URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 06/06/25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

4 czerwca obchodziliśmy Dzień Wolności i Praw Obywatelskich, upamiętniający pierwsze po II wojnie światowej wolne wybory parlamentarne w Polsce. To symboliczna data, przypominająca o fundamentalnym znaczeniu wolności i praw obywatelskich w demokratycznym państwie prawa. Warto pamiętać, że ich ochrona stanowi również istotny element misji Urzędu Ochrony Danych Osobowych.

W związku z otrzymanym zawiadomieniem o możliwych nieprawidłowościach w procesie przetwarzania danych w trakcie wyborów prezydenckich w 2025 r., zwróciłem się z pytaniami do Stowarzyszenia Ruch Kontroli Wyborów (RKW) z prośbą o wyjaśnienia. Zgłoszenie dotyczyło informacji, jakoby członkowie obwodowych komisji wyborczych mieli możliwość weryfikowania uprawnień wyborców głosujących na podstawie zaświadczeń o prawie do głosowania poza miejscem zamieszkania – przy wykorzystaniu aplikacji mobilnej RKW. Aplikacja ta, według posiadanych informacji, nie została autoryzowana przez Krajowe Biuro Wyborcze. W trosce o przejrzystość procesu wyborczego oraz poszanowanie zasad ochrony danych osobowych, wyjaśnienie sytuacji jest niezbędne.

Interweniowałem również ws. uczniów podstawówki, którzy wygenerowali w aplikacji nagie zdjęcie koleżanki i zachęcali na Instagramie innych do wykorzystywania jej wizerunków. Zawiadomiłem Policję o możliwości popełnienia przestępstwa. Było to działanie konieczne, zwłaszcza, że chodziło o ochronę dóbr osobistych małoletniej osoby pokrzywdzonej.

Osoby najmłodsze są najmniej świadome zagrożeń związanych z korzystaniem z usług cyfrowych i najbardziej bezbronne. Z tego względu przekazałem Ministerstwu Cyfryzacji uwagi do projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie. Choć inicjatywa ta jest niewątpliwie potrzebna, projekt zawiera rozwiązania budzące wątpliwości z punktu widzenia prawa do ochrony danych osobowych i prawa do prywatności.

Zwróciłem się również do Ministerstwa Sprawiedliwości z pytaniem o aktualny stan prac nad zapowiedzianą w sierpniu ubiegłego roku inicjatywą legislacyjną, mającą na celu zwiększenie poziomu ochrony danych osobowych znajdujących się w elektronicznych księgach wieczystych. Problem bezprawnego pobierania i wykorzystywania tych danych od dawna jest przedmiotem zainteresowania wielu podmiotów.

W czerwcu przedstawiłem także opinię legislacyjną dla Sejmu co do projektowanych rozwiązań dotyczących możliwości instalowania liczników pokazujących rzeczywiste zużycie paliw gazowych przez odbiorcę i rzeczywisty czas korzystania z gazu. Projekt nie rozstrzyga jednak, kto miałby mieć dostęp do danych z licznika – czy wyłącznie odbiorca, czy również operator systemu dystrybucyjnego lub inne podmioty.

Zgłosiłem ponadto uwagi do projektu ustawy o Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz ustawy o podatku od towarów i usług. Nie kwestionując zasadności zmian służących poprawie warunków prowadzenia działalności gospodarczej, wskazałem na potrzebę doprecyzowania zasad dostępu do systemu teleinformatycznego oraz zakresu informacji przekazywanej za jego pośrednictwem.

Za nami liczne wydarzenia:

- **Rocznica Społecznego Zespołu Ekspertów i powołanie podgrupy ds. sztucznej inteligencji** – dziękuję wszystkim członkom Zespołu za ich czas, zaangażowanie i nieocenione wsparcie prac Urzędu, które zaowocowało licznymi, wartościowymi inicjatywami w minionym roku.
- **Seminarium ws. Europejskich Ram Cyfrowej Tożsamości** – spotkanie pozwoliło nam na wskazanie kierunków, które wyznacza rozporządzenie Unii Europejskiej, jeśli chodzi o zwiększenie bezpieczeństwa w zakresie identyfikacji elektronicznej. Dzięki niemu świeżym okiem spojrzeliśmy na korzyści i potencjał rozwoju eIDAS2 dla biznesu i sektora publicznego.
- **Wykład ekspercki z cyklu „Ochrona danych i technologia”** – ukłony dla Tomasza Izydorczyka, członka SZE, który przybliżył temat operacji na danych osobowych w systemach sztucznej inteligencji z perspektyw podmiotu stosującego, zgodnie z RODO i AI Act.
- **Konferencja „Technologie kwantowe: zagrożenia, wyzwania i szanse dla cyberbezpieczeństwa i ochrony danych osobowych”** – to międzynarodowe wydarzenie zorganizowaliśmy wspólnie z Uniwersytetem Jagiellońskim. Przedstawiliśmy na nim podstawowe zasady działania technologii kwantowych oraz ramy prawne, w jakich te rozwiązania mogą znaleźć bezpieczne zastosowanie z poszanowaniem zasad ochrony danych osobowych i prywatności.
- **23. Spotkanie Grupy organów ochrony danych Europy Środkowo-Wschodniej**, podczas którego wraz z przedstawicielami organów nadzorczych z Europy Środkowo-Wschodniej podpisaliśmy deklarację w sprawie wzmocnienia organów ochrony danych, zapewnienia równowagi regulacyjnej oraz wsparcia dla małych i średnich przedsiębiorstw i organizacji pozarządowych.

- **Seminarium UODO i ZUS – „Wyzwania w udzieleniu informacji publicznej”** – to kolejne wydarzenie z cyklu wspólnych przedsięwzięć naszych instytucji, dzięki którym przybliżamy tematykę ochrony danych osobowych w administracji publicznej.
- **Rozstrzygnięcie konkursu dla studentów na esej**. Komisja konkursowa uhonorowała najlepsze prace studentów, którzy zmierzyli się z kwestiami związanymi z ochroną prywatności studentów w przypadku korzystania przez nich z prywatnych urządzeń elektronicznych podczas zdawania egzaminów na uczelni. Wszystkim wyróżnionym serdecznie gratuluję.

Czerwiec był również czasem spotkań z przedstawicielami branży medycznej. Podczas jednego z nich dyskutowaliśmy o możliwościach stworzenia kodeksu postępowania dla branży wyrobów medycznych. Zależy nam również na poprawie bezpieczeństwa lekarzy i wprowadzeniu systemowych rozwiązań, które by się do tego przyczyniły. By omówić te kwestie spotkałem się po raz kolejny z Prezesem Naczelnej Rady Lekarskiej.

Złożyłem skargę kasacyjną do Naczelnego Sądu Administracyjnego od wyroku WSA w Warszawie, który uwzględnił skargę Santander Bank Polska SA dotyczącą nałożenia przez organ nadzorczy administracyjnej kary pieniężnej w wysokości 1 440 549 zł. Przypominam, że bank nie poinformował Prezesa UODO o incydencie naruszenia ochrony danych osobowych ani nie zawiadomił o tym osób, których dane dotyczą. Sprawa dotyczy zdarzenia z 2018 r., kiedy to dokumenty bankowe zawierające dane osobowe zostały skradzione, a następnie porzucone na śmietniku.

Naczelny Sąd Administracyjny oddalił skargę kasacyjną Krajowej Szkoły Sądownictwa i Prokuratury, która kwestionowała nałożoną przez Prezesa UODO administracyjną karę pieniężną w wysokości 100 tys. zł za naruszenie przepisów o ochronie danych osobowych. NSA nie tylko nie dopatrzył się uchybień w zakresie podstaw nałożenia kary, ale również uznał jej wysokość za w pełni uzasadnioną. Co istotne, Sąd podkreślił, że przy takiej skali naruszeń – leżących po stronie administratora – w przypadku podmiotu prywatnego sankcja byłaby zdecydowanie wyższa.

Przekazałem stanowisko dotyczące udziału Rzeczypospolitej Polskiej w postępowaniu przed Trybunałem EFTA w sprawie E-5/25 Silbernagl, dotyczącym przesłanek odwołania inspektora ochrony danych. Rozstrzygnięcie to może okazać się kluczowe nie tylko dla stosowania art. 38 ust. 3 zd. 2 RODO, lecz także dla dalszego doprecyzowania krajowych regulacji w zakresie odwoływania IOD.

Mam również przyjemność poinformować, że Maria Jęda, Główna Koordynatorka ds. Wielkoskalowych Systemów Informacyjnych UE w UODO została wybrana na Zastępczynię Przewodniczącej Grupy ds. koordynacji nadzoru nad Eurodac. Przypomnę, że EURODAC to unijna

baza odcisków palców osób ubiegających się o azyl oraz osób zatrzymanych spoza UE i EOG. O swoich obowiązkach Maria Jęda opowiada w niniejszym wydaniu biuletynu.

Inną pozytywną wiadomością jest to, że 16 czerwca 2025 r. Parlament Europejski, Rada UE – kierowana przez polską prezydencję – i Komisja Europejska wypracowali porozumienie w sprawie rozporządzenia ustanawiającego dodatkowe przepisy proceduralne dotyczące egzekwowania RODO. Akt ten uprości współpracę krajowych organów ochrony danych podczas stosowania i egzekwowania RODO w sprawach o charakterze transgranicznym.

Z mniej przyjemnych, ale niestety potrzebnych decyzji, muszę wspomnieć o karze, jaką nałożyłem na Gminny Ośrodek Pomocy Społecznej oraz wójta gminy. Tymczasowej utraty danych w GOPS-ie można było uniknąć, gdyby analiza ryzyka została przeprowadzona rzetelnie.

Podobnie, wobec szpitala w Białymstoku zdecydowałem o sankcji za niewdrożenie odpowiednich środków technicznych i organizacyjnych. W wyniku ataku został zablokowany dostęp do systemów informatycznych, co skutkowało naruszeniem poufności i dostępności danych osobowych około 2000 pracowników, w tym możliwością uzyskania do nich nieuprawnionego dostępu.

Na koniec przypominam, że to ostatnie chwile UODO w budynku Intraco. Od lipca Urząd przenosi się do nowej siedziby na ul. Moniuszki 1A w Warszawie. Dokładamy starań, by proces relokacji nie zakłócił bieżącej pracy Urzędu.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W tym numerze zachęcam Was do lektury wywiadu z Marią Jędą, Główną Koordynatorką ds. Wielkoskalowych Systemów Informacyjnych UE w UODO, która została również wybrana na Zastępczynię Przewodniczącej Grupy ds. Koordynacji Nadzoru nad systemem EURODAC. Rozmowa przybliży Wam działanie systemów informatycznych UE, gromadzących dane milionów obywateli i cudzoziemców podróżujących po Europie. Jeśli jesteście ciekawi, jakie są obowiązki UODO w kontekście systemów funkcjonujących w ramach strefy Schengen oraz co powoduje, że pojawiają się rozbieżności w interpretacji przepisów dotyczących tych systemów na poziomie krajowym, koniecznie zajrzyjcie do rozmowy z naszą ekspertką.

Nieustannie powtarzamy, by bezpieczeństwo danych osobowych traktować jak proces, a nie jednorazową inwestycję. W tym wydaniu biuletynu tłumaczymy, że zgodnie z zasadą ochrony danych w fazie projektowania, już na etapie tworzenia aplikacji webowych w szczególności powinniście zwrócić uwagę na minimalizację przetwarzania danych, stosowanie silnych mechanizmów uwierzytelniania oraz odpowiednią segregację informacji, tak by dostęp do danych był możliwy wyłącznie dla osób uprawnionych.

O zasadzie ochrony danych w fazie projektowania i domyślnie z pewnością zapomniała niestety jedna ze słoweńskich szkół, co skutkowało tym, że zewnętrzny dostawca posiłków otrzymał nieograniczony dostęp do całej bazy danych uczniów. Słoweński Urząd Ochrony Danych zdecydował się udzielić szkole nagany.

W czerwcowym wydaniu piszemy też, czym jest ślad cyfrowy i – w oparciu o decyzje PUODO i wyroki sądów – tłumaczymy jak nim zarządzać, by skutecznie ograniczyć nadmierne gromadzenie danych oraz wzmocnić ochronę prywatności w środowisku cyfrowym.

Na prośbę jednego z IOD Prezes UODO odniósł się do możliwości ponownego wykorzystania przez rozgłośnię radiową wyemitowanych na żywo wypowiedzi słuchaczy w formie krótkich urywków dźwiękowych. Opisaną kwestię ocenił zarówno z uwzględnieniem regulacji prawa autorskiego i prawa prasowego, jak i przez pryzmat przepisów o ochronie danych osobowych.

Przybliżamy również decyzję Prezesa UODO, w której udzielił upomnienia dla Starosty za opublikowanie danych obywatela bez podstawy prawnej. Dane skarżącego (imię, nazwisko i adres) trafiły na portal prowadzony przez Starostę.

Włoski organ nadzoru wykazał szereg naruszeń ochrony danych wokół chatbotu „Replika”. Oprócz nałożenia grzywny, nakazał spółce Luka Inc. dostosowanie operacji przetwarzania danych do przepisów rozporządzenia.

Publikujemy oświadczenie irlandzkiej Komisji Ochrony Danych (DPC) w sprawie Meta AI. Powstało ono w rezultacie dwuletniej intensywnej współpracy DPC z wieloma wiodącymi firmami technologicznymi stojącymi na czele rozwoju sztucznej inteligencji, w szczególności w zakresie wykorzystywania danych osób dorosłych do szkolenia dużych modeli językowych w UE/EOG. Zaowocowało to wdrożeniem przez wiele firm ulepszeń i dodatkowych zabezpieczeń ochrony danych przed wprowadzeniem na rynek UE.

Z kolei francuski organ ochrony danych (CNIL) opublikował roczne sprawozdanie za 2024 r. Dokument podsumowuje działania realizowane w ramach czterech kluczowych misji: informowania i ochrony społeczeństwa, wspierania oraz doradzania profesjonalistom i organom administracji publicznej, przewidywania zmian i wdrażania innowacji na rzecz cyfrowej przyszłości, a także monitorowania i egzekwowania przepisów RODO oraz innych regulacji.

W maju w Krakowie odbyła się konferencja Digital Dragons, wydarzenie dotyczące branży gier w Europie. Uczestniczyli w nim przedstawiciele UODO – prezes Urzędu, Mirosław Wróblewski, oraz zastępca dyrektorki Departamentu Współpracy Międzynarodowej, Krzysztof Król. Wystąpienie prezesa dotyczyło konieczności skutecznej weryfikacji wieku graczy w kontekście ochrony dzieci w przestrzeni cyfrowej. Czy wiecie, że aż 71% dzieci spędza w internecie średnio 7 godzin dziennie, a mniej niż połowa rodziców korzysta z dobrowolnych mechanizmów kontroli dostępu?

Pozostając w temacie dzieci i ich praw, podsumowujemy XV edycję Programu „Twoje dane – Twoja sprawa”. W organizowanych przez UODO konkursach i webinarach wzięło udział 5 921 nauczycieli i 61 348 uczniów z 352 szkół podstawowych, ponadpodstawowych i placówek doskonalenia nauczycieli. Jak zwykle dziękujemy za zaangażowanie, świetne pomysły i współpracę w partnerskiej atmosferze.

Nie tylko jubileuszowa edycja Programu za nami, ale również koniec roku szkolnego. Dlatego życzę dzieciom bezpiecznych i wymarzonych wakacji i zapraszam do udziału w XVI edycji naszego edukacyjnego Programu, która rozpocznie się już we wrześniu. Z Wami za to widzimy się przy okazji podwójnego, wakacyjnego numeru biuletynu.

Karol Witowski
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

WIELKOSKALOWE SYSTEMY INFORMACYJNE UE POD NADZOREM

Systemy informatyczne UE gromadzą dane milionów obywateli i cudzoziemców podróżujących po Europie. O tym, jak zapewnia się nadzór nad ich działaniem oraz ochronę praw podstawowych, z Marią Jędą, Główną Koordynatorką ds. Wielkoskalowych Systemów Informacyjnych UE w UODO rozmawiał Karol Witowski, Rzecznik Prasowy UODO.

Objęła Pani nowo utworzone stanowisko Głównego Koordynatora ds. Wielkoskalowych Systemów Informacyjnych UE, a także została wybrana na Zastępczynię Przewodniczącej Grupy ds. Koordynacji Nadzoru nad systemem EURODAC. Zacznijmy zatem od pytania wprowadzającego: czym są Wielkoskalowe Systemy Informacyjne UE?

Wielkoskalowe Systemy Informacyjne UE to zaawansowane technologicznie systemy informatyczne, które cechuje szeroki zakres działania i ogromna liczba przetwarzanych danych. Ich głównym celem jest wspieranie integracji europejskiej w obszarze bezpieczeństwa, współpracy policyjnej i sądowej w sprawach karnych, a także w funkcjonowaniu jednolitego rynku wewnętrznego – a więc w kluczowych filarach Unii Europejskiej.

Systemy te objęte są mechanizmem skoordynowanego nadzoru. Aktualnie funkcjonuje kilka jego form: Komitet Skoordynowanego Nadzoru działający w ramach Europejskiej Rady Ochrony Danych (EROD) oraz Grupy ds. Koordynacji Nadzoru nad Systemem Informacji Celnej i Systemem EURODAC skupione wokół Europejskiego Inspektora Ochrony Danych (EIOD). W przypadku tej ostatniej grupy zostałam wybrana na funkcję zastępcy przewodniczącego.

Jakie systemy obejmuje mechanizm skoordynowanego nadzoru i w jakich obszarach funkcjonuje?

Mechanizm skoordynowanego nadzoru ulegał ewolucji – pierwotnie istniały oddzielne grupy nadzorujące poszczególne systemy, natomiast Komitet Skoordynowanego Nadzoru obejmował

jedynie system IMI. Obecnie dąży się do skupienia tego skoordynowanego nadzoru właśnie w ramach Komitetu.

Obecnie skoordynowany nadzór obejmuje:

• System Informacyjny Schengen (SIS),

• Wizowy System Informacyjny (VIS),

• Europejską Bazę Daktyloskopijną Azylową (EURODAC),

• System automatycznej wymiany danych w ramach współpracy policyjnej (Prüm II),

• System Wjazdu/Wyjazdu (EES),

• Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS),

• Agencję UE ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust),

• Prokuraturę Europejską (EPPO),

• Agencję UE ds. Współpracy Organów Ścigania (Europol),

• System Informacji Celnej (CIS),

• System wymiany informacji na rynku wewnętrznym (IMI).

W najbliższej przyszłości nadzór ten obejmie również:

• Europejski system przekazywania informacji z rejestrów karnych dotyczący obywateli państw trzecich (ECRIS-TCN),

• Interoperacyjność systemów EES, ETIAS, ECRIS-TCN, EURODAC, SIS i VIS,

• Dane przetwarzane w ramach mechanizmu dostosowywania cen na granicach z uwzględnieniem emisji CO_2,

• System informacji dotyczący produktów związanych z wylesianiem,

• Kwestie sektorowe związane z Aktem w sprawie danych (Data Act).

Zakres ten nieustannie się poszerza – można więc zakładać, że kolejne unijne systemy będą objęte mechanizmem skoordynowanego nadzoru.

Na czym polega współpraca między EIOD a krajowymi organami ochrony danych w ramach tego mechanizmu?

1 ROZMOWA Z EKSPERTEM

Podstawę współpracy stanowi art. 62 rozporządzenia 2018/1725 (tzw. „EUDPR”), zgodnie z którym EIOD i krajowe organy ochrony danych – każdy w zakresie swoich kompetencji – współpracują w celu zapewnienia skutecznego nadzoru nad wielkoskalowymi systemami i unijnymi instytucjami.

Współpraca ta obejmuje m.in.:

• wymianę informacji,

• wzajemną pomoc przy audytach i inspekcjach,

• analizę trudności interpretacyjnych,

• opracowywanie wspólnych wniosków i zaleceń,

• popularyzację wiedzy o prawach osób, których dane dotyczą.

W tym celu EIOD i krajowe organy spotykają się w ramach Europejskiej Rady Ochrony Danych lub Europejskiego Inspektora Ochrony Danych, w zależności od systemu. Co dwa lata EROD przekazuje wspólne sprawozdanie z działań w zakresie skoordynowanego nadzoru Parlamentowi Europejskiemu, Radzie i Komisji Europejskiej.

Jakie są obowiązki UODO w kontekście systemów działających w ramach strefy Schengen?

Systemy wspierające zarządzanie granicami i bezpieczeństwo – takie jak SIS, VIS, EES, ETIAS – nakładają na organy ochrony danych dodatkowe obowiązki poza tymi przewidzianymi w RODO. Należą do nich:

1. Regularne audyty przetwarzania danych w tych systemach zgodnie z międzynarodowymi standardami audytu (co 3–4 lata, a w przypadku zmodernizowanego systemu ERODAC nawet co roku).

2. Kontrola logów – zapisów dotyczących historii przetwarzania, w tym identyfikatorów użytkowników i wyszukiwań w celu sprawdzania, czy dane wyszukiwanie było zgodne z prawem.

3. Realizacja pośredniego prawa dostępu, gdy osoba, której dane dotyczą, nie może otrzymać pełnej informacji od administratora krajowego komponentu. W takich sytuacjach organ ochrony danych pełni funkcję pośrednika oceniającego zasadność odmowy dostępu, mając na względzie interes publiczny, bezpieczeństwo i prawa innych osób.

1 ROZMOWA Z EKSPERTEM

(Prawo do pośredniego dostępu do swoich danych jest co prawda przewidziane w art. 17 dyrektywy 2016/680, jednak UODO cały czas alarmuje, że przepis ten nie został w Polsce wdrożony prawidłowo, podczas gdy rozporządzenia ws. systemów wielkoskalowych wymuszają realizację tego obowiązku wprost.)

UODO ma również obowiązek:

• udzielania pomocy i porady osobom fizycznym w zakresie ich praw,

• zapewnienia dostępności tych usług przez cały okres postępowania,

• współorganizowania z Komisją Europejską kampanii informacyjnych.

Komitet Skoordynowanego Nadzoru zgłaszał zastrzeżenia wobec przygotowania kampanii informacyjnej nt. EES przez Komisję Europejską. Jaki jest aktualny stan wdrażania systemu i kampanii?

Pomimo że system EES nie został jeszcze uruchomiony, Komitet Skoordynowanego Nadzoru już na etapie przygotowań sygnalizował Komisji potrzebę pełnego zaangażowania organów ochrony danych. Uruchomienie EES planowane jest obecnie na październik br.

Zgodnie z rozporządzeniem ustanawiającym EES, Komisja ma obowiązek – we współpracy z EIOD i krajowymi organami nadzorczymi – prowadzić kampanię informacyjną skierowaną przede wszystkim do obywateli państw trzecich. Ma ona informować o celach systemu, rodzaju gromadzonych danych, uprawnionych organach oraz prawach osób, których dane dotyczą.

Komitet wyraził zaniepokojenie, że organy te nie zostały odpowiednio włączone w przygotowanie kampanii. Komisja założyła, że kampanie zostaną realizowane przez krajowe instytucje odpowiedzialne za EES, jednak wiele organów nadzorczych nie zostało dotychczas w to zaangażowanych.

Na szczęście, dzięki wspólnym wysiłkom możemy obecnie liczyć na przeprowadzenie kampanii informacyjnej w takiej formie, w jakiej przewiduje to rozporządzenie ustanawiające System Wjazdu/Wyjazdu. Jest to szczególnie istotne, ponieważ EES ma służyć elektronicznej rejestracji czasu i miejsca przekroczenia granicy przez obywateli państw trzecich oraz wyliczaniu okresu ich legalnego pobytu. System ten powinien również wspierać działania związane z bezpieczeństwem i walką z przestępczością. Ponieważ jak do tej pory nie istniała taka baza danych w skali Europy, ważne jest, aby dotrzeć z informacjami na temat praw ochrony danych do osób, które będą podlegały stosownej rejestracji.

1 ROZMOWA Z EKSPERTEM

W marcu 2023 r. uruchomiono zmodernizowany SIS. Jakie nowe wyzwania związane z ochroną danych niesie ta zmiana?

SIS to największy europejski system informacji w zakresie bezpieczeństwa i granic. Nowa wersja systemu umożliwia m.in. dodawanie danych biometrycznych (np. odcisków palców, DNA), a także wprowadzanie nowych kategorii wpisów.

Z jednej strony poprawia to skuteczność działań służb, z drugiej – wiąże się z nowymi wyzwaniami w zakresie ochrony danych osobowych. Dlatego niezbędne jest równoczesne wzmacnianie zabezpieczeń systemu, zarówno technicznych, jak i organizacyjnych, a także zapewnienie odpowiednich środków organom ochrony danych w celu umożliwienia im efektywnego wykonywania powierzonych im zadań.

Czy bierze Pani udział w kontrolach wielkoskalowych systemów?

Oczywiście. Udział w kontrolach to naturalna konsekwencja mojej roli w mechanizmie skoordynowanego nadzoru. Kontrole te są uwzględnione w corocznych planach kontroli sektorowych Prezesa UODO i są publikowane na stronie internetowej Urzędu.

W ramach międzynarodowej współpracy tworzone są również wspólne plany audytowe, a Komitet może wskazywać konkretne zagadnienia do zbadania. Niedawno Komitet Skoordynowanego Nadzoru opublikował raport ze wspólnych kontroli dotyczących wpisów w SIS wykorzystywanych w celu przeprowadzania kontroli niejawnych przez organy porządku publicznego. W tym działaniu brał udział również UODO.

Czy pojawiają się rozbieżności w interpretacji przepisów dotyczących tych systemów na poziomie krajowym?

Tak, i to z różnych powodów. Czasem wynikają one z różnic w tłumaczeniach – jedno słowo może mieć odmienne znaczenie w różnych wersjach językowych tych samych przepisów. Przykładowo, angielskie sformułowanie „assistance” jest przetłumaczone w Polsce jako „pomoc”, ale w innym państwie użyto sformułowania „mediacja”, która w tym kraju ma charakter odpłatny.

Rozbieżności wynikają również z odmiennych tradycji prawnych i kulturowych. Wyraźnie widać to chociażby w sposobie wdrażania dyrektywy policyjnej. Mechanizm skoordynowanego nadzoru służy właśnie temu, by identyfikować i rozwiązywać takie nieścisłości – zarówno w odniesieniu do organów państw członkowskich, jak i w kontekście ochrony praw osób, których dane dotyczą.

1 ROZMOWA Z EKSPERTEM

Jakie wyzwania wiążą się z pełnioną przez Panią funkcją?

Zadań i wyzwań jest wiele. Decyzja Prezesa UODO Mirosława Wróblewskiego o utworzeniu stanowiska Głównego Koordynatora ds. Wielkoskalowych Systemów UE odpowiada na rosnące znaczenie tych systemów i potrzebę zapewnienia ich spójnego nadzoru. Funkcja ta wymaga nie tylko bardzo dobrej znajomości przepisów prawa i rozwiązań technologicznych, ale także umiejętności skutecznej koordynacji działań na poziomie krajowym, jak i międzynarodowym. Szczególnym wyzwaniem jest zapewnienie spójności i efektywności nadzoru w obliczu dynamicznego rozwoju systemów informacyjnych oraz zmieniającego się otoczenia regulacyjnego. Dlatego bardzo dziękuję panu Prezesowi za okazane mi zaufanie i powierzenie realizacji tak istotnego zadania, a także za dostrzeżenie potrzeby systemowego podejścia do nadzoru nad wielkoskalowymi systemami informacyjnymi UE.

Nie bez znaczenia jest także rola Zastępcy Przewodniczącej Grupy ds. Koordynacji Nadzoru nad systemem EURODAC. Prowadzenie prac i posiedzeń grup to odpowiedzialne zadanie, jednak jestem dobrej myśli – zwłaszcza że współpraca w ramach tego mechanizmu przebiega w wyjątkowo dobrej, profesjonalnej atmosferze.

Jakie znaczenie ma Pani rola jako koordynatora i uczestnika tych mechanizmów z punktu widzenia UODO?

Udział UODO w mechanizmach takich jak skoordynowany nadzór czy ocena stosowania dorobku Schengen ma kluczowe znaczenie dla budowania pozycji Urzędu jako partnera instytucji europejskich. Dzięki aktywnemu zaangażowaniu możemy wpływać na interpretację i stosowanie przepisów w praktyce, dzielić się doświadczeniami, ale też uczyć się od innych.

Moja rola jako koordynatora polega na tym, by ten udział był dobrze zorganizowany, spójny i merytorycznie wartościowy – tak, aby głos UODO był słyszalny i traktowany poważnie. To ma wpływ nie tylko na sposób, w jaki Urząd jest postrzegany na forum unijnym, ale także na jakość naszej codziennej pracy na poziomie krajowym.

Choć o wielkoskalowych systemach informacyjnych potrafi Pani mówić z wielką pasją, wiemy, że muzyka to Pani kolejna specjalizacja. Niektórzy mieli przyjemność uczestniczyć w Pani występach chóralnych czy musicalowych, a swoich współpracowników żegna Pani… piosenkami. Skąd w Pani taka muzyczna dusza?

1 ROZMOWA Z EKSPERTEM

Tu chyba zacytuję Ewę Bem: „Moje serce to jest muzyk improwizujący, co ma własny styl i rytm". Muzyka to dla mnie nie tylko pasja, to sposób budowania relacji z ludźmi, dzielenia się emocjami i tworzenia wspólnoty. Śpiewając na pożegnanie współpracowników, chcę im podziękować za wspólny czas – osobiście, od serca. To także pomaga złapać dystans do formalnej rzeczywistości, w której jako urzędnicy funkcjonujemy na co dzień.

Na szczęście takie pożegnania zdarzają się rzadko, dlatego swoje artystyczne potrzeby realizuję głównie w różnorodnych projektach muzycznych, które dają mi ogromną radość i energię. A tej energii naprawdę potrzeba na moim stanowisku!

Dziękujemy za rozmowę i życzymy dalszej energii – zarówno w ramach skoordynowanego nadzoru, jak i na scenie!

Na zdjęciu Maria Jęda, Główna Koordynatorka ds. Wielkoskalowych Systemów Informacyjnych UE oraz Zastępczyni Przewodniczącej Grupy ds. Koordynacji Nadzoru nad systemem EURODAC.
fot. Klaudia Piwek

MOŻLIWOŚĆ POWTÓRNEGO WYKORZYSTANIA PRZEZ ROZGŁOŚNIĘ RADIOWĄ FRAGMENTÓW WYPOWIEDZI SŁUCHACZY

Klauzuli prasowej nie należy postrzegać jako wyłączającej stosowanie ochrony danych osobowych do działalności dziennikarskiej, literackiej lub artystycznej. Wyjątki przewidziane są dla ściśle określonych czynności składających się na proces tworzenia dzieła. Nie dotyczą one natomiast innych celów, w których dane osobowe są przetwarzane w ramach działalności firmy, np. na potrzeby marketingu czy prowadzenia rozliczeń finansowo-księgowych.

Na prośbę jednego z IOD Prezes UODO odniósł się do możliwości ponownego wykorzystania przez rozgłośnię radiową wyemitowanych na żywo wypowiedzi słuchaczy w formie krótkich urywków dźwiękowych. Dla pytającego szczególnie istotne było, czy wykorzystanie w celach promocyjnych, informacyjnych lub archiwalnych krótkich fragmentów wypowiedzi, która została już nadana w audycji, mieści się w ramach dozwolonego użytku i nie wymaga uzyskania dodatkowej zgody. W pytaniu inspektor nie wskazał jednak, jakie cele obejmuje dotychczasowa zgoda słuchacza. Jako argumenty przemawiające za tym, że możliwe jest takie powtórne wykorzystanie wyemitowanych już wypowiedzi, wskazał, że w większości przypadków na podstawie samego nagrania dźwiękowego trudno jednoznacznie zidentyfikować osobę fizyczną oraz że podobne praktyki są stosowane w mediach, np. w przypadku cytowania wypowiedzi prasowych w innych artykułach lub reportażach.

W odpowiedzi Prezes UODO zaznaczył, że opisaną kwestię należy ocenić zarówno z uwzględnieniem regulacji prawa autorskiego i prawa prasowego, jak i przez pryzmat przepisów o ochronie danych osobowych.

Czy głos to dane osobowe?

Stosownie bowiem do art. 4 pkt 1 RODO „dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Oceny, czy określone informacje stanowią dane osobowe (czy dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby), należy dokonywać z uwzględnieniem wszystkich elementów definicji danych osobowych oraz w odniesieniu do danego stanu faktycznego. Istotnym kryterium, które powinno być brane pod uwagę jest również to, kto dysponuje i np. udostępnia określone informacje na temat danej osoby, a także to, kto może być ich odbiorcą. Wskazówki w powyższym zakresie znaleźć można m.in. w motywie 26 RODO.

Biorąc pod uwagę powyższe definicje i wskazówki, głos osoby należy uznać za dane osobowe w przypadku, gdy dla określonego podmiotu istnieje możliwość zidentyfikowania tej osoby. Przy ocenie prawdopodobieństwa powiązania danych z konkretną osobą należy między innymi uwzględniać rozwój technologii i dostępność różnych narzędzi informatycznych umożliwiających przetwarzanie danych osobowych uzyskiwanych lub łączonych z różnych źródeł oraz to, kto może mieć dostęp do tych danych.

Czy można skorzystać z wyłączenia stosowania RODO?

Na podstawie art. 2 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe, a także do wypowiedzi w ramach działalności literackiej lub artystycznej nie stosuje się przepisów art. 5-9, art. 11, art. 13-16, art. 18-22, art. 27, art. 28 ust. 2-10 oraz art. 30 RODO.

Żeby jednak móc powoływać się na to wyłączenie, należy przede wszystkim ustalić, czy mamy do czynienia z działalnością polegającą na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, w tym czy określony materiał ma znamiona materiału prasowego w kontekście art. 2 ust. 1 ustawy o ochronie danych osobowych i art. 7 ust. 2 pkt. 1 i 4 ustawy Prawo prasowe.

Jeśli planowana publikacja nie będzie spełniać warunków do uznania jej za materiał prasowy, to przepisy dotyczące przetwarzania danych osobowych, w tym regulujące przesłanki dopuszczalności ich przetwarzania (art. 6 ust. 1 i art. 9 ust. 2) oraz obowiązek informacyjny (art. 13, art. 14), powinny być stosowane w pełnym zakresie.

Należy podkreślić, że wyłączenie stosowania wymienionych wyżej przepisów RODO nie oznacza, że dziennikarze nie muszą chronić praw osób, których dane przetwarzają, lecz jedynie że ochrona została ukształtowana inaczej. Działalność prasowa podlega bowiem regulacji Prawa prasowego i tam ukształtowane są odmienne konstrukcje mające służyć ochronie osób, których dane są przetwarzane (zob. np. wyrok NSA z 7 września 2021 r. sygn. akt III OSK 2883/21).

Kiedy potrzebna jest odrębna zgoda?

Dla oceny analizowanej kwestii istotne jest też ustalenie, w jakich celach będą przetwarzane dane osobowe (zapis foniczny rozmowy), a także jakie cele obejmuje zgoda wyrażona przez słuchacza. Dzięki temu możliwe będzie stwierdzenie, jakie przepisy prawa znajdą zastosowanie i czy na określone działania niezbędna jest odrębna zgoda w rozumieniu przepisów o ochronie danych osobowych.

Z perspektywy ochrony danych osobowych należy pamiętać, że jeżeli administrator przetwarza dane osobowe, np. publikuje je, to do niego należy określenie: celu przetwarzania danych, podstawy prawnej, zakresu ujawnianych danych oraz okresu, przez jaki będą one przetwarzane. Administrator ma bowiem obowiązek przetwarzania danych osobowych zgodnie z określonymi w art. 5 RODO zasadami: legalności, rzetelności i przejrzystości, ograniczenia celu, adekwatności, prawidłowości oraz integralności i poufności.

Odnosząc się zaś do kwestii przesłanki zgody jako podstawy do przetwarzania danych (w tym do publikacji nagrań rozmów) warto pamiętać, że w każdym przypadku opierania się na przesłance zgody należy zadbać o to, aby osoba, która taką zgodę ma wyrazić, dysponowała dokładnymi i pełnymi informacjami na temat tego, w jaki sposób jej dane (np. nagranie jej wypowiedzi) będą wykorzystywane (w tym m.in. w jakim celu/celach, w jakim zakresie, w jakim okresie). Informacje te są niezbędne, aby osoba ta mogła świadomie wyrazić swoją wolę.

Jednocześnie podkreślić należy, że na gruncie prawa ochrony danych osobowych, aby zgoda mogła stanowić podstawę przetwarzania danych, musi spełniać bardzo konkretne warunki określone w art. 4 pkt 11 oraz w art. 7 RODO.

Artykuł 4 pkt 11 RODO stanowi, że zgoda osoby, której dane dotyczą, oznacza: dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

W pkt. 3.3.1 Wytycznych EROD 05/2020 dotyczących zgody na mocy rozporządzenia 2016/679 wskazano w szczególności, że aby móc uznać, że zgoda jest „świadoma", należy poinformować osobę, której dane dotyczą, o określonych elementach kluczowych w celu dokonania wyboru.
W związku z tym EROD jest zdania, że do uzyskania ważnej zgody wymagane są przynajmniej następujące informacje: 1) tożsamość administratora; 2) cel każdej operacji przetwarzania, w odniesieniu do której prosi się o zgodę; 3) jakie dane (jaki rodzaj danych) będą gromadzone i wykorzystywane; 4) istnienie prawa do wycofania zgody.

Podsumowując, EROD wskazuje, że w zależności od okoliczności i kontekstu sprawy konieczne może być zapewnienie większej ilości informacji, aby umożliwić osobom, których dane dotyczą, rzeczywiste zrozumienie danych operacji przetwarzania.

Gdzie szukać przydatnych informacji?

Jednocześnie warto przypomnieć, że informacje o tym, w jaki sposób rozgłośnie radiowe powinny dbać o zgodne z prawem przetwarzanie danych znaleźć można na stronie internetowej UODO w takich materiałach, jak:

- Rozgłośnie publiczne muszą zadbać o zgodne z prawem przetwarzanie danych,
- Kara dla Polskiego Radia Szczecin za brak procedur chroniących prawa bohaterów publikacji.

fot. pixabay

CZYM JEST ŚLAD CYFROWY I JAK NIM ZARZĄDZAĆ

Zarządzanie śladem cyfrowym wymaga świadomego i odpowiedzialnego funkcjonowania w przestrzeni cyfrowej. Wyrobienie właściwych nawyków oraz znajomość przysługujących nam praw umożliwiają skuteczne ograniczenie nadmiernego gromadzenia danych oraz wzmocnienie ochrony prywatności w środowisku cyfrowym.

W erze cyfryzacji wszelka aktywność w przestrzeni wirtualnej zostawia tzw. ślad cyfrowy. Terminem tym określa się wszystkie informacje, które użytkownicy – często nieświadomie – pozostawiają podczas korzystania z internetu, aplikacji webowych, mobilnych oraz innych usług cyfrowych. Ponieważ dane te są zapisywane, na ich podstawie możliwe jest ustalenie zachowań danej osoby i stworzenie jej profilu. Informacje te mogą być wykorzystane przez wiele różnych podmiotów w bardzo różnych celach. Od przedstawiania nam spersonalizowanych ofert przez firmy, poprzez analizę naszych zachowań przez policję, urzędy skarbowe czy potencjalnych pracodawców, a na możliwości podszywania się pod nas lub przeprowadzania ataków phishingowych przez cyberprzestępców kończąc.

Dlatego świadome zarządzanie cyfrowym śladem jest niezmiernie ważne.

Rodzaje śladów

Ślady cyfrowe – w zależności od tego, w jaki sposób zostały pozostawione lub zapisane – dzieli się na dwie kategorie:

• aktywne – obejmują dane, które samodzielnie podajemy w internecie, lub czynności, które tam wykonujemy (np. publikacje w mediach społecznościowych, zakupy w internecie),

• pasywne – obejmują dane gromadzone automatycznie bez naszej wiedzy za pośrednictwem plików cookies, które są używane za każdym razem, gdy wchodzimy na jakąś stronę internetową. Takie pliki mogą śledzić, ile razy odwiedzamy stronę, z jakiego urządzenia, jaki mamy adres IP, jakie są nasze dane geolokalizacyjne itp.

Ślad cyfrowy jako dane osobowe

Ponieważ znaczna część elementów składających się na ślad cyfrowy umożliwia bezpośrednią lub pośrednią identyfikację osoby fizycznej, może zostać zakwalifikowana jako dane osobowe w rozumieniu art. 4 pkt 1 RODO. Do takich elementów należą w szczególności:

• adresy IP,

• identyfikatory plików cookies,

• dane geolokalizacyjne

• czy unikatowe identyfikatory urządzeń elektronicznych (tzw. fingerprint).

Stanowisko takie jest prezentowane zarówno w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (TSUE), jak i wyrokach WSA czy NSA. Również Prezes Urzędu Ochrony Danych Osobowych w wydawanych decyzjach administracyjnych jednoznacznie przesądzał o takim charakterze wielu cyfrowych śladów.

Przykładowo TSUE w wyroku C-582/14 z 19 października 2016 r. uznał, że dynamiczne adresy IP mogą być klasyfikowane jako dane osobowe w sytuacji, gdy administrator dysponuje środkami umożliwiającymi identyfikację osoby fizycznej. Powoduje to, że nawet dane, które same nie pozwalają na identyfikację osoby, mogą podlegać ochronie na podstawie przepisów RODO, jeżeli istnieje realna możliwość powiązania ich z konkretnym podmiotem danych.

Z kolei Prezes UODO w decyzji z 1 lipca 2021 r. (DKE.523.29.2021), powołując się m.in. na krajowe orzecznictwo, wyjaśnił, że „informacją dotyczącą osoby jest zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio stanowi informację także o niej samej. Adres IP (Internet Protocol Address) jest unikalnym numerem przyporządkowanym urządzeniom sieci komputerowych. Jest zatem informacją dotyczącą komputera a nie konkretnej osoby fizycznej, zwłaszcza wtedy gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej. Adres IP nie zawsze wobec tego może być traktowany jako dane osobowe w rozumieniu rozporządzenia 2016/679. Jednak tam gdzie adres IP jest na dłuższy okres czasu lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej [wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r., sygn. akt I OSK 1079/10]”.

W innej z decyzji (ZSPR.440.331.2019) Prezes UODO przesądził, że informacje dotyczące „kategorii marketingowych” (profilu behawioralnego) przypisanych użytkownikowi na podstawie plików

cookies oraz dane skorelowane z tymi informacjami stanowią dane osobowe. W konsekwencji administrator jest zobligowany do udostępnienia tych danych osobie, której dotyczą, na podstawie art. 15 RODO.

W kontekście kontroli śladu cyfrowego przez użytkowników warto zwrócić uwagę na wyrok TSUE z 1 października 2019 r. w sprawie C-673/17, w którym Trybunał doprecyzował wymogi dotyczące wyrażania zgody na instalację plików cookies. Jak wskazał, zgoda nie jest ważna, jeżeli przechowywanie informacji lub dostęp do informacji już przechowywanych w urządzeniu końcowym użytkownika strony internetowej, za pośrednictwem plików cookie, zostały zaakceptowane za pomocą domyślnie zaznaczonego okienka wyboru, którego zaznaczenie użytkownik ten musi usunąć, aby odmówić udzielenia zgody.

Zarządzanie śladem cyfrowym

Mając świadomość tego, że każda nasza aktywność w środowisku wirtualnym generuje dane podlegające potencjalnemu przetwarzaniu, analizie i profilowaniu i biorąc pod uwagę, jakie rodzi to konsekwencje, warto świadomie zarządzać swoim śladem cyfrowym.

1. Świadome udostępnianie informacji

Fundamentalnym działaniem jest świadome podejmowanie decyzji odnośnie do zakresu oraz odbiorców udostępnianych informacji. Rekomendowane jest ograniczenie przekazywania danych osobowych do niezbędnego minimum. Gdy podanie jakichś danych (np. adresu e-mail lub numeru telefonu) nie jest konieczne, lepiej ich nie udostępniać.

2. Zarządzanie zgodami na pliki cookies

Większość współczesnych witryn internetowych wymaga wyrażenia zgody na stosowanie plików cookies, przy czym często domyślnie aktywowane są pliki marketingowe lub analityczne. Użytkownik ma prawo do ich odrzucenia bez konsekwencji w postaci ograniczenia dostępu do serwisu. Wskazane jest również korzystanie z funkcji prywatności w przeglądarkach, umożliwiających blokowanie śledzących plików cookies podmiotów trzecich, a także systematyczne usuwanie historii przeglądania oraz danych przeglądarki.

3. Wykorzystanie narzędzi zwiększających prywatność

Warto też korzystać z rozwiązań technologicznych wzmacniających ochronę prywatności, takich jak:

- wtyczki do przeglądarek blokujące mechanizmy śledzące,
- przeglądarki zoptymalizowane pod kątem ochrony danych,
- tryb incognito podczas przeglądania,

• sieci VPN podczas korzystania z sieci publicznych, które zapewniają szyfrowanie połączenia, maskowanie adresu IP oraz zabezpieczenie przed atakami typu MITM (Man in the middle).

4. Egzekwowanie uprawnień wynikających z RODO

Nieodzownym elementem kontroli śladu cyfrowego jest aktywne korzystanie z praw przysługujących nam na mocy RODO. Każdy z nas ma prawo do informacji o zakresie przetwarzanych danych, celach przetwarzania oraz potencjalnych odbiorcach. Ponadto możliwe jest żądanie sprostowania, ograniczenia przetwarzania, przeniesienia lub usunięcia danych. W przypadku wątpliwości warto wyjaśniać je z administratorem. Ponadto przysługuje nam również prawo złożenia skargi do Prezesa UODO oraz możliwość dochodzenia swoich praw przed sądem cywilnym.

fot. pixabay

UPOMNIENIE DLA STAROSTY ZA OPUBLIKOWANIE DANYCH OBYWATELA BEZ PODSTAWY PRAWNEJ

Dane skarżącego (imię, nazwisko i adres) trafiły na portal prowadzony przez Starostę. Starostwo po prostu nie zanonimizowało danych przed publikacją informacji o obradach powiatowej komisji ds. skarg i wniosków. Nazwisko obywatela było w nazwie pliku z jego skargą, a cała reszta była w tym załączniku do informacji.

Starosta tłumaczył, że skarga z upublicznionymi danymi osobowymi, o którą tu chodziło, dotyczyła nienależytego wykonywania zadań przez Starostę. Starosta przekazał tę skargę komisji i Radzie Powiatu. Została przez nie rozpoznana na posiedzeniu i opublikowana. Po skardze obywatela usunięto ją, więc nikt już nie ma dostępu do jego danych. Był to jednorazowy incydent, zainteresowany został o tym niezwłocznie powiadomiony. Błąd zdarzył się dlatego, że pracownik Biura Rady, który udostępnił dokumenty na portalu, był przekonany, że dane są udostępniane tylko radnym powiatowym. W ocenie Starosty prawdopodobnie dane te zobaczył tylko ten pracownik i sam zainteresowany. Portal jest bowiem lokalny i nie cieszy się dużą popularnością.

Prezes UODO stwierdził po zbadaniu sprawy, że Starosta nie miał podstawy prawnej do publikowania danych obywatela. Prawo do informacji publicznej, jaką jest tekst o posiedzeniu komisji, podlega ograniczeniu ze względu m.in. na prywatność osoby fizycznej, jeśli nie pełni ona funkcji publicznej.

Starosta naruszył przepisy o ochronie danych osobowych, tj. art. 6 ust. 1 RODO, dlatego Prezes UODO udzielił mu upomnienia. W ocenie Prezesa UODO zastosowanie w niniejszej sprawie tego instrumentu prawnego jest adekwatne do wagi stwierdzonego naruszenia.

Sygnatura sprawy: DS.523.4131.2024

BEZPIECZEŃSTWO DANYCH OSOBOWYCH: PROCES, A NIE JEDNORAZOWA INWESTYCJA

Zgodnie z zasadą *ochrona danych w fazie projektowania*, już na etapie tworzenia aplikacji webowych należy w szczególności minimalizować przetwarzanie danych, stosować silne mechanizmy uwierzytelniania oraz odpowiednią segregację informacji, tak by dostęp do danych był możliwy wyłącznie dla osób uprawnionych.

Żeby wdrożyć tę zasadę, trzeba:

- w pełni kontrolować uprawnienia użytkowników,
- szyfrować dane w transmisji i podczas przechowywania oraz
- cykliczne przeprowadzać audyty i testy penetracyjne.

Dzięki temu możliwe jest wykrycie podatności, zanim zostaną one wykorzystane przez cyberprzestępców.

Zaniedbania w ochronie danych osobowych mogą mieć poważne konsekwencje dla użytkowników. Wyciek informacji medycznych może prowadzić do naruszenia prywatności pacjentów, których diagnozy i historia leczenia stają się dostępne dla osób niepowołanych. Takie incydenty mogą skutkować dyskryminacją, utratą zaufania do systemów ochrony zdrowia oraz stresem związanym z dalszym wykorzystywaniem ich danych. Ujawnienie informacji finansowych może natomiast prowadzić do oszustw kredytowych czy przejęcia kont bankowych. Dlatego tak istotne jest traktowanie ochrony danych jako fundamentu każdej aplikacji, a nie jako dodatkowej funkcjonalności wdrażanej po fakcie.

Ochrona danych w fazie projektowania to podejście pozwalające budować systemy odporne na zagrożenia, zamiast łatać luki w zabezpieczeniach po ich wykryciu. Organizacje powinny uwzględniać tę zasadę od początku, stosując rozwiązania technologiczne zapewniające maksymalną ochronę danych użytkowników. Wprowadzanie najlepszych praktyk, takich jak np. rekomendacje OWASP (Open Web Application Security Project), systematyczne testowanie zabezpieczeń oraz szczegółowa kontrola dostawców oprogramowania to kluczowe kroki ograniczające ryzyko wycieku danych. Nie chodzi tylko o zgodność z przepisami, ale przede wszystkim o ochronę osób, których życie może zostać dotknięte skutkami takich naruszeń.

4 NARUSZENIA I KONTROLE

Projektowanie aplikacji webowych musi uwzględniać nie tylko funkcjonalność i wygodę użytkowników, ale przede wszystkim ich bezpieczeństwo. Już na etapie analizy ryzyka należy identyfikować znane zagrożenia i podatności, które mogą wpływać na ochronę danych. Takie podatności jak np. IDOR (Insecure Direct Object References), SQL Injection, Cross-Site Scripting (XSS) czy brak odpowiedniej kontroli dostępu powinny być eliminowane na poziomie projektowania i wdrażania aplikacji. Ich skuteczne zabezpieczenie pozwala uniknąć przyszłych incydentów i zapewnia użytkownikom pełną ochronę ich danych.

Jednym z wyjątkowo niebezpiecznych zagrożeń jest wykorzystanie podatności IDOR, ponieważ wykorzystanie jej nie wymaga specjalistycznej wiedzy ani zaawansowanych umiejętności hakerskich. W wielu przypadkach wystarczy jedynie ręczna modyfikacja identyfikatora w adresie URL, aby uzyskać dostęp do zasobów, które powinny być chronione. Brak odpowiedniej weryfikacji uprawnień sprawia, że podatność ta może być przypadkowo odkrywana przez zwykłych użytkowników, a także celowo wykorzystywana przez cyberprzestępców do nieautoryzowanego dostępu do danych.

W Polsce podatność IDOR była przyczyną kilku incydentów naruszenia prywatności, np. zmiana identyfikatora zamówienia w URL umożliwiała dostęp do faktur innych klientów.

Każdy taki incydent dowodzi, że ochrona danych osobowych musi być integralną częścią procesu projektowania aplikacji webowych, a nie jedynie dodatkowym mechanizmem wdrażanym po fakcie. Bezpieczeństwo musi być wbudowane w system od początku, aby skutecznie minimalizować ryzyko naruszeń i zapewnić pełną kontrolę nad przetwarzanymi informacjami.

Kluczowe znaczenie ma również systematyczne testowanie zabezpieczeń aplikacji webowych, które stanowi podstawę ochrony danych osobowych. Brak odpowiednich procedur weryfikacji może narazić użytkowników na nieuprawniony dostęp, manipulację lub wykorzystanie ich danych przez osoby trzecie. To może prowadzić do oszustw finansowych, kradzieży tożsamości czy ujawnienia informacji zdrowotnych, bezpośrednio wpływając na ich prywatność i bezpieczeństwo. Dbanie o ciągłe monitorowanie zagrożeń oraz przeprowadzanie audytów i testów penetracyjnych nie tylko minimalizuje ryzyko, ale zapewnia użytkownikom realne poczucie kontroli nad ich danymi.

Cyberprzestępcy mogą wykorzystywać przejęte informacje do oszustw, szantażu czy uzyskania dostępu do kredytów i świadczeń zdrowotnych. Jednym z podstawowych sposobów zapobiegania takim incydentom jest stosowanie najlepszych praktyk bezpieczeństwa, a jednym z najbardziej cenionych źródeł rekomendacji w tej dziedzinie jest OWASP (Open Worldwide Application Security Project). Jedno z kluczowych źródeł najlepszych praktyk dotyczących autoryzacji w aplikacjach internetowych – OWASP Authorization Cheat Sheet podkreśla, że każda operacja związana z autoryzacją powinna być weryfikowana po stronie serwera, a dostęp do danych musi być ograniczony zgodnie z zasadą najmniejszych uprawnień.

4 NARUSZENIA I KONTROLE

Skuteczna ochrona aplikacji webowych wymaga także innych mechanizmów zabezpieczeń, takich jak:

• **Regularne testy penetracyjne** – aplikacje powinny być testowane nie tylko przed wdrożeniem, ale również okresowo oraz po każdej większej aktualizacji, co pozwala na wykrycie nowych podatności i ich eliminację.

• **Tokenizacja danych** – zamiast przewidywalnych identyfikatorów warto stosować losowe tokeny dostępowe, które są trudne do odgadnięcia i dodatkowo zabezpieczone warstwą autoryzacji.

• **Monitorowanie i logowanie incydentów** – rejestrowanie prób nieautoryzowanego dostępu umożliwia wykrycie podejrzanych aktywności i reakcję, zanim dojdzie do większych szkód.

• **Szyfrowanie danych w spoczynku i w tranzycie** – nawet jeśli informacje zostaną przechwycone, ich zaszyfrowanie znacząco utrudnia ich odczytanie przez osoby niepowołane.

fot. pixabay

CNIL UKARAŁ SOLOCAL GRZYWNĄ W WYSOKOŚCI 900 TYSIĘCY EURO

Firma nie wypełniła obowiązków wynikających z francuskiego kodeksu poczty i łączności elektronicznej oraz ogólnego rozporządzenia o ochronie danych w zakresie gromadzenia i potwierdzania zgody.

Streszczenie decyzji

Tło sprawy

Francuski organ nadzoru (CNIL) uczynił prospecting – pozyskiwanie klientów komercyjnych, priorytetowym tematem dochodzeń w 2022 r.; skupił się na praktykach profesjonalistów w tym sektorze, w tym osób, które odsprzedają dane, tzw. brokerów danych.

Przeprowadził dochodzenie w sprawie Solocal Marketing Services – firmy, która uzyskiwała dane potencjalnych klientów głównie od brokerów danych, wydawców konkursów gier i stron testujących produkty. Podmioty te są pierwszymi ogniwami w łańcuchu, głównymi podmiotami zbierającymi dane, odpowiedzialnymi za gromadzenie danych potencjalnych klientów. Solocal Marketing Services wykorzystał te dane do pozyskania klientów komercyjnych za pośrednictwem wiadomości SMS lub e-mail do zainteresowanych osób, w imieniu swojego klienta reklamodawcy. Mógł również przekazywać niektóre z danych swoim klientom, aby z kolei oni mogli sami pozyskać dla siebie klientów przez telefon lub pocztę.

Kluczowe ustalenia

Nieprzestrzeganie obowiązku uzyskania zgody osób fizycznych na otrzymywanie informacji handlowych drogą elektroniczną (art. L.34-5 francuskiego kodeksu poczty i łączności elektronicznej): Komisja ds. ograniczeń uznała, że wprowadzający w błąd wygląd formularzy wykorzystywanych przez brokerów danych uniemożliwił uzyskanie swobodnej i jednoznacznej zgody, odpowiedniej dla wymogów RODO, która stanowiłaby podstawę działań prospectingowych prowadzonych przez spółkę.

Brak wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych (art. 7 RODO): Firma nie dostarczyła francuskiemu organowi nadzorczemu dowodu zgody osób fizycznych, których dane zostały jej przekazane przez jednego z jej głównych dostawców. W rezultacie organ nie był w stanie zbadać formularzy gromadzenia danych stosowanych przez tego dostawcę, a tym samym ważności zgody osób, których dane dotyczą.

Decyzja

Na podstawie wyników kontroli komisja ds. ograniczeń – francuski organ ds.ochrony danych odpowiedzialny za wydawanie sankcji – uznał, że firma nie wypełniła obowiązków wynikających z francuskiego kodeksu poczty i łączności elektronicznej (CPCE) oraz ogólnego rozporządzenia o ochronie danych (RODO) w zakresie gromadzenia i potwierdzania zgody.

Nałożył na Solocal Marketing Services:

• grzywnę w wysokości 900 tysięcy euro, która została podana do wiadomości publicznej; oraz

• nakaz zaprzestania elektronicznej prospekcji handlowej w przypadku braku ważnej zgody, wraz z karą w wysokości 10 tysięcy euro za każdy dzień zwłoki po okresie 9 miesięcy.

Kwota tej grzywny uwzględnia bardzo dużą liczbę osób, których dotyczy (kilka milionów), historyczną pozycję firmy na rynku, korzyści finansowe uzyskane z naruszeń oraz środki podjęte przez firmę w celu wypełnienia niektórych jej zobowiązań od czasu przeprowadzenia kontroli.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pixabay

SŁOWEŃSKI ORGAN OCHRONY DANYCH: SZKOŁY MUSZĄ PRZESTRZEGAĆ ZASADY OCHRONY DANYCH W FAZIE PROJEKTOWANIA I DOMYŚLNIE

Zewnętrzny dostawca posiłków otrzymał nieograniczony dostęp do całej bazy danych uczniów. Tymczasem, by zapobiec wystąpieniu tych nieprawidłowości, wystarczyłoby właściwe wdrożenie zasad ochrony danych w fazie projektowania i domyślnej ochrony danych.

Streszczenie decyzji

Tło sprawy

Słoweński organ ochrony danych wszczął kontrolę z urzędu po otrzymaniu oficjalnego zawiadomienia o naruszeniu ochrony danych. Szkoła zgłosiła nieautoryzowany dostęp do danych uczniów przez zewnętrznego dostawcę posiłków, z którym zawarła umowę na posiłki szkolne. Dostawca uzyskał dostęp do całej bazy danych uczniów szkoły, w tym danych wrażliwych, takich jak dotacje i salda kont, mimo że wymagał jedynie imion i nazwisk do śledzenia posiłków.

Kluczowe ustalenia

Słoweński organ nadzorczy zidentyfikował znaczące nieprawidłowości w szkolnych praktykach ochrony danych. Zewnętrzny dostawca posiłków otrzymał nieograniczony dostęp do całej bazy danych uczniów, w tym do niepotrzebnych mu informacji, takich jak dotacje i salda kont. Szkoła zaniedbała wdrożenie odpowiednich środków w celu zapewnienia ochrony danych w fazie projektowania i domyślnie, zgodnie z art. 25 RODO. Procedura kontrolna ujawniła brak odpowiedniej oceny ryzyka w celu zidentyfikowania i złagodzenia zagrożeń wynikających z przyznania tak szerokiego dostępu do danych wrażliwych. Chociaż szkoła niezwłocznie zgłosiła naruszenie, nie wdrożyła skutecznych, długoterminowych środków, by wyeliminować pierwotne przyczyny i zapobiec ponownemu wystąpieniu naruszenia. Sprawa ta podkreśla znaczenie przyjęcia właściwych protokołów ochrony danych w instytucjach edukacyjnych, które zapewniają bezpieczeństwo i integralność danych osobowych uczniów.

Słoweński urząd ochrony danych udzielił nagany szkole i jej dyrektorowi jako osobie odpowiedzialnej. Administrator danych złożył wniosek o ochronę sądową do lokalnego sądu, który oddalił wniosek i podtrzymał decyzję słoweńskiego organu. Sąd podkreślił, że właściwe wdrożenie zasad ochrony

danych w fazie projektowania i domyślnej ochrony danych mogło zapobiec późniejszym nadużyciom, w tym nieautoryzowanym zmianom danych przez zewnętrznego dostawcę, a nawet potencjalnym oszustwom.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pixabay

WŁOSKI ORGAN OCHRONY DANYCH NAKŁADA GRZYWNĘ NA FIRMĘ STOJĄCĄ ZA CHATBOTEM „REPLIKA”

Włoski organ nadzoru wykazał szereg naruszeń ochrony danych wokół chatbotu „Replika”. Dlatego oprócz nałożenia grzywny, nakazał spółce Luka Inc. dostosowanie operacji przetwarzania danych do przepisów rozporządzenia.

Streszczenie decyzji

Tło sprawy

Postępowanie wywodzi się z dochodzenia wszczętego z urzędu przez włoski organ nadzoru po opublikowaniu doniesień prasowych i wstępnych ustaleń faktycznych przeprowadzonych w sprawie usługi Replika. To chatbot oparty na generatywnym systemie sztucznej inteligencji, opracowany i zarządzany przez amerykańską firmę Luka Inc. Chatbot posiada zarówno interfejs pisemny, jak i głosowy, umożliwiając użytkownikom wygenerowanie „wirtualnego towarzysza”, który może przyjąć rolę powiernika, terapeuty, romantycznego partnera lub mentora.

Kluczowe ustalenia

W trakcie dochodzenia włoski organ stwierdził, że domniemane naruszenia zgłoszone w lutym 2023 r. – kiedy to nakazał zablokowanie aplikacji – rzeczywiście miały miejsce. Do 2 lutego 2023 r. amerykańska spółka nie określiła podstawy prawnej operacji przetwarzania danych przeprowadzanych za pośrednictwem Repliki. Ponadto Luka przedstawiła politykę prywatności, która była nieodpowiednia pod kilkoma względami. Włoski organ stwierdził również, że do 2 lutego 2023 r. spółka nie wdrożyła żadnych mechanizmów weryfikacji wieku – ani podczas rejestracji, ani podczas korzystania z usługi – pomimo zadeklarowania, że osoby niepełnoletnie są wykluczone z grona potencjalnych użytkowników.

Oceny techniczne wykazały, że system weryfikacji wieku wdrożony obecnie przez administratora nadal jest wadliwy pod kilkoma względami.

Z tych powodów, oprócz nałożenia grzywny, włoski organ nadzoru nakazał spółce dostosowanie operacji przetwarzania danych do przepisów rozporządzenia.

Decyzja

Włoski organ nadzoru nałożył na Luka Inc. grzywnę administracyjną w wysokości 5 milionów euro za naruszenie art. 5 ust. 1 lit. a) i art. 6; art. 5 ust. 1 lit. a), art. 12, 13, art. 5 ust. 1 lit. c), art. 24 i art. 25 ust. 1 RODO.

Ponadto włoski organ zastrzega sobie prawo do zbadania i oceny w odrębnym i niezależnym postępowaniu aspektów dotyczących zgodności z prawem operacji przetwarzania danych przeprowadzanych przez Luka Inc. ze szczególnym uwzględnieniem podstaw prawnych przetwarzania danych mających zastosowanie w całym cyklu życia systemu generatywnej sztucznej inteligencji stanowiącego podstawę usługi Replika.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pixabay

OŚWIADCZENIE IRLANDZKIEGO ORGANU OCHRONY DANYCH W SPRAWIE META AI

W ciągu ostatnich dwóch lat irlandzka Komisja Ochrony Danych (DPC) intensywnie współpracowała z wieloma wiodącymi firmami technologicznymi stojącymi na czele rozwoju sztucznej inteligencji, w szczególności w zakresie wykorzystywania danych osobowych osób dorosłych do szkolenia dużych modeli językowych w UE/EOG. Uznając, że aspekty stosowania RODO do tej szybko zmieniającej się technologii pozostają złożone, poprzez swoje zaangażowanie regulacyjne DPC zapewniła, że firmy rozumieją, co jest wymagane w celu ograniczenia wysokiego ryzyka i szkód dla osób fizycznych. Zaowocowało to wdrożeniem przez wiele firm ulepszeń i dodatkowych zabezpieczeń ochrony danych przed wprowadzeniem na rynek UE.

W marcu 2024 r. Meta poinformowała irlandzką Komisję o swoich planach przeszkolenia swojego dużego modelu językowego przy użyciu treści publicznych udostępnianych przez osoby dorosłe na Facebooku i Instagramie w UE/EOG. Po nawiązaniu współpracy z Meta i zapoznaniu się ze wstępną korespondencją DPC zidentyfikowała szereg kwestii związanych z proponowanym wdrożeniem planów Meta.

DPC przekazała swoje obawy firmie Meta, w następstwie czego ta poinformowała DPC w czerwcu 2024 r. o planach wstrzymania szkolenia w zakresie swojego modelu. DPC nawiązała również współpracę z innymi organami nadzorczymi Europejskiej Rady Ochrony Danych (EROD), starając się uzyskać formalną opinię RODO we wrześniu 2024 roku. Celem DPC w dążeniu do uzyskania opinii było osiągnięcie ogólnoeuropejskiej harmonizacji regulacyjnej i jasności w zakresie szeregu kluczowych kwestii związanych ze szkoleniem i wdrażaniem modeli sztucznej inteligencji. Opinia, która została wydana w grudniu 2024 r., zawierała ogólne kryteria, które organy nadzorcze ds. ochrony danych powinny wziąć pod uwagę przy ocenie zgodności przetwarzania danych osobowych w celu opracowania i wdrożenia modeli sztucznej inteligencji.

Po opublikowaniu Opinii, Meta ponownie oceniła swoją propozycję i 27 maja 2025 roku dostarczyła DPC zaktualizowaną dokumentację dotyczącą planów rozpoczęcia szkolenia generatywnych modeli AI. Po zapoznaniu się z propozycjami firmy Meta i po otrzymaniu informacji zwrotnych od innych organów nadzorczych UE/EOG, DPC skierowała do niej szereg zaleceń dotyczących potencjalnego

wpływu na prawa osób fizycznych do ochrony danych. Meta zareagowała na wnioski DPC w trakcie tego procesu i w rezultacie wdrożyła szereg istotnych środków i ulepszeń, w tym następujące:

• Zaktualizowane powiadomienia o przejrzystości dla użytkowników, w tym specjalne powiadomienia dla wszystkich użytkowników zarówno w 2024, jak i 2025 r.;

• Zaktualizowany i łatwiejszy w użyciu formularz sprzeciwu;

• Zapewnienie użytkownikom dłuższego okresu wypowiedzenia i informacji o dostępnych kontrolach w celu zmiany wszystkich opublikowanych postów z publicznych na prywatne, aby uniknąć szkolenia w zakresie modelu;

• Zapewnienie działania formularzy sprzeciwu w aplikacji i we wszystkich jurysdykcjach w całej Europie;

• Zapewnienie dostępu do formularza sprzeciwu przez ponad rok;

• Aktualizacja środków ochrony osób, których dane dotyczą, takich jak deidentyfikacja, filtrowanie zbiorów danych i filtry wyjściowe; oraz

• Aktualizacja ocen ryzyka i innych dokumentów wymaganych na mocy RODO, takich jak ocena uzasadnionego interesu, ocena skutków dla ochrony danych i ocena zgodności.

W ramach stałego monitorowania DPC zażądał od firmy Meta sporządzenia raportu, który między innymi będzie zawierał zaktualizowaną ocenę skuteczności i adekwatności wprowadzonych przez nią środków i zabezpieczeń w odniesieniu do odbywającego się przetwarzania. Sprawozdanie to ma zostać sporządzone w październiku 2025 r.

DPC nadal aktywnie monitoruje wdrażanie formularzy sprzeciwu (i informacji dla użytkowników), aby zapewnić wszystkim zainteresowanym osobom możliwość sprzeciwienia się przetwarzaniu ich publicznych postów (prywatne posty nie są objęte zakresem). Użytkownicy otrzymają powiadomienia na Facebooku i Instagramie informujące ich, w jaki sposób mogą sprzeciwić się przetwarzaniu danych. Użytkownicy otrzymają również informacje o tym, w jaki sposób szkolenie AI wpływa na ich dane osobowe, a także o innych środkach, jakie użytkownicy mogą podjąć, aby uniknąć wykorzystywania ich danych w tym celu, na przykład poprzez zmianę ustawień wszystkich swoich publicznych postów na prywatne.

DPC przypomina wszystkim osobom korzystającym z mediów społecznościowych i platform internetowych o regularnym sprawdzaniu ustawień prywatności i kontroli, aby nadal odzwierciedlały one ich osobiste preferencje.

5 SPRAWY MIĘDZYNARODOWE

DPC będzie nadal oceniać zgodność wszystkich firm w tym obszarze i w razie potrzeby będzie nadal wykonywać pełen zakres swoich funkcji regulacyjnych. Naszym celem na etapie przetwarzania wstępnego jest zapewnienie, że firmy wprowadzają innowacje w sposób odpowiedzialny, łagodzą zidentyfikowane szkody i zagrożenia dla osób fizycznych oraz odpowiednio uwzględniają prawa osób, których dane dotyczą, równoważąc i chroniąc prawa podstawowe przed interesami firm. DPC, jako wiodący organ nadzorczy dla wielu dużych globalnych firm technologicznych, nadal reguluje sprawiedliwie, konsekwentnie i spójnie, dążąc do zapewnienia, że wszystkie podmioty opracowujące i wdrażające modele sztucznej inteligencji w UE/EOG są traktowane w ten sam sposób.

Źródło: Komunikat irlandzkiego organu nadzorczego

fot. pixabay

CNIL PUBLIKUJE ROCZNE SPRAWOZDANIE ZA 2024 R.

Podnoszenie świadomości, kontrole i kary, wykorzystanie sztucznej inteligencji, nowe narzędzia wsparcia, a także współpraca na szczeblu europejskim i międzynarodowym – to kluczowe zagadnienia poruszone w sprawozdaniu. Dokument ten przedstawia najważniejsze wydarzenia oraz liczne osiągnięcia w obszarze ochrony danych osobowych.

Co roku francuska Krajowa Komisja ds. Technologii Informacyjnych i Swobód Obywatelskich (CNIL) publikuje sprawozdanie ze swojej działalności, podsumowując działania realizowane w ramach czterech kluczowych misji: informowania i ochrony społeczeństwa, wspierania oraz doradzania profesjonalistom i organom administracji publicznej, przewidywania zmian i wdrażania innowacji na rzecz cyfrowej przyszłości, a także monitorowania i egzekwowania przepisów ogólnego rozporządzenia o ochronie danych (RODO) oraz innych regulacji. Rok 2024 upłynął pod znakiem intensywnych działań i istotnych postępów.

Kontrole i kary: znaczny wzrost liczby decyzji

W 2024 roku CNIL przeprowadziła kilkaset kontroli u administratorów i podmiotów przetwarzających dane, zarówno w sektorze publicznym, jak i prywatnym. Działania te były podejmowane w odpowiedzi na otrzymane skargi, zgłoszenia naruszeń, bieżące wydarzenia lub w ramach realizacji priorytetowych tematów nadzorczych. Kontrole dotyczyły m.in. zgodności z przepisami dotyczącymi stosowania plików cookie i innych technologii śledzących, zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych (cyberbezpieczeństwo) oraz zasad wykorzystywania systemów dozoru wizyjnego.

W efekcie CNIL wydała łącznie 331 środków naprawczych. Wśród nich znalazło się 87 decyzji nakładających kary, w tym kary pieniężne o łącznej wysokości ponad 55 milionów euro. Znaczącą część – 69 kar – nałożono w ramach uproszczonej procedury wdrożonej w 2022 roku dla spraw o niewielkim stopniu złożoności. Liczba nałożonych w ten sposób kar wzrosła niemal trzykrotnie w porównaniu z rokiem 2023, co potwierdza skuteczność tego trybu postępowania.

Skargi: rekordowa liczba otrzymanych wniosków

Rok 2024 był rekordowy pod względem liczby skarg wniesionych do CNIL – urząd otrzymał łącznie 17 772 skargi dotyczące naruszeń przepisów o ochronie danych osobowych.

Najwięcej skarg dotyczyło obszaru telekomunikacji, internetu i mediów społecznościowych (49%), następnie sektora handlu i usług (19%) oraz środowiska pracy (13%). Dane te potwierdzają rosnące wyzwania związane z masowym przetwarzaniem danych w środowisku cyfrowym oraz konieczność stałego monitorowania zgodności z RODO w różnych sektorach gospodarki.

Cyberbezpieczeństwo: rosnące zagrożenia

W 2024 r. CNIL otrzymała powiadomienia o 5629 naruszeniach danych osobowych, co stanowi wzrost o 20% w porównaniu z rokiem 2023. Oprócz tego znaczącego wzrostu najbardziej niepokojącym trendem jest wzrost liczby naruszeń na bardzo dużą skalę.

Liczba naruszeń bezpieczeństwa, które dotknęły ponad milion osób, podwoiła się w ciągu jednego roku, wzrastając z około dwudziestu do około czterdziestu udanych ataków, dotykając także podmiotów prywatnych i publicznych.

AI: początkowe zasoby wzmacniające narzędzia wsparcia

Rozwój sztucznej inteligencji jest kluczowy dla perspektyw technologicznych i ekonomicznych, jednak rozwój ten wymaga, zgodnie z założeniami, gromadzenia dużej ilości danych, które mogą mieć charakter danych osobowych.

W nawiązaniu do planu działań z 2023 roku, CNIL opublikowała pierwsze zalecenia dotyczące rozwoju systemów AI w formie 12 arkuszy praktycznych, z których 9 opublikowano w wersji ostatecznej po konsultacjach z zainteresowanymi stronami. W dokumentach tych krok po kroku omówiono kwestie, które należy uwzględnić, aby zapewnić innowacyjność z poszanowaniem ochrony danych. Ponadto CNIL wydała pierwszą serię pytań i odpowiedzi dotyczących wykorzystania sztucznej inteligencji generatywnej.

Świadomość społeczna: zwiększona liczba interakcji w celu ochrony nieletnich

Dane nieletnich i ich prawa do nich są w centrum obecnych wydarzeń: dostęp do treści pornograficznych, kontrola rodzicielska i nadzór, cyberprzemoc, edukacja medialna itp. CNIL przeprowadziła 84 akcje w terenie, aby podnieść świadomość w tym zakresie wśród młodych ludzi, ich rodziców, nauczycieli i mediatorów.

Źródło: Komunikat francuskiego organu nadzorczego

PRZEDSTAWICIELE UODO NA KONFERENCJI DIGITAL DRAGONS – WYZWANIA OCHRONY DANYCH W ŚWIECIE GIER

W dniach 18-19 maja 2025 r. w Krakowie odbyła się konferencja Digital Dragons, wydarzenie dotyczące branży gier w Europie. Tegoroczna edycja skupiła się na kwestiach związanych z dynamicznym rozwojem sektora, w tym na aspektach prawnych i ochronie prywatności graczy. W wydarzeniu uczestniczyli przedstawiciele Urzędu Ochrony Danych Osobowych – prezes UODO, Mirosław Wróblewski, oraz zastępca dyrektorki Departamentu Współpracy Międzynarodowej, Krzysztof Król.

Wystąpienie Prezesa UODO: Ochrona dzieci w świecie cyfrowym

Prezes UODO, Mirosław Wróblewski, wygłosił prelekcję zatytułowaną „Verifying Gamers – Age with Privacy in Mind", w której poruszył kwestię konieczności skutecznej weryfikacji wieku graczy w kontekście ochrony dzieci w przestrzeni cyfrowej. W swoim wystąpieniu wskazał, że aż 71% dzieci spędza w internecie średnio 7 godzin dziennie, co czyni kwestię ochrony najmłodszych priorytetem. Podkreślił również, że mniej niż połowa rodziców korzysta z dobrowolnych mechanizmów kontroli dostępu.

Wyjaśnił znaczenie mechanizmów pozwalających na skuteczną weryfikację wieku użytkowników. Przedstawione zostały różne metody – od prostych deklaracji użytkowników, przez skanowanie dokumentów, aż po rozwiązania oparte na sztucznej inteligencji oraz cyfrowe tokeny. Prezes UODO zwrócił uwagę na konieczność równowagi między ochroną prywatności a skutecznością takich mechanizmów, wskazując na obowiązujące regulacje, w tym RODO oraz akt o usługach cyfrowych (DSA).

Ważnym punktem wystąpienia była analiza wytycznych Europejskiej Rady Ochrony Danych (EROD), z lutego 2025 r., które zawierają zestaw 10 zasad dotyczących zgodnej z RODO weryfikacji wieku. Celem tych zasad jest zapewnienie jednolitego podejścia w całej Unii Europejskiej, przy jednoczesnym minimalizowaniu przetwarzania danych i ochronie praw dzieci. Mirosław Wróblewski omówił również możliwości wynikające z nowej wersji rozporządzenia eIDAS 2.0, które może umożliwić stosowanie cyfrowych portfeli tożsamości w kontekście weryfikacji wieku, ograniczając jednocześnie zakres przetwarzanych danych.

5 SPRAWY MIĘDZYNARODOWE

Krzysztof Król uczestniczył w panelu „Legal Summit powered by Rymarz Zdort Maruta", gdzie omawiano prawne wyzwania związane z ochroną danych osobowych w sektorze gier. W szczególności skupiono się na problematyce zbierania danych o aktywności graczy, które mogą mieć charakter danych szczególnych kategorii. Paneliści dyskutowali o odpowiedzialności firm za ich przetwarzanie oraz konieczności stosowania mechanizmów zgodnych z RODO.

Na fot. Mirosław Wróblewski, prezes Urzędu Ochrony Danych Osobowych
Zdjęcie organizatora - Kancelaria RZM

Na fot. wśród panelistów, pierwszy z prawej – Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej w Urzędzie Ochrony Danych Osobowych
Zdjęcie organizatora - Kancelaria RZM

PODSUMOWANIE XV EDYCJI PROGRAMU „TWOJE DANE – TWOJA SPRAWA”

Za nami jubileuszowa, XV edycja ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa”. W organizowanych przez Urząd Ochrony Danych Osobowych konkursach i webinarach wzięły udział 352 szkoły podstawowe, ponadpodstawowe i placówki doskonalenia nauczycieli.

Świadomi od najmłodszych lat – edukacja o ochronie danych osobowych, w tym wizerunku

Program „Twoje dane – Twoja sprawa” to wyjątkowa inicjatywa, która od 15 lat kształtuje postawy młodych ludzi i wzmacnia kompetencje nauczycieli oraz dyrektorów szkół w zakresie ochrony danych osobowych, bowiem zadaniem Urzędu Ochrony Danych Osobowych jest nie tylko egzekwowanie przepisów prawa, ale również budowanie kultury świadomego i odpowiedzialnego korzystania z wolności obywatelskich – w tym prawa do prywatności i ochrony danych.

W bieżącej edycji Programu 61 348 uczniów uczestniczyło w zajęciach i wydarzeniach tematycznych, a 5 921 nauczycieli zostało przeszkolonych i zaangażowanych w działania edukacyjne dotyczące ochrony danych osobowych. Łącznie w ramach tegorocznej inicjatywy UODO odbyło się 6 213 lekcji i wydarzeń edukacyjnych wspierających szkolną edukację. Wiele szkół zorganizowało Dzień Ochrony Danych Osobowych, do UODO zgłoszono aż 449 pomysłów na celebrację tego święta.

W czasie trwania całego Programu zapewniliśmy uczestnikom dostęp do różnorodnych materiałów edukacyjnych, szkoleń i webinariów organizowanych przez UODO – zarówno dla uczniów, jak i dla nauczycieli oraz rodziców.

Finałowy akcent stanowiła uroczysta gala podsumowująca działania uczniów, nauczycieli i szkół zaangażowanych w promowanie ochrony danych osobowych w życiu codziennym oraz świadomego i odpowiedzialnego korzystania z nowych technologii.

Uroczyste podsumowanie XV edycji ogólnopolskiego Programu edukacyjnego „Twoje dane – Twoja sprawa”

Zwieńczeniem XV edycji była Gala Finałowa Konkursów Prezesa UODO, która odbyła się 27 maja 2025 r. w Centrum Konferencyjnym Lotniska Chopina w Warszawie. Wydarzenie zorganizowaliśmy we współpracy z Fundacją Polskich Portów Lotniczych, co zainaugurowało nową współpracę UODO z PPL na rzecz wspierania edukacji o ochronie danych osobowych.

Otwarcia dokonali organizatorzy wydarzenia: Agnieszka Grzelak, zastępczyni Prezesa UODO oraz Joanna Bochniarz, prezeska Fundacji Polskich Portów Lotniczych. W gali udział wzięli finaliści konkursów na najlepszy komiks edukacyjny oraz na najlepszą inicjatywę edukacyjną. Laureaci mieli okazję zaprezentować swoje działania, a spotkanie było nie tylko formą podsumowania pracy uczestników, lecz także przestrzenią do inspirującej wymiany doświadczeń oraz zacieśnienia współpracy między placówkami oświatowymi i instytucjami partnerskimi.

W wydarzeniu uczestniczyła wiceminister edukacji narodowej Katarzyna Lubnauer, która podkreśliła:

„Wiedza o ochronie danych powinna trafić do młodych ludzi, to bardzo ważne. Pracujemy nad zmianami przedmiotów szkolnych, tworzymy nowy przedmiot – edukacja obywatelska; i nie wyobrażam sobie, by uczniowie nie uczyli się o ochronie danych osobowych i tym, jaką one są wartością."

Rzeczniczkę Praw Dziecka reprezentowała Anna Figurniak, dyrektor Biura Dyrektora Generalnego, która przekazała słowa Rzeczniczki Moniki Horny-Cieślak:

„To bardzo ważna chwila. Ochrona danych osobowych dotyczy dzieci. I mamy dużo pracy do wykonania w zakresie uświadamiania, że dane osobowe nie dotyczą tylko dorosłych, tylko dotyczą osób małoletnich."

Obecność przedstawicieli Ministerstwa Edukacji Narodowej oraz Biura Rzeczniczki Praw Dziecka podkreśliła rangę wydarzenia i znaczenie tematyki ochrony danych osobowych w procesie kształcenia młodego pokolenia.

Po części inauguracyjnej, na zaproszenie Fundacji Polskich Portów Lotniczych, laureaci wraz z opiekunami wzięli udział w wyjątkowej wycieczce z przewodnikiem po Lotnisku Chopina. Była to niepowtarzalna okazja do zobaczenia miejsc na co dzień niedostępnych dla pasażerów i poznania kulis funkcjonowania największego portu lotniczego w Polsce. To niezapomniane przeżycie pozwoliło uczestnikom przekonać się, jak w tak specyficznym środowisku organizowana jest ochrona danych osobowych.

Temat edycji: ochrona wizerunku i edukacja cyfrowa

Tegoroczna edycja Programu skupiała się w szczególności na ochronie wizerunku – temacie niezwykle aktualnym w kontekście aktywności młodzieży w mediach społecznościowych oraz ich powszechnego dostępu do nowych technologii. Uczniowie dowiedzieli się, że ich wizerunek to dane osobowe wymagające szacunku i świadomego zarządzania – zarówno przez nich samych, jak i przez otoczenie. Podczas gali wielokrotnie podkreślano, że ochrona wizerunku to nie tylko kwestia praw-

na, ale również element budowania szacunku wobec siebie i innych w przestrzeni cyfrowej.

W trakcie wydarzenia zaprezentowano najciekawsze inicjatywy zrealizowane w szkołach – konkursy, warsztaty, gry, scenariusze lekcji i projekty międzyszkolne. Wszystkie działania łączył wspólny cel: kształtowanie kultury ochrony danych osobowych wśród dzieci i młodzieży.

Szczególnym wsparciem w realizacji celów Programu były konkursy. To narzędzie, które zachęca do głębszego zainteresowania się tematyką ochrony danych osobowych, podejmowania innowacyjnych i atrakcyjnych form edukacji oraz opracowania materiałów, które ułatwiają zrozumienie tej tematyki. Spotkanie było więc doskonałą okazją do uhonorowania osiągnięć laureatów konkursów Prezesa UODO, zaprezentowania efektów Programu, a także do wymiany doświadczeń i zacieśnienia współpracy pomiędzy partnerami, uczestnikami i instytucjami wspierającymi inicjatywę.

Jak podkreślała zastępczyni Prezesa UODO, dr Agnieszka Grzelak: „Ochrona danych osobowych dzieci to nie tylko obowiązek prawny – to realna ochrona ich tożsamości, godności i bezpieczeństwa. Celem naszego Programu jest nie tylko przekazywanie wiedzy, ale budowanie kultury ochrony danych – w każdej szkole, w każdej klasie, w każdej relacji między uczniami, nauczycielami i rodzicami."

W tym duchu tegoroczna edycja Programu pokazała, jak wielkie znaczenie mają inicjatywy edukacyjne w obszarze ochrony danych dzieci, które nie tylko uczą przepisów, ale także kształtują empatię, szacunek i odpowiedzialność – wartości niezbędne w dojrzałym społeczeństwie.

Kontynuacja Programu

UODO zapowiada kontynuację i rozwój Programu w nadchodzącej edycji. W szczególności planowane jest wsparcie szkół w zakresie uwzględniania tematyki ochrony danych osobowych podczas lekcji edukacji zdrowotnej i edukacji obywatelskiej. Takie podejście ma na celu wzmocnienie systemowego podejścia do edukacji nt. ochrony danych osobowych i nadanie jej trwałego miejsca w podstawie programowej. Do tej pory zajęcia dla uczniów były realizowane na lekcji informatyki i etyki oraz w ramach programów profilaktyczno–wychowawczych w szkołach.

„Już dziś zapowiadamy kontynuację i rozszerzenie naszych działań. Skoncentrujemy się na wzmacnianiu kompetencji nauczycieli i dyrektorów szkół – tak, by edukacja w zakresie ochrony danych była nie tylko obowiązkiem, ale i naturalną częścią wychowania ku odpowiedzialnemu obywatelstwu. Dziękujemy za Państwa zaangażowanie, pasję i wiarę w wartość edukacji, która chroni człowieka". – podkreśliła Anna Dudkowska, dyrektorka Departamentu Inicjatyw Edukacyjnych w Urzędzie Ochrony Danych Osobowych.

Zarówno gala, jak i całoroczna praca szkół biorących udział w XV edycji Programu pokazały, że temat danych osobowych – w tym wizerunku – staje się coraz bardziej zrozumiały i istotny dla młodych ludzi. Dzięki zaangażowaniu nauczycieli i wsparciu UODO edukacja w tym zakresie staje się nie tylko obowiązkiem, ale i realną potrzebą najmłodszych pokoleń.

„Z ogromnym uznaniem i wdzięcznością spoglądamy dziś na efekty wspólnej pracy w ramach Programu „Twoje dane – Twoja sprawa". Ten Program to nie tylko cykl działań edukacyjnych – to wyraz naszej głębokiej troski o przyszłość młodego pokolenia, ich bezpieczeństwo i świadomość w świecie pełnym wyzwań cyfrowych. Szczególne wyrazy podziękowania składamy dla tych uczestników, którzy od wielu lat wspierają nasze działania". – zaznaczyła Marta Mikołajczyk, koordynatorka Programu w Departamencie Inicjatyw Edukacyjnych UODO.

Podziękowania

Dziękujemy wszystkim, którzy przyczynili się do sukcesu tej edycji: dyrektorom szkół i placówek doskonalenia nauczycieli, nauczycielom i uczniom – za zaangażowanie w działania i organizację tak wielu społecznie użytecznych inicjatyw.

Serdeczne podziękowania kierujemy do patronów honorowych Programu – Ministra Edukacji Narodowej i Rzecznika Praw Dziecka, za wsparcie edycji i konkursów oraz wieloletnią, nieustającą i owocną współpracę na rzecz ochrony danych osobowych dzieci.

Podziękowania składamy także patronom medialnym za informowanie o realizowanych działaniach, w tym przede wszystkim Głosowi Nauczycielskiemu, Portalowi Oświatowemu, TiK w Edukacji, Polskiemu Radiu Dzieciom, a także TVP2 „Pytanie na Śniadanie".

Szczególne podziękowania kierujemy również do wszystkich kuratoriów oświaty oraz urzędów miast – Warszawy i Krakowa – za aktywny udział w kampanii promocyjnej XV edycji Programu. Dzięki ich zaangażowaniu spoty informacyjne były wyświetlane w komunikacji miejskiej: w Warszawie w dniach 16–22 września oraz w Krakowie w dniach 21–27 września. Spoty dotarły do szerokiego grona odbiorców, zwiększając świadomość społeczną w obszarze ochrony danych osobowych.

Nieocenionym wsparciem przy realizacji XV edycji było także zaangażowanie Polskiej Policji, która publikowała w swoich mediach społecznościowych informacje o naborze do Programu.

Dzięki wspólnym działaniom i zaangażowaniu wielu instytucji mogliśmy po raz kolejny stworzyć inicjatywę, która realnie wpływa na edukację i bezpieczeństwo młodych obywateli.

6 EDUKACJA

Zapraszamy do XVI edycji Programu „Twoje dane – Twoja sprawa”

już we wrześniu!

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl