URZĄD OCHRONY DANYCH OSOBOWYCH

# BIULETYN UODO
# Nr 11/11/25

www.uodo.gov.pl

# SPIS TREŚCI

**Szanowni Państwo,**

5 listopada, w ramach akcji „UODO rusza w kraj”, wraz z ekspertami Urzędu Ochrony Danych Osobowych odwiedziłem Płock. Spotkania z mieszkańcami, przedstawicielami samorządów, instytucji publicznych oraz studentami i seniorami poświęcone były zagadnieniom bezpieczeństwa danych osobowych i odpowiedzialnego korzystania z nowych technologii.

W ramach naszej akcji, promującej wiedzę o prawie do prywatności i danych osobowych, odwiedziliśmy już także Kraków, Tarnów, Katowice, Rzeszów, Kwidzyn, Gdynię i Gdańsk, Poznań, Olsztyn oraz Gorzów Wielkopolski.

Urząd Ochrony Danych Osobowych rozpoczął też w listopadzie kolejny cykl spotkań edukacyjnych dla dzieci i młodzieży z całej Polski w ramach trzeciej edycji programu Ministerstwa Finansów „Lekcje o finansach”.

Wspólnie z Naczelną Radą Adwokacką oraz Stowarzyszeniem Sędziów Polskich „Iustitia” zorganizowaliśmy seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO”. Wydarzenie stanowiło doskonałą okazję do wymiany doświadczeń przedstawicieli świata prawa, nauki i praktyki.

W siedzibie Urzędu zorganizowaliśmy również razem ze Społecznym Zespołem Ekspertów przy Prezesie UODO konferencję „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach”. Jedną z zasadniczych konkluzji z debaty okazała się idea opracowania kodeksu postępowania dla branży medialnej.

Wraz z Uniwersytetem Ekonomicznym w Katowicach zorganizowaliśmy konferencję „Bezpieczeństwo informacji w organizacji i jej zasobów”. Wydarzenie skupiło się na wyzwaniach, jakie niesie rozwój technologii cyfrowych dla ochrony danych w administracji publicznej, edukacji i biznesie.

Konferencja „Nowe wyzwania prawne: Regulacje, zadania regulatorów i ochrona danych” zakończyła tegoroczny z kolei cykl seminariów organizowanych wspólnie z Zakładem Ubezpieczeń Społecznych.

Niezwykle ważnym wydarzeniem jest stworzenie kodeksu postępowania dla prywatnych firm badania opinii i rynku. Doprecyzowuje on zasady ochrony danych osobowych uczestników badań, w tym m.in. pozyskiwanie ich zgody czy profilowanie. Twórcą kodeksu jest Organizacja Firm Badania Opinii i Rynku (OFBOR) – jedyne w Polsce stowarzyszenie pracodawców, skupiające prywatne agencje badawcze. Zatwierdzając ten kodeks byłem i jestem przekonany, że przyczyni się on do zapewnienia wysokiego poziomu ochrony danych osobowych.

Promocja ochrony danych to także włączanie ludzi w dyskusję i wypracowywanie adekwatnych rozwiązań, szczególnie w kontekście rozwijających się dynamicznie nowych technologii. W tym miesiącu zbieraliśmy np. opinie o potrzebach instytucji i organizacji w obszarze wykorzystania sztucznej inteligencji (SI) oraz zapewnienia właściwej ochrony danych osobowych przy stosowaniu tej technologii. Nasze badanie, przygotowane we współpracy z ekspertami, ma pomóc w przygotowaniu działań i materiałów wspierających podmioty w odpowiedzialnym, zgodnym z prawem wdrażaniu modeli i systemów SI. Udało się zebrać ogromny materiał – za, który już analizujemy. Dziękuję za wszystkie przedłożone nam opinie. Pierwsze wnioski chcemy przedstawić Państwu wkrótce.

Z analiz i doświadczenia Urzędu wynika, że przepisy o przetwarzaniu danych w rejestrach publicznych wymagają pilnego przeglądu. Stąd moje wystąpienie do ministra cyfryzacji o dokonanie przeglądu rejestrów publicznych. Chodzi m.in. o Krajowy Rejestr Sądowy, Rejestr Dowodów Osobistych czy Rejestr PESEL. Obecna sytuacja międzynarodowa nakazuje spojrzeć na bezpieczeństwo danych osobowych przetwarzanych w rejestrach publicznych także przez pryzmat zagrożeń dla państwa i bezpieczeństwa narodowego. Rejestry publiczne, w których przetwarzane są dane osobowe zarówno obywateli, jak i innych osób przebywających w Polsce, są bowiem kluczowym elementem systemu naszego bezpieczeństwa. Ochrona danych osobowych jest więc podyktowana nie tylko zagrożeniami dla prywatności jednostki, ale także istotnymi ryzykami dla naszej wspólnoty. Ryzyka te nie ograniczają się do cyberzagrożeń, ale wiążą się z całym spektrum działań związanych z nielegalnym przetwarzaniem danych osobowych.

Współpraca z resortem cyfryzacji jest dla Urzędu Ochrony Danych Osobowych bardzo ważna. Dlatego Prezes UODO i Minister Cyfryzacji zawarli porozumienie w sprawie współpracy przy zgłaszaniu naruszeń ochrony danych osobowych za pomocą systemu S46 – systemu teleinformatycznego wspierającego działanie krajowego systemu cyberbezpieczeństwa.

Sprawy ochrony danych osobowych rozstrzygają się też w sprawach na pierwszy rzut oka nie mających z nimi nic wspólnego. Przykładem nowelizacja ustawy o sporcie, która ma ułatwić rozpoznawanie sportowych talentów wśród dzieci. Odbywać się to jednak będzie poprzez zbieranie danych o dzieciach. Zgłosiliśmy do projektu liczne uwagi.

Jeśli chodzi o interwencje w indywidualnych sprawach, w listopadzie jako Prezes UODO:

- ukarałem komornika sądowego za niezgłoszenie incydentu z naruszeniem ochrony danych. Ta sprawa jest ważna, bo wyjaśniamy w niej po raz kolejny, jak rozumieć pojęcie „mało prawdopodobne ryzyko". Jak wiemy, tylko wtedy administrator nie musi zgłaszać incydentu do organu nadzorczego. Ale RODO rezerwuje to pojęcie do zdarzeń niezwykle rzadkich. Bowiem naruszenie ochrony danych osobowych może mieć negatywne konsekwencje dla osoby, której dane dotyczą, nawet gdy wszystko pozornie będzie wskazywało, że zainteresowana osoba nie poniesie uszczerbku.
- upomniałem – po zbadaniu sprawy – posła Kazimierza Smolińskiego, który w czasie prezydenckiej kampanii wyborczej pokazał publicznie dokumenty z danymi osobowymi, w tym z adresem i numerem księgi wieczystej. Parlamentarzyści mają duże uprawnienia i szeroki mandat, ale realizując go, są administratorem danych, a więc podlegają RODO, które wyraźnie wskazuje, kiedy administrator może przetwarzać, a więc i ujawnić dane osobowe. Pragnę, by ta wiedza się upowszechniała. Stąd też cykl szkoleń, które Urząd Ochrony Danych Osobowych realizuje w tym zakresie.

Listopadowy numer to ostatnie wydanie Biuletynu w 2025 roku, następny będzie łączony numer grudniowo-styczniowy, w związku z czym pragnę złożyć Państwu najserdeczniejsze życzenia świąteczne. Czytelnikom i autorom Biuletynu UODO przekazuję wyrazy uznania za zaangażowanie w budowanie kultury ochrony danych osobowych. Dziękuję za Państwa gotowość do pogłębiania wiedzy w tej ważnej dziedzinie.

Życzę, aby lektura biuletynu była dla Państwa nie tylko źródłem rzetelnych informacji, ale także inspiracją do dalszego podnoszenia standardów ochrony prywatności — w instytucjach, organizacjach i w życiu codziennym. Niech nadchodzący rok przyniesie Państwu satysfakcję z dobrze

***Mirosław Wróblewski***
*Prezes UODO*

Drodzy Czytelnicy!

W tym numerze biuletynu zamieszczamy wywiad z ks. Andrzejem Lewczakiem, Kościelnym Inspektorem Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego. Głównym powodem naszej rozmowy jest porozumienie o współpracy i wzajemnym przekazywaniu informacji ws. ochrony danych, podpisane pomiędzy KIODO PAKP a Prezesem UODO. Z wywiadu dowiemy się, na czym polega system ochrony danych w tym związku wyznaniowym oraz jakie są wyzwania w tym zakresie. Jak podkreśla ks. Lewczak: „Do najważniejszych wyzwań w Kościele prawosławnym zaliczamy: ujednolicenie standardów w rozproszonej strukturze, rozwój kompetencji IT w parafiach, właściwe uregulowanie transferów międzynarodowych oraz edukację duchowieństwa i wolontariuszy".

W tym wydaniu poruszamy również temat usuwania danych z kopii zapasowych systemów informatycznych. Jak przeczytamy w tekście przygotowanym przez ekspertów UODO, „administrator nie może odmawiać zrealizowania przysługującego każdemu z nas prawa do usunięcia danych osobowych, jeśli to żądanie ma uzasadnienie w przepisach prawa. Dane musi usunąć również z kopii zapasowych systemów informatycznych". Przybliżamy też wyjątkowe sytuacje, kiedy takie dane zgodnie z prawem nie muszą być usuwane.

Odnosimy się także do kwestii czynnika ludzkiego, który zazwyczaj jest decydujący w procesie ochrony danych osobowych, bowiem nie istnieje technologia, która całkowicie wyeliminuje ryzyko błędów ludzkich. Ale też człowiek w systemie ochrony danych może być zarówno kontrolerem procesów przetwarzania, jak i autorem złych decyzji. Zatem tylko inwestycja w ludzi – w edukację, kulturę organizacyjną i budowanie odpowiedzialności – jest najważniejszym elementem skutecznej strategii bezpieczeństwa.

Prezentujemy również wykład o ochronie danych osobowych nieletnich i ich wizerunku, przygotowany przez ekspertów UODO.

Jeśli chodzi o najistotniejsze wydarzenia związane z ochroną danych w Europie i z procesem legislacyjnym w tej kwestii, w tym wydaniu przypominamy, że podczas październikowego posiedzenia plenarnego Europejska Rada Ochrony Danych (EROD) wybrała temat piątej skoordynowanej akcji egzekwowania prawa, która będzie dotyczyć zgodności z obowiązkami w zakresie przejrzystości i informacji wynikającymi z ogólnego rozporządzenia o ochronie danych.

W trakcie tego samego posiedzenia EROD przyjęła dwie opinie dotyczące projektów decyzji Komisji Europejskiej ws. przedłużenia ważności decyzji o odpowiednim poziomie ochrony danych dla Wielkiej Brytanii na podstawie ogólnego rozporządzenia o ochronie danych oraz dyrektywy ws. egzekwowania prawa (LED) – do grudnia 2031 r. Zwracamy też uwagę, że Trybunał Sprawiedliwości UE doprecyzowuje zakres pojęcia danych osobowych w kontekście przekazania danych pseudonimizowanych stronom trzecim. I porządkujemy zagadnienie praw osób w systemie Eurodac, jednym z kluczowych elementów unijnej polityki azylowej – to ważne tym bardziej, że mają się pojawić nowe przepisy wynikające z tej polityki.

Na koniec jak zawsze zapowiadamy wydarzenia organizowane przez UODO w najbliższym czasie. Szczególnie polecamy międzynarodową konferencję „The Role of the Council of Europe's Framework Convention on Artificial Intelligence in the Protection of Privacy and Personal Data – Legal, Ethical, and Social Challenges in the AI Era", która odbędzie się 10 grudnia w siedzibie Urzędu.

***Karol Witowski***
*Dyrektor Departamentu Komunikacji Społecznej*
*Rzecznik Prasowy UODO*

# WAŻNY KROK DLA NASZEJ WSPÓLNOTY

**O ochronie danych osobowych w Kościele prawosławnym, o cyberbezpieczeństwie w jego strukturach, a także o współpracy między tym Kościołem a Prezesem UODO w ramach niedawno podpisanego porozumienia – z ks. Andrzejem Lewczakiem, Kościelnym Inspektorem Ochrony Danych Osobowych Polskiego Autokefalicznego Kościoła Prawosławnego, rozmawia Karol Witowski.**

**W jaki sposób porozumienie z Prezesem UODO może się przyczynić do wzmocnienia systemu ochrony danych osobowych w Polskim Autokefalicznym Kościele Prawosławnym?**

To ważny krok dla Polskiego Autokefalicznego Kościoła Prawosławnego. Podpisane 15 października 2025 r. porozumienie otwiera Kościołowi prawosławnemu drogę do stałej współpracy merytorycznej i edukacyjnej z krajowym organem nadzoru. Dzięki temu możemy liczyć na dostęp do aktualnych materiałów szkoleniowych i praktycznych wytycznych, eksperckie wsparcie przy interpretacji przepisów w kontekście specyfiki kościelnej, wspólne działania informacyjne skierowane do duchownych i wiernych, a także – w razie potrzeby – na szybszą ścieżkę konsultacyjną w procesie przygotowywania wewnętrznych procedur. W efekcie zwiększa to spójność podejścia w całej strukturze Kościoła i podnosi standard ochrony danych na poziomie parafii i diecezji.

**Jakie są główne wyzwania w strukturze Kościoła prawosławnego, które przekładają się na potencjalne problemy w obszarze ochrony danych osobowych?**

Najważniejsze wyzwania to rozproszenie organizacyjne (wiele parafii i jednostek o różnym stopniu dostosowania do wymogów prawnych), zróżnicowane systemy dokumentacji (papierowe i elektroniczne), duża rola dokumentów historycznych i rejestrów parafialnych, częste angażowanie osób niebędących pracownikami do przetwarzania danych oraz ograniczone zasoby IT i kadrowe w mniejszych parafiach/jednostkach.

# 1 ROZMOWA Z EKSPERTEM

Dochodzą do tego specyficzne praktyki duszpasterskie – np. prowadzenie ksiąg chrztów czy małżeństw – które wymagają szczególnej uwagi przy określaniu podstaw prawnych i sposobów zabezpieczenia danych.

**Jaki jest podstawowy paradygmat ochrony danych w Kościele prawosławnym?**

Można go ująć w trzech filarach: świadomość duszpasterska, zasada proporcjonalności oraz decentralizacja odpowiedzialności przy centralnym wsparciu. Oznacza to, że ochrona danych jest traktowana jako element posługi duszpasterskiej, przetwarzamy tylko dane niezbędne, a każda jednostka (parafia, diecezja) ponosi odpowiedzialność za własne operacje, mając jednocześnie dostęp do wytycznych, procedur i wsparcia KIODO na poziomie centralnym. W praktyce obejmuje to wzory polityk, instrukcji i klauzul informacyjnych, szkolenia oraz zalecenia dotyczące przechowywania dokumentów i zabezpieczeń technicznych.

**A jak wygląda system obiegu dokumentów między diecezjami?**

Obieg ma charakter hybrydowy. Wiele dokumentów funkcjonuje w formie papierowej i jest przechowywanych lokalnie, a część administracyjno-kadrowa – równolegle w formie elektronicznej. Przekazywanie dokumentów między diecezjami odbywa się przede wszystkim poprzez oficjalną korespondencję pocztową oraz zaszyfrowane załączniki e-mail. KIODO promuje minimalizację przesyłanych danych oraz obowiązek szyfrowania danych przesyłanych drogą elektroniczną.

**Na co dzień Kościół prawosławny musi też na pewno rozwiązywać problem z transferem danych do państw trzecich – to przykład diecezji w Brazylii, która podlega PAKP.**

Tak, diecezja w Brazylii podlega jurysdykcji Kościoła prawosławnego w Polsce, co wymusza analizę zarówno praktycznych, jak i prawnych aspektów przekazywania danych. Ponieważ Brazylia nie znajduje się w obszarze stosowania RODO, konieczne jest zapewnienie odpowiedniej podstawy prawnej i adekwatnych zabezpieczeń. W praktyce ograniczamy transfery do danych niezbędnych z perspektywy działań duszpasterskich i administracyjnych, stosując m.in. szyfrowanie.

**Czy jednostki Kościoła są celem cyberataków, jak Kościół sobie z tym radzi?**

Tak, podobnie jak inne podmioty publiczne i niepubliczne, parafie oraz instytucje kościelne stają się celem phishingu, malware czy ataków na pocztę e-mail.

# 1 ROZMOWA Z EKSPERTEM

Nasza reakcja opiera się na podstawowych zabezpieczeniach technicznych (aktualizacje, antywirusy, zapory), szkoleniach i działaniach podnoszących świadomość użytkowników oraz na procedurach reagowania na incydenty. Nie dysponujemy jednym centralnym systemem, dlatego promujemy zestaw prostych i skutecznych dobrych praktyk, dostosowanych do możliwości mniejszych jednostek.

### Jakie są obecnie największe wyzwania dotyczące ochrony danych w Kościele prawosławnym i jak je osadzić w kontekście wsparcia Prezesa UODO?

Do najważniejszych wyzwań zaliczamy: ujednolicenie standardów w rozproszonej strukturze, rozwój kompetencji IT w parafiach, właściwe uregulowanie transferów międzynarodowych oraz edukację duchowieństwa i wolontariuszy. Prezes UODO może wesprzeć te działania poprzez dostarczanie przystępnych materiałów oraz wzorów procedur uwzględniających specyfikę kościelną, wsparcie szkoleniowe (w tym programy dedykowane), udostępnienie szybkiej ścieżki konsultacyjnej, a także – jeśli to możliwe – inicjatywy wspierające mniejsze jednostki w pozyskiwaniu podstawowych narzędzi IT i zabezpieczeń.

### Czy Kościół prowadził działania informacyjne dla duchownych i wiernych?

Tak, działania informacyjne były i są realizowane na kilku poziomach: poprzez materiały informacyjne i zalecenia (instrukcje, broszury), szkolenia dla duchowieństwa i pracowników parafii, konferencje diecezjalne oraz komunikaty dla wiernych publikowane na stronach parafialnych i w ogłoszeniach. Proces ten rozwijał się stopniowo. Większe ośrodki mają bardziej rozbudowane programy szkoleniowe, natomiast mniejsze parafie częściej opierają się na materiałach centralnych. Porozumienie z UODO pozwoli ten proces uporządkować i rozszerzyć.

### Czy technologie sztucznej inteligencji pomagają w misji religijnej?

Wykorzystanie AI wymaga dużej ostrożności – zwłaszcza w zakresie prywatności, przejrzystości działania algorytmów oraz ryzyka błędnych rekomendacji. Jesteśmy na etapie analiz i obserwacji możliwych zastosowań.

# 1 ROZMOWA Z EKSPERTEM

**Czy Kościół prawosławny otrzymuje wsparcie od instytucji europejskich?**

Obecnie nie korzystamy z takiego wsparcia. Główne działania realizowane są na bazie inicjatyw krajowych oraz współpracy z krajowym organem nadzoru. Korzystamy przede wszystkim z uniwersalnych wytycznych, materiałów edukacyjnych oraz decyzji organów ochrony danych, które kształtują ramy prawne i praktyczne.

**Dziękuję za rozmowę**

# USUWANIE DANYCH Z KOPII ZAPASOWYCH SYSTEMÓW INFORMATYCZNYCH

**Administrator nie może odmawiać zrealizowania przysługującego każdemu z nas prawa do usunięcia danych osobowych, jeśli to żądanie ma uzasadnienie w przepisach prawa. Dane musi usunąć również z kopii zapasowych systemów informatycznych. Dlatego ważne jest, aby korzystać z takich systemów do tworzenia kopii zapasowych, by móc wywiązać się z tego obowiązku.**

W ostatnim czasie osoba pełniąca funkcję inspektora ochrony danych (IOD) zwróciła się do UODO z prośbą o przedstawienie stanowiska w zakresie dopuszczalnego sposobu postępowania z kopiami zapasowymi systemów informatycznych, zawierającymi dane osobowe, w przypadku realizacji prawa do usunięcia danych zgodnie z art. 17 RODO.

Jak wskazała, w dostępnych publicznie materiałach można znaleźć odmienne podejścia do tej kwestii – niektóre nakazują niezwłoczne usuwanie danych, inne dopuszczają przechowywanie danych w kopii zapasowej do czasu jej nadpisania lub usunięcia przy założeniu, że kopia taka zostaje „wyłączona z przetwarzania", czyli dane nie są wykorzystywane w żadnym celu poza ewentualnym przywróceniem systemu w sytuacji awaryjnej.

W odpowiedzi UODO wskazał, że wśród wymienionych w RODO środków technicznych i organizacyjnych, które mają być wdrażane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, znajduje się zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (art. 32 ust. 1 lit. c). Jednym z najprostszych sposobów wypełnienia tego obowiązku jest tworzenie kopii zapasowych przetwarzanych danych osobowych (tzw. backup).

Biorąc pod uwagę fakt, że kopia zapasowa jest niczym innym, jak formą przechowywania, a więc przetwarzania danych osobowych (stosownie do art. 4 ust. 2 RODO), zastosowanie do niej znajdują wszystkie określone w RODO zasady postępowania z danymi osobowymi.

**Administrator powinien korzystać z systemu do tworzenia kopii zapasowych zbudowanego zgodnie z zasadą ochrony danych osobowych w fazie projektowania** (art. 25 ust. 1 RODO). **System ten powinien umożliwiać realizację praw osób, których dane dotyczą, w tym usuwanie danych.** Takie zobowiązanie wynika z ciążącego na administratorze obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać (art. 24 ust. 1 RODO).

**Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych**, a administrator ma obowiązek bez zbędnej zwłoki je usunąć, jeżeli zachodzi jedna z okoliczności wskazanych w art. 17 ust. 1 RODO (np. dane osobowe były przetwarzane niezgodnie z prawem, dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane), a administrator nie może powołać się na jedną z przesłanek wskazanych w art. 17 ust. 3 RODO.

Zgodnie z tym przepisem prawo do usunięcia danych nie będzie realizowane w przypadku, gdy przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Wśród wskazanych przyczyn odmowy realizacji prawa do usunięcia danych osobowych nie został wskazany brak możliwości usunięcia pojedynczych rekordów (zawierających dane osobowe), np. z kopii zapasowej utworzonej w celu zapewnienia bezpieczeństwa i ciągłości przetwarzanych już danych osobowych.

Zatem jeżeli administrator rozpatrując żądanie, nie może powołać się na którąś z przesłanek wskazanych w art. 17 ust. 3 RODO, powinien bez zbędnej zwłoki usunąć dane osobowe, również z kopii zapasowych, ponieważ nie ma już podstawy prawnej do przetwarzania danych osobowych, których dotyczy żądanie usunięcia.

Powyższe stanowisko organu nadzorczego jest zatem zbieżne ze wskazówkami Ministerstwa Cyfryzacji zawartymi w materiale pt. „RODO – Informator", w którym na str. 6 wskazano: „Jeżeli usuwanie z kopii zapasowych pojedynczych rekordów grozi naruszeniem integralności pozostałych gromadzonych danych, to administrator może manualnie przywracać kopie do bazy głównej, a następnie usuwać z nich pojedyncze rekordy i backupować bazy zmniejszone o ten rekord, choć jest to dość czasochłonny proces".

Reasumując, administrator nie może odmawiać nam zrealizowania żądania usunięcia naszych danych osobowych (np. ze względu na to, że jest to czasochłonne), jeśli nasze żądanie ma uzasadnienie w przepisach prawa.

# CZŁOWIEK NAJWAŻNIEJSZYM ELEMENTEM W SYSTEMIE BEZPIECZEŃSTWA INFORMACJI

**Bezpieczeństwo informacji jest jednym z najważniejszych wyzwań współczesnych organizacji. W świecie cyfrowym dane osobowe i poufne informacje przetwarza się prawie wyłącznie z wykorzystaniem systemów teleinformatycznych. Naturalne jest więc koncentrowanie się na technologii: zaporach sieciowych, szyfrowaniu czy procedurach tworzenia kopii zapasowych. Jednak każdy system działa poprawnie wyłącznie wtedy, gdy człowiek zapewnia jego właściwe użycie. Ponieważ to właśnie człowiek – pracownik, współpracownik, użytkownik – jest najważniejszym elementem w systemie bezpieczeństwa informacji.**

## Człowiek jako źródło ryzyka

Nie istnieje technologia, która całkowicie wyeliminuje ryzyko błędów ludzkich. Nawet najbardziej zaawansowane zabezpieczenia mogą zostać osłabione przez nieostrożne działania użytkowników. W praktyce oznacza to, że pracownicy mogą np.:

- przypadkowo udostępnić poufny dokument,
- zapisać hasło w łatwo dostępnym miejscu,
- pozostawić domyślne ustawienia systemu, które są mniej bezpieczne,
- kliknąć w podejrzany link i stać się ofiarą phishingu,
- zignorować ostrzeżenie systemu.

Nie są to zwykle działania celowe. Najczęściej pojawiają się w wyniku codziennych realiów pracy. Najczęściej są one efektem:

- **rutyny**, która prowadzi do lekceważenia procedur i traktowania ich jako zbędnych – bo po dwudziestym razie procedura staje się zbędnym, irytującym krokiem, a nie tarczą ochronną,
- **presji czasu**, która skłania do skrótów i pomijania zabezpieczeń – szczególnie wtedy, gdy biurko ugina się od sterty dokumentów „na wczoraj”,
- **braku świadomości**, że drobne zaniedbanie może mieć poważne konsekwencje dla całej organizacji.

# 3 NARUSZENIA I KONTROLE

### Człowiek jako strażnik bezpieczeństwa

Jednocześnie to właśnie człowiek pozostaje jedynym elementem zdolnym do elastycznego reagowania na sytuacje nieprzewidziane. Algorytm widzi tylko dane, człowiek – kontekst. To pracownik rozpozna nietypowe zachowanie, np. gdy dostawca, który zawsze dzwonił, nagle prosi o pilny przelew e-mailem. Człowiek potrafi:

- **rozpoznać nietypowe zachowanie**, którego system nie wychwyci, np. subtelne sygnały świadczące o próbie manipulacji czy socjotechniki,
- **podjąć decyzję o zatrzymaniu procesu**, kiedy pojawia się wątpliwość, nawet jeśli system nie zgłasza błędu – to umiejętność zatrzymania się i refleksji, której maszyna nie posiada,
- **ocenić kontekst**, czyli uwzględnić czynniki pozatechniczne: relacje międzyludzkie, intencje rozmówcy, sytuację biznesową. Algorytmy mogą analizować dane, ale nie zawsze potrafią uchwycić znaczenie subtelnych okoliczności.

To właśnie ta zdolność do interpretacji i reagowania w sposób nieszablonowy sprawia, że człowiek jest nie tylko potencjalnym źródłem błędów, ale także najważniejszą linią obrony. W sytuacjach, w których system zawodzi lub nie dostrzega zagrożenia, pracownik może zatrzymać eskalację problemu i ochronić organizację przed poważnymi konsekwencjami.

### Co organizacja może zrobić, aby pracownik był najlepszą wersją siebie w systemie bezpieczeństwa informacji?

Wiele zmian, które mogą znacząco poprawić poziom bezpieczeństwa informacji w organizacji, nie wymaga ogromnych budżetów ani skomplikowanych projektów. Często wystarczy konsekwencja w codziennych działaniach i świadome podejście do obowiązków, aby osiągnąć trwałą poprawę. Co ważne, takie usprawnienia wzmacniają nie tylko system bezpieczeństwa informacji, ale również pozytywnie wpływają na kulturę pracy, zaufanie między pracownikami i efektywności całej organizacji.

### Jasne role i odpowiedzialności

Każdy pracownik pełni w organizacji określoną rolę. Aby dobrze się z niej wywiązywać, musi wiedzieć, czego się od niego oczekuje. Nie ma znaczenia, czy chodzi o prezesa, sekretarkę, administratora systemu IT czy archiwistę – **wszyscy powinni mieć jasno określone obowiązki i zakres odpowiedzialności**, bo tylko wtedy mogą wykonywać swoje zadania rzetelnie i bezpiecznie.

# 3 NARUSZENIA I KONTROLE

### Co daje jasny podział ról w praktyce?

- **Przejrzystość** – pracownicy dokładnie wiedzą, za co odpowiadają i jakie mają uprawnienia.
- **Lepsza kontrola ryzyka** – łatwiej wskazać słabe punkty i przypisać działania naprawcze.
- **Odpowiedzialność osobista** – nawet jeśli zadania są delegowane, obowiązek nadzoru pozostaje, co wzmacnia kulturę bezpieczeństwa.
- **Koordynacja** – właściwy podział ról ułatwia współpracę zarówno wewnątrz organizacji, jak i z partnerami zewnętrznymi.

### Skutki braku jasnego podziału ról i odpowiedzialności

Brak przejrzystego przypisania ról i odpowiedzialności może prowadzić do poważnych konsekwencji, takich jak:

- **Nieuprawniony dostęp** – brak kontroli nad tym, kto odpowiada za aktywa, sprzyja ich nadużyciu.
- **Chaos organizacyjny** – pracownicy nie wiedzą, kto podejmuje decyzje, co spowalnia reakcję na incydenty.
- **Brak rozliczalności** – w przypadku naruszenia bezpieczeństwa trudno ustalić winnych i wdrożyć działania naprawcze.
- **Większe ryzyko błędów lub zmowy** – brak rozdzielania obowiązków ułatwia nadużycia i nieumyślne zaniedbania.
- **Utrata reputacji i zaufania** – klienci i partnerzy mogą uznać organizację za nieprofesjonalną i niegodną zaufania.

### „Instrukcja obsługi bezpieczeństwa" – dlaczego jest niezbędna

Każde rozwiązanie techniczne w obszarze bezpieczeństwa wymaga jasnej instrukcji stosowania. Bez niej istnieje ryzyko, że będzie stosowane niezgodnie z przeznaczeniem, a zamiast wzmacniać ochronę – w skrajnych przypadkach może ją nawet osłabić. Dlatego polityki, procedury i instrukcje są niezbędnym elementem systemu bezpieczeństwa informacji.

### Jakie powinny być te dokumenty?

- **Jasne i czytelne** – napisane prostym językiem, tak aby każdy odbiorca miał realną szansę zrozumieć, czego się od niego oczekuje.
- **Dostosowane do odbiorców** – procedury muszą być komunikowane osobom pełniącym konkretne role w takim zakresie, który jest dla nich użyteczny i niezbędny do wywiązania się z ich specyficznych obowiązków.
- **Praktyczne** – powinny wskazywać nie tylko „CO" należy zrobić, ale także „JAK" to zrobić w codziennej pracy, oraz przede wszystkim „DLACZEGO" to ważne.

### Zasady bezpieczeństwa muszą być dopasowane do rzeczywistych obowiązków, aby działały w praktyce

Wrzucone do jednego worka ogólne zasady nie przynoszą efektu. Informowanie np. personelu sprzątającego o procedurach tworzenia kopii zapasowych serwerów nie poprawi poziomu bezpieczeństwa – bo nie jest to ich obszar odpowiedzialności. Z kolei administratorzy systemów IT potrzebują szczegółowych instrukcji technicznych, a pracownicy biurowi – prostych wskazówek dotyczących korzystania z haseł czy ochrony dokumentów.

Dobrze przygotowane polityki i procedury sprawiają, że każdy pracownik wie, **jak korzystać z narzędzi bezpieczeństwa zgodnie z ich przeznaczeniem**, a organizacja zyskuje spójność i skuteczność w działaniu.

### Edukacja

Edukacja pracowników należy do najistotniejszych działań wspierających bezpieczeństwo informacji w organizacji. Tylko dobrze przygotowany pracownik, posiadający odpowiednie kompetencje, jest w stanie skutecznie chronić dane, z którymi pracuje na co dzień.

Programy szkoleniowe muszą odpowiadać na potrzeby konkretnych ról w organizacji. Inne potrzeby ma administrator systemu IT, a inne pracownik biurowy czy osoba odpowiedzialna za obsługę klienta. Ważne jest, aby sposób prowadzenia szkoleń był interesujący i angażujący – nie mogą one być traktowane jako kolejny biurokratyczny obowiązek, lecz jako realna szansa na zwiększenie świadomości i podniesienie poziomu bezpieczeństwa informacji w całej organizacji.

# 3 NARUSZENIA I KONTROLE

## Jak prowadzić skuteczne szkolenia?

- **Odwoływać się do rzeczywistych incydentów** – zarówno tych, które wydarzyły się w organizacji, jak i tych znanych z innych firm, jeśli mają związek z zadaniami realizowanymi przez pracowników.
- **Stawiać na praktykę** – symulacje, ćwiczenia czy warsztaty zwiększają szansę na przyswojenie wiedzy i utrwalenie właściwych zachowań.
- **Dzielić materiał na mniejsze porcje** – lepsze efekty daje częstsze prowadzenie krótszych szkoleń niż rzadkie, ale przeładowane treścią sesje.
- **Uwzględniać najnowsze zagr**ożenia – np. kampanie phishingowe, które są jednym z najczęstszych źródeł incydentów bezpieczeństwa.

Benjamin Franklin powiedział kiedyś: **„Powiedz mi, to zapomnę. Naucz mnie, to może zapamiętam. Zaangażuj mnie, to się nauczę”** – i to najlepiej oddaje sens angażujących szkoleń.

To właśnie zaangażowanie pracowników w proces edukacji sprawia, że stają się oni nie tylko odbiorcami wiedzy, ale też aktywnymi uczestnikami systemu bezpieczeństwa informacji.

## Otwartość w reagowaniu na błędy jako element kultury bezpieczeństwa

Jednym z najważniejszych elementów skutecznego systemu bezpieczeństwa informacji – obok technologii, higieny cyfrowej i jasno określonych ról – jest **kultura otwartości w reagowaniu na błędy**.

## Dlaczego otwartość jest kluczowa?

- **Obawa przed krytyką i ukrywanie incydentów** prowadzi do eskalacji problemów oraz zwiększa ryzyko poważnych naruszeń.
- **Otwarte zgłaszanie błędów** pozwala szybko reagować, minimalizować skutki i wyciągać wnioski na przyszłość.
- **Psychologiczny aspekt** – pracownicy, którzy czują się bezpieczni w przyznawaniu do pomyłek, są bardziej skłonni do współpracy i uczenia się.

# 3 NARUSZENIA I KONTROLE

### Jak budować kulturę otwartości?

- **Brak kar za zgłoszenie błędu** – pracownik powinien wiedzieć, że zgłoszenie incydentu nie jest powodem do sankcji, lecz dowodem odpowiedzialności.
- **Promowanie odwagi w zgłaszaniu** – kierownictwo powinno podkreślać, że lepiej zgłosić nawet drobny problem, niż go zignorować.
- **Docenianie szczerości** – organizacja może nagradzać pracowników, którzy szybko i otwarcie informują o incydentach.
- **Transparentna komunikacja** – jasne procedury zgłaszania i informowania o błędach sprawiają, że proces jest prosty i zrozumiały.

### Korzyści z kultury otwartości

- **Szybsza reakcja** – im wcześniej incydent zostanie zgłoszony, tym łatwiej ograniczyć jego skutki.
- **Uczenie się na błędach** – każdy incydent staje się okazją do poprawy procedur i zwiększenia świadomości.
- **Budowanie zaufania** – pracownicy czują, że organizacja traktuje ich jak partnerów, a nie potencjalnych winnych.
- **Zmniejszenie ryzyka** – otwartość w reagowaniu na błędy minimalizuje prawdopodobieństwo powtarzania tych samych incydentów.

Kultura otwartości w reagowaniu na błędy sprawia, że pracownicy nie boją się przyznać do pomyłek i zgłaszać incydentów. Dzięki temu organizacja może szybciej reagować, skuteczniej się uczyć i budować środowisko, w którym człowiek – zamiast być najsłabszym ogniwem – staje się **najważniejszym elementem systemu bezpieczeństwa informacji**.

### Podsumowanie

Człowiek jest jednocześnie największym źródłem ryzyka i największą wartością w systemie bezpieczeństwa informacji. To jego decyzje, nawyki i świadomość decydują o tym, czy dane pozostaną chronione. Technologia może być tarczą, ale to człowiek decyduje, czy tarcza zostanie właściwie użyta. Dlatego inwestycja w ludzi – w edukację, kulturę organizacyjną i budowanie odpowiedzialności – jest najważniejszym elementem skutecznej strategii bezpieczeństwa.

Pamiętajmy, że o bezpieczeństwie informacji decydują nie tylko firewalle i algorytmy, lecz przede wszystkim ludzie, którzy codziennie podejmują decyzje wpływające na ochronę danych.

# DMA I RODO: EROD I KOMISJA EUROPEJSKA ZATWIERDZAJĄ WSPÓLNE WYTYCZNE W CELU DOPRECYZOWANIA PUNKTÓW STYKU

Europejska Rada Ochrony Danych (EROD) oraz Komisja Europejska zatwierdziły wspólne wytyczne dotyczące współdziałania aktu o rynkach cyfrowych (DMA) oraz ogólnego rozporządzenia o ochronie danych. Są to pierwsze wspólne wytyczne opracowane przez Radę i Komisję Europejską.

Zgodnie ze Strategią EIOD na lata 2024–2027 oraz z celami zawartymi w niedawnym Oświadczeniu Helsińskim, mającymi na celu ułatwienie zgodności z RODO i wzmocnienie spójności, EROD współpracowała z Komisją Europejską – każda w ramach swoich kompetencji – aby zapewnić spójne stosowanie DMA i RODO oraz zwiększyć pewność prawną dla strażników dostępu, użytkowników biznesowych, beneficjentów i osób fizycznych.

### Przewodnicząca EROD, Anu Talus, powiedziała:

„Te wspólne wytyczne są wynikiem owocnej współpracy między EROD a Komisją Europejską. Po raz pierwszy EROD i Komisja Europejska opracowują wytyczne wspólnie. Takie podejście maksymalizuje użyteczność wytycznych, upraszczając zgodność dla firm i zapewniając im większą pewność prawną. Wytyczne pomogą strażnikom dostępu, użytkownikom biznesowym i osobom fizycznym lepiej zrozumieć swoje obowiązki i prawa wynikające z DMA oraz zapewnią spójne, skuteczne i komplementarne stosowanie DMA i prawa ochrony danych UE”.

### Jak DMA i RODO współdziałają

DMA i RODO chronią osoby fizyczne w środowisku cyfrowym, ale ich cele są komplementarne odpowiadają na powiązane wyzwania: prawa jednostki i prywatność w przypadku RODO oraz uczciwość i możliwość konkurowania na rynkach cyfrowych w ramach DMA.

Wiele działań regulowanych przez DMA wiąże się z przetwarzaniem danych osobowych przez strażników dostępu, a w kilku przepisach DMA wyraźnie odwołuje się do definicji i pojęć zawartych w RODO. Wspólne wytyczne wyjaśniają, w jaki sposób strażnicy dostępu mogą wdrażać te przepisy DMA zgodnie z prawem ochrony danych UE. Na przykład EROD i Komisja wskazują, jakie elementy strażnicy powinni uwzględnić, aby spełnić wymogi dotyczące świadomego wyboru i ważnej zgody zgodnie z art. 5 ust. 2 DMA i RODO, a tym samym zgodnie z prawem łączyć lub wykorzystywać dane osobowe w ramach podstawowych usług platformowych.

EROD i Komisja odnoszą się również do innych przepisów, w tym dotyczących dystrybucji aplikacji i sklepów stron trzecich, przenoszenia danych, żądań dostępu do danych oraz interoperacyjności usług komunikacyjnych.

### Kolejne kroki

Rada i Komisja właśnie rozpoczęły wspólne konsultacje publiczne dotyczące pierwszej wersji wytycznych, które potrwają do 4 grudnia 2025 r. Będzie to okazja dla zainteresowanych stron do zgłaszania uwag i opinii.

Wszystkie zgłoszenia zostaną opublikowane na stronie internetowej DMA, do której link zostanie zamieszczony na stronie EROD po zakończeniu okresu konsultacji.

Ostateczna wersja, uwzględniająca opinie z konsultacji, zostanie przygotowana wspólnie przez Radę i Komisję i przyjęta przez EROD oraz Komisję Europejską.

### Więcej wytycznych w przygotowaniu

Po tych pierwszych wspólnych wytycznych z Komisją trwają dalsze prace nad wyjaśnieniem nowego krajobrazu regulacyjnego i utrzymaniem spójnych zabezpieczeń ochrony danych osobowych. W tym kontekście EROD współpracuje z Komisją, a konkretnie z Biurem ds. Sztucznej Inteligencji, nad wspólnymi wytycznymi dotyczącymi współdziałania Aktu o sztucznej inteligencji i przepisów UE o ochronie danych.

**Źródło:**

**Komunikat Europejskiej Rady Ochrony Danych**

DMA and GDPR: EDPB and European Commission endorse joint guidelines to clarify common touchpoints | European Data Protection Board

# SKOORDYNOWANE RAMY EGZEKWOWANIA: EROD WYBIERA TEMAT NA 2026 R.

Podczas październikowego posiedzenia plenarnego Europejska Rada Ochrony Danych (EROD) wybrała temat piątej skoordynowanej akcji egzekwowania prawa, która będzie dotyczyć zgodności z obowiązkami w zakresie przejrzystości i informacji wynikającymi z ogólnego rozporządzenia o ochronie danych. RODO zapewnia, że osoby fizyczne są informowane o przetwarzaniu ich danych (zgodnie z art. 12, 13 i 14). Prawo do informacji jest kluczowym elementem przejrzystości i umożliwia jednostkom większą kontrolę nad ich danymi.

W ramach skoordynowanej akcji EROD nadaje priorytet określonemu tematowi, nad którym krajowe organy ochrony danych pracują na poziomie krajowym. Wyniki tych działań są następnie agregowane i analizowane, co pozwala uzyskać głębszy wgląd w temat oraz umożliwia ukierunkowane działania następcze na poziomie krajowym i europejskim, jeśli zajdzie taka potrzeba.

Uczestniczące organy ochrony danych przystąpią do tej nowej inicjatywy dobrowolnie w nadchodzących tygodniach, a sama akcja zostanie uruchomiona w ciągu 2026 r.

## Dotychczasowe osiągnięcia CEF

W ostatnich latach EROD przeprowadziła różne skoordynowane działania dotyczące różnych tematów, publikując raporty z ich wynikami. W szczególności:

- korzystanie z usług chmurowych przez sektor publiczny (2023)
- wyznaczanie i pozycja inspektorów ochrony danych (2024)
- realizacja prawa dostępu przez administratorów danych (2025)

Na początku tego roku EROD rozpoczęła skoordynowaną akcję dotyczącą prawa do usunięcia danych, czyli „prawa do bycia zapomnianym” (art. 17 RODO). Raport z wynikami tej akcji zostanie przyjęty w nadchodzących miesiącach.

# 4 SPRAWY MIĘDZYNARODOWE

**Tło**

Nowa skoordynowana akcja jest kontynuacją decyzji EROD z października 2020 r. o utworzeniu Skoncentrowanych Ram Egzekwowania (CEF). CEF stanowi kluczowy element strategii EROD na lata 2024–2027, obok utworzenia Puli Ekspertów Wspierających. Obie inicjatywy mają na celu usprawnienie egzekwowania przepisów i współpracy między organami ochrony danych.

**Źródło:**

**Komunikat Europejskiej Rady Ochrony Danych**

Coordinated Enforcement Framework: EDPB selects topic for 2026 | European Data Protection Board

# PROJEKT DECYZJI O ODPOWIEDNIM POZIOMIE OCHRONY DANYCH W WIELKIEJ BRYTANII: EROD PRZYJMUJE OPINIE

Podczas ostatniego posiedzenia plenarnego Europejska Rada Ochrony Danych (EROD) przyjęła dwie opinie dotyczące projektów decyzji Komisji Europejskiej ws. przedłużenia ważności decyzji o odpowiednim poziomie ochrony danych dla Wielkiej Brytanii na podstawie ogólnego rozporządzenia o ochronie danych oraz dyrektywy w sprawie egzekwowania prawa (LED) do grudnia 2031 r.

Opinie EROD, o które zwróciła się Komisja zgodnie z art. 70 ust. 1 lit. s RODO oraz art. 51 ust. 1 lit. g LED, dotyczą proponowanego sześcioletniego przedłużenia dwóch decyzji, które mają wygasnąć w grudniu 2025 r.

Przedłużenie ważności decyzji umożliwi organizacjom i właściwym organom z siedzibą w Europie dalsze przekazywanie danych do podmiotów i organów z siedzibą w Wielkiej Brytanii bez konieczności wdrażania dodatkowych zabezpieczeń.

### Przewodnicząca EROD, Anu Talus, powiedziała:

„EROD z zadowoleniem przyjmuje utrzymującą się zgodność między ramami ochrony danych w Wielkiej Brytanii i Europie mimo ostatnich zmian w brytyjskim systemie prawnym. Wzywam Komisję Europejską do uwzględnienia punktów wskazanych przez Radę oraz zapewnienia skutecznego monitorowania po przyjęciu decyzji. Wzmocni to trwałość decyzji o odpowiednim poziomie ochrony i zapewni większą pewność prawną dla organizacji i organów przekazujących dane osobowe z Europy do Wielkiej Brytanii”.

### Opinia dotycząca RODO

Zdaniem Rady większość zmian wprowadzonych do brytyjskich przepisów o ochronie danych ma na celu ich doprecyzowanie i ułatwienie zgodności z prawem. Niektóre aspekty projektu decyzji wymagają jednak dalszego wyjaśnienia.

EROD zachęca Komisję Europejską do dalszej analizy i monitorowania zmian wynikających z ustawy o uchyleniu i reformie prawa UE (Retained EU Law – Revocation and Reform Act 2023), znanej jako ustawa REUL, w szczególności usunięcia zasady nadrzędności prawa Unii oraz bezpośredniego stosowania zasad prawa UE.

Rada zauważa, że Sekretarz Stanu otrzymał nowe uprawnienia do wprowadzania zmian w nowym systemie ochrony danych poprzez regulacje wtórne, które wymagają mniejszej kontroli parlamentarnej. Dotyczy to m.in. transferów międzynarodowych, zautomatyzowanego podejmowania decyzji oraz zarządzania brytyjskim organem nadzorczym – Information Commissioner's Office (ICO). EROD zachęca Komisję do wskazania w ostatecznej decyzji obszarów, które będą podlegać szczególnemu monitorowaniu, aby ograniczyć ryzyko rozbieżności.

Rada zachęca również Komisję do pogłębienia oceny i monitorowania zasad dotyczących transferów danych z Wielkiej Brytanii do państw trzecich. Nowy test adekwatności, wprowadzony ustawą o danych (Data Use and Access Act, 2025), wymaga, aby poziom ochrony w państwie trzecim nie był istotnie niższy niż ten zapewniany przez brytyjskie przepisy, ale nie odnosi się do ryzyka dostępu ze strony rządu, dostępnych środków odwoławczych dla osób fizycznych ani potrzeby istnienia niezależnego organu nadzorczego.

Komisja powinna także ocenić i monitorować domniemane stosowanie przez rząd Wielkiej Brytanii tzw. Notices of Technical Capability (TCN), które zobowiązują firmy do obchodzenia szyfrowania, co może prowadzić do systemowych luk i zagrozić integralności oraz poufności komunikacji elektronicznej.

Na koniec EROD wzywa Komisję do dalszej oceny i monitorowania zmian w strukturze ICO oraz wykonywania jego uprawnień naprawczych. W tym kontekście Rada pozytywnie ocenia politykę przejrzystości ICO oraz dostępność danych statystycznych i analitycznych dotyczących jego działań egzekucyjnych.

Nowe decyzje o odpowiednim poziomie ochrony będą uzupełnieniem decyzji z 2021 r., które nadal będą obowiązywać w obszarach nieobjętych projektem z 2025 r. EROD opiera się na swoich opiniach z 2021 r. (14/2021 i 15/2021). W szczególności bliska zgodność między ramami RODO a brytyjskim systemem prawnym w kluczowych obszarach, podkreślona w 2021 r., pozostaje aktualna (np. przejrzystość, prawa osób, których dane dotyczą, oraz szczególne kategorie danych).

### Opinia dotycząca LED

EROD z zadowoleniem przyjmuje utrzymującą się zgodność między ramami ochrony danych w Europie i Wielkiej Brytanii oraz zachęca Komisję do uzupełnienia oceny o aspekty dotyczące wyjątków związanych z bezpieczeństwem narodowym. Takie wyjątki mogą uchylać większość zasad ochrony danych oraz niektóre zasady transferów międzynarodowych dla organów ścigania, a także ograniczać uprawnienia kontrolne i egzekucyjne ICO.

Rada zachęca Komisję do analizy brytyjskich zasad dotyczących transferów danych osobowych do państw trzecich, w szczególności nowego testu adekwatności, w sposób analogiczny do opinii dotyczącej RODO.

EROD zwraca też uwagę na bardziej liberalne podejście do zautomatyzowanego podejmowania decyzji oraz nowe uprawnienia przyznane Sekretarzowi Stanu w tym zakresie. Rada przypomina o znaczeniu istotnej kontroli ludzkiej i wzywa Komisję do wyjaśnienia oraz monitorowania możliwych wyjątków od prawa jednostki do uzyskania interwencji człowieka.

Na koniec EROD zauważa, że system nadzoru nad organami ścigania oraz mechanizmy odwoławcze pozostają w dużej mierze niezmienione, i ponownie podkreśla potrzebę ścisłego monitorowania przez Komisję stosowania środków naprawczych oraz dostępnych środków ochrony prawnej dla osób fizycznych w brytyjskim systemie ochrony danych.

**Źródło:**

**Komunikat Europejskiej Rady Ochrony Danych**

Draft UK adequacy decisions: EDPB adopts opinions | European Data Protection Board

# TRYBUNAŁ SPRAWIEDLIWOŚCI DOPRECYZOWUJE ZAKRES POJĘCIA DANYCH OSOBOWYCH W KONTEKŚCIE PRZEKAZANIA DANYCH PSEUDONIMIZOWANYCH STRONOM TRZECIM – C-413/23 P (EIOD V SRB)

Trybunał Sprawiedliwości uchylił wyrok Sądu ogólnego, który unieważnił decyzję Europejskiego Inspektora Ochrony Danych (EIOD).

Po przeprowadzeniu procedury restrukturyzacyjnej Banco Popular Español Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB) 7 czerwca 2017 r. przyjęła wstępną decyzję dotyczącą ewentualnej konieczności wypłaty odszkodowań byłym akcjonariuszom i wierzycielom banku. Ponieważ decyzja ta została podjęta bez wysłuchania tych osób, SRB zorganizowała później procedurę umożliwiającą im przedstawienie uwag do tej decyzji. W ramach tej procedury SRB przekazała część tych uwag, w formie danych pseudonimizowanych, firmie Deloitte – spółce audytorskiej i doradczej, której powierzono ocenę skutków procedury restrukturyzacyjnej dla akcjonariuszy i wierzycieli.

Kilku poszkodowanych akcjonariuszy i wierzycieli złożyło skargi do Europejskiego Inspektora Ochrony Danych, twierdząc, że SRB nie poinformowała ich o przekazaniu danych ich dotyczących osobom trzecim, tj. Deloitte. EIOD uznał, że w tym przypadku Deloitte był odbiorcą danych osobowych skarżących. Ponadto stwierdził, że SRB naruszyła obowiązek informacyjny określony w rozporządzeniu 2018/1725. SRB wniosła następnie skargę o unieważnienie decyzji EIOD do Sądu ogólnego Unii Europejskiej. Sąd ogólny częściowo uwzględnił skargę i unieważnił zaskarżoną decyzję.

Rozpatrując apelację wniesioną przez EIOD, Trybunał Sprawiedliwości uchylił wyrok Sądu ogólnego i przekazał sprawę z powrotem. Kluczowe ustalenia Trybunału Sprawiedliwości:

- Po pierwsze, Trybunał uznał, że Sąd ogólny popełnił błąd prawny, twierdząc, że EIOD powinien był zbadać treść, cel lub skutki uwag przekazanych Deloitte, aby stwierdzić, czy „dotyczyły" one osób, które je złożyły. Trybunał podkreślił, że osobiste opinie lub poglądy, jako wyraz myślenia danej osoby, są z natury rzeczy ściśle z nią związane.

- Po drugie, Trybunał potwierdził, że Sąd ogólny miał rację, wskazując, iż dane pseudonimizowane nie zawsze i dla każdej osoby muszą być uznawane za dane osobowe w rozumieniu rozporządzenia 2018/1725. Zgodnie z orzecznictwem, pseudonimizacja może – w zależności od okoliczności – skutecznie uniemożliwić identyfikację osoby, której dane dotyczą, przez podmioty inne niż administrator.
- Po trzecie, Trybunał stwierdził, że Sąd ogólny popełnił błąd prawny, uznając, że EIOD powinien był ocenić, czy uwagi przekazane Deloitte stanowiły dane osobowe z punktu widzenia Deloitte. Trybunał wyjaśnił, że ocena identyfikowalności osoby, której dane dotyczą, zależy od okoliczności przetwarzania danych w danym przypadku. Obowiązek informacyjny dotyczy relacji prawnej między osobą, której dane dotyczą, a administratorem i odnosi się do informacji przekazanych temu administratorowi – przed ewentualnym przekazaniem ich stronie trzeciej.

W związku z tym Trybunał uznał, że identyfikowalność osoby, której dane dotyczą, należy oceniać w momencie ich zbierania i z perspektywy administratora. Obowiązek informacyjny SRB obowiązywał przed przekazaniem danych i niezależnie od tego, czy dane te były uznawane za dane osobowe z punktu widzenia Deloitte po ewentualnej pseudonimizacji.

**Źródło:**

**Komunikat prasowy Trybunału Sprawiedliwości Unii Europejskiej**

The Court of Justice clarifies the scope of the concept of personal data in the context of a transfer of pseudonymised data to third parties

# PRAWA OSÓB W SYSTEMIE EURODAC – PRZYPOMNIENIE AKTUALNYCH ZASAD

System Eurodac, ustanowiony pierwotnie w 2000 r. i następnie ujednolicony w ramach rozporządzenia (UE) nr 603/2013, pozostaje jednym z kluczowych elementów unijnej polityki azylowej i funkcjonowania systemu dublińskiego. Do czasu wejścia w życie nowych przepisów w ramach reformy przygotowywanej w kontekście paktu migracyjno-azylowego obowiązują dotychczasowe zasady dotyczące realizacji praw osób, których dane są przetwarzane w systemie.

Raport Grupy Nadzorczej Eurodac (Eurodac Supervision Coordination Group) z 2019 r. podkreśla, że:

- prawo dostępu,
- prawo do sprostowania,
- prawo do usunięcia danych,

należą do podstawowych gwarancji ochrony danych osobowych. W obszarze migracji mają one szczególne znaczenie ze względu na potencjalnie daleko idące skutki błędnego lub bezprawnego przetwarzania danych dla osób ubiegających się o ochronę międzynarodową. Ich skuteczne wykonywanie zwiększa przejrzystość przetwarzania, pozwala wykrywać nieprawidłowości, poprawia jakość danych oraz stanowi istotny element nadzoru nad funkcjonowaniem systemu Eurodac.

## Przepisy pozostają w mocy do czasu reformy

Pomimo trwającego procesu wdrożenia nowej wersji Eurodac procedury udzielania dostępu do danych, ich poprawiania i usuwania pozostają niezmienione. Państwa członkowskie są nadal zobowiązane do stosowania obowiązujących przepisów regulacji 603/2013 oraz zapewnienia osobom zarejestrowanym w systemie realnej możliwości wykonywania ich praw.

## Realizacja praw w Polsce – obowiązujące rozwiązania krajowe

W Polsce zasady współpracy organów odpowiedzialnych za wykonywanie przepisów rozporządzenia 603/2013 w sprawach cudzoziemców zostały określone w porozumieniu administracyjnym z 1 czerwca 2015 r., zawartym pomiędzy:

- Komendantem Głównym Policji,
- Komendantem Głównym Straży Granicznej,
- Szefem Urzędu ds. Cudzoziemców,
- Radą ds. Uchodźców,
- Centralnym Laboratorium Kryminalistycznym Policji.

Porozumienie to określa zasady wzajemnej współpracy oraz koordynacji działań organów właściwych w zakresie realizacji przepisów rozporządzenia (UE) nr 603/2013, w tym podział odpowiedzialności, zasady komunikacji, wymianę informacji oraz procedury postępowania przy obsłudze wniosków o dostęp, sprostowanie i usunięcie danych.

Zgodnie z porozumieniem cudzoziemiec, którego dane daktyloskopijne zostały wprowadzone do Eurodac, jest uprawniony do złożenia wniosku ustnie do protokołu lub pisemnie. Wniosek należy kierować do Szefa Urzędu ds. Cudzoziemców.

### Podsumowanie

Choć unijna reforma Eurodac jest w toku, do czasu jej wejścia w życie obowiązuje aktualny reżim prawny oparty na rozporządzeniu 603/2013 oraz krajowym porozumieniu z 2015 r. Przepisy te nadal stanowią podstawę wykonywania praw osób, których dane znajdują się w systemie, a także określają ramy współpracy właściwych organów krajowych. Do momentu wdrożenia nowych regulacji kluczowe pozostaje zapewnienie osobom zarejestrowanym w Eurodac jasnych informacji o przysługujących im uprawnieniach oraz o obowiązujących procedurach ich realizacji.

# OCHRONA WIZERUNKU I PRYWATNOŚĆ MAŁOLETNICH – ZAPIS WYKŁADU

Poniższy materiał został przygotowany na podstawie wystąpienia Pauliny Dawidczyk, dyrektor Departamentu Skarg UODO, które odbyło się podczas wizyty Urzędu w Rzeszowie w ramach akcji „UODO rusza w kraj".

Ochrona wizerunku małoletnich to sprawa absolutnie zasadnicza, jeśli chodzi o społeczny wymiar ochrony danych osobowych i prawo do prywatności. To również zagadnienie istotne z perspektywy szkoły jako placówki oświatowej, czyli administratora danych, ale także z perspektywy nauczycieli, którzy przekazują uczniom informacje o tym, jak chronić dane. I istotne z perspektywy rodziców. Bo to rodzice są odpowiedzialni za udostępnianie wizerunku dzieci.

UODO od wielu lat szczególnie opiekuje się sektorem oświaty, czego wyrazem jest chociażby program „Twoje dane – Twoja sprawa". Urząd stawia na ochronę praw małoletnich i ochronę ich wizerunku, co ma odzwierciedlenie m.in. w kontroli podmiotów oświaty (prowadzonej przez Urząd w ramach kontroli sektorowych), które udostępniają wizerunek dzieci i młodzieży.

Już samo RODO w dwóch motywach wskazuje na konieczność szczególnej ochrony danych małoletnich. W motywie 38 RODO podane jest uzasadnienie, że ta praktyka powinna wynikać z tego, że dzieci mają skromniejszą świadomość swoich praw i konsekwencji swoich działań, zabezpieczeń i tych uprawnień, które przysługują im w związku z przetwarzaniem danych osobowych. Dlatego to dorosły powinien się skupić na ochronie tychże praw. Motyw 58 natomiast wyjaśnia, że w przypadku przetwarzania danych dzieci obowiązki informacyjne odnoszące się do ich praw, wynikających z przepisów o ochronie danych osobowych, powinny być im przekazywane w sposób jasny i nieskomplikowany.

Stawianie na to, aby obowiązek informacyjny był jak najbardziej klarowny, to w ogóle idea RODO – dotyczy nie tylko małoletnich, dotyczy generalnie wszystkich podmiotów danych, zatem oznacza to, że wszelkie obowiązki informacyjne powinny być przekazywane prostym językiem. Administratorom jednak nierzadko wydaje się, że to jakiś obowiązek prawny wynikający z ważnej ustawy, jaką jest RODO. Nic bardziej mylnego: to po prostu ogólna idea RODO, odnosząca się do sfery komunikowania.

# 6 PRACOWNICY UODO

Wizerunek to bardzo ważne dobro i dana osobowa, które są chronione przez wiele praw. Ale dane osobowe i nasza prywatność to również dobra osobiste, a zatem są chronione przez kodeks cywilny. Naruszenie wizerunku może więc powodować odpowiedzialność na gruncie prawa cywilnego, więc osoba, której wizerunek został udostępniony wbrew jej woli, może pozwać naruszyciela czy szkołę, może również domagać się odszkodowania, bo w trybie dochodzenia roszczeń na gruncie obrony dóbr osobistych taki pokrzywdzony może właśnie tego się domagać; może się też domagać odszkodowania na gruncie RODO, jeżeli zwróci się do sądu cywilnego z zarzutem naruszenia ochrony jego danych osobowych.

Ustawa o prawie autorskim i prawach pokrewnych to kolejny akt prawny, który reguluje kwestie przetwarzania wizerunku. Trzeba także pamiętać o kodeksie rodzinnym i opiekuńczym, i o Konstytucji RP, która formułuje fundamentalne prawo do prywatności. Należy również pamiętać o katalogu praw człowieka i obywatela.

Natomiast nierzadko jest tak, i w kontekście wizerunku też trzeba to wiedzieć, że daną osobową może być także zdjęcie osoby, ale bez pokazania jej twarzy. W ostatnim czasie w Departamencie Skarg UODO była rozpatrywana skarga pani, która była zatrudniona w szkole znajdującej się w małej miejscowości, na stanowisku osoby sprzątającej, i myła okna z naruszeniem przepisów BHP. W związku z tą sytuacją ta pani została zwolniona przez dyrekcję placówki. Gazeta lokalna opisała tę historię, umieszczając zdjęcie tej osoby: ta pani była ustawiona tyłem, więc nie było tam widać jej twarzy. Natomiast w tej sytuacji UODO uznał, że doszło do przetwarzania danych osobowych. W tej szkole były zatrudnione trzy panie sprzątające. Akurat dwie z nich były wysokie i szczupłe, a zwolniona pani była niską osobą, bardziej krępej postury, zatem dla mieszkańców małej miejscowości, dla tej szkoły, dla uczniów i dla nauczycieli była absolutnie rozpoznawalna. Zatem nie zawsze jest tak, że musi być ujawniony wizerunek twarzy, abyśmy mogli powiedzieć, że mamy do czynienia z przetwarzaniem wizerunku. Czasami dana informacja wynika z kontekstu sytuacyjnego.

Niezwykle ważną kwestią jest również kwestia zgody na przetwarzanie wizerunku. Zgoda jest przesłanką, która jest wykorzystywana dla zalegalizowania przetwarzania danych, jeśli chodzi o publikację zdjęć. Szkoły używają wizerunków uczniów w celu promowania swoich imprez, w celu zareklamowania swojej działalności. To zrozumiałe i aby było to legalne, musi nastąpić za zgodą osoby, której dane dotyczą, a w przypadku osoby małoletniej – rodzica lub opiekuna prawnego. Według definicji RODO zgoda osoby, której dane dotyczą, lub rodzica, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli w formie oświadczenia lub wyraźnego działania potwierdzającego. Co ważne, zgoda może być odwołana w każdym momencie, zatem jeżeli rodzic zmieni zdanie, to należy to uszanować.

A jak szczegółowo powinna wyglądać zgoda na publikację wizerunku? Przede wszystkim musi być wyrażona w sposób dowolny, więc nie możemy nikogo do wyrażenia takiej zgody zmuszać, nie może być też sytuacji, że jeśli rodzic nie wyraził zgody na publikację wizerunku dziecka, to ono nie będzie mogło brać udziału w jakiejś aktywności w szkole. Zgoda powinna być również precyzyjna i przejrzysta, to znaczy, należy wskazać, czego rzeczywiście ona dotyczy. Nie wystarczy zgoda blankietowa, która wskazuje, że ktoś zgadza się na publikację wizerunku w każdym miejscu na nieokreślony czas, w jakikolwiek sposób, w jakimkolwiek celu. Bo określenie celu pozwala później w kwestiach spornych interpretować i oceniać sytuację, zatem jest czynnością nad wyraz istotną. Zgoda powinna też zawierać opis sposobu wykorzystania wizerunku, czyli powinno być np. zdefiniowane to, gdzie wizerunek będzie publikowany. Jeżeli ktoś chce go publikować w mediach społecznościowych, np. na Facebooku szkoły, to zalecane jest, aby doprecyzować, że te media społecznościowe to będzie właśnie Facebook i żadne inne medium poza nim. Zgoda musi również określać warunki wykorzystania wizerunku, czyli np. jeżeli wiemy już, że zdjęcie będzie podpisywane, opatrywane komentarzem, imieniem dziecka, to są to wszystko warunki wyrażenia zgody w sposób świadomy. I tak, jak już zostało powiedziane, zgoda musi być napisana zrozumiałym językiem, wyrażona na rzecz konkretnego podmiotu, w przypadku szkoły – to ona będzie administratorem danych. Zgoda musi też dotyczyć oznaczonego czasu, no i oczywiście musi być wyrażona przed faktem publikacji.

Jaka powinna być forma zgody? RODO nie narzuca żadnej formy, wskazując, że może być ona dowolna, chyba że mamy do czynienia z danymi szczególnie chronionymi, danymi szczególnej kategorii. Może być oczywiście mailowa, SMS-owa, aby w razie sporu istniał dowód (np. wpłynie skarga do UODO na to, że publikowane są dane, publikowany jest wizerunek dziecka, a tej zgody nie było, i szkoła zgodnie z zasadą rozliczalności będzie mogła się wykazać przed organem taką zgodą, nawet w formie SMS-owej).

A co ze zgodą samego dziecka na publikację wizerunku? Oczywiście póki nie jest pełnoletnie, to według kodeksu rodzinnego i opiekuńczego to rodzic reprezentuje dziecko. Najważniejsza jest odpowiedzialność dorosłego za ochronę prywatności małoletniego, natomiast w przypadku dzieci starszych oczywiście zalecana jest konsultacja z dzieckiem; jeżeli ono już jest na odpowiednim etapie rozwoju, ma odpowiedni stopień dojrzałości – to należałoby uszanować jego zdanie, i wynika to nie tylko z racjonalnego sposobu myślenia, ale też jest to wprost wskazane w kodeksie rodzinnym i opiekuńczym oraz w Konwencji o prawach dziecka.

Najczęściej szkoły publikują wizerunki na stronach internetowych. I nie jest to zakazane. To przecież zrozumiałe, że placówka chce promować swoją działalność. Jeżeli posiada zgodę, jest to działanie legalne.

# 6 PRACOWNICY UODO

W poradniku UODO o ochronie wizerunku dziecka można znaleźć check listę warunków dotyczących tego, czy taka publikacja jest konieczna. I tam są pytania, na które administrator danych w szkole powinien sobie odpowiedzieć, decydując się na upublicznienie wizerunku bądź nie. To pytania przede wszystkim odnoszące się do tego, czy to rzeczywiście konieczne, czy dany cel nie może zostać osiągnięty w inny sposób, czy w przyszłości nie narazimy dziecka na śmieszność? Czy te zdjęcia nie będą wykorzystane?

Ustawa o prawie autorskim i prawach pokrewnych to także akt prawny, który reguluje kwestie rozpowszechniania wizerunku i np. wyłącza on konieczność pozyskania zgody w dwóch sytuacjach: jeżeli jest to rozpowszechnianie wizerunku osoby powszechnie znanej i wizerunek jest uwieczniony w związku z pełnioną przez tę osobę funkcją, ale także jeśli publikowany jest wizerunek osoby stanowiący jedynie szczegół większej całości, takiej jak zgromadzenie, krajobraz, publiczna impreza. Oczywiście kwestii ustawy o prawie autorskim i prawach pokrewnych i kwestii realizacji wymogów tej ustawy nie ocenia Prezes UODO, ale ocenia je sąd cywilny.

To, co rekomenduje UODO, to szczególna ostrożność i pamiętanie o zagrożeniach, czyli np. o tym, że w internecie nic nie ginie: nawet jeżeli coś zostało umieszczone, a później usunięte przez administratora, to przecież w międzyczasie mogło zostać skopiowane. UODO prowadzi wiele postępowań dotyczących osób, które żądają np. od Google'a, aby usunął linki do stron, gdzie były do znalezienia informacje o nich. I czasami zdarza się, że nawet jeżeli administrator usunie te strony, to i tak te informacje są przez jakiś czas indeksowane w sieci. I jest to naprawdę trudny proces, żeby osiągnąć cel w postaci usunięcia danych, a zatem prawo do bycia zapomnianym, które gwarantuje nam RODO w przypadku internetu, czasami niełatwo zrealizować. Zdjęcia i filmy często bowiem przestają być własnością publikujących. I wówczas nie mamy już żadnej kontroli nad tym, co w internecie na nasz temat kiedyś zostało opublikowane.

Pojawia się też problem nieświadomego udostępniania wraz z wizerunkiem szerokiego zakresu informacji. Czasami jest tak, że rodzic, który udostępnia dane na Facebooku, bezwiednie udostępnia cały profil informacji o swoim dziecku, tak np. zdarza się przy fotografiach dokumentujących dzień narodzin. A sprawą już zupełnie zasługującą na potępienie jest troll parenting, czyli pokazywanie filmików z dziećmi w sytuacjach naruszających ich godność.

Kolejnym zagadnieniem jest monitoring wizyjny w szkołach. To może być najbardziej ingerująca w prywatność forma nadzoru. W placówkach edukacyjnych nierzadko jest tak, że monitoring jest wprowadzany bezrefleksyjnie, wśród rodziców panuje wręcz przekonanie, że jeżeli szkoła nie ma monitoringu, to nie jest bezpieczna.

# 6 PRACOWNICY UODO

Regulacje, które określają zasady monitoringu, przede wszystkim wskazują cele, sposób jego prowadzenia, obszary, okres przechowywania nagrań i obowiązki informacyjne. A cele to zwłaszcza zapewnianie bezpieczeństwa uczniom i pracownikom. Zatem jeśli monitoring jest wprowadzany w celach bezpieczeństwa, to nie może być wykorzystywany w innym celu, bo bywają sytuacje, że szkoła za pomocą monitoringu nagrywa np. bójkę czy kryzysową sytuację uczniów podczas przerwy i później to nagranie jest wykorzystywane jako materiał poglądowy na spotkaniu rady pedagogicznej albo psychologów szkolnych. I to jest właśnie wyjście poza cel. I taka sytuacja, jeżeli trafiłaby do rozpatrzenia np. w przypadku złożenia skargi przez osobę, której dane dotyczą, byłaby oceniona przez Prezesa UODO jako naruszenie RODO. W tym kontekście ważne jest też uznanie, że uczniowie i małoletni są podmiotem danych osobowych. Prawo oświatowe w wymogach dotyczących monitoringu szkolnego już wskazuje, z jakimi podmiotami należy skonsultować prowadzenie monitoringu. I wśród nich jest samorząd uczniowski, co świadczy o tym, że opinie ucznia i małoletniego w tym zakresie są nad wyraz istotne.

Musimy również pamiętać, że to szkoła jest administratorem danych. O tym, kto jest administratorem, decydują przepisy. W przypadku placówki edukacyjnej nie ma tu wątpliwości: przepisy oświatowe wskazują na obowiązki szkoły, więc czynią ją administratorem. Z kolei rada rodziców jest oczywiście wewnętrznym organem szkoły, którego obowiązek powołania wynika z przepisów prawa oświatowego, natomiast to zawsze jest organ wewnętrzny o charakterze społecznym, działający w ramach struktury, nieposiadający osobowości prawnej.

Napotykamy także problemy wokół udzielania informacji o uczniu osobom trzecim. Tutaj wskazana jest szczególna ostrożność, czyli nawet krótka weryfikacja, czy mamy do czynienia z rodzicem dziecka, czy opiekunem prawnym, osobą upoważnioną do pozyskania informacji o nieletnim. Możemy to zrobić chociażby przez dodanie jakiegoś pytania kontrolnego.

Jeżeli chodzi o udostępnianie danych, to również w problemach zgłaszanych Prezesowi Urzędu pojawiają się kwestie udostępniania danych o objęciu ucznia pomocą psychologiczno-pedagogiczną, o posiadaniu przez niego orzeczenia o potrzebie kształcenia specjalnego, które, o czym należy pamiętać, są danymi o stanie zdrowia, czyli są to dane szczególnej kategorii. Często też zdarza się tak, że podczas zebrań omawiana jest sytuacja w szkole i pojawia się sprawa konkretnego ucznia, i nauczyciel, prowokowany przez rodziców, którzy chcą poruszyć tę sprawę na forum, musi być ostrożny, próbując wytłumaczyć innym zachowanie ucznia.

Jest również problem publicznego ganienia uczniów. To także stanowi naruszenie prawa do prywatności. Należałoby to robić z zachowaniem wyjątkowej ostrożności i z uwzględnieniem poszanowania prywatności małoletniego.

# 6 PRACOWNICY UODO

W skargach kierowanych do UODO zdarzają się też zarzuty dotyczące wątpliwości, czy dane dzieci są odpowiednio zabezpieczone, jeżeli np. nauczyciele korzystają z prywatnych adresów mailowych albo zabierają klasówki czy dzienniki ucznia do domu. Za każdym razem należy pamiętać o wprowadzeniu odpowiednich środków bezpieczeństwa.

Jeżeli jednak już coś się stanie, to zgłaszanie naruszeń jest obowiązkiem, który ciąży na administratorze danych. Ale nie należy się obawiać, że zgłoszenie naruszenia od razu będzie generowało wszczęcie postępowania. Tak nie jest. Zgłoszenie naruszenia nie równa się automatycznemu wszczęciu postępowania, natomiast służy temu, aby administrator przeanalizował incydent, który nastąpił w jego organizacji. I co ważne: naruszenie nie może być zgłaszane przez inspektora ochrony danych osobowych (IOD nie może go także podpisywać), ponieważ jest on tym, który nadzoruje to, co robi administrator.

**Paulina Dawidczyk**

**Dyrektor Departamentu Skarg UODO**

URZĄD OCHRONY DANYCH OSOBOWYCH

**Prezes UODO zaprasza na wydarzenie edukacyjne, zaplanowane na ostatni miesiąc 2025 r., które będzie można obejrzeć on-line.**

- **Konferencja międzynarodowa: „The Role of the Council of Europe's Framework Convention on Artificial Intelligence in the Protection of Privacy and Personal Data – Legal, Ethical, and Social Challenges in the AI Era"**

Termin: **10 grudnia** 2025 r., godz. 10:00–16:00

Miejsce: **Urząd Ochrony Danych Osobowych**, ul. Stanisława Moniuszki 1A, Warszawa

Organizatorzy: Prezes UODO we współpracy ze Społecznym Zespołem Ekspertów przy Prezesie UODO, z Komitetem Rady Europy ds. Sztucznej Inteligencji Rady Europy (CAI), Komitetem Konwencji nr 108 Rady Europy (T-PD) oraz Europejską Komisją na rzecz Efektywności Wymiaru Sprawiedliwości Rady Europy (CEPEJ)

Formuła: hybrydowa

Celem konferencji jest stworzenie platformy rozmów i współpracy pomiędzy administracją publiczną, środowiskiem eksperckim, organizacjami międzynarodowymi i sektorem technologicznym, mającej na celu wypracowanie rekomendacji dotyczących zgodności polskich regulacji z instrumentami międzynarodowymi Rady Europy oraz podniesienie świadomości wyzwań związanych z przetwarzaniem danych w systemach AI.

Agenda konferencji obejmuje m.in. wystąpienia przedstawicieli Rady Europy oraz polskich i zagranicznych ekspertów w dziedzinie ochrony danych osobowych i sztucznej inteligencji, trzy panele dyskusyjne dotyczące głównych aspektów ochrony danych w świetle konwencji Rady Europy o sztucznej inteligencji, praktycznych aspektów wdrażania i oceny ryzyka związanego
z przetwarzaniem danych przez sztuczną inteligencję oraz wpływu sztucznej inteligencji na wymiar sprawiedliwości i prawa obywateli oraz podsumowanie i rekomendacje dotyczące wdrażania konwencji Rady Europy o sztucznej inteligencji.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl