URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 04/04/25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

na początek przypomnienie: w lipcu 2025 r. UODO zmienia siedzibę. Budynek przy ul. Stawki 2 idzie do remontu. Naszą nową siedzibą będzie budynek przy ul. Moniuszki 1A, 00-014 Warszawa.

Zmiana siedziby nie wiąże się z obowiązkiem zamieszczenia nowego adresu urzędu w klauzulach informacyjnych administratorów ochrony danych. Jednak ci administratorzy, którzy w swoich klauzulach informacyjnych zamieścili dokładny adres UODO, są zobowiązani do aktualizacji tej informacji.

Druga ważna wiadomość: w maju będzie można nas spotkać w Poznaniu. W ramach akcji „UODO rusza w kraj" będziemy tam 20 i 21 maja.

Akcja ta jest elementem naszej działalności edukacyjnej, bowiem im więcej wiemy o danych osobowych, tym sprawniej i lepiej możemy działać. W kwietniu udało nam się wykonać w tym zakresie ważny krok: MEN zgodziło się z naszymi propozycjami i od 1 września 2025 r. uczniowie będą zdobywać wiedzę na temat ochrony danych osobowych nie tylko w ramach przedmiotów informatyka i etyka, ale także w ramach edukacji obywatelskiej oraz edukacji zdrowotnej. To istotna zmiana, która pozwoli młodym ludziom lepiej rozumieć zagadnienia związane z ochroną prywatności, odpowiedzialnym przetwarzaniem danych osobowych, a także z bezpiecznym korzystaniem z technologii cyfrowych.

Dane osobowe dotyczą każdego elementu naszego życia:

• W kwietniu wystąpiłem do Rzecznika Praw Obywatelskich o wsparcie w rozwiązaniu problemu prawnego dotyczącego danych osobowych przetwarzanych w Instytucie Pamięci Narodowej. Zgodnie z dotychczasowym orzecznictwem sądów administracyjnych art. 71 ustawy o IPN nie wyłącza ustanowionych w RODO kompetencji nadzorczych Prezesa Urzędu Ochrony Danych Osobowych w sprawie przetwarzania przez IPN danych osobowych, lecz rozszerza je na dane osób zmarłych.

Tymczasem NSA w wyroku z 5 lutego 2025 r. wyraził pogląd odmienny. Uznał, że art. 71 ustawy o IPN należy odczytywać w ten sposób, że przepisy RODO znajdują zastosowanie wyłącznie do Bazy Materiału Genetycznego, którą IPN tworzy w celu prowadzenia prac poszukiwawczych oraz identyfikacji, a zatem kompetencje PUODO dotyczą tylko danych osobowych przetwarzanych w tej Bazie.

Dlatego zwróciłem się do RPO, by ten wystąpił o podjęcie przez Naczelny Sąd Administracyjny uchwały mającej na celu wyjaśnienie rozbieżności w orzecznictwie sądów administracyjnych. RPO przysługuje takie ustawowe uprawnienie, Prezesowi UODO – nie.

• Poprosiłem Ministra Spraw Zagranicznych, by ustawa o wykonywaniu orzeczeń Europejskiego Trybunału Praw Człowieka uwzględniała zagadnienia dotyczące danych osobowych i prawa do prywatności. PUODO chętnie się w nie włączy. Po to jesteśmy – żeby wspierać i pomagać.

• Ministerstwo Rozwoju uznało nasze uwagi dotyczące przepisów o ułatwieniach w przygotowaniu i realizacji inwestycji mieszkaniowych. Chodzi o to, że w obecnej wersji wymagają zamieszczania numerów ksiąg wieczystych we wnioskach o ustalenie lokalizacji inwestycji oraz w podejmowanych w tych sprawach uchwałach rady gminy. A uchwały te publikowane są następnie w BIP, i każdy może sobie zajrzeć do danych z ksiąg wieczystych. Ministerstwo zapowiedziało, że zmieni te przepisy.

• Zakład pogrzebowy zgubił w czasie transportu dane swoich klientów – znaleziono je w rowie przy drodze. To jedna z tych historii, które pokazują, że gdyby administrator danych przeprowadził porządną analizę ryzyka dla danych, zapewne nie przewoziłby potem swojej dokumentacji na odkrytej przyczepie bez żadnego nadzoru. To poważne zaniedbanie doprowadziło do incydentu i za nie – a nie za zgubienie danych – byłem zmuszony nałożyć na administratora karę finansową.

Stanowiska PUODO

Z naszych ważnych stanowisk chciałbym zwrócić uwagę na wystąpienie do władz Polskiego Radia z przypomnieniem, jak można przetwarzać dane osobowe w materiałach dziennikarskich. To pokłosie głośnej sprawy Radia Szczecin, którego dziennikarz ujawnił dane dziecka, które miało być ofiarą pedofila. Dziecko to potem popełniło samobójstwo.

Wskazaliśmy również na problem kamer nasobnych ratowników medycznych. Po ujawnionych przez media przypadkach ataków na ratowników udzielających pomocy rząd szuka sposobów zwiększenia ich bezpieczeństwa. Jednym z pomysłów jest wyposażenie ratowników w kamery nasobne. Trzeba go jednak rozważyć, uwzględniając głęboką ingerencję takiego rozwiązania w prywatność – zarówno ratowników, jak i osób, którym udzielana jest pomoc. Wystąpienie do Ministra Zdrowia było konsekwencją pisma Krajowej Sekcji Pogotowia Ratunkowego i Ratownictwa Medycznego NSZZ „Solidarność".

Ważne wyroki

Naczelny Sąd Administracyjny podtrzymał decyzję Prezesa UODO o nałożeniu kary administracyjnej w wysokości 25 tys. zł na Śląski Uniwersytet Medyczny w Katowicach za niezgłoszenie naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu osób, których dane dotyczą.

NSA uwzględnił również skargę kasacyjną RPO od wyroku WSA, który wcześniej podtrzymał decyzję PUODO z 6 kwietnia 2020 r. w sprawie tzw. ustawy kagańcowej. NSA uchylając wyrok sądu niższej instancji, przychylił się tym samym do stanowiska RPO, zgodnego z nowym stanowiskiem organu nadzorczego w tej sprawie, gdyż w maju 2024 r. wystosowałem pismo procesowe, w którym wniosłem o uwzględnienie skargi kasacyjnej RPO.

Wiedzą o danych osobowych dzieliliśmy się jak zwykle na licznych spotkaniach i konferencjach

Wspomnę tu tylko o:

• debacie „Przeciwdziałanie przestępstwom w świecie cyfrowym" na 29. Banking & Insurance Forum,

• konferencji Służby Geodezyjnej i Kartograficznej „Wykorzystanie nowoczesnych technologii w geodezji i kartografii",

• konferencji „Ochrona danych osobowych w dobie współczesnych wyzwań" na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu,

• konferencji „Centralny Rejestr Umów Jednostek Sektora Finansów Publicznych jako narzędzie jawności życia publicznego. Plany i wyzwania", zorganizowanej przez Ministerstwo Finansów, Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego oraz Wydział Prawa i Administracji Uniwersytetu Łódzkiego,

• konferencji „Dzień ochrony danych osobowych w medycynie".

Więcej o spotkaniach, które organizujemy i w których bierzemy udział, można się dowiedzieć pod tagiem: https://uodo.gov.pl/tag/spotkanie.

• Kolejny wykład ekspercki z cyklu „Ochrona danych i technologia" jest dostępny pod adresem https://uodo.gov.pl/pl/593/3653.

Na koniec chcę się z Państwem podzielić radością z powodu uhonorowania mnie prestiżowym tytułem „Wybitna Osobowość Roku 2025 – Wizjoner Prawa" podczas gali „Osobowości i Sukcesy" 2025, która odbyła się 13 kwietnia w Warszawie.

Tej nagrody nie byłoby bez byłych i obecnych współpracowników w UODO, Biura RPO, samorządu radców prawnych oraz organizacji społecznych. To wspólna praca i zaangażowanie tych środowisk pozwalają skutecznie chronić prawa obywatelskie, współpracować z instytucjami publicznymi, pozarządowymi, biznesowymi i naukowymi, zarówno w zakresie egzekucji prawa, jak i edukacji prawnej całego społeczeństwa.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Tym razem na łamach Biuletynu gościmy duet ekspertów – Jacka Młotkiewicza, dyrektora Departamentu Kontroli i Naruszeń w UODO oraz Katarzynę Hildebrandt, zastępcę dyrektora DKN. Rozmawiamy m.in. o tym, z jak dużym zainteresowaniem spotkała się publikacja poradnika UODO dotyczącego naruszeń ochrony danych osobowych, o kontrolach sektorowych, oraz o tym, w jakim zakresie DKN współpracuje z organami nadzorczymi z innych państw.

Współdziałanie z pozostałymi urzędami ochrony danych pozwala na obserwację ich dobrych praktyk, co przekłada się na lepsze funkcjonowanie naszego Urzędu. Dlatego cieszymy się z wizyt studyjnych dotyczących wdrażania DGA w Polsce. Dzięki nim dowiemy się, w jaki sposób instytucje w Finlandii i na Węgrzech wdrożyły Akt w sprawie zarządzania danymi, co przyczyni się w bezpośredni sposób do bardziej efektywnego wprowadzenia w życie DGA w naszym kraju.

Podczas lutowego szczytu w Paryżu poświęconego działaniom na rzecz sztucznej inteligencji (AI Action Summit), organy ochrony danych z Australii, Korei, Irlandii, Francji i Wielkiej Brytanii podpisały wspólne oświadczenie, aby potwierdzić swoje zaangażowanie w zarządzanie danymi, które wspiera innowacyjną i chroniącą prywatność sztuczną inteligencję. Mamy nadzieję, że podobnych działań będzie przybywać. W tym kontekście warto wspomnieć, że w marcu Meta wprowadziła dla regionu europejskiego rozwiązanie polegające na wykorzystaniu technologii rozpoznawania twarzy, aby przeciwdziałać zjawisku „celeb-bait", tj. rozpowszechnianiu przez cyberprzestępców treści zawierających przetworzone wizerunki znanych osób.

Rada Europy ogłosiła rok 2025 Europejskim Rokiem Edukacji Cyfrowej (European Year 2025), aby nadać nowy impuls rozwojowi i promocji edukacji cyfrowej we wszystkich państwach członkowskich. To dobra wiadomość. Edukacja jest dla UODO niezwykle ważna. Dbamy o nią w trakcie wszelkich podejmowanych przez nas przedsięwzięć, również w ramach inicjatywy „UODO rusza w kraj". Choć sama akcja skupia się głównie na spotkaniach z mieszkańcami oraz władzami administracji publicznej w poszczególnych województwach, w tym wydaniu periodyku pokazujemy czytelnikom, że dla Urzędu to również sprzyjająca okoliczność, by odwiedzić szkoły, uczestniczące w programie „Twoje dane – Twoja sprawa".

W tym numerze zwracamy uwagę, by przekazując podczas obrad rady miasta określone informacje dotyczące konkretnych osób wyważyć dwie wartości – prawo do informacji publicznej oraz prawo do ochrony danych osobowych. Upublicznianie danych, aby było legalne, musi mieć podstawę

prawną i odbywać się z uwzględnieniem określonych w RODO zasad, w tym ograniczenia celu oraz minimalizacji danych.

Wyjaśniamy, że przewoźnik, decydując się na zlecenie firmie zewnętrznej kontroli biletów i windykacji należności od osób, które nie uiściły opłaty za przejazd, nie przestaje być administratorem przetwarzanych w związku z tym danych osobowych pasażerów.

Przytaczamy decyzję Prezesa UODO dotyczącą monitoringu sąsiedzkiego. Prezes UODO nakazał w niej sąsiadowi skarżącego, by przestał nagrywać to, co się dzieje na klatce schodowej, mimo że sąsiad ten miał w tym interes prawny. Nie był on jednak nadrzędny wobec praw i wolności skarżącego.

W związku z modernizacją Systemu Informacyjnego Schengen, która miała miejsce w 2023 r., Komitet Skoordynowanego Nadzoru opracowuje i sporządza roczne sprawozdanie dla Europejskiej Rady Ochrony Danych na temat wykonywania praw osób, których dane dotyczą, postępowań sądowych i wzajemnego uznawania ostatecznych decyzji dotyczących SIS. Wszystkie państwa członkowskie muszą zapewnić pełne przygotowanie swoich procedur wewnętrznych, aby móc rejestrować statystyki w formacie wymaganym decyzją wykonawczą Komisji i terminowo przekazywać je EROD.

Piszemy też o innych działaniach podejmowanych przez Europejską Radę Ochrony Danych:

• zakończeniu przedłużonych konsultacji publicznych dotyczących wytycznych EROD 1/2025 w sprawie pseudonimizacji;

• rozpoczętych działaniach w ramach skoordynowanego egzekwowania prawa (CEF), na rok 2025. W tym roku CEF skupi się na wdrożeniu prawa do usunięcia danych.

Przybliżamy też dwie kary europejskich organów nadzorczych:

• islandzkiego – za niezgodne z prawem przetwarzanie danych w związku z integracją systemów dokumentacji medycznej oraz

• fińskiego – za zaniedbania w zakresie bezpieczeństwa danych. Kara została nałożona na porównywarkę pożyczek. W porównywarkach firmy brakowało m.in. odpowiednich ograniczeń uniemożliwiających osobom trzecim dostęp do danych zawartych we wnioskach o pożyczkę.

Z życzeniami miłej majówkowej lektury,

Karol Witowski
Rzecznik Prasowy UODO

ZALEŻAŁO NAM NA PRZYGOTOWANIU PORADNIKA KOMPLEKSOWEGO, PRZYSTĘPNEGO I PRZEJRZYSTEGO

Z Jackiem Młotkiewiczem, dyrektorem Departamentu Kontroli i Naruszeń oraz z zastępcą dyrektora, Katarzyną Hildebrandt, rozmawiał Karol Witowski, Rzecznik Prasowy UODO.

28 marca 2025 r. odbyło się webinarium na temat zaktualizowanego poradnika UODO dotyczącego naruszeń ochrony danych osobowych. Webinarium wysłuchało 1500 osób, kilkaset pytań zostało zadanych na czacie. W marcowym numerze „Biuletynu UODO" pojawił się również materiał DKN odnoszący się do zagadnień, które zostały podjęte w przestrzeni publicznej. Oczekiwania wobec Urzędu osób zainteresowanych kontynuacją tematów poruszonych w poradniku są ogromne.

Jacek Młotkiewicz: Temat naruszeń ochrony danych osobowych jest na tyle szeroki, że – jak widać – nie sposób go tak łatwo wyczerpać, nawet poświęcając mu 100-stronicowy poradnik i ponad trzygodzinne webinarium. Ta sytuacja jasno pokazuje, że zarówno teoria, jak i praktyka stosowania przepisów RODO w tym zakresie wciąż rodzi dylematy i sprawia administratorom realne trudności.

Między innymi dlatego zależało nam na przygotowaniu poradnika, który obejmie te zagadnienia w sposób kompleksowy, a zarazem przystępny i przejrzysty. Nasza aktywność wokół kwestii zawartych w poradniku to dowód na to, że staramy się wychodzić naprzeciw tym ogromnym oczekiwaniom, stawiając jednocześnie na otwartą komunikację i dialog.

W mediach pojawiło się wiele komentarzy dot. poradnika. Czy są tam informacje, które wymagają sprostowania, nadinterpretacje, które mogą być szkodliwe?

Katarzyna Hildebrandt: RODO nie jest aktem zero-jedynkowym. Mimo że UODO od początku prezentuje w miarę jednoznaczne stanowisko w sprawie stosowania przepisów dotyczących naruszeń ochrony danych osobowych, na przestrzeni lat narosło wokół nich wiele alternatywnych

interpretacji, a nawet przeinaczeń. Poradnik odegrał tu już ważną rolę w kierunku wyjaśnienia ewentualnych niejasności.

J.M.: Dzięki tak dużemu zainteresowaniu przekaz organu nadzorczego ostatecznie dotarł do bardzo szerokiego grona odbiorców. W niektórych środowiskach branżowych spotkał się jednak z niezrozumieniem, a może nawet z oporem, w którego przyczyny nie chciałbym w tej chwili wnikać. Choć uważnie analizujemy i wyciągamy wnioski z krytycznych uwag, niektóre wypowiedzi wykraczały poza granice konstruktywnej krytyki, zahaczając wręcz o dezinformację. Za potencjalnie szkodliwe z pewnością można uznać te komentarze, które – poprzez daleko idącą nadinterpretację – mogły wzbudzić w administratorach nieuzasadnione obawy, a nawet pewnego rodzaju panikę.
Z największymi „mitami" na temat poradnika zmierzyliśmy się podczas ostatniego webinarium, do obejrzenia którego wszystkich serdecznie zapraszam.

Jak przebiegała praca nad poradnikiem? Ile trwała redakcja i jak bardzo różni się wersja zaktualizowana od poprzedniej?

J.M.: Wstępne prace rozpoczęły się już na przełomie lipca i sierpnia ubiegłego roku, zaraz po zakończeniu otwartych konsultacji społecznych. Przygotowaniem poradnika zajął się zespół pracowników DKN, którego prace koordynował Bartłomiej Kowalski – odpowiedzialny za opracowanie finalnej wersji tekstu.

Poszczególne fragmenty były na bieżąco konsultowane z członkami Społecznego Zespołu Ekspertów przy Prezesie UODO. Powstawaniu poradnika towarzyszyły wielogodzinne, bardzo interesujące i merytoryczne dyskusje, podczas których mieliśmy okazję zderzyć różnorodne punkty widzenia.
Z końcem roku materiał był w zasadzie gotowy. Oczywiście wymagał pewnego dopracowania, w związku z czym oficjalna publikacja miała miejsce 20 lutego. Biorąc pod uwagę ostateczny rozmiar publikacji, tempo było naprawdę przyzwoite.

Choć zdecydowaliśmy się sformułować tekst poradnika na nowo, jego podstawowe założenia pozostały zasadniczo niezmienne. Dokument z 2019 r. stanowił dla nas ważny punkt wyjścia, jednak chcieliśmy nieco rozszerzyć jego formułę i dostosować treść do zmieniających się okoliczności – takich jak rozwój technologii czy nowe wytyczne EROD. Istotny był również aspekt językowy: zależało nam na uproszczeniu przekazu oraz na przedstawieniu omawianych zagadnień w sposób zbliżony do komunikacji innych europejskich organów nadzorczych.

Przyznam, że liczba głosów o „zmianie" czy wręcz „zaostrzeniu podejścia Prezesa UODO" była dla nas zaskoczeniem. Kwestie, które finalnie wzbudziły największe kontrowersje, były bowiem podnoszone przez organ nadzorczy od wielu lat – także w materiale z 2019 r.

1 ROZMOWA Z EKSPERTEM

Podczas webinarium anonim napisał: „Jednym z wniosków po webinarium jest chyba konieczność poprawy polityk ochrony danych osobowych oraz dokumentów do analizy ryzyka celem przeprowadzenia nowej analizy ryzyka dla czynności przetwarzania w organizacji. A przynajmniej uaktualnienia ww. dokumentów”. Co Państwo o tym myślą?

J.M.: Jako dyrektor DKN muszę przede wszystkim wyraźnie podkreślić, że systematyczny przegląd i doskonalenie przyjętych rozwiązań w celu ochrony danych oraz regularna ocena ryzyka to podstawowe obowiązki związane z przetwarzaniem danych osobowych. Jeżeli po webinarium ktoś dostrzegł potrzebę weryfikacji metod stosowania RODO, oznacza to, że nasze działania przynoszą pozytywne efekty, a świadomość administratorów rośnie. Przypominam jednak, że tego rodzaju czynności powinny być realizowane cyklicznie – niezależnie od aktywności UODO w tym zakresie.

Przejdźmy do tematu kontroli sektorowych. Jak mogą Państwo w tym kontekście podsumować 2024 rok? Przypomnijmy: kontrolom podlegali przetwarzający dane przy użyciu internetowych (webowych) aplikacji, organy przetwarzające dane osobowe w systemach SIS i VIS oraz prawidłowości spełnienia obowiązku informacyjnego przez podmioty prywatne.

K.H.: Co do zasady podmioty, które przetwarzają dane przy użyciu aplikacji, stosowały niezbędne zabezpieczenia konieczne do zapewnienia dokonywania operacji na danych w sposób pozwalający zapobiec niepożądanym incydentom. Trzeba jednak mieć na względzie specyfikę takiej działalności i zazwyczaj profesjonalne możliwości i podejście takich podmiotów do tworzonych aplikacji.

Jeśli chodzi o kontrole obejmujące swoim zakresem sposób realizacji obowiązku informacyjnego, organ przyjrzał się klauzulom stosowanym przez biura podróży, hotele, biura pośrednictwa pracy, biura pośrednictwa nieruchomości, placówki medyczne. Trzeba przyznać, że w większości przypadków był on realizowany w sposób prawidłowy, jednakże poprawie powinny ulec drobne elementy, jak np. przejrzystość, zrozumiałość.

Jak co roku kontrolowane były organy publiczne przetwarzające dane w SIS oraz VIS, w tym polskie konsulaty działające za granicą. Każda kontrola przynosi kolejne spostrzeżenia co do funkcjonowania tych systemów zarówno w kontekście przepisów unijnych, które mają do nich zastosowanie, jak i praktycznych aspektów ich wykorzystania.

1 ROZMOWA Z EKSPERTEM

Z kolei w tym roku w dużej mierze koncentrujecie się Państwo na bezpieczeństwie danych medycznych i przetwarzaniu danych dzieci. To jedne z głównych obszarów, na których skupiła się uwaga kontrolerów UODO w 2025 roku. Co możecie Pastwo powiedzieć o tegorocznych kontrolach?

K.H.: Jeśli chodzi o dane dzieci, skupiliśmy się na wizerunku pozyskiwanym i publikowanym w internecie przez szkoły, do których uczęszczają uczniowie. Podstawę przetwarzania takich danych stanowi zgoda rodzica bądź opiekuna prawnego. Dlatego też kontrolujący dokładnie sprawdzali sposób wyrażenia takiej zgody. W skontrolowanych placówkach wymagana zgoda na wykorzystanie wizerunku była pozyskiwana. Zgromadzony w toku kontroli materiał dowodowy jest obecnie analizowany w odniesieniu do poszczególnych aspektów dotyczących prawidłowości tej zgody.

W bieżącym miesiącu rozpoczynamy kontrole w placówkach medycznych, podczas których będziemy się skupiać głównie na sposobie przyznawania dostępu do danych osobowych (procedur w zakresie przyznawanych uprawnień), sposobie tworzenia kopii zapasowych i innych zagadnieniach dotyczących zapewnienia bezpieczeństwa danych pacjentów poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych.

Dużą część działań departamentu stanowią kontrole, których przedmiotem są zagadnienia o charakterze międzynarodowym. Na czym one polegają?

K.H.: Rzeczywiście, nasze kontrole dotyczą również takich kwestii. Obowiązek dokonywania kontroli w tym zakresie wynika z przepisów aktów prawa europejskiego. Wskazują one na konieczność sprawdzania sposobu realizacji wymogów, które powinny spełniać systemy informatyczne, służące do przetwarzania danych wprowadzanych przez służby i organy administracji poszczególnych krajów UE (m.in. w celu zapewnienia wysokiego poziomu bezpieczeństwa strefy Schengen, wspierania realizacji wspólnej polityki wizowej UE), do których należy przede wszystkim System Informacyjny Schengen (SIS) oraz Wizowy System Informacyjny (VIS). Kontrolom poddawana jest Policja, Straż Graniczna, placówki dyplomatyczne i inne organy korzystające z systemów służących do wymiany danych między europejskimi państwami.

Czy współpracujecie z innymi organami?

K.H.: Tak, w ramach mechanizmu skoordynowanego nadzoru współpracujemy z Europejskim Inspektorem Ochrony Danych (EIOD) oraz innymi krajowymi organami. Przykładem może być nasz udział we wspólnej kontroli dotyczącej wpisów w SIS dokonywanych na potrzeby kontroli niejawnych. Wnioski z tej kontroli posłużyły do opracowania zaleceń w zakresie jakości i przechowywania danych.

1 ROZMOWA Z EKSPERTEM

Jeden z pracowników brał udział w kontroli Europolu.

K.H.: Zgadza się. Osoba pracująca w naszym departamencie uczestniczyła w kontroli prowadzonej przez EIOD w siedzibie Europolu. Taka współpraca umożliwia lepsze zrozumienie wyzwań w zakresie ochrony danych osobowych występujących na styku naszych krajowych wyzwań oraz tych na poziomie unijnym.

A co z Ewaluacjami Schengen?

K.H.: To kolejny ważny obszar naszej działalności. Eksperci DKN są regularnie powoływani do udziału w ewaluacjach, co pozwala im również na doskonalenie swoich kompetencji. Udział w misjach ewaluacyjnych przyczynia się do skuteczniejszego nadzoru nad przestrzeganiem regulacji w zakresie ochrony danych w strefie Schengen. Co istotne, ewaluacje pozwalają w krótkim czasie zidentyfikować nieprawidłowości i wspólnie wypracować środki zaradcze, które wzmacniają zaufanie między państwami członkowskimi i zapewniają spójne stosowanie dorobku Schengen.

Dziękuję za rozmowę.

fot. zasoby własne UODO. Na zdjęciach: Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń oraz Katarzyna Hildebrandt, zastępca dyrektora

ZAPEWNIANIE JAWNOŚCI ŻYCIA PUBLICZNEGO MUSI ODBYWAĆ SIĘ Z POSZANOWANIEM RODO

Przekazując podczas obrad rady miasta określone informacje dotyczące konkretnych osób trzeba wyważać dwie wartości – prawo do informacji publicznej oraz prawo do ochrony danych osobowych. Upublicznianie danych, aby było legalne, musi mieć podstawę prawną i odbywać się z uwzględnieniem określonych w RODO zasad, w tym ograniczenia celu oraz minimalizacji danych. W każdym przypadku rozważyć trzeba, czy informacje, które się udostępnia, nie będą naruszały prywatności osoby, której dane dotyczą. Także, gdy pełni ona funkcje publiczne.

Wyważanie dwóch praw – prawa do informacji publicznej/jawności życia publicznego i prawa do ochrony danych osobowych wciąż przysparza jednostkom samorządu terytorialnego licznych problemów.

Ich przykładem może być sprawa, która ostatecznie musiała zostać rozstrzygnięta przez Naczelny Sąd Administracyjny.

Dane można ustalić pośrednio

Dotyczyła ona upublicznienia przez prezydenta miasta – składającego radzie miasta sprawozdanie z działalności między sesjami – informacji dotyczących byłego wiceprezydenta, któremu wypłacony został ekwiwalent za niewykorzystany urlop wypoczynkowy. I choć prezydent nie podał jego imienia i nazwiska, to przekazał wiele informacji, na podstawie których można było pośrednio ustalić, o kogo chodzi.

Wskazał bowiem, że osoba ta:

• była urzędnikiem pełniącym funkcję zastępcy prezydenta miasta,

• uzyskała z tytułu pełnionej funkcji określone świadczenia pieniężne, w tym zasiłek chorobowy za 6 miesięcy,

• nie wykorzystała 51 dni urlopu wypoczynkowego na skutek pobierania zasiłku chorobowego, w związku z czym wypłacono jej ekwiwalent za urlop,

• przeszła na emeryturę, a jej stosunek pracy wygasł konkretnego dnia.

Były wiceprezydent uznał, że upublicznienie informacji dotyczących jego przeszłej pracy w urzędzie miasta, realizacji uprawnień pracowniczych i uzyskanych w związku z tym świadczeń ze wskazaniem ich wysokości było nieuprawnione i złożył skargę do Prezesa UODO.

Wyjaśnienia prezydenta

Prezydent miasta w toku prowadzonego postępowania administracyjnego tłumaczył, że nie użył danych indywidualizujących oraz że powiązanie podanych informacji ze skarżącym nie jest możliwe bez nadmiernego wysiłku i kosztów, gdyż nie był on jedyną osobą, która w przeszłości pełniła funkcję zastępcy prezydenta miasta. W jego ocenie, same kwoty świadczeń pieniężnych i data wygaśnięcia stosunku pracy nie wskazują na konkretną osobę. Prezydent podnosił też, że do końca zatrudnienia w urzędzie miasta skarżący był osobą pełniącą funkcję publiczną, a wszystkie informacje, które podał podczas sesji rady miasta, stanowią informację publiczną, bo dotyczą pełnienia przez skarżącego funkcji publicznych i jako takie podlegają upublicznieniu bez ograniczeń, na mocy art. 1 ust. 1 i art. 5 ust. 2 ustawy o dostępie do informacji publicznej, bowiem dotyczą okresu ich pełnienia. Wskazał, że ich ujawnienie było niezbędne w celu odniesienia się do zarzutów byłego prezydenta dotyczących naruszenia jego praw pracowniczych w zakresie wysokości i terminu wypłaty świadczeń związanych ze stosunkiem pracy łączącym go z miastem.

Podnosił też, że przeszła i obecna aktywność byłego prezydenta (udział w wyborach, pełnienie funkcji prezesa zarządu pewnego stowarzyszenia) powoduje, że trudno uznać go za osobę prywatną.

Upomnienie od Prezesa UODO

Prezes UODO nie podzielił tych argumentów i udzielił prezydentowi miasta upomnienia za udostępnienie danych osobowych skarżącego bez podstawy prawnej.

Jednocześnie wskazał, że informacje przekazane podczas sesji rady miasta stanowią dane osobowe w rozumieniu art. 4 pkt 1 RODO, bowiem prezydent podał m.in., do kiedy wnioskodawca był zatrudniony na stanowisku zastępcy prezydenta i że przeszedł na emeryturę. Takie informacje pozwalają – zwłaszcza mieszkańcom miasta – w prosty sposób pośrednio zidentyfikować wnioskodawcę bez nadmiernego wysiłku i kosztów.

Ponadto Prezes UODO zauważył, że udostępnione zostały nie tylko tzw. dane zwykłe, ale również dane dotyczące zdrowia wnioskodawcy, które w świetle przepisów RODO kwalifikowane są jako dane szczególnej kategorii, podlegające szczególnej ochronie prawnej.

Jednocześnie nie zgodził się z opinią prezydenta miasta, że zaskarżony proces przetwarzania danych osobowych miał oparcie w przepisach ustawy o dostępie do informacji publicznej.

Podniósł również, że prezydent miasta, udostępniając dane osobowe byłego wiceprezydenta, naruszył też zasadę minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO.

Udostępnienie danych osobowych wnioskodawcy w zakwestionowany sposób nie było zatem adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których dane osobowe były przetwarzane.

NSA: bezprawne ujawnienie danych

Ostatecznie sprawa znalazła finał w Naczelnym Sądzie Administracyjnym, który przyznał rację Prezesowi UODO. W wyroku z 13 marca 2025 r. (sygn. akt III OSK 8/22) sąd wskazał, że „Organ nadzoru przeprowadził prawidłową ocenę tego zdarzenia i słusznie uznał, iż mimo niepodania imienia i nazwiska, sposób określenia osoby, o którą chodzi (przez oznaczenie pełniącej funkcji i okresu jej sprawowania, przejście na emeryturę), umożliwiał prostą identyfikację skarżącego. (…) Przekazywanie informacji o finansach publicznych nie wymagało zaś ujawniania danych osobowych uprawnionego. Dane te mogły zostać również zminimalizowane, a tym samym nie musiały być podawane w tak szerokim zakresie".

W ocenie NSA „możliwe było przedstawienie zagadnień związanych z kwestiami finansowymi miasta bez podawania informacji umożliwiających identyfikację skarżącego oraz bez podawania danych osobowych związanych ze stanem zdrowia oraz odnoszących się do wysokości należnych mu świadczeń z poszczególnych tytułów prawnych. Słusznie zatem organ uznał, iż ujawnienie danych nastąpiło bez podstawy prawnej, gdyż działanie podjęte w takich okolicznościach nie miało oparcia w żadnej z przesłanek legalnego przetwarzania danych osobowych określonych w art. 6 ust. 1 lit a-f RODO. (…) Nie było potrzeby informowania Rady Miasta o wysokości świadczeń pieniężnych, jakie obowiązany był wypłacić Urząd Miasta skarżącemu, jak i o okolicznościach korzystania przez niego ze zwolnienia lekarskiego. Istnieją sposoby na przekazanie tego rodzaju informacji, tj. informacji o wydatkach, bez konieczności ujawniania danych osoby, której dotyczy obowiązek zapłaty, bez konieczności podawania tytułów prawnych, jak i informowania o korzystaniu ze zwolnienia lekarskiego. Dopełnienie obowiązku prawnego minimalizacji wykluczyłoby w pełni możliwość identyfikacji osoby, której dotyczyły ujawnione dane. W ten sposób dochowanie przepisowi art. 5 ust. 1 RODO niwelowałoby potrzebę rozpatrywania sprawy przez pryzmat przepisów art. 6 ust. 1 lit. a-f RODO, czy przepisów u.d.i.p." [ustawy o dostępie do informacji publicznej].

Naczelny Sąd Administracyjny wskazał, że „w procesach przetwarzania danych osobowych należy uwzględniać intencję osoby, która przetwarza dane osobowe osób pełniących funkcję publiczną. Można ją ustalić analizując obowiązujące przepisy prawa i stan faktyczny danej sprawy. Nie jest

dopuszczalne użycie przepisu prawa wyłączającego ochronę prawa prywatności (np. art. 5 ust. 2 u.d.i.p.) dla ujawnienia danych osobowych, jeśli na gruncie ustawy o samorządzie gminnym lub innej ustawy nie obowiązuje norma prawna, która nakazuje organowi ujawnienie takich danych w określonych przypadkach. Z punktu widzenia obowiązku informacyjnego organu wykonawczego w stosunku do organu stanowiąco-kontrolnego nie było konieczne przekazanie tych danych. Ujawnienie danych osobowych w takich przypadkach jest więc dokonane bez podstawy prawnej, o której mowa w art. 6 ust. 1 lit. a-f RODO".

W ocenie NSA „niedopuszczalne jest nadużywanie przepisu prawa wyłączającego ochronę prawa prywatności (np. art. 5 ust. 2 u.d.i.p.) dla ujawnienia danych osobowych, jeśli nie obowiązuje norma prawna, która nakazuje organowi ujawnienie takich danych w określonych sytuacjach i trybie. Ujawnienie danych osobowych w takich przypadkach jest dokonane bez podstawy prawnej, o której mowa w art. 6 ust. 1 lit. a-f RODO. W tym znaczeniu doszło również do naruszenia przepisu art. 5 ust. 2 u.d.i.p."

Są wskazówki

Na kanwie tej sprawy warto przypomnieć, że kwestia tego, jak zapewniać jawność działań władzy samorządowej przy jednoczesnym poszanowaniu przepisów o ochronie danych osobowych, jak prowadzić, nagrywać i transmitować obrady kolegialnych organów jednostek samorządu terytorialnego z poszanowaniem zasad RODO został przez UODO omówiony w specjalnym poradniku. Jest on dostępny pod linkiem https://uodo.gov.pl/pl/383/3649.

Podjęty został również w Newsletterze UODO dla IOD nr 6/2019 w materiale „Transmitując sesje rady gminy i udostępniając informacje publiczne, trzeba chronić dane osobowe".

PRZEWOŹNIK JEST ADMINISTRATOREM DANYCH PASAŻERÓW POZYSKANYCH PODCZAS KONTROLI BILETÓW

Przewoźnik, decydując się na zlecenie firmie zewnętrznej kontroli biletów i windykacji należności od osób, które nie uiściły opłaty za przejazd, nie przestaje być administratorem przetwarzanych w związku z tym danych osobowych pasażerów. W świetle przepisów Prawa przewozowego nie jest dopuszczalne zawarcie przez przewoźnika umowy, na podstawie której nastąpiłaby sukcesja prawna na rzecz firmy kontrolującej bilety, bowiem przewoźnik może jedynie upoważnić ją do działania w swoim imieniu.

Jedno z miejskich przedsiębiorstw komunikacyjnych, zamierzające podjąć współpracę z zewnętrzną firmą kontrolującą bilety w autobusach komunikacji miejskiej, zwróciło się do UODO z pytaniem, czy dopuszczalne jest zawarcie przez przewoźnika umowy na kontrolę biletów i windykację, na podstawie której nastąpiłaby sukcesja prawna na rzecz firmy kontrolującej bilety również w zakresie administrowania danymi osobowymi pasażerów.

W odpowiedzi organ nadzorczy zaznaczył, że przetwarzanie danych osobowych pasażerów w związku z kontrolą biletową w środkach komunikacji reguluje art. 33a ustawy z dnia 15 listopada 1984 r. – Prawo przewozowe. Przepis ten stanowi, że przewoźnik lub osoba przez niego upoważniona, legitymując się identyfikatorem umieszczonym w widocznym miejscu, może dokonywać kontroli dokumentów przewozu osób lub bagażu (ust. 1). W razie stwierdzenia braku odpowiedniego dokumentu przewozu przewoźnik lub organizator publicznego transportu zbiorowego albo osoba przez niego upoważniona pobiera właściwą należność za przewóz i opłatę dodatkową albo wystawia wezwanie do zapłaty (ust. 3). W razie stwierdzenia braku ważnego dokumentu poświadczającego uprawnienie do bezpłatnego albo ulgowego przejazdu przewoźnik lub organizator publicznego transportu zbiorowego albo osoba przez niego upoważniona pobiera właściwą należność za przewóz i opłatę dodatkową albo wystawia wezwanie do zapłaty. Pobrana należność za przewóz i opłata dodatkowa, po uiszczeniu opłaty manipulacyjnej odpowiadającej kosztom poniesionym przez przewoźnika lub organizatora publicznego transportu zbiorowego, podlegają zwrotowi, a w przypadku wezwania do zapłaty – umorzeniu, w przypadku udokumentowania przez podróżnego, nie później niż w terminie 7 dni od dnia przewozu, uprawnień do bezpłatnego lub ulgowego przejazdu (ust. 4).

Z powołanego przepisu wynika zatem, że uprawnieni do pozyskiwania i dalszego przetwarzania danych osobowych podróżnych są przewoźnik lub osoba przez niego upoważniona. Analiza treści art. 33a Prawa przewozowego prowadzi zatem do wniosku, że o ile przewoźnik powierzy wykonywanie czynności związanych z kontrolą biletową osobie trzeciej, to – w zakresie umocowania – działa ona każdorazowo na jego rzecz. Dotyczy to zwłaszcza pozyskiwania danych osobowych pasażerów podczas kontroli i dalszego ich przetwarzania w związku z dochodzeniem należności z tytułu opłat za przejazd bez ważnego biletu.

Z takiego ukształtowania przez ustawodawcę relacji między przewoźnikiem a podmiotem, który zostaje przez niego upoważniony do prowadzenia kontroli biletowej, wynika zatem, iż decyzje o celach i środkach przetwarzania danych osobowych pasażerów w każdym przypadku należą wyłącznie do przewoźnika. W konsekwencji status administratora danych pasażerów zawsze przysługiwał będzie przewoźnikowi.

Podkreślić przy tym należy, że art. 33a Prawa przewozowego ma charakter bezwzględnie obowiązujący, wobec czego niedopuszczalne jest odmienne ukształtowanie ww. spraw w drodze umowy między przewoźnikiem a osobą trzecią. Stanowisko takie znajduje również odzwierciedlenie w orzecznictwie (np. postanowienie Sądu Najwyższego z 23 października 2003 r., sygn. akt IV KK 265/02).

W świetle powyższego stwierdzić należy, iż w każdym przypadku skutki prawne działań podejmowanych przez pracowników firm, które dokonują kontroli biletowej za zgodą i wiedzą przewoźnika, powstają bezpośrednio w sferze prawnej z jednej strony – przewoźnika, a z drugiej – podróżnego. Nie jest zatem dopuszczalne zawarcie przez przewoźnika umowy, na podstawie której nastąpiłaby sukcesja prawna na rzecz firmy kontrolującej bilety, bowiem przewoźnik może jedynie upoważnić ją do działania w swoim imieniu. W konsekwencji, wszelkie umowy między przewoźnikami a firmami kontrolującymi bilety muszą być rozumiane jako dotyczące powierzenia wykonywania czynności w imieniu przewoźnika. W opinii organu nadzorczego w zakresie dotyczącym przetwarzania danych osobowych pasażerów przepis art. 33a Prawa przewozowego daje podstawę do zawarcia między przewoźnikiem a firmą kontrolującą umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 28 RODO.

KAMERA W WIZJERZE TO NIEDOZWOLONA FORMA MONITORINGU KLATKI SCHODOWEJ

PUODO nakazał sąsiadowi skarżącego, by przestał nagrywać to, co się dzieje za drzwiami mieszkania.

Nieznana osoba nękała sąsiada podrzucając mu skórki od banana i kartki pod drzwi. Nie mogąc ustalić, kto to, sąsiad zainstalował zaawansowaną kamerę z detekcją ruchu, noktowizją. Kamera nagrywała obraz i dźwięk – skarżący nagrywany był za każdym razem, gdy wychodził i wchodził do mieszkania. Sąsiad nie zapytał go o zgodę na monitoring. Interwencje skarżącego nie pomogły, stąd skarga do PUODO.

Sąsiad wyjaśnił PUODO, że kamera nie ma na celu naruszenia prywatności skarżącego ani żadnej innej osoby, lecz „wynika z zagrożenia mojego bezpieczeństwa z powodu powtarzających się na przestrzeni ostatnich miesięcy ataków na drzwi wejściowe do mojego mieszkania, wycieraczkę przed drzwiami wejściowymi oraz obszar klatki schodowej przylegający do mojego mieszkania. Powyższe ataki zgłaszałem wielokrotnie do administracji wspólnoty mieszkaniowej oraz na policję. Niestety ataki powtarzały się, pomimo dokonanych przeze mnie zgłoszeń. Ponieważ ani działania administracji, ani policji nie były w stanie zapobiec dalszym atakom i zapewnić mi poczucia bezpieczeństwa w moim własnym mieszkaniu, byłem zmuszony zainstalować kamerę w wizjerze. Chciałbym zaznaczyć, iż w wyniku instalacji kamery wspomniane powyżej ataki ustały”.

PUODO po zbadaniu sprawy stwierdził, że sąsiad nie może skorzystać z wyjątku RODO pozwalającego na monitoring (art. 2 ust. 2 lit. c RODO), gdyż pozwala on tylko na monitoring własnej nieruchomości. A kamera w wizjerze obejmowała zasięgiem klatkę schodową i drzwi innych mieszkań.

Zatem choć sąsiad miał interes prawny, by nagrywać to, co dzieje się na klatce schodowej, nie jest on nadrzędny wobec praw i wolności skarżącego. Ma on prawo do prywatności i tego, by sąsiad nie przetwarzał jego danych osobowych.

Dodatkowo kamera sąsiada nagrywała głos – a nie są to informacje niezbędne do celu, jaki spełnić miała kamera. Funkcje, które nie są niezbędne, powinny zostać dezaktywowane. Chodzi przecież o korytarz i klatkę schodową, gdzie ludzie mogą rozmawiać bez ryzyka, że ktoś ich nagrywa.

3 WYBRANE DECYZJE UODO

Podkreślić również należy, że uprawnienia do stosowania funkcji rejestracji głosu posiadają jedynie służby porządkowe i specjalne na podstawie ustaw regulujących ich działalność.

PUODO uzupełnia swoją decyzję wskazaniami wyroków sądów, które podzielają taką interpretację sytuacji z kamerą w wizjerze.

Sygnatura sprawy: DS.523.703.2024

fot. pixabay

DANE NA TEMAT REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ, W SCHENGEN

W związku z modernizacją Systemu Informacyjnego Schengen, która miała miejsce w 2023 r., Komitet Skoordynowanego Nadzoru – Coordinated Supervision Committee (CSC) opracowuje i sporządza roczne sprawozdanie dla Europejskiej Rady Ochrony Danych na temat wykonywania praw osób, których dane dotyczą, postępowań sądowych i wzajemnego uznawania ostatecznych decyzji dotyczących SIS[1].

Nie jest to działanie przypisane CSC, ale stanowi sprawozdanie z działań państw członkowskich w odniesieniu do wykonywania praw osób, których dane dotyczą, w związku z przetwarzaniem danych w SIS na trzech poziomach: administratora danych, organu ochrony danych realizującego pośrednie prawo dostępu oraz sądów jako sądowego środka odwoławczego.

W przypadku tego pierwszego sprawozdania okresem objętym sprawozdaniem jest okres od 7 marca 2023 r., tj. od dnia, w którym SIS weszło w zakres kompetencji CSC, do 31 grudnia 2023 r. Kolejne sprawozdania będą sporządzane w ujęciu rocznym (tj. od dnia 1 stycznia do dnia 31 grudnia) i będą zawierać ocenę i porównanie z rokiem poprzednim.

Opracowano wzór sprawozdania dla państw członkowskich na temat wykonywania praw osób, których dane dotyczą, związanych z SIS. Format wzoru do stosowania przez państwa członkowskie na potrzeby sprawozdawczości w zakresie praw osób, których dane dotyczą, związanych z rozporządzeniami w sprawie SIS określono w decyzji wykonawczej Komisji (UE) 2022/22061. Wzór sprawozdania znajduje się w dodatku 1 do niniejszego sprawozdania.

Zróżnicowanie okresów sprawozdawczych i brakujących danych oznacza, że pełne porównanie między państwami członkowskimi a ogólnym wykonywaniem praw osób, których dane dotyczą, w ramach SIS jest problematyczne.

[1] Zgodnie z art. 54 ust. 3 rozporządzenia (UE) 2018/1861 i art. 68 ust. 3 rozporządzenia (UE) 2018/1862

4 NARUSZENIA I KONTROLE

Wnioski o udzielenie dostępu do danych

Zgodnie z przepisami SIS[2], osoby, których dane dotyczą, mogą korzystać z prawa dostępu przewidzianego w art. 15 rozporządzenia 2016/679 (RODO) oraz w art. 14 dyrektywy 2016/680 (DODO). Należy zauważyć, że w odniesieniu do SIS RODO ma zastosowanie w przypadku[3]:

• kontroli granicznej,

• kontroli policyjnych i celnych,

• badania warunków i podejmowania decyzji dotyczących wjazdu i pobytu obywateli państw trzecich na terytorium państw członkowskich,

• kontroli bezpieczeństwa w odniesieniu do obywateli państw trzecich, którzy ubiegają się o ochronę międzynarodową,

• rozpatrywania wniosków wizowych i podejmowania decyzji w sprawie tych wniosków.

Z kolei DODO stosuje się w przypadku przetwarzania danych do celów zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Dlatego, w przypadku, kiedy obowiązuje RODO, osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

---

[2] Art. 53 rozporządzenia 2018/1861 oraz art. 67 rozporządzenia 2018/1862

[3] Art. 51 ust. 2 rozporządzenia 2018/1861 oraz art. 66 ust. 2 rozporządzenia 2018/1862

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W przypadku osoby, których dane są przetwarzane w trybie DODO, przysługuje jej prawo do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli takie dane są przetwarzane, prawo dostępu do danych osobowych i do następujących informacji:

a) cele i podstawa prawna przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;

e) informacje o prawie do żądania od administratora sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby;

f) informacje o prawie wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;

g) wskazanie, jakie dane osobowe są przetwarzane, oraz wszelkie dostępne informacje o ich pochodzeniu.

Jak wynika z danych CSC, wpłynęło 41 434 wniosków o udzielenie dostępu do danych, z czego administratorzy rozpatrzyli pozytywnie wnioski w 47% przypadków. Najwięcej wniosków wpłynęło do administratorów w Szwajcarii (6365), Austrii (6355), Słowenii (5084), Włoszech (4891), Rumunii (3825), Niemczech (3190) i Francji (2838). Największy odsetek rozpatrzonych wniosków zaobserwowano w Czechach (101%), Estonii (100%), Islandii (100%), Niemczech (99%), Niderlandach (99%), Malcie (99%), Luksemburgu (98%), Bułgarii (97%), Słowenii (97%), Szwecji (94%), Danii (88%), Francji (84%), Grecji (75%), Słowacji (71%), Węgrzech (70%), Belgii (68%), Portugalii (57%).

4 NARUSZENIA I KONTROLE

Pośrednie prawo dostępu za pośrednictwem organów nadzorczych

Administrator może podjąć decyzję o nieprzekazywaniu całości lub części informacji osobie, której dane dotyczą, w zakresie – a także przez tak długi okres – w jakim takie częściowe lub zgodnie z prawem krajowym, całkowite ograniczenie stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów osoby, której dane dotyczą, po to aby:

a) uniemożliwić utrudnianie prowadzenia urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur;

b) uniemożliwić utrudnianie zapobiegania przestępstwom, ich wykrywania, prowadzenia w ich sprawie postępowań przygotowawczych lub ich ścigania lub wykonywania kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe; lub

e) chronić prawa i wolności innych osób.

W takich przypadkach osoba, której dane dotyczą, może również wykonywać swoje prawa za pośrednictwem organów ochrony danych[4].

Dane CSC wskazują, że w 2023 r. organy ochrony danych rozpatrzyły pozytywnie wnioski o pośrednie prawo dostępu w 15% przypadków. Należy zauważyć, że – jak stwierdzono w Ewaluacjach Schengen – nie wszystkie państwa UE prawidłowo wdrożyły obowiązek zapewnienia pośredniego dostępu określonego w art. 17 dyrektywy o ochronie danych w sprawach karnych. Niestety, również w Polsce stwierdzono brak pełnej transpozycji wdrożenia przepisów w tym zakresie[5], a zalecenie dostosowania tych przepisów uznano za priorytetowe[6].

Najwięcej wniosków o dostęp do danych za pośrednictwem organów ochrony danych wpłynęło do Włoch (373), Francji (275), Bułgarii (98), Belgii (78) i Rumunii (76). W przypadku Bułgarii, Estonii, Niemiec, Malty wszystkie wnioski zostały pozytywnie rozpatrzone. Z kolei Francja pozytywnie rozpatrzyła 11% wniosków.

[4] Art. 53 ust. 3 rozporządzenia 2018/1861 oraz art. 67 ust. 3 rozporządzenia 2018/1862

[5] https://home-affairs.ec.europa.eu/document/download/aa985c3b-2c11-47e7-99e3-a7459e7c2bc8_en?filename=Schengen%20evaluation%20of%20Poland.pdf

[6] Zalecenie nr 45 Ewaluacji Schengen w Polsce

4 NARUSZENIA I KONTROLE

Prawo do sprostowania danych

Zgodnie z przepisami SIS[7] osoby, których dane dotyczą, mogą korzystać z prawa do sprostowania danych przewidzianego w art. 16 RODO oraz w art. 16 ust. 1 DODO. Dane CSC wskazują, że zasadniczo wpłynęło mało wniosków o sprostowanie danych (50). W większości przypadków wnioski są rozpatrywane przez administratorów danych. Najwięcej wniosków o sprostowanie wpłynęło w Niderlandach (25), Węgrzech (9) i Portugalii (6). Z kolei najwięcej pozytywnie rozpatrzonych wniosków o sprostowanie odnotowuje Belgia (8), Dania (3), Bułgaria (2), Łotwa (1).

Pośrednie prawo do sprostowania danych za pośrednictwem organów nadzorczych

Zgodnie z przepisami DODO, w odniesieniu do przypadków odmowy sprostowania danych, osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego.

Jak wynika z danych CSC, zdarzały się przypadki, w których do organów ochrony danych wpłynęło więcej wniosków niż do samych administratorów – Francja (128:0), Belgia (78:2). Z danych CSC wynika również, że wnioski kierowane do organów nadzorczych nie zostały rozpatrzone pozytywnie.

Wnioski o usunięcie danych

Zgodnie z przepisami SIS[8] osoby, których dane dotyczą, mogą korzystać z prawa do usunięcia danych przewidzianego w art. 17 RODO oraz w art. 16 ust. 2 DODO. Zgodnie z art. 17 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

c) dane osobowe były przetwarzane niezgodnie z prawem;

d) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

---

[7] Art. 53 ust. 3 rozporządzenia 2018/1861 oraz art. 67 ust. 3 rozporządzenia 2018/1862

[8] Zalecenie nr 45 Ewaluacji Schengen w Polsce

4 NARUSZENIA I KONTROLE

Zgodnie z art. 16 ust. 2 DODO, państwa członkowskie nakładają na administratora wymóg usunięcia bez zbędnej zwłoki danych osobowych i zapewniają, by osoba, której dane dotyczą, miała prawo uzyskać od administratora usunięcie bez zbędnej zwłoki jej danych osobowych, jeżeli przetwarzanie narusza przepisy przyjęte na podstawie art. 4, 8 i 10, lub jeżeli dane osobowe muszą zostać usunięte w celu wypełnienia obowiązku prawnego ciążącego na administratorze. Natomiast zgodnie z art. 16 ust. 3 DODO, zamiast usunięcia, administrator ogranicza przetwarzanie, jeżeli:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić; lub

b) dane osobowe muszą zostać zachowane do celów dowodowych.

Jeżeli przetwarzanie jest ograniczone na mocy pkt. a), przed zniesieniem tego ograniczenia administrator informuje o tym osobę, której dane dotyczą.

Z danych CSC wynika, że w sumie wpłynęło 2441 wniosków o usunięcie danych, z czego 1044 do administratora we Francji, 438 w Niemczech, 320 w Portugalii, 265 w Czechach, 151 w Niderlandach. Najwięcej rozpatrzonych pozytywnie wniosków odnotowano we Francji (905) i Belgii (93).

Pośrednie prawo do usunięcia danych za pośrednictwem organów nadzorczych

Zgodnie z przepisami DODO, w odniesieniu do przypadków odmowy usunięcia danych, osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego. Takie wnioski wpłynęły w Belgii (78), Francji (35), Grecji (13). Jednakże tylko w przypadku Portugalii organ nadzorczy wyegzekwował usunięcie danych jednej osoby, której dane dotyczą.

Postępowania sądowe

Każdej osobie przysługuje prawo do wniesienia do sądu, na mocy prawa krajowego państwa członkowskiego żądania o dostęp do informacji, ich sprostowanie, ich usunięcie lub ich uzyskanie lub o zapłatę odszkodowania w związku z wpisem dotyczącym tej osoby[9]. Państwa członkowskie zobowiązują się wzajemnie do wykonywania orzeczeń lub decyzji kończących postępowanie w sprawie wydanych przez sądy.

Jak wynika z danych CSC, w 13 przypadkach wszczęto postępowania sądowe, z czego 7 w Czechach, 3 we Francji, 2 w Szwecji i 1 w Niderlandach. Tylko w 4 przypadkach sąd orzekł na korzyść skarżącego: w Czechach 3 i we Francji 1.

[9] Art. 54 ust. 1 rozporządzenia 2018/1861 oraz art. 68 ust. 1 rozporządzenia 2018/1862

4 NARUSZENIA I KONTROLE

Te liczby mogą wskazywać, że statystyki gromadzone przez systemy wymiaru sprawiedliwości państw członkowskich nie obejmują obecnie tego rodzaju postępowań sądowych ze względu na fakt, że jest to nowy obowiązek sprawozdawczy.

Uwagi ogólne

Jakość i szczegółowość danych dostarczonych przez państwa członkowskie za ten okres sprawozdawczy była bardzo różna i w wielu przypadkach wymagane informacje nie zostały przekazane.

Sprawozdawczość w zakresie tych statystyk jest nowym obowiązkiem państw członkowskich, jednak dla pomyślnego funkcjonowania SIS – i szeregu powiązanych wielkoskalowych systemów informatycznych UE – bardzo ważne jest, aby dane dotyczące praw osób, których dane dotyczą, były rejestrowane, zestawiane i terminowo przekazywane Europejskiej Radzie Ochrony Danych.

Wszystkie państwa członkowskie muszą zapewnić pełne przygotowanie swoich procedur wewnętrznych, aby móc rejestrować te statystyki w formacie wymaganym decyzją wykonawczą Komisji i terminowo przekazywać je Europejskiej Radzie Ochrony Danych.

fot. pexels

ZAKOŃCZONO PRZEDŁUŻONE KONSULTACJE PUBLICZNE DOTYCZĄCE WYTYCZNYCH EROD 1/2025 W SPRAWIE PSEUDONIMIZACJI

Dziękujemy za zaangażowanie i cenny wkład wszystkich zainteresowanych stron w konsultacje publiczne dotyczące wytycznych EROD 1/2025 w sprawie pseudonimizacji. Ten kluczowy proces odgrywa istotną rolę w opracowaniu wytycznych mających na celu lepsze zabezpieczenie danych oraz wsparcie procesów pseudonimizacji w Unii Europejskiej.

Z uwagi na istotę poruszanych tematów oraz ich techniczny charakter, konsultacje zostały przedłużone o kolejne dwa tygodnie, by zapewnić wszystkim możliwość dogłębnego zapoznania się z materiałem, i przygotowania uwag. Łączny czas trwania konsultacji wyniósł osiem tygodni i zakończył się 14 marca.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pexels

CEF 2025: ROZPOCZĘCIE SKOORDYNOWANEGO EGZEKWOWANIA PRAWA DO USUNIĘCIA DANYCH

Europejska Rada Ochrony Danych (EROD) rozpoczęła działania w ramach skoordynowanego egzekwowania prawa (CEF), na rok 2025. Po rocznych skoordynowanych działaniach w zakresie prawa dostępu w 2024 r., w tym roku CEF skupi się na wdrożeniu innego prawa do ochrony danych – prawa do usunięcia danych lub „prawa do bycia zapomnianym" (art. 17 RODO).

Rada wybrała ten temat podczas sesji plenarnej w październiku 2024 r., ponieważ jest to jedno z najczęściej wykonywanych praw wynikających z RODO, na które organy ochrony danych często otrzymują skargi od osób fizycznych.

Kolejne kroki

W 2025 r. w inicjatywie wezmą udział 32 organy ochrony danych w całej Europie.

Wkrótce organy te skontaktują się z wieloma administratorami z różnych sektorów w całej Europie, wszczynając nowe formalne postępowania wyjaśniające lub przeprowadzając działania informacyjne. W tym drugim przypadku mogą również zdecydować o podjęciu dodatkowych działań następczych, jeśli zajdzie taka potrzeba.

Organy ochrony danych sprawdzą, w jaki sposób administratorzy przetwarzają otrzymane wnioski o usunięcie danych i odpowiadają na nie, a w szczególności, w jaki sposób stosują warunki i wyjątki dotyczące korzystania z tego prawa.

Organy ochrony danych pozostaną w ścisłym kontakcie, aby omawiać swoje ustalenia przez cały rok. Wyniki krajowych działań zostaną zagregowane i przeanalizowane razem, aby uzyskać głębszy wgląd w temat, umożliwiając ukierunkowane działania następcze zarówno na poziomie krajowym, jak i unijnym.

Kontekst

CEF jest kluczowym działaniem Europejskiej Rady Ochrony Danych w ramach jej strategii na lata 2024-2027, mającym na celu usprawnienie egzekwowania prawa i współpracy między organami ochrony danych.

5 SPRAWY MIĘDZYNARODOWE

W ciągu ostatnich trzech lat przeprowadzono trzy poprzednie działania CEF dotyczące różnych tematów:

1. korzystania z usług w chmurze przez sektor publiczny,
2. wyznaczenia i pozycji inspektorów ochrony danych, oraz
3. wdrożenia prawa dostępu przez administratorów danych.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pixabay

ZARZĄDZANIE DANYMI I SZTUCZNA INTELIGENCJA: PIĘĆ ORGANÓW OCHRONY DANYCH ZOBOWIĄZUJE SIĘ DO WSPARCIA INNOWACYJNEJ SZTUCZNEJ INTELIGENCJI, KTÓRA CHRONI PRYWATNOŚĆ

Podczas szczytu poświęconego działaniom na rzecz sztucznej inteligencji (AI Action Summit), który odbył się w Paryżu (6–11 lutego 2025 r.), organy ochrony danych z Australii, Korei, Irlandii, Francji i Wielkiej Brytanii podpisały wspólne oświadczenie, aby potwierdzić swoje zaangażowanie w zarządzanie danymi, które wspiera innowacyjną i chroniącą prywatność sztuczną inteligencję.

W ramach paryskiego szczytu poświęconego działaniom na rzecz sztucznej inteligencji koreański organ ochrony danych (PIPC) oraz francuski organ nadzorczy (CNIL) wspólnie zorganizowały wydarzenie we współpracy z Organizacją Współpracy Gospodarczej i Rozwoju (OECD). Przy tej okazji trzy inne organy biorące udział w wydarzeniu podpisały wspólne oświadczenie.

Tworzenie niezawodnych ram zarządzania dla godnej zaufania sztucznej inteligencji

Celem inicjatywy jest promowanie ram zarządzania sztuczną inteligencją dających pewność prawną interesariuszom i gwarancje dla osób fizycznych, zwłaszcza pod względem przejrzystości i poszanowania praw podstawowych.

W oświadczeniu podkreślono liczne możliwości, jakie oferuje sztuczna inteligencja w różnych obszarach, takich jak innowacje, badania naukowe, gospodarka i społeczeństwo. Ostrzega także przed wieloma zagrożeniami związanymi z ochroną danych osobowych i prywatności, dyskryminacją i stronniczością algorytmiczną, a także dezinformacją.

Aby zapewnić zgodność sztucznej inteligencji z obowiązującymi przepisami, organy zalecają uwzględnienie zasad ochrony danych już na etapie projektowania systemów sztucznej inteligencji, wdrożenie solidnego zarządzania danymi i przewidywania ryzyka.

Oświadczenie podkreśla również rosnącą złożoność przetwarzania danych za pomocą sztucznej inteligencji w takich obszarach jak zdrowie i usługi publiczne, bezpieczeństwo publiczne, zasoby ludzkie i edukacja.

5 SPRAWY MIĘDZYNARODOWE

Wskazuje na różnorodność zaangażowanych podmiotów i potrzebę ram regulacyjnych dostosowanych do postępu technologicznego.

Zobowiązania organów w obliczu wyzwań stawianych przez sztuczną inteligencję:

• wyjaśnienie podstaw prawnych przetwarzania danych w ramach sztucznej inteligencji;

• wymiana informacji i ustanowienie odpowiednich środków bezpieczeństwa;

• monitorowanie technicznych i społecznych skutków sztucznej inteligencji poprzez zaangażowanie różnych zainteresowanych stron;

• zachęcanie do innowacji przy jednoczesnym ograniczaniu niepewności prawnej;

• wzmocnienie współpracy z innymi właściwymi organami (ochrona konsumentów, konkurencja, własność intelektualna).

Źródło: Komunikat francuskiego organu nadzorczego

fot. pixabay

KARA ISLANDZKIEGO ORGANU ZA NIEZGODNE Z PRAWEM PRZETWARZANIE DANYCH W ZWIĄZKU Z INTEGRACJĄ SYSTEMÓW DOKUMENTACJI MEDYCZNEJ

Islandzki organ nadzorczy nałożył karę w wysokości ponad 33 tysięcy euro na Podstawową Opiekę Zdrowotną Obszaru Stołecznego. Dochodzenie przeprowadzone przez Urząd Nadzoru ujawniło, że Podstawowa Opieka Zdrowotna zawarła kilka umów dotyczących integracji systemów dokumentacji medycznej, z których tylko jedna spełniała wymogi ustawy nr 55/2009 o dokumentacji medycznej.

Informacje ogólne

• Data wydania ostatecznej decyzji: 11 lutego 2025 r.

• Sprawa krajowa

• Administrator danych: Podstawowa Opieka Zdrowotna Obszaru Stołecznego

• Odniesienia prawne: Artykuł 5 (Zasady przetwarzania danych osobowych), Artykuł 6 (Zgodność przetwarzania z prawem).

• Decyzja: stwierdzone naruszenie, administracyjna kara pieniężna

• Słowa kluczowe: zgodność z prawem przetwarzania, grzywna administracyjna, dane wrażliwe

Streszczenie decyzji

Geneza sprawy

Islandzki organ nadzoru (Persónuvernd) wszczął dochodzenie w sprawie integracji systemów dokumentacji medycznej przez Podstawową Opiekę Zdrowotną Obszaru Stołecznego w następstwie orzeczenia organu w sprawie skargi dotyczącej przetwarzania dokumentacji medycznej przez urzędnika medycznego Urzędu Transportu (sprawa nr 2023071182). Dochodzenie w sprawie skargi ujawniło, że Podstawowa Opieka Zdrowotna zawarła umowę z Islandzkim Urzędem Transportu w sprawie integracji systemów dokumentacji medycznej, która nie spełniała wymogów prawa krajowego, tj. ustawy nr 55/2009 o dokumentacji medycznej.

5 SPRAWY MIĘDZYNARODOWE

Dochodzenie w sprawie integracji dokumentacji medycznej przez Podstawową Opiekę Zdrowotną było ograniczone do zgodności przetwarzania danych z prawem.

Kluczowe ustalenia

Dochodzenie przeprowadzone przez Urząd Nadzoru ujawniło, że Podstawowa Opieka Zdrowotna zawarła kilka umów dotyczących integracji systemów dokumentacji medycznej, z których tylko jedna spełniała wymogi ustawy nr 55/2009 o dokumentacji medycznej. Zgodnie z art. 20 ust. 2 tej ustawy na integrację systemów dokumentacji medycznej wymagane jest zezwolenie Ministra Zdrowia oraz potwierdzenie islandzkiego Urzędu Ochrony Danych Osobowych dotyczące bezpieczeństwa przetwarzania danych osobowych w zintegrowanym systemie. Ponieważ Podstawowa Opieka Zdrowotna nie spełniła tych wymogów podczas integracji jedenastu stron w swoim systemie dokumentacji medycznej, nie zapewniła zgodności przetwarzania z prawem (art. 5 ust. 1 lit. a), art. 6 ust. 1 i art. 9 ust. 1 RODO).

Decyzja

Islandzki organ nadzorczy nałożył grzywnę w wysokości 33 854 euro na Podstawową Opiekę Zdrowotną Obszaru Stołecznego.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pixabay

KARA FIŃSKIEGO ORGANU NADZORCZEGO ZA ZANIEDBANIA W ZAKRESIE BEZPIECZEŃSTWA DANYCH

Fiński organ nadzorczy nałożył karę w wysokości 950 tysięcy euro na porównywarkę pożyczek Sambla Group. W porównywarkach firmy brakowało m.in. odpowiednich ograniczeń uniemożliwiających osobom trzecim dostęp do danych zawartych we wnioskach o pożyczkę.

Informacje ogólne

• Data wydania ostatecznej decyzji: 17 grudnia 2024 r.

• Sprawa krajowa

• Odniesienia prawne: Artykuł 5 (Zasady dotyczące przetwarzania danych osobowych), Artykuł 25 (Ochrona danych w fazie projektowania i domyślna), Artykuł 32 (Bezpieczeństwo przetwarzania)

• Decyzja: grzywna administracyjna, nakaz powiadomienia o naruszeniu danych osobowych, nagana

• Słowa kluczowe: bezpieczeństwo danych, naruszenie ochrony danych osobowych, dostęp osób trzecich do danych osobowych

Streszczenie decyzji

Geneza sprawy

Fiński organ ds. ochrony danych osobowych (Tietiosuojavaltuutetun Toimisto) wszczął dochodzenie na podstawie skargi złożonej przez klienta. Wiosną 2024 r. dochodzenie techniczne ujawniło poważne problemy z bezpieczeństwem danych w usługach porównywania pożyczek administratora. Spółce nakazano natychmiastowe zaprzestanie przetwarzania danych osobowych dotyczących osób ubiegających się o pożyczkę w jej usługach elektronicznych.

Kluczowe ustalenia

W porównywarkach pożyczek Sambla Group brakowało odpowiednich ograniczeń uniemożliwiających osobom trzecim dostęp do danych zawartych we wnioskach o pożyczkę (art. 32 RODO, art. 25 RODO i art. 5 ust. 1 lit. f) RODO). Ze względu na słabe zabezpieczenie danych, treść wniosków kredytowych

klientów była dostępna dla osób trzecich za pośrednictwem osobistych adresów URL przeznaczonych dla klientów. Każdy, kto miał dostęp do adresu URL i wystarczającą wiedzę techniczną, aby wykorzystać lukę w zabezpieczeniach, zyskiwał bezpośredni dostęp do danych. Dochodzenie techniczne wykazało, że adresy URL były celem phishingu, a dane osobowe zostały ujawnione stronom trzecim. Informacje dostępne za pośrednictwem linków obejmowały co najmniej dane kontaktowe wnioskodawcy pożyczki, a także informacje o jego dochodach, kosztach mieszkaniowych, stanie cywilnym i posiadanych dzieciach.

Decyzja

Fiński organ nałożył na administratora grzywnę administracyjną w wysokości 950 tysięcy euro. Nakazano mu również powiadomienie swoich klientów o incydencie. Administrator ogłosił, że zaprzestał korzystania z podatnych adresów URL i poprawił bezpieczeństwo danych w swoich usługach.

Źródło: Komunikat Europejskiej Rady Ochrony Danych

fot. pixabay

META WPROWADZA ROZWIĄZANIE MAJĄCE NA CELU WALKĘ Z „CELEB-BAIT”

3 marca Meta wprowadziła dla regionu europejskiego rozwiązanie polegające na wykorzystaniu technologii rozpoznawania twarzy, aby przeciwdziałać zjawisku „celeb-bait”, tj. rozpowszechnianiu treści zawierających przetworzone wizerunki osób znanych przez cyberprzestępców.

Zjawisko to jest niebezpieczne dla użytkowników portali społecznościowych oraz stanowi wyjątkowo nikczemne naruszenie dóbr osobistych oraz prywatności osób, których wizerunek zostaje użyty przez cyberprzestępców. Tworzą oni fałszywe profile celebrytów, wykorzystując ich rozpoznawalność oraz reputację, jaką się cieszą, aby oszukiwać ludzi i uzyskiwać korzyści finansowe.

Dlatego wprowadzanie skutecznych i godnych zaufania narzędzi, które pozwolą przeciwdziałać „celeb-bait”, jest tak ważne. Warto wspomnieć, że Urząd Ochrony Danych Osobowych był bardzo zaangażowany w działania przeciw „celeb-bait” w związku ze sprawą dotyczącą wykorzystania wizerunku pana Rafała Brzoski oraz pani Omeny Mensah. Zatem tym bardziej cieszy nas wiadomość o staraniach Meta, aby zgodnie z naszymi zaleceniami wprowadzić skuteczne rozwiązanie problemu.

Rozwiązanie wprowadzane przez Meta polega na wykorzystaniu analizy twarzy, w tym technologii rozpoznawania twarzy, aby szybko wykryć potencjalne wprowadzające w błąd treści wykorzystujące wizerunek danej osoby. Meta zapewnia również o dużej skuteczności narzędzia oraz o możliwości weryfikacji z udziałem człowieka wyników takiej analizy. Narzędzie zostało wprowadzone z uwzględnieniem przepisów o ochronie danych, a organy nadzorcze były informowane o planach Meta.

Prezes UODO zaznaczył, że jest jeszcze za wcześnie na ocenę nowego instrumentu, jednak jest on wart uwagi. Temat pozostaje otwarty, a dalsze wdrożenie i skuteczność narzędzia będą monitorowane.

Źródło: Strona internetowa firmy Meta

„UODO RUSZA W KRAJ” – ODWIEDZAMY PLACÓWKI EDUKACYJNE

Wobec braku jednostek zamiejscowych, czy delegatur regionalnych, aby lepiej zrozumieć lokalne problemy związane z wyzwaniami dotyczącymi ochrony danych osobowych, we wrześniu 2024 roku powstała inicjatywa Prezesa Urzędu Ochrony Danych Osobowych pn. „UODO rusza w kraj”. Polega ona na cyklicznych spotkaniach z mieszkańcami oraz władzami administracji publicznej w poszczególnych województwach. To także sprzyjająca okoliczność, by odwiedzić szkoły, uczestniczące w programie „Twoje dane – Twoja sprawa”.

Jednym z bardzo ważnych obszarów edukacyjnej działalności Prezesa Urzędu Ochrony Danych Osobowych jest wsparcie oferowane oświacie oraz edukacja dzieci i młodzieży. Spotkania w ramach akcji „UODO rusza w kraj” są doskonałą okazją, aby odwiedzać placówki edukacyjne, biorące udział w XV edycji programu PUODO „Twoje dane – Twoja sprawa”. W wydarzeniach uczestniczą zaproszeni dyrektorzy, nauczyciele, członkowie rad rodziców czy sami uczniowie, prezentujący inicjatywy realizowane w ich placówkach w ramach Programu. Spotkania sprzyjają wymianie doświadczeń oraz dobrych praktyk w zakresie ochrony danych osobowych oraz cyberbezpieczeństwa dzieci i młodzieży.

Pierwsze wojewódzkie spotkanie środowisk oświatowych odbyło się w Zespole Szkół nr 1 w Kwidzynie. Szkoła od lat bierze udział w programie „Twoje dane – Twoja sprawa” oraz jest laureatem konkursu pt. „Inicjatywa edukacyjna roku 2023/24”, organizowanego w ramach tego Programu.

Kolejna odsłona działań miała miejsce w Szkole Podstawowej nr 17 im. Strzelców Podhalańskich w Rzeszowie. Uczestnicy mieli okazję wysłuchać prelekcji ekspertów UODO, którzy podczas spotkania poruszyli m.in. temat ochrony wizerunku w odniesieniu do poradnika przygotowanego przez Urząd Ochrony Danych Osobowych przy współpracy z Fundacją Orange. Publikacja koncentruje się w szczególności na ochronie wizerunku dzieci. To zagadnienie istotne z perspektywy szkół, które jako placówki oświatowe, są administratorami danych osobowych uczniów i publikują ich wizerunki, np. w materiałach promocyjnych. Poradnik uwzględnia również punkt widzenia nauczycieli, którzy chcą dzielić się wiedzą o ochronie danych osobowych.

6 EDUKACJA

RODO jednoznacznie wskazuje, że dane osobowe dzieci, w tym ich wizerunek, podlegają szczególnej ochronie. Najmłodsi mają bowiem mniejszą świadomość swoich praw i możliwych konsekwencji podejmowanych działań, dlatego to dorośli powinni w szczególności zadbać o ich bezpieczeństwo. Na przykładzie motywu 58. RODO podkreślono, że w przypadku przetwarzania danych dzieci, obowiązki informacyjne muszą być przekazywane w sposób prosty i zrozumiały. W ramach spotkań przedstawiono również, czym są dane osobowe i dlaczego wizerunek także do nich należy.

Zwrócono również uwagę na konieczność ograniczenia ilości publikacji zawierających wizerunki uczniów. Sama zgoda nie oznacza przyzwolenia na nieograniczone i bezrefleksyjne publikowanie takich zdjęć. Nawet jeśli działanie to jest legalne z formalnego punktu widzenia, warto zadać sobie pytanie, czy jest ono naprawdę uzasadnione. Dobrą praktyką, szczególnie w przypadku starszych dzieci, jest konsultowanie z nimi decyzji o ewentualnym upublicznieniu ich wizerunku. Takie podejście świadczy nie tylko o rozsądku, ale też wynika z przepisów Kodeksu rodzinnego i opiekuńczego oraz Konwencji o Prawach Dziecka.

Przedstawiciel szkoły przedstawił działania edukacyjne podejmowane przez szkołę w zakresie ochrony danych osobowych. Uczestnicy spotkania dyskutowali na najbardziej aktualne tematy, poruszyli kwestie powszechnego udostępniania w internecie informacji o dzieciach i młodzieży – zwłaszcza ich wizerunku – oraz omówili trudności, z jakimi mierzą się dyrektorzy szkół i nauczyciele w tym obszarze.

W ramach akcji „UODO rusza w kraj” Urząd Ochrony Danych Osobowych był już obecny w czterech województwach: małopolskim, śląskim, pomorskim i podkarpackim. Przed nami kolejne wyjazdy i ciekawe oraz inspirujące spotkania z administratorami, inspektorami ochrony danych, władzami, mieszkańcami oraz przedstawicielami różnych środowisk, w tym oświaty.

ROK 2025 EUROPEJSKIM ROKIEM EDUKACJI CYFROWEJ

Rada Europy ogłosiła rok 2025 Europejskim Rokiem Edukacji Cyfrowej (European Year 2025), aby nadać nowy impuls rozwojowi i promocji edukacji cyfrowej we wszystkich państwach członkowskich.

Europejski Rok 2025 stanowi wyjątkową okazję do zwiększenia widoczności i wpływu edukacji na rzecz obywatelstwa cyfrowego oraz potwierdzenia jej wartości. Tegoroczne obchody będą stanowić strategiczną platformę dla kluczowych interesariuszy z sektora publicznego, prywatnego i obywatelskiego do współpracy, wyznaczania wspólnych celów i dzielenia się najlepszymi praktykami. Inicjatywa zapewni zwięzłą, ale skuteczną przestrzeń do mierzenia osiągnięć i wspólnego definiowania mapy drogowej dla przyszłości edukacji w zakresie obywatelstwa cyfrowego. Oczekuje się, że dzięki usprawnionym wysiłkom inicjatywa ta przyspieszy rozwój edukacji obywatelstwa cyfrowego, zapewniając jej odporność i skuteczność w stale zmieniającym się krajobrazie cyfrowym.

27-28 maja w Strasbourgu odbędzie się Forum Cyfrowej Edukacji Obywatelskiej. Forum stanowi pomoc dla państw członkowskich w dalszym tworzeniu włączających, opartych na równości i wzmacniających środowisk uczenia się. Forum ma sprzyjać włączeniu edukacji cyfrowej jako priorytetu politycznego, przeprojektowaniu metod pedagogicznych i warunków uczenia się, a także wykorzystaniu technologii cyfrowych z korzyścią dla wszystkich uczących się. Ostatecznym celem Forum jest przyczynienie się do określenia realistycznych działań w odpowiedzi na wyzwania, które pojawiły się lub zostały wzmocnione przez technologie cyfrowe.

Głównymi celami Forum są:

• promowanie wielostronnej współpracy wykorzystującej w pełni korzyści płynące z edukacji na rzecz obywatelstwa cyfrowego,

• prezentacja inicjatyw Cyfrowej Edukacji Obywatelskiej i szerzenie wiedzy na poziomie ogólnoeuropejskim i międzynarodowym, oraz

• zatwierdzenie kierunków tematycznych i opracowanie konkretnych działań w ramach mapy drogowej na najbliższe 5 lat.

6 EDUKACJA

Dodatkowe informacje można znaleźć tutaj.

Źródło: materiał Rady Europy

fot. pixabay

PRZEDSTAWICIELE UODO POJADĄ DO FINLANDII I NA WĘGRY, BY DOWIEDZIEĆ SIĘ, JAK SKUTECZNIE WDROŻYĆ DGA

Decyzją Komisji Europejskiej z 31 marca br. UODO otrzyma dofinansowanie na organizację wizyt studyjnych dotyczących wdrażania DGA w Polsce.

Dofinansowanie zostało przyznane w ramach inicjatywy flagowej PACE – Public Administration Cooperation Exchange Instrumentu Wsparcia Technicznego. Celem inicjatywy jest budowanie potencjału administracyjnego poprzez promowanie współpracy i wymiany transgranicznej między państwami członkowskimi.

Projekt ma skutkować wymianą doświadczeń i krajowych perspektyw w zakresie ochrony danych, w szczególności w stosowaniu nowych rozwiązań prawnych, jakim jest Akt w sprawie zarządzania danymi (DGA). Organizacja serii wizyt studyjnych dotyczących wdrażania DGA, ma wesprzeć współpracę i zapewnić transgraniczną wymianę najlepszych praktyk pomiędzy Polską, Finlandią i Węgrami.

Zaplanowane wizyty studyjne umożliwią przedstawicielom Urzędu Ochrony Danych Osobowych poznanie metod pracy fińskiej Agencji Transportu i Komunikacji Traficom oraz węgierskiego Krajowego Urzędu Ochrony Danych i Wolności Informacji, odpowiedzialnych za wdrożenie i wykonywanie zadań w związku z DGA. Pozwoli to na zdobycie wiedzy o tym, w jaki sposób instytucje w Finlandii i na Węgrzech wdrożyły Akt w sprawie zarządzania danymi, w szczególności: ustalenie, jak w praktyce wygląda wdrażanie nałożonych przez DGA obowiązków.

Spotkania przyczynią się w bezpośredni sposób do bardziej efektywnego wdrożenia DGA w Polsce, umożliwiając czerpanie z dobrych praktyk podmiotów mających doświadczenie w tym zakresie.

Projekt PACE – Data Governance Act implementation znajduje się na liście polskich projektów, które uzyskały wsparcie w ramach Instrumentu Wsparcia Technicznego w 2025 r.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl