URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 11/11/24

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

skuteczna ochrona danych osobowych – jednego z najcenniejszych dziś dóbr – wymaga doskonalenia zarządzania opartego na analizie ryzyka. Nic nam po tym, gdy po fakcie wskażemy winnych zaniedbań, bo szkód nie da się już naprawić.

RODO każe nam stawiać na prewencję i analizę ryzyka. W naszej pracy kładziemy na to duży nacisk. Aby zaś wiedza o tym, jak należy przeciwdziałać ryzyku dla danych, szerzyła się, konieczna jest rozmowa i odwoływanie się do konkretów. Ba, bez rozmowy znalezienie takich rozwiązań będzie bardzo trudne.

Działania sektorowe

Dlatego 15 listopada 2024 r. wraz ze Społecznym Zespołem Ekspertów przy Prezesie UODO oraz Konfederacją Lewiatan zorganizowaliśmy seminarium „Ochrona zdrowia w zatrudnieniu a RODO". Zebraliśmy na nim problemy, jakie pojawiają się przy przetwarzaniu **informacji o zdrowiu pracowników** (kierowanie na badania z zakresu pracy w związku z kryzysem psychicznym czy aktywizacja osób z niepełnosprawnościami). Pomoże nam to w pracach nad aktualizacją poradnika o danych osobowych w zatrudnieniu.

Podobną sektorową konferencję zorganizowaliśmy 28 listopada wspólnie z ZUS. Poświęcona ona była najważniejszym **zmianom, jakie zaszły w systemie prawnym w 2024**, z perspektywy ochrony danych osobowych. Rozmawialiśmy też o konsekwencjach kolejnej rewolucji, która dokonuje się na naszych oczach: tej związanej ze sztuczną inteligencją.

Debaty eksperckie

O unijnym **Akcie o sztucznej inteligencji** miałem możliwość opowiadać na konferencji w Akademii im. Leona Koźmińskiego w Warszawie „Prawne Wyzwania Technologii Dysruptywnych" (ang. "Legal Challenges of Disruptive Technologies") 7-8 listopada 2024 roku. Zwróciłem uwagę, że nasze zabiegi związane z ochroną danych osobowych dotyczą praw podstawowych obywateli Unii Europejskiej.

Zwróciłem uwagę na fakt, że wiele organizacji, wdrażających systemy AI wysokiego ryzyka, będzie zobowiązanych do przeprowadzenia oceny oddziaływania na prawa podstawowe (ang. FRIA – Fundamental Rights Impact Assessment) celem umożliwienia wczesnego identyfikowania potencjalnych zagrożeń dla praw podstawowych i podjęcia odpowiednich środków w celu ich łagodzenia.

W listopadzie aktywnie uczestniczyliśmy też w wymianie poglądów na temat ochrony danych osobowych na arenie międzynarodowej. To bardzo ważne źródło wiedzy i dobrych praktyk.

18-19 listopada 2024 r. w Brukseli, razem z kilkudziesięciu ekspertami z różnych krajów, uczestniczyłem w 74. spotkaniu Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Technologii, zwanej również Grupą Berlińską. **Dyskutowaliśmy m.in. o neurotechnologii i technologii immersyjnej (rozszerzonej rzeczywistości), rozwiązaniach chmurowych i mechanizmach globalnych sygnałów preferencji opt out i powiązanych technologiach.**

Dane osobowe z perspektywy człowieka

Inną perspektywę na problemy z danymi osobowymi dały nam **spotkania w Katowicach** w ramach akcji „UODO rusza w kraj". Tam też omawialiśmy problemy z zakresu danych osobowych z ekspertami z Uniwersytetu Ekonomicznego w Katowicach na współorganizowanej konferencji naukowej. Mieliśmy też ważne spotkanie z Federacją Uniwersytetów Trzeciego Wieku. To, że dane osobowe postrzegane są różnie przez różne generacje to oczywistość. Osoby, które zakończyły edukację, a nawet aktywność zawodową zanim rewolucja cyfrowa na dobre zmieniła nasze życie, mają do danych inne podejście. Naszym zadaniem jest wspierać ich i wskazywać, jak chronić swoje prawa w gospodarce, w której za towary i usługi płaci się informacjami o sobie (danymi). Podpisaliśmy też z Federacją Uniwersytetów Trzeciego Wieku porozumienie o współpracy.

Nie tylko osoby starsze mogą mieć kłopot w rozumieniu, czym są dane osobowe. Dziennikarze Radia ZET zaalarmowali opinię publiczną, że strażnicy graniczni pozwalają sobie na nieuprawnione zaglądanie do **bazy PESEL**. Wyciągają tak np. dane o znanych osobach. Sprawę prowadzi prokuratura, ale postępowanie trwa bardzo długo. Tymczasem w interesie nas wszystkich jest to, by zakończyło się sprawnie i by wprowadzono odpowiednie zabezpieczenia przed nadużywaniem dostępu do danych w Straży Granicznej. Stąd moja interwencja u Komendanta Głównego Straży Granicznej.

Dane osobowe i prawo

Nasza praca polega też na analizowaniu projektów ustaw pod kątem danych osobowych, a także wyroków europejskich sądów.

Zwrócę tu tylko Państwa uwagę na naszą opinię do projektu ustawy wprowadzającej rejestr psów i kotów. Ma on przeciwdziałać bezdomności zwierząt w ten sposób, że dzięki czipowi zarejestrowanemu w centralnej bazie łatwo będzie można ustalić, kto jest opiekunem zwierzęcia. Projekt nie został jednak odpowiednio zanalizowany pod kątem ochrony danych osobowych. Tymczasem zakłada powstanie bazy danych, w której znajdzie się wiele milionów obywateli z wieloma danymi o nich. To, że takie dane łatwo będzie można pobrać skanując czip psa na spacerze w parku, to najmniejszy problem z tym związany. Opisuję ten projekt, by pokazać, że nie ma dziś takiej dziedziny, w której dane osobowe nie miałyby znaczenia. **Analizowanie skutków regulacji pod kątem bezpieczeństwa danych musi się stać w Polsce standardem legislacyjnym.**

Druga ważna rzecz to wyrok TSUE w połączonych sprawach o sygn. C-182/22 i C-189/22 Scalable Capital i in. **Dotyczy on roszczeń odszkodowawczych z tytułu szkody niemajątkowej spowodowanej naruszeniem przepisów o ochronie danych osobowych.** W naszej ocenie nie wymaga on co prawda zmiany polskich przepisów, ale będzie miał znaczenie dla ich interpretacji.

Kary za narażenie danych na niebezpieczeństwo

Na końcu chcę Państwu powiedzieć **o karach**, jakie PUODO zmuszony był nałożyć za naruszanie bezpieczeństwa danych osobowych. Piszę o tym właśnie na końcu, gdyż choć o karach UODO mówi się dużo i głośno, to stanowią one niewielką część naszej działalności. Ich wysokość ustalana jest w proporcji do rocznego obrotu administratora. Ale znaczenie ma także, jak administrator zachował się po incydencie i czy współpracował przy tym z PUODO. Celem naszych postępowań jest bowiem to, by podobny incydent nie przytrafił się ponownie.

• Za nieprzestrzeganie zasad ochrony danych osobowych PUODO ukarał firmę sprzedającą m.in. drzwi antywłamaniowe ponad 350 tys. zł kary. Wspólnicy spółki cywilnej, której firma powierzyła przetwarzanie danych, zostali ukarani karą 9,8 tys. zł. Konsekwencją nieprzestrzegania tych zasad był skuteczny niestety atak hakerski na dane osobowe w firmie.

• PUODO nałożył na dwie instytucje miejskie w Kutnie kary 15 tys. zł i 20 tys. zł, m.in. za niewdrożenie odpowiednich środków technicznych i organizacyjnych, w wyniku czego doszło do naruszenia ochrony danych osobowych. Zgubiono nieszyfrowanego pendrive'a z danymi osobowymi około 1500 osób. Karę ponad 24 tys. zł otrzymała również spółka obsługująca te instytucje w zakresie zmiany programu kadrowo-płacowego.

• 25 tys. zł administracyjnej kary pieniężnej nałożył Prezes UODO na Powiatowego Inspektora Nadzoru Budowlanego w Częstochowie za niewyznaczenie inspektora ochrony danych, a w konsekwencji brak publikacji jego danych kontaktowych i brak zawiadomienia o tych danych organu nadzorczego.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Przez cały rok organizowaliśmy wraz z ZUS seminaria, które dotyczyły zagadnień związanych z ochroną danych osobowych. Obserwujemy jak te wydarzenia przekładają się na Waszą znajomość tematów – komunikujecie to za pośrednictwem infolinii Urzędu, cieszycie się z udostępnianych ze spotkań nagrań. Dlatego też postanowiliśmy przeprowadzić wywiad z ekspertami Zakładu Ubezpieczeń Społecznych, Agnieszką Gębicką, dyrektor Biura Ochrony Danych Osobowych w ZUS oraz Sławomirem Wichrowskim, jej zastępcą. To niezwykły duet pasjonatów, którzy pokazują jak teoretyczne rozważania przełożyć na praktyczne działanie i wzmocnienie ochrony danych. Publikacja wywiadu zbiega się czasowo z konferencją podsumowującą cykl organizowanych wspólnie seminariów „Wyzwania związane z ochroną danych osobowych. Spojrzenie z perspektywy 2024 roku".

Przedstawiciele trzeciego sektora kontynuują współpracę z Urzędem Ochrony Danych Osobowych z myślą o stworzeniu kodeksu postępowania dla organizacji pozarządowych. Przez najbliższe miesiące planowane jest podejmowanie działań promujących inicjatywę oraz przeprowadzenie z zainteresowanymi organizacjami konsultacji m.in. z zakresu zagadnień, które mogłyby zostać uregulowane w kodeksie postępowania.

Prezes UODO udzielił upomnienia pewnej spółce za to, że przetwarzała bez zgody zainteresowanego nimi blogera jego dane w celach marketingowych. Naganne jest także to, że firma nie odpowiadała na żądania skarżącego, by go z bazy usunąć.

Jak można wykorzystywać dostęp do danych elektronicznych do celów egzekwowania prawa i wymiaru sprawiedliwości w sprawach karnych? W debacie na ten temat eksperci od ochrony danych wielokrotnie ostrzegali przed przyznawaniem organom ścigania nadmiernych uprawnień. Zdaniem Europejskiej Rady Ochrony Danych mogłoby to być równoznaczne z masowym nadzorem i powodować poważną ingerencję w prawa podstawowe.

Pozornie niewinne zdjęcia i filmy zamieszczane w mediach społecznościowych mogą mieć nieprzewidziane konsekwencje. O zagrożeniach dla prywatności dzieci – cyfrowym kidnappingu oraz sharentingu – piszemy w listopadowym wydaniu „Biuletynu UODO".

Bezpieczeństwem dzieci w internecie zajmują się również inne europejskie organy nadzorcze. 2 października 2024 r. hiszpański odpowiednik UODO (AEPD) wydał dokument „Internet domyślnie bezpieczny dla dzieci i rola weryfikacji wieku". Przeanalizowano w nim, w jaki sposób można chronić

dzieci i młodzież w internecie bez konieczności inwigilacji i naruszania prywatności wszystkich użytkowników oraz bez narażania młodych osób na możliwość ich zlokalizowania. Analiza wyjaśnia, że obecnie wiele usług internetowych opiera się na strategiach opartych w najlepszym razie na reagowaniu po wykryciu, że szkoda lub jej wpływ już wystąpiły. Najwyższy czas to zmienić.

17 października 2024 r. Komisja Europejska przyjęła pierwsze przepisy wykonawcze dotyczące cyberbezpieczeństwa podmiotów i sieci o znaczeniu krytycznym. Podstawą jest dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii – dyrektywa NIS2.

Podczas posiedzenia plenarnego w październiku 2024 roku Europejska Rada Ochrony Danych wybrała temat czwartego skoordynowanego działania w zakresie egzekwowania prawa (CEF). Będzie ono dotyczyło wdrożenia prawa do usunięcia danych („prawa do bycia zapomnianym") przez administratorów. Organy ochrony danych dołączą do tego działania na zasadzie dobrowolności w nadchodzących tygodniach, a samo działanie rozpocznie się w pierwszym półroczu 2025 roku.

Coraz więcej mówi się o pomysłach na bezpieczniejsze podróżowanie w strefie Schengen. Komisja Europejska proponuje wspólne ramy korzystania z cyfrowych poświadczeń podróżnych oraz nową aplikację „EU Digital Travel" umożliwiającą przemieszczającym się osobom tworzenie i przechowywanie cyfrowych poświadczeń podróżnych. Dzięki nowym przepisom podróżowanie do strefy Schengen i w strefie Schengen będzie łatwiejsze i bezpieczniejsze.

Pozostając w temacie podróży – 4 października 2024 roku Komisja Europejska i Kanada przy okazji szczytu G7 podpisały umowę o przekazywaniu danych dotyczących przelotu pasażera.

W tym numerze omawiamy również kilka bardzo głośnych wyroków Trybunału Sprawiedliwości Unii Europejskiej, o których rozpisywały się media. Zachęcamy do zapoznania się z nimi i sprawdzenia, czy w sprawach, które nas dotyczą, możemy powołać się na orzeczenia TSUE.

Życzę miłej lektury i siadam do przygotowywania podwójnego numeru „Biuletynu UODO". Będzie on bardziej obszerny niż tradycyjnie wydawany co miesiąc periodyk i zadbamy, by znalazły się w nim wyjątkowe materiały, będące podsumowaniem zbliżającego się końca roku i stawiające czoła nowym wyzwaniom. Tych w Nowym Roku z pewnością nie zabraknie.

Karol Witowski
p.o. Rzecznika Prasowego UODO

NAJBARDZIEJ PODATNYM CZYNNIKIEM NA POWSTAWANIE RÓŻNEGO RODZAJU UCHYBIEŃ JEST CZYNNIK LUDZKI

Z Agnieszką Gębicką, dyrektor Biura Ochrony Danych Osobowych w ZUS oraz Sławomirem Wichrowskim, jej zastępcą, rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO.

