URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 10/10/25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

W październiku miałem okazję spotkać się z wieloma z Was – dzięki naszej akcji „UODO rusza w kraj" o problemach związanych z ochroną danych osobowych miałem zaszczyt rozmawiać z mieszkańcami, samorządowcami, przedsiębiorcami, inspektorami ochrony danych i naukowcami w województwach warmińsko-mazurskim i lubuskim.

Program „UODO rusza w kraj" jest częścią niezwykle ważnej dla nas działalności edukacyjnej w zakresie ochrony danych. Regularnie informujemy o niej na naszej stronie internetowej i w mediach społecznościowych.

Jest dla nas niezwykle ważne, że w trakcie różnych spotkań możemy się z Państwem dzielić wiedzą z zakresu ochrony prywatności i danych osobowych, słuchać Państwa obserwacji, notować i odpowiadać na pytania. To pozwala nam lepiej diagnozować problemy, z którymi wszyscy się borykamy, i szukać dla nich rozwiązań.

Te problemy wiążą się przede wszystkim ze stale postępującymi zmianami technologicznymi i prawnymi.

Przetwarzanie danych w systemach państwowych

Naszym październikowym sukcesem jest to, że rząd uwzględnił uwagi Prezesa UODO do projektu systemu e-rejestracji do lekarzy. System ułatwi życie pacjentom i nie pozwoli na marnowanie wysiłku w ochronie zdrowia. Trzeba jednak pamiętać, że będzie przetwarzał dane osobowe, i powinien to robić tak, by chronić prywatność i nie narażać pacjentów na niepotrzebne ryzyko związane z przetwarzaniem danych.

Nadal prowadzę korespondencję z MSWiA na temat przetwarzania danych osobowych w systemach policyjnych. Problem dotyczy nie tylko Polski, a chodzi o to, że służby policyjne niechętnie usuwają ze swych wewnętrznych rejestrów dane osobowe. Jeśli ktoś raz tam trafi, w praktyce zawsze może pozostawać w „kręgu podejrzanych", nawet jeśli kara za przestępstwo dawno się zatarła. Trybunał Sprawiedliwości Unii Europejskiej w odpowiedziach na pytania prejudycjalne od sądów z krajów UE stale wskazuje, że należy zmienić przepisy krajowe tak, by dane w policyjnych rejestrach nie były przechowywane w nieskończoność. Nawet jeśli dany wyrok nie dotyczy Polski, ma dla nas znaczenie, bo pokazuje, w jaki sposób Unia Europejska chce chronić prywatność swoich obywateli. Dlatego regularnie zwracamy uwagę na ten problem.

Poszanowanie prywatności buduje bowiem zaufanie do państwa i jego służb.

Elementem systemu ochrony prywatności jest też właściwe umiejscowienie inspektorów ochrony danych w strukturze organizacji. Policja nadal ma z tym kłopot ze względu na wadliwość przepisów. Zwróciłem na to po raz kolejny uwagę MSWiA.

Kiedy należy powiadomić Prezesa UODO o incydencie

Ważnym problemem, którym zajmowaliśmy się w październiku, jest kwestia, kiedy administrator danych powinien powiadomić Prezesa UODO oraz osobę, której dane dotyczą, o incydencie.

W dwóch sprawach administratorzy – błędnie naszym zdaniem – uznali incydent za rodzący ryzyko „mało prawdopodobne". Administratorzy dochodzili do takiego wniosku tylko dlatego, że chodziło o jednorazowe pomylenie adresatów korespondencji (chodzi tu o wygraną przed NSA sprawę dotyczącą danych finansowych i o decyzję Prezesa UODO o karze w sprawie danych zdrowotnych).

Naszą argumentację przedstawiliśmy w decyzji. NSA zaś w uzasadnieniu wyroku w drugiej sprawie przedstawił argumenty prawne na poparcie sposobu rozumowania Prezesa UODO. Sprawy te pokazują, jak właściwie szacować ryzyko i kiedy można mówić o ryzyku minimalnym.

Gorąco zachęcam Państwa do zapoznania się z argumentacją prawną, którą zreferowaliśmy w komunikatach na naszej stronie internetowej.

Prawo banków do danych niedoszłych klientów

W dwóch kolejnych sprawach udało nam się przed NSA potwierdzić nasze stanowisko, że banki i Biuro informacji Kredytowej nie mogą przetwarzać danych osób, które wystąpiły z wnioskiem kredytowym, ale ostatecznie nie zawarły umowy. Sprawdzanie zdolności kredytowej upoważnia do przetwarzania danych, ale tylko w trakcie tego procesu, a nie po nim.

Szczegóły dotyczące tych ważnych rozstrzygnięć można znaleźć TU.

Pozostałe ważne decyzje Prezesa UODO i wyroki

W głośnej sprawie monitoringu wizyjnego na oddziale neonatologii w Centrum Zdrowia Ujastek Wojewódzki Sąd Administracyjny podtrzymał decyzję Prezesa UODO ze stycznia tego roku o karze dla administratora. Chodzi o monitoring ukryty w zegarach na oddziale – rejestrował on bez wiedzy zainteresowanych wszystko, co działo się w salach, w tym rozmowy rodziców, karmienie i pielęgnację dzieci. Monitoring miał pomóc w zwalczaniu zakażeń w placówce. Został jednak wprowadzony niezgodnie z przepisami, a cała sprawa wyszła na jaw dopiero wtedy, gdy zaginęły karty pamięci z zapisem nagrań z ukrytych kamer.

Współpraca z sądami

Wspólnie z sądami doprecyzowujemy mechanizmy powiadamiania Prezesa UODO o sprawach o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych. Obowiązek taki nakłada na sądy art. 94 ust. 1 ustawy o ochronie danych osobowych. Dotyczy to spraw określonych w art. 79 lub art. 82 ogólnego rozporządzenia o ochronie danych (RODO).

W zgłaszaniu tych spraw pomocne mogą być formularze, które sami opracowaliśmy, a po uwagach prezesów sądów apelacyjnych zmodyfikowaliśmy. 6 listopada organizujemy w UODO seminarium poświęcone tym zagadnieniom. Tego dnia zostaną też opublikowane formularze do komunikacji sądów z Prezesem UODO.

Z innych ważnych spraw chciałbym zwrócić Państwa uwagę na to, że od 10 października 2025 r. stosuje się bezpośrednio przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/900 ws. przejrzystości i targetowania reklamy politycznej. Ma ono pomóc obywatelom w dokonywaniu świadomych wyborów, ułatwiając rozpoznawanie reklamy politycznej oraz zrozumienie, kto za nią stoi i czy jest to reklama targetowana.

Rozporządzenie wprowadza m.in.:

- obowiązek ujawniania finansowania reklam politycznych ze wskazaniem, kto za nimi stoi i kto je finansuje;
- obowiązek ich oznaczania w taki sposób, by odbiorca nie miał wątpliwości, z jakim rodzajem przekazu ma do czynienia;
- ograniczenie targetowania sprowadzające się głównie do zakazu profilowania użytkowników na podstawie danych szczególnej kategorii;
- mechanizmy mające przeciwdziałać dezinformacji i jej rozpowszechnianiu w przestrzeni cyfrowej;
- obowiązek prowadzenia rejestrów i europejskiego repozytorium politycznych materiałów reklamowych;
- zakaz ingerencji państw trzecich w wybory.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W tym wydaniu biuletynu proponujemy wywiad z Marią Drabczyk i dr. hab. Dominikiem Lubaszem, koordynatorami prac nad sztuczną inteligencją Grupy roboczej Społecznego Zespołu Ekspertów przy Prezesie UODO. Motywem przewodnim naszej rozmowy jest ankieta, która została rozesłała do organizacji reprezentujących różne branże, szczególnie jednak te należące do sektora publicznego oraz sektora przedsiębiorców. Inicjatywa ma na razie charakter pilotażowy, a jej cel to zbadanie potrzeb wsparcia w zakresie odpowiedzialnego wykorzystania AI i danych osobowych zgodnie z RODO. Jak wyjaśniają nasi rozmówcy: „Chcemy widzieć nasze działanie jako pierwszy krok, z potencjałem współpracy z innymi sektorami i typami podmiotów. Mamy świadomość tego, jak duże są potrzeby". Gorąco zachęcam do wzięcia udziału w ankiecie, formularz dostępny będzie on-line do 15 listopada tego roku, a jego wypełnienie zajmuje ok. 10 minut.

W tym numerze piszemy o przepisach ustawy o bezpieczeństwie osób przebywających na obszarach wodnych i o tym, że szczegółowo regulują one na kwestie udostępniania danych zawartych w rejestrze działań ratowniczych. Odpowiedzi w tej sprawie musiał udzielić Prezes UODO po tym, jak w ostatnim czasie do jednostek wodnego ochotniczego pogotowia ratunkowego wpłynęła duża liczba wniosków o udostępnienie – w trybie dostępu do informacji publicznej – rejestru działań ratowniczych.

Odnosimy się także do nakazu usunięcia danych osoby publicznej z platformy społecznościowej, który wydał Prezes UODO wobec jednej z organizacji pozarządowych zajmujących się obserwowaniem incydentów wywołanych przez rasizm i ksenofobię. Jak możemy się dowiedzieć z konkluzji decyzji organu nadzorczego, działalność statutowa tego rodzaju organizacji nie zwalnia ich z przestrzegania przepisów rozporządzenia 2016/679, bowiem każda organizacja pozarządowa, która przetwarza dane osobowe, staje się administratorem tych danych.

Staramy się również wyjaśnić, jak prawidłowo ocenić ryzyko w przypadku naruszenia ochrony danych osobowych i dlaczego jest to kluczowe dla zapewnienia zgodności z RODO. To nad wyraz ważne zagadnienie, gdyż właśnie od ryzyka dla praw lub wolności osób fizycznych zależy zakres obowiązków spoczywających na administratorach i podmiotach przetwarzających. Takich czynników, które należy uwzględnić po naruszeniu ochrony danych, jest w naszym katalogu siedem.

W tym wydaniu przeczytacie też o najistotniejszych wydarzeniach związanych z ochroną danych w Europie i o bieżącym unijnym procesie legislacyjnym. Podczas wrześniowego posiedzenia plenarnego Europejska Rada Ochrony Danych przyjęła wytyczne dot. wzajemnego oddziaływania między Aktem o usługach cyfrowych (DSA) a ogólnym rozporządzeniem o ochronie danych. To pierwsze wytyczne EROD skupione na relacji między RODO a niedawno przyjętym prawem cyfrowym UE. Podsumowujemy również brukselską konferencję RAID (Regulation of AI, Internet & Data, 28–29 września), która zgromadziła przedstawicieli regulatorów, instytucji unijnych, firm technologicznych oraz ekspertów z całego świata. W spotkaniu uczestniczyli prezes UODO Mirosław Wróblewski oraz Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej UODO. Z kolei 1 października w Pradze odbyła się dziewiąta edycja konferencji Privacy Days – największego wydarzenia w Czechach poświęconego ochronie danych osobowych i gospodarce cyfrowej.

Piszemy także, czym w istocie jest System Wjazdu/Wyjazdu (EES), czyli nowe narzędzie zarządzania granicami w strefie Schengen, ustanowione dla zapobiegania nielegalnej migracji i zwiększenia bezpieczeństwa wewnętrznego. Jego uruchomienie stanowi jeden z kluczowych kroków we wdrażaniu nowej generacji systemów informacyjnych w obszarze zarządzania granicami. EES dołączył tym samym do innych wielkoskalowych systemów informatycznych UE – takich jak System Informacyjny Schengen (SIS), Wizowy System Informacyjny (VIS) czy Europejski System Informacji o Podróży oraz Zezwoleń na Podróż (ETIAS). W Polsce nadzór nad przetwarzaniem danych w EES sprawuje Prezes UODO. System objęty jest też unijnym mechanizmem skoordynowanego nadzoru, w ramach którego współpracują krajowe organy ochrony danych i Europejski Inspektor Ochrony Danych.

Na zakończenie Biuletynu 10/2025 zapraszamy do uczestnictwa w zaplanowanych na listopad inicjatywach edukacyjnych UODO. A wśród nich – w seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO” oraz w konferencji „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach”.

Karol Witowski
Dyrektor Departamentu Komunikacji Społecznej
Rzecznik Prasowy UODO

CHCEMY POZNAĆ POTRZEBY I PROBLEMY ORGANIZACJI W WYKORZYSTYWANIU AI

O odpowiedzialnym wykorzystywaniu sztucznej inteligencji Karol Witowski rozmawia z koordynatorami prac nad sztuczną inteligencją Grupy roboczej Społecznego Zespołu Ekspertów przy Prezesie UODO: dr. hab. Dominikiem Lubaszem, partnerem zarządzającym Kancelarii Radców Prawnych lubasz&wspólnicy, i Marią Drabczyk, prezeską zarządu Centrum Cyfrowe

Urząd Ochrony Danych Osobowych wspólnie z Grupą roboczą ds. sztucznej inteligencji opracował i rozesłał ankietę, której celem jest zbadanie aktualnych praktyk, wyzwań i potrzeb wsparcia w zakresie odpowiedzialnego wykorzystania AI i danych osobowych zgodnie z RODO. Ankieta została wysłana do organizacji reprezentujących różne branże. Jakie branże znajdują się w Państwa zainteresowaniu? Są jakieś szczególne?

Maria Drabczyk: Zacznijmy od naszego celu: chcemy stworzyć, mieszczące się w kompetencjach Prezesa Urzędu Ochrony Danych Osobowych, mechanizmy wsparcia, projektowania oraz wdrażania systemów AI, odpowiedzialnego i zgodnego z RODO. Zależy nam na rozwoju mądrych inwestycji w nowe technologie oraz promowaniu zrównoważonego rozwoju.

Nasze działanie ma charakter pilotażowy, dlatego też zdecydowaliśmy się zawęzić je do kilku typów organizacji. Skoncentrujemy się na wybranych przedstawicielach sektora publicznego oraz sektorze przedsiębiorców, w szczególności MŚP i start-upach. Jednostki publiczne (samorządowe, edukacyjne, medyczne, kulturalne) pełnią kluczowe funkcje społeczne i dysponują ograniczonymi zasobami. Potencjał AI w tych obszarach jest ogromny – od usprawnienia usług i zarządzania danymi po zwiększenie dostępności kultury i edukacji – jednak obserwujemy w nich niedosyt kompetencji i potrzebę wsparcia. Podobnych trudności doświadczają przedsiębiorcy tworzący i wykorzystujący rozwiązania AI.

1 ROZMOWA Z EKSPERTAMI

Szczególnie MŚP i start-upy często nie mają dostępu do eksperckiej wiedzy prawniczej, etycznej i technicznej, a brak wsparcia może prowadzić do nieodpowiedzialnych wdrożeń, ograniczać innowacyjność i obniżać zaufanie użytkowników. Dlatego oba sektory potrzebują systemowych mechanizmów wsparcia – wiedzy, dobrych praktyk i narzędzi – które umożliwią im bezpieczne, zgodne z regulacjami i etyczne wykorzystanie sztucznej inteligencji, wzmacniając tym samym konkurencyjność i zaufanie do europejskich rozwiązań. Chcemy widzieć nasze działanie jako pierwszy krok, z potencjałem współpracy z innymi sektorami i typami podmiotów. Mamy świadomość tego, jak duże są potrzeby.

W jaki dokładnie sposób zostanie wykorzystana ankieta?

M.D.: Ankieta ma dla nas charakter diagnostyczny: chcemy poznać realne potrzeby i problemy organizacji w zakresie zgodnego z prawem wykorzystywania AI. Wyniki będą opracowane w formie raportu, którego podsumowanie zostanie upublicznione. Będzie to baza do przygotowania wytycznych, materiałów edukacyjnych i warsztatów. Planujemy także spotkania warsztatowe, które pozwolą pogłębić analizę wyników i wypracować praktyczne rekomendacje.

Jak wyobrażają sobie Państwo pracę Grupy roboczej w najbliższym roku, dwóch? Czy może się okazać konieczne rozszerzenie Grupy o nowych ekspertów z różnych dziedzin w związku z dynamicznie rozwijającą się sztuczną inteligencją? Właściwie co chwila pojawiają się kolejne wyzwania w sprawie AI.

Dominik Lubasz: Nasza praca została zaplanowana etapowo. W pierwszej fazie (do 12 miesięcy) skupimy się na badaniach i pierwszych wytycznych. W kolejnym etapie (12–24 miesięcy) chcemy wdrażać szkolenia, publikować materiały i prowadzić warsztaty. Niewątpliwie w miarę pojawiania się nowych wyzwań – np. związanych z rozwojem generatywnej AI czy wdrażaniem unijnego Aktu o AI – będziemy otwarci na poszerzenie zespołu o nowych ekspertów z dziedzin technicznych, etycznych czy społecznych.

Jak w Państwa opinii technologie sztucznej inteligencji mogą wpłynąć na znaczenie i sens RODO? Czy może się okazać, że konieczna będzie rewolucja w filozofii przepisów RODO i całkiem nowe ujęcie prawne, być może nawet coś w rodzaju nowego RODO?

D.L.: RODO zachowuje pełną aktualność: jego zasady – takie jak przejrzystość, minimalizacja danych czy rozliczalność – są uniwersalne i niezwykle potrzebne w erze AI. Sztuczna inteligencja nie oznacza końca RODO, ale raczej potrzebę jego nowej interpretacji i praktycznych narzędzi dostosowanych do realiów technologicznych. Mówimy więc bardziej o ewolucji niż rewolucji – o wzmocnieniu stosowania zasad, a nie ich odrzuceniu.

1 ROZMOWA Z EKSPERTAMI

Umocnienia wymagają zrozumienie i zaadaptowanie podejścia opartego na ryzyku do tego nowego kontekstu technologicznego, wskazanie kluczowych aspektów analizy ryzyka, oceny skutków dla ochrony danych czy uwzględnienie ochrony danych w fazie projektowania. Elastyczność i neutralność technologiczna tych instrumentów regulacyjnych powoduje, że nie jest potrzebna zmiana RODO w związku z rozwojem sztucznej inteligencji, lecz wsparcie w jego stosowaniu. Edukowanie w tym obszarze jest też misją Prezesa UODO.

Czy planują Państwo umieścić pracę Grupy roboczej w kontekście zmieniającej się sytuacji zagrożenia geopolitycznego? Czy w tej kwestii mogą się pojawić jakieś działania priorytetowe, dotyczące np. dezinformacji generowanej również za pomocą AI?

M.D.: Aktualna sytuacja pokazuje, jak ważne jest odpowiedzialne i etyczne wykorzystanie danych. Żyjemy w czasach, w których większość narracji oparta jest na danych. Pytanie, czy są to dane wiarygodne, pochodzące z pewnego źródła, rzetelnie opracowane. Tu często nie mamy pewności. Praca z AI w kontekście danych wymaga od nas krytycznego myślenia i krytycznego spojrzenia na dane – ich proweniencję, sposób wykorzystania. I tu potrzebne są konkretne kompetencje i wskazówki, które mamy nadzieję zebrać i szerzej udostępnić.

D.L.: Tak, nie można ignorować kontekstu geopolitycznego. Sztuczna inteligencja jest wykorzystywana także do generowania treści dezinformacyjnych czy manipulacyjnych. W tym zakresie widzimy rolę Prezesa UODO w edukowaniu, jak chronić dane i prywatność w obliczu zagrożeń hybrydowych.

Czy może dojść do sytuacji, w której państwa UE zdecydują, że sztuczną inteligencję należy hamować poprzez zakazy jej stosowania?

D.L.: Akt o AI już przewiduje zakazy dla określonych zastosowań, które zagrażają prawom człowieka – jak systemy oceny społecznej czy niektóre formy masowej inwigilacji. Unia Europejska idzie jednak w stronę regulacji proporcjonalnych i opartych na analizie ryzyka, a nie generalnych zakazów hamujących rozwój technologii.

M.D.: Dlatego też równie ważne wydają się właśnie działania mające na celu podniesienie kompetencji użytkowników i twórców rozwiązań AI, dzięki którym ta innowacja będzie rozwijana w sposób odpowiedzialny i zgodny z prawem i wartościami – w tym poszanowaniem prywatności.

1 ROZMOWA Z EKSPERTAMI

Czy Państwa zdaniem istnieje ryzyko, że możliwości sztucznej inteligencji rozwiną się do tego stopnia, że ochrona danych osobowych będzie potrzebowała jakiegoś oddzielnego systemu – i będzie można również go zaliczyć do sztucznej inteligencji – który będzie sprawował kontrolę nad danymi? Czy tym samym nie popadniemy w cyfrową walkę, w której o wiele mniejsze znaczenie będą miały same przepisy?

D.L.: Możemy sobie wyobrazić rozwiązania oparte na AI, wspierające inspektorów ochrony danych czy compliance. Nie oznacza to jednak, że prawo stanie się zbędne. Wręcz przeciwnie – przepisy RODO pozostają fundamentem, a narzędzia AI mogą jedynie wspomóc ich egzekwowanie. Celem jest wzmocnienie nadzoru, nie jego automatyzacja kosztem człowieka.

Jak pojmują Państwo rolę Grupy roboczej w obszarze wchodzących w życie rozporządzeń UE dotyczących sztucznej inteligencji?

D.L.: Grupa robocza ma pełnić funkcję łącznika między teorią w obszarze technologii, etyki i prawa a praktyką wdrażania regulacji. Będziemy wspierać interpretację nowych przepisów dotyczących ochrony danych, w szczególności Aktu ws. sztucznej inteligencji, przygotowywać materiały pomocnicze i wspierać dialog między regulatorami, administracją i biznesem. Nasza rola to nie tylko analiza prawna, ale i tworzenie przestrzeni wymiany doświadczeń.

Link do ankiety: https://wydarzenia.uodo.gov.pl/?r=ankietaAI

Dziękuję za rozmowę

UDOSTĘPNIANIE DANYCH Z REJESTRU DZIAŁAŃ RATOWNICZYCH

Przepisy ustawy o bezpieczeństwie osób przebywających na obszarach wodnych szczegółowo regulują kwestie udostępniania danych zawartych w rejestrze działań ratowniczych. Do ich pozyskiwania nie powinna być wykorzystywana procedura dostępu do informacji publicznej.

W ostatnim czasie do jednostek wodnego ochotniczego pogotowia ratunkowego (WOPR) coraz częściej wpływają wnioski o udostępnienie – w trybie dostępu do informacji publicznej – rejestru działań ratowniczych. Ponieważ zawiera on wiele danych osobowych, w tym tych należących do szczególnych kategorii w rozumieniu RODO, przedstawiciele WOPR zwrócili się do UODO z prośbą o wyjaśnienie, jak mają postępować z takimi wnioskami.

UODO w odpowiedzi – zgodnie ze swoją właściwością – udzielił ogólnych wskazówek w zakresie ochrony danych osobowych.

Wziął przy tym pod uwagę, że wszystkie działania, jakie podejmują ratownicy wodni, są dokumentowane w rejestrze działań ratowniczych, który (stosownie do art. 14 ust. 3 ustawy z 18 sierpnia 2011 r. o bezpieczeństwie osób przebywających na obszarach wodnych) zawiera takie dane, jak:

1) imię i nazwisko osoby, której udzielono pomocy w ramach działań ratowniczych, datę i miejsce urodzenia oraz adres zamieszkania;
2) rodzaj doznanego urazu lub zachorowania osoby, o której mowa w pkt 1;
3) rodzaj udzielonej pomocy;
4) miejsce wypadku;
5) imiona i nazwiska ratowników wodnych udzielających pomocy;
6) datę prowadzenia działań ratowniczych;
7) czas i miejsce przekazania osoby, o której mowa w pkt 1, jednostkom systemu Państwowe Ratownictwo Medyczne lub innym służbom.

Znajduje się w nim zatem wiele danych dotyczących osób poszkodowanych i podejmowanych w stosunku do nich czynności ratowniczo-medycznych, a więc danych, które zgodnie z przepisami RODO podlegają szczególnej ochronie.

Jednocześnie Urząd podkreślił, że powołana ustawa przewiduje szczególny tryb udostępniania danych i informacji z rejestru działań ratowniczych, a zasady udostępniania danych osobowych z tego rejestru zostały w sposób wyczerpujący opisane w jej art. 14 ust. 5.

Stanowi on, że podmiot uprawniony do wykonywania ratownictwa wodnego udostępnia informacje z rejestru działań ratowniczych na pisemny wniosek:

1) osobie, której udzielono pomocy w ramach działań ratowniczych, oraz

2) Policji, prokuraturze, sądom, dyrektorowi parku narodowego i zakładom ubezpieczeń w związku z prowadzonym przez nie postępowaniem.

W opinii UODO przepisy prawa w tym zakresie należy interpretować ściśle i zawężająco. Katalog podmiotów, którym dane mogą być udostępnione, nie może być rozszerzany, a udostępnienie danych może się odbywać jedynie po spełnieniu warunków określonych w powołanym przepisie. Przede wszystkim zaś dane zgromadzone w rejestrze mogą być udostępniane wyłącznie osobie, której udzielono pomocy w ramach działań ratowniczych, oraz organom wskazanym w art. 14 ust. 5 pkt 2 w związku z prowadzonym przez nie postępowaniem.

Rejestr działań ratowniczych ma charakter niejawny, na co jednoznacznie wskazuje ustawodawca, określając szczególny tryb udostępniania danych oraz środki bezpieczeństwa wskazane w art. 14 ust. 6.

Udostępnianie informacji w trybie dostępu do informacji publicznej, przewidzianym w ustawie z 6 września 2001 r. o dostępie do informacji publicznej, stanowi odrębną procedurę, dotyczącą innego zakresu przedmiotowego. Procedura ta nie może być wykorzystywana do obchodzenia trybu uzyskiwania danych, określonego w ustawie o bezpieczeństwie osób przebywających na obszarach wodnych.

SIEDEM CZYNNIKÓW RYZYKA, KTÓRE NALEŻY UWZGLĘDNIĆ PO NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Podejście oparte na ryzyku to fundament prawa ochrony danych osobowych. To właśnie od ryzyka dla praw lub wolności osób fizycznych zależy zakres obowiązków spoczywających na administratorach i podmiotach przetwarzających. Poniżej wyjaśniamy, jak prawidłowo ocenić ryzyko w przypadku naruszenia ochrony danych osobowych i dlaczego jest to kluczowe dla zapewnienia zgodności z RODO.

Dlaczego należy oceniać ryzyko

Przetwarzanie danych osobowych wiąże się z **ryzykiem naruszenia praw lub wolności osób fizycznych**. Oznacza to możliwość wystąpienia rozmaitych szkód majątkowych i niemajątkowych, a w niektórych przypadkach nawet zagrożenia dla bezpieczeństwa osobistego lub zdrowia. Administratorzy i podmioty przetwarzające muszą więc podejmować działania, aby **skutecznie zapobiegać ewentualnym negatywnym konsekwencjom** dla osób, których dane dotyczą. Stanowi to podstawę regulacji dotyczących ochrony danych osobowych.

Ryzyko dla osób fizycznych powinno być analizowane w różnych kontekstach:

- Z jednej strony niezbędne są **analizy systemowe**, wykonywane zarówno na etapie projektowania operacji przetwarzania, jak i w ich trakcie. Pozwalają one realizować zasady ochrony danych osobowych oraz powstrzymywać naruszenia ich bezpieczeństwa. Stopień ryzyka związanego z przetwarzaniem decyduje także o konieczności przeprowadzenia oceny skutków dla ochrony danych (art. 35 ust. 1 RODO).
- Z drugiej strony – w przypadku wystąpienia naruszenia ochrony danych osobowych – kluczowe stają się **analizy incydentalne**, skoncentrowane na okolicznościach konkretnego zdarzenia. Umożliwiają one identyfikację wynikających z niego zagrożeń oraz skuteczne im zaradzenie. Co równie istotne, pomagają prawidłowo określić obowiązki prawne administratora, takie jak konieczność zgłoszenia incydentu organowi nadzorczemu oraz zawiadomienia o nim osób, których dane dotyczą (art. 33 ust. 1 i art. 34 ust. 1 RODO).

3 NARUSZENIA I KONTROLE

Ryzyko a obowiązki prawne

Zgodnie z art. 33 ust. 1 RODO administratorzy powinni **zgłaszać naruszenia ochrony danych osobowych** właściwym organom nadzorczym. Zgłoszenie nie jest jednak wymagane, jeżeli wystąpienie ryzyka jest **mało prawdopodobne**, czyli gdy brak jest realnych przesłanek, by mogło dojść do negatywnych konsekwencji dla osób fizycznych. W sytuacjach, w których naruszenie ochrony danych osobowych **może powodować wysokie ryzyko**, administratorzy zobowiązani są dodatkowo do zawiadomienia o zdarzeniu osób, których dane dotyczą, stosownie do art. 34 ust. 1 RODO.

Obowiązek prawny	**Próg ryzyka uruchamiający obowiązek**	**Próg ryzyka zwalniający z obowiązku**
Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust. 1 RODO)	Naruszenie ochrony danych osobowych **może wywołać ryzyko** dla praw lub wolności osób fizycznych	Jest **mało prawdopodobne**, że naruszenie ochrony danych osobowych wywoła **ryzyko** dla praw lub wolności osób fizycznych
Zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 ust. 1 RODO)	Naruszenie ochrony danych osobowych **może wywołać wysokie ryzyko** dla praw lub wolności osób fizycznych	Jest **mało prawdopodobne**, że naruszenie ochrony danych osobowych wywoła **wysokie ryzyko** dla praw lub wolności osób fizycznych

Ocena ryzyka związanego z naruszeniem ochrony danych osobowych służy nie tylko ustaleniu, czy w konkretnej sytuacji powstaje obowiązek jego zgłoszenia lub zawiadomienia o nim osób, których dane dotyczą. Jej celem jest również **określenie zakresu i rodzaju środków zaradczych**, jakie należy podjąć w reakcji na zdarzenie.

Jednocześnie należy pamiętać, że zgodnie z art. 33 ust. 5 RODO administratorzy powinni **dokumentować wszelkie naruszenia ochrony danych osobowych**. W tym przypadku obowiązek nie zależy od ryzyka i wynika z samego faktu wystąpienia takiego zdarzenia.

3 NARUSZENIA I KONTROLE

Jak oceniać ryzyko w przypadku naruszenia ochrony danych osobowych

Jak widać, przepisy RODO wymagają od administratorów **kompleksowego rozumienia zagrożeń wynikających z naruszeń bezpieczeństwa danych**. Ograniczenie się do przypisania zdarzeniu określonego poziomu ryzyka (np. wysokiego) może nie wystarczyć. Analiza ryzyka powinna uwzględniać **rzeczywisty kontekst zdarzenia**, jego przyczyny i możliwe skutki dla osób fizycznych.

Aby prawidłowo ocenić ryzyko związane z naruszeniem ochrony danych osobowych, warto wziąć pod uwagę **siedem podstawowych czynników**:

1. Rodzaj naruszenia ochrony danych osobowych

Wśród naruszeń ochrony danych osobowych można wyróżnić naruszenia **poufności, integralności i dostępności** danych. Prawidłowe ustalenie rodzaju naruszenia ma kluczowe znaczenie przy ocenie związanego z nim ryzyka. Inne konsekwencje mogą bowiem wystąpić w przypadku **nieuprawnionego ujawnienia danych**, a inne – gdy doszło do ich **utracenia, zniszczenia lub pomyłkowej modyfikacji**.

Warto pamiętać, że niektóre incydenty mogą naruszać więcej niż jeden z tych atrybutów (np. w wyniku ataku ransomware). W takich sytuacjach katalog potencjalnych skutków dla osób fizycznych może być znacznie szerszy.

2. Charakter, wrażliwość i zakres danych osobowych

Wynik analizy ryzyka zależy także od **charakteru, wrażliwości i zakresu danych osobowych**, które zostały naruszone. Administrator powinien zidentyfikować kategorie tych danych i ocenić ich znaczenie w określonym kontekście. Przykładowo, dane wymienione w art. 9 ust. 1 i art. 10 RODO znajdują się pod szczególną ochroną prawną, ponieważ ich naruszenie może stanowić poważną ingerencję w prywatność osoby fizycznej. Należą do nich m.in. dane biometryczne, dane dotyczące zdrowia czy dane ujawniające poglądy polityczne. W wielu sytuacjach zazwyczaj można również przyjąć, że dane o charakterze powszechnym (np. informacje o preferencjach lub zainteresowaniach) będą mniej wrażliwe niż dane finansowe.

Należy jednak pamiętać, że **wrażliwość danych zależy od kontekstu** – informacje pozornie neutralne, takie jak imię i nazwisko czy adres zamieszkania, również mogą negatywnie wpłynąć na sytuację jednostki.

W przypadku naruszenia poufności warto też przeanalizować, **jaki zestaw informacji stał się dostępny dla osób nieuprawnionych**. Znaczenie mają przy tym nie tylko dane ujawnione bezpośrednio, lecz także te, które w wyniku incydentu można łatwo połączyć z konkretną osobą (np. loginy i hasła umożliwiające dostęp do innych systemów lub kont użytkowników).

3. Łatwość identyfikacji osób, których dane dotyczą

Niektóre dane osobowe, np. numer PESEL, mogą umożliwiać **jednoznaczną identyfikację osoby fizycznej**. W innych przypadkach ustalenie tożsamości wymaga dodatkowych informacji, wysiłku lub zastosowania specjalistycznych narzędzi technicznych. Łatwość identyfikacji osób, których dane dotyczą, ma istotne znaczenie przy ocenie ryzyka związanego z naruszeniem ochrony danych osobowych. Im trudniej przypisać określone informacje do konkretnej osoby, tym mniejsze ryzyko naruszenia jej praw lub wolności. Skuteczna **pseudonimizacja, anonimizacja** lub **szyfrowanie** danych może znacząco ograniczyć ryzyko negatywnych skutków incydentu.

4. Dotkliwość konsekwencji dla osób, których dane dotyczą

Ocena ryzyka związanego z naruszeniem ochrony danych osobowych powinna obejmować także **wagę możliwych konsekwencji** zdarzenia dla osób, których dane dotyczą. Należy rozważyć, jak poważne mogą być potencjalne szkody – zarówno **materialne**, mające wymiar ekonomiczny, jak i **niematerialne**, o charakterze osobistym lub społecznym. Do pierwszej grupy można zaliczyć np. kradzież tożsamości skutkującą wykorzystaniem danych do zawarcia niechcianych umów. Wśród szkód niematerialnych znajdują się m.in. poczucie wstydu czy dyskryminacja. Część skutków może mieć **charakter złożony** – np. utrata reputacji (szkoda niematerialna) może prowadzić do utraty dochodów (szkoda materialna).

Przy ocenie dotkliwości warto także uwzględnić **czas trwania i nieodwracalność skutków**. Im dłużej dane pozostają poza kontrolą administratora i im trudniej ograniczyć ich dalsze wykorzystanie, tym wyższa jest dotkliwość incydentu. Krótkotrwała utrata dostępu do usługi dla kilku użytkowników może mieć ograniczone konsekwencje, natomiast ujawnienie danych genetycznych lub biometrycznych w internecie może prowadzić do długotrwałych szkód, których nie da się w pełni naprawić.

5. Cechy szczególne osoby, której dane dotyczą

Przy ocenie ryzyka warto uwzględnić również **cechy i sytuację osób, których dane zostały naruszone**. Dotkliwość skutków incydentu zależy nie tylko od kategorii danych osobowych, lecz także od **indywidualnej podatności** konkretnej osoby na ich wykorzystanie. Wyższe ryzyko może występować w przypadku osób małoletnich, osób starszych, pacjentów, osób z niepełnosprawnościami lub takich, które pozostają w zależności służbowej, ekonomicznej lub prawnej. Naruszenie danych tych osób może prowadzić do poważniejszych konsekwencji, ponieważ dysponują one mniejszymi możliwościami ochrony swoich praw lub ograniczenia skutków zdarzenia.

Znaczenie mają też **czynniki społeczne** – np. gdy incydent dotyczy osób należących do mniejszości lub uczestniczących w działaniach związków zawodowych czy organizacji społecznych.

W takich przypadkach nawet ujawnienie pozornie nieszkodliwych informacji może skutkować naruszeniem prywatności, stygmatyzacją lub narażeniem na presję ze strony innych podmiotów.

6. Cechy szczególne administratora

Ryzyko związane z naruszeniem ochrony danych osobowych zależy też od **specyfiki administratora**. Znaczenie mają m.in. zakres i skala przetwarzania, a także rodzaj działalności – inne konsekwencje może mieć incydent w placówce medycznej, a inne w niewielkiej organizacji społecznej.

Warto również uwzględnić **pozycję zaufania społecznego lub szczególną odpowiedzialność administratora** – np. w przypadku instytucji publicznych czy podmiotów przetwarzających dane osób w trudnej sytuacji życiowej. W takich przypadkach oczekiwania wobec standardów ochrony danych są wyższe, a konsekwencje incydentów – bardziej dotkliwe.

7. Liczba osób, których dane dotyczą

Przy ocenie ryzyka należy też uwzględnić **skalę zdarzenia**, rozumianą jako liczbę osób, których dane zostały nim objęte. Nawet jeśli skutki dla pojedynczej osoby wydają się ograniczone, wysoka liczba poszkodowanych może znacząco zwiększyć ogólny poziom ryzyka i wymagać podjęcia bardziej zaawansowanych działań zaradczych.

Warto jednak pamiętać, że **liczba osób dotkniętych naruszeniem ochrony danych osobowych wpływa przede wszystkim na prawdopodobieństwo wystąpienia negatywnych konsekwencji**, lecz nie zawsze na ich wagę. Poważne lub nieodwracalne skutki mogą bowiem wystąpić także w przypadku incydentu dotyczącego jednej osoby – zwłaszcza gdy naruszone dane mają charakter szczególnie wrażliwy.

Skuteczna rozliczalność

Zasada rozliczalności wymaga od administratora nie tylko przestrzegania przepisów RODO, ale także możliwości wykazania zgodności z prawem. Rzetelna analiza ryzyka po wystąpieniu naruszenia ochrony danych osobowych – oparta na uwzględnieniu przedstawionych powyżej czynników – pozwala administratorowi w sposób przejrzysty uzasadnić zarówno podjęcie, jak i zaniechanie określonych działań.

Dokumentowanie oceny ryzyka na podstawie obiektywnych kryteriów ma kluczowe znaczenie nie tylko dla bezpieczeństwa osób, których dane dotyczą, lecz i dla samego administratora. Właściwie udokumentowana analiza ryzyka to nie tylko obowiązek, ale również dowód dojrzałości organizacyjnej i świadomego podejścia do ochrony danych osobowych.

WZAJEMNE ODDZIAŁYWANIE DSA I RODO: EROD PRZYJMUJE WYTYCZNE

Podczas wrześniowego posiedzenia plenarnego Europejska Rada Ochrony Danych przyjęła wytyczne dotyczące wzajemnego oddziaływania między Aktem o usługach cyfrowych (DSA) a ogólnym rozporządzeniem o ochronie danych (RODO). Są to pierwsze wytyczne EROD skupione na relacji między RODO a niedawno przyjętym prawem cyfrowym UE.

DSA ma na celu uzupełnienie przepisów RODO, aby zapewnić najwyższy poziom ochrony praw podstawowych w przestrzeni cyfrowej. Jego głównym celem jest stworzenie bezpieczniejszego środowiska on-line, w którym chronione są prawa podstawowe wszystkich użytkowników, w tym prawo do wolności wypowiedzi. Dotyczy usług pośrednictwa internetowego, takich jak wyszukiwarki i platformy.

Wiele przepisów zawartych w DSA wiąże się z przetwarzaniem danych osobowych przez dostawców usług pośrednictwa. Wytyczne EROD wspierają spójne stosowanie DSA i RODO, o ile niektóre przepisy DSA dotyczą przetwarzania danych osobowych przez takich dostawców i zawierają odniesienia do pojęć i definicji z RODO.

Choć interpretacja DSA należy do właściwych organów, przy wsparciu Europejskiej Rady ds. Usług Cyfrowych oraz sądów UE, istnieje wiele przepisów, które odnoszą się do RODO. Należą do nich:

- systemy zgłaszania i działania, które umożliwiają osobom fizycznym lub podmiotom zgłaszanie nielegalnych treści
- systemy rekomendacyjne wykorzystywane przez platformy internetowe do automatycznego prezentowania określonych treści użytkownikom w określonym porządku lub z określoną widocznością
- przepisy zapewniające wysoki poziom prywatności, bezpieczeństwa i ochrony nieletnich oraz zakazujące reklam profilowanych opartych na ich danych
- przejrzystość reklam na platformach internetowych
- zakaz reklam profilowanych opartych na szczególnych kategoriach danych

Wytyczne EROD pomagają zrozumieć, jak stosować RODO w kontekście obowiązków wynikających z DSA.

EROD dostarcza również praktycznych wskazówek dotyczących współpracy między organami regulacyjnymi w celu skoordynowania egzekwowania przepisów, co zapewni większą pewność prawną dla dostawców usług pośrednictwa i ostatecznie ochroni prawa i wolności jednostek.

Wytyczne zostaną poddane konsultacjom publicznym, dając zainteresowanym stronom możliwość zgłaszania uwag i opinii.

Przewodnicząca EROD, Anu Talus, powiedziała: „Poprzez wyjaśnienie relacji między DSA a RODO te wytyczne stanowią istotny krok w kierunku zapewnienia spójnego i skutecznego cyfrowego kodeksu UE, a także pomogą w ochronie podstawowych praw i wolności jednostek. Mam nadzieję, że zainteresowane strony, w tym właściwe organy DSA, skorzystają z możliwości udziału w konsultacjach publicznych".

Dalsze działania w toku

Po publikacji pierwszych wytycznych dotyczących relacji między RODO a DSA trwają dalsze prace z innymi organami regulacyjnymi w celu wyjaśnienia nowego krajobrazu regulacyjnego i utrzymania spójnych zabezpieczeń ochrony danych osobowych. W tym kontekście EROD współpracuje z Komisją Europejską nad wspólnymi wytycznymi dotyczącymi relacji między Aktem o rynkach cyfrowych a RODO, a także nad wytycznymi dotyczącymi relacji między Aktem o sztucznej inteligencji a przepisami UE o ochronie danych.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Interplay between the DSA and the GDPR: EDPB adopts guidelines | European Data Protection Board

FRANCUSKI ORGAN NADZORCZY: PLIKI COOKIES I REKLAMY WSTAWIANE MIĘDZY E-MAILE – GOOGLE UKARANE ADMINISTRACYJNĄ KARĄ FINANSOWĄ 325 MLN EURO PRZEZ CNIL

Geneza sprawy

W następstwie skargi złożonej przez organizację None Of Your Business (NOYB) 24 sierpnia 2022 r. francuski organ nadzorczy CNIL przeprowadził kilka kontroli w latach 2022 i 2023 dotyczących usługi poczty Gmail oraz procesu zakładania konta Google.

Kluczowe ustalenia

Śledztwo wykazało, że Google Ireland Limited oraz Google LCC wyświetlały reklamy w formie e-maili wśród wiadomości w zakładkach „Promocje" i „Społeczności" w usłudze Gmail. CNIL uznał, że wyświetlanie takich reklam wymagało zgody użytkowników Gmaila, zgodnie z artykułem L. 34-5 francuskiego Kodeksu Pocztowego i Komunikacji Elektronicznej.

Ponadto CNIL stwierdził, że podczas tworzenia konta Google użytkownicy byli zachęcani do wyboru plików cookies związanych z wyświetlaniem spersonalizowanych reklam kosztem plików służących do wyświetlania reklam ogólnych. Użytkownicy nie byli jasno informowani, że korzystanie z plików cookies do celów reklamowych było warunkiem dostępu do usług Google. Zgoda uzyskana w tym kontekście nie była więc ważna, co stanowiło naruszenie francuskiej ustawy o ochronie danych osobowych.

Decyzja

Za te dwa naruszenia CNIL wydał publiczną decyzję nakładającą:

- Dwie administracyjne kary finansowe o łącznej wysokości 325 mln euro na Google (200 mln euro na Google LLC oraz 125 mln euro na Google Ireland Limited);

- Nakaz wdrożenia, w ciągu sześciu miesięcy, środków mających na celu zaprzestanie wyświetlania reklam między wiadomościami w skrzynkach użytkowników Gmaila bez uprzedniej zgody oraz zapewnienie ważnej zgody użytkowników na stosowanie plików cookies podczas tworzenia konta Google. W przypadku niewykonania nakazu każda z firm będzie zobowiązana do zapłaty kary w wysokości 100 mln euro za każdy dzień opóźnienia.

Źródło:

Komunikat Francuskiego Organu Ochrony Danych

Cookies and advertisements inserted between emails: GOOGLE fined 325 million euros by the CNIL | CNIL

TELEMARKETING: WŁOSKI ORGAN NADZORCZY NAKŁADA ADMINISTRACYJNE KARY FINANSOWE W WYSOKOŚCI 3 MLN EURO NA FIRMĘ ENERGETYCZNĄ I 850 TYS. EURO NA ZAANGAŻOWANE AGENCJE

Geneza sprawy

Włoski organ nadzorczy wykonując swoje uprawnienia dochodzeniowe i kontrolne na podstawie włoskiego prawa o ochronie danych osobowych, przeprowadził szereg czynności kontrolnych we współpracy ze specjalnym oddziałem ds. ochrony prywatności i oszustw technologicznych Guardia di Finanza po otrzymaniu skargi od redaktora programu telewizyjnego.

Skarga dotyczyła zjawiska już znanego włoskiemu organowi nadzorczemu, czyli działalności nieautoryzowanych call centers (działających bez formalnego upoważnienia od klientów i niefigurujących w Rejestrze Operatorów Komunikacyjnych, prowadzonym przez krajowy organ ds. komunikacji), które posiadały listy danych osobowych osób kontaktowanych telefonicznie w celu zaproponowania im aktywacji usług telefonicznych lub energetycznych, również poprzez zmianę operatora.

Kluczowe ustalenia

Śledztwo ujawniło istotne dowody nielegalnych działań polegających na wykorzystaniu list klientów, którzy niedawno zmienili dostawcę energii. Operatorzy call centers kontaktowali się z nimi, sugerując nieistniejące usterki techniczne przy zmianie operatora i, wzbudzając obawy o potencjalne straty finansowe, nakłaniali do zawarcia nowej umowy.

System ten opierał się na wykorzystaniu list danych osobowych pozyskanych od innych firm należących do tej samej sieci bez uzyskania konkretnej zgody i bez wcześniejszego poinformowania osób, których dane dotyczyły. Listy te zawierały szczegółowe informacje o klientach.

Śledztwo wykazało również, że przedstawiciele firmy energetycznej utrzymywali bezpośredni i stały kontakt z osobami prowadzącymi agresywne działania telemarketingowe. Jednak po uzyskaniu informacji o wynikach dochodzenia firma energetyczna cofnęła upoważnienie agencji zaangażowanej w incydenty i wdrożyła środki naprawcze mające na celu podniesienie poziomu bezpieczeństwa operacji przetwarzania danych realizowanych w jej imieniu.

Decyzja

Włoski organ nałożył administracyjne kary finansowe w wysokości 3 mln euro na firmę energetyczną oraz 850 tys. euro na zaangażowane agencje w związku z naruszeniami artykułów 5(1), 6, 7, 13, 24, 25, 28 i 32 RODO oraz art. 130 włoskiego Kodeksu ochrony danych osobowych.

Organ nakazał również firmie energetycznej poinformowanie wszystkich osób, których dane nielegalnie trafiły do jej systemów, o wynikach postępowania oraz zweryfikowanie istnienia podwykonawców, którzy nie zostali należycie zakontraktowani. Wszystkim zaangażowanym agencjom nakazano zaprzestanie korzystania z list kontaktowych, których legalności nie mogą udowodnić.

Źródło:

Komunikat Włoskiego Organu Ochrony Danych

COMUNICATO STAMPA - Telemarketing: dal Garante privacy sanzioni per... - Garante Privacy

RAID 2025: REGULACJA JAKO SIŁA NAPĘDOWA INNOWACJI – UDZIAŁ UODO W MIĘDZYNARODOWEJ DEBACIE O PRZYSZŁOŚCI OCHRONY DANYCH

28–29 września 2025 r. w Brukseli odbyła się konferencja RAID (Regulation of AI, Internet & Data), która zgromadziła przedstawicieli regulatorów, instytucji unijnych, firm technologicznych oraz ekspertów z całego świata. W wydarzeniu uczestniczyli prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski oraz Krzysztof Król, zastępca dyrektor Departamentu Współpracy Międzynarodowej UODO.

RAID 2025 – o przyszłości regulacji cyfrowych

Konferencja RAID 2025 była poświęcona wyzwaniom związanym z regulacją sztucznej inteligencji, internetu i danych osobowych w kontekście dynamicznego rozwoju technologii cyfrowych. W ramach siedmiu paneli dyskusyjnych poruszono kluczowe tematy dotyczące równowagi między ochroną prywatności a innowacyjnością, międzynarodowymi transferami danych, interoperacyjnością systemów oraz wpływem regulacji na sektor zdrowia i gospodarkę cyfrową.

W pierwszym panelu podkreślono, że choć globalne porozumienie w sprawie AI jest mało realne, konieczne są mechanizmy koordynacji działań regulatorów. Zwrócono uwagę na potrzebę szkoleń i budowania kompetencji kontekstowych w zakresie stosowania przepisów, a także na wyzwania związane z nakładaniem się regulacji takich jak AIA, DGA, DA i RODO.

Panel trzeci skupił się na międzynarodowych przepływach danych. Przedstawiciele firm takich jak Microsoft i Deutsche Telekom zaprezentowali swoje podejście do zapewnienia zgodności z przepisami, m.in. poprzez lokalizację serwerów w EOG, stosowanie klauzul umownych i wewnętrznych zasad BCR. EIOD zwrócił uwagę na napięcia związane z lokalizacją danych i potrzebę kompatybilnych systemów prawnych.

W panelu poświęconym sektorowi zdrowia dyskutowano o interakcji między AI Act, GDPR i Europejską Przestrzenią Danych Zdrowotnych (EHDS). Eksperci wskazywali na brak spójności w podejściu do danych zanonimizowanych i pseudonimizowanych oraz potrzebę jasnych regulacji dotyczących roli administratorów i inspektorów ochrony danych w badaniach klinicznych.

Ostatni panel, zatytułowany „Can Regulation Help Drive Innovation?”, był poświęcony roli regulatorów w wspieraniu rozwoju technologicznego. Dyskutowano o tym, jak ramy prawne mogą sprzyjać inwestycjom i współpracy międzysektorowej, a także o roli zasad FAIR (findability, accessibility, interoperability, reusability) w budowaniu efektywnych ekosystemów danych.

Stanowisko Prezesa UODO

Podczas konferencji RAID 2025 prezes Mirosław Wróblewski uczestniczył w panelu poświęconym wpływowi regulatorów na innowacje. W odpowiedzi na pytanie o związek prywatności i innowacji, podkreślił potrzebę wydawania interpretacji łączących różne sektory. Zaznaczył, że ochrona danych musi iść w parze z zapewnieniem potencjału konkurencyjnego. Wskazał również na konieczność analizowania prawa przez wszystkie organy włączone do systemu regulacyjnego, a także na znaczenie orzeczeń sądowych, takich jak sprawa Bundeskartellamt, które wskazują na potrzebę zmiany podejścia regulacyjnego.

Prezes UODO zwrócił uwagę na potencjał regulacyjnych piaskownic, które mogą przynieść zmniejszony zakres nadzoru organów ochrony danych, otwierając dostęp do danych i związany z nimi potencjał. Podkreślił znaczenie kompleksowej i spójnej interpretacji przepisów oraz współpracy właściwych organów i interesariuszy. Zaznaczył również, że konieczne jest zapewnienie większej koordynacji i spójności między organami krajowymi i europejskimi oraz opracowanie przepisów proceduralnych dotyczących współpracy w celu wymiany danych między regulatorami. Budowanie pozytywnej atmosfery sprzyjającej innowacjom to zadanie wszystkich zainteresowanych stron.

WARSZTATY META „DESIGN JAM" W BERLINIE – REFLEKSJE Z PERSPEKTYWY OCHRONY DANYCH OSOBOWYCH

1 października 2025 r. przedstawicielka Departamentu Współpracy Międzynarodowej UODO uczestniczyła w warsztatach „Design Jam" zorganizowanych przez firmę Meta w Berlinie. Spotkanie miało charakter praktyczno-konsultacyjny i odbywało się zgodnie z zasadą Chatham House Rule, co sprzyjało otwartej wymianie opinii między ekspertami z różnych krajów i sektorów.

Tematem przewodnim wydarzenia były wyzwania związane z generatywną sztuczną inteligencją (GenAI), w szczególności w kontekście przejrzystości i kontroli nad przetwarzaniem danych osobowych. Uczestnicy mieli okazję wspólnie analizować scenariusze związane z komunikacją zasad prywatności, personalizacją usług, ze zgodą na nagrywanie dźwięku oraz z projektowaniem interfejsów głosowych.

Udział przedstawicielki UODO umożliwił zaprezentowanie polskiej perspektywy w zakresie ochrony danych osobowych oraz wymianę doświadczeń z innymi regulatorami i ekspertami. Spotkanie stanowiło okazję do pogłębienia dialogu na temat zgodności rozwiązań technologicznych z RODO oraz promowania dobrych praktyk w projektowaniu usług opartych na AI.

Warsztaty pokazały, że otwarta współpraca między sektorem technologicznym a organami ochrony danych osobowych jest kluczowa dla budowania zaufania i odpowiedzialnego rozwoju innowacyjnych rozwiązań.

PRIVACY DAYS PRAGUE 2025: O PROCEDURACH, AI I PRZYSZŁOŚCI OCHRONY DANYCH

1 października 2025 r. w Pradze odbyła się dziewiąta edycja konferencji Privacy Days – największego wydarzenia w Czechach poświęconego ochronie danych osobowych i gospodarce cyfrowej. Tegoroczna odsłona, zorganizowana przez Stowarzyszenie na rzecz Ochrony Danych Osobowych, zgromadziła ekspertów, praktyków i przedstawicieli administracji z całej Europy w celu omówienia najnowszych wyzwań regulacyjnych i technologicznych w obszarze prywatności. W wydarzeniu uczestniczył również Krzysztof Król, zastępca dyrektor Departamentu Współpracy Międzynarodowej Urzędu Ochrony Danych Osobowych, który przedstawił doświadczenia UODO w zakresie kodeksów postępowania i mechanizmów certyfikacji.

AI, biometria i dzieci w centrum uwagi

Jednym z głównych tematów konferencji były wyzwania związane z przetwarzaniem danych w kontekście sztucznej inteligencji. Jak zauważył Petr Jager, prawnik specjalizujący się w ochronie danych i zastępca dyrektora czeskiego organu ochrony danych, przetwarzanie danych biometrycznych w połączeniu z AI – zwłaszcza w kontekście monitoringu – staje się coraz trudniejsze do oceny prawnej. Wskazał również na napięcie między zasadą minimalizacji danych a potrzebami innowacji, które, jego zdaniem, jest nieuniknione. Kluczowym czynnikiem pozostają zasoby, jakimi dysponują organy ochrony danych.

W kontekście międzynarodowym Petr Jager podkreślił trzy priorytetowe obszary zainteresowania Europejskiej Rady Ochrony Danych: przetwarzanie danych przez AI, ochrona dzieci w internecie oraz mechanizmy weryfikacji wieku.

Reforma prawa proceduralnego

Znaczną część dyskusji poświęcono reformie prawa proceduralnego w zakresie ochrony danych. Petr Jager zwrócił uwagę, że czeskie przepisy nadal nie są w pełni zgodne z RODO, a praktyka orzecznicza – m.in. wyrok czeskiego Naczelnego Sądu Administracyjnego z 2024 r. – wskazuje na potrzebę zmian.

Obecne terminy (30–60 dni) są niewystarczające dla przeprowadzenia pełnego postępowania, które często wymaga wstępnej analizy, dwóch etapów dochodzenia i formalnego postępowania administracyjnego.

W odpowiedzi na te wyzwania Słowacja przygotowała projekt nowej ustawy o ochronie danych osobowych. Jak poinformowała Jana Sisakowa z Ministerstwa Sprawiedliwości Słowacji, nowe przepisy obejmują m.in. uproszczone procedury dla kodeksów postępowania i certyfikacji, możliwość stosowania środków tymczasowych podczas kontroli oraz wprowadzenie skarg jako podstawy wszczęcia postępowania. Nowa ustawa o ochronie danych w sektorze egzekwowania prawa (LED) ma wejść w życie 1 stycznia 2026 r., a Ministerstwo Sprawiedliwości stanie się jednym z siedmiu organów właściwych w tym zakresie.

Europejskie i międzynarodowe orzecznictwo

Ważnym elementem konferencji była analiza orzecznictwa Trybunału Sprawiedliwości UE oraz sądów krajowych. Nils G. Indahl z Norwegii omówił sprawę rejestrów chrztów (C-12/25), w której kluczowe znaczenie ma motyw 55 RODO. Norwegia powołała specjalną grupę roboczą ds. interpretacji tego przepisu w różnych wersjach językowych. Wskazano również na sprawę Telenor, w której sąd krajowy obniżył karę ze względu na długi czas trwania postępowania – bez konsultacji z sądem EOG.

Alenka Antloga, inspektorka ochrony danych z ICO Słowenia, przedstawiła przegląd aktualnych dokumentów EDPB oraz orzeczeń TSUE, w tym spraw C-141/12, C-372/12, C-579/21 (Pannki – Bank) i C-203/22. Podkreśliła znaczenie wspólnej interpretacji przepisów i konieczność dalszego rozwoju praktyki orzeczniczej dotyczącej ochrony danych.

SYSTEM WJAZDU/WYJAZDU (EES) – NOWE NARZĘDZIE ZARZĄDZANIA GRANICAMI Z POSZANOWANIEM OCHRONY DANYCH OSOBOWYCH

12 października br. państwa strefy Schengen uruchomiły System Wjazdu/Wyjazdu (Entry/Exit System – EES) – wielkoskalowy system informacyjny, ustanowiony w celu zapobiegania nielegalnej migracji, zwiększenia bezpieczeństwa wewnętrznego oraz usprawnienia zarządzania granicami zewnętrznymi Schengen. Jego uruchomienie stanowi jeden z kluczowych kroków we wdrażaniu nowej generacji systemów informacyjnych w obszarze zarządzania granicami i zapewnienia bezpieczeństwa (tzw. Pakiet dotyczący inteligentnych granic).

System Wjazdu/Wyjazdu zastąpi dotychczasową praktykę stemplowania paszportów przy przekraczaniu granic zewnętrznych strefy Schengen. Dane dotyczące wjazdu i wyjazdu obywateli państw trzecich – zarówno podróżujących z wizą krótkoterminową, jak i zwolnionych z obowiązku wizowego – będą rejestrowane elektronicznie. Dzięki temu rozwiązaniu odprawy na granicach mają przebiegać szybciej, a zarządzanie ruchem granicznym ma być bardziej efektywne. Wdrażanie systemu będzie się odbywać stopniowo: początkowo obejmie ok. 10 proc. przejść granicznych, a w ciągu sześciu miesięcy od daty uruchomienia rejestracja danych ma objąć wszystkie przejścia.

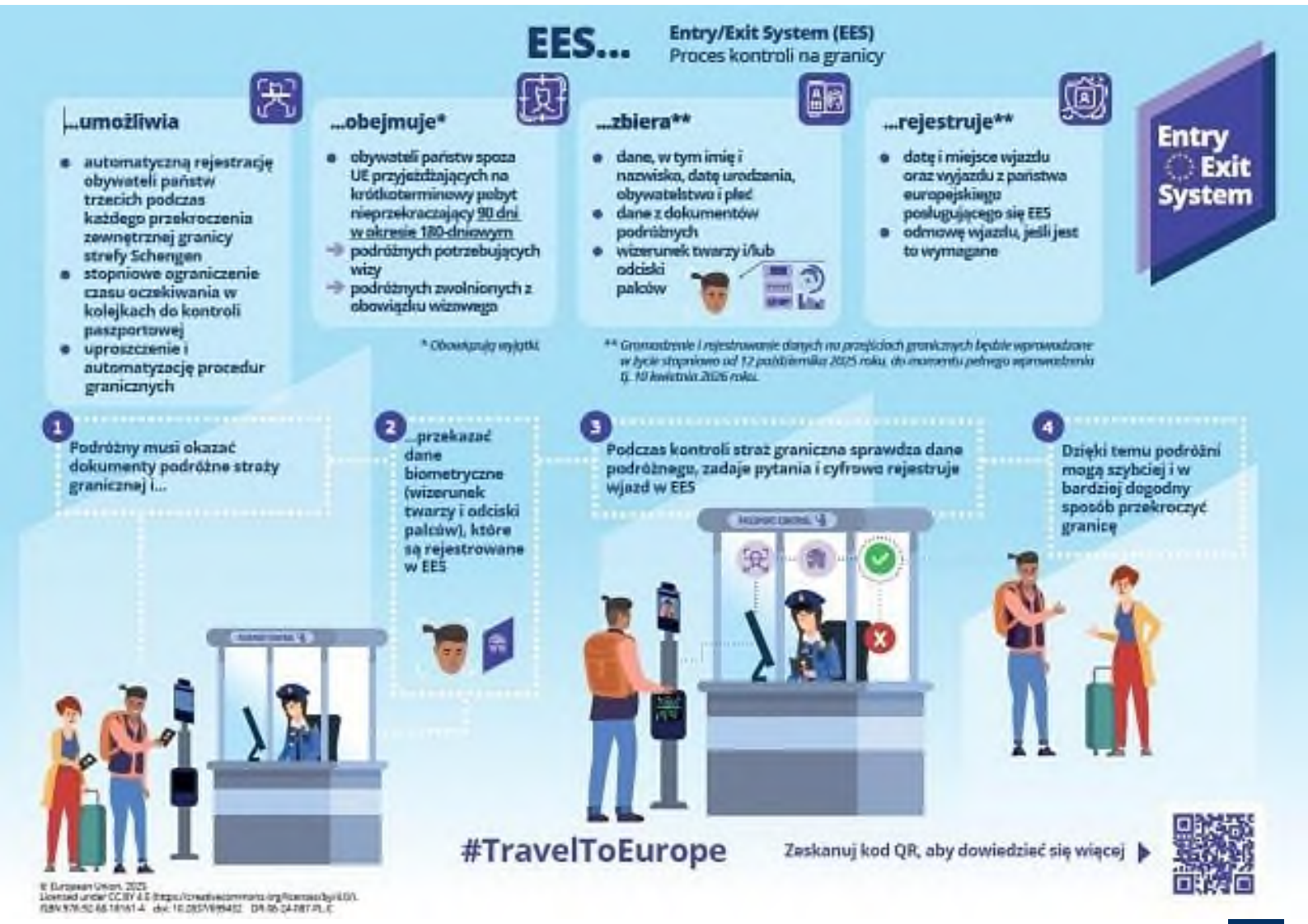
EES będzie przetwarzać dane osobowe niezbędne do identyfikacji podróżnych i rejestrowania ich przekroczeń granicy, w tym imię i nazwisko, datę i miejsce urodzenia, daty wjazdu i wyjazdu, a także dane biometryczne – wizerunek twarzy i odciski palców. Ze względu na szczególnie wrażliwy charakter tych informacji kluczowe znaczenie ma zapewnienie osobom fizycznym możliwości skutecznego korzystania z przysługujących im praw oraz utrzymanie wysokiego poziomu nadzoru nad przetwarzaniem danych.

Przetwarzanie danych w EES odbywa się w ramach dwóch reżimów ochrony danych osobowych. W odniesieniu do działań organów granicznych i migracyjnych stosowane jest ogólne rozporządzenie o ochronie danych (RODO), natomiast przetwarzanie danych do celów zapobiegania i zwalczania przestępczości odbywa się zgodnie z dyrektywą (UE) 2016/680 (tzw. DODO), wdrożoną w Polsce ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i ze zwalczaniem przestępczości.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Ochrona danych osobowych pozostaje prawem podstawowym, którego poszanowanie jest integralnym elementem funkcjonowania Systemu Wjazdu/Wyjazdu. Osoby, których dane są przetwarzane w EES, mają prawo dostępu do swoich danych, ich sprostowania, uzupełnienia lub usunięcia, a także ograniczenia przetwarzania. Organy przetwarzające dane – takie jak straż graniczna, służby migracyjne czy, w określonych przypadkach, organy ścigania – są zobowiązane do zapewnienia skutecznych mechanizmów realizacji tych praw.

W Polsce nadzór nad przetwarzaniem danych osobowych w EES sprawuje Prezes Urzędu Ochrony Danych Osobowych. System objęty jest także unijnym mechanizmem skoordynowanego nadzoru, w ramach którego współpracują krajowe organy ochrony danych i Europejski Inspektor Ochrony Danych. Kooperacja ta odbywa się w ramach Komitetu Skoordynowanego Nadzoru, który służy wymianie informacji, wzajemnej pomocy przy kontrolach, analizie wspólnych problemów interpretacyjnych i praktycznych oraz opracowywaniu wspólnych zaleceń. Komitet wspiera również działania na rzecz podnoszenia świadomości w zakresie praw osób, których dane są przetwarzane w systemie EES.



OBLICZANIE CYKLU AUDYTU W WIELKOSKALOWYCH SYSTEMACH INFORMATYCZNYCH UE

Wielkoskalowe systemy informatyczne Unii Europejskiej – takie jak System Informacyjny Schengen (SIS), Wizowy System Informacyjny (VIS), System Wjazdu/Wyjazdu (EES) czy Europejski System Informacji o Podróży oraz Zezwoleń na Podróż (ETIAS) – stanowią kluczowe narzędzia wspierające zarządzanie granicami, politykę wizową i bezpieczeństwo w strefie Schengen. Ze względu na skalę przetwarzania danych osobowych oraz ich znaczenie dla ochrony praw podstawowych akty prawne regulujące funkcjonowanie tych systemów przewidują obowiązek regularnych audytów prowadzonych przez właściwe organy nadzorcze.

Przepisy unijne ustanawiają szczegółowe wymogi dotyczące częstotliwości przeprowadzania audytów. W przypadku SIS, VIS oraz w ramach interoperacyjności minimalna częstotliwość wynosi raz na cztery lata, natomiast dla systemów EES i ETIAS – co najmniej raz na trzy lata. Przestrzeganie tych cykli audytowych ma istotne znaczenie nie tylko z punktu widzenia zapewnienia ciągłości nadzoru, lecz także w kontekście unijnego mechanizmu Ewaluacji Schengen. W trakcie tych ewaluacji eksperci z Komisji Europejskiej i państw członkowskich oceniają, czy organy ochrony danych prawidłowo realizują swoje obowiązki w zakresie nadzoru nad przetwarzaniem danych w systemach wielkoskalowych.

W związku z powyższym Komitet Skoordynowanego Nadzoru (Coordinated Supervision Committee – CSC) opracował wspólne zalecenia dotyczące sposobu obliczania cyklu audytu oraz interpretacji przepisów unijnych w tym zakresie. Zgodnie z tymi wytycznymi pełne cztery lata kalendarzowe bez zakończonego audytu w SIS, VIS lub w ramach interoperacyjności (oraz trzy lata w odniesieniu do EES i ETIAS) należy uznać za niezgodne z obowiązującymi regulacjami. Wynika to bezpośrednio z brzmienia odpowiednich aktów prawnych UE, które określają maksymalne dopuszczalne odstępy między kolejnymi audytami.

Cykl audytu powinien być obliczany w latach, zgodnie z art. 3 ust. 2 lit. c) rozporządzenia Rady nr 1182/71, określającego zasady ustalania okresów, dat i terminów w aktach przyjętych przez instytucje Unii Europejskiej.

Kluczowe znaczenie ma także ustalenie momentu, od którego należy liczyć początek kolejnego cyklu. Za taki punkt odniesienia uznaje się datę zakończenia audytu, rozumianą jako moment, w którym zrealizowano wszystkie zaplanowane działania audytowe. Może to być ostatni dzień wizyty na miejscu, dzień podpisania sprawozdania z audytu lub inny moment wynikający z krajowych procedur i stosowanych międzynarodowych standardów.

Jednocześnie, biorąc pod uwagę niezależny status organów nadzorczych, zaleca się pozostawienie im pewnej swobody w określaniu, kiedy audyt uznaje się za zakończony – zwłaszcza w sytuacjach, gdy występują nieprzewidziane okoliczności, takie jak opóźnienia proceduralne, konieczność uzyskania dodatkowych informacji czy ograniczenia operacyjne. Elastyczność ta nie może jednak prowadzić do przekroczenia maksymalnych odstępów czasowych, określonych w aktach prawnych UE.

Organy nadzorcze pozostają właściwe do samodzielnego ustalania terminu rozpoczęcia kolejnego audytu, o ile mieści się on w granicach przewidzianych przepisami. Przepisy unijne określają bowiem minimalną częstotliwość kontroli, lecz nie nakładają obowiązku ich przeprowadzania według sztywnego harmonogramu. Ta autonomia ma zasadnicze znaczenie dla uwzględnienia krajowej specyfiki działania organów ochrony danych, w tym dostępnych zasobów, priorytetów w planowaniu nadzoru oraz wyników poprzednich audytów.

Ujednolicone podejście do sposobu obliczania cyklu audytu w systemach wielkoskalowych sprzyja spójności praktyk nadzorczych w całej Unii Europejskiej i wzmacnia zaufanie do skuteczności ochrony danych osobowych w ramach zintegrowanego zarządzania granicami.

URZĄD OCHRONY DANYCH OSOBOWYCH

Prezes UODO zaprasza na wydarzenia edukacyjne, zaplanowane na ostatni kwartał 2025 r. Wszystkie będzie można obejrzeć on-line. Będą dotyczyć szerokiego spektrum tematów, tak aby każdy znalazł coś ciekawego dla siebie. Serdecznie zapraszamy.

- **Seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO"**

Termin: **6 listopada** 2025 r., godz. 10:00–15:00

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

Organizatorzy: Prezes Urzędu Ochrony Danych Osobowych, Stowarzyszenie Sędziów Polskich „Iustitia" oraz Naczelna Rada Adwokacka
Formuła: hybrydowa

Wydarzenie będzie przestrzenią do otwartego dialogu, w którym przedstawiciele świata prawa, nauki i praktyki będą mogli podzielić się swoimi obserwacjami i propozycjami rozwiązań, odpowiadającymi na wyzwania związane z dynamicznym rozwojem orzecznictwa w obszarze ochrony danych osobowych. Stanie się również ważnym głosem w dyskusji dotyczącej doniosłej roli sądów i Prezesa UODO w kształtowaniu orzecznictwa jednolitego i spójnego z ogólnym rozporządzeniem o ochronie danych.

- **Konferencja „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach"**

Termin: **19 listopada** 2025 r., godz. 10:00–14:30

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

Organizatorzy: Urząd Ochrony Danych Osobowych oraz Społeczny Zespół Ekspertów przy Prezesie UODO
Formuła: hybrydowa

W dobie szybkiego przepływu informacji i dynamicznego rozwoju mediów ochrona danych osobowych staje się jednym z kluczowych wyzwań współczesnego dziennikarstwa. Coraz częściej dziennikarze stają przed dylematem dotyczącym tego, jak rzetelnie informować opinię publiczną, jednocześnie respektując prawo do prywatności osób, których dane przetwarzają.
W programie konferencji zostały przewidziane trzy panele dyskusyjne z udziałem ekspertów prawa prasowego, przedstawicieli mediów, praktyków ochrony danych oraz reprezentantów instytucji nadzorczych, podczas których poruszymy kwestie dotyczące misji mediów w kontekście prawa do prywatności, granic ujawniania tożsamości w materiałach prasowych czy sposobów ochrony danych osobowych przez media. Celem konferencji jest stworzenie przestrzeni do dialogu i wypracowania wspólnych standardów działania, które będą zgodne nie tylko z obowiązującym prawem, ale przede wszystkim będą służyć etycznemu dziennikarstwu.

URZĄD OCHRONY DANYCH OSOBOWYCH

- **Konferencja „Nowe horyzonty biometrii – bezpieczeństwo, tożsamość, rozwój“**

Termin: **26 listopada** 2025 r., godz. 10:00–16:00

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

Organizatorzy: Urząd Ochrony Danych Osobowych, Fundacja AI One Health

Formuła: hybrydowa

Oblicza biometrii, jej dotychczasowe osiągnięcia i perspektywy rozwoju, a także prawne aspekty jej wykorzystania – to główne tematy tego wydarzenia. Eksperci przedstawią uczestnikom możliwości i korzyści, jakie niesie z sobą wdrożenie oraz stosowanie technologii biometrycznych, oraz przykłady wdrożeń rozwiązań biometrycznych. Skuteczne zarządzanie danymi biometrycznymi wymaga bowiem równowagi między innowacjami a ochroną prywatności, co oznacza ich ochronę przed nieautoryzowanym dostępem i konieczność określenia wyraźnego celu.

- **Konferencja „Nowe wyzwania prawne: regulacje, zadania regulatorów i ochrona danych w 2025 roku”**

Termin: **27 listopada** 2027 r., godz. 10:00–14:30

Miejsce: **Centrala ZUS** przy ul. Szamockiej 3/5, Warszawa

Organizatorzy: Urząd Ochrony Danych Osobowych oraz Zakład Ubezpieczeń Społecznych
Formuła: hybrydowa

Konferencja obejmie tematykę nowych regulacji prawnych, które zaczęły obowiązywać w 2025 r., ze szczególnym uwzględnieniem roli instytucji, które uczestniczą w ich wdrażaniu. Paneliści zabiorą głos ws. odpowiedzialności regulatorów w zakresie nadzoru nad rynkiem danych i zapewnienia przez nich bezpieczeństwa prawnego. Istotnym zagadnieniem będzie ochrona danych osobowych i nowe wyzwania, jakie niesie z sobą dalsza cyfryzacja.

URZĄD OCHRONY DANYCH OSOBOWYCH

- **Konferencja „Nowe zadania UODO" (tytuł niepotwierdzony)**

Termin: **1 grudnia** 2025 r., godz. 10:00–14:00

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

Organizatorzy: Urząd Ochrony Danych Osobowych
Formuła: hybrydowa

Konferencja ta zawiera się w cyklu wydarzeń poświęconych nowym zadaniom Prezesa Urzędu Ochrony Danych Osobowych w zakresie zarządzania danymi. Projekt ustawy o zarządzaniu danymi, która ma na celu wdrożenie unijnego Aktu w sprawie zarządzania danymi (DGA), przyznaje Prezesowi UODO nowe zadania i kompetencje związane m.in. z nadzorem nad instytucjami pośredniczącymi w udostępnianiu danych. Tej tematyce będzie poświęcona konferencja.

- **Konferencja „Rola Konwencji ramowej Rady Europy o sztucznej inteligencji w ochronie prywatności i danych osobowych – wyzwania prawne, etyczne i społeczne w erze sztucznej inteligencji" (konferencja prowadzona po angielsku, tłumaczenie na polski tylko dla uczestników stacjonarnych)**

Termin: **10 grudnia** 2025 r., godz. 10:00–14:00

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

Organizatorzy: Prezes Urzędu Ochrony Danych Osobowych, Społeczny Zespół Ekspertów przy Prezesie UODO, Komitet Rady Europy ds. Sztucznej Inteligencji (CAI), Komitet Konwencji 108 (T-PD) oraz Europejska Komisja na rzecz Efektywności Wymiaru Sprawiedliwości (CEPEJ)
Formuła: hybrydowa

W trakcie konferencji planowane są wystąpienia przedstawicieli Rady Europy oraz polskich i zagranicznych ekspertów w dziedzinie ochrony danych osobowych i sztucznej inteligencji. Wezmą oni udział w trzech panelach dyskusyjnych, dotyczących głównych aspektów ochrony danych w świetle Konwencji Rady Europy o sztucznej inteligencji, praktycznych aspektów wdrażania i oceny ryzyka związanego z przetwarzaniem danych przez sztuczną inteligencję oraz wpływu sztucznej inteligencji na wymiar sprawiedliwości i prawa obywateli.

6 EDUKACJA

PREZES UODO WSPIERA KAMPANIĘ „DZIECIŃSTWO BEZ PRZEMOCY 2025”

Prezes Urzędu Ochrony Danych Osobowych wspiera kampanię Rzecznik Praw Dziecka „**Dzieciństwo bez Przemocy 2025**”, mobilizującą do zapobiegania krzywdzeniu dzieci. Zespół UODO z pełnym przekonaniem popiera inicjatywę, mającą na celu ochronę praw dziecka oraz budowanie świadomości społecznej na temat przemocy wobec najmłodszych.

W ramach wsparcia kampanii, koordynowanej przez Fundację Dajemy Dzieciom Siłę, Prezes UODO zachęca do udziału w webinariach dla dorosłych i rodziców, mających na celu budowanie świadomości społecznej na temat przemocy wobec najmłodszych. O kampanii, trwającej w okresie 10.2025–19.11.2025 r., będziemy informować podczas wydarzeń organizowanych przez UODO, a także włączymy się w inne działania wspierające tę inicjatywę, tak ważną dla przestrzegania praw najmłodszych.

PROGRAM „TWOJE DANE – TWOJA SPRAWA”

W ramach kampanii promującej program „Twoje dane – Twoja sprawa” informacja dotycząca rekrutacji do programu „TD–TS” została wyświetlona na ekranach komunikacji miejskiej w Warszawie we wrześniu 2025 r. Natomiast w październiku planowana jest emisja tego materiału w komunikacji miejskiej w Krakowie.

Działanie to podejmujemy w ramach współpracy z urzędami miasta w celu zachęcenia szkół i placówek doskonalenia nauczycieli do udziału w XVI edycji programu „Twoje dane – Twoja sprawa”. Dziękujemy Urzędowi m.st. Warszawa oraz Urzędowi Miasta Kraków za wsparcie.

6 EDUKACJA

KONFERENCJA „Prywatność i sztuczna inteligencja w edukacji" – konferencja dla nauczycieli i dyrektorów szkół

W jaki sposób wspierać dzieci i młodzież w ochronie prywatności w erze dynamicznego rozwoju technologii cyfrowych? Jak rozmawiać z uczniami o ochronie prywatności, higienie cyfrowej i odpowiedzialnym korzystaniu z internetu? Na co zwracać uwagę przy wdrażaniu rozwiązań opartych na sztucznej inteligencji w edukacji?

Na te i wiele innych pytań odpowiadali eksperci podczas konferencji szkoleniowej **„Prywatność i sztuczna inteligencja w edukacji"**, zorganizowanej przez Urząd Ochrony Danych Osobowych. Wydarzenie odbyło się 22–23 października 2025 r. w formule hybrydowej.

Cel wydarzenia
Konferencja miała na celu podniesienie kompetencji nauczycieli w zakresie ochrony danych osobowych oraz odpowiedzialnego korzystania z nowoczesnych technologii. Wydarzenie umożliwiło zdobycie aktualnej wiedzy, rozwinięcie praktycznych umiejętności oraz wymianę doświadczeń, co przyczyni się do zwiększenia efektywności działań edukacyjnych z dziećmi i młodzieżą.

Program konferencji
- **22 października 2025 r.** – Część I: „Sztuczna inteligencja i ochrona danych osobowych w edukacji"
- **23 października 2025 r.** – Część II: „Prywatność ucznia w cyfrowym świecie. Dobre praktyki w edukacji"

Przez dwa dni uczestnicy mieli okazję wysłuchać wystąpień ekspertów ds. sztucznej inteligencji, edukacji, ale również liderów programu „Twoje dane – Twoja sprawa", którzy od lat biorą w nim udział i z zaangażowaniem dzielą się swoimi doświadczeniami oraz wiedzą.

Wśród zaproszonych gości znaleźli się:
- Katarzyna Lubnauer – Sekretarz Stanu w Ministerstwie Edukacji Narodowej
- Monika Horna-Cieślak – Rzeczniczka Praw Dziecka
- Posłanka Monika Rosa – Przewodnicząca Komisji Sejmowej ds. Dzieci i Młodzieży
- Joanna Bochniarz – Prezeska Fundacji Polskie Porty Lotnicze
- Magdalena Bigaj – Prezeska Fundacji Instytutu Cyfrowego Obywatelstwa
- r. pr. Maciej Groń – kierownik Działu Analiz Strategicznych i Budowania Świadomości w NASK – Państwowym Instytucie Badawczym
- Piotr Otrębski – rzecznik prasowy, zastępca dyrektora Departamentu Komunikacji w Ministerstwie Edukacji Narodowej
- Kamil Śliwowski – edukator kompetencji cyfrowych

6 EDUKACJA

KONFERENCJA „Prywatność i sztuczna inteligencja w edukacji" – konferencja dla nauczycieli i dyrektorów szkół

W konferencji uczestniczyli przedstawiciele szkół biorących udział w Programie „Twoje dane – Twoja sprawa" – laureatki konkursów organizowanych przez Prezesa UODO oraz dr Joanna Gnutek, nauczycielka Szkoły Podstawowej nr 23 w Lublinie – laureatka Nagrody im. Michała Serzyckiego, przyznawanej za szczególne osiągnięcia w dziedzinie edukacji o ochronie danych osobowych. Są to nauczycielki i dyrektorki szkół niezwykle zaangażowane w działania edukacyjne wśród dzieci i młodzieży, którzy wspierają misję UODO od wielu lat.

XVI edycja programu „Twoje dane – Twoja sprawa"

Konferencja zainaugurowała XVI edycję ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa", skierowanego do szkół podstawowych, ponadpodstawowych oraz placówek doskonalenia nauczycieli. Program wspiera budowanie świadomości uczniów w zakresie bezpieczeństwa informacji, ochrony prywatności oraz odpowiedzialnego korzystania z technologii cyfrowych.

UODO RUSZA W KRAJ

URZĄD OCHRONY DANYCH OSOBOWYCH

W październiku odwiedziliśmy kolejne województwa w ramach akcji „UODO rusza w kraj", tj. województwo warmińsko-mazurskie i lubuskie. Zorganizowane w tych województwach spotkania miały na celu nie tylko przybliżenie problematyki ochrony danych osobowych mieszkańcom tych województw, ale również skierowanie przekazu do przedstawicieli administracji publicznej, sektora szkolnictwa, biznesu i organizacji pozarządowych z regionu.

UODO RUSZA W KRAJ

Przypominamy, że UODO na stałe zmienił 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 je zaktualizować.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl