023 r. sytuację inspektorów analizowała Europejska Rada Ochrony Danych RODO (EROD – więcej o współpracy PUODO z Radą niżej). Prezes UODO przekazał do raportu EROD następujące, zidentyfikowane polskie problemy dot. IOD:

- obciążanie IOD obowiązkami administratora, np. prowadzeniem rejestru czynności przetwarzania,
- zawieranie umowy powierzenia przetwarzania danych osobowych pomiędzy administratorem a IOD,
- udzielanie IOD pełnomocnictwa do reprezentowania administratora w sprawach z zakresu ochrony danych osobowych,
- świadczenie przez firmy zatrudniające inspektorów ochrony danych usług outsourcingu funkcji IOD i jednocześnie usług polegających na wykonywaniu za administratora tzw. „wdrożenia RODO”.

W swoim raporcie EROD stwierdziła, że we wszystkich państwach trzeba prowadzić więcej działań uświadamiających, informacyjnych i egzekucyjnych (powinny robić to organy nadzorcze takie jak PUODO). Inspektorzy ochrony danych powinni mieć dosyć możliwości, czasu i zasobów na odświeżenie wiedzy i zapoznanie się z najnowszymi rozwiązaniami.

Kodeksy postępowania i akredytacje

RODO (art. 40) jest podstawą do tworzenia kodeksów postępowania, których celem jest doprecyzowanie i pomoc w stosowaniu RODO w danej branży.

Przygotowanie kodeksu postępowania to proces długotrwały, wymagający wytężonej i skrupulatnej pracy. Zainteresowani mogą sięgnąć do Sprawozdania, bo wylicza ono błędy, jakich w tej pracy można uniknąć.

Przyjęcie kodeksu daje wiele korzyści. Nie jest nią tylko gwarancja pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy. Administratorzy mogą także

liczyć na nadzór nad procesami przetwarzania danych osobowych przez niezależny podmiot monitorujący kodeks.

Takie podmioty monitorujące w celu uzyskania akredytacji PUODO muszą wykazać swoją niezależność w stosunku do twórcy kodeksu oraz to, że mają odpowiednie zasoby do pełnienia swojej roli.

Dotychczas Prezes UODO zatwierdził dwa kodeksy. Pierwszy z nich został zatwierdzony w 2022 r. „Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych" opracowany przez Federację Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie. Akredytacji do monitorowania jego stosowania udzielił spółce Jamano. Natomiast w 2023 r. organ nadzorczy zatwierdził Kodeks postępowania dla sektora ochrony zdrowia, przygotowany przez Polską Federację Szpitali i udzielił akredytacji spółce KPMG Advisory do monitorowania przestrzegania jego postanowień. Dokument ten to pierwszy w Europie kodeks obejmujący podmioty publiczne i prywatne z sektora medycznego.

W sieci instytucji europejskich

PUODO współpracuje z innymi organami nadzorczymi. Współpraca ta daje lepsze gwarancje ochrony danych w Europie niż działanie w pojedynkę i zapewnia jednakowe stosowanie RODO w państwach UE..

Sieć współpracy jest kluczowa dla skarg, których przedmiotem jest transgraniczne przetwarzanie danych. Takie skargi rozpatruje bowiem organ nadzorczy w kraju, w którym siedzibę lub przedstawicielstwo ma administrator (podmiot, na który wnosimy skargę). Poprzez szeroką współpracę i współdziałanie wszystkich organów nadzorczych w zakresie ochrony danych osobowych, rozpatrywanie skarg transgranicznych ma, zdaniem Prezesa UODO, znaczny wpływ na większą świadomość korzystania ze swoich praw przez skarżących.

Sprawy dotyczące takich administratorów jak Meta czy Twitter są we właściwości irlandzkiego organu nadzorczego (Data Protection Commission), gdyż spółki te mają swoje przedstawicielstwa w Irlandii. Z tego powodu tamtejszy organ jest wiodący w sprawach naruszenia przepisów o ochronie danych wobec osób znajdujących się w UE. Postępowania wobec tzw. gigantów technologicznych powodują zawsze większy rozdźwięk społeczny, który wpływa na świadomość ludzi.

Należy zauważyć, że o ile współpraca z niemieckimi organami nadzorczymi, a także z francuskim czy irlandzkim organem nadzorczym przebiega sprawnie, to kontakt z włoskim, luksemburskim oraz holenderskim organem nadzorczym bywał w 2023 r. utrudniony, m.in. z uwagi na różnice w zakresie stosowanych krajowych procedur występujących w prowadzonych postępowaniach.

W 2023 r. skargi o charakterze transgranicznym dotyczyły najczęściej realizacji praw skarżących wobec administratorów oferujących dostęp do portali społecznościowych, takich jak Facebook oraz Instagram, zwłaszcza w zakresie prawa dostępu do danych oraz prawa usunięcia danych, jak również braku przejrzystej komunikacji z administratorem, czy braku udzielenia terminowej odpowiedzi na żądania ujęte w rozdziale III RODO. W ramach

postępowań, zainicjowanych skargami, które wpłynęły w 2023 r. administratorzy zazwyczaj udzielali wyczerpujących odpowiedzi na zadane pytania oraz nie ukrywali ewentualnych naruszeń ochrony danych, tłumacząc je często błędem ludzkim.

Konta użytkowników na dużych platformach mediów społecznościowych

Wiele skarg w 2023 r. odnosiło się do działalności dużych platform mediów społecznościowych. Dotyczyły one:

- braku możliwości uzyskania dostępu do danych osobowych lub ich usunięcia,
- braku przejrzystej komunikacji z administratorem, a także
- żądania przekazania nadmiernej ilości danych w celu weryfikacji tożsamości użytkowników tych platform, na przykład skanów dokumentów tożsamości.

Tu warto wskazać, że aby pomoc PUODO (a także innych organów ochrony danych w Europie) była skuteczna, należy się od niego domagać nie przywrócenia konta lub funkcjonalności. Na to nie ma on żadnego wpływu. Jeśli konto zostało usunięte/zablokowane, PUODO może interweniować jedynie w sprawie znajdujących się na nim danych osobowych. Zadaniem Prezesa UODO jest ocena procesu przetwarzania danych osobowych, a nie kwestii związanych z obsługą kont użytkowników stron internetowych i aplikacji.

Jak zatem należy formułować skargi? Pokazała to sprawa skasowania konta na Instagramie. Skarżący wskazał, że administrator portalu bezpodstawnie odebrał mu dostęp do konta na Instagramie. A było ono połączone z działalnością zarobkową skarżącego. Stracił więc kontakt z kontrahentami i zaufanie budowane latami. Prezes UODO przekazał skargę irlandzkiemu organowi nadzorczemu (Data Protection Commission – DPC). DPC nie podjął jednak sprawy, bo – tak jak PUODO – nie ma kompetencji w sprawie przywracania kont.

DPC przesłał jednak „listę kontrolną" elementów, które w jego opinii powinna zawierać skarga o charakterze transgranicznym w sprawie danych osobowych. Skarga powinna zawierać:

1. Kopię żądania do administratora, by spełnił prawa osoby, której dane dotyczą, w tym data złożenia żądania.
2. Kopię odpowiedzi od administratora (jeśli przyszła) z datą udzielenia odpowiedzi.
3. Dowód, czy administrator skorzystał z przedłużenia o dwa miesiące terminu na realizację żądania, na podstawie art. 12 ust. 3 RODO, a jeżeli tak, to wskazanie daty poinformowania przez administratora osoby, której dane dotyczą o przedłużeniu terminu.
4. Szczegóły wszelkich dodatkowych informacji wymaganych przez administratora w celu weryfikacji tożsamości osoby, której dane dotyczą zgodnie z art. 12 ust. 6 RODO.
5. Kopie wszelkiej innej korespondencji między osobą, której dane dotyczą, a administratorem w związku z żądaniem spełnienia prawa osoby, której dane dotyczą.
6. Kopie wszelkiej stosownej korespondencji między zainteresowanym organem nadzorczym a osobą, której dane dotyczą, oraz administratorem, w stosownych przypadkach, w związku z żądaniem spełnienia prawa osoby, której dane dotyczą.

7. Kopię skargi osoby, której dane dotyczą, do zainteresowanego organu nadzorczego, przedstawiającą datę złożenia skargi.
8. Przetłumaczone dokumenty dla każdego z powyższych, jeśli jest to wymagane.

DPC wskazał, że lista kontrolna ma na celu dostarczenie innym organom ochrony danych przewodnika dotyczącego informacji i/lub dokumentów, których potrzebuje DPC w celu oceny i postępów potencjalnych skarg transgranicznych w zakresie żądania dotyczącego praw osób, których dane dotyczą, złożonych zgodnie z art. 15–22 RODO.

Irlandzki organ nadzorczy zwrócił się do Prezesa UODO z prośbą o weryfikację każdej skargi na podmiot mający siedzibę na terenie Irlandii pod kątem ww. listy kontrolnej.

Współpraca między organami nadzorczymi w ramach rozpoznawania sprawy o charakterze lokalnym. W jednej ze spraw chodziło o to, że administrator posiadający swój oddział w Rumunii, nie spełnił żądania skarżącego, by usunąć jego dane osobowe. We współpracy z rumuńskim organem nadzorczym Prezesowi UODO udało się ustalić, że sprawa ta dotyczy wyłącznie oddziału w Rumunii i ma wpływ wyłącznie na osoby, których dane dotyczą w Rumunii. Sprawa została wiec poprowadzona na szczeblu lokalnym przez rumuński organ nadzorczy na podstawie art. 56 ust. 2 RODO. Skarżący podpisywał umowy wyłącznie z oddziałem banku w Rumunii, a sprawa miała charakter indywidualny i dotyczyła nieprawidłowości w przetwarzaniu danych skarżącego.

Zapytania innych organów nadzorczych

Prezes UODO jest zobowiązany na podstawie przepisów RODO do udzielania odpowiedzi na pytania zadane mu przez inne organy nadzorcze z państw Unii Europejskiej. Obowiązki te realizowane są w oparciu o mechanizmy spójności i współpracy uregulowane w art. 63 i nast. RODO. Zapytania od innych organów nadzorczych kierowane są do polskiego regulatora za pośrednictwem Systemu IMI (Internal Market Information System), tj. Systemu Wymiany Informacji na Rynku Wewnętrznym. Tą samą drogą przekazywane są odpowiedzi na przedłożone zapytania.

W 2023 r. do Prezesa UODO wpłynęło **27 zapytań organów nadzorczych z innych państw**, w tym m.in. z: Francji, Holandii, Słowenii, Słowacji, Włoch, Lichtensteinu, Finlandii, Norwegii, Irlandii, Malty, Niemiec, Danii, Cypru. Dla porównania, w 2022 r. takich pytań wpłynęło 41, w 2021 r. – 25, zaś w 2020 r. – 14.

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 (EROD).

Szczegółowe dane o współpracy PUODO z Radą znaleźć można w Sprawozdaniu za rok 2023. Chcielibyśmy zwrócić uwagę na to, że w 2023 r. EROD przygotowała m.in.:

- przewodnik po ochronie danych dla małych firm;
- wzór formularza skargi, ułatwiającego składanie skarg przez osoby fizyczne i ich późniejsze rozpatrywanie przez organy nadzorcze w sprawach transgranicznych;
- koordynowała zadania w zakresie egzekwowania prawa przy korzystaniu z usług w chmurze przez sektor publiczny.

Grupy zadaniowe EROD

W 2023 r. pracownicy UODO reprezentowali polski organ nadzorczy także w grupach zadaniowych i sieciach EROD między innymi w :

- grupie zadaniowej ds. 101 skarg, która zajmuje się rozpatrywaniem skarg wniesionych przez organizację NOYB. 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;
- grupie zadaniowej ds. ChatGPT;
- grupie zadaniowej ds. wzajemnych relacji prawa ochrony danych osobowych, prawa konkurencji i prawa konsumentów;
- grupie zadaniowej ds. plików cookies.

EROD 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 2023 r. przedstawiciele UODO uczestniczyli w posiedzeniach:

- 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);
- Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac, który zawiera odciski palców wszystkich zarejestrowanych osób ubiegających się o azyl w państwach członkowskich UE i krajach współpracujących.

Przedstawiciel UODO uczestniczył także w pracach Komitetu Skoordynowanego Nadzoru (CSC) obejmujących działania nadzorcze nad Systemem Informacyjnym Schengen (SIS II), a także nad systemem informacyjnym rynku wewnętrznego (IMI), Eurojust i Europol.

Wiążące i pilne decyzje EROD:

EROD jest nie tylko miejscem wypracowywania stanowisk i analizowania problemów. Może w sytuacjach pilnych i nadzwyczajnych reagować korzystając z prawa, jakie dają mu art. 65 i 66 RODO. W 2023 r. EROD przyjęła dwie wiążące decyzje na podstawie art. 65 RODO i jedną pilną decyzję na podstawie art. 66 RODO.

W kwietniu 2023 r. EROD rozstrzygnęła spór dotyczący kary nałożonej na Meta Platforms Ireland Limited (Meta) oraz nakazu zapewnienia zgodności przetwarzania danych w

wiążącej decyzji nr 1/2023. Rada poleciła irlandzkiemu organowi nadzorczemu zmianę projektu decyzji i nałożenie kary na Meta. Na tej podstawie irlandzki organ nadzorczy nałożył na Meta karę w wysokości 1,2 mld euro za przekazywanie przez tę spółkę danych osobowych do USA na podstawie standardowych klauzul umownych. Meta została zobowiązana do dostosowania swoich transferów danych do przepisów RODO.

W sierpniu 2023 r. EROD rozstrzygnęła spór dotyczący projektu decyzji irlandzkiego organu nadzorczego w sprawie przetwarzania danych osobowych użytkowników w wieku od 13 do 17 lat przez TikTok Technology Limited (TikTok IE). W następstwie wiążącej decyzji EROD, irlandzki organ nadzorczy wydał ostateczną decyzję, w której stwierdził, że TikTok IE naruszył zasadę rzetelności RODO podczas przetwarzania danych osobowych dotyczących dzieci w wieku od 13 do 17 lat i nałożył upomnienie, nakaz przestrzegania przepisów oraz karę w wysokości 345 mln euro.

W następstwie pilnej decyzji wiążącej EROD nr 1/2023 z dnia 27 października 2023 roku, irlandzki organ nadzorczy przyjął 10 listopada 2023 r. ostateczną decyzję, nakładając na Meta zakaz przetwarzania danych osobowych do celów reklamy behawioralnej na podstawie umowy i uzasadnionego interesu. Wiążąca decyzja EROD w trybie pilnym została wydana w następstwie wniosku norweskiego organu nadzorczego o podjęcie ostatecznych środków, które obowiązywałyby w całym Europejskim Obszarze Gospodarczym (EOG). Początkowo norweski organ nadzorczy wprowadził trzymiesięczny zakaz przetwarzania danych osobowych obywateli Norwegii do celów reklamy behawioralnej. Zakaz obowiązywał tylko na terenie Norwegii. Rada doprowadziła swym działaniem do rozszerzania zakazu na cały EOG.

Prawo europejskie i uwagi PUODO do polskich aktów prawnych

Dla ochrony danych ważne są także orzeczenia Trybunału Sprawiedliwości Unii Europejskiej. TSUE bada sytuacje w różnych krajach Unii i analizuje różne rozwiązania – jego stanowiska oznaczają konieczność przejrzenia polskiego prawa pod kątem dostosowania do jego orzeczeń i unijnych regulacji. TSUE broni praw obywateli Polski.

Choć pytania, które zadawały sądy państw członkowskich Trybunałowi w 2023 r. dotyczyły różnorodnej tematyki, to można zauważyć, iż najczęściej związane były z obowiązkami administratora wobec podmiotów danych oraz prawem do usunięcia lub sprostowania danych. Wynikały one w dużej mierze z intensywnego rozwoju społeczeństwa informacyjnego i postępu technologicznego, co przekładało się na pytania o interpretację przepisów RODO w świetle nowych rozwiązań technologicznych.

Ze spraw, które zostały rozstrzygnięte przez TSUE w 2023 r. większość, w ocenie organu nadzorczego, nie wymagała dokonania zmian w polskim prawie. Wpływała jednak na interpretację przepisów. Jedynie odnosząc się do wyroku w sprawie C-252/21 Meta Platforms i in./Facebook e.a., Prezes UODO stwierdził konieczność zmiany przepisów. Wyrok w tej sprawie ma charakter precedensowy, ponieważ dotyczy konieczności współdziałania organu ds. konsumentów z organem ds. ochrony danych osobowych w sytuacji, gdy ta sama sprawa dotyczy zarówno ochrony praw konsumentów, jak i danych osobowych. Dlatego w zajętym stanowisku organ nadzorczy za istotne uznał podjęcie dyskusji i rozważenie przyjęcia

przepisów prawa krajowego rozstrzygających problematykę współpracy między organem nadzorczym a organem ochrony konkurencji celem uniknięcia sporów kompetencyjnych i dualizmu rozstrzygnięć.

Polskie prawo - wyzwania

Analizując wyroki TSUE i pytania prejudycjalne do TSUE z innych państw (patrz Sprawozdanie), a także przepisy RODO, Prezes UODO może zgłaszać uwagi do przygotowywanych aktów prawnych. Może też wskazywać potrzebę zmian przepisów, zanim zauważą to odpowiedzialne instytucje.

Prawodawca nie pyta PUODO o zdanie

Niestety, także w 2023 r. organy publiczne pomijały UODO w procesie konsultacji podczas prac nad nowymi przepisami. Dlatego istotne projekty aktów normatywnych dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie nie trafiały do oceny Prezesa UODO. Jest to nie tylko działanie wbrew obowiązującym przepisom i obowiązkom, ale także utrata okazji do eksperckiego wsparcia projektodawcy przez organ nadzorczy na jak najwcześniejszym etapie procesu legislacyjnego. W dużej części przypadków projekty niekonsultowane z Prezesem UODO na etapie prac legislacyjnych rządu są do niego później kierowane z prośbą o opinię/stanowisko przez Sejm i Senat.

Prawodawca nie robi testu prywatności

Przepisy RODO wymagają, by każde przetwarzanie danych osobowych było planowane z uwzględnieniem koncepcji ochrony danych (i prywatności) w fazie projektowania (*privacy by design*), jak i w czasie samego przetwarzania.

Gdy twórca przepisów przewiduje, że przetwarzanie danych osobowych będzie prowadzone z wykorzystaniem określonych rozwiązań informatycznych, to od samego początku 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,

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.

Edukacja

Choć Polacy są coraz bardziej świadomi zagrożeń w obszarze ochrony danych osobowych, wielu z nich nadal nie wie, jak właściwie zareagować w przypadku utraty danych. Nie potrafią też przewidzieć negatywnych konsekwencji takiego zdarzenia. Dodatkowo – szybki rozwój nowych technologii wciąż stawia przed nami nowe wzywania.

Dlatego dla Prezesa UODO działania edukacyjne są niezwykle ważną częścią jego aktywności. Podejmuje szeroko zakrojone działania informacyjne i edukacyjne, których różnorodna forma i dynamika przyczynia się do wzrostu świadomości obywateli. Oto przykłady:

Program edukacyjny „Twoje dane - Twoja sprawa" (TDTS) to sztandarowe przedsięwzięcie UODO, na skalę ogólnopolską. Angażuje całe społeczności szkolne, uczy małych i dużych, dociera swoim zasięgiem do uczniów, nauczycieli, dyrektorów, rodziców, a nawet seniorów. Średnio, co roku w ramach programu odbywa się kilka tysięcy lekcji i różnorodnych wydarzeń skierowanych do uczniów, nauczycieli, rodziców, seniorów i środowiska lokalnego. W każdej jego edycji bierze udział około 50 000 uczniów, a ponad 5 000 nauczycieli jest zaangażowanych w te działania. W ramach programu organizowane są webinaria z cyklu „RODO w szkolnej ławce" dla dyrektorów szkół, nauczycieli oraz szkolnych inspektorów ochrony danych, a także webinaria dla dzieci szkół podstawowych i ponadpodstawowych („Na jaką przynętę dasz się złapać?") oraz uczniów edukacji wczesnoszkolnej („Z Rodusiem chronimy dane osobowe"). Powstało ponad 4 000 cennych społecznie przedsięwzięć na rzecz ochrony danych osobowych dzieci, z których najciekawsze zostały wyróżnione w ramach organizowanych przez PUODO konkursów. Dlatego, jako wyzwane na kolejne lata dostrzegamy rozwój tego przedsięwzięcia i dotarcie z nim do coraz liczniejszej grupy odbiorców.

Urząd Ochrony Danych Osobowych opracował poradniki, wytyczne i podręczniki dla IOD w ramach działań prowadzonych wspólnie z organami nadzorczymi innych państw.

PUODO współpracuje ze szkołami wyższymi, a eksperci Urzędu wspierają swoją wiedzą ważne wydarzenia przeznaczone dla różnych odbiorców, w tym 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.

W 2023 r. eksperci UODO przeprowadzili także szkolenie dla pracowników Kancelarii Prezesa Rady Ministrów.

W 2023 roku PUODO i jego przedstawiciele aktywnie uczestniczyli w ok. 100 wydarzeniach krajowych i międzynarodowych, zorganizowanych w Polsce przez UODO lub inne podmioty oraz w ok. 200 wydarzeniach międzynarodowych i europejskich, w tym w posiedzeniach plenarnych EROD i spotkaniach podgrup.

Wyzwania stojące przed UODO

Wyzwaniem na 2024 rok będzie też weryfikowanie zapewniania właściwej ochrony danych osobowych przetwarzanych przy użyciu chmur, aplikacji, portali, wspólnych systemów czy innych rozwiązań informatycznych. Są one coraz powszechniej stosowane i – niestety – coraz częściej tworzone z pominięciem określonych w RODO zasad.

Ważnym zadaniem jest zaangażowanie się organu nadzorczego w postępowania legislacyjne wdrażające do porządku krajowego europejskich aktów horyzontalnych – zwłaszcza z tzw. pakietu cyfrowego.

Aktem, który wymagał będzie najpilniejszych prac jest Akt w sprawie zarządzania danymi (rozporządzenie Parlamentu Europejskiego i Rady 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie 2018/1724). Akt wszedł w życie 24 września 2023 r.

Drugim tak istotnym aktem jest obowiązujący od 17 lutego 2024 Akt o usługach cyfrowych (rozporządzenie Parlamentu Europejskiego i Rady 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE).

***

Jak widać, przetwarzanie danych osobowych jest zjawiskiem dotyczącym wszystkich niemalże dziedzin życia i mającym wpływ na całe życie społeczne. Prezes UODO ma świadomość, że jego praca nie może się ograniczać do działań eksperckich, co pokazuje pełny zapis Sprawozdania z jego działalności w 2023 roku.

Wnioski z realizacji swoich zadań Prezes UODO wyciąga i analizuje na bieżąco, czego efekty są już widoczne. Ważnym zadaniem PUODO jest dotarcie do szerszych grup obywateli, by skutecznie wykonywać powierzone mu zadania.

Wspomnijmy tu tylko o powołanym już w 2024 r. Społecznym Zespole Ekspertów przy Prezesie UODO, który ma ułatwiać identyfikowanie istotnych problemów związanych z danymi osobowymi oraz komunikować stanowiska PUODO.

Wypracowane przez lata poradniki dotyczące stosowania prawa danych osobowych muszą zostać zaktualizowane, co już dzieje się w 2024 r. w ramach społecznych konsultacji.

W 2024 r. PUODO zaczął też pracować nad upraszczaniem języka stosowanego w Urzędzie, w którym w zrozumiały i przystępny sposób przedstawiane są zagadnienia prawne oraz zapewniona jest dobra komunikacja z obywatelami.