Są Państwo nierozłącznym duetem, który świetnie się uzupełnia. Pani przez lata pełniła funkcję IOD-a w ZUS-ie, zaś Pan był zastępcą IOD. Dziś mam przyjemność pogratulować Wam nowych stanowisk, teraz jesteście dyrekcją nowopowstałego Biura Ochrony Danych Osobowych. Jak ta zmiana w strukturze ZUS wpłynie na pracę zespołu inspektorów ochrony danych w ZUS?

Bardzo dziękujemy! Proces transformacji Naszej komórki w Biuro Ochrony Danych Osobowych następował w drodze naturalnej ewolucji, gdzie stopniowo Zespół wspomagający pracę Inspektora Ochrony Danych dojrzewał do pełnienia jakże ważnej roli w Naszej Instytucji. Dzisiaj możemy powiedzieć z pełną odpowiedzialnością, że jesteśmy otoczeni grupą fantastycznych, zaangażowanych w swoją pracę osób, na których możemy zawsze liczyć. Jesteśmy zdania, że przeobrażenie się Wieloosobowego Stanowiska Inspektora Ochrony Danych w komórkę rangi departamentu jest namacalną formą uznania Naszych pracowników i docenienia ich ciężkiej pracy. Zmiana rangi komórki ochrony danych osobowych jest też niewątpliwie związana ze skalą realizacji zadań, gdyż jak wiemy Zakład Ubezpieczeń Społecznych jest ogromnym administratorem danych realizującym swe obowiązki na rzecz milionów Klientów.

Co do samej organizacji pracy Biura, to należy wspomnieć, że nie odbiega ona co do zasady od tego jak wyglądała ona sprzed wprowadzenia zmian organizacyjnych. Złożoność oraz skala realizowanych zadań powodowała konieczność przekształcenia stosunkowo płaskiej struktury pracowniczej w bardziej zorganizowane instrumenty organizacyjne. Zespoły zadaniowe zostały przekształcone w Wydziały, na czele których stoją naczelnicy oraz powołano wysokospecjalistyczne samodzielne stanowiska, które dopełniają swym zakresem realizowanych zadań czynności wchodzące w zakres Biura Ochrony Danych Osobowych. Wspomniana skala realizacji zadań powoduje, że w swojej strukturze posiadamy wyspecjalizowane wydziały wspomagające Inspektora Ochrony Danych przy realizacji zadań związanych z oceną skutków ochrony danych, doradztwa w zakresie obsługi spraw związanych z naruszeniami przepisów o ochronie danych oraz kwestiami stricte prawnymi

oraz związanymi z podnoszeniem kwalifikacji pracowników z zakresu ochrony danych osobowych. Posiadamy również wspominane wcześniej stanowiska odpowiedzialne za realizację audytów zgodności czynności przetwarzania z przepisami o ochronie danych osobowych oraz wspierające pracę Inspektora Ochrony Danych, chociażby przy organizacji coraz częściej realizowanych aktywności edukacyjnych prowadzonych wspólnie z Urzędem Ochrony Danych Osobowych.

Warto również podkreślić, że umiejscowienie Biura Ochrony Danych Osobowych bezpośrednio w Pionie Strategii i Analiz, który podlega Prezesowi ZUS, zapewnia pełną niezależność i autonomię Inspektora Ochrony Danych. Takie usytuowanie organizacyjne jest nie tylko zgodne z wymaganiami art. 38 RODO dotyczącymi niezależności IOD, ale również wzmacnia jego mandat w zakresie monitorowania zgodności z przepisami o ochronie danych osobowych w tak dużej i złożonej instytucji, jaką jest ZUS.

Dzięki tej strukturze IOD ma bezpośredni dostęp do najwyższego kierownictwa, co pozwala na skuteczne raportowanie, podejmowanie kluczowych decyzji oraz natychmiastową reakcję na pojawiające się wyzwania. Jest to także dowód na strategiczne podejście ZUS do ochrony danych osobowych, gdzie IOD nie tylko pełni rolę doradczą, ale także aktywnie uczestniczy w budowaniu systemów ochrony danych, procesów zarządzania ryzykiem oraz działań edukacyjnych i prewencyjnych na rzecz bezpieczeństwa informacji w całej organizacji.

Jak stworzyć prężnie działający zespół? Jaką macie organizację, kulturę pracy i jakie jej elementy są Państwa zdaniem ważne, by praca przynosiła efekty?

Wszystko w naszej opinii zaczyna się od wyboru odpowiednich osób do pracy w komórce ochrony danych osobowych. Problematyka ochrony danych osobowych wymaga ciągłego doskonalenia się, również w obszarach, które z pozoru nie są wprost związane z ochroną praw podstawowych osób fizycznych w związku z przetwarzaniem danych osobowych. To znak naszych czasów oraz kwestia gwałtownego rozwoju techniki. Dlatego też, do pracy w Naszej komórce od zawsze poszukiwaliśmy osób cechujących się nastawieniem na rozwój. Dzisiaj uważamy, że to od nieustannego doskonalenia zależy sukces bądź porażka w tworzeniu zespołu wspomagającego pracę Inspektora Ochrony Danych.

Powyższe powoduje, że pracownicy Biura Ochrony Danych Osobowych często uczestniczą w różnego rodzaju formach podnoszenia kwalifikacji zawodowych, powodujących, że – jak to się potocznie mówi – są „partnerami do rozmowy” we wszelkiego rodzaju dyskusjach problemowych związanych z ochroną danych osobowych. Nierzadko, nasi pracownicy sami wchodzą w role trenerskie, dzieląc się swoją wiedzą i doświadczeniem z pracownikami Naszej Instytucji. Jesteśmy z tego szczególnie dumni.

1 ROZMOWA Z EKSPERTEM

Co do kultury pracy to gdybyśmy musieli opisać jednym słowem jaka jest jej cecha charakterystyczna, to wskazalibyśmy słowo „otwartość". Otwartość rozumiana bardzo szeroko i na wielu płaszczyznach, tzn. otwartość na pomysły pracowników, otwartość na pytania z ich strony, czy też otwartość na odmienność zdań. W dzisiejszych czasach poziom wiedzy i świadomości uprawnień wynikających z przepisów prawa wśród społeczeństwa systematycznie rośnie. Z jednej strony jest to powód do zadowolenia, z drugiej zaś powoduje konieczność posiadania zespołów elastycznych, uczących się oraz otwartych na nowe wyzwania, wcześniej nieznanych z uwagi na aktualny poziom techniki lub uregulowania prawne. Dlatego tak ważne jest naszym zdaniem zapewnienie pracownikom poczucia bezpieczeństwa oraz obdarzanie ich zaufaniem. Tylko w taki sposób można mówić nie tylko o efektywnej pracy, ale przede wszystkim pracy, która jest satysfakcjonująca.

W 2022 r. otrzymała Pani tytuł Lidera EMR przyznawany przez firmę PBSG. Wyróżniony został również Zakład Ubezpieczeń Społecznych. Nagroda przyznawana jest osobom oraz organizacjom, które wdrażają najlepsze praktyki w zakresie zarządzania ryzykiem w ochronie danych osobowych.

Tak, wyróżnienie to traktuję jako ogromny zaszczyt zarówno w kategorii osobistej, jak i zawodowej. To namacalna forma uhonorowania Naszych wysiłków jakie były włożone w proces wdrożenia mechanizmów szacowania ryzyka, leżącego u podstaw zarządzania danymi osobowymi.

Jako przykład tych działań należy bez wątpienia wskazać wdrożone mechanizmy oceny skutków dla ochrony danych (DPiA), który stanowi obowiązkowy etap prac projektowych realizowanych w Zakładzie Ubezpieczeń Społecznych. Dzisiaj, normą jest, że każdy projekt i inicjatywa realizowana w Zakładzie poprzedzona jest analizą pozwalającą na opisanie całego procesu przetwarzania danych oraz obiektywną ocenę konieczności przetwarzania danych i ich proporcjonalności. Dokonywana analiza w realny sposób pozwala wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych.

Rozpowszechnienie praktyki analizy ryzyka w obszarze ochrony danych osobowych w całej organizacji było zadaniem wymagającym konsekwentnego podejścia i wsparcia na wielu poziomach. Przyzwyczajenie organizacji do konieczności przeprowadzania DPIA dla wszystkich nowych projektów wymagało profesjonalnego i aktywnego wsparcia merytorycznego dla biznesu, jak również dostosowania istniejących wewnętrznych aktów prawnych. Wprowadzono zmiany w procedurach i regulacjach wewnętrznych, aby jasno określić role, obowiązki i harmonogramy związane z procesem DPIA. Dzięki temu DPIA stała się integralnym elementem realizacji projektów, co wpłynęło na budowanie świadomości oraz wzmocnienie odpowiedzialności za ochronę danych na poziomie całej organizacji.

1 ROZMOWA Z EKSPERTEM

W ślad za wdrożeniem opisanych powyżej instytucji normatywnych, implementowano również narzędzie informatyczne, wspomagające przeprowadzania DPiA, o których mowa wyżej, ułatwiając Inspektorowi Ochrony Danych uwzględnianie w swojej pracy ryzyka związanego z operacjami przetwarzania danych osobowych. Wdrożenie tego rodzaju narzędzia wspomagającego stało się niezbędne z punktu widzenia skali Zakładu Ubezpieczeń Społecznych oraz charakteru zadań przez niego wykonywanych.

UODO wraz z ZUS-em zorganizował w tym roku cykl czterech wspólnych spotkań związanych z tematyką ochrony danych osobowych. 9 października br. w Chorzowie podczas seminarium „Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji" mówili Państwo nt. wdrożenia tej dyrektywy w organizacji z perspektywy IOD. No właśnie: jak dostosować swoje procesy w organizacjach, by były one zgodne z NIS2? Jakie są Państwa zdaniem najważniejsze podobieństwa i różnice między NIS2 i RODO?

Materia ujęta w dyrektywie NIS 2 jest bardzo szeroka i dotyczy kwestii związanych ze zbudowaniem zdolności w zakresie cyberbezpieczeństwa w całej UE. Powyższe nakłada szereg obowiązków na podmioty kluczowe i ważne, do których zalicza się m.in. Zakład Ubezpieczeń Społecznych. Celem dyrektywy NIS2 jest złagodzenie zagrożeń dla sieci i systemów informatycznych wykorzystywanych do świadczenia usług w najważniejszych sektorach, np. administracji publicznej jak również zapewnienie ciągłości działania w przypadku wystąpienia incydentów.

Niezwykle ważną kwestią z punktu widzenia dyrektywy NIS 2 jest zapewnienie przez każdy z podmiotów kluczowych środków zarządzania ryzykiem w cyberbezpieczeństwie. Środki te obejmują m.in. politykę analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługę incydentów oraz zapewnienie ciągłości działania, np. poprzez zarządzanie kopiami zapasowymi, przywrócenie normalnego działania i zarządzanie kryzysowe.

Podobnie jak RODO, dyrektywa NIS 2 bazuje na podejściu opartym na ryzyku i ciągłym doskonaleniu organizacji na podstawie cyklu PDCA. Obydwie regulacje przewidują dotkliwe kary pieniężne za niedochowanie ich zapisów. Duży nacisk w dyrektywie NIS 2 został położony na systemowe budowanie postaw osób zarządzających i pracowników poprzez organizację cyklicznych szkoleń, mających na celu umiejętność rozpoznawania ryzyk w zakresie cyberbezpieczeństwa oraz zarządzanie nimi. Stanowi to kolejne podobieństwo z RODO, gdzie również przewiduje się powołanie funkcji Inspektora Ochrony Danych, do którego głównych obowiązków należy prowadzenie szkoleń i podejmowanie działań zwiększających świadomość po stronie administratora danych i jego personelu.

1 ROZMOWA Z EKSPERTEM

Dyrektywa NIS 2 podobnie jak RODO implementowana będzie do polskiego porządku prawnego poprzez wprowadzenie przepisów wprowadzających, doszczegóławiając kwestie pozostające w sferze wpływu krajów członkowskich. Podobieństwa między obiema regulacjami obejmują obowiązek zgłaszania – w przypadku NIS 2 są to incydenty związane z cyberbezpieczeństwem, a w przypadku RODO naruszenia ochrony danych osobowych.

Jak powinno wyglądać właściwe wdrożenie polityki AI w organizacji? W czasie seminarium przytoczyła Pani interesujący przykład pracownika, który dla ułatwienia swojej pracy korzysta z Chata GPT i wprowadza do niego informacje prawnie chronione.

Musimy pamiętać, że sztuczna inteligencja to ogromne możliwości i ogromna odpowiedzialność. Te dwie zmienne trzeba obowiązkowo brać pod uwagę przy rozważaniu implementacji sztucznej inteligencji w swojej organizacji. W dzisiejszych czasach widzimy nieustający trend licytowania się różnego rodzaju firm w deklaracjach dotyczących wdrożenia określonych modeli językowych jako integralnych części świadczonych przez siebie usług.

Na drugiej stronie bieguna widzimy również stosunkowo niewielki procent wdrożeń tej technologii – niewielki w stosunku do skali złożonych deklaracji. To wskazuje jednoznacznie, że implementacja tak zaawansowanej technologii jest wyzwaniem dla organizacji, w tym instytucji sektora finansów publicznych. Wszystkim tym wysiłkom przygląda się europejski ustawodawca, który po raz pierwszy w historii opublikował akt normatywny – AI Act – starający się uporządkować najbardziej palące kwestie związane ze sztuczną inteligencją. Zapisy tego rozporządzenia będą miały bezpośredni wpływ na kierunki wdrożenia sztucznej inteligencji w krajach członkowskich UE.

Odpowiadając zatem na pytanie jak powinno wyglądać wdrożenie polityki AI w organizacji należy przede wszystkim wskazać, że powinno ono nastąpić z pełnym poszanowaniem przepisów regulujących tę kwestię. Jest to oczywiście warunek podstawowy, lecz nie jedyne kryterium sukcesu wdrożenia technologii wykorzystującej algorytmy sztucznej inteligencji. Wdrażając regulacje odnoszące się do zasad wykorzystywania sztucznej inteligencji w organizacji należy wskazać, iż regulacje te muszą być „szyte na miarę". Bardzo nęcącym może być chęć skorzystania z wzorców wypracowanych przez inne instytucje, jednakże musimy pamiętać, że organizacja organizacji nie równa, przez co bezrefleksyjne i oderwane od rzeczywistości kopiowanie rozwiązań wypracowanych przez konkurencję może być nie tylko nie najlepszym pomysłem, ale może powodować bardzo konkretne ryzyka. Przykładem może być cytowany na wstępie przypadek wprowadzania do czata GPT informacji chronionych.

1 ROZMOWA Z EKSPERTEM

Dlatego też, zaczynając myśleć o wprowadzeniu sztucznej inteligencji oraz norm regulujących jej wykorzystanie musimy zacząć od zidentyfikowania ryzyk jakie są związane z wykorzystywaniem sztucznej inteligencji. Oczywiście, charakter tych ryzyk będzie inny dla firm, a inny dla instytucji publicznych, jednakże niezbędnym jest poznanie ich wszystkich tak, aby im przeciwdziałać.

W pewnych sytuacjach wynik analizy ryzyka może przynieść konstatację, iż przy obecnym stanie techniki nie jesteśmy w stanie implementować mechanizmów sztucznej inteligencji z uwagi na ryzyko, jakiemu nie jesteśmy w stanie przeciwdziałać, narażając tym samym prawa i wolności osób fizycznych.

Kolejnym istotnym elementem, jaki musi być wzięty przy pracach ukierunkowanych na skodyfikowanie zasad wykorzystywania AI w organizacji jest zaangażowanie wszystkich interesariuszy – od Zarządu do pracowników liniowych. Sztuczna inteligencja, niesłusznie zresztą utożsamiana jest wyłącznie z obszarem IT. Obserwujemy jednak, że w coraz większym zakresie to komórki biznesowe są beneficjentami automatyzacji pracy przy wykorzystaniu AI. Dlatego też, zespół odpowiedzialny za wdrożenie sztucznej inteligencji w danej organizacji powinien prowadzić szeroko rozumiane działania informacyjno-edukacyjne wśród wszystkich komórek organizacji, tak aby zmaksymalizować korzyści płynące z jej wdrożenia oraz zminimalizować ewentualne straty nią spowodowane.

Osobną kwestią jaka powinna być brana pod uwagę przy procesie wdrożenia sztucznej inteligencji jest analiza spodziewanych korzyści wynikających z jej implementacji w stosunku do poniesionych kosztów związanych z jej wdrożeniem. Kwestia ta jednak w porównaniu do wcześniej poruszonych czynników, tj. analizy ryzyka oraz działań informacyjno-edukacyjnych ma znaczenie drugoplanowe, jednakże obligatoryjnie musi być wzięta pod uwagę, chociażby w jednostkach sektora finansów publicznych.

Bardzo ważnym dla nas wydarzeniem było seminarium UODO i ZUS dot. wdrożenia ustawy o sygnalistach oraz ochrony danych osobowych w miejscu pracy. W swojej prezentacji poruszyli Państwo temat ryzyk naruszenia praw i wolności osób w procesie zgłaszania naruszeń prawa. Jak w praktyce organizacja może zminimalizować wystąpienie tych ryzyk? Jak powinna wyglądać modelowa procedura w tym zakresie?

Sprawami oczywistymi, poruszanymi zresztą podczas naszego wystąpienia były takie czynniki jak maksymalne ograniczenie dostępu do danych sygnalistów oraz zapewnienie odpowiedniego bezpieczeństwa technologicznego – stanowiącego gwarancje anonimowości osób dokonujących zgłoszeń. Równie ważnym czynnikiem jest odpowiedni dobór osób, którym zostaną powierzone obowiązki związane z obsługą spraw sygnalistów. Mówiliśmy również o konieczności przeprowadzania regularnych audytów oraz cyklicznych szkoleniach pracowników z tematyki ochrony danych osobowych. Podnoszone przez nas argumenty nie straciły w żaden sposób na aktualności.

Dzisiaj jednak wiemy, że najbardziej podatnym czynnikiem na powstawanie różnego rodzaju uchybień jest czynnik ludzki. Dlatego też, w naszych rozważaniach dotyczących najskuteczniejszych metod minimalizujących ryzyko jakie może powstać przy obsłudze tego rodzaju spraw jest kwestia postaw, wiedzy i umiejętności pracowników. W swoje praktyce zawodowej dostrzegamy bowiem niejednoznaczny stosunek pracowników do kwestii dokonywania zgłoszeń przez sygnalistów. Głęboko wierzymy w to, iż ma to swoje podstawy w doświadczeniach historycznych, niemniej jednak konieczna jest zmiana postrzegania w tym zakresie. Musimy przecież pamiętać, że poza powołanymi organami kontroli państwowej oraz wewnętrznymi służbami audytu funkcjonującymi w większości instytucji, czynnik społeczny jest naturalnym dopełnieniem procesu nadzoru. Dlatego też jako podstawowe kryterium powodzenia przy implementacji mechanizmów obsługi spraw sygnalistów wskazalibyśmy kwestię budowania odpowiedniej kultury organizacyjnej. Oczywiście, budowanie tego rodzajów podstaw wśród pracowników jest procesem założonym i czasochłonnym, ale korzyści wynikające z włożonych wysiłków w tym zakresie będą procentować na przyszłość. Stoimy na stanowisku, że wdrożenie przepisów w sprawie ochrony osób zgłaszających naruszenia nie jest kolejnym zadaniem do przysłowiowego „odhaczenia” w drodze jednorazowego wdrożenia, lecz całym procesem, którego powodzenie zależy od pełnego zaangażowania całej organizacji.

Musimy również pamiętać, że natura zgłoszeń dokonywanych przez sygnalistów wymaga szczególnej staranności i delikatności. To od prawidłowej obsługi zgłoszeń, u podstaw których powinna stać ochrona danych osobowych osób dokonujących zgłoszenia, zależy poziom zaufania jakim pracownicy będą obdarzać instytucję zgłoszeń nieprawidłowości jakie pojawiają się w ich miejscu pracy.

Przechodząc do procedury, wydaje się zasadnym, aby poza zapisami, które wskazaliśmy jako niezbędne do ujęcia w niej, znalazły się również elementy podkreślające wagę i znaczenie zgłoszeń dokonywanych przez sygnalistów. Bez wątpienia dobrą praktyką będzie zaangażowanie do tworzenia procedury jak najszerszej grupy interesariuszy, tak aby nie była ona postrzegana jako wyłącznie regulacja dotycząca komórki kontroli wewnętrznej, HR lub innej. Upowszechnienie prac i zaangażowanie do pracy szerokiej grupy pracowników, rekrutujących się z różnych działów jest właśnie elementem budowania wspierającej kultury organizacyjnej.

Mija rok od Waszego wystąpienia w czasie konferencji poświęconej nowym technologiom w kontekście ochrony danych osobowych. Przybliżaliście wtedy problemy audytu IOD z uwagi na wykorzystanie nowych technologii. Temat opisaliście w styczniowym numerze „Biuletynu UODO” (01/2024). Czy do tamtych refleksji możecie coś dodać? Czy pojawiły się jakieś wyzwania, z których rok temu nie zdawaliśmy sobie jeszcze sprawy?

1 ROZMOWA Z EKSPERTEM

Tematy poruszane w tamtym momencie nie straciły na aktualności, z tą jednak różnicą, że jesteśmy bogatsi o dalsze doświadczenia i co bardzo ważne, pierwszy akt podstawowy regulujący wykorzystanie sztucznej inteligencji przez Państwa członkowskie UE, czyli AI Act. To najlepiej dowodzi, że zidentyfikowane przez nas niebezpieczeństwa związane z wykorzystaniem sztucznej inteligencji w kontekście ochrony danych osobowych są nadal w polu troski i naszej uwagi.

Podstawową kwestią, a zarazem najważniejszym niebezpieczeństwem związanym z wykorzystywaniem nowoczesnych technologii, w tym AI jest potencjalne ryzyko dyskryminacji mogące prowadzić do naruszeń praw i wolności osób fizycznych i w konsekwencji do odpowiedzialności podmiotu wykorzystującego tę technologię. Mówiąc o odpowiedzialności mamy na myśli element wzięcia pełnej odpowiedzialności za cały proces przetwarzania danych biorących udział w procesie, począwszy od ich gromadzenia po finalny produkt, jakim jest decyzja firmy ubezpieczeniowej w postaci indywidualizowanej polisy bądź oferty kredytu wygenerowanej przez instytucję finansową.

Te wszystkie nowe technologie wyglądają bardzo atrakcyjnie, ale nie możemy zapominać, że u ich źródła znajdują się – czy też z dużym prawdopodobieństwem mogą się znajdować – nasze dane osobowe. Dzisiejsza praktyka w tym zakresie jest niestety z naszych obserwacji różna. Przetwarzanie danych osobowych przez wyspecjalizowane podmioty dokonywane jest nierzadko na podstawie zawiłych i nieczytelnych regulaminów z dyskusyjnym prawem konsumenta do wglądu w cały proces. Jeszcze gorzej wygląda sytuacja związana z transparentnością w zakresie miejsc, w których są wirtualnie przetwarzane dane osobowe.

Dlatego rozpatrując kwestię prawidłowości przetwarzania danych osobowych w kontekście nowych technologii, trzeba mieć na uwadze stały element edukacyjny, uświadamiający wśród społeczeństwa przysługujące prawa oraz zagrożenia wynikające ze stosowania tych technologii. Wydaje się, że tego rodzaju działania uświadamiające powinny odbywać się od najmłodszych lat, przez co zagadnienia związane z ochroną praw osób fizycznych wynikających z przetwarzania danych osobowych przy wykorzystaniu nowoczesnych technologii powinny być stałym elementem programowym w szkołach podstawowych oraz średnich. Jako Biuro Ochrony Danych Osobowych w ZUS widzimy tutaj również swoją rolę oraz możliwość wniesienia realnego wkładu w tego rodzaju działania.

Dziękuję za rozmowę.

ORGANIZACJE POZARZĄDOWE CHCĄ STWORZYĆ SWÓJ KODEKS POSTĘPOWANIA

Przedstawiciele trzeciego sektora kontynuują współpracę z Urzędem Ochrony Danych Osobowych z myślą o stworzeniu kodeksu postępowania dla organizacji pozarządowych.

Na prośbę Fundacji Onkologicznej Alivia, 6 listopada br. odbyło się spotkanie przedstawicieli Urzędu Ochrony Danych Osobowych z inicjatorami stworzenia kodeksu postępowania dotyczącego ochrony danych osobowych w sektorze organizacji pozarządowych. Było ono kontynuacją rozmów na temat ochrony danych osobowych w trzecim sektorze rozpoczętych w sierpniu br. (https://uodo.gov.pl/pl/138/3337).

Na listopadowym spotkaniu poruszono m.in. takie kwestie, jak:

• legitymacja do złożenia projektu kodeksu postępowania,

• reprezentatywność grupy podmiotów tworzących kodeks,

• krąg podmiotów zainteresowanych przystąpieniem do kodeksu,

• wyznaczenie podmiotu monitorującego przestrzeganie postanowień kodeksu,

• zakres konsultacji społecznych.

Przez najbliższe miesiące planowane jest podejmowanie działań promujących inicjatywę oraz przeprowadzenie z zainteresowanymi organizacjami konsultacji dotyczących m.in. zakresu zagadnień, które mogłyby zostać uregulowane w kodeksie postępowania.

Prezes Urzędu Ochrony Danych Osobowych wspiera tę inicjatywę i zachęca do kontaktu z jej autorami.

Dane kontaktowe zostaną opublikowane na stronie internetowej Urzędu w sekcji poświęconej inicjatywom w tym zakresie: https://uodo.gov.pl/pl/426/2790.

UPOMNIENIE ZA WYSYŁANIE NEWSLETTERA DO BLOGERA PO TYM, JAK WYRAŹNIE WSKAZAŁ, ŻE SIĘ NA TO NIE ZGADZA

Prezes UODO udzielił upomnienia I. SA za to, że przetwarzała bez zgody zainteresowanego jego dane w celach marketingowych.
I nie zareagowała na żądanie usunięcia tych danych.

PUODO reaguje tu na skargę obywatela. Skarżący prowadził popularnego bloga i traktowany był przez wiele instytucji oraz firm jako lider opinii. Dlatego liczne firmy wysyłały mu informacje prasowe. W 2020 r. obywatel poprosił jednak I. SA, by więcej informacji już mu nie przesyłać, bo nie są mu potrzebne. Wielokrotnie prosił o wypisanie go z list mailingowych.

I. SA wyjaśniła jednak, że jej zadaniem jest docieranie do dziennikarzy z aktualnymi informacjami, zaś dane skarżącego „zostały pozyskane ze źródeł powszechnie dostępnych". Dane te zostały wprowadzone do bazy dziennikarzy, a „podstawą prawną był uzasadniony interes administratora danych polegający na świadczeniu klientom usług informacyjnych". Zgoda na przetwarzanie informacji marketingowych nie była zdaniem spółki potrzebna, bo „newslettery dla dziennikarzy nie są informacjami marketingowymi".

PUODO ustalił jednak, że newslettery I. SA były w istocie działalnością marketingową: chodziło w nich o zachęcenie adresatów do odwiedzenia strony internetowej, gdzie zamieszczane były informacje. Naganne jest także to, że firma nie odpowiadała na żądania blogera, by go z bazy usunąć.

I. SA usunęła dane blogera dopiero po interwencji PUODO.

Sygnatura sprawy: DS.523.6184.2022

DOSTĘP DO DANYCH NA RZECZ SKUTECZNEGO EGZEKWOWANIA PRZEPISÓW

Jak można wykorzystywać dostęp do danych elektronicznych do celów egzekwowania prawa i wymiaru sprawiedliwości w sprawach karnych? W debacie na ten temat eksperci od ochrony danych wielokrotnie ostrzegali przed przyznawaniem organom ścigania nadmiernych uprawnień. Mogłoby to być równoznaczne z masowym nadzorem i powodować poważną ingerencję w prawa podstawowe. Dotyczy to w szczególności zasad i okresu przechowywania danych, a także odpowiedniego zabezpieczenia danych i ich szyfrowania.

Musimy zapewnić równowagę między prawami osób a interesami organów ścigania, które poszukują sprawców przestępstw, zwłaszcza tych popełnionych w internecie. Niedawno wskazał to Trybunał Sprawiedliwości UE[1]. Proponowane środki powinny być zgodne z zasadami ochrony danych i prywatności, a dostęp do danych powinien być przyznawany wyłącznie w kontekście postępowań karnych, indywidualnie rozpatrywany, i zasadniczo podlegać zezwoleniu sądowemu.

Przechowywanie danych

Przechowywanie danych było przedmiotem licznych debat w Unii Europejskiej. Pokazują one złożoność tematu i trudności w znalezieniu właściwej równowagi między potrzebą ochrony osób przed nowoczesnymi formami nadzoru elektronicznego. Z drugiej strony wskazują na konieczność wykorzystania technologii w dochodzeniach karnych.

Zakres podmiotowy i przedmiotowy wszelkich przyszłych unijnych ram prawnych dotyczących zatrzymywania danych osobowych i dostępu do nich jest jednym z kluczowych elementów oceny niezbędności i proporcjonalności. W tym względzie TSUE stwierdził już, że uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu jest co do zasady zakazane i może być uzasadnione wyłącznie ochroną bezpieczeństwa narodowego, jeżeli dane państwo członkowskie stoi w obliczu poważnego jego zagrożenia, które jest rzeczywiste i aktualne lub przewidywane[2].

Szeroki i ogólny obowiązek zatrzymywania danych w formie elektronicznej przez podmioty zajmujące się przetwarzaniem danych (tj. wszelkiego rodzaju dostawców usług, którzy mogliby zapewnić dostęp do wszelkich dowodów elektronicznych) rozszerzyłby zakres zatrzymywania danych poza bariery ustanowione w orzecznictwie. Byłby zatem wysoce problematyczny.

4 NARUSZENIA I KONTROLE

Niedawny wyrok TSUE w sprawie Hadopi wskazuje[3], że w pewnych okolicznościach ogólne zatrzymywanie adresów IP przypisanych do źródła połączenia internetowego, a także danych dotyczących tożsamości cywilnej użytkowników środków łączności elektronicznej może być zgodne z prawem.

Trybunał wyjaśnił, że uogólnione i niezróżnicowane przechowywanie adresów IP nie stanowi poważnej ingerencji w prawa podstawowe. Może być więc dopuszczalne na mocy prawa Unii w celu zwalczania wszelkiego rodzaju czynów zabronionych. Jednakże jest to ściśle ograniczone. Obejmuje przypadki, gdy wykluczone jest, by przechowywanie danych mogło prowadzić do poważnych ingerencji w życie prywatne danej osoby ze względu na możliwość wyciągnięcia precyzyjnych wniosków na jej temat. W związku z tym każde połączenie tych adresów IP z innymi przechowywanymi danymi, które pozwalałoby na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane byłyby w ten sposób przechowywane, musi zostać zakazane.

Zatrzymywanie adresów IP w sposób ogólny i niezróżnicowany nie może w żaden sposób zostać automatycznie rozszerzone na inne (bardziej wrażliwe) dane o ruchu i lokalizacji, które mogłyby z łatwością umożliwić stworzenie bardziej szczegółowego profilu użytkownika.

Bezpieczeństwo danych i szyfrowanie

Szyfrowanie ma zasadnicze znaczenie dla zapewnienia bezpieczeństwa i poufności danych osobowych i komunikacji elektronicznej. Zapewnia silne techniczne zabezpieczenia przed dostępem do tych informacji przez inne osoby niż użytkownik i wybrani przez niego odbiorcy, w tym dostawcy. W szczególności, w kontekście komunikacji interpersonalnej, prawdziwe szyfrowanie typu end-to-end („E2EE") obejmujące urządzenia końcowe i zawarte w nich dane, z kluczami deszyfrującymi posiadanymi wyłącznie przez użytkowników, jest podstawowym narzędziem zapewniającym poufność komunikacji elektronicznej.

Uniemożliwienie korzystania z szyfrowania lub osłabienie skuteczności zapewnianej przez nie ochrony miałoby poważny wpływ na poszanowanie życia prywatnego i poufności użytkowników, na ich wolność wypowiedzi, a także na innowacje i rozwój gospodarki cyfrowej, która opiera się na wysokim poziomie zaufania i pewności, jakie gwarantują takie technologie.

Dostawcy mogą stanąć przed techniczną koniecznością zastosowania środków osłabiających szyfrowanie w sposób masowy wobec wszystkich użytkowników, aby móc zrealizować prawny nakaz przechwycenia lub dostępu, nawet w przypadkach, gdy pierwotny nakaz przechwycenia lub dostępu był ograniczony do konkretnej osoby lub konkretnej grupy osób.

4 NARUSZENIA I KONTROLE

Takie masowe osłabienie szyfrowania – czy to poprzez środki wymagane od dostawców, czy poprzez osłabienie technicznych standardów szyfrowania – może prowadzić do wysokiego ryzyka naruszenia praw podstawowych osób fizycznych w UE, w szczególności w kontekście łączności elektronicznej. W tym względzie Europejski Trybunał Praw Człowieka stwierdził, że „obowiązek odszyfrowywania zaszyfrowanych komunikatów typu end-to-end może sprowadzać się do wymogu, aby dostawcy takich usług osłabili mechanizm szyfrowania dla wszystkich użytkowników; w związku z tym nie jest on proporcjonalny do zamierzonych uzasadnionych celów".

Zasadniczo każdy wymóg techniczny dla dostawców, który może potencjalnie wpływać na podstawowe prawa i wolności osób fizycznych, powinien być ustanowiony przez prawo, które szanuje istotę podstawowych praw i wolności oraz jest uważane za niezbędne i proporcjonalne w demokratycznym społeczeństwie.

Opracowano na podstawie Stanowiska EROD nr 5/2024 w sprawie zaleceń grupy wysokiego szczebla ds. dostępu do danych w celu skutecznego egzekwowania prawa[4].

[1] Wyrok Trybunału Sprawiedliwości z dnia 30 kwietnia 2024 r., La Quadrature du Net i in., sprawa C-470/21, ECLI:EU:C:2024:370, pkt 116 i 117 oraz z dnia 4 października 2024 r., Bezirkshauptmannschaft Landeck, C- 548/21, ECLI:EU:C:2024:830, pkt 97

[2] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2020 r., La Quadrature du Net i in., sprawy połączone C-511/18, C-512/18 i C-520/18, ECLI:EU:C:2020:791, pkt 137.

[3] Wyrok Trybunału Sprawiedliwości z dnia 30 kwietnia 2024 r., La Quadrature du Net i in., sprawa C-470/21, ECLI:EU:C:2024:370.

[4] https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf

OD SHARENTINGU DO CYFROWEGO KIDNAPPINGU: WIZERUNEK DZIECKA W DOBIE AI I DEEPFAKE

Pozornie niewinne zdjęcia i filmy zamieszczane w mediach społecznościowych mogą mieć nieprzewidziane konsekwencje.

Internetowe platformy, media społecznościowe, sztuczna inteligencja (AI) oraz technologie takie jak deepfake, wprowadzają nas w erę, w której nie tylko łatwo dzielić się treściami, ale i nimi manipulować. Jednym z najnowszych i najszerzej omawianych problemów w ostatnim czasie jest zjawisko „sharentingu", polegające na udostępnianiu wizerunku swoich dzieci w sieci.

Warto pamiętać, że wizerunek, jako dana osobowa, podlega szczególnej ochronie na mocy przepisów RODO. Dlatego Prezes Urzędu Ochrony Danych Osobowych od lat zwraca uwagę na potrzebę świadomego i odpowiedzialnego zarządzania swoim wizerunkiem w przestrzeni cyfrowej. Problem ten został poruszony również w poradniku „Wizerunek dziecka w internecie. Publikować czy nie?", który został przygotowany przez UODO i Fundację Orange. Jego celem jest podniesienie świadomości na temat ryzyka, jakie niesie za sobą zbyt swobodne udostępnianie wizerunków dzieci w sieci, a także dostarczenie rodzicom i opiekunom praktycznych wskazówek, jak chronić prywatność swoich dzieci w świecie cyfrowym.

Sharenting – czy na pewno wiemy, co udostępniamy?

Sharenting to zjawisko, które szturmem zdobyło media społecznościowe, stając się częścią codziennego życia wielu rodziców. Sam termin jest połączeniem angielskich słów „share" (dzielić się) i „parenting" (rodzicielstwo), odzwierciedlając modę na udostępnianie zdjęć, filmów i innych szczegółów z życia dzieci w internecie. Co może wydawać się nieszkodliwym sposobem dzielenia się uroczymi momentami i osiągnięciami swoich pociech, niesie ze sobą jednak ryzyka, o których wielu rodziców często zapomina.

Czy rzeczywiście kontrolujemy, kto widzi udostępnione materiały? Jedno zdjęcie z pierwszych kroków dziecka czy film z urodzin mogą szybko rozprzestrzenić się po sieci, zyskując dostęp do tysięcy, jeśli nie milionów użytkowników. Wystarczy chwila nieuwagi – brak odpowiednich ustawień prywatności lub publikacja na otwartym profilu – by zdjęcia znalazły się w rękach nieznajomych. Często zapominamy, że udostępniając te materiały, oddajemy część prywatności naszego dziecka, narażając je na nadużycia. Co gorsza, publikowanie takich treści może prowadzić do tzw. cyfrowego kidnappingu, czyli wykorzystania wizerunku dziecka do tworzenia fałszywych kont i materiałów deepfake.

5 NOWE TECHNOLOGIE

Cyfrowy Kidnapping – nowe zagrożenie dla prywatności dzieci

Cyfrowy kidnapping, czyli kradzież tożsamości dziecka w świecie wirtualnym, to problem, który narasta w erze nowoczesnych technologii, takich jak sztuczna inteligencja i deepfake. Rodzice, chcąc dzielić się codziennymi chwilami swoich pociech w mediach społecznościowych, często nie zdają sobie sprawy, że mogą przekazać „klucze" do wizerunku dziecka osobom postronnym.

Jak wygląda cyfrowy kidnapping w praktyce? Wystarczy kilka zdjęć lub filmików udostępnionych w sieci, by ktoś stworzył fałszywe profile, strony internetowe, a nawet materiały wideo, które prezentują dziecko w innym, często przerażającym lub kompromitującym kontekście.

Dzięki technologii deepfake oszuści mogą generować materiały wizualne, które wyglądają tak realistycznie, że trudno je odróżnić od prawdziwych nagrań. Wyobraźmy sobie film, w którym wizerunek dziecka zostaje „przyklejony" do sceny z nieodpowiednią treścią, na przykład materiału przeznaczonego wyłącznie dla dorosłych. Takie manipulacje mogą prowadzić nie tylko do cyberprzemocy i zastraszania, ale również do głębokich urazów psychicznych i emocjonalnych.

Co ciekawe, już teraz pojawiają się przypadki, gdzie zmanipulowane obrazy dzieci wykorzystywane są w reklamach, kampaniach politycznych czy jako narzędzia do wyłudzania danych. Ten problem przestaje być jedynie teoretycznym zagrożeniem, a staje się realnym ryzykiem, które dotyka coraz więcej rodzin na całym świecie. Współczesne technologie nie tylko umożliwiają tworzenie fałszywych treści, ale także utrudniają ich wykrywanie, co sprawia, że cyfrowy kidnapping jest jednym z najbardziej niepokojących zagrożeń, przed którymi stają dzisiejsi rodzice.

Inne zagrożenia związane z cyfrowym kidnappingiem: Doxxing, Catfishing

Doxxing, czyli ujawnianie prywatnych informacji o osobie bez jej zgody, to jedno z poważniejszych zagrożeń związanych z cyfrowym kidnappingiem. W przypadku dzieci, informacje udostępnione przez rodziców – takie jak adres, szkoła, hobby czy szczegóły codziennych aktywności – mogą być wykorzystane przez osoby o złych intencjach. Przykładem może być ujawnienie lokalizacji dziecka, co naraża je na kontakt z nieznajomymi, cyberprzemoc lub nawet fizyczne niebezpieczeństwo. Ujawnione informacje mogą być też użyte do szantażu rodziny lub rozpowszechniania fałszywych treści w internecie.

Catfishing to inny sposób wykorzystywania zdjęć dzieci. Przestępcy podszywają się pod nie, aby zdobywać zaufanie innych, często również dzieci, w celu uzyskania kompromitujących informacji, zdjęć lub nawet nawiązania kontaktu osobistego. W skrajnych przypadkach takie fałszywe profile są używane do manipulacji emocjonalnej i wyłudzania danych od innych dzieci lub ich rodzin.

5 NOWE TECHNOLOGIE

Phishing i socjotechnika – zdjęcia i dane osobowe mogą zostać wykorzystane w atakach phishingowych, gdzie przestępcy próbują zdobyć dodatkowe informacje od ofiary. Oszuści tworzą fałszywe wiadomości, podszywając się pod znane osoby, aby wyłudzić hasła lub dane kart kredytowych. Znając prywatne informacje ofiary, przestępcy łatwiej zdobywają jej zaufanie, co zwiększa skuteczność takich ataków.

Jak chronić wizerunek dziecka w cyfrowym świecie?

1. Przemyśl, zanim opublikujesz: Zanim udostępnisz wizerunek dziecka, zastanów się, kto może mieć dostęp do tej treści. Ograniczaj publikowanie intymnych i kompromitujących materiałów.

2. Korzystaj z ustawień prywatności: Media społecznościowe oferują różne opcje zabezpieczenia postów. Upewnij się, że zdjęcia Twojego dziecka nie są dostępne publicznie, a jedynie dla najbliższej rodziny i znajomych.

3. Rozmawiaj z dzieckiem: dostosuj do jego wieku informacje o prywatności i zagrożeniach w sieci. Wyjaśnij, dlaczego warto być ostrożnym z publikowaniem prywatnych materiałów.

4. Nie taguj i nie oznaczaj miejsc: Unikaj oznaczania lokalizacji i podawania pełnych imion i nazwisk dzieci w postach. To ograniczy możliwości śledzenia dziecka przez osoby niepowołane.

5. Korzystaj z aplikacji do edycji: Zamiast udostępniać wizerunek dziecka, warto zastosować specjalne aplikacje, które pozwalają na rozmycie twarzy lub jej zasłonięcie.

Kiedy sztuczna inteligencja rozwija się szybciej niż regulacje prawne, rodzice muszą być bardziej świadomi niż kiedykolwiek wcześniej. Zwłaszcza gdy w grę wchodzi wizerunek dzieci, które same jeszcze nie mają pełnej kontroli nad swoją obecnością w sieci. Warto zadać sobie pytanie, czy publikując zdjęcia naszych dzieci jesteśmy pewni, że nie przyczyniamy się do tworzenia cyfrowych kopii ich wizerunku, nad którymi stracimy kontrolę?

NOWE PRZEPISY ZWIĘKSZAJĄCE CYBERBEZPIECZEŃSTWO KRYTYCZNYCH PODMIOTÓW I SIECI W UE

17 października 2024 r. Komisja Europejska przyjęła pierwsze przepisy wykonawcze dotyczące cyberbezpieczeństwa podmiotów i sieci o znaczeniu krytycznym. Podstawą jest dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS2).

Akt wykonawczy szczegółowo określa środki zarządzania ryzykiem cybernetycznym, a także przypadki, w których incydent należy uznać za istotny, a przedsiębiorstwa dostarczające infrastrukturę cyfrową i usługi cyfrowe powinny zgłosić go organom krajowym. Jest to kolejny ważny krok w kierunku zwiększenia cyberodporności krytycznej infrastruktury cyfrowej w Europie.

Przyjęte rozporządzenie wykonawcze będzie miało zastosowanie do określonych kategorii firm świadczących usługi cyfrowe, takich jak:

- dostawcy usług przetwarzania w chmurze,
- dostawcy usług centrów danych,
- internetowe platformy handlowe,
- wyszukiwarki internetowe,
- i platformy społecznościowe, by wymienić tylko kilka z nich.

Dla każdej kategorii dostawców usług akt wykonawczy określa również, kiedy incydent jest uznawany za istotny.

Przyjęcie rozporządzenia wykonawczego zbiega się z terminem transpozycji dyrektywy NIS2 do prawa krajowego przez państwa członkowskie. Od 18 października 2024 r., wszystkie państwa członkowskie muszą stosować środki niezbędne do przestrzegania zasad cyberbezpieczeństwa NIS2, w tym środki nadzoru i egzekwowania.

Kolejne kroki

Rozporządzenie wykonawcze zostanie opublikowane w Dzienniku Urzędowym w odpowiednim czasie i wejdzie w życie 20 dni później.

6 SPRAWY MIĘDZYNARODOWE

Kontekst

Pierwszy ogólnounijny akt prawny dotyczący cyberbezpieczeństwa, dyrektywa NIS, wszedł w życie w 2016 r. i pomógł osiągnąć wspólny poziom bezpieczeństwa sieci i systemów informatycznych w całej UE. W ramach swojego kluczowego celu politycznego, jakim jest dostosowanie Europy do ery cyfrowej, Komisja zaproponowała w grudniu 2020 r. przegląd dyrektywy w sprawie bezpieczeństwa sieci i informacji. Po wejściu w życie w styczniu 2023 r. państwa członkowskie musiały dokonać transpozycji dyrektywy NIS2 do prawa krajowego do dnia 17 października 2024 r.

Dyrektywa NIS2 ma na celu zapewnienie wysokiego poziomu cyberbezpieczeństwa w całej Unii. Obejmuje ona podmioty działające w sektorach o krytycznym znaczeniu dla gospodarki i społeczeństwa, w tym dostawców publicznych usług łączności elektronicznej, zarządzania usługami ICT, usług cyfrowych, gospodarki ściekami i odpadami, przestrzeni kosmicznej, zdrowia, energii, transportu, wytwarzania produktów o krytycznym znaczeniu, usług pocztowych i kurierskich oraz administracji publicznej.

Dyrektywa zaostrza wymogi bezpieczeństwa nałożone na firmy i odnosi się do bezpieczeństwa łańcuchów dostaw i relacji z dostawcami. Usprawnia ona obowiązki sprawozdawcze, wprowadza bardziej rygorystyczne środki nadzorcze dla organów krajowych, a także surowsze wymogi w zakresie egzekwowania prawa i ma na celu harmonizację sankcji we wszystkich państwach członkowskich. Pomoże to zwiększyć wymianę informacji i współpracę w zakresie zarządzania kryzysami cybernetycznymi na poziomie krajowym i unijnym.

Więcej informacji:

Akt wykonawczy

Zestawienie informacji na temat dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (NIS2)

Pytania i odpowiedzi na temat NIS2: Nowa strategia UE w zakresie cyberbezpieczeństwa i nowe przepisy zwiększające odporność fizycznych i cyfrowych podmiotów krytycznych

Źródło: komunikat Komisji Europejskiej

CEF 2025 – ,,PRAWO DO BYCIA ZAPOMNIANYM”

Podczas posiedzenia plenarnego w październiku 2024 r. Europejska Rada Ochrony Danych (EROD) wybrała temat czwartego skoordynowanego działania w zakresie egzekwowania prawa (CEF). Będzie ono dotyczyło wdrożenia prawa do usunięcia danych („prawa do bycia zapomnianym”) przez administratorów. Organy ochrony danych dołączą do tego działania na zasadzie dobrowolności w nadchodzących tygodniach, a samo działanie rozpocznie się w pierwszym półroczu 2025 r.

Prawo do usunięcia danych (art. 17 RODO) jest jednym z najczęściej wykonywanych praw do ochrony danych, na które organy ochrony danych często otrzymują skargi. Celem tego skoordynowanego działania będzie między innymi ocena wdrażania tego prawa w praktyce. Zostanie to na przykład dokonane poprzez analizę i porównanie procesów wdrożonych przez różnych administratorów w celu zidentyfikowania najważniejszych kwestii związanych z przestrzeganiem tego prawa, ale także w celu uzyskania przeglądu najlepszych praktyk.

W ramach skoordynowanych działań w zakresie egzekwowania przepisów EROD nadaje priorytet konkretnemu tematowi, nad którym organy ochrony danych mają pracować na szczeblu krajowym. W ciągu ostatnich trzech lat organy ochrony danych koordynowały już swoje krajowe działania dotyczące różnych tematów, a mianowicie: wykorzystania chmury w sektorze publicznym, wyznaczania i pozycji inspektorów ochrony danych oraz wdrażania prawa dostępu przez administratorów danych.

Wyniki tych krajowych działań są następnie agregowane i analizowane razem, aby uzyskać głębszy wgląd w temat i umożliwić ukierunkowane działania następcze zarówno na poziomie krajowym, jak i unijnym.

W 2023 r. EROD opublikowała sprawozdanie ze swoich pierwszych skoordynowanych działań w zakresie korzystania z usług w chmurze przez sektor publiczny.

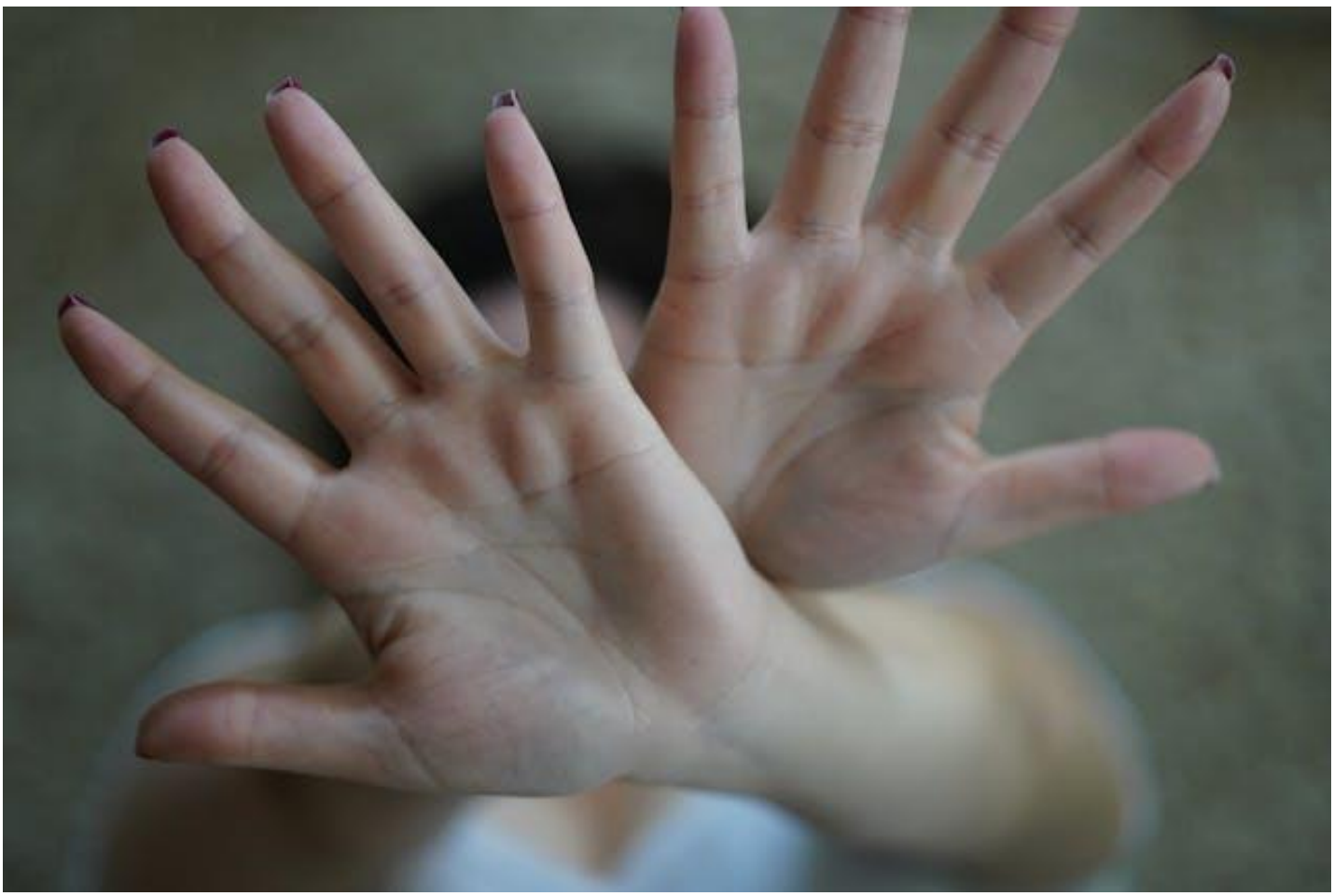
Na początku tego roku EROD udostępniła również sprawozdanie z wyników drugiego skoordynowanego działania dotyczącego wyznaczania i pozycji inspektorów ochrony danych.

Sprawozdanie z wyników skoordynowanych działań w zakresie prawa dostępu w 2024 r. zostanie przyjęte na początku 2025 r.

6 SPRAWY MIĘDZYNARODOWE

Skoordynowane działania są następstwem decyzji podjętej przez EROD w październiku 2020 r. o ustanowieniu skoordynowanych ram egzekwowania prawa (CEF). CEF jest kluczowym działaniem EROD w ramach strategii na lata 2024-2027, wraz z grupą ekspertów wspierających EROD (SPE). Obie inicjatywy mają na celu usprawnienie egzekwowania prawa i współpracy między organami ochrony danych.

Źródło: komunikat Europejskiej Rady Ochrony Danych



Fot. pexels

AEPD PUBLIKUJE ANALIZĘ DOTYCZĄCĄ OCHRONY DZIECI I MŁODZIEŻY W ŚRODOWISKU CYFROWYM

2 października 2024 r. hiszpański organ nadzorczy (AEPD) wydał dokument „Internet domyślnie bezpieczny dla dzieci i rola weryfikacji wieku". Przeanalizowano w nim, w jaki sposób można chronić dzieci i młodzież w internecie bez konieczności inwigilacji i naruszania prywatności wszystkich użytkowników oraz bez narażania dzieci na możliwość ich zlokalizowania i na nowe zagrożenia.

Analiza ta skupia się na obowiązku przestrzegania zasad ochrony danych zawartych w ogólnym rozporządzeniu o ochronie danych (RODO) oraz innych przepisach, które uzupełniają lub pogłębiają ochronę małoletnich.

Dokument przedstawia **różne strategie ochrony** dzieci i młodzieży w internecie, definiując różne przypadki:

• ochronę przed nieodpowiednimi treściami,

• bezpieczne środowisko dla dzieci,

• zgodę na przetwarzanie danych osobowych,

• i projektowanie przyjazne dzieciom.

Analiza wyjaśnia, że obecnie wiele usług internetowych opiera się na strategiach opartych w najlepszym razie na reagowaniu po wykryciu, że szkoda lub jej wpływ już wystąpiły. Jedną z przyjętych strategii jest umożliwienie dostawcom usług internetowych rozpoznania nieletnich użytkowników, na przykład poprzez tworzenie określonych przestrzeni lub kont dla dzieci. Strategie te wymagają inwazyjnej interwencji w postaci nadzoru lub profilowania, które naruszają prywatność wszystkich użytkowników: pozwalają na lokalizowanie nieletnich i łatwy dostęp do tych danych dla każdego podstępnego podmiotu, legitymizują przetwarzanie dodatkowych danych osobowych dzieci, dostosowują wiadomości do podejmowania decyzji, które im nie odpowiadają, lub ukrywają cele profilowania w odniesieniu do wprowadzających w błąd lub uzależniających wzorców.

Jak podkreślono, AEPD gromadzi przykłady i dobre praktyki w celu ochrony małoletnich przed zagrożeniami związanymi z dostępem do treści dla dorosłych, takimi jak kontakt z osobami,

które mogą im zagrażać, zawieranie umów na produkty i usługi, monetyzacja ich danych osobowych, wywoływanie uzależniających zachowań wpływających na ich integralność fizyczną lub psychiczną i inne aspekty.

Podkreślono również znaczenie posiadania systemu weryfikacji wieku. Sprawia to, że **ciężar dowodu spoczywa na osobie w ustalonym wieku** umożliwiającym dostęp do treści, a nigdy na osobie nieletniej. W ten sposób osoba niepełnoletnia nie musi udowadniać, że jest niepełnoletnia, ani nie musi ujawniać się w celu zablokowania treści, kontaktów, zachowań lub umów.

Wdrożenie systemu weryfikacji wieku wymaga dostosowania usług internetowych tak, aby był on skuteczny, nie generował nowych zagrożeń, nie pozwalał na lokalizację małoletnich i nie pociągał za sobą utraty swobód wszystkich użytkowników internetu. W tym celu takie dostosowanie musi być zgodne z zasadami minimalizacji przetwarzania danych osobowych w fazie projektowania i z domyślną ochroną danych.

AEPD zaznaczyła również, że decyzje dotyczące zarządzania ryzykiem, na które narażone są dzieci, powinny opierać się na ocenie skutków przetwarzania dla ochrony danych osobowych.
Aby zrealizować ocenę skutków dla ochrony danych, należy przestrzegać m.in. zasady minimalizacji danych, a w przypadku weryfikacji wieku system nie musi weryfikować konkretnego wieku lub daty urodzenia, a jedynie przekroczenie progu wiekowego.

Źródło: komunikat hiszpańskiego organu ds. ochrony danych (AEPD)

Fot. pexels

IRLANDZKA KOMISJA OCHRONY DANYCH NAŁOŻYŁA NA META IRELAND GRZYWNĘ W WYSOKOŚCI 91 MILIONÓW EURO

Komisja Ochrony Danych (DPC) ogłosiła 27 września 2024 r. ostateczną decyzję w następstwie postępowania prowadzonego w sprawie Meta Platforms Ireland Limited (META). Postępowanie to zostało wszczęte w kwietniu 2019 r., po tym jak META powiadomiła DPC, że nieumyślnie przechowywała niektóre hasła użytkowników mediów społecznościowych w „zwykłym tekście" w swoich wewnętrznych systemach (tj. bez ochrony kryptograficznej lub szyfrowania).

W czerwcu 2024 r. DPC przedłożyła projekt decyzji pozostałym organom nadzorczym, których sprawa dotyczy w UE/EOG, zgodnie z wymogami art. 60 RODO. Pozostałe organy nie zgłosiły zastrzeżeń do projektu decyzji.

Decyzja, która została podjęta przez komisarzy ds. ochrony danych, dr Desa Hogana i Dale'a Sunderlanda, i przekazana do META obejmuje skierowanie upomnienia oraz nałożenie administracyjnej kary pieniężnej w wysokości 91 mln euro.

Decyzja DPC zawiera następujące ustalenia dotyczące naruszenia RODO:

• art. 33 ust. 1 RODO, ponieważ META nie powiadomiła DPC o naruszeniu ochrony danych osobowych dotyczącym przechowywania haseł użytkowników w postaci zwykłego tekstu;

• art. 33 ust. 5 RODO, ponieważ META nie udokumentowała naruszeń ochrony danych osobowych dotyczących przechowywania haseł użytkowników w postaci zwykłego tekstu;

• art. 5 ust. 1 lit. f) RODO, ponieważ META nie zastosowała odpowiednich środków technicznych lub organizacyjnych w celu zapewnienia odpowiedniego zabezpieczenia haseł użytkowników przed nieuprawnionym przetwarzaniem; oraz

• art. 32 ust. 1 RODO, ponieważ META nie wdrożyła odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka, w tym możliwości zapewnienia ciągłej poufności haseł użytkowników.

Zastępca komisarza w DPC, Graham Doyle, skomentował: „Powszechnie przyjmuje się, że hasła użytkowników nie powinny być przechowywane w postaci zwykłego tekstu, biorąc pod uwagę ryzyko nadużyć, które wynikają z dostępu osób do takich danych. Należy pamiętać, że hasła będące przedmiotem rozważań w tej sprawie są szczególnie wrażliwe, ponieważ umożliwiałyby dostęp do kont użytkowników w mediach społecznościowych".

6 SPRAWY MIĘDZYNARODOWE

Kontekst

W marcu 2019 r. META powiadomiła DPC, że nieumyślnie przechowywała niektóre hasła użytkowników mediów społecznościowych w „zwykłym tekście" w swoich wewnętrznych systemach (tj. bez ochrony kryptograficznej lub szyfrowania). META opublikowała również informacje dotyczące tego incydentu w marcu 2019 r. Hasła te nie zostały udostępnione podmiotom zewnętrznym.

Zakres postępowania, które rozpoczęło się w kwietniu 2019 r., obejmowało ocenę przestrzegania przez META ogólnego rozporządzenia o ochronie danych (RODO), a w szczególności tego, czy META wdrożyła środki zapewniające poziom bezpieczeństwa odpowiedni do ryzyka związanego z przetwarzaniem haseł oraz czy META wypełniła swoje obowiązki w zakresie dokumentowania i powiadamiania DPC o naruszeniach ochrony danych osobowych.

Decyzja DPC odnosi się do zasad RODO dotyczących integralności i poufności. RODO wymaga od administratorów danych wdrożenia odpowiednich środków bezpieczeństwa przy przetwarzaniu danych osobowych, biorąc pod uwagę takie czynniki jak ryzyko dla użytkowników usług oraz charakter przetwarzania danych. Aby utrzymać bezpieczeństwo, administratorzy danych powinni ocenić ryzyka związane z przetwarzaniem i wdrożyć środki w celu ich złagodzenia. Ta decyzja podkreśla konieczność podejmowania takich działań podczas przechowywania haseł użytkowników.

RODO wymaga również, aby administratorzy danych odpowiednio dokumentowali naruszenia danych osobowych oraz informowali organy ochrony danych o występujących naruszeniach. Naruszenie ochrony danych osobowych, jeśli nie zostanie rozwiązane w odpowiedni i terminowy sposób, może prowadzić do szkód, takich jak utrata kontroli nad danymi osobowymi. Dlatego, gdy administrator danych dowiaduje się, że doszło do naruszenia ochrony danych osobowych, powinien niezwłocznie powiadomić organ nadzorczy w sposób określony w artykule 33 RODO.

Decyzja zawiera następujące uprawnienia naprawcze:

1. upomnienie zgodnie z art. 58 ust. 2 lit. b) RODO; oraz

2. administracyjną karę pieniężną w łącznej wysokości 91 mln euro zgodnie z art. 58 ust. 2 lit. i) i art. 83 RODO.

Artykuł 60 RODO reguluje procedurę współpracy między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy.

Źródło: komunikat Irlandzkiej Komisji Ochrony Danych (DPC)

PIERWSZY PRZEGLĄD RAM OCHRONY PRYWATNOŚCI DANYCH UE-USA STWIERDZA, ŻE WŁADZE USA WDROŻYŁY ELEMENTY KONSTYTUTYWNE TYCH RAM

9 października 2024 r. Komisja Europejska opublikowała sprawozdanie po pierwszym przeglądzie decyzji stwierdzającej odpowiedni poziom ochrony w odniesieniu do ram ochrony prywatności danych UE-USA (DPF) dla danych osobowych przekazywanych z Unii Europejskiej do organizacji w USA.

Na podstawie informacji zebranych podczas przeglądu Komisja stwierdza, że władze USA wdrożyły wszystkie elementy konstytutywne ram. Obejmuje to wdrożenie **zabezpieczeń w celu ograniczenia dostępu do danych osobowych** przez amerykańskie organy wywiadowcze do tego, co jest konieczne i proporcjonalne do ochrony bezpieczeństwa narodowego, oraz ustanowienie niezależnego i bezstronnego mechanizmu dochodzenia roszczeń. Sprawozdanie zawiera również szereg **zaleceń** mających na celu zapewnienie dalszego skutecznego funkcjonowania ram, takich jak opracowanie wspólnych wytycznych między organami USA i organami ochrony danych UE w sprawie kluczowych wymogów DPF. Komisja będzie nadal monitorować rozwój sytuacji i okresowo składać sprawozdania na temat funkcjonowania ram.

Przegląd opiera się na wkładzie szerokiego grona podmiotów, w tym organizacji społeczeństwa obywatelskiego, stowarzyszeń handlowych, unijnych organów ochrony danych, organów amerykańskich zaangażowanych we wdrażanie ram, a także opinii publicznej za pośrednictwem portalu „Wyraź swoją opinię".

Sprawozdanie opiera się również na informacjach zebranych podczas spotkania przeglądowego w lipcu 2024 r. między komisarzem ds. sprawiedliwości Didierem Reyndersem, sekretarz handlu USA Giną Raimondo i ich ekspertami. W skład delegacji UE na spotkanie przeglądowe weszli przedstawiciele Komisji Europejskiej i Europejskiej Rady Ochrony Danych.

Więcej informacji na temat przekazywania danych między UE a USA można znaleźć na stronie Komisji Europejskiej.

Źródło: komunikat Komisji Europejskiej

KOMISJA PROPONUJE OPRACOWANIE APLIKACJI EU DIGITAL TRAVEL, KTÓRA UŁATWI BEZPIECZNE PODRÓŻOWANIE W STREFIE SCHENGEN

Komisja Europejska przyjęła 8 października 2024 r. dwa wnioski dotyczące cyfryzacji paszportów i dowodów osobistych oraz aplikacji „EU Digital Travel", używanych podczas podróży poza granice strefy Schengen.

Obywatele UE i obywatele państw trzecich podlegają systematycznej kontroli przy przekraczaniu granic zewnętrznych UE. Obecnie kontrole te przeprowadza się fizycznie na przejściu granicznym. **W samym 2023 r. granicę przekroczono 600 mln razy.** Konieczne jest przyspieszenie kontroli granicznych i ułatwienie życia podróżującym, przy jednoczesnym utrzymaniu wysokiego poziomu bezpieczeństwa i kontroli każdego podróżnego.

Komisja proponuje zatem **wspólne ramy korzystania z cyfrowych poświadczeń podróżnych** oraz nową aplikację **„EU Digital Travel"** umożliwiającą podróżnym tworzenie i przechowywanie cyfrowych poświadczeń podróżnych. Dzięki nowym przepisom podróżowanie do strefy Schengen i w strefie Schengen będzie **łatwiejsze i bezpieczniejsze.**

Nowe przepisy o cyfrowych paszportach i dowodach osobistych

Cyfrowe poświadczenia podróżne to cyfrowa wersja danych przechowywanych w paszportach i dowodach osobistych. Dane te obejmują informacje zawarte w mikroprocesorze paszportu lub dowodu osobistego, w tym wizerunek twarzy posiadacza, ale nie odciski palców. Cyfrowy dokument podróży można przechowywać na telefonie komórkowym. Podróżni będą mogli bezpłatnie uzyskać cyfrową wersję swoich dokumentów, a korzystanie z niej będzie dobrowolne.

Korzyści:

• **sprawniejsze i szybsze przekraczanie granicy**: przy wjeździe lub wyjeździe z UE zarówno obywatele unijni, jak i obywatele państw trzecich będą mogli przedkładać cyfrowe paszporty i dowody osobiste przed podróżą do wcześniejszej kontroli granicznej;

• **ułatwienie swobodnego przemieszczania się i zmniejszenie obciążeń administracyjnych dla obywateli UE:** państwa członkowskie mogą zezwolić obywatelom UE na korzystanie z cyfrowych

dowodów osobistych do celów rejestracji i identyfikacji. Przykładowo mogą one być wykorzystywane przy zameldowaniu się w innym państwie członkowskim lub w dostępie do systemów identyfikacji elektronicznej;

• **poprawa skuteczności kontroli granicznych:** służby graniczne będą mogły przeznaczyć czas i zasoby na wykrywanie przestępstw i przemytu migrantów dzięki możliwości wcześniejszej kontroli cyfrowych poświadczeń podróżnych;

• **poprawa bezpieczeństwa w strefie Schengen:** cyfrowe poświadczenia podróżne ułatwią służbom granicznym weryfikację autentyczności i integralności dokumentów podróży, co utrudni oszustom korzystanie z fałszywych dokumentów i nielegalne przekraczanie granic.

Aplikacja EU Digital Travel

Aplikacja EU Digital Travel zostanie przygotowana przez Komisję przy wsparciu eu-LISA i będzie dostępna w całej UE. Z aplikacji będą mogli korzystać wszyscy obywatele UE i obywatele państw trzecich, którzy mają paszport biometryczny lub unijny dowód osobisty i którzy wjeżdżają lub wyjeżdżają ze strefy Schengen.

Dzięki aplikacji EU Digital Travel podróżni będą mogli:

• tworzyć cyfrowe poświadczenia podróżne, korzystając z paszportów lub – w przypadku obywateli UE – z dowodów osobistych.

• z wyprzedzeniem przedkładać służbom granicznym plany podróży **i dokumenty**, co skróci czas oczekiwania na przejściach granicznych, ponieważ większość kontroli zostanie przeprowadzona wcześniej.

• **chronić swoje dane:** aplikacja wymaga zgody użytkownika na przetwarzanie danych osobowych. Ponadto państwa członkowskie będą zobowiązane do wyszkolenia służb granicznych w zakresie przepisów dotyczących bezpieczeństwa i ochrony danych przed udzieleniem im prawa dostępu do tych danych.

Aplikacja EU Digital Travel będzie dostępna od 2030 r. Umożliwi to przechowywanie cyfrowych poświadczeń podróżnych w europejskim portfelu tożsamości cyfrowej.

Co dalej?

Rada i Parlament Europejski muszą wyrazić zgodę na wnioski Komisji. Po ich przyjęciu zgodnie z odpowiednimi procedurami opracowana zostanie aplikacja EU Digital Travel oraz niezbędne normy techniczne.

6 SPRAWY MIĘDZYNARODOWE

Kontekst

Przyjęte przez Komisję wnioski są zgodne ze strategią Schengen przyjętą w 2021 r., w której zobowiązano się do dalszej cyfryzacji procedur na granicach zewnętrznych. Są one związane z powstaniem europejskich portfeli tożsamości cyfrowej, w których można będzie przechowywać cyfrowe paszporty i dowody osobiste wraz z cyfrowymi prawami jazdy, receptami lekarskimi i innymi dokumentami.

Inicjatywa stanowi wsparcie strategii Komisji „Cyfrowa Europa" i „cyfrowy kompas" w ramach celów cyfrowej dekady Europy, czyli cyfryzacji usług publicznych i zapewnienia wszystkim obywatelom Unii identyfikacji cyfrowej do 2030 r.

Więcej informacji:

Wniosek dotyczący rozporządzenia ustanawiającego aplikację do elektronicznego przedkładania danych (aplikacja EU Digital Travel)

Wniosek dotyczący rozporządzenia Rady ustanawiającego cyfrowe poświadczenie podróżne oparte na dowodzie osobistym

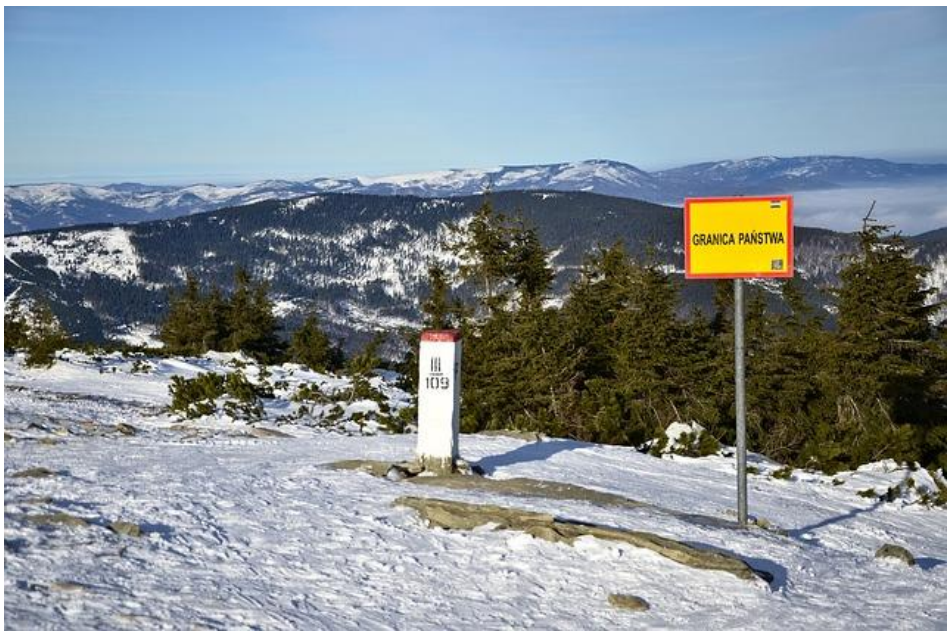
Bezpieczeństwo dokumentów – Komisja Europejska (europa.eu)

Swobodny przepływ i pobyt – Komisja Europejska (europa.eu)

Pytania i odpowiedzi dotyczące aplikacji EU Digital Travel

Zestawienie informacji o aplikacji EU Digital Travel

Źródło: komunikat Komisji Europejskiej



Fot. pixabay

KOMISJA EUROPEJSKA I KANADA PODPISUJĄ UMOWĘ O PRZEKAZYWANIU DANYCH DOTYCZĄCYCH PRZELOTU PASAŻERA

4 października 2024 r., przy okazji szczytu G7, komisarz Johansson podpisała umowę o przekazywaniu danych dotyczących przelotu pasażera (PNR) między UE a Kanadą, wraz z kanadyjskim ministrem bezpieczeństwa publicznego, instytucji demokratycznych i spraw międzyrządowych, Dominikiem Leblanc.

Dane PNR to informacje dostarczane przez pasażerów i gromadzone przez linie lotnicze w normalnym toku ich działalności. Ich wykorzystanie i analiza są niezbędnym narzędziem do walki z terroryzmem, poważną i zorganizowaną przestępczością, w tym handlem narkotykami i wykorzystywaniem dzieci.

Teraz Parlament Europejski i Rada muszą wyrazić zgodę przed zawarciem tej umowy. Gdy umowa zostanie zawarta i wejdzie w życie, pozwoli Kanadzie i państwom członkowskim UE na wymianę informacji o pasażerach przez przewoźników lotniczych operujących między nimi. Ta wymiana informacji wzmocni współpracę w zakresie egzekwowania prawa między UE a Kanadą. Jednocześnie nowa umowa ustanawia wysokie standardy bezpieczeństwa, prywatności i ochrony danych.

UE podpisała już umowy umożliwiające unijnym przewoźnikom przekazywanie danych PNR do Stanów Zjednoczonych i Australii. Umowa ta jest kolejnym krokiem w zobowiązaniu Komisji Europejskiej do wzmocnienia współpracy w zakresie egzekwowania prawa w oparciu o wspólne wartości praw podstawowych.

Źródło: Komisja Europejska

WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ W SPRAWIE C-768/21 TR PRZECIWKO LAND HESSEN

26 września 2024 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie C-768/21 TR przeciwko Land Hessen, w którym orzekł, że na organie nadzorczym nie spoczywa obowiązek wykonania uprawnień naprawczych, w tym zastosowania kary pieniężnej, w każdym przypadku naruszenia ochrony danych. Organ może odstąpić od wykonania uprawnień naprawczych, jeżeli administrator z własnej inicjatywy podjął już niezbędne środki.

W Niemczech pewna kasa oszczędnościowa stwierdziła, że jedna z jej pracownic uzyskała wielokrotny, nieuprawniony dostęp do danych osobowych jednego z klientów kasy. O fakcie tym kasa oszczędnościowa nie poinformowała klienta, ponieważ jej inspektor ochrony danych uznał, że nie istniało wysokie ryzyko naruszenia praw klienta. Odpowiedzialna pracownica potwierdziła bowiem na piśmie, że nie skopiowała ani nie przechowywała danych, że nie przekazała ich osobom trzecim oraz że nie zrobi tego w przyszłości. Ponadto kasa oszczędnościowa wyciągnęła wobec niej konsekwencje dyscyplinarne. Kasa oszczędnościowa powiadomiła jednak o rzeczonym naruszeniu inspektora ochrony danych kraju związkowego Hesji.

Po tym, jak klient przypadkowo dowiedział się o tym fakcie, złożył skargę do tegoż inspektora ochrony danych. Po wysłuchaniu kasy oszczędnościowej inspektor ochrony danych poinformował klienta, że nie uważa za konieczne wykonywania jakichkolwiek uprawnień naprawczych względem kasy oszczędnościowej. Klient wniósł następnie powództwo do sądu niemieckiego, żądając nakazania inspektorowi ochrony danych wykonania uprawnień naprawczych względem kasy oszczędnościowej, w szczególności zastosowania kary pieniężnej.

Sąd niemiecki zwrócił się do Trybunału Sprawiedliwości o dokonanie wykładni ogólnego rozporządzenia o ochronie danych (RODO) w tym zakresie.

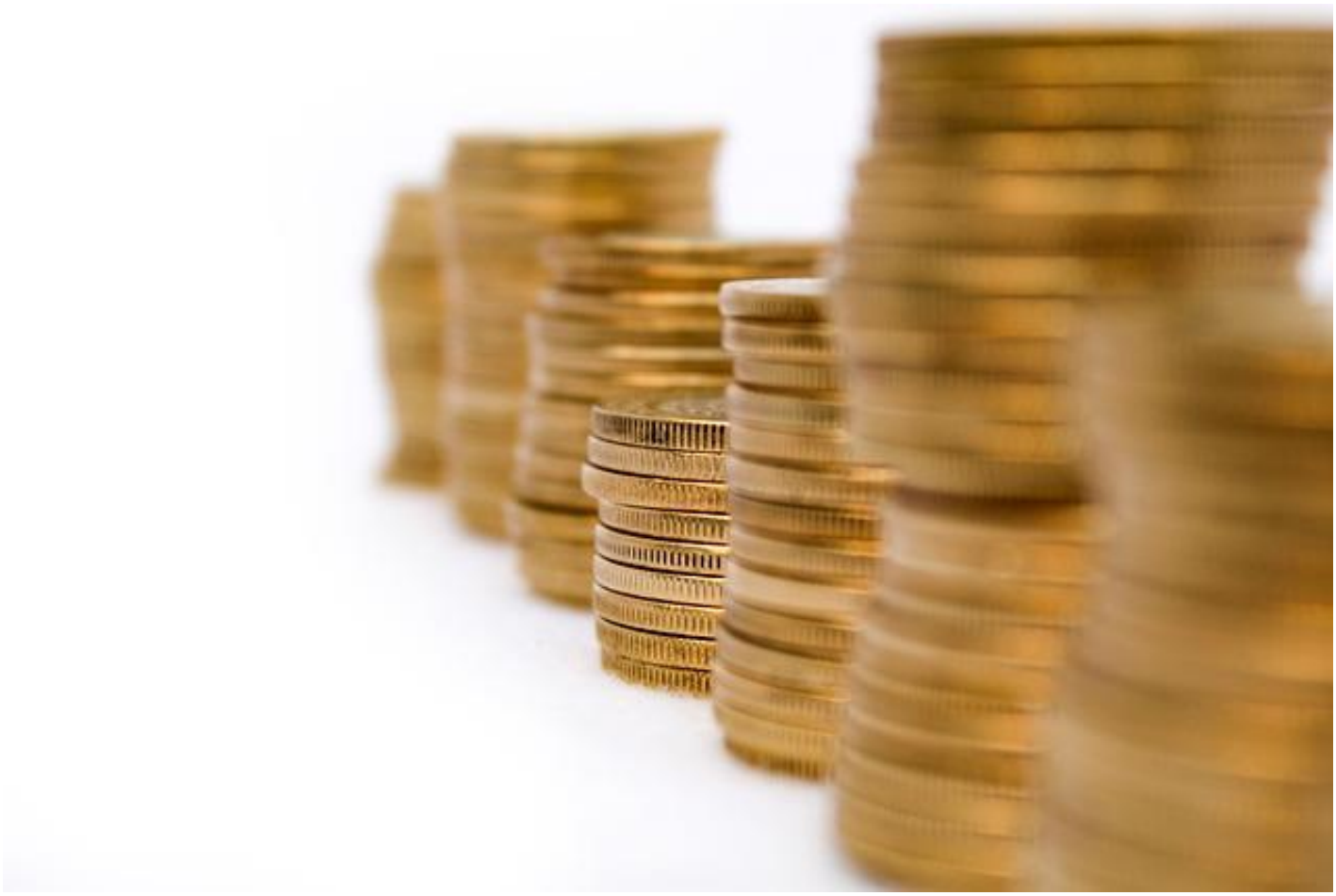
Trybunał odpowiedział, że w przypadku stwierdzenia naruszenia ochrony danych osobowych na organie nadzorczym (w niniejszym przypadku inspektorze ochrony danych kraju związkowego) nie spoczywa obowiązek wykonania uprawnienia naprawczego (organ nadzorczy może w szczególności udzielić upomnienia administratorowi, nakazać mu spełnienie żądania osoby, której dane dotyczą lub dostosować operacje przetwarzania do przepisów RODO lub wreszcie zastosować,

,oprócz lub zamiast tych środków, administracyjną karę pieniężną), w szczególności zastosowania administracyjnej kary pieniężnej, **jeżeli takie działanie nie jest odpowiednie, niezbędne lub proporcjonalne do usunięcia stwierdzonego uchybienia i zapewnienia pełnego przestrzegania RODO.** Może to mieć miejsce w szczególności w przypadku, gdy administrator danych, po powzięciu wiadomości o naruszeniu, podjął niezbędne działania w celu zapewnienia, że naruszenie ustanie i się nie powtórzy.

RODO pozostawia organowi nadzorczemu zakres uznania co do sposobu, w jaki powinien on usunąć stwierdzone uchybienie. Ten zakres uznania jest jednak ograniczony koniecznością zapewnienia spójnego i wysokiego stopnia ochrony danych osobowych poprzez rygorystyczne stosowanie przepisów RODO.

Do sądu niemieckiego należy zbadanie, czy inspektor ochrony danych przestrzegał tych granic.

Tekst wyroku w języku polskim dostępny jest na stronie TSUE.



Fot. pixabay

WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ W SPRAWIE C-446/21 SCHREMS

4 października 2024 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie C-446/21 Schrems, w którym orzekł, że internetowa sieć społecznościowa Facebook nie może wykorzystywać, bezterminowo i bez uwzględnienia ich charakteru, wszystkich danych osobowych pozyskanych do celów ukierunkowanej reklamy.

Okoliczność, iż Maximilian Schrems wypowiedział się na temat swojej orientacji seksualnej w trakcie dyskusji panelowej, nie upoważnia operatora platformy internetowej sieci społecznościowej do przetwarzania innych danych dotyczących jego orientacji seksualnej, pozyskanych w danym wypadku poza tą platformą w celu ich agregacji i analizy, służących kierowaniu do niego zindywidualizowanych reklam.

Maximilian Schrems zakwestionował przed austriackimi sądami przetwarzanie, w jego opinii niezgodne z prawem, jego danych osobowych przez spółkę Meta Platforms Ireland w ramach internetowej sieci społecznościowej Facebook. Konkretnie miał na myśli dane dotyczące jego orientacji seksualnej.

Meta Platforms Ireland gromadzi dane osobowe użytkowników Facebooka, w tym M. Schremsa, dotyczące ich aktywności zarówno w ramach tej sieci społecznościowej, jak i poza nią. Chodzi w szczególności o dane dotyczące przeglądania platformy internetowej, jak i stron internetowych oraz aplikacji podmiotów zewnętrznych. W tym celu Meta Platform korzysta z plików „cookies", „wtyczek społecznościowych" oraz „pikseli" umieszczanych na odnośnych stronach internetowych.

W świetle informacji, którymi dysponuje M. Schrems, Meta Platforms Ireland ma również możliwość pozyskiwania informacji na temat jego zainteresowań tematami wrażliwymi, takimi jak orientacja seksualna, dzięki czemu może ona kierować do niego ukierunkowane reklamy dotyczące tej tematyki. Nasuwa się zatem pytanie, czy skoro M. Schrems jednoznacznie podał swoje wrażliwe dane osobowe do wiadomości publicznej, wypowiadając się na temat swojej orientacji homoseksualnej w trakcie dyskusji panelowej, tym samym zgodził się na ich przetwarzanie na podstawie przepisów ogólnego rozporządzenie o ochronie danych (RODO).

W tym kontekście austriacki sąd najwyższy zwrócił się do Trybunału Sprawiedliwości o dokonanie wykładni RODO.

Trybunał odpowiedział, po pierwsze, że przewidziana w RODO **zasada „minimalizacji danych" stoi na przeszkodzie temu, by wszystkie dane osobowe**, które zostały pozyskane przez administratora danych takiego jak operator platformy internetowej sieci społecznościowej od osoby, której dane dotyczą, lub od podmiotów zewnętrznych, które zostały zebrane zarówno na tej platformie, jak i poza nią, **były bezterminowo i bez względu na charakter tych danych agregowane, analizowane i przetwarzane do celów ukierunkowanej reklamy.**

Po drugie, w ocenie Trybunału nie można wykluczyć, że wskutek swojej wypowiedzi, która padła w trakcie panelu dyskusyjnego M. Schrems jednoznacznie podał swoją orientację seksualną do wiadomości publicznej. Dokonanie stosownych ustaleń w tym względzie należy do austriackiego sądu najwyższego.

Okoliczność, że osoba, której dane dotyczą, w sposób oczywisty upubliczniła dane dotyczące swojej orientacji seksualnej, skutkuje tym, że dane te mogą być przetwarzane w drodze odstępstwa od zakazu przewidzianego w art. 9 ust. 1 RODO. Jednakże sama ta okoliczność nie pozwala na przetwarzanie innych danych osobowych dotyczących orientacji seksualnej tej osoby.

W związku z tym okoliczność, iż dana osoba wypowiedziała się na temat swojej orientacji seksualnej w trakcie dyskusji panelowej nie upoważnia operatora platformy internetowej sieci społecznościowej do przetwarzania innych danych dotyczących orientacji seksualnej tej osoby, pozyskanych w danym wypadku poza tą platformą za pośrednictwem aplikacji i stron internetowych podmiotów zewnętrznych w celu ich agregacji i analizy służących kierowaniu do niego zindywidualizowanej reklamy.

Tekst wyroku w języku polskim dostępny jest na stronie TSUE.

WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ W SPRAWIE C-21/23 LINDENAPOTHEKE

4 października 2024 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie C-21/23 Lindenapotheke, w którym orzekł, że państwa członkowskie mogą przewidzieć możliwość kwestionowania przed sądem naruszenia ochrony danych osobowych jako zakazanej nieuczciwej praktyki handlowej przez konkurentów domniemanego sprawcy tego naruszenia.

Sprzedaż przez internet leków zastrzeżonych dla aptek wymaga wyraźnej zgody klienta na przetwarzanie jego danych, nawet jeśli leki te dostępne są bez recepty.

Niemiecki federalny trybunał sprawiedliwości, który ma rozstrzygnąć spór między dwoma konkurującymi ze sobą farmaceutami, zwrócił się do Trybunału Sprawiedliwości UE o dokonanie wykładni RODO. **Trybunał stwierdził, że RODO nie stoi na przeszkodzie uregulowaniu krajowemu, które pozwala konkurentom domniemanego sprawcy naruszenia ochrony danych osobowych zakwestionować je przed sądem jako zakazaną nieuczciwą praktykę handlową.** Taka możliwość skorzystania ze środka prawnego przez konkurentów istnieje obok przewidzianych w RODO uprawnień interwencyjnych organów nadzorczych odpowiedzialnych za monitorowanie i egzekwowanie stosowania RODO, a także obok przewidzianych w tym rozporządzeniu możliwości dochodzenia roszczeń przez osoby, których dane dotyczą.

Ponadto Trybunał orzekł, że informacje podane przez klientów przy zamawianiu przez internet leków zastrzeżonych dla aptek stanowią dane dotyczące zdrowia w rozumieniu RODO, nawet jeśli sprzedaż tych leków nie wymaga recepty lekarskiej. W związku z tym sprzedawca musi informować tych klientów w sposób dokładny, pełny i łatwo zrozumiały o konkretnych cechach i celach przetwarzania tych danych oraz zwracać się do nich o wyraźne wyrażenie zgody na takie przetwarzanie.

Niemiecki federalny trybunał sprawiedliwości ma rozstrzygnąć spór między dwoma niemieckimi farmaceutami. Farmaceuta będący właścicielem apteki „Lindenapotheke” sprzedaje od 2017 r. na Amazonie leki, których sprzedaż jest zastrzeżona dla aptek. Klienci muszą podać szereg informacji przy zamawianiu tych leków przez internet.

6 SPRAWY MIĘDZYNARODOWE

Opierając się na niemieckich przepisach dotyczących nieuczciwych praktyk handlowych, farmaceuta będący konkurentem właściciela „Lindenapotheke" wniósł do sądu niemieckiego o nakazanie temu ostatniemu zaprzestania tej działalności do czasu zapewnienia klientom możliwości udzielenia uprzedniej zgody na przetwarzanie danych dotyczących zdrowia. Sądy w I i II instancji uznały, że ta sprzedaż faktycznie stanowi nieuczciwą i niedozwoloną praktykę, ponieważ jest sprzeczna z rozporządzeniem w sprawie ochrony danych osobowych (RODO). W przypadku braku wyraźnej zgody klientów kupujących produkty lecznicze sprzedaż prowadzi bowiem do przetwarzania danych dotyczących zdrowia zakazanego na podstawie tego rozporządzenia.

Niemiecki federalny trybunał sprawiedliwości zastanawia się, czy przepisy krajowe, które umożliwiają konkurentowi wystąpienie na drogę sądową przeciwko domniemanemu sprawcy naruszeń RODO na podstawie zakazu nieuczciwych praktyk handlowych, są zgodne z tym rozporządzeniem. Zgodnie z RODO, co do zasady, to do krajowych organów nadzorczych należy monitorowanie i egzekwowanie stosowania tego rozporządzenia, zaś do osób, których dane dotyczą (w tym przypadku klientów) – obrona ich praw. Sąd niemiecki chciałby również dowiedzieć się, czy informacje podane podczas kupowania leków przez internet, których sprzedaż jest zastrzeżona dla aptek, stanowią dane dotyczące zdrowia w rozumieniu RODO, nawet wtedy gdy leki te nie wymagają recepty lekarskiej. W związku z tym sąd ten zwrócił się do Trybunału Sprawiedliwości UE.

Trybunał odpowiedział w pierwszej kolejności, że **RODO nie stoi na przeszkodzie uregulowaniu krajowemu, które** – poza prawami i uprawnieniami przyznanymi w RODO krajowym organom nadzorczym, osobom, których dane dotyczą, i stowarzyszeniom reprezentującym te osoby – **pozwala konkurentom** domniemanego sprawcy naruszenia ochrony danych osobowych **wystąpić przeciwko niemu na drogę sądową ze względu na naruszenia tego rozporządzenia na podstawie zakazu nieuczciwych praktyk handlowych.** Wręcz przeciwnie, **przyczynia się to niezaprzeczalnie do wzmocnienia praw osób, których dane dotyczą,** i do zapewnienia im wysokiego poziomu ochrony. Ponadto może to okazać się **szczególnie skuteczne**, ponieważ w ten sposób **można by zapobiec dużej liczbie naruszeń RODO.**

W drugiej kolejności Trybunał uznał, że **informacje** (takie jak ich nazwisko, adres dostawy i dane niezbędne do jednoznacznego ustalenia leków) **podane przez klientów przy zamawianiu przez internet leków zastrzeżonych dla aptek stanowią dane dotyczące zdrowia w rozumieniu RODO, nawet jeśli sprzedaż tych leków nie wymaga recepty lekarskiej.**

Dane te umożliwiają bowiem ujawnienie – poprzez intelektualny proces kojarzenia lub dedukcji – informacji na temat stanu zdrowia zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, ponieważ następuje ustalenie związku między tą osobą a lekiem, wskazaniami

terapeutycznymi lub jego zastosowaniem, bez względu na to, czy informacje dotyczą klienta bądź dowolnej innej osoby, dla której dokonuje on zamówienia. Bez znaczenia jest zatem, że w braku recepty lekarskiej istnieje jedynie pewne prawdopodobieństwo, a nie absolutna pewność, że leki te są przeznaczone dla klientów, którzy je zamówili. Dokonywanie rozróżnienia w zależności od rodzaju produktów leczniczych oraz tego, czy ich sprzedaż wymaga czy też nie recepty lekarskiej, byłoby sprzeczne z celem RODO polegającym na zapewnieniu wysokiego poziomu ochrony.
W związku z tym sprzedawca musi informować tych klientów w sposób dokładny, pełny i łatwo zrozumiały o konkretnych cechach i celach przetwarzania owych danych oraz zwracać się do nich o wyraźne wyrażenie zgody na takie przetwarzanie.

Tekst wyroku dostępny jest na stronie TSUE.

Fot. pixabay

WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ W SPRAWIE C-548/21 BEZIRKSHAUPTMANNSCHAFT LANDECK

4 października 2024 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie C-548/21 Bezirkshauptmannschaft Landeck, w którym orzekł, że policja może uzyskać dostęp do danych zawartych w telefonie komórkowym nie tylko w ramach walki z poważną przestępczością. Uzyskanie tego dostępu jest jednak uwarunkowane wcześniejszym zezwoleniem sądu lub niezależnego organu, zaś sam dostęp musi być proporcjonalny.

Uzyskanie przez policję dostępu, w ramach postępowania przygotowawczego, do danych osobowych przechowywanych w telefonie komórkowym może stanowić poważną, a nawet szczególnie poważną ingerencję w prawa podstawowe osoby, której dane dotyczą. Możliwość uzyskania dostępu do tego rodzaju danych niekoniecznie jest ograniczona do walki z poważną przestępczością. Ustawodawca krajowy powinien określić elementy, które należy uwzględnić, aby uzyskać taki dostęp, jak np. charakter lub kategorie odnośnych przestępstw. W celu zapewnienia poszanowania zasady proporcjonalności w każdym konkretnym przypadku, należy rozważyć wszystkie istotne okoliczności danego przypadku. Możliwość uzyskania tego dostępu jest ponadto uzależniona od wcześniejszego zezwolenia sądu lub niezależnego organu, z wyjątkiem pilnych i należycie uzasadnionych przypadków. Osoba, której dane dotyczą, musi zostać powiadomiona o powodach udzielenia zezwolenia niezwłocznie po ustaleniu, że przekazanie takich informacji nie zagrozi prowadzonemu postępowaniu.

W trakcie kontroli na obecność narkotyków funkcjonariusze austriackiej policji zatrzymali telefon komórkowy adresata przesyłki po stwierdzeniu, że adresowana do niego paczka zawierała 85 gramów marihuany. Następnie funkcjonariusze policji bezskutecznie usiłowali odblokować telefon komórkowy w celu odczytania przechowywanych na nim danych. Próba odblokowania telefonu została podjęta bez nakazu prokuratury ani zezwolenia sądu, nie została odnotowana w protokole z przeprowadzanych czynności, zaś sam zainteresowany nie został o niej poinformowany.

Zainteresowany zakwestionował przed austriackim sądem zatrzymanie swojego telefonu komórkowego. Dopiero w ramach tego postępowania dowiedział się o próbach jego odblokowania. Austriacki sąd zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy uregulowanie austriackie,

które, jak utrzymuje, uprawnia funkcjonariuszy policji do podjęcia takich czynności, jest zgodne z prawem Unii. Sąd ten wskazuje, że przestępstwo zarzucane zainteresowanemu jest zagrożone karą pozbawienia wolności do jednego roku i w związku z tym stanowi jedynie występek.

Trybunał Sprawiedliwości na początku wyjaśnił, że wbrew temu, co twierdzą niektóre rządy, właściwe przepisy prawa Unii mają zastosowanie nie tylko w przypadku udanej próby dostępu do danych osobowych zawartych w telefonie komórkowym, lecz również w przypadku próby, która zakończyła się niepowodzeniem.

Trybunał stwierdził następnie, że uzyskanie dostępu do wszystkich danych zawartych w telefonie komórkowym może stanowić szczególnie poważną ingerencję w prawa podstawowe osoby, której dane dotyczą. Owe dane, które mogą obejmować wiadomości, zdjęcia i historię przeglądania internetu pozwalają w danym wypadku na wyciągnięcie bardzo precyzyjnych wniosków na temat życia prywatnego tej osoby. Ponadto mogą obejmować dane szczególnie wrażliwe.

Waga przestępstwa, w sprawie którego prowadzone jest postępowanie przygotowawcze stanowi jeden z kluczowych elementów oceny proporcjonalności tak poważnej ingerencji. **Jednakże uznanie, że jedynie walka z poważną przestępczością może uzasadniać dostęp do danych zawartych w telefonie komórkowym, niesłusznie ograniczyłoby uprawnienia dochodzeniowe właściwych organów. Mogłoby to doprowadzić do zwiększenia ryzyka bezkarności przestępstw w ujęciu ogólnym, a tym samym do podważenia procesu tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości w Unii.** Niemniej taka ingerencja w życie prywatne i ochronę danych musi być przewidziana ustawą, co oznacza, że **ustawodawca krajowy powinien określić w sposób wystarczająco precyzyjny elementy**, które należy wziąć pod uwagę, w szczególności **charakter lub kategorie rozpatrywanych przestępstw.**

Dostęp taki powinien być też uzależniony od uprzedniej kontroli dokonywanej albo przez sąd, albo przez niezależny organ administracyjny, z wyjątkiem pilnych i należycie uzasadnionych przypadków. Kontrola ta powinna zapewniać właściwą równowagę między uzasadnionymi interesami związanymi z potrzebami postępowania przygotowawczego w ramach zwalczania przestępczości z jednej strony a prawami podstawowymi do poszanowania życia prywatnego i ochrony danych osobowych z drugiej strony.

Wreszcie, osoba, której dane dotyczą, musi zostać powiadomiona o powodach udzielenia zezwolenia na uzyskanie dostępu do jej danych niezwłocznie po ustaleniu, że przekazanie takich informacji nie zagrozi prowadzonemu dochodzeniu.

Tekst wyroku dostępny jest na stronie TSUE.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl