URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 04/04/24

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

tak jak informowałem przed miesiącem, dalej pracujemy nad tworzeniem i wzmocnieniem sieci współpracy z organizacjami społecznymi, w tym przede wszystkim z organizacjami zrzeszającymi inspektorów ochrony danych osobowych, po to by lepiej komunikować się i wspólnie rozwiązywać problemy związane z przetwarzaniem danych osobowych. Chcemy wspólnie tworzyć podstawy nowoczesnej ochrony danych osobowych i ich bezpiecznego przetwarzania. Pracujemy także nad branżowymi kodeksami postępowania i nad procesem certyfikacji. Planujemy aktualizację poradników UODO, będziemy w najbliższym czasie ogłaszać w tej sprawie publiczne konsultacje społeczne.

To wszystko było także przedmiotem moich kwietniowych spotkań wraz z zastępcami, między innymi z kościelnym inspektorem ochrony danych, inspektorami ochrony danych osobowych izb radców prawnych oraz Krajowej Izby Radców Prawnych, Związkiem Banków Polskich, Ogólnopolskim Stowarzyszeniem Ochrony Danych Osobowych w Sektorze Medycznym czy Stowarzyszeniem Marketingu Bezpośredniego.

Jednocześnie działamy na rzecz wzmocnienia praw obywateli w zakresie prywatności. Dane osobowe będą bardziej bezpieczne i lepiej przetwarzane, jeśli więcej obywateli będzie umiało upominać się o swoje prawo.

Aby wzmocnić ten proces wycofałem skargę kasacyjną mojego poprzednika na decyzję WSA w Warszawie w sprawie przetwarzania przez Pocztę Polską danych 30 mln obywateli z bazy PESEL w czasie przygotowywania do wyborów korespondencyjnych w kwietniu 2020 r. Chodziło o skargę obywatela, który poskarżył się na bezpodstawne posługiwanie się jego danymi. To stanowisko ma już potwierdzenie w wyrokach sądów, a przede wszystkim w wyroku NSA. Wycofanie skargi oznacza, że uprawomocnia się korzystny dla obywatela wyrok WSA. Dla UODO aktywność obywatelska w sprawie ochrony danych ma ogromne znaczenie.

Równocześnie konkretyzuję też nasze zaangażowanie w prawną edukację obywatelską. Nasi przedstawiciele dzielili się np. w kwietniu swoją wiedzą z zakresu ochrony praw podstawowych m.in. z uczniami Liceum Ogólnokształcącego im. Piotra Skargi w Grójcu. Warsztaty odbyły się z inicjatywy Fundacji Aktywna Demokracja, a ich celem jest propagowanie wśród młodych osób wiedzy na temat praw konstytucyjnych oraz zachęcanie do podejmowania aktywności obywatelskich.

O wyzwaniach i dobrych praktykach w zakresie ochrony prywatności dzieci i młodzieży rozmawialiśmy na konferencji 26 kwietnia 2024 r. W jej trakcie podpisałem porozumienie o współpracy pomiędzy Urzędem Ochrony Danych Osobowych a Rzeczniczką Praw Dziecka w zakresie inicjatyw edukacyjnych i badawczych dotyczących danych osobowych dzieci i młodzieży.

Miałem też na tym spotkaniu zaszczyt wręczyć wraz z moją szanowną koleżanką, Rzeczniczką Praw Dziecka Moniką Horną-Cieślak, nagrodę im. Michała Serzyckiego za promowanie wartości ochrony danych osobowych i prawa do prywatności. Jej laureatką w tym roku została nauczycielka – dr Joanna Hałoń-Gnutek, której inicjatywy i działania przyczyniają się do podnoszenia poziomu wiedzy i świadomości uczniów w zakresie ochrony danych osobowych i prawa do prywatności.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Wstęp do kwietniowego numeru chciałbym zacząć od podziękowań dla Adama Sanockiego, który od początku powstania „Biuletynu UODO" witał Was na łamach naszego wydawnictwa, zachęcając do zapoznania się z poszczególnymi materiałami. Dyrektor Departamentu Komunikacji Społecznej, Rzecznik Prasowy UODO przez ponad 5 lat reprezentował organ nadzorczy na zewnątrz. Był niezastąpiony w roli prowadzącego konferencje, moderatora debat, eksperta i wielkiego entuzjasty ochrony danych osobowych i prywatności. Teraz czekają na niego kolejne zawodowe wyzwania, którym – jestem przekonany – z sukcesami stawi czoła. Powodzenia Adamie!

W tym miesiącu szczególnie zachęcam do przeczytania wywiadu z Konradem Komornickim, Zastępcą Prezesa Urzędu Ochrony Danych Osobowych. Rozmawialiśmy m.in. o tym dlaczego język, którym posługuje się Urząd powinien być zrozumiały, prosty i inkluzywny; jakie są jego pomysły na sprawne działanie UODO; i dlaczego bezpieczeństwo danych osobowych dzieci jest mu szczególnie bliskie.

Ochrona prywatności i danych osobowych najmłodszych to kwestie, które bardzo absorbują Prezesa UODO, dlatego też poświęciliśmy im sporo miejsca w biuletynie. Poruszamy temat budzący wiele kontrowersji – GPS oraz aplikacji do kontroli rodzicielskiej w celu monitorowania miejsca pobytu dzieci. Przetwarzanie danych geolokalizacyjnych ma wyjątkowe znaczenie z punktu widzenia danych osobowych dziecka. Niestety niektóre instytucje zdają się zapominać o tym, że dzieci mają prawo do ochrony swoich danych. Tak było w przypadku szkoły językowej, która zbierała dane dzieci, by przekazać ofertę rodzicom. Prezes Urzędu Ochrony Danych Osobowych stwierdził m.in. naruszenie przez przedsiębiorcę obowiązków informacyjnych zarówno wobec dziecka, jak i rodzica. Namawiam do zapoznania się ze szczegółami tej decyzji.

Informujemy nt. zmian legislacyjnych Unii Europejskiej – nowych przepisów dot. przejrzystości i targetowania reklamy politycznej, które mają przeciwdziałać manipulowaniu informacjami i obcym ingerencjom w wybory, a także zatwierdzeniu przez Parlament Europejski aktu w sprawie sztucznej inteligencji.

Polecam artykuł dot. biometrycznej weryfikacji tożsamości klientów usług płatniczych. UODO przypomina, że przetwarzanie przez instytucje finansowe danych biometrycznych klientów na potrzeby weryfikacji ich tożsamości nie powinno być podstawową, a tym bardziej jedyną stosowaną w tym celu metodą.

Piszemy też m.in. o tym, jak informować o wygaszeniu decyzji o rejestracji pojazdu, o dochodzeniu, jakie wszczął włoski organ ochrony danych przeciwko OpenAI, przytaczamy kilka głośnych wyroków Europejskiego Trybunału Sprawiedliwości Unii Europejskiej, jak również Europejskiego Trybunału Praw Człowieka.

Zapewniam, że najnowszy numer „Biuletynu UODO" to duża dawka potrzebnej wiedzy na temat ochrony danych osobowych. Życzę miłej lektury!

Karol Witowski
Zastępca Rzecznika Prasowego UODO

BYCIE BLIŻEJ OBYWATELA NIE MOŻE BYĆ PUSTYM SLOGANEM

Z Konradem Komornickim, Zastępcą Prezesa UODO rozmawiał Karol Witowski, Zastępca Rzecznika Prasowego UODO

Pomimo, że był Pan kontrkandydatem Mirosława Wróblewskiego na stanowisko PUODO zdają się Panowie mieć ze sobą wiele wspólnego, jeśli chodzi o wizję działania Urzędu. Zbliżony stosunek do dyrektywy policyjnej, podkreślenie prymatu człowieka i przestrzegania Konstytucji, sprzeciw wobec bezrefleksyjnego stosowania RODO, wprowadzenie prostego języka w komunikacji... Jakie jeszcze wspólne poglądy na funkcjonowanie UODO łączą Pana z obecnym prezesem, a co jest przedmiotem Państwa dyskusji, jeśli może Pan zdradzić?

Przypomnę, że nie pierwszy raz w historii organu właściwego do spraw ochrony danych osobowych wcześniejsi kontrkandydaci później ze sobą współpracowali. W 2006 roku, Śp. Pan Michał Serzycki, późniejszy GIODO konkurował z Panem Andrzejem Lewińskim, który później został jego zastępcą. Z Panem Prezesem Wróblewskim łączy nas wiele, chociaż mamy odmienne doświadczenia zawodowe i wykształcenie.

Co do dyrektywy policyjnej nigdy nie ukrywałem, że podzielam tutaj pogląd wyrażony przez Rzecznika Praw Obywatelskich. Krótko wspomnę tu o art. 17 dyrektywy, gdzie ustawa daje wprawdzie możliwość złożenia skargi do PUODO, ale ma ona przysługiwać wtedy, kiedy dane osobowe są przetwarzane niezgodnie z prawem. Skąd jednak mamy wiedzieć, że są niewłaściwie przetwarzane?

Poza tym jestem zwolennikiem stworzenia organu nadzorującego służby specjalne. Służby mogą, a raczej mają obowiązek inwigilować przestępców, terrorystów itp., natomiast nie mają prawa robić tego nadmiarowo i bez jakichkolwiek obwarowań prawnych. Instytucje nadzorujące służby pod kątem przetwarzania danych osobowych funkcjonują w innych państwach, jak Niemcy czy Francja.

Prawo do prywatności mamy zapisane w Konstytucji, ale za rzadko o nim rozmawiamy. Bardzo podoba mi się włączenie UODO w akcję edukacyjną Tour de Konstytucja – spotkania organizowane w całym kraju szerzące wiedzę o prawach i wolnościach konstytucyjnych to dobry krok, by

upowszechniać w społeczeństwie ideę poszanowania dla praw obywatelskich, w tym ochrony danych osobowych.

Podzielam zdanie Prezesa, że RODO ma nam pomagać, a nie przeszkadzać. Prezes Wróblewski podąża mocno w tę stronę od pierwszego dnia przejęcia sterów w UODO. Jest w tym konsekwentny, co bardzo sobie cenię. To „proste RODO" łączy się ze sposobem w jaki się komunikujemy. Bycie bliżej obywatela nie może być pustym sloganem. Mówmy do ludzi tak, by nas zrozumieli. Muszą nas rozumieć, żeby wiedzieli jakie mają prawa i jak mają o nie walczyć. Taka specjalistyczna komunikacja, czasami rozbudowana, choć pozornie precyzyjna nie jest zrozumiała dla większości ludzi. Trochę to porównam z tzw. umowami frankowymi. Oczywiście dotyczy to innego obszaru, ale w coś tym jest. Dlatego bardzo mi zależy na tym, żeby nasze komunikaty były zrozumiałe i proste, tak aby skutecznie przekazywać najważniejsze informacje.

Czy coś nas dzieli z Prezesem Wróblewskim? Dyskutujemy ze sobą cały czas. Zarówno z Prezesem Wróblewskim, jak i z prof. Grzelak szukamy rozwiązań. Docieramy się ze sobą, wsłuchując się nie tylko w swoje poglądy, ale również głosy z zewnątrz – chociażby Konfederacji Lewiatan, Stowarzyszenia Inspektorów Ochrony Danych Osobowych czy Krajowej Rady Radców Prawnych.

Prezes Wróblewski kilkukrotnie mówił, że UODO powinien być bardziej Urzędem Ochrony Danych niż Urzędem Ochrony Danych Osobowych. Jak Pan się zapatruje na takie spojrzenie i jakie jest Pana zdanie na ten temat?

Precyzując UODO powinno być Urzędem Ochrony Danych ze szczególnym uwzględnieniem ochrony danych osobowych. Rzeczą oczywistą jest to, że coraz więcej danych osobowych przenika się z innymi danymi w tzw. świecie cyfrowym. Dlatego nie sposób nie zgodzić się z takim spojrzeniem, które ma sprostać wyzwaniom. Prace trwają szczególnie co do harmonizacji przepisów w kontekście implementacji unijnych rozwiązań.

Podkreśla Pan, że społeczeństwo nie może być elitarne, a język którym posługuje się Urząd powinien być zrozumiały, prosty i inkluzywny. Popularyzacja tzw. prostego języka, odpowiadającego zasadom dostępności i komunikacji publicznej w Urzędzie, w którym dotychczas prym wiódł trudny, precyzyjny język prawniczy jest dużym wyzwaniem. Na jaki efekt tych zmian Pan liczy?

Urząd Ochrony Danych Osobowych ma wybitnych specjalistów, którzy niewątpliwie znają się doskonale na swojej pracy. Od strony merytorycznej oceniam ich bardzo wysoko. Czasem jednak ogrom wiedzy, kompetencje nie do podważenia i ciągłe przebywanie w otoczeniu osób o wykształceniu prawniczym

może być pewną rutyną. Trudno, posługując się specjalistycznym językiem dotrzeć do osób, które z tym dyskursem nie mają styczności na co dzień. Przepisy RODO i stanowiska Urzędu powinny być przekazywane w taki sposób, by każdy obywatel mógł je zrozumieć. Posługując się językiem prostym i zrozumiałym dla każdego, jesteśmy w stanie rzetelnie przekazać informacje. Nie chcę więcej sytuacji, w których społeczeństwo zastanawia się, co UODO miał na myśli publikując takie, a nie inne stanowisko. Wszyscy jesteśmy różni, z uwagi na status społeczny, wykształcenie, wiek, płeć itd., ale mamy takie samo prawo do uzyskania zrozumiałych informacji. Oczywiście temat jest bardziej skomplikowany, ponieważ dokumenty muszą precyzyjnie określać stan prawny, a tę precyzję i jednoznaczność gwarantuje właśnie język prawniczy. Pogodzenie tych dwóch światów to wyzwanie, które już podjęliśmy i zamierzamy konsekwentnie realizować. Takie wnioski też płyną ze spotkań ze środowiskami inspektorów ochrony danych osobowych.

Pana doświadczenie pod kątem systemów teleinformatycznych jest imponujące. Przez 25 lat nadzorował Pan piony teleinformatyczne poważnych instytucji. Jakie usprawnienia w tym zakresie chciałby Pan wprowadzić w UODO?

Rzeczywiście przez 25 lat w nadzorowałem szeroko pojęty system zarządzania bezpieczeństwem informacji, zarówno w największych państwowych podmiotach, jak i prywatnych z różnego rodzaju sektorów gospodarki. Bezspornie znacząca część tych zadań polegała na zapewnieniu ochrony systemów teleinformatycznych, w których m.in. dane osobowe były przetwarzane na masową skalę. Jakie usprawnienia chciałbym wprowadzić? To pewne usprawnienia z wykorzystaniem technologii teleinformatycznych w komunikacji wewnętrznej, a przede wszystkim zewnętrznej. Nie zapeszając powiem, że już uruchomiliśmy projekty, które temu służą. Szczegóły niebawem.

Podczas konferencji „Przyszłość ochrony danych osobowych w Polsce – w przededniu wyboru nowego Prezesa Urzędu Ochrony Danych Osobowych" w Sejmie zastanawiał się Pan, dlaczego nie ma kodeksu postępowania dla samorządu terytorialnego. Prace nad kodeksami trwają. Jakie są plany powstania takiego kodeksu?

Jak wiemy, samorządy terytorialne każdego szczebla od gminy po województwo i jego jednostki organizacyjne przetwarzają najwięcej naszych danych osobowych zarówno w formie tradycyjnej, jak i cyfrowej. Pracowałem na kierowniczych stanowiskach w warszawskim samorządzie i z doświadczenia wiem, że taki kodeks może być pomocnym narzędziem dla administratorów i podmiotów przetwarzających w jednostkach samorządu terytorialnego. Kodeks pokazałby nie tylko zgodności z RODO, ale także praktyczną ścieżkę w dążeniu do zachowania jak najwyższego poziomu w stosowaniu przepisów dotyczących ochrony danych osobowych. Unaoczniłby czytelną relację pomiędzy

administratorami danych osobowych w kontaktach wewnątrz samorządu (np. prezydent miasta a szef podległej mu jednostki organizacyjnej). Już nie mówiąc o kwestiach bezpieczeństwa teleinformatycznego.

Mamy na to doskonały moment. Jesteśmy świeżo po wyborach samorządowych, gdzie kształtują się nowe władze i ich organizacje np.: Unia Metropolii Polskich, Związek Powiatów Polskich itp.

Jeszcze przed wakacjami będziemy chcieli usiąść do stołu i opracować model działania i współpracy na rzecz bezpieczeństwa ochrony danych osobowych w samorządzie terytorialnym.

Wielokrotnie podkreślał Pan jak ważne jest stanowisko IOD w organizacji. Jak Urząd chce wzmocnić pozycję Inspektora Ochrony Danych?

Powiem krótko. Wystarczy prześledzić stronę www.uodo.gov.pl i zobaczyć ostatnią aktywność PUODO w tym zakresie. Spotykamy się ze wszystkimi organizacjami i stowarzyszeniami zrzeszającymi IOD-ów. Otwartość i współpraca. To nas cechuje. Co do wzmocnienia pozycji inspektora była o tym mowa m.in. 9 kwietnia br. na konferencji zorganizowanej przez UODO. Poświęcona ona była m.in. wzmocnieniu roli IOD poprzez podkreślenie jego niezależności. Przywołaliśmy sprawozdanie EROD podsumowujące działania i rekomendacje organów nadzorczych w ramach CEF DPO. Oczywiście kolejnym adresatem wzmocnienia roli IOD są administratorzy danych osobowych. Nie ukrywam, że i tu będziemy prowadzili lobbing na rzecz wzmocnienia roli IOD. M.in. wspomniana przeze mnie kwestia rozmów z jednostkami samorządu terytorialnego i ich organizacjami ma temu służyć. Takim działaniem są też spotkania z samorządami gospodarczymi zrzeszającymi największych pracodawców w naszym kraju. A wiem, że zdarzają się sytuacje, gdzie w podmiocie przetwarzającym dane na masową skalę IOD znany jest przez Administratora jedynie z tzw. pieczątki i nie wie nawet jak ona/on wygląda. To jest niedopuszczalne.

Jak umożliwić obywatelowi skonsultowanie skargi, zanim trafi ona do UODO? Czy pomoc infolinii, która jest niezwykle zaangażowana w rozwiązywanie problemów dzwoniących, wystarczy?

Nasza Infolinia to zespół dobrze przeszkolonych specjalistów, którzy mają bardzo dużą wiedzę prawniczą z zakresu ochrony danych osobowych. Każdego dnia, od poniedziałku do piątku, w godzinach 10-14 udzielają porad, konsultacji z zakresu danych osobowych. Mamy pewne plany związane ze zmianą godzin pracy Infolinii, zależy nam na uelastycznieniu modelu funkcjonowania tej formy kontaktu ze społeczeństwem, aby Infolinia była bardziej dostępna.

1 ROZMOWA Z EKSPERTEM

Jeśli chodzi o przyjmowanie interesantów to nie posiadamy oddziałów terenowych, nasze biuro mieści się w Warszawie. Chciałbym, żeby obywatel miał możliwość umówienia się na kontakt telefoniczny z ekspertem z Urzędu w celu omówienia swojej sprawy. Teoretycznie jest to układ idealny dla obydwu stron, bo pozwala na szybką, efektywną komunikację klienta ze specjalistą z Urzędu, a czasem i ekspresowe rozwiązanie problemu osoby, która zwraca się do nas o pomoc. W praktyce jednak mamy ograniczony budżet, a co za tym idzie limit w postaci personelu, miejsca i czasu, którego wciąż nam brakuje. Do tego dochodzi problem z uwierzytelnianiem rozmówców. Sukcesywnie staramy się przezwyciężyć wszystkie te trudności.

Gościł Pan ostatnio na konferencji podsumowującej „Projekt innowacyjno-wdrożeniowy w zakresie oceny funkcjonalnej" zorganizowanej przez Ministerstwo Edukacji Narodowej w Katowicach, gdzie stwierdził Pan, że tematyka ta jest Panu bliska również z osobistych względów – jest Pan tatą 5,5 latka. Czy to sprawia, że jest Pan bardziej zaangażowany w sprawy dot. ochrony danych osobowych dzieci? Bezpieczeństwo danych osób niepełnoletnich to też przestrzeń, w której dostrzegamy szczególną aktywność Prezesa.

Jest to przedmiot zainteresowania Prezesa, który patrzy na najmłodszych z troską i wie, że w dzieci trzeba inwestować, musimy je wspierać, szczególnie, że nierozwiązane problemy wrócą do nas ze zdwojoną siłą.

Jeśli chodzi o mnie, to jak każdy człowiek występuję w wielu rolach. Aktywność zawodowa jest dla mnie niezwykle ważna, ale jednocześnie również rola taty to nieodłączny fundament, na którym stoję i nic nie jest w stanie tego zmienić. Z tego względu dodatkowo zainteresował mnie projekt innowacyjno-wdrożeniowy przedstawiony przez MEN i to, że mogę przyjrzeć się mu z dwóch stron – specjalisty bezpieczeństwa danych oraz rodzica. Utworzenie platformy, bazy, w której dla rodzica i osoby, która ma udzielić pomoc dziecku, dostępne są informacje z różnych organizacji: szpitali, przychodni, poradni psychologiczno-pedagogicznej itp. to wspaniały pomysł i rozwiązanie systemowe, którego bardzo nam brakuje. To wsparcie dla rodzin, szybka i efektywna pomoc specjalistów, ograniczenie kosztów (chociażby przez to, że specjaliści nie dyblują badań, bo mają dostęp to wyników badań już zrealizowanych). Korzyści mógłbym długo wymieniać.

I nie zapominajmy, że jesteśmy systemem naczyń połączonych. Problemy dziecka są nie tylko problemem jego i rodziny, w której dorasta, ale także całych społeczności. Na konferencji mowa była chociażby o samobójstwach dzieci, których można uniknąć, gdy dostęp do informacji jest szybki, a pomoc jest udzielona natychmiast. Takie wydarzenie jak samobójstwo zostawia ślad nie tylko wśród najbliższych ofiary, ale w znacząco szerszym gronie.

1 ROZMOWA Z EKSPERTEM

O wyzwaniach i dobrych praktykach w zakresie ochrony prywatności dzieci i młodzieży będziemy też rozmawiać 26 kwietnia 2024 r. podczas konferencji zorganizowanej przez Prezesa UODO we współpracy z Rzeczniczką Praw Dziecka. Myślę, że temat ten musi nieustająco wybrzmiewać w naszej komunikacji. Mówmy głośno o najważniejszych problemach oraz dobrych praktykach w zakresie ochrony prywatności i danych osobowych dzieci i młodzieży. Podkreślajmy kwestie dotyczące podmiotowości dzieci i potrzeby respektowania ich zdania. Musimy być szczególnie uważni na ich prawa w dobie dynamicznego rozwoju technologicznego i wyzwań, jakie rodzi dla ochrony danych osobowych powszechne wykorzystanie sztucznej inteligencji. Bądźmy też otwarci na wszelkie pomysły i rozwiązania innych państw członkowskich UE do skutecznej ochrony danych osobowych najmłodszych.

Przypomnę, że to wszystko wpisuje się w art. 57 RODO, który mówi o zadaniach organu nadzorczego tj. m.in. o upowszechnianiu w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz o rozumieniu tych zjawisk. Szczególną uwagę poświęca właśnie działaniom skierowanym do dzieci.

Podczas konferencji w Katowicach mówił Pan o stworzeniu teleinformatycznego systemu centralnego, międzysektorowej bazy danych pod kątem pozyskiwania danych. Proszę powiedzieć, na co należy zwrócić szczególną uwagę podczas budowania takiej bazy.

Zadaniem Urzędu na pewno będzie wskazanie ryzyk i potencjalnych niebezpieczeństw zw. z przetwarzaniem danych przez ten system. Zadeklarowałem pełne wsparcie UODO w przeprowadzeniu tego procesu. Liczę na współpracę innych resortów i, po konstruktywnych konsultacjach, wypracowaniu wspólnego modelu. Pojawia się tu konieczność udzielenia odpowiedzi na kilka kluczowych pytań, między innymi o to kto jest administratorem danych osobowych, czyli podmiotem, który będzie ustalał cele i szczegóły przetwarzania danych. Czy bezpośrednio będzie przetwarzał te dane? Jaka jest rola koordynatora instytucjonalnego? Jaka będzie ocena skutków dla przetwarzania tych danych? Ministerstwa muszą wypracować model ogólnokrajowy, jednak pozostaje kwestia tego jak będzie to wyglądało w terenie.

Idealny wydaje się model centralny, gdyż system rozproszony powoduje kłopoty w sytuacji zmiany miejsca zamieszkania. W takiej sytuacji dane za nim nie idą. Co więcej, system centralny jest bezpieczniejszy od wielu systemów lokalnych, z uwagi na jego pełną rozliczalność, legalność. Przypomnę jeszcze, że mówimy o przetwarzaniu danych wrażliwych, danych szczególnej kategorii. Pamiętajmy też, że do 16 roku życia przetwarzanie danych dzieci odbywa się za zgodą rodzica. W grę wchodzi także kwestia wyboru wykonawcy systemu. Jeżeli postępowanie prowadzone byłoby

na zasadzie, że każdy powiat jest zamawiającym, to w takim wypadku mielibyśmy 314 postępowań?

Musimy uwzględnić również privacy by design i zastanowić się, kto będzie miał dostęp do tego systemu i w jakim zakresie. Nie możemy dopuścić do ich nadmiarowego przetwarzania. Przyjrzenia wymaga kwestia wymagań funkcjonalnych i niefunkcjonalnych tego systemu. Zagadnień jest wiele, ale przy woli i zaangażowaniu wszystkich stron, wierzę, że możliwe jest stworzenie systemu teleinformatycznego, w którym wszystkie wspomniane przeze mnie elementy zostaną uwzględnione na każdym etapie jego projektowania.

Przypomnę, że to wszystko wpisuje się w art. 57 RODO, który mówi o zadaniach organu nadzorczego tj. m.in. o upowszechnianiu w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz o rozumieniu tych zjawisk. Szczególną uwagę poświęca właśnie działaniom skierowanym do dzieci.

Bardzo dziękuję za rozmowę.

BIOMETRYCZNA WERYFIKACJA TOŻSAMOŚCI KLIENTÓW USŁUG PŁATNICZYCH

Przetwarzanie przez instytucje finansowe danych biometrycznych klientów na potrzeby weryfikacji ich tożsamości nie powinno być podstawową, a tym bardziej jedyną stosowaną w tym celu metodą. Natomiast wyłączną przesłanką legalizującą takie działanie powinna być wyraźna i świadoma zgoda osób, których dane dotyczą.

W związku z trwającą w środowisku finansistów dyskusją i wpływającymi pytaniami, UODO zajmował się w ostatnim czasie kwestią wykorzystywania analiz behawioralnych w celu ograniczania transakcji oszukańczych w płatnościach bezgotówkowych.

Ponieważ korzystanie z tej technologii stanowi głęboką ingerencję w – zagwarantowane przepisami Karty Praw Podstawowych Unii Europejskiej (art. 7 i art. 8 ust. 1), Konstytucji RP (art. 47 i art. 51) oraz RODO – prawo do prywatności i prawo do ochrony danych osobowych, zagadnienie to budzi szczególne zainteresowanie organu nadzorczego w kontekście zgodności z zasadami ochrony danych osobowych.

Szczególne dane wymagają wzmożonej ochrony

Stosowanie przez instytucje finansowe analizy behawioralnej (np. sposobu pisania na klawiaturze czy sposobu poruszania myszą komputera) i tworzenie na podstawie cech charakterystycznych dla danego użytkownika jego unikalnego profilu oraz późniejsze wykorzystywanie tych danych w celu uwierzytelniania klientów usług płatniczych wiąże się z przetwarzaniem danych biometrycznych w rozumieniu art. 4 pkt 14 RODO, które należą do danych szczególnych kategorii i których wykorzystywanie – stosownie do art. 9 RODO – podlega wzmocnionej ochronie.

Dane biometryczne w RODO i Wytycznych

Stosownie do art. 4 pkt 14 RODO „dane biometryczne" oznaczają dane, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub specjalnego przetwarzania technicznego oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Dane biometryczne są danymi szczególnej kategorii w rozumieniu art. 9 ust. 1 RODO.

Wiele cennych informacji i wskazówek dotyczących danych biometrycznych i ich przetwarzania zawartych jest w takich dokumentach, jak przyjęta 27 kwietnia 2012 r. Opinia 3/2012 Grupy Roboczej Art. 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193) czy przyjęte 29 stycznia 2020 r. Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo.

Europejska Rada Ochrony Danych (EROD) w Wytycznych 3/2019 wskazała, że aby dane były uznane za biometryczne należy wziąć pod uwagę łącznie trzy elementy: 1) charakter danych – dane dotyczą cech fizycznych, fizjologicznych lub behawioralnych danej osoby fizycznej, 2) środki i sposób przetwarzania wynikać muszą z użycia odpowiedniej technologii oraz 3) dane są przetwarzane w celu jednoznacznej identyfikacji osoby fizycznej.

Jednocześnie w dobie szybkiego rozwoju nowoczesnych technologii przetwarzania danych, zwłaszcza takich jak te oparte na algorytmach sztucznej inteligencji, można zakładać, że unikalne profile klientów dostawców usług płatniczych pozwolą na uzyskanie dodatkowych jeszcze informacji, których ostateczny zakres trudno obecnie przewidzieć.

Dlatego każda decyzja administratora o pozyskiwaniu danych opartych na biometrii powinna być poprzedzona szczególnie wnikliwą analizą. Przetwarzanie takich danych powinno się odbywać nie tylko z poszanowaniem zasady legalności (art. 5 ust. 1 lit. a RODO), ale także być działaniem adekwatnym oraz stosownym i ograniczonym z punktu widzenia realizacji zakładanego celu (art. 5 ust. 1 lit. c RODO).

Takie stanowisko znajduje potwierdzenie w orzecznictwie Trybunału Konstytucyjnego, m.in. w wyroku z 11 kwietnia 2000 r. (sygn. akt K 15/98), w którym TK stwierdza, że: „poszukując odpowiedzi na pytanie, czy ingerencja w sferę konstytucyjnego prawa jednostki jest zgodna z zasadą konieczności, należy rozważyć, czy cel, do którego dąży ustawodawca można osiągnąć przy pomocy środków równie skutecznych, ale mniej uciążliwych dla jednostki".

W świetle powyższego przed wprowadzeniem do stosowania tego rodzaju technik identyfikacji klientów instytucje finansowe powinny przedstawić szczegółowe analizy co do tego, czy rzeczywiście zasadne jest przyjęcie, że podstawowa metoda weryfikacji klienta musi być oparta na analizie jego cech biometrycznych. Instrumentami pomocnymi w dokonaniu takiej oceny są zarówno analiza ryzyka, jak i ocena skutków dla ochrony danych (art. 35 RODO).

Jednocześnie podkreślić należy, że w świetle RODO zasadą jest zakaz przetwarzania danych biometrycznych (art. 9 ust. 1 RODO), a odstępstwo od niego powinno mieć wyraźne oparcie w jednym z wyjątków wprost wymienionych w ust. 2 tego przepisu.

Przepisy sektorowe nie dają odpowiednich gwarancji

Dokonując analizy dopuszczalności przetwarzania danych biometrycznych w celu uwierzytelniania klientów usług płatniczych w pierwszej kolejności rozważyć należy, czy obowiązujące przepisy prawa krajowego regulujące działalność instytucji finansowych pozwalają na przetwarzanie danych biometrycznych do takich celów.

Artykuł 9 ust. 2 lit. g RODO przewiduje, że dane szczególnych kategorii mogą być przetwarzane, gdy jest to niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Wskazać należy, że istniejące przepisy prawa nie mogą stanowić podstawy prawnej do stosowania przez dostawców usług płatniczych systemów gromadzących dane biometryczne. Art. 10 ustawy z 19 sierpnia 2011 r. o usługach płatniczych stanowiący, że dostawcy, organizacje płatnicze i podmioty prowadzące systemy płatności przetwarzają dane osobowe w zakresie niezbędnym do zapobiegania oszustwom związanym z wykonywanymi usługami płatniczymi, prowadzeniem schematu płatniczego lub prowadzeniem systemu płatności oraz dochodzenia i wykrywania tego rodzaju oszustw przez właściwe organy, nie uprawnia banków i innych instytucji sektora finansowego do przetwarzania danych biometrycznych w celu dotyczącym zapobiegania oszustwom. Przepis ten nie przewiduje bowiem odpowiednich gwarancji dla ochrony praw i interesów osób, których dane miałyby być przetwarzane. W szczególności nie przewiduje, jakie dane i w jakim zakresie miałyby być przetwarzane w tym celu, czy w każdej sytuacji, czy jedynie w przypadkach konkretnych wątpliwości co do tożsamości osoby dokonującej płatności, i w jaki konkretnie sposób. Dodatkowo wskazać należy, że obecne brzmienie art. 10 ustawy o usługach

płatniczych zostało nadane art. 118 ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). W wersji ustawy sprzed 4 maja 2019 r. przepis ten stanowił wprost o danych osobowych szczególnych kategorii jako wyłączonych z przetwarzania, stanowiąc o przetwarzaniu „(…) z wyjątkiem danych, o których mowa w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 […]". Treść zmienionego art. 10 nie została jednak wzbogacona o jakiekolwiek elementy gwarancyjne dla podmiotów danych, a zatem nie może być uznana za odpowiednią podstawę przetwarzania danych biometrycznych przez instytucję finansową.

Zgoda i warunki jej wyrażania

W tej sytuacji w ocenie organu nadzorczego jedyną przesłanką, która mogłaby być brana pod uwagę jako podstawa legalizacji przetwarzania danych biometrycznych przez instytucje finansowe, jest świadoma i wyraźna zgoda osoby, której dane dotyczą, a zatem przesłanka wskazana w art. 9 ust. 2 lit. a RODO. Żeby można było mówić o wyrażeniu zgody wyraźnej, konieczne jest, by administrator poinformował ją o ryzykach związanych z przetwarzaniem takich danych, zasadach ich przetwarzania, stosowanych zabezpieczeniach i przysługujących jej uprawnieniach. Zgoda powinna także wyraźnie precyzować cel przetwarzania w momencie jej odbierania. Powinna istnieć również alternatywna metoda, z której podmiot danych mógłby skorzystać w przypadku braku zgody tak, aby nie zostać pozbawionym możliwości skorzystania z konkretnej usługi.

Analizie poddane powinno być także stanowisko EROD wyrażone w Wytycznych 6/2020 w sprawie wzajemnych zależności między dyrektywą PSD2 a RODO". EROD wskazuje m.in., że: „Prawnie uzasadnionym interesem dostawcy usług płatniczych, którego sprawa dotyczy, może być przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom, o ile charakteru nadrzędnego nie mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Czynności przetwarzania w celu zapobiegania nadużyciom powinny opierać się na starannej ocenie poszczególnych przypadków przez administratora zgodnie z zasadą rozliczalności". W ww. Wytycznych EROD wskazuje, że: „Wyraźna zgoda, o której mowa w art. 94 ust. 2 PSD2, jest zgodą umowną. Oznacza to, że art. 94 ust. 2 PSD2 należy interpretować w ten sposób, że zawierając umowę z dostawcą usług płatniczych na podstawie tej dyrektywy, osoby, których dane dotyczą, muszą być w pełni świadome szczególnych kategorii danych osobowych, które będą przetwarzane.

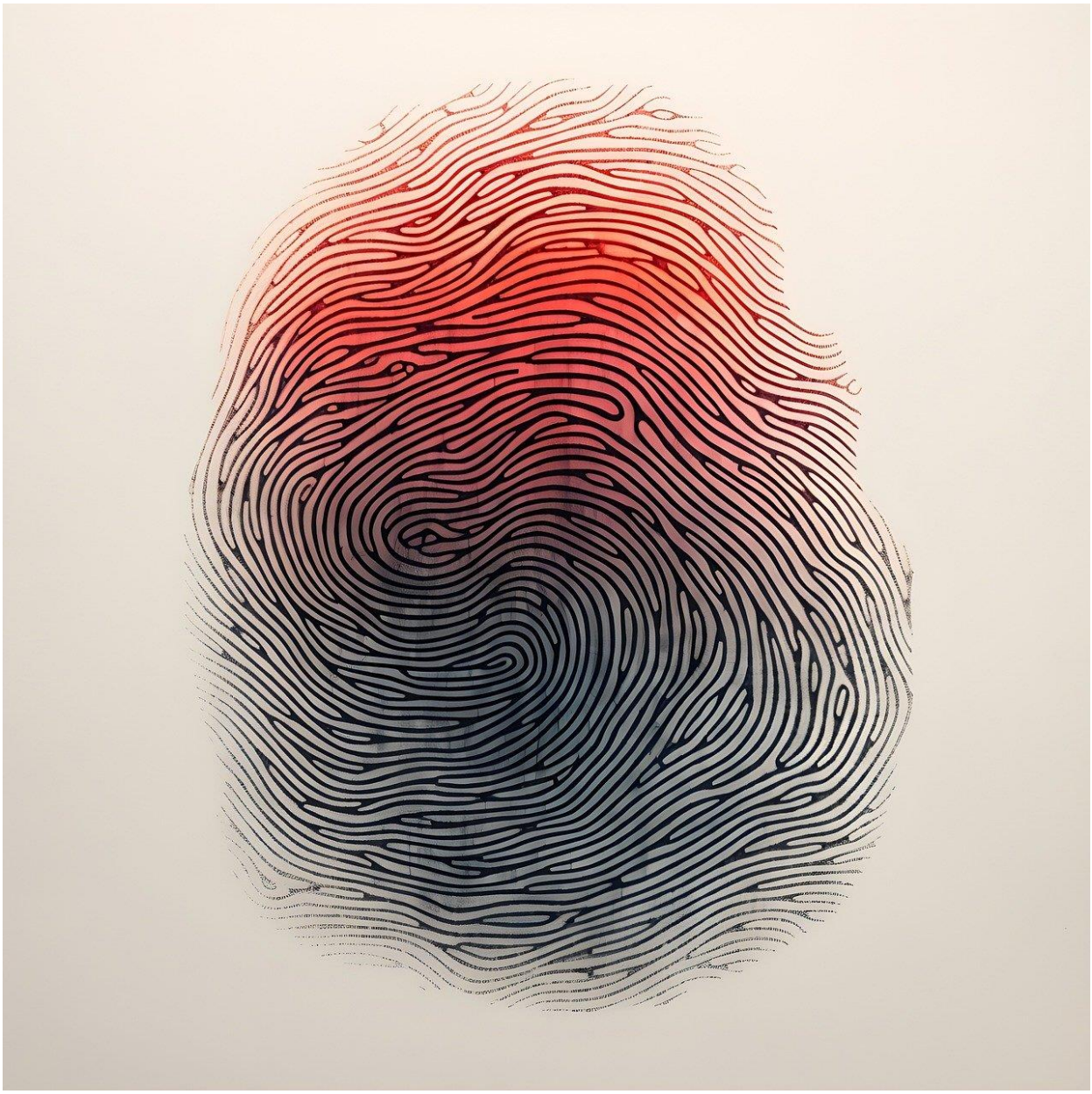
Ponadto należy poinformować je o konkretnym celu (usługa płatnicza), w którym ich dane osobowe będą przetwarzane, i muszą one wyraźnie zgodzić się na te klauzule. Klauzule takie powinny wyraźnie odróżniać się od pozostałych kwestii poruszanych w umowie, a osoba, której dane dotyczą, musiałaby wyraźnie je zaakceptować".

Wskazać należy, że zgodnie z art. 7 ust. 3 RODO osoba, której dane dotyczą, może w dowolnym momencie wycofać zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Zgodnie z motywem 59 RODO administrator powinien przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej zgodnie z RODO, w tym mechanizmy żądania - i gdy ma to zastosowanie bezpłatnego uzyskiwania - w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Odmowa udzielenia zgody nie powinna wpływać niekorzystnie na sytuację klienta.

W kontekście zgody, która powinna być odbierana przez bank od klienta, należy także zwrócić uwagę na regulację art. 22 RODO dotyczącą profilowania. Weryfikacja za pomocą urządzeń opartych na technikach analizy behawioralnej powinna być przeanalizowana pod kątem zgodności z postanowieniami ww. przepisu, który w ust. 1 przewiduje że: „Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa". Wyjątki dopuszczające stosowanie przez administratora tego rodzaju metod przewiduje ust. 2 tego przepisu. W kontekście analizowanych przepisów, przyjmując, że weryfikacja klienta przy pomocy jego danych behawioralnych będzie zachodzić wyłącznie po spełnieniu warunków określonych w art. 22 ust. 2 lit. c RODO, zgoda wyraźna powinna być rozumiana w sposób analogiczny do tej, o której stanowi art. 9 ust. 2 lit. a RODO. Istotne jest także, aby bank, stosując metody oparte na profilowaniu, uwzględnił w procesie przetwarzania wymagania stawiane przez art. 22 ust. 3 RODO, który nakłada na administratora obowiązek wprowadzenia gwarancji dotyczących możliwości zakwestionowania decyzji: „W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji".

Konkluzja

Przy wszystkich wskazanych wyżej uwagach i zastrzeżeniach przyjąć należy, że przetwarzanie przez instytucje finansowe danych biometrycznych klientów nie powinno być podstawową metodą weryfikacji tożsamości klienta. Zbieranie takich danych na podstawie zgody klienta obwarowane zaś jest szeregiem szczegółowych warunków, których spełnienie jest decydujące dla legalności tego procesu.



fot. pixabay

JAK INFORMOWAĆ O WYGASZENIU DECYZJI O REJESTRACJI POJAZDU?

Ustalając zakres danych zamieszczonych w publicznym obwieszczeniu o wygaśnięciu decyzji o rejestracji pojazdu, kierować się należy ogólnymi zasadami z art. 5 RODO, w tym celowości i minimalizacji danych. Pamiętać również należy o ustaleniu właściwego okresu publikacji takiego obwieszczenia.

W związku z przepisami ustawy z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości, które dopuszczają zawiadamianie o wygaśnięciu decyzji o rejestracji pojazdu poprzez publiczne obwieszczenie, do UODO wpływają pytania, czy w takim obwieszczeniu można podać numery rejestracyjne pojazdów kwalifikujących się do wygaszenia rejestracji. Zgodnie bowiem ze stanowiskiem UODO numery rejestracyjne pojazdów stanowią dane osobowe.

Odpowiadając na te wątpliwości organ nadzorczy wskazał, że zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) danymi osobowymi są 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.

Numery tablic rejestracyjnych są zaś informacją, za pośrednictwem której możliwe jest zidentyfikowanie – w sposób pośredni – osoby fizycznej, będącej właścicielem pojazdu. Zgodnie z definicją danych osobowych zawartą w RODO każdy identyfikator urządzenia, na przykład numer VIN, bloku silnika pojazdu lub smartfonu, będzie stanowił dane osobowe, o ile będą one umożliwiały identyfikację posiadacza tak oznaczonego urządzenia.

Numery rejestracyjne, którymi właściciele dysponują przez cały czas posiadania pojazdu, mogą pozwolić na identyfikację konkretnych osób nie tylko odpowiednim organom, ale również osobom

fizycznym, np. sąsiadom, znajomym, współpracownikom. Są oni w stanie powiązać numer rejestracyjny pojazdu z konkretną osobą. Ponadto inne osoby także mogą na podstawie numeru rejestracyjnego zidentyfikować właściciela pojazdu, składając odpowiednio uzasadniony wniosek do Centralnej Ewidencji Pojazdów i Kierowców.

Biorąc pod uwagę powyższe UODO stoi na stanowisku, że numery rejestracyjne pojazdów stanowią dane osobowe, o ile umożliwiają identyfikację posiadacza pojazdu. Stanowisko to znajduje także odzwierciedlenie w orzecznictwie sądów, np. w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 13 kwietnia 2017 r. (sygn. akt VII SA/Wa 1069/16) czy w wyroku WSA z 25 kwietnia 2014 r. (sygn. akt II SA/Wa 30/14), choć ostatnio istnieją także odrębne orzeczenia w tej kwestii (np. wyrok NSA z 28 czerwca 2019 r., sygn. akt I OSK 2063/17). Warto jednak dodać, że stanowisko polskiego organu nadzorczego jest zbieżne ze stanowiskiem wielu innych krajowych organów ochrony danych (np. z Niemiec czy Włoch). Także orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej oraz sądów w innych krajach, jak choćby w Niemczech, uznaje jednoznacznie numery rejestracyjne pojazdów za dane osobowe. Warto dodać, że ostatnio Trybunał Sprawiedliwości Unii Europejskiej orzekł, że nr VIN pojazdu posiada status danej osobowej, jeśli może być użyty do identyfikacji właściciela pojazdu lub innej osoby (wyrok TSUE z 9 listopada 2023 r. w sprawie C-319/22).

Należy jednak pamiętać, że zgodnie z motywem 5 RODO prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności.

Organy administracji publicznej są zobowiązane działać w granicach i na podstawie obowiązujących przepisów prawa regulujących ich działalność. Zgodnie z art. 6 ust. 1 RODO przetwarzanie danych (w tym ich udostępnianie) jest zgodne z prawem, m.in. gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (lit. c).

W niniejszej sprawie istnieje ustawowy obowiązek właściwego organu administracyjnego (starosty) zawiadomienia właściciela pojazdu o wygaśnięciu decyzji o rejestracji pojazdu. Zgodnie z art. 17 ust. 1 ustawy z dnia 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości decyzje o rejestracji pojazdu wydane przed dniem 14 marca 2005 r. dotyczące pojazdów nieposiadających ważnego okresowego badania technicznego, w stosunku do których ich posiadacze nie dopełnili obowiązku zawarcia umowy obowiązkowego ubezpieczenia odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych, jeżeli pojazd im podlega, przez okres dłuższy niż 10 lat, przypadający bezpośrednio przed dniem wejścia w życie niniejszej ustawy,

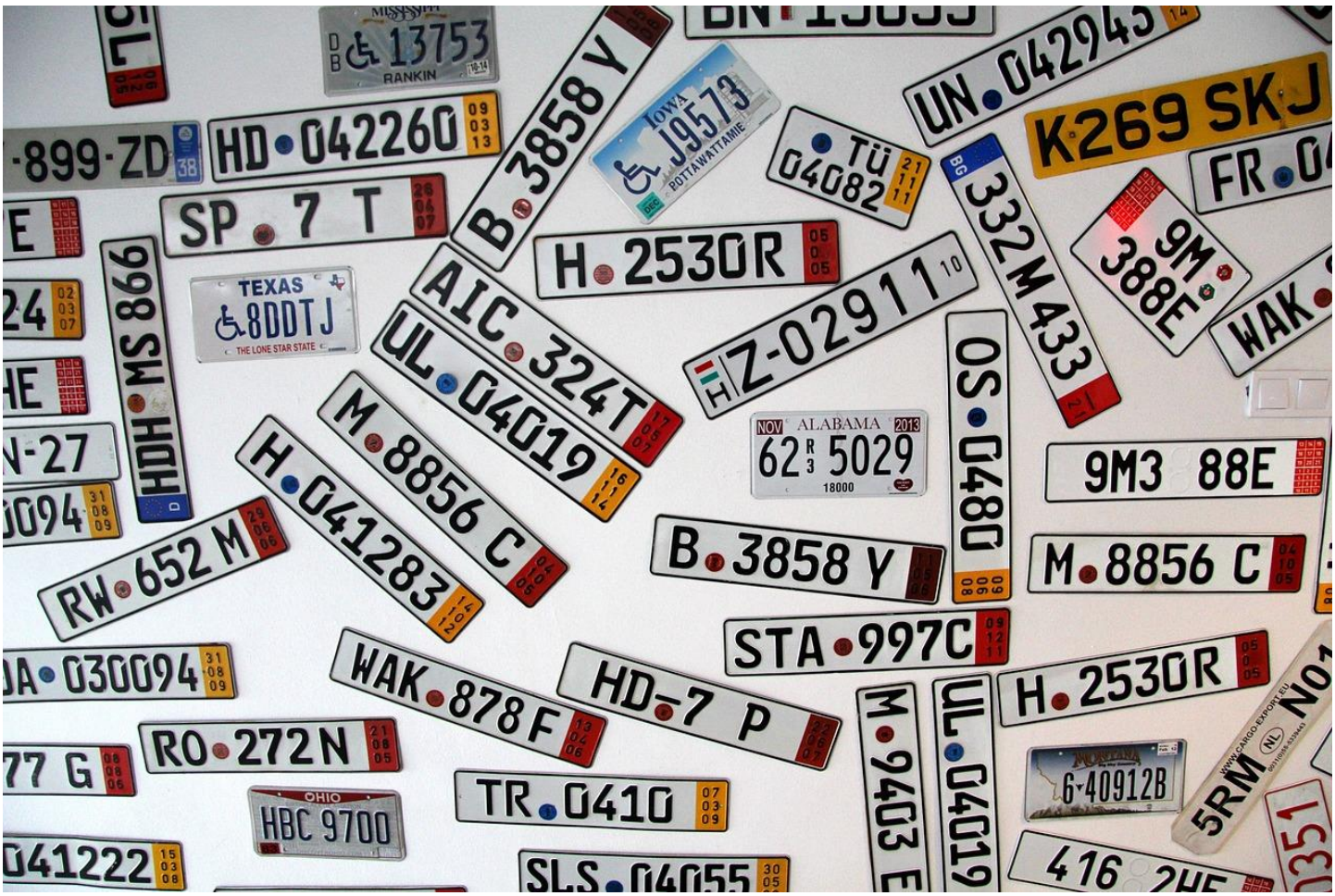
wygasają z dniem 10 czerwca 2024 r. Takie zawiadomienie o wygaśnięciu decyzji może odbywać się przez publiczne obwieszczenie (art. 17 ust. 3). Przepisy te nie wskazują jednak, jaka miałaby być treść takiego publicznego obwieszczenia, podobnie jak przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Te ostatnie określają, że jeżeli przepis szczególny tak stanowi, zawiadomienie stron o decyzjach i innych czynnościach organu administracji publicznej może nastąpić w formie publicznego obwieszczenia, w innej formie publicznego ogłoszenia zwyczajowo przyjętej w danej miejscowości lub przez udostępnienie pisma w Biuletynie Informacji Publicznej na stronie podmiotowej właściwego organu administracji publicznej (art. 49 ust. 1). Dzień, w którym nastąpiło publiczne obwieszczenie, inne publiczne ogłoszenie lub udostępnienie pisma w Biuletynie Informacji Publicznej wskazuje się w treści tego obwieszczenia, ogłoszenia lub w Biuletynie Informacji Publicznej. Zawiadomienie uważa się za dokonane po upływie czternastu dni od dnia, w którym nastąpiło publiczne obwieszczenie, inne publiczne ogłoszenie lub udostępnienie pisma w Biuletynie Informacji Publicznej (art. 49 ust. 2).

Podkreślić jednak należy, że celem publicznego obwieszczenia, które jest fakultatywne, jest zapewnienie szybkiego skutku doręczenia decyzji adresatowi (tak też wyrok Naczelnego Sądu Administracyjnego z 1 lutego 2023 r., sygn. akt III OSK 1825/21).

W sytuacji braku przepisów regulujących dane zagadnienie (tu zakres danych w obwieszczeniu publicznym) zastosowanie znajdują ogólne zasady z art. 5 RODO. Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”). Niezbędne jest również, w świetle zasady celowości (art. 5 ust. lit. b RODO) i ograniczenia czasowego (art. 5 ust. lit. e RODO) określenie, jak długo te obwieszczenia publiczne muszą być publikowane w BIP. W przypadkach, w których prawo nie reguluje okresu retencji danych, administrator, po przeprowadzeniu odpowiednich analiz, powinien określić ten okres tak, aby przetwarzanie danych było zgodne z celami, w których je pozyskano. Zasadność tego stanowiska została potwierdzona w orzecznictwie sądów administracyjnych – jako przykład należy przywołać fragment uzasadnienia do wyroku Wojewódzkiego Sądu Administracyjnego w Lublinie z 1 marca 2016 r. (sygn. akt II SA/Lu 876/15): „[z] art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych wynika zasada ograniczenia czasowego udostępnienia danych osobowych w Biuletynie Informacji Publicznej. Zasada ta oznacza, że nawet jeśli określone dane odpowiadają celowi, dla którego są zbierane, to nie powinny być przetwarzane, w tym udostępniane innym podmiotom ad finitum. Czasowym wyznacznikiem powinno być natomiast osiągnięcie celu przetwarzania.” Podkreślić należy, iż wyrok ten zachowuje aktualność także przy obecnie obowiązujących przepisach o ochronie danych osobowych.

2 UODO SYGNALIZUJE

W związku z powyższym, to administrator (starosta) powinien dokonać oceny, czy w myśl zasady proporcjonalności, minimalizacji i ograniczenia czasowego publikacja numeru rejestracyjnego pojazdu w publicznym ogłoszeniu jest niezbędna do wykonania obowiązku wynikającego z art. 17 ust. 3 ustawy o zmianie niektórych ustaw w celu ograniczenia niektórych skutków kradzieży tożsamości. Warto też zauważyć, że dokonując takiej oceny należy wziąć pod uwagę, że o ile numer rejestracyjny pojazdu może identyfikować osobę fizyczną, to już imię i nazwisko oraz adres zamieszkania dokonuje wprost takiej identyfikacji. Okoliczność ta powinna także być wzięta pod rozwagę przy ostatecznym kształtowaniu zakresu danych osobowych podlegających udostępnieniu i upublicznieniu w określonym terminie.



fot. pixabay

UPOMNIENIE DLA SZKOŁY JĘZYKOWEJ, KTÓRA ZBIERAŁA DANE DZIECI, BY PRZEKAZAĆ OFERTĘ RODZICOM

Przedsiębiorca prowadzący szkołę językową zbierał dane dzieci, by następnie przekazać swą ofertę lekcji języka rodzicom. Prezes UODO po skardze rodzica stwierdził naruszenie RODO. Danych osobowych nie można przetwarzać powołując się na zgodę dziecka. Upomnienie UODO przedsiębiorca zaskarżył, jednak sąd tę skargę oddalił.

Przedstawiciel szkoły językowej na lekcji w szkole podstawowej wręczył uczniom, w tym córce skarżącej, formularz będący prośbą o przekazanie informacji o organizowanych przez nią kursach językowych. Dziewczynka wypełniła formularz podając imię, nazwisko, numer telefonu swój i swojej mamy oraz wskazała klasę, do której chodzi.

Przedstawiciel szkoły językowej skontaktował się telefonicznie z matką dziewczynki i chciał jej przedstawić ofertę kursów językowych. Matka spytała go, skąd ma jej dane. Usłyszała, że za zgodą dyrektora szkoły podstawowej, dzieci na lekcji wypełniły i wyraziły zgodę na przetwarzanie danych osobowych. W korespondencji z przedsiębiorcą matka zakwestionowała podstawy prawne przetwarzania danych osobowych jej oraz jej córki oraz podniosła niewypełnienie wobec niej obowiązku informacyjnego z art. 14 RODO.

Następnie matka złożyła skargę do UODO.

Prezes Urzędu Ochrony Danych Osobowych zbadał sprawę i ustalił, że:
• Przedsiębiorca uważał, że przetwarzał jedynie imię córki skarżącej, klasę i numer telefonu matki. Jednak naprawdę dysponował on szerszym zakresem danych – również informacją o konkretnej szkole, do której chodziła małoletnia, nazwiskiem dziecka i jego numerem telefonu.

• Przedsiębiorca nie wykazał, aby dysponował zgodą matki jako przedstawiciela ustawowego dziecka na przetwarzanie jego danych. W toku postępowania powołał się na art. 8 RODO, zgodnie z którym w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat.

UODO zakwestionował te wyjaśnienia, ponieważ w chwili wyrażenia przez dziewczynkę rzekomej zgody na przetwarzanie danych, dziewczynka nie miała ukończonych 16 lat. Nie mogła więc samodzielnie wyrazić zgody na przetwarzanie swoich danych osobowych, a tym bardziej nie mogła wyrazić zgody na przetwarzanie danych osobowych swojego rodzica.

• Nadto nie można było uznać, aby zebranie danych dziecka i jego rodzica do przedstawienia oferty kursów językowych stanowiło usługę społeczeństwa informacyjnego, za jaką można by uznać dopiero świadczenie nauki języka obcego za pośrednictwem platformy e-learningowej. Dane natomiast były przetwarzane przez przedsiębiorcę w celach marketingowych, w tym w celu marketingu bezpośredniego.

• UODO uznał, że przedsiębiorca, chcąc przedstawić ofertę kursów językowych nie był w żaden sposób uprawniony do pozyskania danych osobowych od małoletniego dziecka, a czyniąc to postąpił niezgodnie z prawem i nierzetelnie. Nadto Prezes Urzędu Ochrony Danych Osobowych uznał, że przedsiębiorca w sposób niezgodny z prawem pozyskał dane skarżącej i jej córki, wobec czego stwierdził naruszenie art. 6 ust. 1 oraz art. 5 ust. 1 RODO. W ocenie organu Przedsiębiorca nie musiał pozyskiwać jakichkolwiek danych, aby przedstawić ofertę kursów językowych.

Prezes Urzędu Ochrony Danych Osobowych stwierdził również naruszenie przez Przedsiębiorcę obowiązków informacyjnych zarówno wobec dziewczynki (art. 13 RODO), jak i jej matki (art. 14 RODO). Przedsiębiorca jako administrator powinien wypełnić obowiązek informacyjny w sposób skuteczny, natomiast scedował realizację tego obowiązku informacyjnego na dziecko, poprzez wręczenie mu klauzuli informacyjnej do przekazania rodzicowi. Organ ocenił tę praktykę za niezgodną z przepisami i uznał, że nie było to skuteczne wykonanie obowiązków informacyjnych wobec matki. Natomiast w odniesieniu do małoletniej organ uznał przede wszystkim, że przedłożona jej klauzula informacyjna była nieprawidłowa, bowiem nie zawierała podstawowych informacji, wynikających z art. 13 RODO. Nadto Przedsiębiorca nie był w stanie wykazać, że dziewczyna się z nią zapoznała. Tym samym organ nadzorczy upomniał Przedsiębiorcę za naruszenie przepisów art. 13 i 14 RODO.

Przedsiębiorca skierował do WSA skargę na decyzję Prezesa Urzędu Ochrony Danych Osobowych, która wyrokiem z 19.03.2024 r. została oddalona.

Sygnatura sprawy: DS.523.6678.2022

MECHANIZM OCENY WDRAŻANIA DOROBKU SCHENGEN: PRZYSZŁA KOLEJ NA POLSKĘ, WIĘC I NA UODO

Instytucje publiczne, w tym Prezes Urzędu Ochrony Danych Osobowych przechodziły w kwietniu 2024 r. cykliczną ocenę tego, jak wdrożyły i stosują ochronę danych osobowych w ramach dorobku Schengen.

Strefa Schengen jest jednym z najważniejszych osiągnięć Unii Europejskiej. Dzięki niej ludzie mogą podróżować bez kontroli na granicach wewnętrznych, a obrót towarami i usługami jest łatwiejszy. Współpraca w ramach Schengen rozpoczęła się 14 czerwca 1985 r. wraz z podpisaniem „układu z Schengen" przez pięć państw. UE cały czas pracuje nad takim funkcjonowaniem obszaru bez kontroli na granicach wewnętrznych, który zwiększałby poczucie wzajemnego zaufania między państwami członkowskimi. Musi przy tym uwzględniać nową rzeczywistość i wyzwania odmienne od tych sprzed 40 lat.

Na system Strefy Schengen składają się nie tylko środki na granicach zewnętrznych i środki wyrównawcze (wspólna polityka wizowa, współpraca policyjna, polityka dotycząca powrotów i System Informacyjny Schengen). Równie ważny jest solidny mechanizm oceny i monitorowania, dotyczący ochrony danych osobowych[1] i poszanowania innych praw podstawowych.

System mechanizmu oceny Schengen, któremu w tym roku podlega Polska, zbudowany jest tak, by wymogi Strefy spełniali wszyscy partnerzy. Niedociągnięcia w jednym państwie członkowskim mogą mieć wpływ na wszystkie pozostałe państwa, a w konsekwencji – stwarzać zagrożenie dla całej strefy Schengen.

Unia Europejska osiąga to przy pomocy bezstronnych i obiektywnych ocen, które umożliwią zidentyfikowanie niedociągnięć w zakresie praktycznego stosowania przepisów.

Zgodnie z rozporządzeniem 2022/922[2] za organizację procesu odpowiada Komisja Europejska. To ona informuje o wynikach ocen Parlament Europejski i parlamenty narodowe.

Komisja przeprowadza oceny wspólnie z ekspertami z państw członkowskich i przy wsparciu ze strony organów i jednostek organizacyjnych Unii (zgodnie z art. 70 TFUE). Właśnie to partnerskie podejście czyni ocenę skuteczną i wzmacnia wzajemne zaufanie.

4 NARUSZENIA I KONTROLE

Eksperci z państw członkowskich sprawdzają czynności osób na równorzędnych stanowiskach, wskazując rozwiązania i wzywają do podejmowania działań, jeśli państwo członkowskie ich nie wdraża. Ponadto w proces podejmowania decyzji włączona jest Rada UE, która przyjmuje zalecenia na wniosek Komisji.

fot. pixabay

[1]Głównymi aktami ustawodawczymi mającymi zastosowanie w dziedzinie ochrony danych osobowych, są ogólne rozporządzenie o ochronie danych oraz dyrektywa o ochronie danych w sprawach karnych w połączeniu ze szczegółowymi przepisami dotyczącymi ochrony danych zawartymi w dorobku prawnym Schengen dotyczącym Systemu Informacyjnego Schengen (SIS) i Wizowego Systemu Informacyjnego (VIS).

[2] Rozporządzenie Rady (UE) 2022/922 z dnia 9 czerwca 2022 r. w sprawie ustanowienia i funkcjonowania mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz w sprawie uchylenia rozporządzenia (UE) nr 1053/2013, Dz.U. UE L 160 z 15.6.2022, str. 1—27

DZIECI POD CYFROWĄ OPIEKĄ: GEOLOKALIZACJA W SŁUŻBIE RODZICIELSKIEJ CZUJNOŚCI?

Czy i z jakich urządzeń informujących o miejscu pobytu dziecka korzystać? Jak działają i jakie ryzyka trzeba wziąć pod uwagę?

W dobie cyfrowej transformacji, kiedy technologia coraz bardziej przenika codzienne życie, nieuniknione stało się jej wykorzystanie w kontekście rodzicielstwa. Jednym z aspektów, który wzbudza wiele kontrowersji, jest geolokalizacja i użycie GPS oraz aplikacji do kontroli rodzicielskiej w celu monitorowania miejsca pobytu dzieci.

Choć niewątpliwie wykorzystanie tych narzędzi wynika z troski o bezpieczeństwo, stawia jednak przed rodzicami szereg pytań dotyczących prywatności, zaufania, a także technicznych i prawnych aspektów ich stosowania. Kluczowe więc staje się zrozumienie, jak dokładnie działa technologia GPS, w jaki sposób aplikacje do monitorowania przetwarzają dane, a także jakie są możliwości, ale i zagrożenia wynikające ze stosowania technologii do kontroli rodzicielskiej.

Co to jest geolokalizacja

Geolokalizacja polega na ustaleniu informacji o położeniu geograficznym urządzenia, m.in. za pomocą systemu GPS (Global Positioning System). GPS to system nawigacji satelitarnej umożliwiający określenie pozycji obiektu. Działa 24 godziny na dobę, w każdych warunkach pogodowych. Wykorzystuje sieć co najmniej 24 satelitów krążących wokół Ziemi. Każdy z nich wysyła informacje o swojej pozycji i dokładnym czasie. Odbiornik GPS, analizując dane z kilku satelitów, jest w stanie określić swoją dokładną lokalizację.

Właśnie to rozwiązanie umożliwia rodzicom w czasie rzeczywistym śledzenie, gdzie są ich dzieci, czy dotarły bezpiecznie do szkoły, czy wróciły do domu.

Narzędzia dla rodziców

Na rynku dostępnych jest wiele różnych rodzajów aplikacji tego typu. Wiele jest też rozwiązań oferujących kompleksową kontrolę rodzicielską. Narzędzia te różnią się między sobą zakresem funkcji,

stopniem zaawansowania i sposobem, w jaki integrują się z codziennymi aktywnościami dzieci i rodziców.

Niektóre oferują nie tylko funkcje śledzenia lokalizacji, ale również możliwość monitorowania aktywności dziecka w internecie, ograniczania czasu spędzanego przed ekranem, czy blokowania dostępu do nieodpowiednich treści. Mają one na celu nie tylko ochronę przed zagrożeniami w sieci, ale również wspieranie zdrowych nawyków cyfrowych.

Wbudowane w smartfony systemy kontroli rodzicielskiej

Wiele współczesnych smartfonów ma już wbudowane funkcje kontroli rodzicielskiej. Producenci takich urządzeń coraz częściej wprowadzają też możliwość monitorowania lokalizacji, dając rodzicom narzędzie do sprawdzania, gdzie ich dzieci spędzają czas.

Lokalizator GPS dla dziecka

Lokalizatory GPS dla dzieci dostępne są w różnych formach – od urządzeń do noszenia, przez zegarki, po aplikacje na smartfony. Oferują one funkcje takie jak strefy bezpieczeństwa, które powiadamiają rodziców, gdy dziecko opuści zdefiniowany bezpieczny obszar, czy przyciski SOS, pozwalające na szybki kontakt w sytuacji zagrożenia.

Możliwości i zagrożenia

GPS wymaga odpowiedzialnego i przemyślanego użycia, dlatego tak ważne jest, aby równoważyć troskę o bezpieczeństwo z poszanowaniem prywatności i autonomii dziecka, a także zwrócić uwagę, czy wybrane rozwiązanie jest zgodne z obowiązującymi przepisami o ochronie danych osobowych.

- Dane lokalizacyjne, jeśli nie są odpowiednio chronione, mogą stać się celem dla cyberprzestępców.
- Powiązanie danych lokalizacyjnych z ich konkretnym użytkownikiem, jakie następuje dzięki tym rodzicielskim aplikacjom, może być ryzykowne. Codzienne wzorce, takie jak trasa, którą porusza się dziecko, mogą nieświadomie zdradzić miejsce jego zamieszkania czy adres szkoły. Anonimizacja danych, w praktyce nie taka prosta, może tu nie wystarczyć.
- Dzieci nie mogą być przedmiotem nadmiernego nadzoru, gdyż może to naruszać ich prywatność (prawo do prywatności przysługuje także dzieciom). Efektem będzie ograniczanie poczucia niezależności dziecka i zaufania w relacji z rodzicami.

5 NOWE TECHNOLOGIE

Jak bezpiecznie chronić dziecko?

Przy wyborze odpowiedniego i bezpiecznego rozwiązania GPS do śledzenia lokalizacji dziecka warto zwrócić uwagę na kilka kwestii:

1. Sprawdzenie zgodności z przepisami o ochronie danych

Choć wydaje się to żmudne, naprawdę trzeba przeczytać politykę prywatności dostawcy i ustalić, jakie dane są zbierane, jak są używane, jak długo są przechowywane i kto ma do nich dostęp. Przed zezwoleniem na dostęp do lokalizacji, należy dokładnie sprawdzić, jakie uprawnienia są przez nią wymagane w trakcie instalacji i użytkowania. Czy wszystkie z nich są rzeczywiście niezbędne dla jej właściwego działania?

2. Wybór zaufanego producenta

Warto wybierać produkty i usługi od renomowanych producentów, którzy mają pozytywne recenzje i są znani z przestrzegania przepisów o ochronie danych. Warto upewnić się, że dostawca stosuje silne mechanizmy szyfrowania danych oraz inne środki bezpieczeństwa, aby chronić dane lokalizacyjne przed nieuprawnionym dostępem.

3. Wiek i zgoda dziecka

Ważne jest, aby rozmawiać z dzieckiem na temat używania takich technologii, informować je o powodach monitorowania i uzyskać jego zgodę. Wspólne ustalenie zasad korzystania z urządzenia może pomóc w budowaniu zaufania.

4. Regularne przeglądy i aktualizacje

Trzeba sprawdzać, czy urządzenie lub aplikacja regularnie otrzymuje aktualizacje oprogramowania, które poprawiają ich bezpieczeństwo. Należy też regularnie przeglądać ustawienia prywatności i bezpieczeństwa urządzenia lub aplikacji, aby upewnić się, że są one aktualne i adekwatne do zmieniających się potrzeb i okoliczności.

Wybór odpowiedniego rozwiązania GPS do śledzenia dziecka powinien być zawsze wynikiem świadomej decyzji, uwzględniającej zarówno potrzeby rodziców/opiekunów, jak i prawo dziecka do prywatności.

5 NOWE TECHNOLOGIE

Włączenie dziecka w proces decyzyjny i regularne rozmowy o bezpiecznym korzystaniu z technologii mogą również pomóc w kształtowaniu świadomości na temat ochrony danych i prywatności.

Przetwarzanie danych geolokalizacyjnych ma szczególne znaczenie z punktu widzenia danych osobowych dziecka. Nieodpowiednie podejście do przekazywania informacji przez osoby zarządzające tymi danymi, jak również przez rodziców, może prowadzić do sytuacji, w której dzieci od najmłodszych lat przyzwyczajają się do ciągłego monitorowania. To z kolei może sprawić, że w przyszłości będą one traktować stałe śledzenie jako normalny aspekt życia, nie odbierając go jako naruszenie prywatności.

fot. pixabay

SZTUCZNA INTELIGENCJA: WŁOSKI ORGAN OCHRONY DANYCH WSZCZYNA POSTĘPOWANIE W SPRAWIE "SORA" OPENAI

OpenAI została poproszona o dostarczenie informacji na temat algorytmu, który tworzy krótkie filmy na podstawie instrukcji tekstowych.

Włoski organ ochrony danych wszczął dochodzenie przeciwko OpenAI, amerykańskiej spółce, która w ostatnich tygodniach ogłosiła wprowadzenie na rynek nowego modelu sztucznej inteligencji "Sora". Według zapowiedzi jest on w stanie tworzyć dynamiczne, realistyczne i kreatywne sceny na podstawie krótkich instrukcji tekstowych.

Biorąc pod uwagę możliwe konsekwencje, jakie usługa "Sora" może mieć dla przetwarzania danych osobowych użytkowników w Unii Europejskiej, a w szczególności we Włoszech, włoski organ poprosił OpenAI o przedstawienie szeregu wyjaśnień.

Firma będzie musiała wyjaśnić w ciągu 20 dni, czy nowy model AI jest już dostępny publicznie i czy jest lub będzie oferowany użytkownikom w Unii Europejskiej. OpenAI będzie również musiało wytłumaczyć organowi ochrony danych szereg kwestii, takich jak:

• w jaki sposób algorytm jest szkolony;
• jakie dane są gromadzone i przetwarzane w celu szkolenia algorytmu, w szczególności czy są to dane osobowe;
• czy gromadzone są szczególne kategorie danych (przekonania religijne lub światopoglądowe, poglądy polityczne, dane genetyczne, dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej danej osoby);
• i jakie źródła są wykorzystywane.

W przypadku, gdy usługa jest lub będzie oferowana użytkownikom znajdującym się w UE, organ ochrony danych zwrócił się do OpenAI o stwierdzenie, czy przewidziane metody informowania użytkowników i osób niebędących użytkownikami o procedurach przetwarzania danych i podstawach prawnych tego przetwarzania są zgodne z RODO.

Źródło: komunikat włoskiego organu nadzorczego

SKOORDYNOWANE DZIAŁANIE EROD W ZAKRESIE EGZEKWOWANIA PRAWA: PRAWO DOSTĘPU DO DANYCH OSOBOWYCH

Trzecim skoordynowanym działaniem Europejskiej Rady Ochrony Danych (EROD) będzie w 2025 r. wdrażanie prawa dostępu do danych osobowych.

Przez cały rok zajmować się tym będzie 31 organów ochrony danych, w tym siedem niemieckich na szczeblu krajowym.

Podczas sesji plenarnej w październiku 2023 r. EROD wybrała prawo dostępu jako temat swojego trzeciego skoordynowanego działania w zakresie egzekwowania prawa (CEF) na rok 2024. Stanowi ono sedno ochrony danych i jest tematem dużej liczby skarg do organów ochrony danych. W szczególności umożliwia ono osobom fizycznym sprawdzenie, czy ich dane osobowe są przetwarzane przez organizacje w sposób zgodny z przepisami. Pozwala też na korzystanie z innych praw do ochrony danych, takich jak prawo do sprostowania i usunięcia danych.

W 2023 r. EROD przyjęła „Wytyczne dotyczące praw osób, których dane dotyczą - prawo dostępu”, aby pomóc organizacjom w odpowiadaniu na wnioski o dostęp do danych składane przez osoby fizyczne zgodnie z wymogami określonymi w RODO.

Aby ocenić, w jaki sposób organizacje przestrzegają prawa dostępu w praktyce, uczestniczące organy ochrony danych wdrożą CEF na wiele sposobów:

- organizacje otrzymają kwestionariusze, które pomogą w ustaleniu faktów lub określeniu, czy postępowanie przygotowawcze jest uzasadnione;
- rozpoczęcie postępowanie przygotowawczego; i/lub
- monitorowanie trwających postępowań przygotowawczych.

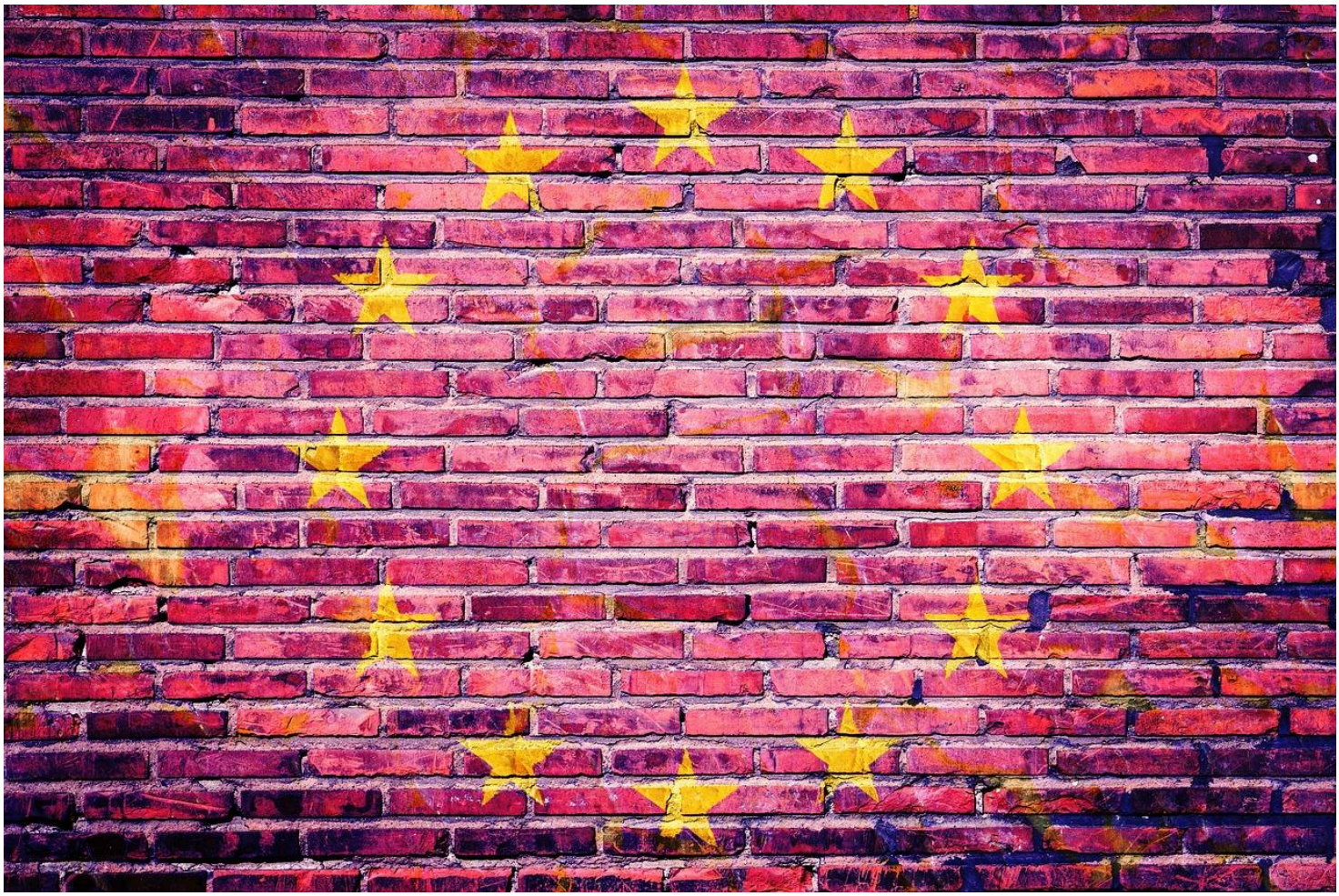
Wyniki wspólnej inicjatywy zostaną przeanalizowane w skoordynowany sposób, a organy ochrony danych podejmą decyzję o ewentualnym dalszym nadzorze i działaniach w zakresie egzekwowania prawa. Wszystkie wyniki zostaną zebrane, co zapewni głębszy wgląd w temat i umożliwi ukierunkowane działania następcze na szczeblu UE. Po zakończeniu działań EROD opublikuje sprawozdanie z wyników tej analizy.

6 SPRAWY MIĘDZYNARODOWE

Ta seria działań jest trzecią inicjatywą w ramach skoordynowanych ram egzekwowania prawa (CEF), których celem jest usprawnienie egzekwowania prawa i współpracy między organami ochrony danych.

Poprzednie skoordynowane działania dotyczyły korzystania z usług w chmurze przez sektor publiczny w 2022 r. oraz wyznaczania i pozycji inspektorów ochrony danych w 2023 r.

Źródło: komunikat EROD



fot. pixabay

KORZYSTANIE PRZEZ KOMISJĘ EUROPEJSKĄ Z PLATFORMY MICROSOFT 365 NARUSZA PRZEPISY O OCHRONIE DANYCH INSTYTUCJI I ORGANÓW UE

Komisja Europejska (Komisja) naruszyła kilka kluczowych zasad ochrony danych podczas korzystania z platformy Microsoft 365 – stwierdził EIOD w wyniku postępowania wyjaśniającego. W decyzji EIOD nałożył na Komisję środki naprawcze.

EIOD stwierdził, że Komisja naruszyła kilka przepisów rozporządzenia (UE) 2018/1725, unijnego prawa o ochronie danych instytucji, organów i jednostek organizacyjnych UE (EUI), w tym przepisy dotyczące przekazywania danych osobowych poza UE/Europejski Obszar Gospodarczy (EOG).

W szczególności Komisja nie zapewniła odpowiednich zabezpieczeń w celu zagwarantowania, że dane osobowe przekazywane poza UE/EOG będą miały zapewniony zasadniczo równoważny poziom ochrony, jaki jest gwarantowany w UE/EOG.

Ponadto w umowie z Microsoftem Komisja nie określiła w wystarczający sposób, jakie rodzaje danych osobowych mają być gromadzone i do jakich wyraźnych i określonych celów podczas korzystania z Microsoft 365. Naruszenia Komisji jako administratora danych dotyczą również przetwarzania danych, w tym przekazywania danych osobowych, dokonywanego w jej imieniu.

Europejski inspektor ochrony danych Wojciech Wiewiórowski powiedział: "Obowiązkiem instytucji, organów, urzędów i agencji UE jest dopilnowanie, aby wszelkiemu przetwarzaniu danych osobowych poza UE/EOG i na jej terytorium, w tym w kontekście usług w chmurze, towarzyszyły solidne zabezpieczenia i środki ochrony danych. Jest to niezbędne do zapewnienia ochrony informacji osób fizycznych, zgodnie z wymogami rozporządzenia (UE) 2018/1725, za każdym razem, gdy ich dane są przetwarzane przez instytucję UE lub w jej imieniu".

W związku z tym EIOD postanowił nakazać Komisji, ze skutkiem od 9 grudnia 2024 r., zawieszenie wszystkich przepływów danych wynikających z korzystania z Microsoft 365 do Microsoft oraz do jego podmiotów powiązanych i podwykonawców przetwarzania znajdujących się w państwach spoza UE/EOG nieobjętych decyzją stwierdzającą odpowiedni stopień ochrony.

Inspektor postanowił również nakazać Komisji dostosowanie operacji przetwarzania danych

wynikających z korzystania z platformy Microsoft 365 do rozporządzenia (UE) 2018/1725. Komisja musi wykazać zgodność z obydwoma nakazami do dnia 9 grudnia 2024 r.

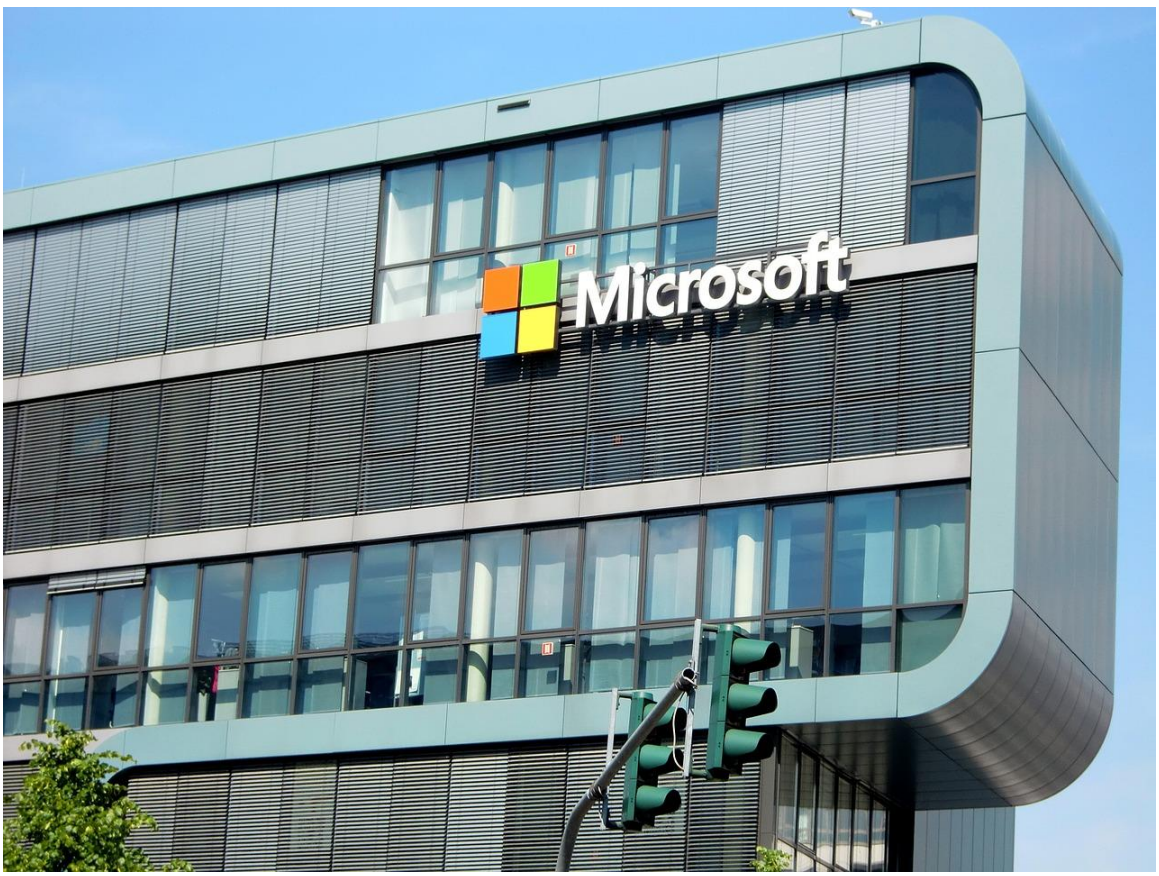
EIOD uważa, że nałożone przez niego środki naprawcze są odpowiednie, niezbędne i proporcjonalne w świetle wagi i czasu trwania stwierdzonych naruszeń.

Wiele ze stwierdzonych naruszeń dotyczy wszystkich operacji przetwarzania prowadzonych przez Komisję lub w jej imieniu przy użyciu platformy Microsoft 365 i ma wpływ na dużą liczbę osób fizycznych.

EIOD bierze również pod uwagę potrzebę niezagrażania zdolności Komisji do wykonywania jej zadań w interesie publicznym lub do sprawowania władzy publicznej powierzonej Komisji, a także potrzebę zapewnienia Komisji odpowiedniego czasu na wdrożenie przewidywanego zawieszenia odpowiednich przepływów danych oraz na zapewnienie zgodności przetwarzania danych z rozporządzeniem (UE) 2018/1725.

Środki nałożone przez EIOD w decyzji z dnia 8 marca 2024 r. pozostają bez uszczerbku dla wszelkich innych lub dalszych działań, które może podjąć EIOD.

Źródło: informacja prasowa EIOD



fot. pixabay

UE WPROWADZA NOWE PRZEPISY DOTYCZĄCE PRZEJRZYSTOŚCI I TARGETOWANIA REKLAMY POLITYCZNEJ

Rada przyjęła 11 marca 2024 r. nowe rozporządzenie dotyczące przejrzystości i targetowania reklamy politycznej, które pomoże przeciwdziałać manipulowaniu informacjami i obcym ingerencjom w wybory.

Dzięki niemu obywatelom ma być łatwiej:

• rozpoznawać reklamę polityczną;
• rozumieć, kto za nią stoi;
• i czy jest ona reklamą targetowaną,
a tym samym dokonywać świadomych wyborów. Sprawi również, że działalność w zakresie reklamy politycznej odbywać się będzie z pełnym poszanowaniem prawa do prywatności i że chronione będą wolność opinii i wolność wypowiedzi.

Główne elementy nowego rozporządzenia
Nowe przepisy dotyczą przejrzystości i targetowania reklamy politycznej w związku z wyborami, referendum lub procesem legislacyjnym na szczeblu UE lub w państwie członkowskim. Nie podlega im treść reklam politycznych ani inne aspekty reklamy politycznej – takie jak prowadzenie kampanii politycznych – które nadal regulowane są szczególnymi przepisami krajowymi państw członkowskich.

Nie mają także wpływu na treść podlegająca odpowiedzialności redakcyjnej ani na poglądy wyrażane we własnym imieniu.

Zgodnie z przepisami:

• Reklamom politycznym muszą towarzyszyć oznakowania i łatwe do odnalezienia ogłoszenia gwarantujące przejrzystość. Muszą one wyraźnie wskazywać, że chodzi właśnie o reklamę polityczną i zawierać pewne kluczowe informacje, w tym na temat sponsora, wyborów lub referendów, do których się odnoszą, opłat oraz wszelkich zastosowanych technik targetowania.
• Targetowanie reklamy politycznej w internecie będzie dozwolone wyłącznie na ściśle określonych warunkach. Dane muszą być gromadzone od osoby, której dane dotyczą, i mogą

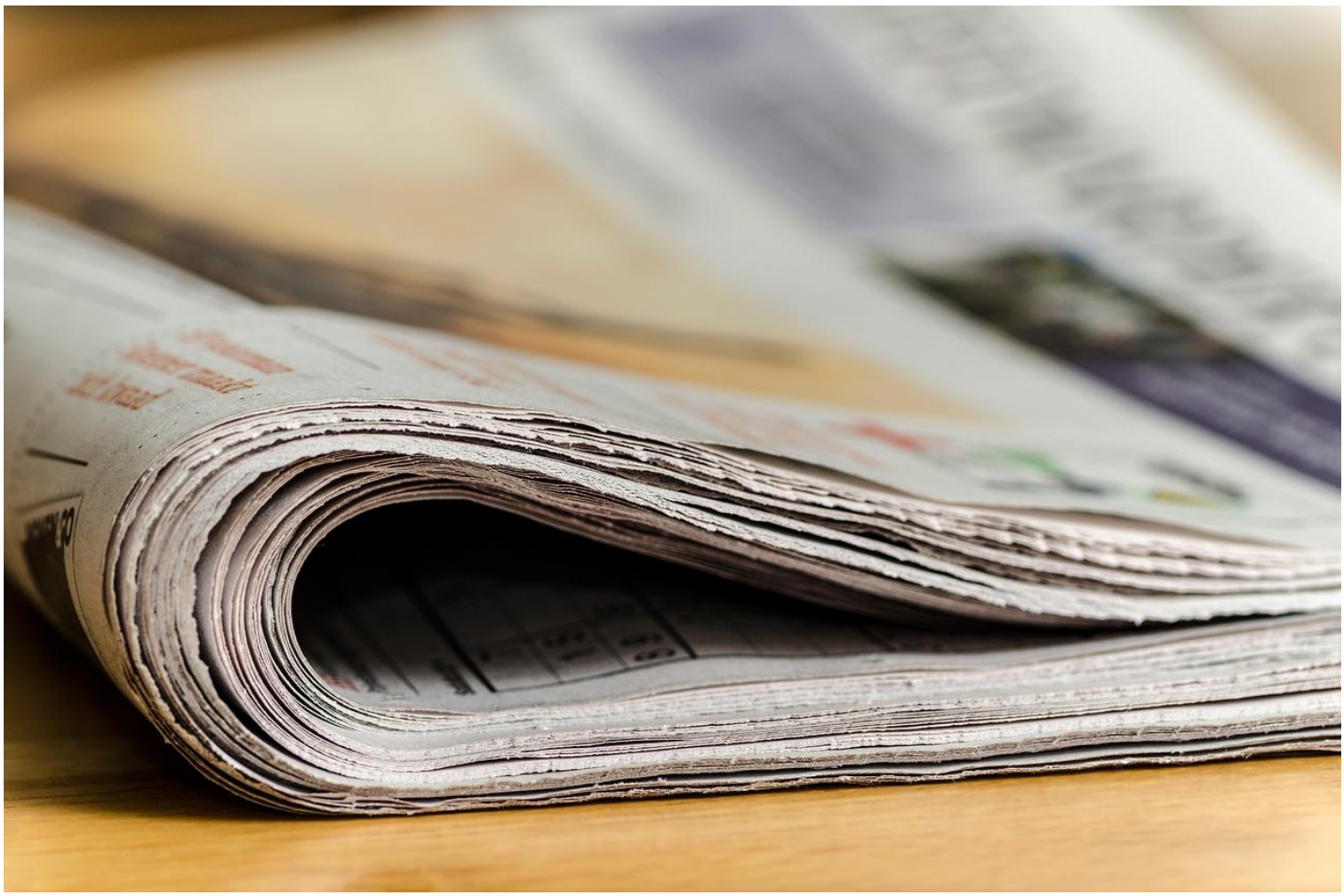
być wykorzystywane dopiero po udzieleniu przez nią wyraźnej, specjalnej zgody na ich wykorzystanie do celów reklamy politycznej. Szczególne kategorie danych osobowych, takie jak dane ujawniające pochodzenie rasowe lub etniczne lub poglądy polityczne, nie mogą być wykorzystywane do profilowania.

• Aby zapobiec obcym ingerencjom, wprowadzony zostanie zakaz świadczenia usług reklamowych sponsorom z państw trzecich w okresie trzech miesięcy przed wyborami lub referendum.

Co dalej?

Rozporządzenie zostanie teraz podpisane, po czym ukaże się w Dzienniku Urzędowym UE i wejdzie w życie 20 dni później. Większość jego przepisów zacznie obowiązywać 18 miesięcy po wejściu w życie, tj. jesienią 2025 r.

Źródło: informacja prasowa Rady UE i Rady Europejskiej



fot. pixabay

AKT W SPRAWIE SZTUCZNEJ INTELIGENCJI – POSŁOWIE PRZYJMUJĄ PRZEŁOMOWE PRZEPISY

13 marca 2024 r. Parlament Europejski zatwierdził akt w sprawie sztucznej inteligencji, który zapewnia bezpieczeństwo i przestrzeganie praw podstawowych, a jednocześnie wspiera innowacje.

W grudniu 2023 r., po negocjacjach z państwami członkowskimi, Parlament przyjął rozporządzenie w sprawie SI. 523 posłów głosowało za, 46 przeciw, a 49 posłów wstrzymało się od głosu.

Rozporządzenie ma chronić prawa podstawowe, demokrację, praworządność i środowisko przed systemem sztucznej inteligencji wysokiego ryzyka. Jednocześnie ma wspierać innowacje i sprawić, że Europa będzie liderem w dziedzinie AI. Rozporządzenie określa obowiązki w stosunku do sztucznej inteligencji w oparciu o potencjalne ryzyko z nią związane i jej możliwe skutki.

Zakaz pewnych zastosowań

Nowe przepisy zakazują pewnych zastosowań sztucznej inteligencji, które zagrażają prawom obywateli. Są to między innymi systemy kategoryzacji biometrycznej, które wykorzystują cechy wrażliwe i nieukierunkowane pobieranie wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej, by stworzyć bazy danych służące rozpoznawaniu twarzy.

• Zakazane będą też rozpoznawanie emocji w miejscu pracy i w instytucjach edukacyjnych, klasyfikacja punktowa obywateli, prognozowanie przestępczości (wyłącznie na podstawie profilowania osoby lub oceny jej cech).
• Nie będzie też dozwolona sztuczna inteligencja, która manipuluje zachowaniem ludzi lub wykorzystuje ich słabości.

Wyjątki dla organów ścigania

Organom ścigania z reguły nie wolno korzystać z systemów identyfikacji biometrycznej. Są jednak pewne wyjątki, które wąsko zdefiniowano na zamkniętej liście. Organy te mogą wykorzystywać systemy identyfikacji biometrycznej w czasie rzeczywistym tylko wtedy, gdy spełniły ściśle określone warunki. Na przykład mogą je stosować w określonym czasie i w określonym położeniu geograficznym. Muszą też posiadać specjalne zezwolenie sądowe lub administracyjne. Mogą je

wykorzystywać, by odnaleźć zaginioną osobę lub zapobiegać atakowi terrorystycznemu. Istnieją też tzw. systemy zdalnej identyfikacji biometrycznej post factum. Ich stosowanie wiąże się z wysokim ryzykiem i wymaga zezwolenia sądowego, ponieważ systemy takie wykorzystuje się do wyszukiwania w związku z przestępstwem.

Obowiązki dotyczące systemów wysokiego ryzyka

Szczególne obowiązki określono również dla innych systemów sztucznej inteligencji wysokiego ryzyka. A to dlatego, że stanowią one potencjalne zagrożenie dla zdrowia, bezpieczeństwa, praw podstawowych, środowiska, demokracji czy praworządności. Obszary, w których wykorzystuje się takie systemy, to na przykład infrastruktura krytyczna, edukacja i szkolenie zawodowe, zatrudnienie, podstawowe usługi prywatne i publiczne (np. opieka zdrowotna, bankowość). Opierają się też na nich niektóre systemy organów ścigania. Wykorzystuje się je, by zarządzać migracją i granicami oraz na potrzeby wymiaru sprawiedliwości i procesów demokratycznych (np. by wpływać na wybory).

Takie systemy muszą oceniać i ograniczać ryzyko oraz prowadzić rejestry zdarzeń. Muszą też być przejrzyste i dokładne oraz podlegać kontroli przez człowieka. Dzięki rozporządzeniu obywatele zyskają prawo złożenia skargi dotyczącej systemów SI. Będą także otrzymywać wyjaśnienia decyzji podejmowanych przez systemy sztucznej inteligencji wysokiego ryzyka, które mają wpływ na ich prawa.

Wymogi przejrzystości

Systemy sztucznej inteligencji ogólnego przeznaczenia i modele sztucznej inteligencji ogólnego przeznaczenia, na których oparte są takie systemy, muszą spełniać określone wymogi przejrzystości i być zgodne z unijnym prawem autorskim oraz publikować dokładne zestawienia materiałów użytych podczas trenowania swoich modeli. Najbardziej zaawansowane modele sztucznej inteligencji ogólnego przeznaczenia, które mogą stwarzać ryzyko systemowe, będą musiały spełniać dodatkowe wymagania. Operatorzy SI będą musieli między innymi przeprowadzać oceny modeli, oceniać i ograniczać ryzyko systemowe, zgłaszać incydenty.

Należy też wyraźnie oznaczać nieautentyczne lub zmanipulowane obrazy, treści audio lub wideo, tzw. deepfakes.

Działania wspierające innowacje i MŚP

Należy ustanowić na szczeblu krajowym „piaskownice regulacyjne”, czyli środowisko ułatwiające opracowywanie i testowanie innowacyjnych systemów sztucznej inteligencji przed wprowadzeniem do obrotu, oraz testowanie w warunkach rzeczywistych. Należy też zapewnić MŚP i przedsiębiorstwom typu start-up łatwy dostęp do nich. Dzięki temu będzie można opracowywać

i trenować innowacyjne systemy SI przed wprowadzeniem na rynek.

Kolejne kroki

Rozporządzenie muszą jeszcze ostatecznie zweryfikować prawnicy lingwiści. Ma ono zostać przyjęte przed końcem kadencji (tzw. procedura sprostowania). Rozporządzenie musi też formalnie przyjąć Rada.

Rozporządzenie wejdzie w życie 20 dni po publikacji w Dzienniku Urzędowym, a w pełni obowiązywać będzie 24 miesiące po jego wejściu w życie.

Wyjątki to:

• zakazy niedozwolonych praktyk (będą obowiązywać sześć miesięcy po wejściu rozporządzenia w życie),

• kodeksy postępowania (dziewięć miesięcy po wejściu w życie),

• przepisy o sztucznej inteligencji ogólnego przeznaczenia, w tym dotyczące zarządzania (12 miesięcy po wejściu w życie)

• oraz obowiązki dotyczące systemów wysokiego ryzyka (36 miesięcy po wejściu w życie).

Kontekst

Akt o sztucznej inteligencji stanowi bezpośrednią odpowiedź na propozycje obywateli z Konferencji w sprawie przyszłości Europy (COFE). Chodzi w szczególności o:

• propozycję 12(10) w sprawie zwiększenia konkurencyjności UE w sektorach strategicznych,

• propozycję 33(5) w sprawie bezpiecznego i godnego zaufania społeczeństwa, w tym przeciwdziałania dezinformacji i zapewnienia ostatecznej kontroli przez ludzi,

• wniosek nr 35 w sprawie promowania innowacji cyfrowych (3) przy jednoczesnym zapewnieniu nadzoru ze strony człowieka oraz (8) godnego zaufania i odpowiedzialnego korzystania ze sztucznej inteligencji, ustanawiania zabezpieczeń i zapewniania przejrzystości,

• a także wniosek nr 37 (3) w sprawie wykorzystywania sztucznej inteligencji i narzędzi cyfrowych w celu poprawy dostępu obywateli do informacji, w tym osób niepełnosprawnych.

Źródło: komunikat prasowy Parlamentu Europejskiego

WYROK TSUE W SPRAWIE C-46/23 ÚJPESTI POLGÁRMESTERI HIVATAL

Organ nadzorczy państwa członkowskiego może nakazać usunięcie danych przetwarzanych niezgodnie z prawem, nawet bez żądania osoby, której dane dotyczą. Takie usunięcie może dotyczyć zarówno danych uzyskanych od tej osoby, jak i danych pochodzących z innego źródła.

W 2020 r. urząd miasta Újpest (Węgry) podjął decyzję o udzieleniu pomocy finansowej osobom szczególnie narażonym na skutki pandemii COVID-19. W tym celu zwrócił się do węgierskiego skarbu państwa i do urzędu czwartego okręgu miasta stołecznego Budapeszt o przekazanie danych osobowych niezbędnych do sprawdzenia warunków kwalifikowalności do uzyskania pomocy.

Zawiadomiony w drodze zgłoszenia węgierski organ odpowiedzialny za ochronę danych osobowych („organ nadzorczy") ustalił, że zarówno urząd miasta Újpest, węgierski skarb państwa, jak i organ municypalny naruszyły przepisy RODO. W związku z tym zastosowano kary pieniężne.

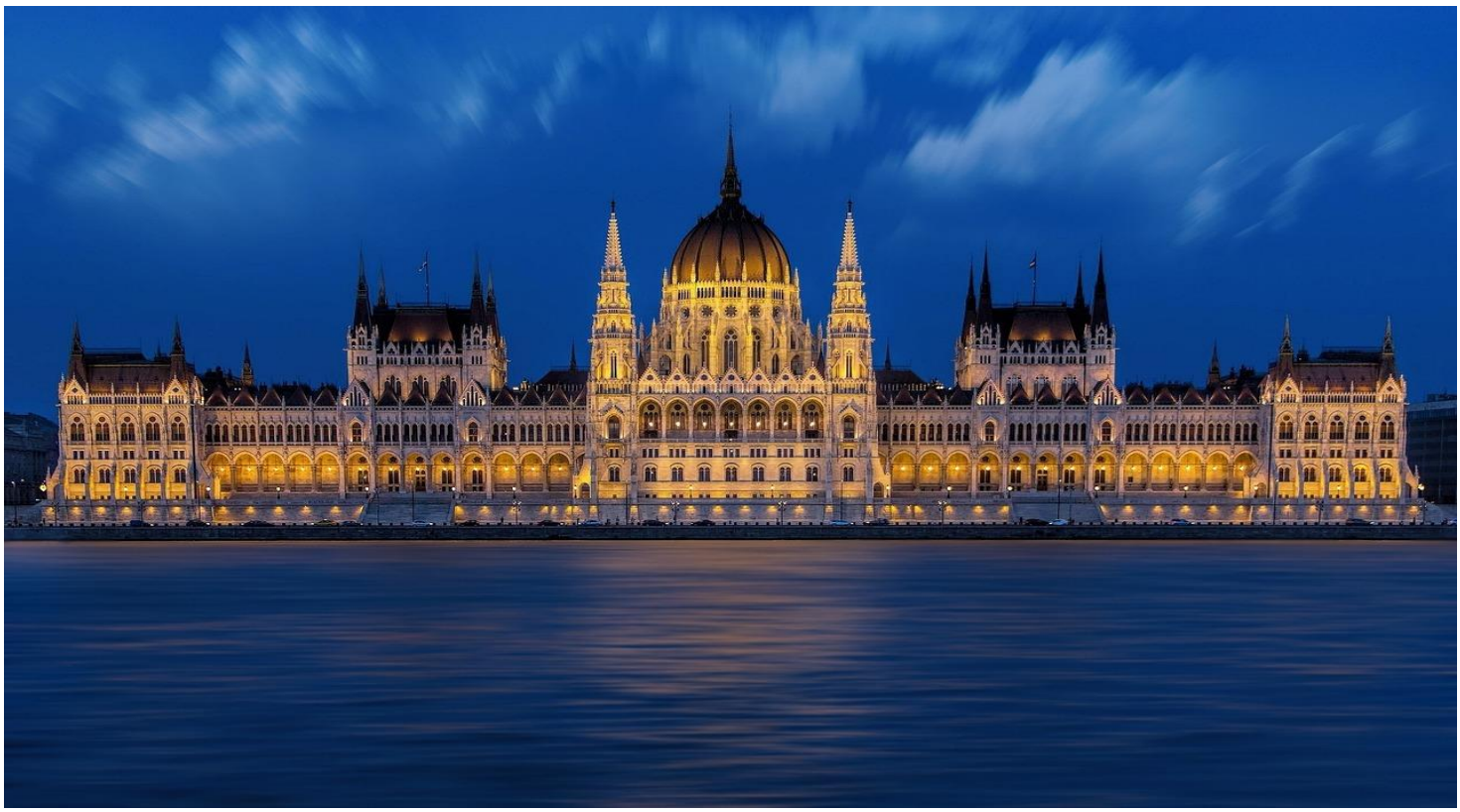
Organ nadzorczy stwierdził, że administracja Újpestu nie poinformowała – w terminie jednego miesiąca – osób, których dane dotyczą, ani o celach wykorzystywania ich danych, ani o ich prawach w dziedzinie ochrony danych. Ponadto organ ten nakazał administracji Újpestu usunięcie danych osób kwalifikujących się do pomocy, które o tę pomoc nie wystąpiły.

Administracja Újpestu kwestionuje tę decyzję przed sądem dla miasta stołecznego Budapeszt, twierdząc, że organ nadzorczy nie jest uprawniony do nakazania usunięcia danych osobowych bez uprzedniego żądania osoby, której dane dotyczą.

Węgierski sąd zwrócił się do Trybunału Sprawiedliwości o dokonanie wykładni RODO. W wyroku Trybunał Sprawiedliwości orzekł, że organ nadzorczy państwa członkowskiego może nakazać z urzędu – tj. nawet bez uprzednio wyrażonego w tym celu żądania osoby, której dane dotyczą – usunięcie danych przetwarzanych niezgodnie z prawem, jeżeli taki środek jest konieczny dla wywiązania się z powierzonego mu zadania polegającego na egzekwowaniu pełnego przestrzegania RODO. Jeżeli organ ten stwierdzi, że przetwarzanie danych nie jest zgodne z RODO, ma obowiązek usunąć stwierdzone naruszenie, nawet bez uprzedniego żądania osoby, której dane dotyczą. Wymóg wyrażenia takiego żądania oznaczałby bowiem, że administrator danych mógłby w razie jego braku, zachować rozpatrywane dane i nadal przetwarzać je w sposób niezgodny z prawem.

Poza tym organ nadzorczy państwa członkowskiego może nakazać usunięcie danych osobowych przetwarzanych niezgodnie z prawem zarówno wtedy, gdy pochodzą one bezpośrednio od osoby, której dotyczą, jak i w przypadku innego źródła pochodzenia.

Źródło: komunikat TSUE



fot. pixabay

WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI W SPRAWIE C-755/21 P KOČNER PRZECIWKO EUROPOL

Europol i państwo członkowskie, w którym wystąpiła szkoda w wyniku niezgodnego z prawem przetwarzania danych w ramach współpracy między tymi podmiotami, ponoszą odpowiedzialność solidarną.

Zainteresowana osoba, która domaga się pełnego naprawienia przez Europol lub dane państwo członkowskie poniesionej przez nią szkody, powinna jedynie wykazać, że przy okazji współpracy między tymi dwoma podmiotami miało miejsce niezgodne z prawem przetwarzanie danych, w wyniku którego poniosła ona szkodę.

Nie jest wymagane, by osoba ta ustaliła, któremu z tych dwóch podmiotów można przypisać owo niezgodne z prawem przetwarzanie danych.

Po zabójstwie na Słowacji 21 lutego 2018 r. słowackiego dziennikarza i jego narzeczonej – Jána Kuciaka i Martiny Kušnírovej – słowackie władze wszczęły szeroko zakrojone dochodzenie. Na ich wniosek Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) pobrała dane zapisane w dwóch telefonach komórkowych, które należały do Mariana Kočnera. Europol przekazał wspomnianym organom sporządzone przez siebie sprawozdania kryminalistyczne oraz twardy dysk zawierający zakodowane dane pobrane z tych telefonów. W maju 2019 r. słowacka prasa opublikowała informacje dotyczące M. Kočnera pobrane z jego telefonów komórkowych, w szczególności transkrypcje prowadzonej przez niego wymiany wiadomości o charakterze intymnym. Ponadto w jednym ze sprawozdań Europol wskazał, że M. Kočner przebywa w areszcie od 2018 r. w związku z podejrzeniem popełnienia przestępstwa finansowego oraz że jego nazwisko jest między innymi bezpośrednio związane z tzw. „listami członków mafii" i „Panama Papers".

M. Kočner wystąpił do Sądu Unii Europejskiej z żądaniem zasądzenia na jego rzecz kwoty 100 000 euro tytułem zadośćuczynienia za krzywdę, jakiej miał doznać w wyniku niezgodnego z prawem przetwarzania jego danych. W wyroku z dnia 29 września 2021 r. Sąd oddalił tę skargę. Orzekł po pierwsze, że M. Kočner nie przedstawił dowodu istnienia związku przyczynowego między krzywdą a działaniem Europolu, a po drugie, że nie dowiódł, iż tzw. „listy członków mafii" zostały sporządzone i były prowadzone przez Europol. M. Kočner wniósł odwołanie do Trybunału Sprawiedliwości.

W wyroku Trybunał orzekł, iż prawo Unii ustanawia reżim odpowiedzialności solidarnej Europolu i zainteresowanego państwa członkowskiego, w którym wystąpiła szkoda powstała wskutek niezgodnego z prawem przetwarzania danych w ramach współpracy między tymi podmiotami.

• Na pierwszym etapie odpowiedzialność solidarna Europolu lub zainteresowanego państwa członkowskiego może być dochodzona odpowiednio przed Trybunałem Sprawiedliwości Unii Europejskiej lub przed właściwym sądem krajowym.
• W stosownym przypadku etap drugi może zostać przeprowadzony przed zarządem Europolu celem ustalenia „ostatecznej odpowiedzialności" Europolu lub zainteresowanego państwa członkowskiego za odszkodowanie przyznane pokrzywdzonej osobie fizycznej.

Aby owa odpowiedzialność solidarna mogła zostać stwierdzona w ramach etapu pierwszego, zainteresowana osoba fizyczna powinna wykazać jedynie, że w ramach współpracy między Europolem a danym państwem członkowskim miało miejsce niezgodne z prawem przetwarzanie danych, w wyniku którego poniosła ona szkodę. W przeciwieństwie do tego, co orzekł Sąd, Trybunał stwierdził, że nie jest wymagane, by osoba ta ustaliła ponadto, któremu z tych dwóch podmiotów można przypisać owo niezgodne z prawem przetwarzanie danych. W konsekwencji Trybunał uchylił w tym zakresie wyrok Sądu.

Wydając ostateczne rozstrzygnięcie w przedmiocie tego sporu, Trybunał orzekł, że niezgodne z prawem przetwarzanie danych, które polegało na ujawnieniu nieupoważnionym osobom danych dotyczących konwersacji o charakterze intymnym między M. Kočnerem a jego przyjaciółką, doprowadziło do podania tych danych przez słowacką prasę do wiadomości publicznej. Trybunał uznał, że takie niezgodne z prawem przetwarzanie danych naruszyło prawo M. Kočnera do poszanowania jego życia prywatnego i rodzinnego, oraz prawo do poszanowania komunikowania się, jak również ugodziło w jego dobre imię i reputację. Tytułem zadośćuczynienia za doznaną krzywdę Trybunał zasądził na rzecz M. Kočnera kwotę 2 000 euro.

Źródło: komunikat TSUE

WYROK ETPCZ W SPRAWIE MOLDOVAN PRZECIWKO UKRAINIE (NR 62020/14)

Sprawa dotyczyła odrzucenia powództwa cywilnego Oleksandra Moldovana o sądowe uznanie ojcostwa. Sądy oddaliły jego wniosek zasadniczo dlatego, że nie udało mu się udowodnić, że jego matka i zmarły domniemany ojciec kiedykolwiek żyli w konkubinacie lub że ten ostatni kiedykolwiek uznał jego ojcostwo w jakikolwiek sposób.

Skarżący, Oleksandr Volodymyrovych Moldovan, jest obywatelem Ukrainy, który urodził się w 1993 roku i mieszka we wsi Chornivka w obwodzie czerniowieckim (Ukraina). Pan Moldovan urodził się poza związkiem małżeńskim. Osoba, którą uważał za swojego ojca, zmarła w 2012 roku.

Powołując się na Artykuł 8 (prawo do poszanowania życia prywatnego i rodzinnego) Europejskiej Konwencji Praw Człowieka, Mołdawianin skarży się, że sądy odmówiły uwzględnienia dowodów DNA, nalegając zamiast tego na stosowanie przestarzałych przepisów wymagających dowodu konkubinatu i innych okoliczności "społecznych".

Trybunał uznał, że doszło do naruszenia art. 8 Europejskiej Konwencji Praw Człowieka. Przyznane zostało zadośćuczynienie:

- szkoda niemajątkowa: 4 500 euro;
- koszty i wydatki: 500 euro.

Źródło: Wyrok Europejskiego Trybunału Praw Człowieka

WYROK ETPCZ W SPRAWIE VAGDALT PRZECIWKO WĘGROM (NR 9525/19)

Sprawa dotyczyła niemożności uznania skarżącego za ojca jego córki.

Skarżący, István Vagdalt, jest obywatelem węgierskim urodzonym w 1961 roku i mieszkającym w Répcelak (Węgry).

Mąż matki został zarejestrowany jako ojciec dziecka, ale test DNA wykazał, że skarżący jest biologicznym ojcem dziecka. Władze krajowe uznały, że postępowanie mające na celu uregulowanie statusu rodzinnego dziecka leżało w najlepszym interesie dziecka, ale nie zostało zakończone z powodu błędów popełnionych przez władze krajowe. W konsekwencji, wszelkie kwestie związane z ojcostwem uległy przedawnieniu, pozbawiając skarżącego możliwości nawiązania relacji prawnych z córką.

Powołując się na art. 8 (prawo do poszanowania życia prywatnego i rodzinnego) Europejskiej Konwencji Praw Człowieka, skarżący zarzuca, że nie był w stanie uzyskać uznania swojego ojcostwa, ponieważ władze krajowe były nieskuteczne w prowadzeniu postępowania.

Trybunał uznał, że doszło do naruszenia art. 8 Europejskiej Konwencji Praw Człowieka. Przyznane zostało zadośćuczynienie:

- szkoda niemajątkowa: 10 000 euro;
- koszty i wydatki: 10 000 euro.

Źródło: Wyrok Europejskiego Trybunału Praw Człowieka

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl