URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 07_08/07_08/25

www.uodo.gov.pl

SPIS TREŚCI

SPIS TREŚCI

6. EDUKACJA

Szanowni Państwo,

lipiec i sierpień to naturalny czas wakacji, ale nie znaczy to, że Urząd Ochrony Danych Osobowych pracował w tym miesiącu na zwolnionych obrotach. Wręcz przeciwnie – z kilku powodów był to dla nas okres wyjątkowo intensywny.

Przede wszystkim od lipca Urząd Ochrony Danych Osobowych pracuje w nowej siedzibie – przy ul. Moniuszki 1A w Warszawie. Precyzyjnie zaplanowaliśmy i przeprowadziliśmy operację przeprowadzki tak, by jakość i tempo naszej pracy na tym nie ucierpiały.

Jeśli chodzi o sprawy merytoryczne, to w ostatnich dwóch miesiącach udało nam się przekonać do swoich argumentów sądy w następujących kwestiach:

- Naczelny Sąd Administracyjny potwierdził, że ewentualne przyszłe roszczenia byłego klienta banku nie uzasadniają przetwarzania jego danych osobowych;
- Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę firmy Panek SA na decyzję o nałożeniu na nią kary. W tej sprawie chodziło o naruszenie przepisów o ochronie danych osobowych w trakcie uruchamiania nowej witryny internetowej tej firmy;
- I również WSA w Warszawie potwierdził moją decyzję, która nakładała administracyjną karę pieniężną na spółkę Delta za brak informatycznej analizy ryzyka i niewdrożenie odpowiednich do tego ryzyka środków zabezpieczających;
- Do NSA złożyłem skargę kasacyjną w sprawie, w której prokuratura podczas konferencji prasowej ujawniła dane osoby pokrzywdzonej. We wrześniu 2024 r. nałożyłem na Prokuraturę Krajową karę pieniężną, jednak Wojewódzki Sąd Administracyjny w Warszawie uchylił ją, stąd skarga kasacyjna. Spór dotyczy tego, czy prokuratura miała podstawy prawne, by ujawnić dane osoby pokrzywdzonej napaścią i powód tej napaści, mimo że ofiara nie jest osobą publiczną i ma prawo do ochrony swej prywatności.

W lipcu i sierpniu starałem się wskazywać władzom publicznym na problemy prawne i organizacyjne, które pojawiają się w związku z rozwojem możliwości wykorzystywania danych osobowych:

- Do Pierwszego Prezesa Sądu Najwyższego wystąpiłem z prośbą o wyjaśnienie, dlaczego Sąd publikuje niekoniecznie skutecznie zanonimizowane pisma. Chodzi m.in. o protesty wyborcze, które Sąd publikował co prawda po usunięciu imienia i nazwiska obywatela, ale ujawniając jego odręczne pismo, przez które też można zidentyfikować osobę;
- W sprawie CEIDG skierowałem wystąpienie do Ministra Finansów. Model powszechnej jawności danych osobowych przedsiębiorców podlegających wpisowi do Centralnej Ewidencji i Informacji o Działalności Gospodarczej wymaga rewizji. Jest tam dużo łatwo dostępnych danych, w tym adres, pod którym prowadzona jest działalność, który często jest tożsamy z miejscem zamieszkania, co ingeruje w prywatność takich osób;
- Ministrowi Zdrowia zasugerowałem, że warto zachęcać podmioty medyczne do stosowania bardziej profesjonalnych metod ochrony danych. Jedną z nich jest przyjmowanie przez te podmioty kodeksów postępowania albo uzyskiwanie certyfikatów na wszystkie procedury w zakresie ochrony danych. A świadczeniodawcy, którzy stosują takie zasady, powinni uzyskiwać dodatkowe punkty przy kontraktowaniu usług z Narodowego Funduszu Zdrowia.

To ważne, bo w ostatnim czasie zmuszony byłem wielokrotnie do nałożenia kar pieniężnych na placówki medyczne za niewdrożenie odpowiednich środków organizacyjnych i technicznych chroniących dane osobowe pacjentów i pracowników.

Tymczasem kodeksy mogą wesprzeć podmioty medyczne, wskazując im, co jest poprawne, legalne i etyczne w działaniach związanych z przetwarzaniem danych.

- Z kolei Ministrowi Cyfryzacji przedstawiłem – po dyskusji z członkami Społecznego Zespołu Ekspertów oraz grupy ds. sztucznej inteligencji przy Prezesie UODO – uwagi do projektu „Polityki rozwoju sztucznej inteligencji w Polsce do 2030 roku". Podkreśliłem m.in. to, że w dokumencie brakuje podejścia sektorowego dla poszczególnych obszarów funkcjonowania państwa. Projekt nie przewiduje też konieczności przejrzenia aktów prawnych już obowiązujących pod kątem przetwarzania danych. A niewątpliwie należałoby to zrobić;

- Ministrowi Cyfryzacji doradziłem też, że warto zmienić przepisy ustawy o ewidencji ludności w celu umożliwienia rodzicom i opiekunom prawnym zastrzegania numeru PESEL osoby małoletniej. Cieszę się na wstępną pozytywną reakcję Ministra Cyfryzacji – już wkrótce podejmiemy z ministerstwem roboczą współpracę, by wypracować konkretne rozwiązania w tym zakresie;

- Także do Ministra Cyfryzacji skierowałem pismo z wnioskiem dotyczącym wyroku TSUE w sprawie C-470/21. Moim zdaniem powinien on doprowadzić do zmiany polskich przepisów co do przetwarzania danych osobowych chronionych tajemnicą komunikacji elektronicznej. Zmiany powinny objąć zasady dostępu organów ścigania do danych objętych tajemnicą komunikacji elektronicznej uregulowane w Prawie komunikacji elektronicznej;

- Do Ministra Sprawiedliwości zwróciłem się z prośbą o zmianę przepisów o niepodjętych depozytach w aresztach śledczych i zakładach karnych. Ponieważ brakuje szczegółowych przepisów, zakłady penitencjarne posługują się przepisami ogólnymi i ogłaszają w Biuletynie Informacji Publicznej listę osób, które nie podjęły depozytów. Co oczywiście ujawnia fakt pozbawienia wolności w przypadku tych osób;
- Ministrę Edukacji poprosiłem o wyniki analiz dotyczących stosowania monitoringu wizyjnego w placówkach oświatowych prowadzonego na podstawie przepisów Prawa oświatowego. Dzięki temu chciałbym się upewnić, czy analiza ta uwzględnia także aspekty związane z przetwarzaniem i ochroną danych osobowych;
- Wniosłem również o zmianę przepisów o ochronie środowiska, tak aby wyeliminować wątpliwości dotyczące zakresu przetwarzanych danych osobowych przy pracach nad programami ochrony powietrza;
- Do Ministra Spraw Wewnętrznych i Administracji napisałem w sprawie ważnego wyroku TSUE w sprawie kontroli policyjnej. Trybunał ocenił niemieckie przepisy, ale zastosowanie uwag TSUE w polskich przepisach pozwoli lepiej chronić prawa polskich obywateli. Chodzi o sytuację, kiedy policja przejmuje komuś telefon i próbuje go sprawdzić. To, kiedy jest to dopuszczalne, powinno być precyzyjnie zdefiniowane;
- Ponownie wystąpiłem też do szefowej Służby Cywilnej ponawiając wniosek o zmianę rozporządzenia Prezesa Rady Ministrów o stanowiskach w służbie cywilnej, które nie określają jako osobnego stanowiska Inspektora Ochrony Danych. Uzupełnienie wykazu stanowisk urzędniczych o stanowisko IOD jest potrzebne, aby inspektorzy mogli dobrze i skutecznie wykonywać swoje zadania;
- Z Ministerstwa Sprawiedliwości otrzymałem informację, że niebawem ruszą rządowe prace nad zmianą ustawy o księgach wieczystych. Ministerialna wersja projektu już jest. Chodzi o lepszą ochronę danych osobowych obywateli przy dostępie do ksiąg, co od początku mojej kadencji postuluję.

W czasie wakacji byłem zmuszony nałożyć kilka kar finansowych. Do takiego środka uciekam się rzadko, w sytuacjach, gdy nie ma już innego wyjścia:

- Nałożyłem karę pieniężną w wysokości 18 tysięcy złotych na przedsiębiorcę prowadzącego działalność gastronomiczną, który nie odpowiedział na wezwania Prezesa UODO i nie udzielił informacji na temat okoliczności sprawy, w której być może naruszył przepisy o ochronie danych osobowych;
- Karę w łącznej wysokości blisko 17 milionów złotych nałożyłem też na McDonald’s Polska. Spółka powierzyła przetwarzanie danych pracowników sieci restauracji zewnętrznej firmie w celu zarządzania grafikami pracy. Brak analizy ryzyka tego procesu, wdrożenia odpowiednich

zabezpieczeń, realizacji postanowień umowy powierzenia przetwarzania danych osobowych – to wszystko doprowadziło do ujawnienia danych w publicznie dostępnym katalogu;

- Karę w wysokości 32 tysięcy złotych nałożyłem na przychodnię, która nie uwzględniła wszystkich ryzyk dla danych pacjentów, kiedy lekarz zabiera dokumentację na wizyty domowe. Doszło do kradzieży samochodu lekarza i dane dotyczące zdrowia trafiły w niewiadome ręce. Nasze postępowanie wykazało, że takiego zagrożenia nie brano pod uwagę, więc nie próbowano się przed nim zabezpieczyć. A można np. używać teczek na dokumentację z szyfrowanym zamkiem;

- Na ING Bank Śląski nałożyłem karę w wysokości ponad 18 milionów złotych za to, że nadmiernie skanował dowody osobiste klientów i potencjalnych klientów nawet wtedy, gdy ci składali np. reklamacje. Tymczasem przetwarzanie danych osobowych pozyskiwanych poprzez kopiowanie (skanowanie) dokumentów tożsamości przez bank musi być poprzedzone analizą celowości, tj. zweryfikowaniem, czy rzeczywiście taka czynność jest niezbędna;

- Udzieliłem też upomnienia komitetom wyborczym: Rafała Trzaskowskiego oraz Karola Nawrockiego, za ujawnienie danych i miejsca pobytu osoby, której mieszkanie kupił Karol Nawrocki. Zbadałem obie sprawy w toku dwóch oddzielnych postępowań administracyjnych i wydałem dwie decyzje administracyjne.

W środku wakacji, na przełomie lipca i sierpnia, byliśmy – podobnie zresztą jak rok temu – na festiwalu Pol'and'Rock. To dobre miejsce do tego, aby przede wszystkim młodym ludziom przekazywać wiedzę o tym, jak chronić dane w świecie cyfrowym.

W strefie UODO przez cztery dni eksperci Urzędu odbyli setki spotkań i rozmów z uczestnikami festiwalu. Poza tym Urząd zorganizował na festiwalu liczne spotkania, prelekcje, wykłady i debaty, m.in. przy współpracy ekspertów Społecznego Zespołu przy Prezesie UODO. Im oraz pracownikom Urzędu Ochrony Danych Osobowych bardzo za to dziękuję. Dziękuję wszystkim za odwiedzenie namiotu UODO. Do zobaczenia, mam nadzieję, w Czaplinku także za rok.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Na wakacyjny numer tradycyjnie czekaliście aż dwa miesiące, wracamy więc z obszernym materiałem, w którym zaciekawić Was może wywiad z Piotrem Drobkiem, dyrektorem Departamentu Innowacyjności i Zarządzania Danymi w UODO. Opowiada w nim o zadaniach, jakie będzie wykonywała komórka organizacyjna, którą dowodzi, zachęcając wszystkich zainteresowanych tą tematyką do kontaktu z departamentem już teraz, nie czekając na wejście w życie przepisów ustawy o zarządzaniu danymi.

Poruszamy temat dochodzenia przedawnionych roszczeń i tłumaczymy, że zamienia się ono w tzw. roszczenie niezupełne i wierzyciel może nadal podejmować czynności windykacyjne. Jest to jego prawnie uzasadniony interes, a jednocześnie przesłanka legalizująca przetwarzanie danych osobowych.

Przypominamy, że nieprawidłowe doręczenie wiadomości lub dokumentu zawierających dane osobowe może doprowadzić do naruszenia ochrony danych osobowych. Nie ma przy tym znaczenia, czy doszło do niego z powodu błędu zawinionego przez administratora, czy z innej przyczyny.

Opisujemy wybraną decyzję Prezesa UODO: do PUODO zgłosiła się dłużniczka, która twierdziła, że bank nie miał prawa przekazać jej danych do Biura Informacji Kredytowej po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem, bowiem się na to wyraźnie nie zgodziła. Zdaniem organu nadzorczego, bank dopełnił jednak obowiązków wynikających z Prawa bankowego, miał więc prawo przekazać dane dłużniczki do BIK.

Bardzo polecam artykuł nt. komunikatu publicznego jako wyjątkowej formy zawiadomienia osób fizycznych o naruszeniu ochrony danych osobowych. Dowiecie się w jakich sytuacjach, administrator danych może zamiast indywidualnego zawiadomienia zastosować komunikat publiczny lub inną podobnie skuteczną formę.

W podwójnym numerze piszemy też o decyzjach europejskich organów nadzorczych. Warta zapamiętania jest ta wydana przez federalny niemiecki organ nadzorczy, który nałożył kary administracyjne w łącznej wysokości 45 milionów euro na Vodafone – m.in. za niewystarczający nadzór i procedury audytowe wobec agencji partnerskich. To, co zasługuje na uznanie, to że Vodafone, poza usunięciem naruszeń, przekazał kilka milionów euro na rzecz organizacji

zajmujących się promowaniem ochrony danych, umiejętności medialnych i kompetencji cyfrowych oraz zwalczaniem cyberprzemocy. Spółka w pełni współpracowała z organem dostarczając dowodów, których ten nie pozyskałby samodzielnie, a które były dla niej obciążające. Okoliczności te niemiecki urząd uwzględnił na korzyść spółki, odpowiednio zmniejszając karę.

Wiosną przedstawiciele UODO brali udział w licznych międzynarodowych spotkaniach, które potwierdziły wagę współpracy organów europejskich w tworzeniu zrównoważonego systemu ochrony danych osobowych. Każde z wydarzeń było niezwykłą okazją do wymiany doświadczeń, omówienia kluczowych wyzwań regulacyjnych oraz wspólnej refleksji nad przyszłością prywatności cyfrowej:

• 6–9 maja 2025 roku w Batumi uczestniczyliśmy w 33. Europejskiej Konferencji Organów Ochrony Danych Osobowych – Spring Conference 2025, organizowanej przez gruziński organ ochrony danych;

• 12 maja 2025 r. w siedzibie firmy Meta w Berlinie braliśmy udział w eksperckim spotkaniu „Meta Design Jam", poświęconemu najnowszym osiągnięciom w zakresie generatywnej sztucznej inteligencji (GenAI) oraz prognozom dotyczącym kluczowych trendów technologicznych na najbliższe miesiące;

• 12–16 maja 2025 r. w Wenecji byliśmy na międzynarodowej konferencji Privacy Symposium, organizowanej przez Uniwersytet Ca' Foscari oraz partnerów instytucjonalnych i akademickich z całej Europy;

• 11–13 czerwca 2025 r. w Berlinie podgrupa ds. zgodności, zdrowia i eAdministracji (CEH) zorganizowała warsztaty certyfikacyjne. Gospodarzem wydarzenia był berliński organ nadzorczy (BfID);

• 16–18 czerwca 2025 r. w siedzibie Rady Europy w Strasburgu uczestniczyliśmy w pierwszej edycji HUDERIA Academy – intensywnym szkoleniu poświęconym praktycznemu stosowaniu metodyki oceny wpływu systemów sztucznej inteligencji na prawa człowieka, demokrację i rządy prawa;

• 19–20 czerwca 2025 r. w siedzibie CNIL w Paryżu braliśmy udział w międzynarodowym seminarium pt. Artificial intelligence, data protection and fundamental rights, zorganizowanym w ramach projektu JuLIA (Justice, fundamental rights and Artificial Intelligence).

W tym wydaniu biuletynu przybliżamy też sprawozdanie Grupy ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS SCG) podsumowujące półtoraroczną działalność prowadzoną w okresie od początku 2023 r. do września 2024 r.

Rada Europy organizuje międzynarodowy konkurs na plakat i film krótkometrażowy na temat obywatelstwa cyfrowego obywateli. Termin nadsyłania prac upływa 14 września. My z kolei, jak co roku, serdecznie zachęcamy uczniów i nauczycieli do udziału w XVI edycji ogólnopolskiego programu edukacyjnego UODO „Twoje dane – Twoja sprawa”. Przygotowaliśmy dla Was moc atrakcji, które wzmocnią Waszą wiedzę o ochronie danych osobowych oraz prawie do prywatności. Rejestracja trwa od 1 września do 21. października br.

Początek Programu to dla nas symboliczny koniec wakacji. Pewnie większość z Was już wróciła z urlopu, a wielu myślami jest przy początku roku szkolnego, który z reguły oznacza zmiany w codziennym harmonogramie. Trzymam kciuki za gładkie wejście w jesienną rzeczywistość.

Karol Witowski
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

BUDUJEMY ZESPÓŁ DO REALIZACJI ZADAŃ WYNIKAJĄCYCH M.IN. Z AKTU O ZARZĄDZANIU DANYMI

O nowych zadaniach Urzędu, które wynikają z aktu w sprawie zarządzania danymi, z Piotrem Drobkiem, dyrektorem Departamentu Innowacyjności i Zarządzania Danymi w UODO rozmawiał Karol Witowski, rzecznik prasowy UODO.

Departament Innowacyjności i Zarządzania Danymi istnieje w UODO od niedawna. Dlaczego został wydzielony w strukturze Urzędu i z jakimi zadaniami UODO wiąże się jego działanie?

Utworzenie nowego departamentu wiąże się przede wszystkim z planowanym przyznaniem Prezesowi UODO nowych zadań związanych z pełnieniem funkcji organu właściwego do spraw usług pośrednictwa danych i organu właściwego do spraw rejestracji organizacji altruizmu danych, a także innych zadań, które wynikają z aktu w sprawie zarządzania danymi[1]. Realizacja nowych zadań wiązać się będzie z rozszerzeniem zakresu działania Urzędu poza klasycznie rozumiany obszar ochrony danych osobowych. Dlatego konieczne było utworzenie odrębnej komórki organizacyjnej, która – uwzględniając specyfikę tej tematyki – będzie mogła kompleksowo się nią zająć. Regulacje unijne tworzą ramy prawne, które umożliwiają szersze wykorzystywanie danych osobowych i nieosobowych w celu tworzenia innowacyjnych produktów i usług, przy pełnym poszanowaniu praw podstawowych.

W najbliższym czasie, od 12 września, w państwach UE powinny być stosowane przepisy aktu w sprawie danych (Data Act), jednocześnie od września 2023 r., czyli od niemal dwóch lat powinny już być w pełni wdrożone przepisy aktu w sprawie zarządzania danymi (Data Governance Act, DGA), ale, jak wiemy, do dziś m.in.

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

w Polsce to nie nastąpiło – obecnie jesteśmy w trakcie przygotowywania odpowiedniej ustawy. Obowiązują już również niektóre przepisy aktu w sprawie sztucznej inteligencji (AI Act). Jak rozumieć te rozbieżności i jak sobie z nimi poradzić w perspektywie codziennej pracy Pana departamentu?

Ustawodawca unijny w ostatnich latach przyjął różne akty prawne odnoszące się do środowiska cyfrowego i szeroko rozumianego zarządzania danymi. Niewątpliwie wyzwaniem jest zapewnienie ich spójnego stosowania, co wymaga działań zarówno na poziomie unijnym, jak i krajowym. Wszystkie ze wskazanych aktów prawnych są unijnymi rozporządzeniami. Co oznacza, że stosuje się je bezpośrednio w krajowych porządkach prawnych. Niemniej zapewnienie ich pełnego stosowania jest uzależnione od przyjęcia w poszczególnych państwach członkowskich UE odpowiednich ustaw. Niestety Polska zalicza się do stosunkowo licznej grupy państw członkowskich UE, w których takich aktów prawnych jeszcze nie ma. Z perspektywy działania kierowanego przeze mnie departamentu oczywiście kluczowe znaczenie ma uchwalenie ustawy o zarządzaniu danymi, której wejście w życie jest formalnym warunkiem rozpoczęcia przez Prezesa UODO realizacji nowych zadań wynikających z aktu w sprawie zarządzania danymi. Wspieramy merytorycznie prace nad projektem ustawy i w tym zakresie ściśle współpracujemy z Ministerstwem Cyfryzacji. Liczymy na to, że po wakacjach projekt zostanie przyjęty przez Radę Ministrów i skierowany do Sejmu RP. Będziemy wspierać prace nad projektem ustawy również na kolejnych etapach procesu legislacyjnego. Jednocześnie, nie czekając na jego zakończenie intensywnie przygotowujemy się do wykonywania nowych zadań. Budujemy odpowiedni zespół i jego kompetencje merytoryczne, przygotowujemy materiały informacyjne i planujemy różne działania mające na celu zwiększenie zainteresowania tworzącego się sektora pośrednictwa danych i organizacji altruizmu danych.

Ostatnio w ramach dyskusji o danych w świecie cyfrowym pojawia się pojęcie altruizmu danych. Co ono oznacza?

Akt w sprawie zarządzania danymi definiuje altruizm danych – jest to dzielenie się danymi na podstawie wyrażonej przez osoby, których dane dotyczą, zgody na przetwarzanie dotyczących ich danych osobowych lub na podstawie udzielonego przez posiadaczy danych pozwolenia na wykorzystywanie ich danych nieosobowych, bez żądania ani otrzymania za to wynagrodzenia wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych do celów leżących w interesie ogólnym, jak opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie

polityki publicznej lub do celów badań naukowych leżących w interesie ogólnym. Aby budować zaufanie do organizacji altruizmu danych i zachęcać do dzielenia się danymi z pobudek altruistycznych, akt w sprawie zarządzania danymi przewiduje możliwość nadania statusu uznanej w Unii organizacji altruizmu danych.

Czasem pojawia się także pojęcie danych nieosobowych. Czy to dla przyszłych działań Pana departamentu jakieś nowe pole działań?

Jak już wcześniej powiedziałem, akt w sprawie zarządzania danymi obejmuje swoim zakresem zarówno dane osobowe i nieosobowe. Tym samym będziemy zajmowali się również działalnością dotyczącą danych nieosobowych.

Czy Urząd będzie prowadził działania informacyjne w zakresie nowych zadań wynikających z aktu w sprawie zarządzania danymi?

Oczywiście. Najbliższe miesiące chcemy wykorzystać na budowanie świadomości w zakresie pośrednictwa danych, altruizmu danych oraz zasad przekazywania danych nieosobowych do państw trzecich. W lipcu zorganizowaliśmy webinarium na temat nowych zadań Prezesa UODO, z którego nagraniem można się zapoznać na naszej stronie internetowej. Kolejne webinaria na ten temat będą się odbywały cyklicznie. Jednocześnie jesienią planujemy organizację dwóch konferencji dotyczących aktu w sprawie zarządzania danymi. Pracujemy także nad materiałami informacyjnymi i nową zakładką na stronie internetowej urzędu.

Czy osoby lub podmioty zainteresowane tematyką pośrednictwa danych lub altruizmu danych mogą liczyć na kontakt z Pana departamentem?

Tak, zapraszamy wszystkich zainteresowanych tą tematyką do kontaktu z naszym departamentem już teraz, nie czekając na wejście w życie przepisów ustawy o zarządzaniu danymi. Adres poczty elektronicznej do naszego departamentu to: dizd@uodo.gov.pl. Jednocześnie serdecznie zapraszamy na nasze webinaria i konferencje poświęcone tej tematyce.

Dziękuję za rozmowę.

DOCHODZENIE PRZEDAWNIONYCH ROSZCZEŃ

Ponieważ roszczenie przedawnione zamienia się w tzw. roszczenie niezupełne (naturalne), wierzyciel może nadal podejmować czynności windykacyjne. I jest to jego prawnie uzasadniony interes, a jednocześnie przesłanka legalizująca przetwarzanie danych osobowych.

Przedawnienie roszczenia nie skutkuje jego wygaśnięciem, lecz zmianą w tzw. roszczenie niezupełne (naturalne). Jego istotą jest niemożność przymusowego egzekwowania. Potwierdza to m.in. orzecznictwo Sądu Najwyższego. Przykładowo w wyroku z 9 lutego 2018 r. (sygn. akt I CSK 246/17) Sąd Najwyższy wskazał, że „Zgodnie z art. 117 k.c., skutkiem przedawnienia nie jest wygaśniecie roszczenia, a tylko niemożność uzyskania ochrony przewidzianej prawem i w konsekwencji możności uzyskania jego przymusowego zaspokojenia z majątku dłużnika".

Oznacza to, że wierzyciel może nadal podejmować czynności windykacyjne zmierzające do pozasądowej regulacji zobowiązania. Zgodnie ze stanowiskiem Sądu Najwyższego zawartym w wyroku z 27 stycznia 2016 r. (sygn. akt II CSK 67/15), mimo braku możliwości przymusowej realizacji, wygasłe zobowiązanie nadal może być przedmiotem czynności prawnych, takich jak uznania, ugody, potrącenia czy odnowienia. Wskazał też, że realizacja roszczenia naturalnego przez dłużnika na rzecz wierzyciela nie jest świadczeniem nienależnym.

Gdy dłużnik nie uznaje roszczenia

Podkreślić należy, że w sytuacji, w której dłużnik nie uznaje przedawnionego roszczenia, Prezes Urzędu Ochrony Danych Osobowych w swoich postępowaniach nie bada kwestii istnienia lub nieistnienia zobowiązania. Takie sprawy, zgodnie z art. 1 ustawy z 17 listopada 1964 r. Kodeks postępowania cywilnego (k.p.c.), są sprawami cywilnymi i powinny być rozpatrywane w postępowaniach prowadzonych przez sądy powszechne.

Potwierdza to, zachowujący wciąż aktualność, wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 8 stycznia 2010 r. (sygn. akt II SA/Wa 1069/09), w którym sąd wskazał, że „Generalny Inspektor Ochrony Danych Osobowych nie dokonuje oceny umów cywilnoprawnych, nie bada także zasadności roszczeń, ani wymagalności wierzytelności. Nie może także oceniać prawidłowości wykonywania umów, wprowadzania do nich zmian, nie ma prawa kontrolować podstaw ich wypowiadania, czy rozwiązywania. Dotyczy to wszelkich umów cywilnoprawnych, w tym także umów przelewu wierzytelności. Problematyka ta podlega bowiem kognicji

sądów powszechnych, ze względu na ich aspekt cywilnoprawny".

W konsekwencji kwestionowanie przez dłużnika istnienia roszczenia pozostaje bez znaczenia dla legalności procesu przetwarzania, dopóki istnienie wierzytelności nie zostanie podważone we właściwym trybie i formie.

Takie stanowisko Prezes UODO zajął m.in. w decyzji (DS.523.282.2023) odwołującej się do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 6 lipca 2006 r. (sygn. akt II SA/Wa 2226/05), w którym sąd uznał, że „Dopóki ważność umowy nie zostanie podważona we właściwym trybie i formie, umowa stanowi dokument wywołujący określone skutki prawne podlegające także ocenie w świetle ustawy o ochronie danych osobowych".

Takie podejście UODO potwierdził ostatnio Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z 8 maja 2024 r. (sygn. akt II SA/Wa 1889/23) wskazał, że „organ zajmuje się wyłącznie kwestią dotyczącą przetwarzania danych osobowych i poza ową materię nie może wykraczać by uchronić się przed zarzutem naruszenia prawa. (…) dla celu ustalenia podstaw faktyczno-prawnych dopuszczalności przetwarzania danych osobowych, wystarczające jest samo uwiarygodnienie faktu istnienia np. cywilnoprawnego stosunku zobowiązaniowego pomiędzy stronami, z którego administrator danych wywodzi swoje prawo do ich przetwarzania".

Podstawa prawna przetwarzania danych osobowych

Dla przetwarzania danych osobowych w związku z dochodzeniem przedawnionych roszczeń podstawowe znaczenie ma podstawa prawna działań podejmowanych przez wierzycieli.

Zgodnie z art. 6 ust. 1 lit. f RODO przetwarzanie danych jest dopuszczalne, gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Dodatkowo w motywie 47 RODO wyjaśniono, że podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz.

Należy uznać, że dochodzenie przez podmiot roszczeń finansowych jest prawnie uzasadnionym interesem i w tym sensie nadrzędnym nad prawami i wolnościami osoby, której dane dotyczą. Dochodzenie roszczeń nie stanowi bowiem nieproporcjonalnego ograniczenia tych praw i wolności.

Przetwarzanie danych osobowych w celu dochodzenia wierzytelności przedawnionych ma zatem oparcie w art. 6 ust. 1 lit. f RODO. Przy czym dla zaistnienia tej przesłanki konieczna jest także odpowiednia analiza, o której mowa w wytycznych EROD 1/2024 dotyczących przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f RODO i ustalenie, zgodnie z art. 5 ust. 1 lit. b i c RODO, jakie dane są niezbędne dla realizacji konkretnego celu.

W wydanych decyzjach Prezes UODO uznawał za niedopuszczalny proces przetwarzania danych w celu związanym z ewentualnym dochodzeniem przyszłych roszczeń lub ewentualną koniecznością obrony przed nimi w sytuacji, gdy administratorzy zakładali w praktyce automatyzm przetwarzania danych w celach, które jeszcze nie zaistniały. Zdaniem organu nadzorczego brak jest uzasadnienia dla przyjęcia, iż terminy dotyczące przedawnienia roszczeń wynikających ze stosunków zobowiązaniowych określają jednocześnie ramy czasowe, w których dane osobowe mogą być przetwarzane przez administratora. Przedawnienie roszczenia nie wywołuje skutków na gruncie ochrony danych osobowych, nie wpływa bowiem na fakt istnienia roszczenia, a powoduje jedynie zmianę w sferze zarzutów procesowych w postaci możliwości podniesienia okoliczności przedawnienia w sporze sądowym. Organ nadzorczy w wydanych decyzjach podkreślał, że okolicznością usprawiedliwiającą przetwarzanie danych osobowych w celu dochodzenia roszczeń jest sam fakt istnienia roszczenia oraz zamiar jego dochodzenia. Nie jest nią natomiast zmiana w uprawnieniach procesowych podmiotu pozwanego.

Stanowisko o niedopuszczalności przetwarzania danych „na zapas” znalazło potwierdzenie w orzecznictwie Naczelnego Sądu Administracyjnego w wyrokach z 27 marca 2018 r. (sygn. akt I OSK 1459/16), z 6 marca 2019 r. (sygn. akt I OSK 994/17), a także z 8 stycznia 2025 r. (sygn. akt III OSK 4868/21). Aktualność zachowują przy tym warunki określone w ww. wytycznych EROD.

Zakończenie czynności windykacyjnych nie oznacza także, że administrator natychmiast musi usunąć dane dłużnika. O ile bowiem występują inne cele wynikające z odrębnych przepisów prawa, dla realizacji których przetwarzanie danych jest konieczne, dane w tych celach w okresie wskazanym w przepisach administrator będzie zobowiązany przetwarzać (np. na podstawie art. 74 ust. 1, 2 i 3 ustawy z dnia 29 września 1994 r. o rachunkowości, art. 70 § 1 w zw. z art. 86 § 1 ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa czy też art. 49 ust. 1 i 2 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu).

Tym samym **proces przetwarzania danych dłużnika po zakończeniu działań windykacyjnych, do czasu upływu terminów obowiązkowego przechowywania dokumentacji,**

wynikających z ww. przepisów prawa, należy uznać za prawidłowy i znajdujący oparcie w przesłance wynikającej z art. 6 ust. 1 lit. c RODO.

Gdy dłużnik nie aktualizuje danych kontaktowych

Zdarza się, że w toku dochodzenia należności wierzyciel pozyskuje informację o tym, iż wybrane kategorie danych osobowych dłużnika (np. numer telefonu, adres e-mail) nie są już aktualne. Bywa tak, gdyż dłużnicy nie aktualizują swoich danych osobowych, upatrując w tym sposób na uchylenie się od spełnienia zaległych zobowiązań.

W takiej sytuacji administrator powinien podjąć kroki mające na celu wyeliminowanie nieprawidłowości polegającej na przetwarzaniu nieaktualnych danych osobowych. Zgodnie bowiem z art. 5 ust. 1 lit. d RODO, dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").

Zasada ta nie powinna być interpretowana jako nałożony na administratora obowiązek systematycznego poszukiwania danych nieprawidłowych (zob. wyrok Naczelnego Sądu Administracyjnego z 15 kwietnia 2025 r. sygn. III OSK 567/22). W sytuacji, gdy dłużnik nie aktualizuje swojego adresu, choć był wcześniej informowany o potrzebie niezwłocznego powiadomienia wierzyciela o każdej zmianie danych, ponosi on konsekwencje związane z nieodebraniem korespondencji skierowanej na znany wierzycielowi adres. Stanowisko to znajduje potwierdzenie w utrwalonym orzecznictwie sądów cywilnych w sprawach o zapłatę (zob. wyrok Sądu Apelacyjnego w Poznaniu z 7 czerwca 2018 r., sygn. akt I ACa 1260/17; wyrok Sądu Okręgowego w Nowym Sączu z 16 stycznia 2019 r., sygn. akt I C 994/18; wyrok Sądu Rejonowego w Gdyni z 3 listopada 2020 r., sygn. akt I C 925/19).

Pamiętać jednocześnie należy, że administrator jest zobowiązany do zachowania należytej staranności i powinien podejmować działania mające na celu ograniczenie ryzyk dla naruszenia praw i wolności osób, do których kierowana jest korespondencja w związku z dochodzeniem roszczeń, tak, aby osoby nieuprawnione nie zapoznawały się z danymi dłużnika, gdyż przekazanie danych osobie trzeciej będzie stanowiło naruszenie art. 5 ust. 1 lit. a i lit. d RODO.

Nowe dane – weryfikacja prawidłowości

Także w momencie pozyskania nowego adresu dłużnika z zewnętrznych źródeł (np. poprzez działanie podmiotów oferujących usługę aktualizacji danych dłużników lub ze stron internetowych) wierzyciel powinien zbadać, czy pozyskany adres to adres dłużnika, w stosunku do którego prowadzone były czynności windykacyjne. Brak weryfikacji tożsamości potencjalnego dłużnika może skutkować bowiem bezprawnym pozyskaniem danych osobowych osoby trzeciej oraz dalszym ich

przetwarzaniem bez podstawy prawnej. W takiej sytuacji administrator narusza zasady zgodności z prawem, prawidłowości i integralności oraz poufności, o których mowa w art. 5 ust. 1 lit. a, b i f RODO.

Należy podkreślić, że na administratorze danych spoczywa obowiązek podjęcia odpowiednich działań organizacyjnych i wdrożenia mechanizmów identyfikacji, które zagwarantują prawidłowość przetwarzanych danych, oraz zapobiegną pozyskiwaniu danych osób trzecich, zwłaszcza w sytuacji, gdy osoba trzecia ma dane tożsame (np. w zakresie nazwiska) z danymi dłużnika, a sam fakt zbieżności pewnych danych nie stanowi o wystąpieniu interesu prawnego w ich przetwarzaniu po stronie wierzyciela.

Ponadto w momencie, gdy osoba trzecia, której dane administrator pozyskał w przeświadczeniu, że należą do dłużnika, zwraca się do niego żądaniem usunięcia jej danych osobowych (w tym danych kontaktowych), administrator zobowiązany jest do spełnienia tego żądania.

fot. pexels

PRAWIDŁOWO WPISANY ADRES E-MAIL – BŁĘDNE DORĘCZENIE. CZY TO NARUSZENIE OCHRONY DANYCH OSOBOWYCH?

Nieprawidłowe doręczenie wiadomości lub dokumentu zawierających dane osobowe może doprowadzić do naruszenia ochrony danych osobowych. Nie ma przy tym znaczenia, czy doszło do niego z powodu błędu zawinionego przez administratora, czy z innej przyczyny. Dla oceny danego przypadku szczególne znaczenie ma to, czy na skutek takiego zdarzenia może dojść do nieuprawnionego ujawnienia danych osobowych, a więc naruszenia poufności danych.

Ostatnio jeden z inspektorów ochrony danych zwrócił się z prośbą o wyjaśnienie, czy sytuację, w której wiadomość e-mail została prawidłowo zaadresowana przez administratora, lecz na skutek działania algorytmów dostawcy poczty elektronicznej została dostarczona do innej osoby, należy uznać za naruszenie ochrony danych osobowych.

Dla zobrazowania problemu przesłał następujący opis:

1. Administrator danych przesłał wiadomość e-mail na adres, który prawidłowo wskazywał adresata (np. jan.kowalski@...).

2. Z uwagi na specyfikę działania usługi poczty e-mail i ignorowanie kropki w adresie e-mail przed znakiem „@”, wiadomość została przekierowana do innej osoby (np. jankowalski@...).

3. Administrator danych dochował należytej staranności w zakresie adresowania wiadomości i nie miał wpływu na wewnętrzne mechanizmy dostarczania wiadomości przez usługę poczty e-mail.

IOD zapytał, czy w opisanej sytuacji mamy do czynienia z naruszeniem ochrony danych osobowych w rozumieniu przepisów RODO, a jeśli tak, to jakie kroki powinien podjąć administrator, aby uniknąć wystąpienia podobnego przypadku w przyszłości.

W odpowiedzi UODO, nie znając wszystkich szczegółów sprawy, przekazał wskazówki pomocne w rozstrzygnięciu przedstawionych wątpliwości.

Kiedy dochodzi do naruszenia ochrony danych osobowych?

Przez pojęcie „naruszenia ochrony danych osobowych” należy rozumieć „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" (art. 4 pkt 12 RODO).

Inaczej mówiąc, naruszeniem ochrony danych osobowych jest zakłócenie bezpieczeństwa przetwarzanych danych osobowych, które może wpłynąć na ich poufność, integralność lub dostępność.

Prezes UODO w decyzji z 9 grudnia 2020 r. (sygn. DKN.5131.5.2020) wskazał, że „z naruszeniem ochrony danych mamy do czynienia zarówno wówczas, gdy do zdarzenia dojdzie wskutek świadomego działania, jak i wtedy, gdy doprowadzi do niego nieumyślność. (…) Jego skutkiem jest bowiem udostępnienie danych osobowych osobie nieuprawnionej, co oznacza, iż doszło do naruszenia poufności danych".

W Poradniku UODO „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" (str. 8) wskazano również, że naruszenie ochrony danych osobowych pojawia się więc zawsze, gdy dochodzi do zdarzenia, które:

• jest incydentem bezpieczeństwa;

• dotyczy przetwarzanych danych osobowych;

• może doprowadzić do ich nieuprawnionego zniszczenia, utracenia, zmodyfikowania, ujawnienia lub dostępu do nich.

Tym samym naruszeniem ochrony danych osobowych nie jest zdarzenie, które nie spełnia któregoś z tych warunków. Co istotne dochodzi do niego bez względu na to, czy wystąpi przez przypadek (np. w wyniku błędu, zaniedbania lub nieprzewidzianej awarii technicznej) czy też na skutek celowego, bezprawnego działania.

Z naruszeniem ochrony danych osobowych możemy mieć zatem do czynienia nawet w sytuacji niezawinionego działania administratora. Istotą takiego zdarzenia jest bowiem nieuprawnione ujawnienie danych osobowych skutkujące naruszeniem poufności danych. A zatem w sytuacji nieprawidłowego doręczenia dokumentu zawierającego dane osobowe, mimo niezawinionego działania administratora, dochodzi do naruszenia poufności danych osobowych.

Zatem gdy wiadomość e-mail została prawidłowo zaadresowana przez administratora, lecz na skutek działania algorytmów dostawcy poczty elektronicznej została dostarczona do innej osoby, możemy mieć do czynienia z naruszeniem ochrony danych osobowych. W tej sytuacji konieczna może być też realizacja obowiązków określonych w art. 33 i 34 RODO, tj. zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienie osoby, której dane zostały ujawnione, o zaistniałym naruszeniu.

Ochrona na przyszłość

UODO zwrócił też uwagę, że administrator, mając wiedzę na temat przedstawionej „podatności" usługi poczty e-mail, w pierwszej kolejności powinien uwzględnić ją w analizie ryzyka.

Jednocześnie jako przykładowe wskazówki, jak chronić się przed wystąpieniem tego typu naruszenia w przyszłości, podał:

• przekazywanie danych osobowych w zaszyfrowanych plikach [przy jednoczesnym przekazywaniu hasła umożliwiającego odszyfrowanie innym kanałem],

• możliwość skierowania „próbnej" wiadomości e-mail niezawierającej danych osobowych, a po potwierdzeniu jej otrzymania, przesłanie wiadomości z danymi osobowymi.

Warto też zaznaczyć, że pomocne informacje dotyczące powyższego zagadnienia znaleźć można również w rozdziale 6 wskazanego wyżej poradnika dotyczącego naruszeń, zatytułowanym „Zaradzanie naruszeniom ochrony danych osobowych".

Pomocne materiały

Jednocześnie wskazówki dotyczące postępowania z naruszeniami ochrony danych znaleźć można w:

• Wytycznych EROD 9/2022 dotyczących zgłaszania naruszenia ochrony danych osobowych na podstawie RODO (https://uodo.gov.pl/pl/537/2902),

• Wytycznych EROD 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych (https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_pl),

• we wspomnianym poradniku UODO dotyczącym naruszeń ochrony danych osobowych i nagraniach z webinariów na temat tego poradnika (https://www.uodo.gov.pl/pl/138/3621).

BANK DOPEŁNIŁ OBOWIĄZKÓW WYNIKAJĄCYCH Z PRAWA BANKOWEGO, MIAŁ WIĘC PRAWO PRZEKAZAĆ DANE DŁUŻNICZKI DO BIK

Do PUODO zgłosiła się dłużniczka, która twierdziła, że „S" Bank SA nie miał prawa przekazać jej danych do Biura Informacji Kredytowej SA po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem, bowiem się na to wyraźnie nie zgodziła. Jej zdaniem bank nie miał prawa przetwarzać jej danych.

Chodziło o niespłacony kredyt. Zaległości były na tyle duże, że bank wypowiedział klientce umowę.

W takiej sytuacji prawa instytucji finansowej do przetwarzania danych osobowych byłego klienta regulują przepisy art. 105a ust 3. prawa bankowego, a nie wola dłużnika. PUODO stoi na stanowisku – potwierdzonym teraz także orzeczeniami NSA – że zgłoszenie do BIK możliwe jest, jeśli zaległość w spłacie wynosi 60 dni, klient został powiadomiony o zamiarze przetwarzania danych po wygaśnięciu zobowiązania wynikającego z umowy i od momentu tego powiadomienia minęło 30 dni.

W tym wypadku bank wykazał przed PUODO, że zawiadomił klientkę o zamiarze przetwarzania jej danych po wygaśnięciu zobowiązania wynikającego z umowy. Zrobił to mailem, na adres, który podała w umowie. Strony wcześniej umówiły się na taką formę komunikacji.
Bank dysponuje dowodem, że klientka mail odebrała.

Przekazanie danych do BIK nastąpiło dopiero po kilku miesiącach, a nie 30 dni później. Zatem spełniony został wymóg poinformowania, o którym mowa w art. 105a ust. 3 prawa bankowego.

Tym samym zdaniem PUODO bank spełnił wymagania prawa.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych w przedmiotowej sprawie zaistniała określona w art. 6 ust. 1 lit. f RODO przesłanka legalizująca obecny proces przetwarzania danych osobowych skarżącej przez bank w systemie BIK w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

Sygnatura sprawy: DS.523.3117.2024

KOMUNIKAT PUBLICZNY JAKO WYJĄTKOWA FORMA ZAWIADOMIENIA OSÓB FIZYCZNYCH O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. Wprowadzenie

W obecnych czasach incydenty bezpieczeństwa obejmujące dane osobowe, które jednocześnie stanowią naruszenia ochrony danych osobowych, stają się coraz bardziej powszechne. Jest to związane z postępującą globalizacją, cyfryzacją, ale także geopolityką. Jedne wynikają z błędu ludzkiego, inne z zamierzonych działań, np. osób z zewnątrz.

W przypadku powstania naruszenia ochrony danych osobowych niezwykle istotne jest nie tylko szybkie usunięcie skutków naruszenia, ale także odpowiednie poinformowanie osób, których dane dotyczą.

Przepisy zarówno rozporządzenia 2016/679[1], jak również ustawy grudniowej[2] zakładają, że osoba fizyczna, której dane zostały objęte zdarzeniem, mogącym powodować wysokie ryzyko naruszenia jej praw lub wolności, powinna zostać zawiadamiana przez administratora danych o takim naruszeniu. Zasadą jest, że zawiadomienie realizowane jest indywidualnie – administrator bezpośrednio zawiadamia osobę o naruszeniu ochrony jej danych osobowych. Są jednak sytuacje, w których indywidualne zawiadomienie nie jest możliwe (np. brak danych adresowych, zawiadomienie wymaga nadmiernego wysiłku lub kosztów – na ten temat więcej w kolejnych artykułach). Wówczas administrator może zawiadomić osobę o naruszeniu poprzez komunikat publiczny.

Komunikat publiczny należy traktować jako wyjątek od ogólnej zasady indywidualnego zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych.

[1] rozporządzenie 2016/679 - 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 (Dz. Urz. UE L 119 z 4.05.2016 r., str. 1, Dz. Urz. UE L 127 z 23.05.2018 r., str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021 r., str. 35).

[2] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

2. Podstawy prawne stosowania komunikatu publicznego

Zgodnie z art. 34 ust. 3 lit. c) rozporządzenia 2016/679 (analogiczne rozwiązane występuje w art. 45 ust. 4 ustawy grudniowej), administrator danych może zamiast indywidualnego zawiadomienia zastosować komunikat publiczny lub inną podobnie skuteczną formę, jeżeli:

1) indywidualne zawiadomienie osoby wymagałoby niewspółmiernie dużego wysiłku (ze względu na koszty, dużą liczbę osób),

lub

2) administrator ma problem ze zidentyfikowaniem osób, których dane dotyczą, przy jednoczesnym powstaniu wysokiego ryzyka naruszenia ich praw lub wolności.

W takich przypadkach komunikat publiczny pełni rolę alternatywnego środka powiadamiania. Musi być on jednak równie skuteczny w informowaniu o naruszeniu ochrony danych osobowych, jak indywidualne zawiadomienia – co oznacza, że forma, kanał komunikacji oraz treść komunikatu powinny być dostosowane do odbiorcy.

Jednakże należy pamiętać, że administrator formułując komunikat publiczny powinien „stosować komunikaty dedykowane, które nie powinny być przesyłane razem z innymi informacjami, na przykład newsletterem, czy standardową wiadomością. Pomoże to przekazać informacje o naruszeniu w jasny i przejrzysty sposób. Powiadomienia ograniczającego się do komunikatu prasowego czy firmowego bloga nie uznaje się za skuteczne powiadomienie osoby fizycznej o naruszeniu.”[3] Na marginesie wskazać należy, iż skuteczność takiego zawiadomienia może badać organ nadzorczy. W takim przypadku administrator musi być w stanie wykazać jego skuteczność.

3. Charakterystyka komunikatu publicznego

Komunikat publiczny nie ma jednej, sztywno określonej formy – jego skuteczność ocenia się przez pryzmat możliwości dotarcia do jak najszerszego grona osób potencjalnie dotkniętych incydentem. Musi on także zawierać stosowne elementy. Najczęściej stosowane formy komunikatu publicznego to:

1) ogłoszenia na stronie internetowej administratora danych;

2) publikacje w lokalnych lub ogólnokrajowych mediach;

3) powiadomienia za pośrednictwem mediów społecznościowych;

4) komunikaty prasowe lub konferencje prasowe.

[3] Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0 czerwiec 2019 r., s. 29

4 NARUSZENIA I KONTROLE

Dobór formy powinien być oparty na analizie grupy docelowej i kanałów komunikacji, z których korzystają osoby, których dane zostały naruszone. Należy pamiętać, że nie każdy korzysta z internetu, jak również nie każdy czyta papierowe wydanie gazet.

Komunikat publiczny powinien zawierać te same informacje co zawiadomienie indywidualne[4]. Należy także pamiętać o:

• przejrzystym języku – komunikat powinien być zrozumiały dla odbiorcy, bez technicznego żargonu, bez używania ogólnych sformułowań (np. kradzież tożsamości, strata finansowa); taki komunikat powinien być zrozumiały także przez osoby niepracujące „na przepisach prawa",

• dostępności – informacja powinna być łatwo dostępna przez rozsądny okres czasu.

4. Przykłady zastosowania komunikatu publicznego:

1) naruszenie polegało na zagubieniu dokumentów przez kuriera, zawierających dokumentację rejestrową dawców (szeroki zakres danych, wraz z numerem PESEL oraz danymi genetycznymi). Dane zbierane były od turystów wypoczywających w nadmorskiej miejscowości, zatem czasowo w niej przebywających). Administrator zdecydował o zawiadomieniu tych osób poprzez komunikat publiczny z uwagi na to, że nie miał on wiedzy kogo dotyczyło naruszenie ochrony danych osobowych (zaginione dokumenty były jedyną kopią). Problemem jednak było miejsce jego zawieszenia – bowiem było to lobby hotelu w nadmorskiej miejscowości wypoczynkowej. Prawdopodobieństwo zapoznania się z komunikatem przez osoby, których dane dotyczą, było znikome, ze względu na to, że najprawdopodobniej osoby, które wypełniły zagubione formularze, były w tym miejscu na wakacjach i prędko nie wrócą. Z uwagi na to, że administrator postanowił wyłącznie o takim kanale zawiadomienia, Prezes UODO uznał, iż skuteczność takiego zawiadomienia jest znikoma. Organ skierował do administratora wystąpienie, w którym zobowiązuje go do zamieszczenia komunikatu na stronie internetowej.

2) podmiot leczniczy ucierpiał w czasie powodzi, tracąc całą dokumentację medyczną – zawiadomił poprzez komunikat umieszczony na drzwiach przychodni, na Instagramie oraz na swojej stronie na Facebooku – organ uznał, iż działania administratora były wystarczające.

5. Dobre praktyki w publikowaniu komunikatów publicznych:

1) stosowanie prostego i jasnego języka – odbiorcami są często osoby bez wiedzy prawniczej (używanie sformułowań jak np. zawarcie umów cywilnoprawnych nie dla każdego będzie zrozumiałym sformułowaniem, ale zawarcie umowy pożyczki czy kredytu będzie zrozumiałe dla każdego);

[4] https://uodo.gov.pl/pl/598/3563

2) wielokanałowość – równoległe użycie różnych form dotarcia zwiększa skuteczność;

3) aktualizowanie komunikatu – np. w razie zmiany sytuacji (zidentyfikowanie nowych osób poszkodowanych);

4) pozycjonowanie komunikatu w przypadku wyboru miejsca umieszczenia jako strony internetowej administratora – okres, przez jaki powinien być udostępniony komunikat powinien uwzględniać m.in. charakter i okoliczności naruszenia ochrony danych osobowych, zakres danych objętych takim naruszeniem, miejsce w jakim do niego doszło, czas trwania, wiek osób;

5) opis charakteru naruszenia powinien pozwolić osobom fizycznym czytającym taki komunikat powiązanie ze swoimi danymi, tak aby mogły ocenić, czy dotyczy on ich danych osobowych (np. osoby legitymowane przez policję/ straż graniczną w okresie wakacyjnym w takiej i takiej lokalizacji);

6) współpraca z UODO – konsultacja treści komunikatu z organem nadzorczym, szczególnie w przypadkach wątpliwych, reagowanie na uwagi oraz wystąpienia Prezesa UODO;

7) transparentność i odpowiedzialność – unikanie minimalizowania znaczenia incydentu, rzetelne informowanie.

6. Wnioski

Komunikat publiczny jest narzędziem o wyjątkowym charakterze w arsenale środków stosowanych przez administratorów danych w sytuacjach wystąpienia naruszenia ochrony danych osobowych. Choć nie zastępuje on standardowego, indywidualnego powiadomienia, w określonych przypadkach jest koniecznością. Kluczowe znaczenie ma jego forma, treść oraz kanał komunikacji – muszą być dostosowane do odbiorców i zapewniać realne dotarcie do osób poszkodowanych. Prawidłowe zastosowanie komunikatu publicznego, poparte dobrymi praktykami i odpowiednią dokumentacją, nie tylko ogranicza skutki incydentu, ale także zwiększa zaufanie do administratora danych. Dlatego jego opracowanie powinno być częścią szerszej strategii zarządzania incydentami w organizacjach przetwarzających dane osobowe.

FRANCUSKI ORGAN NADZORCZY NAKŁADA GRZYWNĘ W WYSOKOŚCI 80 TYSIĘCY EURO NA FIRMĘ CALOGA

Francuski odpowiednik polskiego Urzędu Ochrony Danych Osobowych (CNIL) nałożył na spółkę CALOGA karę za działalność komercyjną polegającą na pozyskiwaniu klientów bez ich zgody oraz przekazywanie ich danych partnerom bez ważnej podstawy prawnej.

Streszczenie decyzji

Początek sprawy

W związku z tym, że CNIL uznał komercyjne działania marketingowe za priorytetowy obszar kontroli w 2022 roku, skupił się na praktykach podmiotów działających w tym ekosystemie – w szczególności pośredników zajmujących się odsprzedażą danych, tzw. brokerów danych. Przeprowadził dochodzenie wobec firmy CALOGA, która pozyskiwała dane potencjalnych klientów głównie od innych brokerów danych, wydawców konkursów oraz stron testujących produkty (czyli tzw. pierwotnych zbieraczy danych). CALOGA wykorzystywała te dane do prowadzenia kampanii marketingowych drogą mailową w imieniu swoich klientów reklamowych. Część danych mogła być również przekazywana klientom, aby ci samodzielnie prowadzili działania marketingowe.

Kluczowe ustalenia

• **Brak uzyskania zgody na przesyłanie treści marketingowych drogą elektroniczną** (art. L.34-5 francuskiego Kodeksu Poczty i Komunikacji Elektronicznej (CPCE)): formularze stosowane przez brokerów danych były mylące, co uniemożliwiało uzyskanie dobrowolnej i jednoznacznej zgody według RODO – a to właśnie ona powinna stanowić podstawę działań marketingowych firmy.

• **Brak poszanowania prawa do wycofania zgody** (art. L.34-5 CPCE w odniesieniu do art. 7 RODO): system wdrożony przez CALOGA nie umożliwiał użytkownikom wypisania się z różnych baz danych firmy jednym kliknięciem. Wycofanie zgody było więc trudniejsze niż jej udzielenie.

• **Brak odpowiedniej podstawy prawnej do przetwarzania danych** (art. 6 RODO): jako broker danych, CALOGA przekazywała bazy danych innym partnerom, którzy prowadzili działania marketingowe w imieniu swoich klientów. Firma powoływała się na uzasadniony interes jako podstawę prawną, jednak zgodnie z przepisami wymagane było uzyskanie zgody osób, których dane dotyczyły – czego nie dokonano.

• **Brak określenia i przestrzegania proporcjonalnego okresu przechowywania danych** (art. 5 ust. 1 lit. e RODO): za każdym razem, gdy potencjalny klient otworzył wiadomość e-mail – nawet przypadkowo – firma przedłużała okres przechowywania jego danych w bazie, potencjalnie bez ograniczeń.

Decyzja

Na podstawie wyników kontroli, komisja dyscyplinarna CNIL – organ odpowiedzialny za nakładanie sankcji – uznała, że firma CALOGA naruszyła przepisy francuskiego Kodeksu Poczty i Komunikacji Elektronicznej (CPCE) oraz ogólnego rozporządzenia o ochronie danych (RODO).

Nałożyła na CALOGA grzywnę w wysokości 80 tysięcy euro i upubliczniła swoją decyzję. Wysokość kary uwzględniała m.in. dużą liczbę osób, których dane dotyczyły, długoletnią obecność firmy na rynku, korzyści finansowe wynikające z naruszeń oraz fakt, że firma zakończyła działalność w 2024 roku.

Źródło: komunikat francuskiego organu nadzorczego

fot. pexels

FEDERALNY NIEMIECKI ORGAN NADZORCZY NAKŁADA KARY ADMINISTRACYJNE W ŁĄCZNEJ WYSOKOŚCI 45 MILIONÓW EURO NA VODAFONE

Niemiecki organ nadzorczy (BfDI) nałożył kary na Vodafone za niewystarczający nadzór i procedury audytowe wobec agencji partnerskich, nieodpowiednie środki bezpieczeństwa dotyczące portalu usług online; dał również upomnienie za wykryte słabości w systemach informatycznych. Vodafone GmbH, poza usunięciem naruszeń, przekazał kilka milionów euro na rzecz organizacji zajmujących się promowaniem ochrony danych, umiejętności medialnych i kompetencji cyfrowych oraz zwalczaniem cyberprzemocy.

Streszczenie decyzji

Początek sprawy

Federalny niemiecki organ nadzorczy ds. ochrony danych wszczął postępowanie wyjaśniające wobec partnerów agencyjnych Vodafone GmbH oraz portalu usług online firmy po otrzymaniu zewnętrznych informacji, niezależnych od jakichkolwiek formalnych skarg.

Kluczowe ustalenia

Vodafone GmbH to dostawca usług telekomunikacyjnych działający na rynku niemieckim.
Firma korzysta z różnych kanałów dystrybucji, w tym z lokalnych punktów sprzedaży, z których część prowadzona jest przez agencje partnerskie. Działają one pod marką Vodafone i są zobowiązane do przestrzegania wytycznych firmy. Ich systemy informatyczne opierają się na sprzęcie i oprogramowaniu dostarczanym przez Vodafone. Przetwarzanie danych klientów regulowane jest umowami powierzenia przetwarzania danych.

W toku dochodzenia ujawniono braki w nadzorze i audycie procesorów danych oraz luki w systemach IT, które stwarzały ryzyko nadużyć danych klientów w celach oszustwa – ryzyko to w niektórych przypadkach się zmaterializowało.

Dodatkowo Vodafone oferuje klientom portal usług online. W połączeniu z infolinią firmy, niemiecki organ nadzorczy wykrył słabości w procesie uwierzytelniania kont użytkowników, które mogły

prowadzić do nadużyć związanych z kartami eSIM. Firma podjęła działania naprawcze w celu usunięcia stwierdzonych nieprawidłowości.

Decyzja

Federalny niemiecki organ nadzorczy nałożył grzywnę w wysokości 15 milionów euro za niewystarczający nadzór i procedury audytowe wobec agencji partnerskich oraz dodatkową grzywnę w wysokości 30 milionów euro za niewystarczające środki bezpieczeństwa dotyczące portalu usług online. Wydał też upomnienie za wykryte słabości w systemach informatycznych.

Na uwagę zasługuje fakt, że Vodafone GmbH nie tylko usunął naruszenia, ale też przekazał kilka milionów euro na rzecz organizacji zajmujących się promowaniem ochrony danych, umiejętności medialnych i kompetencji cyfrowych oraz zwalczaniem cyberprzemocy (po uprzednim uzgodnieniu beneficjentów oraz wysokości przekazywanych darowizn z organem nadzorczym). Spółka w pełni współpracowała z organem dostarczając dowodów, których organ nie pozyskałby samodzielnie, a które były dla niej obciążające – które to okoliczności organ poczytał na korzyść spółki, odpowiednio zmniejszając karę. Spółka uiściła nałożone kary w całości.

Źródło: komunikat Europejskiej Rady Ochrony Danych oraz notatka grupy Fining Taskforce

fot. pexels

FIŃSKI ORGAN NADZORCZY NAKŁADA KARĘ NA APTEKĘ ZA UCHYBIENIA W OCHRONIE DANYCH W SKLEPIE INTERNETOWYM

Fiński odpowiednik UODO nałożył karę administracyjną w wysokości 1,1 miliona euro na Yliopiston Apteekki z powodu nieprawidłowości w zakresie ochrony danych osobowych wykrytych w jej sklepie internetowym, związanych z korzystaniem z usług śledzenia. Dane dotyczące korzystania przez klientów ze sklepu internetowego wyciekły do firm świadczących usługi śledzenia za pośrednictwem narzędzi analitycznych i technologii śledzenia dostępnych na stronie internetowej.

Streszczenie decyzji

Początek sprawy

Fiński organ nadzorczy ds. ochrony danych osobowych (Data Protection Ombudsman) rozpoczął dochodzenie w sprawie praktyk Yliopiston Apteekki po tym, jak doktorant z Uniwersytetu w Turku skontaktował się z urzędem. W ramach badań nad funkcjonowaniem internetowych usług zdrowotnych, badacz przeanalizował ruch sieciowy i wykrył braki w zakresie ochrony danych w fińskich aptekach internetowych. Fiński organ prowadzi obecnie podobne postępowania wobec innych aptek internetowych.

Kluczowe ustalenia

Yliopiston Apteekki wykorzystywała pliki cookie i inne technologie śledzące w swoim sklepie internetowym w sposób, który powodował przekazywanie danych o interakcjach użytkowników – dotyczących m.in. leków na receptę i bez recepty – bezpośrednio do firm takich jak Google i Meta. Przykładowo, dostawcy usług śledzących otrzymywali informacje o tym, kiedy klient dodał produkt do koszyka lub kliknął przycisk zakupu.

Przekazywane dane obejmowały również adresy IP użytkowników oraz inne dane identyfikujące, które mogły posłużyć do jednoznacznego rozpoznania osoby. Jeśli użytkownik był zalogowany na swoje konto Google lub Facebook w czasie korzystania z apteki internetowej, Google i Meta mogły go bezpośrednio zidentyfikować.

Decyzja

Fiński organ stwierdził, że firma naruszyła artykuły 32 oraz 5 ust. 1 lit. f RODO. Nałożył na Yliopiston Apteekki administracyjną karę pieniężną w wysokości 1,1 miliona euro. Dodatkowo wydał ostrzeżenie, ponieważ firma nie zapewniła odpowiedniego poziomu bezpieczeństwa danych osobowych generowanych i gromadzonych w związku z korzystaniem z apteki internetowej.

Postępowanie dotyczyło praktyk stosowanych przez aptekę w okresie od maja 2018 r. do września 2022 r. Firma poinformowała, że zaprzestała korzystania z technologii śledzących Google i Meta we wrześniu 2022 r. Fiński organ udzielił również wskazówek dotyczących pozostałych technologii śledzących, które apteka nadal stosuje.

Źródło: komunikat fińskiego organu nadzorczego

fot. pexels

NORWESKI ORGAN NADZORCZY NAKŁADA KARY ZA NIEZGODNE Z PRAWEM UDOSTĘPNIANIE DANYCH OSOBOWYCH ZA POMOCĄ PIKSELI ŚLEDZĄCYCH

Norweski Urząd Ochrony Danych Osobowych (Datatilsynet) po przeprowadzonej kontroli sześciu stron internetowych korzystających z technologii pikseli śledzących, stwierdził, że wszystkie niezgodnie z prawem udostępniały dane osobowe użytkowników stronom trzecim.

Streszczenie decyzji

Początek sprawy

Norweski Urząd Ochrony Danych Osobowych (Datatilsynet) przeprowadził kontrolę sześciu stron internetowych korzystających z technologii pikseli śledzących. Celem inspekcji było przede wszystkim zwiększenie świadomości na temat stosowania tych narzędzi na stronach internetowych.

Piksele śledzące to technologia, która automatycznie przesyła informacje o osobach odwiedzających stronę lub aplikację do podmiotów trzecich. Może obejmować dane o odwiedzanych podstronach, podejmowanych działaniach czy dodanych produktach do koszyka.

Kluczowe ustalenia

Urząd uznał, że wszystkie sześć stron objętych kontrolą niezgodnie z prawem udostępniało dane osobowe użytkowników stronom trzecim. Norweski organ nadzorczy stwierdził również naruszenia obowiązku informacyjnego wobec użytkowników. W kilku przypadkach przekazywane dane miały charakter wrażliwy.

Decyzja

W jednej ze spraw Datatilsynet nałożył grzywnę administracyjną w wysokości około 22 tysięcy euro. W pozostałych przypadkach wydał upomnienia.

Źródło: komunikat norweskiego organu nadzorczego

33. EUROPEJSKA KONFERENCJA ORGANÓW OCHRONY DANYCH OSOBOWYCH – SPRING CONFERENCE 2025, BATUMI, GRUZJA

W dniach 6–9 maja 2025 roku w Batumi odbyła się 33. Europejska Konferencja Organów Ochrony Danych Osobowych – Spring Conference 2025. Organizowana przez Personal Data Protection Service of Georgia konferencja zgromadziła przedstawicieli europejskich i międzynarodowych organów ochrony danych osobowych, ekspertów, specjalistów ze środowisk naukowych oraz instytucji publicznych i prywatnych, by wspólnie analizować aktualne wyzwania i kierunki rozwoju w zakresie ochrony danych w kontekście globalnej transformacji cyfrowej.

W liście powitalnym do uczestników, prezes gruzińskiego organu nadzorczego, dr Lela Janashvili, podkreśliła wagę międzynarodowej współpracy, wymiany najlepszych praktyk i podnoszenia kultury ochrony danych osobowych. W obliczu przyspieszonego postępu technologicznego i coraz szerszego wykorzystania sztucznej inteligencji, rola organów nadzorczych staje się kluczowa dla zagwarantowania poszanowania praw jednostki.

Program merytoryczny konferencji obejmował szereg debat panelowych poświęconych najbardziej aktualnym zagadnieniom w obszarze ochrony danych osobowych:

Panel I: Innovation Under Regulation – dyskusja koncentrowała się na powiązaniach pomiędzy krajowymi regulacjami dotyczącymi ochrony danych, rozporządzeniem UE o sztucznej inteligencji (AI Act) oraz Ramową Konwencją Rady Europy w sprawie AI, praw człowieka, demokracji i rządów prawa. Paneliści analizowali, jak prawo może skutecznie chronić prywatność w środowiskach opartych na AI.

Panel II: From Playrooms to Platforms – panel poświęcony był ochronie prywatności dzieci w środowisku cyfrowym, w szczególności w kontekście narzędzi edukacyjnych, platform rozrywkowych oraz technologii opartych na AI.

Panel III: The Pulse of Privacy – omówiono wyzwania związane z ochroną danych zdrowotnych, w tym przepływem danych transgranicznych, odpowiedzialnością dostawców usług medycznych i firm technologicznych oraz potrzebą pogodzenia innowacji z ochroną praw jednostki.

Panel IV: Evolving Roles of DPOs and Privacy Professionals – dyskusja dotyczyła zmieniającej się roli inspektorów ochrony danych (Data Protection Officer – DPO) oraz specjalistów ds. prywatności w kontekście nowych regulacji i wyzwań technologicznych.

Panel V: Small DPAs Against Big Cases – panel skupił się na działaniach mniejszych organów nadzorczych w sprawach wymagających dużych zasobów, podkreślając znaczenie strategii, determinacji oraz współpracy międzynarodowej przy dochodzeniu praw osób fizycznych wobec globalnych podmiotów.

Panel VI: United for Data Protection – eksperci dyskutowali o roli edukacji i świadomości społecznej w budowaniu kultury ochrony danych oraz o znaczeniu współpracy między organami nadzorczymi, organizacjami międzynarodowymi i sektorem prywatnym.

Panel VII: Other Activities – podczas tej części konferencji przyjęto końcową rezolucję, zaprezentowano raport roczny Grupy Sterującej Spring Conference, przedstawiono gospodarza European Case Handling Workshop 2024 oraz zapowiedź ECHW i Spring Conference w 2026 roku.

Panel VIII: Legal vs. Ethical AI – panel poświęcony był złożonym relacjom pomiędzy wymogami prawnymi a odpowiedzialnością etyczną w procesie projektowania i wdrażania systemów AI.

Panel IX: Privacy-Enhancing Technologies – analizie poddano zastosowanie technologii wzmacniających prywatność (PETs), ich rolę w udostępnianiu danych w sposób zgodny z przepisami, jak również ich wykorzystanie w inteligentnych miastach i systemach AI.

Wydarzenia towarzyszące

Data Protection in Georgia – Challenges and Opportunities – przedstawiciele gruzińskiego organu ochrony danych osobowych zaprezentowali nowe regulacje krajowe, najnowsze inicjatywy edukacyjne oraz międzynarodowe partnerstwa, podkreślając aktywną rolę Gruzji w europejskim systemie ochrony prywatności.

Fundamental Rights Impact Assessment in AI – The Catalan FRIA Model Template – Kataloński organ nadzorczy (APDCAT) zaprezentował model szacowania wpływu sztucznej inteligencji na prawa podstawowe (FRIA – fundamental rights impact assessment), będący odpowiedzią na wymagania regulacyjne AI Act. Model ten został opracowany z udziałem sektora publicznego i prywatnego i wykorzystywany jest w praktyce w analizie wysokiego ryzyka zastosowań AI.

5 SPRAWY MIĘDZYNARODOWE

Konferencja w Batumi potwierdziła rosnącą wagę współpracy europejskiej i globalnej w tworzeniu zrównoważonego systemu ochrony danych osobowych. Wymiana doświadczeń, omówienie kluczowych wyzwań regulacyjnych oraz wspólna refleksja nad przyszłością prywatności cyfrowej stanowią istotny wkład w dalszy rozwój tej dziedziny.

W wydarzeniu uczestniczyły przedstawicielki Urzędu Ochrony Danych Osobowych: zastępczyni prezesa UODO, Agnieszka Grzelak, oraz dyrektorka Departamentu Współpracy Międzynarodowej, Maria Owczarek.

Źródło: komunikat gruzińskiego organu nadzorczego

fot. pexels

META DESIGN JAM – GENERATYWNA SZTUCZNA INTELIGENCJA, TRANSPARENTNOŚĆ I KONTROLA. SPOTKANIE EKSPERCKIE W BERLINIE

12 maja 2025 r. w siedzibie firmy Meta w Berlinie odbyło się eksperckie spotkanie pn. Meta Design Jam, poświęcone najnowszym osiągnięciom w zakresie generatywnej sztucznej inteligencji (GenAI) oraz prognozom dotyczącym kluczowych trendów technologicznych na najbliższe miesiące. Organizatorem wydarzenia był zespół Meta Trust, Transparency & Control Labs, a uczestnikami byli przedstawiciele środowisk naukowych, administracji publicznej, organizacji społecznych, prawnicy, inspektorzy ochrony danych oraz reprezentanci organów nadzorczych z Polski i Niemiec.

Celem spotkania było zaprezentowanie rozwiązań technologicznych opracowywanych przez Meta oraz zebranie opinii uczestników na temat oczekiwanych standardów przejrzystości i kontroli w usługach opartych na AI.

Kluczowe elementy warsztatów

I. Interaktywne ćwiczenia z funkcjonalności GenAI

Warsztaty rozpoczęto od prezentacji funkcji rozwijanych przez Meta, w tym personalizowanych asystentów AI, zdolnych do zapamiętywania informacji oraz wykorzystywania danych użytkownika w celu generowania kontekstowych rekomendacji. Przedstawiono również ewolucję interfejsów komputerowych – od klawiatury, poprzez ekrany dotykowe, po obsługę głosową.

Podczas ćwiczeń zwracano uwagę na różnice językowe i znaczeniowe w postrzeganiu usług cyfrowych przez użytkowników. Wskazano też na oczekiwania dotyczące personalizacji usług, przy jednoczesnym wyrażaniu obaw związanych z przejrzystością, możliwością nadużyć i trudnością w zrozumieniu zasad przetwarzania danych.

II. Analiza scenariuszy i zastosowań AI

W drugiej części spotkania zaprezentowano trzy scenariusze dotyczące wykorzystania AI w obszarach zdrowia, edukacji oraz wsparcia psychicznego. Szczególnie interesujące były rozwiązania wspierające proces edukacyjny – umożliwiające integrację z systemami uczelni, planowanie spotkań z nauczycielami, sugerowanie strategii uczenia się i technik poprawiających efektywność nauki.

Formuła tej części miała charakter konsultacyjny – przedstawiane koncepcje zestawiano z doświadczeniami uczestników, aby lepiej zrozumieć ich oczekiwania wobec przyszłych narzędzi AI.

III. Transparentność i kontrola użytkownika

Ostatni blok poświęcono rozwiązaniom służącym informowaniu użytkowników o zasadach przetwarzania danych w aplikacjach mobilnych. Uczestnicy oceniali przedstawione projekty w czterech kategoriach: świadomość, wartość, sprawczość oraz zaufanie. Wśród testowanych funkcji znalazły się m.in. planowanie spotkań, tryb prywatny (bez zapamiętywania preferencji), możliwość usuwania treści, dostęp do polityki prywatności i jej wyjaśnianie z pomocą pytań pomocniczych.

Zaprezentowane rozwiązania stawały się coraz bardziej zaawansowane, odpowiadając na zgłaszane przez uczestników potrzeby i wątpliwości. Zebrane opinie zostaną opublikowane na stronie TTC Labs, a organizatorzy zadeklarowali chęć utrzymania kontaktu z uczestnikami spotkania.

Wnioski i dalsze działania

Z perspektywy uczestników spotkanie stanowiło istotny sygnał transparentności podejmowanych przez Meta działań oraz próbę wdrożenia uwag regulatorów do projektowanych rozwiązań. Uczestnicy podkreślali również potencjał zacieśnienia współpracy w zakresie oceny i konsultowania przyszłych rozwiązań z zakresu przetwarzania danych.

W spotkaniu uczestniczył przedstawiciel Urzędu Ochrony Danych Osobowych, Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej.

PRIVACY SYMPOSIUM 2025 – MIĘDZYNARODOWA WYMIANA WIEDZY I DOŚWIADCZEŃ W WENECJI

W dniach 12–16 maja 2025 r. w Wenecji odbyła się kolejna edycja międzynarodowej konferencji Privacy Symposium, organizowanej przez Uniwersytet Ca' Foscari oraz partnerów instytucjonalnych i akademickich z całej Europy. W wydarzeniu uczestniczył prezes Urzędu Ochrony Danych Osobowych, Mirosław Wróblewski, który reprezentował Polskę w gronie ponad 300 prelegentów i ekspertów z zakresu ochrony danych osobowych, prawa, technologii i etyki.

Konferencja stanowiła platformę wymiany wiedzy, doświadczeń i dobrych praktyk w zakresie ochrony prywatności i zgodności z przepisami prawa w dobie dynamicznych zmian technologicznych. Jej celem było wsparcie międzynarodowego dialogu, współpracy i konwergencji regulacyjnej w obszarze ochrony danych.

Program konferencji obejmował ponad 100 sesji tematycznych, podzielonych na kilkanaście ścieżek merytorycznych, w tym:

• **Artificial Intelligence and Compliance** – poświęcona wyzwaniom regulacyjnym związanym z rozwojem sztucznej inteligencji, w tym kwestiom przejrzystości, odpowiedzialności i bezpieczeństwa systemów AI.

• **International Cooperation** – dotycząca współpracy transgranicznej i harmonizacji standardów ochrony danych na poziomie międzynarodowym.

• **Technology and Compliance** – analizująca wpływ nowych technologii, takich jak blockchain, metaverse czy komputery kwantowe, na zgodność z przepisami o ochronie danych.

• **Health and Medical Data Compliance** – skupiająca się na przetwarzaniu danych medycznych, wtórnym wykorzystaniu danych w badaniach oraz transferach międzynarodowych.

• **Accountability, Trust, and Privacy Enhancing Technologies (PET)** – omawiająca narzędzia wspierające ochronę danych, w tym anonimizację, pseudonimizację i certyfikację.

• **Socio-Economic Perspective** – poświęcona społecznym i gospodarczym aspektom ochrony danych oraz ich wpływowi na codzienne życie obywateli.

• **Philosophy of Privacy** – eksplorująca filozoficzne podstawy prawa do prywatności i jego znaczenie dla godności i autonomii jednostki.

W ramach konferencji odbyły się również sesje naukowe, warsztaty praktyczne dla inspektorów ochrony danych oraz panele poświęcone wdrażaniu przepisów w praktyce.

Prezes UODO uczestniczył jako prelegent w panelu poświęconym kryptografii postkwantowej (post-quantum cryptography). Uczestnicy sesji analizowali, w jaki sposób nowe podejścia do kryptografii mogą wzmocnić strategie ochrony danych oraz zabezpieczyć infrastrukturę cyfrową wobec zagrożeń związanych z rozwojem technologii kwantowych.

W ramach dyskusji poruszono m.in. kwestie:

• jak kryptografia postkwantowa może zapewnić bezpieczeństwo danych w długoterminowej perspektywie;

• jak oceniać trwałość i skuteczność rozwiązań kryptograficznych w kontekście ewolucji technologii kwantowej;

• jakie nowe możliwości dla ochrony danych i bezpieczeństwa cyfrowego niesie rozwój kryptografii odpornych na komputery kwantowe.

Udział w sesji był okazją do przedstawienia perspektywy regulacyjnej w kontekście przyszłościowych wyzwań technologicznych oraz do zaprezentowania podejścia polskiego organu do kwestii bezpieczeństwa danych w zmieniającym się środowisku cyfrowym.

Źródło: strona internetowa Privacy Symposium

CERTYFIKACJA W PRAKTYCE – WARSZTATY CEH W BERLINIE

W dniach 11–13 czerwca 2025 r. w Berlinie odbyły się warsztaty certyfikacyjne zorganizowane przez podgrupę ds. zgodności, zdrowia i eAdministracji (CEH). Gospodarzem wydarzenia był berliński organ nadzorczy (BfID), a w spotkaniu uczestniczyli przedstawiciele europejskich organów nadzorczych, jednostek akredytujących oraz właściciele mechanizmów certyfikacji. W wydarzeniu wzięły udział również przedstawicielki Urzędu Ochrony Danych Osobowych.

Certyfikacja jako sygnał odpowiedzialności

Warsztaty otworzyli przedstawiciele niemieckich organów nadzorczych: Komisarz Andreas Hartl, Marit Hansen oraz Bettina Gayk. Podkreślali oni znaczenie certyfikacji jako narzędzia budującego zaufanie i zapewniającego wysoki standard ochrony danych w erze cyfrowej. Certyfikacja została wskazana jako kluczowy element wykazywania zgodności z RODO.

Współpraca z jednostkami akredytującymi

Pierwszy panel poświęcono współpracy z krajowymi jednostkami akredytującymi. Przedstawiciele European Accreditation (EA) oraz Accredia omówili procesy akredytacyjne, różnice między certyfikacją obowiązkową a dobrowolną oraz wyzwania związane z walidacją certyfikatów. Szczególną uwagę poświęcono współpracy między organami nadzorczymi a jednostkami akredytującymi – zarówno w zakresie formalnym, jak i praktycznym.

Perspektywa właścicieli mechanizmów certyfikacji

W kolejnych sesjach głos zabrali właściciele mechanizmów certyfikacji, m.in. Europrivacy, Brand Compliance oraz Datenschutzcert. Wskazywali na rosnące zainteresowanie certyfikacją, zwłaszcza wśród dużych organizacji, ale także na bariery, z jakimi mierzą się mniejsze podmioty – wysokie koszty, czasochłonność procesu oraz niska świadomość korzyści płynących z certyfikacji.

Wyzwania i dobre praktyki

Dyskutowano również o problemie tzw. „certyfikatów ochrony danych" niezwiązanych z RODO, które mogą wprowadzać w błąd i podważać zaufanie do certyfikacji zgodnej z rozporządzeniem.

5 SPRAWY MIĘDZYNARODOWE

Wskazano na potrzebę tworzenia pakietów certyfikacyjnych obejmujących różne akty prawne oraz na znaczenie przejrzystości i współpracy między interesariuszami od najwcześniejszych etapów procesu.

W stronę dojrzałego rynku certyfikacji

Zwieńczeniem pierwszego dnia była dyskusja właścicieli mechanizmów certyfikacji, którzy zgodnie podkreślali potrzebę dalszego rozwoju rynku, zwiększenia liczby podmiotów certyfikujących oraz dostosowania mechanizmów do potrzeb MŚP. Wskazali również na konieczność przyjęcia szerszej, globalnej perspektywy w ocenie skuteczności certyfikacji jako narzędzia zgodności.

Udział UODO w warsztatach CEH wpisuje się w działania Urzędu na rzecz wspierania skutecznych i transparentnych mechanizmów zgodności z RODO oraz aktywnego uczestnictwa w europejskich inicjatywach w zakresie certyfikacji.

fot. pexels

HUDERIA ACADEMY – SZKOLENIE RADY EUROPY W ZAKRESIE OCENY RYZYKA I WPŁYWU SYSTEMÓW AI, STRASBURG

W dniach 16–18 czerwca 2025 r. w siedzibie Rady Europy w Strasburgu odbyła się pierwsza edycja HUDERIA Academy – intensywnego szkolenia poświęconego praktycznemu stosowaniu metodyki oceny wpływu systemów sztucznej inteligencji na prawa człowieka, demokrację i rządy prawa (HUDERIA). Wydarzenie zorganizowano z inicjatywy Komitetu ds. Sztucznej Inteligencji Rady Europy (CAI), przy wsparciu Instytutu Alana Turinga. W szkoleniu uczestniczył przedstawiciel Urzędu Ochrony Danych Osobowych – Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej.

Cel i znaczenie HUDERIA Academy

HUDERIA (Human Rights, Democracy and the Rule of Law Impact Assessment) to metodyka opracowana przez CAI jako narzędzie wspierające wdrażanie Ramowej Konwencji Rady Europy w sprawie sztucznej inteligencji. Jej celem jest zapewnienie, aby systemy AI były projektowane, wdrażane i nadzorowane w sposób zgodny z podstawowymi wartościami demokratycznymi. Szkolenie miało na celu wyposażenie przedstawicieli administracji publicznej, organów nadzorczych i ekspertów w wiedzę i umiejętności niezbędne do stosowania HUDERIA w praktyce.

Program i przebieg szkolenia

W trzydniowym programie uczestniczyło ponad 80 osób z całego świata, reprezentujących różne sektory i instytucje. Zajęcia odbywały się w formie warsztatów, prezentacji eksperckich i interaktywnych ćwiczeń, obejmujących m.in.:

- **Wprowadzenie do HUDERIA i jej genezy** – z udziałem przewodniczącego CAI, Mario Hernándeza Ramosa, oraz przedstawicieli Sekretariatu Rady Europy;
- **Podstawy techniczne AI i wyzwania związane z dużymi modelami językowymi (LLM)** – prezentacja dr Murielle Popa-Fabre;
- **Ewolucja HUDERIA i jej powiązania z AI Act oraz RODO** – sesja prowadzona przez dr Davida Leslie z Instytutu Alana Turinga;

• **Zastosowanie analizy kontekstowej COBRA i oceny wpływu (RIA)** – analiza przypadków, w tym skutków dla godności ludzkiej, grup wrażliwych i pracowników sektora publicznego;

• **Zastosowanie narzędzi dydaktycznych, takich jak MIRO**, do wspólnego opracowywania scenariuszy i dokumentacji.

W trakcie sesji poruszano również kwestie adaptacji HUDERIA do wymogów unijnego AI Act, integracji z krajowymi mechanizmami oceny ryzyka oraz możliwości współpracy między organami krajowymi.

HUDERIA stanowi zaawansowane i kompletne narzędzie wspierające odpowiedzialne zarządzanie AI. Wskazywano na potrzebę unikania podejścia silosowego w tworzeniu krajowych mechanizmów oceny ryzyka oraz na potencjał HUDERIA jako wspólnego punktu odniesienia. Zwrócono również uwagę na konieczność dalszego rozwijania modułów sektorowych i konsultacji z organami krajowymi.

fot. zasoby własne UODO

5 SPRAWY MIĘDZYNARODOWE

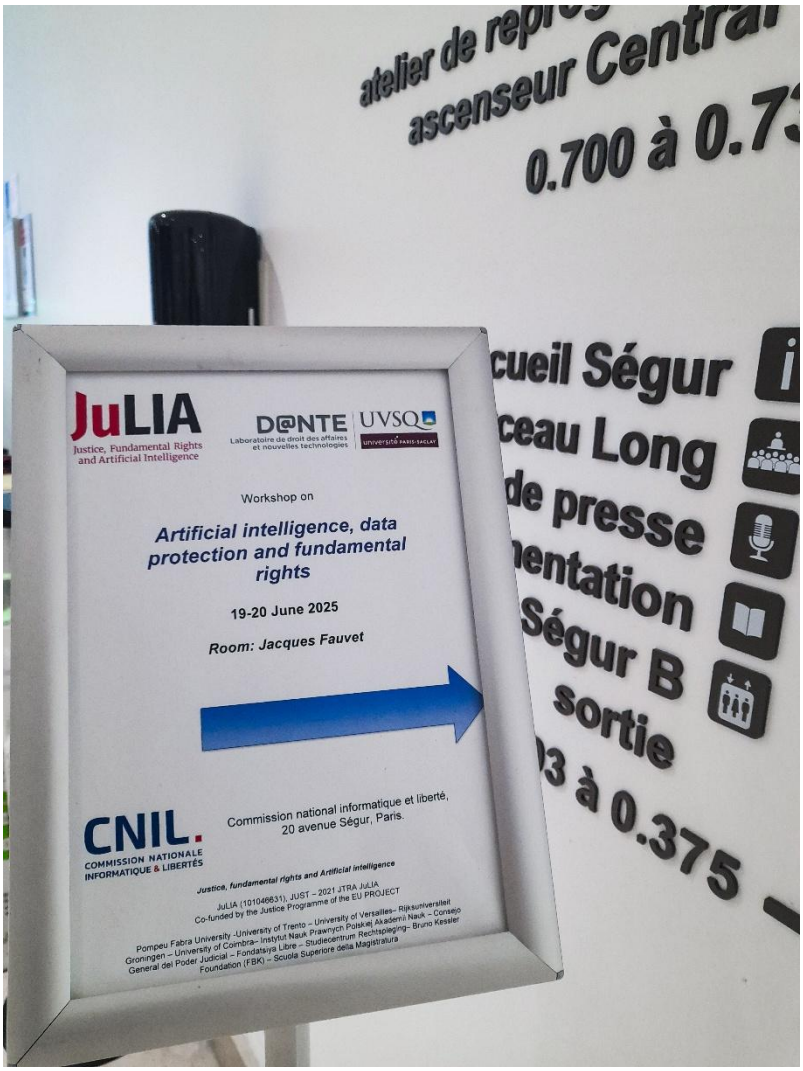
Zgodnie z zapowiedziami CAI, ostateczna wersja metodyki HUDERIA może zostać przyjęta jesienią 2025 r. lub wiosną 2026 r. Jej wdrożenie będzie stanowić istotny krok w kierunku zapewnienia, że rozwój sztucznej inteligencji w Europie odbywa się z poszanowaniem praw człowieka i zasad demokratycznych.

Udział UODO w HUDERIA Academy wpisuje się w działania Urzędu na rzecz aktywnego uczestnictwa w międzynarodowych inicjatywach dotyczących odpowiedzialnego rozwoju technologii oraz wzmacniania kompetencji w zakresie oceny ryzyka i wpływu systemów AI. W wydarzeniu wzięła udział Maria Owczarek, dyrektorka Departamentu Współpracy Międzynarodowej.

fot. zasoby własne UODO

SZTUCZNA INTELIGENCJA, OCHRONA DANYCH I PRAWA PODSTAWOWE – SEMINARIUM W PARYŻU

W dniach 19–20 czerwca 2025 r. w siedzibie francuskiego organu ochrony danych osobowych (CNIL) w Paryżu odbyło się międzynarodowe seminarium pt. Artificial intelligence, data protection and fundamental rights, zorganizowane w ramach projektu JuLIA (Justice, fundamental rights and Artificial Intelligence). W wydarzeniu uczestniczył przedstawiciel Urzędu Ochrony Danych Osobowych, Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej.



fot. zasoby własne UODO

Celem spotkania było omówienie wyzwań i ryzyk związanych z wykorzystaniem systemów sztucznej inteligencji w kontekście ochrony danych osobowych i praw podstawowych, zarówno na etapie pozyskiwania danych (incoming data), jak i ich przetwarzania oraz wykorzystywania (outgoing data).

Główne zagadnienia i przebieg seminarium

Seminarium otworzyli przedstawiciele CNIL oraz partnerzy akademiccy projektu JuLIA. W wystąpieniu inauguracyjnym Sekretarz Generalny CNIL, Vincent Villette, przedstawił dane dotyczące działalności organu w 2024 r.: 17 tysięcy skarg, 321 kontroli, 180 nakazów i 87 sankcji na łączną kwotę ponad 55 mln euro. Wskazał również trzy kluczowe obszary ryzyka w kontekście AI: przejrzystość i informowanie użytkowników, delegowanie decyzji systemom AI oraz bezpieczeństwo systemów (w tym zagrożenia typu data poisoning).

W dalszej części dnia omówiono m.in.:

• **Zbieranie danych dla systemów AI** – w tym zagadnienia związane z pseudonimizacją orzeczeń sądowych i polityką otwartych danych;

• **Zastosowanie AI w sądownictwie** – z udziałem przedstawicieli UNESCO, francuskiego Ministerstwa Spraw Wewnętrznych oraz hiszpańskiego sędziego Jose Marii Fernándeza Seijo;

• **Warsztaty Justice Lab** – praca w grupach nad praktycznymi scenariuszami;

• **Panel nt. egzekwowania prawa** – z udziałem przedstawicieli organów ochrony danych z Francji, Włoch i Polski, w tym Krzysztofa Króla z UODO;

• **Anonimizacja i pseudonimizacja dokumentów sądowych** – prezentacja narzędzi wykorzystywanych we Francji i Hiszpanii, w tym systemu KENDOJ analizującego powiązania między orzeczeniami.

Drugi dzień poświęcono zagadnieniom związanym z tzw. outgoing data, czyli wynikami przetwarzania danych przez systemy AI. W programie znalazły się m.in.:

• **Panel nt. roszczeń zbiorowych i strategii procesowych** – z udziałem ekspertów z Hiszpanii i Francji;

• **Kolejna sesja Justice Lab** – kontynuacja pracy grupowej;

• **Wystąpienie końcowe** – wygłoszone przez Alexandre'a Lépine'a z Europejskiej Rady Ochrony Danych.

Seminarium w Paryżu stanowiło istotne forum wymiany doświadczeń między przedstawicielami organów nadzorczych, środowisk akademickich i praktyków prawa. Szczególną wartość miały dyskusje dotyczące praktycznego stosowania narzędzi AI w wymiarze sprawiedliwości oraz wyzwań związanych z zapewnieniem przejrzystości i poszanowania praw jednostki w zautomatyzowanych procesach decyzyjnych.

Udział przedstawiciela UODO w panelu poświęconym egzekwowaniu prawa był okazją do zaprezentowania polskiej perspektywy oraz do nawiązania kontaktów z partnerami z innych państw członkowskich UE. Wydarzenie wpisuje się w działania Urzędu na rzecz aktywnego uczestnictwa w międzynarodowej debacie o odpowiedzialnym rozwoju sztucznej inteligencji i ochronie danych osobowych.

Źródło: strona internetowa Justice, Fundemental Rights and Artificial Inteligence (JULIA)

SPRAWOZDANIE ZE SKOORDYNOWANEGO NADZORU NAD WIZOWYM SYSTEMEM INFORMACYJNYM

Grupa ds. Koordynacji Nadzoru nad Wizowym Systemem Informacyjnym (VIS SCG) przyjęła sprawozdanie podsumowujące półtoraroczną działalność prowadzoną w okresie od początku 2023 r. do września 2024 r.

Czym jest VIS

Wizowy System Informacyjny (VIS), służący wymianie danych wizowych między państwami członkowskimi, został utworzony decyzją Rady 2004/512/WE z dnia 8 czerwca 2004 r. i uzupełniony rozporządzeniem 2008/767/WE. W 2021 r. system poddano reformie – przyjęto rozporządzenia (UE) 2021/1134 i 2021/1133, umożliwiające m.in. powiązania z innymi bazami danych UE.

Grupa ds. Koordynacji Nadzoru nad VIS (VIS SCG), złożona z przedstawicieli krajowych organów ochrony danych oraz Europejskiego Inspektora Ochrony Danych (EIOD), została powołana na mocy rozporządzenia w celu zapewnienia spójnego nadzoru nad VIS. Członkowie Grupy regularnie wymieniają się doświadczeniami i najlepszymi praktykami, analizują wyzwania nadzorcze oraz szukają wspólnych rozwiązań.

Spotkania Grupy VIS SCG

W sprawozdawczym okresie (tj.od stycznia 2023 r. do września 2024 r.) odbyły się trzy spotkania Grupy. Każde z nich składało się z dwóch części:

• Pierwsza poświęcona była prezentacjom Komisji Europejskiej i agencji eu-LISA, odpowiadającej za zarządzanie operacyjne systemami SIS, VIS oraz Eurodac. Podczas tej części spotkania KE i eu-LISA przedstawiły najnowsze zmiany w zakresie funkcjonowania Wizowego Systemu Informacyjnego (VIS) mające wpływ na ochronę danych osobowych. Dzięki temu członkowie Grupy mieli zapewniony bieżący dostęp do kluczowych informacji umożliwiających skuteczny nadzór.

• Druga część spotkań skoncentrowała się na wymianie doświadczeń i dyskusjach między organami ochrony danych. Omówiono kwestie wymagające działań na poziomie krajowym oraz nowe zmiany prawne i technologiczne budzące zainteresowanie organów nadzorczych VIS.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Główne obszary działalności Grupy VIS SCG

Monitorowanie wdrażania zmienionego rozporządzenia w sprawie VIS

Grupa regularnie zapraszała przedstawicieli Komisji Europejskiej, by informowali o postępach we wdrażaniu zreformowanego rozporządzenia w sprawie VIS. Szczególną uwagę poświęcono:

• pobieraniu odcisków palców od dzieci,

• dostępowi organów ścigania do danych,

• rozszerzeniu systemu na wizy długoterminowe i dokumenty pobytowe,

• strukturze nadzoru nad systemem.

Przegląd cyfryzacji procedury wizowej

27 kwietnia 2022 r. Komisja Europejska przedstawiła projekt reformy w zakresie cyfryzacji procedury wizowej. Jej celem jest:

• uproszczenie procesu składania wniosków wizowych poprzez utworzenie unijnej platformy,

• cyfryzacja naklejki wizowej oraz procedur aplikacyjnych,

• podniesienie poziomu bezpieczeństwa strefy Schengen.

Niektóre grupy wnioskodawców – m.in. osoby aplikujące po raz pierwszy – nadal będą zobowiązane do osobistej wizyty w konsulacie lub centrum wizowym w celu identyfikacji i pobrania danych biometrycznych. Nowa platforma ma automatycznie określać państwo członkowskie właściwe do rozpatrzenia wniosku.

VIS SCG przeanalizowała projekt i zwróciła się do Komisji o bieżące informowanie o dalszych etapach prac legislacyjnych.

Przegląd mechanizmu oceny Schengen

Z dniem 1 października 2022 r. weszło w życie nowe rozporządzenie w sprawie mechanizmu oceny i monitorowania dorobku Schengen. Jest ono częścią szerszej reformy systemu Schengen, obejmującej m.in. nową strategię jego rozwoju oraz planowaną zmianę kodeksu granicznego.

W ramach działań nadzorczych Grupa VIS SCG omówiła z Komisją Europejską doświadczenia wynikające z Ewaluacji Schengen prowadzonej według nowych zasad, w szczególności w kontekście ochrony danych i możliwych skutków dla nadzoru nad przetwarzaniem danych w VIS.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Wspólny plan inspekcji VIS

VIS SCG przyjęła wspólny plan inspekcji, który ma wspierać krajowe organy ochrony danych w realizacji ich zadań kontrolnych. Dokument przewiduje:

• ujednolicone podejście do kontroli w państwach członkowskich,

• elastyczność dostosowaną do struktur federalnych i krajowych procedur,

• możliwość porównywania wyników inspekcji na poziomie europejskim.

Sprawozdanie w sprawie wcześniejszego usuwania danych z VIS

VIS przewiduje automatyczne usuwanie danych po upływie ustawowych okresów ich przechowywania. Jednak na poziomie krajowym stwierdzono nieprawidłowości w zakresie wcześniejszego usuwania danych w odniesieniu do osób ubiegających się o wizę, które uzyskały obywatelstwo państwa członkowskiego.

W celu zbadania tego zagadnienia VIS SCG przyjęła w czerwcu 2021 r. kwestionariusz skierowany do organów krajowych i organów ochrony danych. Odpowiedzi udzieliło 26 państw. Na tej podstawie w listopadzie 2023 r. sporządzono sprawozdanie zawierające główne wnioski i zalecenia.

Zmiany w modelu skoordynowanego nadzoru

Na mocy rozporządzenia (UE) 2021/1134, które zmienia m.in. rozporządzenie (WE) nr 767/2008, nadzór nad VIS ma być obecnie prowadzony w ramach Europejskiej Rady Ochrony Danych (EROD), a dokładniej – Komitetu Skoordynowanego Nadzoru (CSC).

Dotychczas mechanizm ten był obsługiwany przez Europejskiego Inspektora Ochrony Danych. Przyszłe działania VIS SCG będą prowadzone zgodnie z art. 62 rozporządzenia (UE) 2018/1725 (EUDPR), który przewiduje zharmonizowany model skoordynowanego nadzoru nad wielkoskalowymi systemami informacyjnymi UE.

Zgodnie z tym przepisem EIOD i krajowe organy nadzorcze muszą współpracować w ramach EROD, by skutecznie realizować zadania nadzorcze nad systemami informatycznymi UE.

Treść sprawozdania VIS SCG, wraz ze sprawozdaniami krajowymi, dostępna jest na stronie EROD.

DOŁĄCZ DO XVI EDYCJI PROGRAMU „TWOJE DANE – TWOJA SPRAWA”!

Już we wrześniu Prezes Urzędu Ochrony Danych Osobowych rozpoczyna XVI edycję ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa”. Jego celem jest podniesienie świadomości uczniów i nauczycieli w zakresie ochrony danych osobowych oraz prawa do prywatności.

W dobie powszechnego dostępu do internetu i dynamicznego rozwoju technologii cyfrowych, edukacja w tym obszarze staje się szczególnie istotna. Program zachęca młodych ludzi do refleksji nad tym, jak skutecznie chronić swoje dane, które informacje warto zabezpieczać oraz jakie konsekwencje może nieść ich nieprzemyślane udostępnianie. Dzięki temu uczniowie nie tylko poznają obowiązujące przepisy prawa, ale także rozwijają poczucie odpowiedzialności i wrażliwości społecznej.

Zapraszamy szkoły podstawowe, ponadpodstawowe oraz placówki doskonalenia nauczycieli do udziału w tym wyjątkowym przedsięwzięciu, które od lat angażuje kolejne pokolenia uczniów i nauczycieli, aby świadomie i odpowiedzialnie zarządzali danymi osobowymi.

6 EDUKACJA

Co czeka uczestników w tej edycji?

- szkolenia dla szkolnych koordynatorów,
- zajęcia dla uczniów,
- webinaria, konferencje i spotkania,
- konkursy i inicjatywy lokalne,
- gala finałowa konkursów.

Ważne daty:

Program pod honorowym patronatem Ministra Edukacji oraz Rzecznika Praw Dziecka jest wsparciem i uzupełnieniem zagadnień zawartych w podstawach programowych kształcenia ogólnego.

W tym roku istotnym tematem podejmowanych działań w ramach XVI edycji Programu będzie ochrona danych osobowych w kontekście wyzwań związanych z rozwojem sztucznej inteligencji, a także bezpiecznych podróży.

Szczegóły i formularz zgłoszenia znajdą Państwo na stronie: www.uodo.gov.pl/tdts

Dodatkowe pytania w sprawie Programu? Nasi eksperci są do dyspozycji: tdts@uodo.gov.pl

UODO PROMUJE PROGRAM TAKŻE PODCZAS OGÓLNOPOLSKICH WYDARZEŃ

Urząd Ochrony Danych Osobowych aktywnie informuje o kolejnej edycji programu „Twoje dane – Twoja sprawa" podczas licznych wydarzeń edukacyjnych, adresowanych do przedstawicieli szkół i placówek doskonalenia nauczycieli. Jednym z przykładów takich działań była konferencja „Uwaga! Smartfon", zorganizowana 4 czerwca 2025 r. w Lublinie, gdzie UODO zaprezentował program za pośrednictwem własnego stoiska informacyjnego.

Wydarzenie poświęcone było tematyce odpowiedzialnego korzystania z urządzeń mobilnych i narzędzi cyfrowych przez różne grupy społeczne – w szczególności dzieci, młodzież i seniorów – oraz konieczności dostosowania przepisów prawa do wyzwań związanych z ochroną prywatności, zdrowia psychicznego i bezpieczeństwa w cyfrowym świecie. Na stoisku UODO udzielane były bezpłatne konsultacje wszystkim uczestnikom zainteresowanym tematyką ochrony danych osobowych, a także prezentowane założenia programu edukacyjnego „Twoje dane – Twoja sprawa" oraz jego dotychczasowe rezultaty. Wiele osób miało okazję bezpośrednio porozmawiać z przedstawicielami UODO, zadać pytania dotyczące programu i dowiedzieć się, jak można wziąć udział w jego kolejnej edycji.

Dodatkowo, przedstawiciel Urzędu poprowadził warsztaty „Co poszło nie tak? – i dlaczego warto uczyć się na cudzych błędach", oparte na rzeczywistych przykładach naruszeń ochrony danych osobowych w placówkach edukacyjnych. Uczestnicy wzięli aktywny udział w analizie przypadków, poznając najczęstsze błędy oraz praktyczne sposoby ich unikania.

RADA EUROPY ORGANIZUJE MIĘDZYNARODOWY KONKURS NA PLAKAT I FILM KRÓTKOMETRAŻOWY NA TEMAT OBYWATELSTWA CYFROWEGO

Konkurs „International Poster and Short Film Competition on Digital Citizenship” jest organizowany w ramach „Europejskiego Roku Edukacji Cyfrowej Obywateli 2025”, inicjatywy prowadzonej przez Radę Europy.

Europejski Rok Edukacji Cyfrowej Obywateli 2025 ma na celu podkreślenie wartości edukacji cyfrowej w kształtowaniu cyfrowej przyszłości obywateli, pomagając w budowaniu integracyjnych i demokratycznych społeczeństw. Poprzez rozwój podstawowych kompetencji, w tym kluczowych umiejętności, wartości, postaw i wiedzy, obywatele mogą uczyć się, łączyć, angażować i rozwijać się razem w cyfrowo wzbogaconym świecie.

Wyzwania związane z szybkim rozprzestrzenianiem się przełomowych technologii, takich jak ChatGPT, jeszcze bardziej podkreśliły znaczenie krytycznych kwestii poruszanych w ramach edukacji cyfrowej obywateli (Digital Citizenship Education – DCE).

Walka z dezinformacją, cyberprzemocą, mową nienawiści w internecie, podniesienie kompetencji cyfrowych, popularyzacja cyfrowych etykiet, wykorzystanie danych osobowych i bezpieczeństwo cyfrowe należą do podstawowych wyzwań, przed którymi stoimy w dzisiejszym cyfrowym świecie. Aby skutecznie przeciwdziałać rozwijającym się zagrożeniom, musimy wspierać edukację cyfrową.

W tym kontekście artyści, projektanci i operatorzy są zaproszeni do wybrania dowolnego z celów Europejskiego Roku Edukacji Cyfrowej 2025 i domen koncepcji edukacji cyfrowej Rady Europy i stworzenia plakatów lub krótkich filmów. Prace konkursowe mają na celu przedstawienie różnorodnych perspektyw na tematy związane z obywatelstwem cyfrowym i podniesienie świadomości w tym obszarze w społeczeństwie. Po zakończeniu konkursu mogą zostać zorganizowane wystawy, aby jeszcze bardziej wzmocnić jego wpływ.

Konkurs jest otwarty zarówno dla zawodowych, jak i niezawodowych projektantów i twórców filmów krótkometrażowych, którzy są obywatelami lub rezydentami jednego z 46 państw członkowskich Rady Europy, a także Stolicy Apostolskiej i Kazachstanu.

6 EDUKACJA

Udział w konkursie jest bezpłatny.

Oceniane będą wyłącznie plakaty i filmy krótkometrażowe, które są zgodne z określonymi tematami i mieszczą się w celu i zakresie konkursu. Tematyka konkursu:

- Dostęp i integracja
- Uczenie się i kreatywność
- Media i informacje
- Umiejętność czytania i pisania
- Etyka i empatia
- Zdrowie i dobre samopoczucie
- E-obecność i komunikacja
- Aktywne uczestnictwo
- Prawa i obowiązki
- Prywatność i bezpieczeństwo
- Świadomość konsumencka.

Uczestnicy mogą przesłać maksymalnie trzy zgłoszenia w każdej kategorii (plakat lub film krótkometrażowy) i muszą być wyłącznymi autorami swoich prac. Zgłoszenia nie mogą być wcześniej nagradzane, wystawiane (w tym na platformach mediów społecznościowych, YouTube, online itp.).

Jeśli w zgłoszeniu występuje jakakolwiek osoba, uczestnik musi uzyskać odpowiednią zgodę, upewnić się, że zgłoszenie nie narusza praw autorskich osób trzecich oraz przestrzegać wszelkich innych obowiązujących przepisów podczas tworzenia plakatów lub filmów krótkometrażowych.

Rada Europy zastrzega sobie prawo do wycofania zgłoszenia, które w jakikolwiek sposób nie przestrzega regulaminu konkursu, celów Europejskiego Roku oraz zasad praw człowieka, demokracji i praworządności Rady Europy.

Termin nadsyłania prac upływa 14 września 2025 r.

Warunki uczestnictwa opisane są tutaj.

Plakaty promujące konkurs Konkurs „International Poster and Short Film Competition on Digital Citizenship”

Przypominamy, że UODO na stałe zmieniło swoją siedzibę

Dlatego od lipca 2025 r. prosimy kierować korespondencję na nowy adres: **Urząd Ochrony Danych Osobowych, ul. Moniuszki 1A, 00-014 Warszawa**. Pod nim znajdują się biura Urzędu oraz punkt kancelaryjny.

W wypadku kierowania korespondencji na stary adres Urzędu (ul. Stawki 2, 00-193 Warszawa) będzie ona do końca 2025 roku przekierowywana na nowy adres.

Zmiana siedziby nie wiąże się z obowiązkiem zamieszczenia nowego adresu Urzędu w klauzulach informacyjnych administratorów ochrony danych.

Jednak administratorzy, którzy w swoich klauzulach informacyjnych zamieścili poprzedni adres UODO muszą usunąć informacje adresowe UODO albo zaktualizować je.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl