URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 02/02/25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

w lutym w Urzędzie Ochrony Danych Osobowych wiele się działo. Szczególną Państwa uwagę chciałbym zwrócić na nową, zaktualizowaną **wersję poradnika dla administratorów, jak należy się zachować w przypadku stwierdzenia naruszenia ochrony danych osobowych.**

Nowa wersja „Poradnika dotyczącego naruszeń ochrony danych osobowych" uwzględnia najnowsze interpretacje przepisów, orzecznictwo oraz praktyczne wskazówki, które ułatwią administratorom podejmowanie właściwych decyzji w przypadku wystąpienia naruszenia ochrony danych osobowych. Ważną rolę w jego przygotowaniu odegrał Społeczny Zespół Ekspertów przy Prezesie Urzędu Ochrony Danych Osobowych, który wspierał doradczo Urząd w tworzeniu dokumentu.

W lutym Prezes UODO przyznał też po raz ósmy doroczną Nagrodę im. Michała Serzyckiego za działania na rzecz ochrony danych osobowych i prawa do prywatności. Miałem zaszczyt wyróżnić:

• **Katarzynę Szymielewicz, prezeskę Fundacji Panoptykon i samą Fundację** za wieloletnie działania na rzecz ochrony prywatności i wolności w erze cyfrowej,

• **dr. Konrada Ciesiołkiewicza za wkład w ochronę** przed niebezpieczeństwami czyhającym w sieci,

• **Helsińską Fundację Praw Człowieka** – za działania na rzecz ochrony praw człowieka, demokracji i praworządności w Polsce oraz Europie Środkowo-Wschodniej, jak również za eksperckie podejście do ochrony osób, których prawa zostały naruszone, oraz wspieranie rozwoju społeczeństwa obywatelskiego.

Wyzwania dla ochrony danych

UODO był współorganizatorem konferencji, podczas której zajmowaliśmy się wyzwaniami związanymi z ochroną danych osobowych i prawem do prywatności osób transpłciowych w związku z zatrudnieniem.

17 lutego spotkałem się z przedstawicielami ambasadorów państw Unii Europejskiej. Była to okazja do nawiązania relacji, których celem jest zwiększenie ochrony danych osobowych obywateli UE.

Jednym z problemów, z jakimi w Europie się mierzymy, jest technologia generatywnej sztucznej

inteligencji, wykorzystywana teraz także przez chiński, a więc niepodlegający unijnym regulacjom, chatbot DeepSeek. Biorąc pod uwagę informacje zamieszczone przez dostawcę tej usługi w jego polityce prywatności, zaleciliśmy daleko idącą ostrożność w korzystaniu z tej aplikacji oraz innych usług. Byliśmy pierwszym organem w Europie, który opublikował takie ostrzeżenie. Kontaktowaliśmy się też z innymi instytucjami i korzystały one z naszego komunikatu.

Nowe prawo

Jak co miesiąc przygotowaliśmy opinie i analizy do przygotowywanych przez rząd aktów prawnych. Jest wśród nich stanowisko PUODO w sprawie kamer nasobnych ratowników medycznych. Po głośnej sprawie zabójstwa ratownika, który został ugodzony nożem, kiedy udzielał pomocy, pojawił się pomysł, by poprawić bezpieczeństwo ratowników dzięki kamerom nasobnym rejestrującym zdarzenia. PUODO musi jednak zwrócić uwagę, że takie kamery rejestrowałyby mnóstwo informacji i danych osobowych, więc zasady ich użycia muszą być opisane w ustawie przygotowanej także na podstawie analizy ryzyka dla danych osobowych.

Zgłosiliśmy uwagi do projektu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029 oraz do monitoringu wizyjnego w placówkach medycznych.

W sądach

W lutym zapadły ważne dla ochrony danych osobowych wyroki sądowe.

NSA podtrzymał stanowisko PUODO w sprawie statusu ksiąg wieczystych jako zawierających dane osobowe, oddalając skargę kasacyjną Głównego Geodety Kraju. NSA w kolejnym wyroku podtrzymał zaś decyzję Prezesa UODO o nałożeniu 100 tys. zł kary pieniężnej w związku z uniemożliwianiem przez GGK przeprowadzenia kontroli przez pracowników UODO.

WSA w Warszawie podtrzymał też decyzję Prezesa UODO w sprawie dotyczącej przekazania bez podstawy prawnej danych naukowców z bazy POL-on Ministerstwu Zdrowia do analiz stopnia zaszczepienia przeciw COVID-19 na uczelniach.

NSA podtrzymał także stanowisko PUODO ws. kary dla SGGW. Sprawa dotyczyła naruszenia przez uczelnię obowiązków wynikających z przepisów o ochronie danych osobowych, w którego efekcie doszło do incydentu: dane osobowe kandydatów na studia zostały wyeksportowane na prywatny komputer pracownika, zaś na skutek kradzieży tego urządzenia została naruszona ich poufność.

NSA potwierdził również nasze stanowisko, że bank nie może przetwarzać danych osoby, której odmówił kredytu.

W końcu NSA zgodził się z Prezesem UODO, że wypytywanie pasażera autobusu o nazwisko to przetwarzanie danych. Sprawę zainicjowała skarga pasażera autobusu na to, że kierowca zażądał od niego podania na głos imienia i nazwiska. Nie wystarczyło mu pokazanie elektronicznego biletu. W ten sposób dane pasażera poznały inne osoby w autobusie, a nie było do tego podstaw.

WSA w Warszawie stanął tu na stanowisku, że sytuacja ta może naruszać dobra osobiste pasażera (więc może on złożyć pozew cywilny), jednak nie doszło do przetwarzania danych. NSA nie zgodził się z tym stanowiskiem WSA i przyznał rację Prezesowi UODO.

Złożyliśmy też do NSA skargę kasacyjną w niezwykle ważnej dla ochrony danych osobowych sprawie. Dotyczy ona naruszenia danych osobowych w wyniku dostarczenia uszkodzonej i niekompletnej przesyłki sądowej przez operatora pocztowego. WSA w Warszawie uznał, że jest to problem z zakresu sprawowania wymiaru sprawiedliwości, co oznacza, że nie może jej oceniać PUODO. W skardze kasacyjnej podtrzymujemy stanowisko: pozostawienie w obrocie prawnym tego wyroku WSA może doprowadzić do sytuacji, że osoby objęte podobnym naruszeniem danych pozostaną bez ochrony prawnej, zagwarantowanej m.in. przepisami Konstytucji RP.

***

Na końcu jak zwykle muszę Państwa poinformować o karach nakładanych przez PUODO. Robimy to tylko w sytuacjach, gdy jest to konieczne i niezbędne. Tym razem chodziło o opisywaną w mediach sprawę oddziału neonatologiczego, w którym zamontowano zegary z ukrytymi kamerami. A następnie zapis z tych kamer, rejestrujący wizerunki rodziców i dzieci, a także rozmowy rodziców, przepadł bez wieści. Po zbadaniu sprawy PUODO uznał, że ten monitoring wizyjny został wprowadzony niezgodnie z obowiązującymi przepisami, ponadto miał charakter niejawny – o prowadzonej rejestracji obrazu nie zostali poinformowani ani pacjenci, ani pracownicy placówki.

Dwie nałożone w tej sprawie kary wyniosły łącznie 1 145 891,25 zł.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W tym numerze przybliżamy Wam sylwetkę społeczniczki, od zawsze zaangażowanej w prawa obywatelskie. To Anna Grzelak, dyrektor utworzonego w ramach reorganizacji w UODO Departamentu Projektów Społecznych i Zrównoważonego Rozwoju. Z rozmowy dowiecie się m.in., czym zajmuje się nowo powstały departament, jakie są tegoroczne plany Urzędu na udział w kolejnej edycji Pol'and'Rock festiwal, a także akcji „UODO rusza w kraj" oraz co oznacza zrównoważony rozwój w przypadku UODO.

Czyim zadaniem jest dopełnianie obowiązku informacyjnego? Przypominamy, że choć jest to zadanie administratora, podmiot przetwarzający może wspierać go w jego realizacji. Jak to wygląda w szczegółach, dowiecie się z artykułu w dziale „UODO sygnalizuje".

UODO zdecydował się wydać upomnienie dla Wójta Gminy za krótkotrwałe udostępnienie danych obywatelki na BIP. Jak wyjaśnił Prezesowi UODO wójt, problem został spostrzeżony chwilę wcześniej i dane osobowe zostały usunięte z BIP na trzy minuty przed otrzymaniem pisma obywatelki.

W lutowym wydaniu „Biuletynu UODO" sporo miejsca poświęcamy strefie Schengen – piszemy o zaleceniach Schengen dla Polski w obszarze ochrony danych osobowych, przypominając, że przetwarzanie danych osobowych w Wielkoskalowych Systemach Informacyjnych Unii Europejskiej, w tym przetwarzanie danych osobowych SIS/VIS podlega kontroli sektorowej UODO, zgodnie z przyjętym przez Prezesa UODO planem na 2025 r. W odrębnym materiale informujemy, że 1 stycznia Rumunia i Bułgaria stały się pełnoprawnymi członkami strefy Schengen po zniesieniu kontroli osób na wewnętrznych granicach lądowych.

Podkreślamy, że edukacja użytkowników jest kluczowym elementem bezpieczeństwa danych w dobie nowych technologii. Ochrona danych osobowych w erze AI wymaga zrównoważonego podejścia łączącego solidne ramy regulacyjne, kompleksową edukację użytkowników i odpowiedzialne wdrażanie technologii.

Francuski organ nadzorczy (CNIL) publikuje swój plan strategiczny na lata 2025–2028. Koncentruje on swoje działania wokół czterech głównych osi stanowiących istotę rozwoju społeczeństwa cyfrowego: sztucznej inteligencji, ochrony nieletnich w internecie, cyberbezpieczeństwa oraz dwóch zastosowań cyfrowego życia codziennego: aplikacji mobilnych i tożsamości cyfrowej.

Europejska Rada Ochrony Danych podczas posiedzenia plenarnego w lutym 2025 r. przyjęła oświadczenie w sprawie gwarancji wieku i postanowiła utworzyć grupę zadaniową ds. egzekwowania sztucznej inteligencji. EROD przyjęła również zalecenia dotyczące Światowego Kodeksu Antydopingowego Światowej Agencji Antydopingowej (WADA) z 2027 r.

Jak zawsze dużo mówimy o ochronie danych w firmach, z których usług masowo korzystają ludzie na całym świecie. W tym miesiącu pod lupę bierzemy działania Netflixa oraz TikToka. Holenderski organ ochrony danych nałożył na Netflix grzywnę w wysokości 4,75 mln euro. Dochodzenie wykazało, że Netflix m.in. nie informował klientów wystarczająco jasno w swoim oświadczeniu o ochronie prywatności o tym, co dokładnie robi z ich danymi.

Z kolei Komisja Europejska wszczęła w grudniu 2024 r. formalne postępowanie przeciwko TikTokowi w związku z podejrzeniem naruszenia aktu o usługach cyfrowych z uwagi na obowiązek TikToka dotyczący właściwej oceny i ograniczenia ryzyka systemowego związanego z uczciwością wyborów, zwłaszcza w kontekście niedawnych wyborów prezydenckich w Rumunii w dniu 24 listopada.

Życzę miłej lektury!

Karol Witowski
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

JESTEŚMY ODPOWIEDZIALNI ZA EFEKTY NASZYCH DZIAŁAŃ WOBEC OBYWATELA

Z Anną Grzelak, dyrektor Departamentu Projektów Społecznych i Zrównoważonego Rozwoju rozmawiał Karol Witowski, Rzecznik Prasowy UODO.

Została Pani dyrektorką utworzonego w ramach reorganizacji w UODO Departamentu Projektów Społecznych i Zrównoważonego Rozwoju. Czym zajmuje się nowo powstały departament?

Departament Projektów Społecznych i Zrównoważonego Rozwoju powstał, ponieważ Prezes Urzędu widzi bardzo dużą potrzebę powszechnego dostępu do wiedzy z zakresu ochrony danych osobowych dla wszystkich obywateli i lepszego powszechnego rozumienia przepisów prawa związanych z ochroną danych. Bezpieczeństwo obywatela i jego danych jest dla nas kluczowe.

Naszym zadaniem jest poszerzanie współpracy z interesariuszami – nawiązywanie tej współpracy i poszukiwanie jej nowych form, bo przecież ochrona danych dotyczy każdego z nas, każdego obywatela, każdej obywatelki. Prowadzimy analizę potrzeb poszczególnych grup społecznych i zawodowych w zakresie ochrony danych, aby móc w sposób najbardziej dopasowany opracować zakres i model projektów.

Będziemy obecni wszędzie tam, gdzie możemy szerzyć wiedzę i pomagać w zrozumieniu treści rozporządzenia regulującego kwestie ochrony danych osobowych, ale też, aby pomóc obywatelom zastosować jego zapisy. Będziemy pracowali nad stworzeniem praktycznych wskazówek jak zabezpieczać dane np. przy zakupach internetowych, jak pracować podczas podróży, jak chronić wizerunek swój oraz dzieci itd. Ale to na czym zależy nam najbardziej, to szerokie rozumienie po co chronimy dane osobowe i jakie mogą być skutki ich szerokiego rozpowszechniania.

Planujemy być też obecni na festiwalach i imprezach publicznych, gdzie każdy obywatel będzie mógł przyjść i porozmawiać z naszymi ekspertami, rozwiać swoje wątpliwości, skorzystać z materiałów edukacyjnych.

Pracowała Pani w Biurze Rzecznika Praw Obywatelskich. Zajmowała się tam Pani m.in. organizacją i koordynacją wydarzeń, koordynacją prac zespołów projektowych, utrzymywaniem zrównoważonego rozwoju, budowaniem i utrzymywaniem pozytywnych relacji z interesariuszami Biura RPO, relacjonowaniem wydarzeń,

1 ROZMOWA Z EKSPERTEM

koordynacją i prowadzeniem konkursów czy inicjowaniem kampanii społecznych… Zadania, za które była Pani odpowiedzialna można by długo wymieniać. Jak to doświadczenie przekłada się na Pani pracę w UODO?

Praca w Biurze Rzecznika Praw Obywatelskich to niezwykłe doświadczenie, które, mam wrażenie, mnie ukształtowało – zarówno mój system wartości, wrażliwość czy spojrzenie na problemy społeczne. Myślę, że to w dużej mierze dzięki temu patrzę na człowieka, a nie na sprawę. Wydarzenia, kampanie, w których miałam swój udział służyły temu, aby prowadzić dialog celem rozwiązania problemów społecznych. I to, co zawsze mną kierowało, to to, że osoby, których temat dotyczy muszą być częścią tego dialogu. A obszar tych działań był niezwykle szeroki.

Ważne też jest, aby dostosowywać język i narzędzia do potrzeb osób, do których projekty są kierowane, szczególnie poprzez wykorzystanie nowych możliwości technologicznych, ale też zmieniającego się otoczenia informacyjnego i cywilizacyjnego. Myślę, że to są doświadczenia, które mogą być pomocne w UODO m.in. przy rozwijaniu działań odpowiadających na potrzeby interesariuszy. Bo przecież ochrona danych dotyczy każdego z nas, obejmuje wszystkich.

Prezes UODO deklarował udział UODO w kolejnej edycji Pol'and'Rock festiwal. Czy może to Pani potwierdzić i zdradzić część pomysłów na udział Urzędu w tym wydarzeniu?

Zdecydowanie tak. To jest jedna z form realizacji dostępu do wiedzy i potrzeb obywateli. Festiwale są do tego wyśmienitą okazją. Ten akurat festiwal jest ogólnodostępny, jest bezpłatny i wszyscy mogą tam być. A strefa organizacji pozarządowych, instytucji, urzędów dla obywateli jest niezwykle ciekawa, aby szerzyć wiedzę na temat praw obywateli, obowiązków Państwa wobec obywateli i nawiązywać relacje i współpracę.

Zdradzić mogę jedynie, że każda z osób, która odwiedzi nasz namiot uzyska informację i pomoc w zakresie prawa do ochrony danych, uzyska wiedzę o tym, jak w tym nowoczesnym świecie – nowych technologii, aplikacji komputerowych, edukacji cyfrowej – dbać o swoje bezpieczeństwo i zabezpieczać swoje dane. Będziemy na pewno rozmawiać o ochronie wizerunku, monitoringu i innych ważnych obszarach, w których żyjemy na co dzień. Więcej nie mogę zdradzić, ale bardzo serdecznie zapraszamy do udziału, bo to naprawdę unikatowe wydarzenie.

Koordynuje Pani regionalne działania w ramach akcji „UODO rusza w kraj". Jakie są plany i założenia projektu na ten rok?

1 ROZMOWA Z EKSPERTEM

W 2025 będziemy kontynuowali projekt „UODO rusza w kraj”, w ramach którego odwiedzimy kolejne województwa. W trakcie spotkań będziemy się starali przybliżać problematykę ochrony danych oraz pracę Urzędu Ochrony Danych Osobowych mieszkańcom Polski.

W czasie trwania projektu spotykamy się z przedstawicielami jednostek samorządu terytorialnego, bo to właśnie oni są najbliżej obywatela. Rozmawiamy również z uczniami, seniorami, przedsiębiorcami oraz społecznością lokalną. Podczas tych spotkań pracownicy UODO mogą lepiej zidentyfikować zagadnienia, charakterystyczne dla odwiedzanych regionów, oferujemy również porady prawne z zakresu ochrony danych osobowych, których udzielają specjaliści na co dzień pracujący w infolinii UODO. Jest to możliwość, by twarzą w twarz z ekspertem Urzędu skonsultować swój problem czy rozwiać wątpliwości dotyczące ochrony danych.

Na ten rok zaplanowaliśmy spotkania w województwach: podkarpackim (Rzeszów), świętokrzyskim (Kielce), lubuskim (Gorzów Wielkopolski), wielkopolskim (Poznań), mazowieckim (Płock), kujawsko-pomorskim (Bydgoszcz), zachodniopomorskim (Szczecin), warmińsko-mazurskim (Olsztyn).

Departament Projektów Społecznych i Zrównoważonego Rozwoju zajmuje się także rozwojem współpracy m.in. z organizacjami pozarządowymi oraz środowiskami społecznymi. Jakie działania będziecie w tym zakresie podejmować?

Moje wcześniejsze doświadczenia zawodowe, ale też te z mojej osobistej działalności społecznej zaowocowały znajomością wielu środowisk społecznych i ludzi o podobnych celach i wartościach. Organizacje pozarządowe, a raczej szerzej społeczeństwo obywatelskie znają bardzo dobrze problemy swoich interesariuszy od strony praktycznej. Wiedzą, z czym mierzą się ludzie w różnych obszarach życia społecznego, w tym również w obszarze bezpieczeństwa i ochrony danych. Wspólnie będziemy podejmować działania, aby je rozpoznać, znaleźć przyczyny i poszukać rozwiązań – prawnych, społecznych.

Nasze zadanie to połączenie potrzeb środowisk różnych grup społecznych z wiedzą naszych ekspertów, celem zabezpieczenia danych obywateli reprezentujących różne grupy społeczne.

Będziemy współpracować ze wszystkimi departamentami urzędu. Mamy tu fantastycznych ekspertów, którzy już wykonali i codziennie wykonują wielką pracę edukacyjną i świadomościową. Prowadzą szkolenia, spotkania, tworzą programy edukacyjne. To, co chcemy osiągnąć, to szeroki dostęp do tej wiedzy dla każdego obywatela.

My będziemy wspierać ekspertów w szerzeniu tej wiedzy, aby trafiała do możliwie najszerszej grupy obywateli, szczególnie tych, którzy jej potrzebują najbardziej. Wspólnie będziemy rozwijać działania świadomościowe, szerzyć wiedzę o tym jak odpowiedzialnie i etycznie przetwarzać dane, zarówno w kontekście indywidualnym, jak i instytucjonalnym, tworzyć platformy wymiany doświadczeń dla

środowisk organizacji i ekspertów.

A powszechny dostęp do zasobów urzędu i wiedzy naszych ekspertów to jeden z obszarów zrównoważonego rozwoju.

Co oznacza zrównoważony rozwój w przypadku UODO?

Kilka tysięcy wpływających spraw rocznie sprawia, że UODO ma dość szeroki obraz problemów w zakresie ochrony danych oraz sytuacji, w których dochodzi do naruszeń w tym zakresie.

Bycie odpowiedzialnym za obecne i przyszłe pokolenia oznacza inwestowanie w zasoby ludzkie, w ochronę środowiska, relacje z otoczeniem, a jednocześnie informowanie o tych działaniach. Przyczynia się to do szerzenia dobrych praktyk i kształtowania warunków dla zrównoważonego rozwoju społecznego i ekonomicznego zarówno w zakresie realizacji ustawowych zadań urzędu, jak i kształtując wewnętrzne środowisko i strategie. Rozwój nowych technologii ma tu niebagatelne znaczenie. Zarówno ze względu na wpływ środowiskowy, ale również na człowieka i jego bezpieczeństwo. Dlatego będziemy wdrażać standardy zrównoważonego rozwoju w codziennej działalności. Ale tak jak wspomniałam, zależy nam, aby wiedza i doświadczenie naszych ekspertów były dostępne dla wszystkich obywateli. We wszystkim co robimy, jesteśmy odpowiedzialni za efekty naszych działań wobec obywatela.

Zajmiemy się opracowaniem, wdrożeniem i realizacją strategii zrównoważonego rozwoju, opierającej się na wartościach naszego urzędu i jego pracowników, uwzględniając wrażliwość społeczną, dbałość o środowisko naturalne w świecie coraz bardziej narażonym na działalność człowieka.

Pracując na początek nad obszarem ładu organizacyjnego staramy się opierać na wartościach, kierunku myślenia, jaki przyświeca pracownikom przy realizacji swoich codziennych obowiązków w obszarach działalności urzędu. Takie podejście posłuży poprawie efektywności zarządzania z uwzględnieniem interesu społecznego, wzajemnego poszanowania oraz zasad etycznych.

Czym jest wellbeing w miejscu pracy i jak go dobrze wdrożyć ? To jedno z zagadnień, którymi ma się Pani zajmować w UODO.

W sposób naturalny funkcjonowanie UODO opiera się na przyjętych wartościach oraz uwzględnienia w swoich działaniach zasady zrównoważonego rozwoju.

Tworzenie przyjaznego środowiska pracy ma ogromny wpływ na efekty naszych działań wobec obywatela.

Będziemy starali się tworzyć coraz bardziej przyjazne środowisko pracy, wolne od dyskryminacji, nierówności, zintegrowane, tworzące silny, sprawiedliwy i przyjazny urząd.

Dzięki temu, że posiadamy pracowników w każdym wieku i z różnym doświadczeniem możemy uczyć

się od siebie wzajemnie. Osoby posiadające długi staż pracy mogą przekazywać swoją wiedzę i umiejętności nowym pracownikom, a grupa osób ze znacznie krótszym stażem pracy może wnieść świeże spojrzenie na wiele spraw, zaproponować nowe, może prostsze, „szybsze" rozwiązanie.

Będziemy starali się włączać pracowników w procesy decyzyjne. Bo przecież NIC O NAS BEZ NAS.

Badamy obszary, w których należy podjąć działania mogące usprawnić pracę zespołu UODO. Po ich zidentyfikowaniu podejmiemy działania wdrożeniowe.

Jednym z naszych głównych celów jest stworzenie środowiska pracy zapewniającego work-life-balance oraz możliwości rozwoju i edukacji, aby życie prywatne i zawodowe pracowników tworzyły spójną całość, w zgodzie z systemem wartości organizacji.

Dlatego podejmiemy szereg działań, aby to było możliwe. Jesteśmy przekonani, że dzięki takim działaniom możemy zwiększać efektywność pracowników oraz zapewnić im większą satysfakcję z pracy.

Przyjście do Urzędu prof. Grzelak (zbieżność nazwisk przypadkowa) i pojawienie się feminatywów w języku komunikacji UODO zbiegło się z coraz bardziej widocznym podkreślaniem w mainstreamie wagi głosu kobiet. Domyślam się, że temat jest Pani bliski, chociażby dlatego, że jest Pani częścią Vital Voices Polska, której misją jest inwestowanie w kobiety o potencjale przywódczym w Polsce, Europie i Azji. Przybliżmy czytelnikom – „Vital Voices zajmuje się organizacją spotkań kobiet, które chcą osiągnąć więcej (Mentees) z osobami, które już osiągnęły wiele i dzielą się swoim doświadczeniem (Mentorzy)".

Temat jest mi bardzo bliski. Zaczyna się od języka. Używanie feminatywów ma na celu zwiększenie równości płci, budowanie środowiska bardziej inkluzywnego. Kobiety w różnych dziedzinach życia społecznego spotykają się nadal z nierównościami i dyskryminacją. Sytuacja oczywiście się poprawia, ale nadal chociażby na rynku pracy mamy do czynienia np. z luką płacową czy doświadczaniem dyskryminacji w związku z życiem rodzinnym.

Dlatego są mi bliskie inicjatywy, które wspierają kobiety w przezwyciężaniu trudności, a także zapewnieniu wzajemnego wsparcia. Vital Voices Polska to jedna z nich. Miałam niezwykłą przyjemność brać udział w programie mentoringowym organizowanym przez fundację. To był bardzo intensywny czas nauki – zajęć praktycznych, warsztatów i wykładów, spotkań z liderkami biznesu, polityki, przedsiębiorczości, jak również spotkań networkingowych. Było to dla mnie ważne doświadczenie, ale też duża możliwość pracy rozwojowej. Teraz już w roli mentorki mogę oddać to, co otrzymałam, tą siłę do działania na wielu obszarach.

Ale to nie jedyna inicjatywa, która jest mi bardzo bliska. Staram się wspierać również inne. Bardzo ważna jest dla mnie inicjatywa Kobiety w Centrum. Służąca inspirowaniu, dodawaniu odwagi, poczucia bezpieczeństwa i pewności siebie, tak aby kobiety na żadnym etapie swojego życia nie musiały z czegoś rezygnować. Kobiety wspierają się wzajemnie i pomagają sobie zarówno w sprawach zawodowych i życiowych.

Miałam też wielką przyjemność współpracować z Erą Nowych Kobiet.

Wszystkie te inicjatywy, jak i wiele innych pomagają nam zmniejszać nierówności płci i pracować nad poprawą jakości życia kobiet w Polsce.

Co może Pani nam o sobie powiedzieć, co pozwoli nam lepiej Panią poznać?

Jak wspomniałam na początku doświadczenie pracy zawodowej, ale też życiowe, pozwala mi działać na wielu polach. Śmiało mogę o sobie powiedzieć, że jestem typem nowoczesnego (na pewno niestereotypowego) urzędnika. Jestem otwarta na wszelkie nowości, współpracę z różnymi środowiskami bez uprzedzeń czy tworzenia niepotrzebnych barier.

Jestem też społecznikiem. Staram się być aktywna w działaniach na rzecz rozwiązywania problemów lokalnej społeczności i tworzenia przyjaznego otoczenia. Działam w obszarze edukacji, wspierając rodziców i szkoły w osiąganiu coraz to nowych celów. Rozwiązuję również problemy wynikające ze zmieniających się warunków cywilizacyjno-rozwojowych. To właśnie środowiska lokalne namówiły mnie do udziału w wyborach samorządowych, gdzie jako kandydatka społeczna zdobyłam mandat do Rady Dzielnicy Wola. Dzięki temu mogę mieć wpływ na kształtowanie naszej najbliższej rzeczywistości, ale też pomagać mieszkańcom w rozwiązywaniu ich problemów lokalnych, poprawiać jakość naszego wspólnego życia. To daje ogromną satysfakcję.

Ale równie ważne jest dla mnie życie rodzinne, które staram się bardzo mocno pielęgnować.

A swoim dzieciom chciałabym przekazać między innymi jakie wartości mi przyświecają w działalności zarówno zawodowej, jak i społecznej.

Dziękuję za rozmowę.

CZYIM ZADANIEM JEST DOPEŁNIANIE OBOWIĄZKU INFORMACYJNEGO?

Choć dopełnianie obowiązku informacyjnego to zadanie administratora, podmiot przetwarzający może wspierać go w jego realizacji. Jednak musi przy tym działać na wyraźne polecenie i zgodnie z instrukcjami administratora. Administrator musi zaś mieć pełną kontrolę nad treścią i zakresem obowiązku informacyjnego.

Takie stanowisko UODO przedstawił w odpowiedzi na pytanie jednego z inspektorów ochrony danych (IOD). Dotyczyło ono możliwości realizacji obowiązku informacyjnego przez podmiot przetwarzający działający na upoważnienie i pod kontrolą administratora.

UODO wskazał, że zgodnie z art. 13 i 14 RODO administrator udziela osobie, której dane dotyczą, wymienionych w tych przepisach informacji na temat przetwarzania jej danych osobowych. Wskazane przepisy nie wymieniają podmiotu przetwarzającego jako właściwego do spełnienia obowiązku informacyjnego. Ponadto językowa wykładnia tego przepisu sugeruje, że obowiązek ten spoczywa wyłącznie na administratorze.

Warto też zwrócić uwagę na zadania podmiotu przetwarzającego wymienione w art. 28 ust. 3 jako elementy obligatoryjne umowy powierzenia przetwarzania. Przepis ten nie wymienia wśród nich realizacji praw osoby, której dane dotyczą, w tym spełnienia obowiązku informacyjnego.

Wytyczne Grupy Roboczej art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679 (GR260 rev.01), w których szczegółowo omówiono problematykę obowiązku informacyjnego na podstawie art. 13 i 14 RODO (sekcja „Informacje udzielane osobie, której dane dotyczą – art. 13 i 14”), również nie odnoszą się do możliwości spełnienia obowiązku informacyjnego przez podmiot przetwarzający, a wszelkie zawarte w wytycznych wskazówki dotyczące tego zagadnienia odnoszą się do administratora.

Wobec powyższego administrator powinien mieć pełną kontrolę nad treścią klauzuli informacyjnej, a podmiot przetwarzający, wspierając administratora w realizacji jego obowiązków, może jedynie działać zgodnie z instrukcjami administratora. Niemniej może on – działając na wyraźne polecenie i zgodnie z instrukcjami administratora – wspierać go w realizacji obowiązku informacyjnego, przekazując treść tego obowiązku osobom, których dane dotyczą.

UPOMNIENIE DLA WÓJTA GMINY W. ZA KRÓTKOTRWAŁE UDOSTĘPNIENIE DANYCH OBYWATELKI NA BIP

Dane te znalazły się w załączniku do uchwały Rady Gminy. Było to imię, nazwisko oraz adres zamieszkania. Skargę na to złożyła do Prezesa UODO osoba, której dane zostały ujawnione.

Osoba ta zaskarżyła wcześniej do WSA akt prawa miejscowego (zmianę Regulaminu utrzymania czystości i porządku w gminie). Sąd przesłał tę skargę do Rady Gminy, by ta zajęła stanowisko w sprawie. Rada przyjęła uchwałę o udzieleniu odpowiedzi sądowi. Załącznikiem do niej była właśnie ta odpowiedź. I tam były dane skarżącej – dokument przy publikacji na stronie Biuletynu Informacji Publicznej Urzędu nie został zanonimizowany.

27 minut po tym, jak dane pojawiły się na BIP, skarżąca złożyła pismo, w którym domagała się usunięcia swoich danych. Jak wyjaśnił Prezesowi UODO wójt W., problem został spostrzeżony chwilę wcześniej i dane osobowe zostały usunięte z BIP na trzy minuty przed otrzymaniem pisma obywatelki. Wójt, zgodnie z przepisami RODO, poinformował skarżącą o naruszeniu jej danych osobowych oraz o usunięciu jej danych osobowych ze strony BIP.

Prezes UODO zbadał sprawę i stwierdził, że doszło do naruszenia przepisów o ochronie danych osobowych. Udzielił Wójtowi upomnienia, wyjaśniając, że jest to decyzja adekwatna do skali naruszenia i reakcji na nią wójta jako administratora danych.

Sygnatura sprawy: DS.523.4742.2023

ZALECENIA SCHENGEN DLA POLSKI W OBSZARZE OCHRONY DANYCH OSOBOWYCH

Polska zasadniczo spełnia wymogi w zakresie ochrony danych w dorobku Schengen. Są jednak niedociągnięcia, na które nasz kraj musi zwrócić uwagę.

Eksperci Komisji Europejskiej i państw członkowskich przeprowadzili od marca do kwietnia 2024 r. ocenę stosowania przez Polskę dorobku Schengen. Procedura ta obejmowała także ochronę danych osobowych. Wynikiem tego działania jest sprawozdanie z oceny stosowania przez Polskę dorobku Schengen w 2024 r., które zostało przyjęte przez Komisję Europejską.

Czym jest mechanizm oceny dorobku Schengen?

Strefa bez kontroli na granicach wewnętrznych opiera się na skutecznym i wydajnym stosowaniu przepisów Schengen przez państwa członkowskie. Zasady te obejmują

- środki zabezpieczające granice zewnętrzne,
- środki kompensujące brak kontroli na granicach wewnętrznych,
- oraz solidne ramy monitorowania.

Środki te wzmacniają swobodę przemieszczania się i zapewniają wysoki poziom bezpieczeństwa, sprawiedliwości i ochrony praw podstawowych, w tym ochrony danych osobowych.

Mechanizm oceny i monitorowania Schengen jest kluczowym zabezpieczeniem zapewniającym dobre funkcjonowanie strefy Schengen. Zespół składający się z ekspertów z państw członkowskich i Komisji raz na siedem lat ocenia każde państwo członkowskie i państwo stowarzyszone w ramach Schengen pod kątem pełnego stosowania przepisów Schengen.

Po przeprowadzeniu oceny Komisja sporządza sprawozdanie, które zawiera zalecenia dotyczące działań naprawczych, jakie powinien podjąć oceniany kraj, a także priorytety ich wdrożenia i terminy realizacji.

W 2022 r. przyjęto nowe ramy ocen Schengen, co doprowadziło do bardziej usprawnionych i kompleksowych zaleceń dla poszczególnych krajów. Zapoczątkowało to trzecią generację ocen Schengen. Wstępny harmonogram weryfikacji stosowania przepisów Schengen w każdym kraju UE został określony w wieloletnim programie oceny na lata 2023-2029 i jego zmianach. W uzupełnieniu

i potwierdzeniu tego planowania przyjmowane są roczne programy ewaluacji, zawierające szczegółowe harmonogramy ewaluacji przeprowadzanych w danym roku.

Jak wypada Polska?

Jak zauważyli ewaluatorzy, wojna w Ukrainie ma istotny wpływ na wdrażanie przez Polskę dorobku Schengen, ponieważ nasz kraj jest odpowiedzialny za zabezpieczenie odcinka granicy z Ukrainą, który jest dotknięty bezprecedensowym napływem osób ubiegających się o ochronę międzynarodową i stosujący specjalny system ochrony ustanowiony przez UE.

Pomimo złożonego otoczenia i wyzwań Polska skutecznie wdraża dorobek Schengen i zapewnia znaczący wkład w funkcjonowanie strefy Schengen. **Komisja Europejska wraz z ekspertami państw członkowskich stwierdziła, że Polska zasadniczo spełnia wymogi w zakresie ochrony danych. Stwierdzone niedociągnięcia dotyczą głównie:**

• wyłączenia z zakresu stosowania polskiej ustawy transponującej dyrektywę o ochronie danych w sprawach karnych niektórych rodzajów przetwarzania danych osobowych w niektórych dziedzinach prawa krajowego oraz niektórych organów w zakresie, w jakim dotyczy to również danych przetwarzanych w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym (VIS);

• braku odzwierciedlenia ról i obowiązków Centralnego Organu Technicznego Krajowego Systemu Informatycznego (COT KSI) i właściwych organów jako współadministratorów w odniesieniu do przetwarzania danych osobowych w SIS i VIS, co skutkuje pewnymi niedociągnięciami w zakresie nadzoru nad całymi systemami, takimi jak brak skutecznego monitorowania własnej działalności;

• braku pośredniego dostępu do danych w SIS za pośrednictwem Urzędu Ochrony Danych Osobowych, w przypadku gdy odmówiono dostępu do danych osobowych, ich sprostowania lub usunięcia oraz braku sądowego środka ochrony prawnej w odniesieniu do odpowiedzi administratora na wnioski osób, których dane dotyczą, w kontekście SIS i VIS.

Z oceny wynika, że obszarami priorytetowymi dla Polski z zakresu ochrony danych osobowych są: dostosowanie zakresu polskiej ustawy transponującej dyrektywę o ochronie danych w sprawach karnych w zakresie, w jakim ma ona wpływ na przetwarzanie danych osobowych w SIS i VIS, oraz zagwarantowanie skutecznego mechanizmu monitorowania własnej działalności przez COT-KSI i właściwe organy.

W wyniku okresowej oceny Polski z 2024 r. sformułowano 105 zaleceń dotyczących działań naprawczych mających na celu wyeliminowanie przez Polskę niedociągnięć i wyeliminowanie obszarów wymagających poprawy wskazanych w sprawozdaniu z oceny. W zakresie ochrony danych osobowych zalecenia dla Polski dotyczą m.in:

• zapewnienia pełnej transpozycji dyrektywy (UE) 2016/680 w odniesieniu do przetwarzania danych osobowych wymienionych w art. 3 pkt. 1 polskiej ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości; ponadto należy zapewnić transpozycję dyrektywy (UE) 2016/680 również w odniesieniu do danych osobowych przetwarzanych na podstawie dorobku Schengen przez organy wymienione w art. 3 pkt. 2 polskiej ustawy z dnia 14 grudnia 2018 r., np. przetwarzanie danych osobowych z SIS i VIS do celów wymienionych w dorobku prawnym dotyczącym SIS i VIS; **(zalecenie priorytetowe)**

• zapewnienia, aby osoby, których dane dotyczą, mogły wykonywać swoje prawa dostępu do danych osobowych w Systemie Informacyjnym Schengen, ich sprostowania i usunięcia za pośrednictwem Urzędu Ochrony Danych Osobowych, w przypadku gdy administrator odmówił takiego dostępu do danych osobowych przetwarzanych w Systemie Informacyjnym Schengen, ich sprostowania lub usunięcia zgodnie z art. 53 ust. 3 rozporządzenia (UE) 2018/1861 i art. 67 ust. 3 rozporządzenia (UE) 2018/1862 oraz art. 19 rozporządzenia (UE) 2018/1860; **(zalecenie priorytetowe)**

• zagwarantowania, by osoby, których dane dotyczą, mogły korzystać z prawa do skutecznego środka ochrony prawnej przed sądem przeciwko decyzji administratora dotyczącej praw osób, których dane dotyczą, oraz by były informowane o tym prawie w odpowiedzi administratora zgodnie z art. 53 ust. 3 i art. 54 ust. 1 rozporządzenia (UE) 2018/1861, art. 67 ust. 3 i art. 68 ust. 1 rozporządzenia (UE) 2018/1862 oraz art. 19 rozporządzenia (UE) 2018/1860; **(zalecenie priorytetowe)**

• zapewnienia, aby role i obowiązki Centralnego Organu Technicznego Krajowego Systemu Informatycznego (Komendant Główny Policji) i właściwych organów w odniesieniu do przetwarzania danych osobowych SIS zostały wyjaśnione w prawie i praktyce zgodnie z art. 24 i 26 rozporządzenia (UE) 2016/679 oraz art. 19 i 21 dyrektywy (UE) 2016/680;

• dokonania oceny we współpracy z Urzędem Ochrony Danych Osobowych prawa Centralnego Biura Antykorupcyjnego do wprowadzania do SIS wpisów związanych z zagrożeniami dla bezpieczeństwa narodowego;

• zapewnienia, aby wszystkie organy przetwarzające dane SIS i korzystające z niego proaktywnie, regularnie i wyrywkowo sprawdzały rejestry dotyczące wszystkich działań użytkowników w oparciu o skoordynowane podejście;

• proaktywnego informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych w SIS i VIS oraz o wykonywaniu ich praw (np. w postaci ulotek, plakatów) w komendach policji i na lotniskach;

• zapewnienia, aby Centralny Organ Techniczny Krajowego Systemu Informatycznego - Komendant Główny Policji (administrator COT KSI) znalazł alternatywną procedurę dla polskiej Elektronicznej Platformy Usług Administracji Publicznej (ePUAP) w odniesieniu do elektronicznego wniosku o realizację praw osób, których dane dotyczą, tak aby osoby, których dane dotyczą, bez możliwości złożenia wniosku za pośrednictwem ePUAP, mogły również wykonywać swoje prawa osób, których dane dotyczą, drogą elektroniczną;

• zapewniła, aby wszystkie zalecenia dotyczące aspektów ochrony danych związanych z zarządzaniem krajowego SIS były również przedmiotem działań naprawczych w związku z zarządzaniem krajowego VIS.

Działania następcze i monitorowanie

W ciągu dwóch miesięcy od przyjęcia sprawozdania państwo członkowskie jest zobowiązane do przedłożenia planu działania określającego, w jaki sposób zamierza naprawić zidentyfikowane niedociągnięcia.

Po konsultacji z zespołem, który przeprowadził działanie w zakresie oceny, Komisja przedstawi Polsce analizę adekwatności planu działań w terminie miesiąca od jego przedłożenia. Jeżeli Komisja uzna, że plan działań nie jest adekwatny, Polska będzie musiała przedłożyć zmieniony plan działań w terminie miesiąca od otrzymania wyników analizy. Komisja przedstawi również analizę planu działań Radzie UE.

Od dnia potwierdzenia otrzymania analizy planu działań Polska będzie składać Komisji Europejskiej i Radzie sprawozdanie z realizacji swojego planu działań co sześć miesięcy aż do momentu, gdy Komisja uzna, że plan działań został w pełni zrealizowany. Plan działań naprawczych zostanie zamknięty, w przypadku gdy Komisja uzna, że plan działań został w pełni zrealizowany, o czym Polska zostanie poinformowana.

Plan kontroli sektorowych UODO

Warto przy tej okazji przypomnieć, że przetwarzanie danych osobowych w Wielkoskalowych Systemach Informacyjnych Unii Europejskiej, w tym przetwarzanie danych osobowych SIS/VIS podlega kontroli sektorowej UODO, zgodnie z przyjętym przez Prezesa UODO planem na 2025 r.

Źródła:

Schengen Evaluation and Monitoring Mechanism

Schengen Evaluation of POLAND

4 NARUSZENIA I KONTROLE

Podstawa prawna:

Rozporządzenie Rady (UE) 2022/922 z dnia 9 czerwca 2022 r. w sprawie ustanowienia i funkcjonowania mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz w sprawie uchylenia rozporządzenia (UE) nr 1053/2013

fot. pixabay

EDUKACJA UŻYTKOWNIKÓW JAKO KLUCZOWY ELEMENT OCHRONY DANYCH W DOBIE NOWYCH TECHNOLOGII

Rozwój sztucznej inteligencji (AI) i nowych technologii sprawił, że ochrona danych stała się jednym z najistotniejszych wyzwań środowiska cyfrowego. Urządzenia połączone z internetem i gromadzenie danych cyfrowych stwarza bezprecedensowe możliwości. Rodzi jednak także wyzwania dla prywatności i bezpieczeństwa.

Integracja technologii AI z codziennymi operacjami fundamentalnie przekształciła krajobraz cyfrowy. W miarę jak systemy AI przetwarzają coraz więcej danych, pojawiają się pytania dotyczące przejrzystości, zgodności z regulacjami i aspektów etycznych. Solidne ramy edukacyjne dla użytkowników stanowią fundament minimalizacji tych zagrożeń przy jednoczesnej maksymalizacji korzyści płynących z narzędzi cyfrowych.

Zrozumienie Wartości Danych i Prywatności

Współczesne organizacje muszą uznać, że skuteczna ochrona danych rozpoczyna się od kompleksowego zrozumienia wartości danych osobowych. Użytkownicy potrzebują wiedzy i edukacji o wykorzystywaniu informacji o nich przez podmioty trzecie, potencjalnych konsekwencji nieumyślnego ujawnienia danych oraz mechanizmów, poprzez które systemy AI prowadzą profilowanie użytkowników. To zrozumienie stanowi podstawę świadomego podejmowania decyzji w interakcjach cyfrowych.

Wdrażanie Zabezpieczeń w Środowiskach Wspomaganych przez AI

Współczesna ochrona danych wymaga zaawansowanego podejścia do wdrażania zabezpieczeń.

Organizacje powinny priorytetowo traktować szkolenia w zakresie:

1. Zaawansowanych protokołów uwierzytelniania, w tym uwierzytelniania wieloskładnikowego i zarządzania silnymi hasłami;

2. Identyfikacji i łagodzenia nowych zagrożeń, szczególnie ataków wykorzystujących AI, takich jak zaawansowany phishing i materiały typu deepfake;

3. Strategicznego zarządzania ustawieniami prywatności w platformach wykorzystujących AI i mediach społecznościowych;

4. Wdrażania protokołów anonimizacji i szyfrowania danych.

Ramy Regulacyjne i Zgodność

Dokładne zrozumienie krajobrazu regulacyjnego jest niezbędne dla skutecznej ochrony danych.

Kluczowe obszary koncentracji obejmują:

1. Ogólne Rozporządzenie o Ochronie Danych (RODO) i jego implikacje dla przetwarzania danych;

2. Akt w sprawie Sztucznej Inteligencji (AI Act) i jego wpływ na wdrażanie AI;

3. Wymogi Aktu o Usługach Cyfrowych (DSA) i Aktu o Zarządzaniu Danymi (DGA);

4. Prawa użytkowników dotyczące ograniczeń przetwarzania danych i ochrony przed profilowaniem automatycznym.

Zagrożenia

Brak odpowiedniej wiedzy na temat ochrony danych osobowych może prowadzić m.in. do:

1. Udostępnienia danych osobowych w mediach społecznościowych;

2. Padanie ofiarą oszustw internetowych, cyberprzestępcy coraz częściej stosują techniki socjotechniczne (np. phishing), przed którymi ochroni nas tylko i wyłącznie nasza świadomość z zakresu cyberbezpieczeństwa;

3. Zaniedbanie podstawowych środków bezpieczeństwa, nieaktualizowanie oprogramowania, używanie tych samych haseł do różnych kont czy korzystanie z nieszyfrowanego komunikatora do przesyłania poufnych danych, dokumentów, kopii dowodów osobistych itp. może prowadzić do wycieku danych.

Narzędzia wspierające edukację użytkowników

1. Kampanie informacyjne organizowane przez instytucje publiczne i organizacje pozarządowe, mające na celu podnoszenie świadomości nt. ochrony danych.

2. Szkolenia i warsztaty pozwalające na zdobycie podstawowych umiejętności z zakresu cyberbezpieczeństwa i cyberhigieny.

3. Materiały edukacyjne takie jak poradniki lub kursy online, które pozwolą użytkownikom samodzielnie zdobywać wiedzę na temat ochrony prywatności.

4. Wbudowane funkcje ochrony w systemach operacyjnych i aplikacjach. Nowoczesne oprogramowanie coraz częściej oferuje intuicyjne narzędzia takie jak menedżery haseł generujące długie i trudne do złamania hasła, dedykowane aplikacje do weryfikacji dwuetapowej, które pomagają użytkownikom w zabezpieczaniu swoich danych.

5 NOWE TECHNOLOGIE

Jak zwiększać świadomość społeczną?

Włączenie tematyki ochrony danych do programów szkolnych jest jednym z kluczowym kroków, ponieważ dzieci i młodzież powinny być uczone bezpiecznych nawyków korzystania z internetu już od najmłodszych lat. Edukacja w tym zakresie powinna być realizowana nie tylko w ramach zajęć informatycznych, ale także w przedmiotach z obywatelską odpowiedzialnością i etyką cyfrową.

Standardem powinny być także obowiązkowe dodatkowe zajęcia z cyberbezpieczeństwa lub połączenie ich z informatyką.

Istotną rolę odgrywa współpraca sektora publicznego i prywatnego. Firmy technologiczne, instytucje rządowe oraz organizacje pozarządowe powinny wspólnie działać na rzecz podnoszenia świadomości społecznej, organizując kampanie edukacyjne oraz wdrażając rozwiązania ułatwiające użytkownikom ochronę ich prywatności. Wzajemna wymiana doświadczeń i wspólne działania pozwolą skutecznie dotrzeć do różnych grup społecznych.

Współczesne media społecznościowe odgrywają bardzo ważną rolę w życiu użytkowników, dlatego niezbędne jest promowanie odpowiedzialnych praktyk na tych platformach. Portale internetowe powinny edukować swoich użytkowników na temat ustawień prywatności oraz zagrożeń związanych z publikowaniem danych.

Podsumowanie

Mimo wzrastającej świadomości społecznej, nadal istnieją liczne wyzwania. Szybki rozwój technologii wymaga od użytkowników nieustannego aktualizowania swojej wiedzy, co nie jest łatwe w natłoku informacji. Dodatkowo, wciąż wiele osób nie posiada dostatecznej wiedzy na temat obowiązujących przepisów prawnych – mimo, że RODO funkcjonuje już od kilku lat, nadal nie wszyscy wiedzą, jakie mają prawa i jak mogą je egzekwować.

Ochrona danych osobowych w erze AI wymaga zrównoważonego podejścia łączącego solidne ramy regulacyjne, kompleksową edukację użytkowników i odpowiedzialne wdrażanie technologii. Poprzez wspieranie świadomego obywatelstwa cyfrowego i wdrażanie silnych praktyk cyberbezpieczeństwa, organizacje mogą lepiej chronić prywatność przy jednoczesnym rozwoju innowacji technologicznych.

Sukces w tym przedsięwzięciu zależy od ciągłej adaptacji do pojawiających się zagrożeń i stałego zaangażowania w zasady ochrony prywatności.

USTALENIA RAPORTU KRAJOWEGO IRLANDZKIEGO ORGANU NADZORCZEGO W RAMACH SKOORDYNOWANYCH RAM EGZEKWOWANIA PRAWA NA 2024 R.

W 2024 r. irlandzki organ nadzorczy – Komisja Ochrony Danych (DPC) uczestniczyła w trzecim skoordynowanym działaniu Europejskiej Rady Ochrony Danych (EROD), które koncentrowało się na prawie dostępu. Działanie to miało na celu ocenę poziomu świadomości i zrozumienia Wytycznych EROD 01/2022 dotyczących prawa dostępu wśród administratorów danych. Prawo dostępu ma fundamentalne znaczenie dla ochrony danych i jest jednym z najczęściej wykonywanych praw. Umożliwia ono osobom fizycznym sprawdzenie, czy organizacje przetwarzają ich dane osobowe zgodnie z prawem.

Aby wnieść wkład w tę inicjatywę, DPC przeprowadziło kompleksowe badanie za pomocą kwestionariusza rozesłanego do 30 organizacji z różnych sektorów. Otrzymane odpowiedzi zostały przeanalizowane i włączone do krajowego raportu DPC, który jest załączony do głównego raportu opublikowanego przez EROD.

Niektóre z głównych ustaleń raportu krajowego DPC były następujące:

• Organizacje, które ustanowiły dobrze zorganizowane praktyki i zespoły ds. zgodności w zakresie obsługi wniosków o dostęp do danych (SAR), wykazały najwyższy poziom zgodności i świadomości przepisów RODO.

• Organizacje, które otrzymały większą liczbę SAR, miały zwykle lepiej udokumentowane wewnętrzne procesy zarządzania tymi wnioskami w porównaniu z tymi, które otrzymały minimalną liczbę wniosków.

• Organizacje, które stosowały zautomatyzowane systemy przepływu pracy, narzędzia cyfrowe, oprogramowanie lub systemy biletowe, były bardziej skuteczne w zarządzaniu i śledzeniu wniosków o dostęp.

Określając zakres danych osobowych w odpowiedzi na SAR, irlandzki organ nadzorczy zauważył dobre praktyki u respondentów, którzy stosują listę kontrolną dotyczącą miejsca przechowywania

danych osobowych, w tym dobre wykorzystanie Rejestru Czynności Przetwarzania, który pozwoli zidentyfikować, czy przetwarzane są jakiekolwiek nowe dane.

Źródło: informacja ze strony irlandzkiego organu nadzorczego (DPC)

fot. pixabay

CNIL PUBLIKUJE SWÓJ PLAN STRATEGICZNY NA LATA 2025–2028

W latach 2025–2028 francuski organ nadzorczy (CNIL) skoncentruje swoje działania wokół czterech głównych osi stanowiących istotę rozwoju społeczeństwa cyfrowego: sztucznej inteligencji, ochrony nieletnich w internecie, cyberbezpieczeństwa oraz dwóch zastosowań cyfrowego życia codziennego: aplikacji mobilnych i tożsamości cyfrowej.

Oś 1 – Sztuczna inteligencja

Sztuczna inteligencja i jej liczne zastosowania niosą za sobą poważne zagrożenia dla prywatności, cyberbezpieczeństwa i etyki. W szczególności popularyzacji generatywnej sztucznej inteligencji towarzyszy wzrost potencjalnie złośliwych lub wprowadzających w błąd treści, czego dowodem są deepfaki przedstawiające ludzkie głosy lub wizerunki.

CNIL będzie zatem kontynuować prace nad wyjaśnieniem ram prawnych dotyczących sztucznej inteligencji, prowadzić dialogi oraz rozwijać możliwości audytu.

Oś 2 – Nieletni

Technologie cyfrowe są wszechobecne w codziennym życiu nieletnich, co niesie za sobą szczególne ryzyko cyberprzemocy, ryzyko dla ochrony prywatności i narażenie na nieodpowiednie treści.

W obliczu tych wyzwań CNIL będzie wzmacniać dialog z dziećmi, ich otoczeniem (rodzicami, nauczycielami i wychowawcami) oraz środowiskiem edukacyjnym (podmiotami publicznymi, przedsiębiorstwami, organami regulacyjnymi i organizacjami międzynarodowymi), aby stworzyć bezpieczniejsze środowisko cyfrowe dla dzieci i młodzieży.

Oś 3 – Cyberbezpieczeństwo

Ostatnie lata, a zwłaszcza rok 2024, charakteryzowały się licznymi cyberatakami, których ofiarami padła znaczna część populacji. W obliczu ryzyka kradzieży danych osobowych, zwłaszcza danych bankowych i dotyczących zdrowia, cyberbezpieczeństwo stało się realnym problemem społecznym.

Współpracując ze środowiskiem cyberbezpieczeństwa, CNIL będzie czuwać nad tym, aby organizacje podejmowały odpowiednie środki ochronne oraz będzie podnosić świadomość osób fizycznych na temat ryzyka, aby były one lepiej chronione przed skutkami cyberzagrożeń.

6 SPRAWY MIĘDZYNARODOWE

Oś 4 – Codzienne użytkowanie technologii cyfrowych: aplikacje mobilne i tożsamość cyfrowa

W ramach ostatniej osi swojego planu strategicznego CNIL postanowił skupić się na dwóch głównych aspektach codziennego życia cyfrowego:

• po pierwsze, aplikacji mobilnych, w przypadku których podniesie świadomość użytkowników na temat swoich zaleceń opublikowanych w 2024r;

• po drugie, gwarancji, że podmioty publiczne i prywatne będą opracowywać i wdrażać tożsamości cyfrowe zgodne z przepisami oraz z poszanowaniem prawa i wolności jednostki.

Źródło: strona francuskiego organu nadzorczego (CNIL)

fot. pixabay

HOLENDERSKI ORGAN NAKŁADA GRZYWNĘ NA NETFLIX ZA NIEWŁAŚCIWE INFORMOWANIE KLIENTÓW

Dochodzenie wykazało, że Netflix m.in. nie informował klientów wystarczająco jasno w swoim oświadczeniu o ochronie prywatności o tym, co dokładnie robi z ich danymi. W związku ze stwierdzonymi naruszeniami holenderski organ nadzorczy nałożył na Netflix karę w wysokości 4,75 mln euro.

Informacje ogólne

• Data wydania ostatecznej decyzji: 26 listopada 2024 r.

• Sprawa transgraniczna, procedura One-Stop-Shop: decyzja została podjęta przez krajowe organy nadzoru zgodnie z procedurą współpracy One-Stop-Shop (OSS).

• LSA: Niderlandy

• i CSA: Austria (dwie osoby, których dane dotyczą, z Austrii złożyły skargę do austriackiego organu nadzorczego)

• Odniesienie prawne: art. 5 (Zasady dotyczące przetwarzania danych osobowych), art. 12 (Przejrzyste informacje, komunikacja i sposoby wykonywania praw przez osobę, której dane dotyczą), art. 13 (Informacje, które należy przekazać w przypadku gromadzenia danych osobowych od osoby, której dane dotyczą), art. 15 (Prawo dostępu przysługujące osobie, której dane dotyczą).

• Decyzja: administracyjna kara pieniężna

• Słowa kluczowe: grzywna administracyjna, przejrzystość, prawa osoby, której dane dotyczą, wykonywanie praw osoby, której dane dotyczą, konto użytkownika, Prawo do informacji

Streszczenie decyzji

Geneza sprawy

Holenderski organ nadzorczy (SA) wszczął dochodzenie w następstwie skarg złożonych przez None of your business (noyb), austriacką organizację pozarządową zajmującą się ochroną prywatności. Skargi te zostały złożone do austriackiego organu ochrony danych i przekazane holenderskiemu organowi nadzorczemu, ponieważ Netflix ma swoją główną europejską siedzibę w Holandii.

6 SPRAWY MIĘDZYNARODOWE

Kluczowe ustalenia

Dochodzenie wykazało, że Netflix nie informował klientów wystarczająco jasno w swoim oświadczeniu o ochronie prywatności o tym, co dokładnie robi z ich danymi (art. 5 ust. 1 lit. a) i art. 12 ust. 1 w związku z art. 13 ust. 1 lit. c), e) i f) RODO) oraz art. 13 ust. 2 lit. a) RODO). Ponadto klienci nie otrzymywali wystarczających informacji, gdy pytali Netflix, jakie dane firma gromadzi na ich temat. Tym samym doszło do naruszenia RODO z art. 5 ust. 1 lit. a) i art. 12 ust. 1 w związku z art. 15 ust. 1 lit. a), c) i d) oraz art. 15 ust. 2 RODO).

W kilku punktach Netflix przekazał klientom zbyt mało informacji lub informacje te były niejasne. Firma nie przedstawiła wystarczająco jasno

• celów i podstawy prawnej gromadzenia i wykorzystywania danych osobowych (art. 13 ust. 1 lit. c) i art. 5 ust. 1 lit. a) RODO);

• które dane osobowe są udostępniane przez Netflix innym podmiotom i dlaczego dokładnie tak się dzieje (art. 13 ust. 1 lit. e) i art. 15 ust. 1 lit. c) RODO);

• jak długo Netflix przechowuje dane (art. 13 ust. 2 lit. a) i art. 15 ust. 1 lit. d) RODO);

• w jaki sposób Netflix zapewnia bezpieczeństwo danych osobowych, gdy firma przekazuje je do krajów spoza Europy (art. 13 ust. 1 lit. f) i art. 15 ust. 2 RODO).

Decyzja

Holenderski SA nałożył na Netflix grzywnę w wysokości 4,75 mln euro.

Źródło: strona EROD

Więcej informacji:

Decyzja krajowa **Netflix fined for not properly informing customers** (angielski), **Boete Netflix voor niet goed informeren klanten** (holenderski)

EROD PRZYJMUJE OŚWIADCZENIE W SPRAWIE GWARANCJI WIEKU, TWORZY GRUPĘ ZADANIOWĄ DS. EGZEKWOWANIA SZTUCZNEJ INTELIGENCJI I PRZEKAZUJE ZALECENIA WADA

Podczas posiedzenia plenarnego w lutym 2025 r. Europejska Rada Ochrony Danych (EROD) przyjęła oświadczenie w sprawie gwarancji wieku i postanowiła utworzyć grupę zadaniową ds. egzekwowania sztucznej inteligencji. Ponadto Rada przyjęła również zalecenia dotyczące Światowego Kodeksu Antydopingowego Światowej Agencji Antydopingowej (WADA) z 2027 r.

W oświadczeniu w sprawie gwarancji wieku EROD wymienia dziesięć zasad zgodnego przetwarzania danych osobowych przy określaniu wieku lub przedziału wiekowego danej osoby. Oświadczenie ma na celu zapewnienie spójnego europejskiego podejścia do weryfikacji wieku, aby chronić nieletnich przy jednoczesnym przestrzeganiu zasad ochrony danych.

Przewodnicząca EROD Anu Talus: „Weryfikacja wieku ma zasadnicze znaczenie dla zapewnienia, że dzieci nie uzyskują dostępu do treści nieodpowiednich dla ich wieku. Jednocześnie metoda weryfikacji wieku musi być jak najmniej inwazyjna, a dane osobowe dzieci muszą być chronione. Zasady przedstawione przez EROD pomogą branży ocenić wiek danej osoby w sposób zgodny z zasadami ochrony danych, jednocześnie chroniąc dobro dzieci”.

EROD współpracuje również z Komisją Europejską w zakresie weryfikacji wieku w kontekście grupy roboczej Digital Services Act (DSA).

Podczas sesji plenarnej Rada postanowiła również rozszerzyć zakres grupy zadaniowej ChatGPT o egzekwowanie przepisów dotyczących sztucznej inteligencji. Ponadto członkowie EROD podkreślili potrzebę koordynacji działań organów ochrony danych w zakresie pilnych, wrażliwych kwestii i w tym celu utworzą zespół szybkiego reagowania.

Przewodnicząca EROD Anu Talus: „GDPR to ramy prawne, które promują odpowiedzialne innowacje. RODO zostało zaprojektowane w celu utrzymania wysokich standardów ochrony danych przy jednoczesnym pełnym wykorzystaniu potencjału innowacji, takich jak sztuczna inteligencja, z korzyścią dla naszej gospodarki. Grupa zadaniowa EROD ds. egzekwowania AI i przyszły zespół szybkiego reagowania odegrają kluczową rolę w zapewnieniu tej równowagi, koordynując działania

organów ochrony danych i wspierając je w poruszaniu się po złożoności AI przy jednoczesnym przestrzeganiu silnych zasad ochrony danych".

Podczas sesji plenarnej EROD przyjęła również zalecenia dotyczące Światowego Kodeksu Antydopingowego WADA 2027. Podczas przetwarzania danych osobowych do celów antydopingowych niezbędne jest poszanowanie i ochrona danych osobowych sportowców. W wielu przypadkach będzie się to wiązało z przetwarzaniem wrażliwych danych osobowych, takich jak dane zdrowotne pochodzące z próbek biologicznych.

Głównym celem EROD jest ocena zgodności Kodeksu Antydopingowego WADA i Międzynarodowego Standardu Ochrony Danych (ISDP) z RODO. Kodeks Antydopingowy i Standardy powinny nakładać na Krajowe Organizacje Antydopingowe (NADOS) obowiązek przestrzegania standardu równoważnego z RODO podczas przetwarzania danych osobowych do celów antydopingowych.

Zalecenia EROD odnoszą się do kluczowych zasad ochrony danych, takich jak potrzeba odpowiedniej podstawy prawnej do przetwarzania danych osobowych i ograniczenia celu. Zalecenia odnoszą się również do faktu, że osoby fizyczne muszą być w pełni informowane o przetwarzaniu ich danych osobowych i mogą skutecznie korzystać ze swoich praw.

Źródło: strona EROD

Statement 1/2025 on Age Assurance | European Data Protection Board

fot. pixabay

EROD PUBLIKUJE PÓŁROCZNY RAPORT CSC

EROD opublikowała półroczne sprawozdanie z działalności Komitetu Nadzoru Skoordynowanego (CSC) (lipiec 2022 - grudzień 2024).

W ciągu ostatnich dwóch lat Komitet pracował nad integracją wielkoskalowych systemów informatycznych UE wchodzących w jego zakres. W okresie sprawozdawczym przejął nadzór nad zmodernizowanym Systemem Informacyjnym Schengen (SIS) i Wizowym Systemem Informacyjnym (VIS).

Ponadto Komitet przygotowywał się do wprowadzenia nowych systemów i wdrożenia przepisów dotyczących interoperacyjności.

Komitet opublikował również zestaw zaleceń dotyczących obowiązków administratorów danych w zakresie przejrzystości systemu wymiany informacji na rynku wewnętrznym (IMI).

Ponadto w lipcu 2023 r. Komitet opublikował „Systemy informacyjne Europolu – przewodnik dotyczący wykonywania praw osób, których dane dotyczą: prawo dostępu, sprostowania, usunięcia i ograniczenia".

W następstwie sprawozdania z audytu przeprowadzonego przez EIOD w 2022 r. w sprawie przetwarzania przez Europol danych osobowych małoletnich poniżej 15. roku życia, przekazanych Europolowi przez państwa trzecie i organizacje międzynarodowe oraz oznaczonych jako podejrzane, KOK podjęła skoordynowane działania w celu przeanalizowania wkładu kilku państw członkowskich.

W ciągu ostatnich dwóch lat Komitet promował również dialog i zaangażowanie z zainteresowanymi stronami, w szczególności ze społeczeństwem obywatelskim.

Przyszłe prace CSC

W nadchodzących latach CSC jest gotowa przyjąć w swoje szeregi kolejne systemy informatyczne UE oraz organy, urzędy i agencje UE. Ponieważ zakres działalności CSC nadal się rozszerza, Komitet będzie stale weryfikował swoją organizację i funkcjonowanie, aby zapewnić skuteczny i wydajny nadzór.

Ponadto CSC będzie nadal pomagać krajowym organom ochrony danych (DPA) w ich pracy, zapewniając dalsze wyjaśnienia dotyczące interpretacji przepisów unijnych i krajowych. Komitet będzie również wspierał wymianę informacji i najlepszych praktyk oraz zapewniał wsparcie dla

wspólnych audytów i skoordynowanych inspekcji.

Wykorzystując swoje unikalne ramy i szeroką perspektywę, CSC zapewni właściwe monitorowanie wielu przepływów danych między systemami, interakcji przekrojowych i wymiany informacji między agencjami i organami UE. W tym celu i aby zagwarantować wysoki poziom ochrony danych, Komitet będzie nadal rozwijał skoordynowane działania nadzorcze.

Kontekst

CSC to grupa organów ochrony danych, które wspólnie zapewniają skoordynowany nadzór nad wielkoskalowymi systemami informatycznymi oraz organami, urzędami i agencjami UE objętymi jego zakresem.

CSC funkcjonuje i pozycjonuje się w sposób autonomiczny oraz przyjmuje własny regulamin i metody pracy. Komitet został ustanowiony w ramach Europejskiej Rady Ochrony Danych.

Źródło: strona EROD

fot. pixabay

WCHODZI W ŻYCIE AKT DOTYCZĄCY CYBERODPORNOŚCI

10 grudnia 2024 r. wszedł w życie przełomowy akt prawny dotyczący cyberodporności. To duży krok naprzód w wysiłkach UE na rzecz ochrony obywateli i przedsiębiorstw przed zagrożeniami cybernetycznymi.

Akt w sprawie cyberodporności jest **pierwszym w historii aktem prawnym UE** wprowadzającym obowiązkowe wymogi w zakresie cyberbezpieczeństwa w odniesieniu do produktów zawierających elementy cyfrowe.

Rozporządzenie nakłada na producentów większą odpowiedzialność za zagwarantowanie bezpieczeństwa sprzętu i oprogramowania. Kluczowe znaczenie dla aktu mają nowe obowiązki producentów w zakresie dostarczania aktualizacji oprogramowania, które **naprawiają luki w zabezpieczeniach i oferują konsumentom wsparcie w zakresie bezpieczeństwa**. Poprzez zwiększenie przejrzystości w obszarze cyberzagrożeń i bezpieczeństwa produktów akt umożliwia konsumentom dokonywanie bardziej świadomych wyborów dotyczących produktów dostępnych na rynku UE.

Produkty będą opatrzone oznakowaniem CE wskazującym, że są zgodne z wymogami rozporządzenia. Główne obowiązki wynikające z ustawy będą miały zastosowanie od dnia 11 grudnia 2027 r.

Henna Virkkunen, wiceprzewodnicząca wykonawcza Komisji Europejskiej, powiedziała: „Zobowiązujemy się do uczynienia Europy bezpiecznym miejscem dla naszych obywateli i przedsiębiorstw. To nowe rozporządzenie stanowi ważny krok naprzód w zapewnianiu, aby produkty cyfrowe w UE nie stwarzały cyberzagrożeń dla konsumentów w UE”.

Akt w sprawie cyberodporności uzupełnia ramy cyberbezpieczeństwa NIS 2, które weszły w życie w 2023 roku. Jest to część szeregu kompleksowych środków wdrażanych przez UE w celu wzmocnienia cyberbezpieczeństwa w coraz bardziej cyfrowej i połączonej Europie.

Źródło: informacja prasowa Komisji Europejskiej

KOMISJA WSZCZYNA FORMALNE POSTĘPOWANIE PRZECIWKO TIKTOKOWI W SPRAWIE RYZYKA ZWIĄZANEGO Z WYBORAMI NA PODSTAWIE AKTU O USŁUGACH CYFROWYCH

Komisja Europejska wszczęła w grudniu 2024 r. formalne postępowanie przeciwko TikTokowi w związku z podejrzeniem naruszenia aktu o usługach cyfrowych z uwagi na obowiązek TikToka dotyczący właściwej oceny i ograniczenia ryzyka systemowego związanego z uczciwością wyborów, zwłaszcza w kontekście niedawnych wyborów prezydenckich w Rumunii w dniu 24 listopada.

Przewodnicząca Komisji Ursula von der Leyen powiedziała:

„Musimy chronić nasze demokracje przed wszelkiego rodzaju obcymi ingerencjami. Ilekroć podejrzewamy taką ingerencję, zwłaszcza podczas wyborów, musimy działać szybko i stanowczo. Po poważnych przesłankach wskazujących, że podmioty zagraniczne ingerowały w rumuńskie wybory prezydenckie za pomocą TikToka, obecnie dokładnie badamy, czy TikTok naruszył akt o usługach cyfrowych, nie przeciwdziałając takim zagrożeniom. Powinno być jasne, że w UE wszystkie platformy internetowe, w tym TikTok, muszą zostać pociągnięte do odpowiedzialności”.

Postępowanie skoncentruje się na zarządzaniu ryzykiem związanym z wyborami lub dyskursem obywatelskim na temat następujących obszarów:

• **systemy rekomendacji** TikTok, w szczególności ryzyko związane ze skoordynowaną nieautentyczną manipulacją lub zautomatyzowaną eksploatacją usługi.

• Polityka TikToka w zakresie **reklam politycznych i płatnych treści politycznych**.

W odniesieniu do obu elementów jednym z podejrzeń, które Komisja zamierza zbadać, jest to, czy TikTok starannie ograniczył ryzyko stwarzane przez szczególne regionalne i językowe aspekty wyborów krajowych.

Zapoznaj się z pełnym komunikatem prasowym.

Więcej informacji na temat:

- Akt o usługach cyfrowych
- Nadzór nad wyznaczonymi bardzo dużymi platformami internetowymi i wyszukiwarkami w ramach aktu o usługach cyfrowych
- Ramy egzekwowania na podstawie aktu o usługach cyfrowych

Źródło: informacja prasowa Komisji Europejskiej

fot. pixabay

BUŁGARIA I RUMUNIA PRZYSTĘPUJĄ DO STREFY SCHENGEN

1 stycznia Rumunia i Bułgaria stały się pełnoprawnymi członkami strefy Schengen po zniesieniu kontroli osób na wewnętrznych granicach lądowych.

Kontrole na wewnętrznych granicach powietrznych i morskich między Bułgarią i Rumunią a państwami strefy Schengen zostały już zniesione od 31 marca 2024 r. Przyjęcie obu państw członkowskich do strefy Schengen pobudzi podróże, handel i turystykę oraz przyczyni się do wzmocnienia rynku wewnętrznego.

Kontekst

Komisja po raz pierwszy potwierdziła, że zarówno Bułgaria, jak i Rumunia są gotowe do przystąpienia do strefy Schengen w 2011 r. Od tego czasu Bułgaria i Rumunia nadal wykazują, że spełniają warunki przystąpienia do strefy Schengen.

Strefa Schengen

Schengen to największa na świecie przestrzeń wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych. Strefa Schengen gwarantuje swobodny przepływ ponad 450 mln obywateli UE, a także obywateli państw trzecich mieszkających w UE lub odwiedzających UE jako turyści, studenci uczestniczący w wymianie lub w celach biznesowych (każdy legalnie przebywający w UE).

Układ z Schengen podpisano 14 czerwca 1985 r. na łodzi rzecznej „Księżniczka Marie-Astrid" nad Mozelą w miejscowości na styku trzech państw: Luksemburga, Niemiec i Francji. Umowa została podpisana przez rządy Belgii, Francji, Niemiec, Luksemburga i Niderlandów.

Projekt Unii Europejskiej wprowadził strefę Schengen na wyższy poziom. Ustanawiając prawo do swobodnego przemieszczania się w 1992 r., położono podwaliny pod wspólną przestrzeń europejską. Ramy unijne wchłonęły wszystkie przepisy Schengen w 1997 r. i osiągnęły kolejny kamień milowy w 2007 r., realizując zobowiązanie do stworzenia **„przestrzeni wolności, bezpieczeństwa i sprawiedliwości bez granic wewnętrznych"**. Strefa Schengen jest jedynym regionem na świecie, w którym wzajemne zaufanie między krajami sąsiadującymi jest tak ugruntowane, a wartość swobodnego przepływu tak fundamentalna, że jej członkowie podjęli krok w kierunku zniesienia kontroli granicznych, zobowiązując się do dzielenia zarówno korzyści, jak i obowiązków wynikających z tej niezrównanej integracji.

6 SPRAWY MIĘDZYNARODOWE

Obecnie Unia liczy 27 państw członkowskich i upoważnia 26 z nich – wszystkie z wyjątkiem Irlandii – do ścisłej współpracy we wszystkich obszarach objętych przepisami Schengen. W pracach tych uczestniczą cztery państwa spoza UE: Islandia, Norwegia, Szwajcaria i Liechtenstein.

Schengen to znacznie więcej niż podróże bez granic. Wzywa do koordynacji zarówno w obrębie strefy Schengen, jak i z państwami trzecimi. Państwa strefy Schengen ściśle współpracują w zakresie bezpieczeństwa i migracji poprzez wspólną politykę wizową, wspólne operacje policyjne i wymianę informacji w czasie rzeczywistym między organami ścigania, a także zharmonizowane procedury powrotu osób nieposiadających prawa do pobytu w strefie Schengen. Najnowocześniejsze systemy informatyczne, takie jak System Informacyjny Schengen (SIS), pomagają identyfikować zagrożenia i zarządzać granicami przy jednoczesnym zagwarantowaniu praw podstawowych, w tym ochrony danych.

Źródło: artykuł Komisji Europejskiej

fot. pixabay

ZWIĘKSZENIE CYBERBEZPIECZEŃSTWA SEKTORA OPIEKI ZDROWOTNEJ

Komisja przedstawiła plan działania UE na rzecz zwiększenia cyberbezpieczeństwa szpitali i świadczeniodawców. Inicjatywa ta jest kluczowym priorytetem w ciągu pierwszych 100 dni nowej kadencji i ma na celu stworzenie bezpieczniejszego środowiska dla pacjentów.

Tylko w 2023 r. państwa UE zgłosiły 309 poważnych cyberincydentów wymierzonych w sektor opieki zdrowotnej – więcej niż jakikolwiek inny sektor krytyczny. Ponieważ świadczeniodawcy coraz częściej korzystają z cyfrowej dokumentacji medycznej, ryzyko zagrożeń związanych z danymi nadal rośnie. Może to mieć wpływ na wiele systemów, w tym elektroniczną dokumentację medyczną, systemy przepływu pracy w szpitalach i urządzenia medyczne, zagrażać opiece nad pacjentem, a nawet narażać życie.

Aby sprostać tym wyzwaniom, UE pracuje nad wzmocnieniem sektora opieki zdrowotnej i zwiększeniem jego odporności na cyberzagrożenia. Nowy plan działania opiera się na obowiązujących przepisach, takich jak ogólnounijne przepisy dotyczące cyberbezpieczeństwa, i **rozszerza jego zakres o ogólne praktyki**. Koncentruje się on na **zapobieganiu** zagrożeniom dla cyberbezpieczeństwa, **ich wykrywaniu oraz łagodzeniu ich skutków**. Plan ma również na celu utworzenie **ogólnoeuropejskiego centrum wsparcia cyberbezpieczeństwa**, by zapewnić szpitalom i świadczeniodawcom bardziej dostosowane wytyczne. Do końca roku zostanie on udoskonalony w ramach podejścia opartego na współpracy i będzie stopniowo wdrażany w ciągu najbliższych 2 lat.

Cyfryzacja sektora opieki zdrowotnej umożliwia lepsze usługi dla pacjentów dzięki innowacjom, a także wielu innym korzyściom. UE jest nadal zaangażowana we wspieranie środowiska opieki zdrowotnej, w którym technologia wzmacnia pozycję pacjentów, usprawnia opiekę i wspiera pracowników służby zdrowia.

Więcej informacji:

Cyberbezpieczeństwo szpitali i świadczeniodawców

Nowy plan na rzecz trwałego dobrobytu i konkurencyjności Europy

Cyberbezpieczeństwo

Komunikat prasowy: Komisja przedstawia plan działania na rzecz ochrony sektora zdrowia przed cyberatakami

Europejski plan działania na rzecz cyberbezpieczeństwa szpitali i świadczeniodawców

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Źródło: artykuł Komisji Europejskiej

fot. pixabay

PYTANIA I ODPOWIEDZI DOTYCZĄCE CYBERBEZPIECZEŃSTWA SZPITALI I ŚWIADCZENIODAWCÓW

Dlaczego Komisja Europejska zaproponowała plan działania na rzecz cyberbezpieczeństwa w opiece zdrowotnej?

Cyberzagrożenia dla systemów opieki zdrowotnej rosną, zarówno pod względem częstotliwości, jak i zaawansowania. Szpitale i podmioty świadczące opiekę zdrowotną, które stanowią infrastrukturę krytyczną naszych systemów opieki zdrowotnej, są szczególnie narażone na cyberataki, takie jak oprogramowanie szantażujące lub naruszenia ochrony danych. Incydenty te mogą zakłócić kluczowe usługi medyczne i zagrozić bezpieczeństwu pacjentów i ich danych.

Komisja działa w trybie pilnym, aby sprostać tym wyzwaniom, zapewniając zarówno bezpieczeństwo, jak i wiarygodność transformacji cyfrowej opieki zdrowotnej.

W jaki sposób plan działania zwiększa zaufanie pacjentów i pracowników służby zdrowia?

Zaufanie jest podstawą cyfrowej opieki zdrowotnej. Zapewniając bezpieczeństwo i odporność systemów, plan działania zapewnia pacjentów, że ich dane są bezpieczne, a ich opieka nie zostanie zakłócona.

Dla pracowników służby zdrowia plan zapewnia narzędzia i szkolenia, które pomogą im pewnie poruszać się po platformach cyfrowych. To podwójne podejście – chroniące zarówno pacjentów, jak i pracowników służby zdrowia – tworzy środowisko opieki zdrowotnej, w którym narzędzia cyfrowe są akceptowane i cieszą się zaufaniem.

W jaki sposób niniejszy plan działania uzupełnia obowiązujące przepisy UE, takie jak dyrektywa NIS 2?

Plan działania opiera się na istniejących ramach prawnych w dziedzinie cyberbezpieczeństwa – w szczególności na dyrektywie NIS 2, akcie w sprawie cybersolidarności (w tym mechanizmie cyberkryzysowym), akcie w sprawie cyberbezpieczeństwa (w tym europejskiej certyfikacji cyberbezpieczeństwa), rozporządzeniu w sprawie wyrobów medycznych i akcie w sprawie cyberodporności. Zapewniają one wysoki wspólny poziom cyberbezpieczeństwa w całej UE.

W dyrektywie NIS 2, w której określono obowiązki sektorów krytycznych, w tym opieki zdrowotnej, rozszerzono zakres wymogów cyberbezpieczeństwa na usługi podstawowe obejmujące laboratoria

referencyjne UE, podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych, producentów podstawowych produktów i preparatów farmaceutycznych (w tym szczepionek), producentów wyrobów medycznych uznanych za krytyczne podczas stanu zagrożenia zdrowia publicznego.

Jeśli chodzi o plan działania, skupiono się w szczególności na wyjątkowych podatnościach i potrzebach szpitali i placówek opieki zdrowotnej.

Plan działania ma przede wszystkim na celu wspieranie sektora w podejmowaniu podstawowych środków w zakresie cyberbezpieczeństwa, o których wiemy, że zmienią prawdopodobieństwo wystąpienia cyberincydentu. Gwarantuje to, że systemy opieki zdrowotnej są przygotowane do radzenia sobie z konkretnymi zagrożeniami, na które są narażone. Szczególną uwagę poświęca budowaniu zdolności, inwestycjom oraz pomaganiu szpitalom i świadczeniodawcom w podejmowaniu niezbędnych środków gotowości w zakresie cyberbezpieczeństwa. Ustanawia również sposoby pomocy takim podmiotom w przypadku wystąpienia incydentu, aby zapewnić jak najszybsze i najskuteczniejsze reagowanie i odzyskiwanie danych, tak aby można było szybko przywrócić normalne operacje.

Jaka będzie rola nowego Europejskiego Centrum Wsparcia w dziedzinie Cyberbezpieczeństwa dla szpitali i świadczeniodawców?

W planie działania proponuje się m.in. utworzenie ogólnoeuropejskiego **centrum wsparcia cyberbezpieczeństwa** dla szpitali i świadczeniodawców, aby zapewnić im dostosowane do potrzeb wytyczne, narzędzia i usługi. ENISA, unijna agencja ds. cyberbezpieczeństwa, ustanowi Centrum w ramach swoich własnych struktur. Zapewni on realizację planu działania w sposób spójny i usprawniony, unikając jednocześnie tworzenia nowych struktur administracyjnych.

Centrum Wsparcia opracuje kompleksowy katalog usług konkretnych rozwiązań wzmacniających cyberbezpieczeństwo sektora. Będzie współpracować z państwami członkowskimi i korzystać z praktycznych doświadczeń organizacji opieki zdrowotnej.

W jaki sposób niniejszy plan działania wspiera europejską przestrzeń danych dotyczących zdrowia?

Europejska przestrzeń danych dotyczących zdrowia (EHDS) to sztandarowy projekt UE mający na celu cyfryzację opieki zdrowotnej, w którym ustanowiono jasne zasady wykorzystywania danych dotyczących zdrowia do lepszego świadczenia opieki zdrowotnej, badań naukowych, innowacji i kształtowania polityki.

6 SPRAWY MIĘDZYNARODOWE

Odporna i bezpieczna infrastruktura ma zasadnicze znaczenie dla wdrożenia europejskiej przestrzeni danych dotyczących zdrowia. W niniejszym planie określono konkretne działania mające na celu zapewnienie przetwarzania danych w szpitalach i świadczeniodawcach, którzy działają zarówno jako świadczeniodawcy, jak i użytkownicy danych odnoszących się do zdrowia w europejskiej przestrzeni danych dotyczących zdrowia.

Oprócz niniejszego planu działania i przepisów dotyczących cyberbezpieczeństwa przyszłe rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia przewiduje również szczególne zabezpieczenia w odniesieniu do przetwarzania danych osobowych dotyczących zdrowia. Zawiera ono na przykład zabezpieczenia obejmujące zarządzania logowaniem i identyfikacją w systemach elektronicznej dokumentacji medycznej lub ponownego wykorzystywania danych w bezpiecznych środowiskach przetwarzania.

W jaki sposób plan działania zagwarantuje, że cyberincydenty nie zakłócą opieki nad pacjentem?

Jednym z głównych filarów planu działania jest szybkie reagowanie i odbudowa.

Obejmuje to:

• Opracowanie usługi subskrypcji odzyskiwania oprogramowania ransomware i rozszerzenie repozytorium dostępnych narzędzi do odszyfrowywania oprogramowania ransomware.

• Zachęcanie szpitali do stosowania solidnych systemów tworzenia kopii zapasowych w celu ochrony krytycznych danych.

• Zwiększenie zdolności reagowania kryzysowego poprzez szkolenia i współpracę na szczeblu UE.

Środki te mają na celu zminimalizowanie wpływu cyberincydentów na usługi opieki zdrowotnej, zapewniając pacjentom nieprzerwaną opiekę.

Jaką rolę w realizacji tego planu działania odgrywają państwa członkowskie?

Państwa członkowskie odegrają kluczową rolę we wdrażaniu planu działania poprzez:

• Koordynację krajowych strategii cyberbezpieczeństwa w opiece zdrowotnej.

• Dzielenie się informacjami na temat zagrożeń i najlepszymi praktykami ponad granicami.

• Wspieranie szpitali i świadczeniodawców w przyjmowaniu niezbędnych środków.

Zachęca się państwa członkowskie do opracowania krajowych planów działania ukierunkowanych na cyberbezpieczeństwo w sektorze opieki zdrowotnej. Plany te określałyby konkretne zagrożenia dla cyberbezpieczeństwa, na jakie narażone są systemy opieki zdrowotnej, oraz krajowe działania

podejmowane w celu zaradzenia tym zagrożeniom, przy jednoczesnym zapewnieniu skutecznego wykorzystania zasobów i praktyk na szczeblu europejskim.

W jaki sposób będzie mierzony sukces planu działania?

Aby zmierzyć powodzenie tego planu, ENISA, w porozumieniu z Komisją, będzie regularnie składać sprawozdania z postępów odpowiednim grupom i organizacjom. Sprawozdania te będą zawierać dane z unijnego indeksu cyberbezpieczeństwa, który pomoże ocenić, jak dobrze sektor opieki zdrowotnej radzi sobie pod względem cyberbezpieczeństwa. Informacje te pokażą, czy plan działa i wywiera pozytywny wpływ.

Co mogą zrobić pacjenci, aby wesprzeć realizację celów planu działania?

Pacjenci mogą wnieść swój wkład, informując o cyberbezpieczeństwie i podejmując kroki w celu ochrony własnych cyfrowych danych dotyczących zdrowia. Na przykład:

• Korzystanie z wiarygodnych mechanizmów uwierzytelniania (np. unijnego portfela tożsamości cyfrowej) na potrzeby internetowych portali zdrowotnych.

• Zgłaszanie podejrzanych działań, takich jak próby phishingu.

• Zaufanie do świadczeniodawców, którzy stosują się do zalecanych przez UE środków w zakresie cyberbezpieczeństwa.

Bezpieczny ekosystem opieki zdrowotnej zależy od aktywnego uczestnictwa wszystkich.

Jaki jest harmonogram realizacji planu działania?

W niniejszym komunikacie przedstawiono jasny plan zwiększenia bezpieczeństwa europejskiego sektora opieki zdrowotnej przed zagrożeniami cybernetycznymi. Plan tworzy centralne centrum wsparcia cyberbezpieczeństwa, ułatwiając szpitalom i świadczeniodawcom współpracę w celu zachowania bezpieczeństwa w internecie.

Ten plan to dopiero początek. Komisja rozpoczyna szerszą rozmowę ze wszystkimi zainteresowanymi stronami, w tym świadczeniodawcami, rządami i ekspertami, aby wysłuchać ich pomysłów i informacji zwrotnych. Komisja wykorzysta ten wkład, aby uczynić plan bardziej szczegółowym i ukierunkowanym na potrzeby szpitali i innych świadczeniodawców. Zalecenia te zostaną udostępnione do końca 2025 r.

Aby osiągnąć ten cel, Komisja wzywa wszystkie państwa członkowskie i zainteresowane strony do współpracy na rzecz zwiększenia cyberbezpieczeństwa sektora opieki zdrowotnej.

6 SPRAWY MIĘDZYNARODOWE

Aby uzyskać więcej informacji:

Plan działania w sprawie cyberbezpieczeństwa szpitali i świadczeniodawców

Komunikat prasowy

Zestawienie informacji

Źródło: Pytania i odpowiedzi dotyczące cyberbezpieczeństwa szpitali i świadczeniodawców przygotowane przez Komisję Europejską

fot. pixabay

ZROZUMIENIE WPŁYWU INTERAKCJI CZŁOWIEKA ZE SZTUCZNĄ INTELIGENCJĄ NA DYSKRYMINACJĘ

Ponieważ systemy sztucznej inteligencji są coraz częściej wykorzystywane do wspomagania podejmowania decyzji w sektorach o wysokiej stawce, takich jak kredyty i rekrutacja, eksperci ds. projektowania i analizy behawioralnej z Laboratorium Polityki UE postanowili zbadać kluczową kwestię ludzkiego nadzoru nad decyzjami wspieranymi przez sztuczną inteligencję. Przy wsparciu Europejskiego Centrum Przejrzystości Algorytmicznej (ECAT) Komisja Europejska starała się lepiej zrozumieć, w jaki sposób ludzie wchodzą w interakcje ze sztuczną inteligencją.

Sprawiedliwość w AI: bardziej złożona niż sądziliśmy

Intuicyjnie można by sądzić, że ludzki nadzór może służyć jako kontrola przed uprzedzeniami AI. Jednak kompleksowe badanie Komisji Europejskiej, które łączy w sobie badania ilościowe i jakościowe, opowiada inną historię.

KE odkryła, że nadzorujący pracę ludzi są tak samo skłonni postępować zgodnie z radami systemów AI, niezależnie od tego, czy są one zaprogramowane pod kątem uczciwości, czy nie. Sugeruje to, że sam ludzki nadzór jest niewystarczający, aby zapobiec dyskryminacji; w rzeczywistości może nawet ją utrwalać.

W opisywanym eksperymencie ilościowym wzięli udział specjaliści ds. HR i bankowości z Włoch i Niemiec, którzy podejmowali decyzje dotyczące zatrudniania i udzielania kredytów pod wpływem zaleceń sztucznej inteligencji. Wyniki były dość uderzające: użycie „sprawiedliwej” sztucznej inteligencji zmniejszyło na przykład uprzedzenia ze względu na płeć, ale nie wyeliminowało wpływu wcześniej istniejących ludzkich uprzedzeń w podejmowaniu decyzji.

Jakościowe spostrzeżenia z wywiadów i warsztatów z uczestnikami i ekspertami ds. sztucznej inteligencji potwierdziły te ustalenia. Specjaliści często przedkładali interesy firmy nad sprawiedliwość, podkreślając potrzebę jaśniejszych wytycznych dotyczących tego, kiedy należy pominąć sugestie AI.

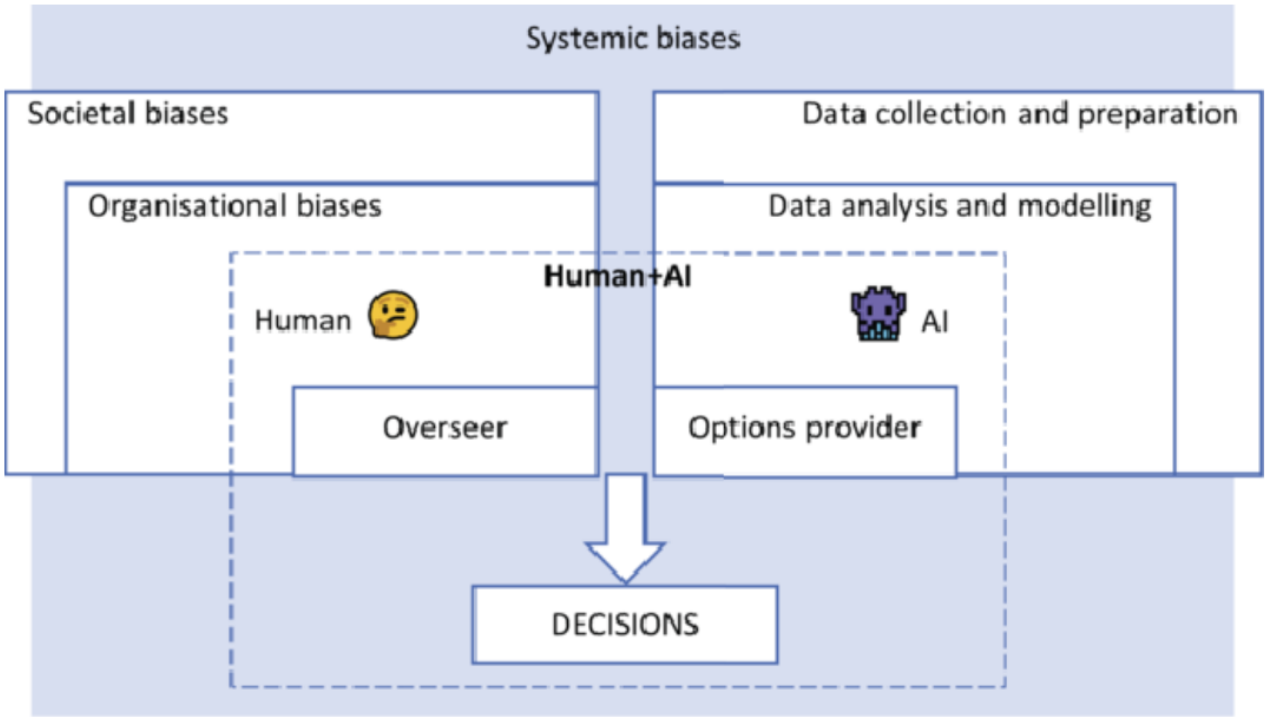
W kierunku sprawiedliwości systemowej

Wnioski z badania wskazują na potrzebę przejścia od indywidualnego nadzoru do zintegrowanego systemu zaprojektowanego w celu przeciwdziałania uprzedzeniom zarówno ze strony człowieka, jak i sztucznej inteligencji. Prawdziwy nadzór obejmuje coś więcej niż tylko programowanie sztucznej inteligencji tak, aby była sprawiedliwa lub poleganie na indywidualnym osądzie. Wymaga on holistycznego podejścia, takiego jak

• Środki techniczne mające na celu zapewnienie, że systemy sztucznej inteligencji są projektowane i aktualizowane z myślą o sprawiedliwości.

• Strategie organizacyjne mające na celu promowanie kultury, która priorytetowo traktuje sprawiedliwość i zapewnia szkolenia w zakresie zarządzania narzędziami sztucznej inteligencji.

• Interwencje polityczne, które ustanawiają jasne wytyczne dotyczące współpracy człowieka ze sztuczną inteligencją.



Tło decyzyjne człowieka i sztucznej inteligencji oraz ich wzajemne oddziaływanie

Komisja Europejska

Wzmocnienie pozycji decydentów

Aby skutecznie łagodzić uprzedzenia, decydenci potrzebują narzędzi i wytycznych, które pomogą im zrozumieć, kiedy i jak zastąpić zalecenia AI. Ciągłe monitorowanie i ocena wyników wspomaganych przez sztuczną inteligencję są niezbędne do identyfikowania i eliminowania pojawiających się uprzedzeń.

Co więcej, dając decydentom dostęp do danych na temat ich wyników i potencjalnych uprzedzeń, możemy wspierać bardziej refleksyjne i odpowiedzialne podejście do podejmowania decyzji wspieranych przez sztuczną inteligencję.

Informowanie o akcie o sztucznej inteligencji i nie tylko

Na początku ubiegłego roku przyjęto unijny akt prawny dotyczący sztucznej inteligencji, wyznaczający standardy regulacji w tym zakresie na całym świecie. Ustalenia KE są szczególnie istotne dla wprowadzenia tego aktu w życie, podkreślając konsekwencje ludzkiego nadzoru. Dostarczając praktycznych spostrzeżeń, Komisja stara się informować o przyszłych standardach i wytycznych, które nie tylko zapewnią zgodność z ustawą o sztucznej inteligencji, ale także ujawnią praktyczne kwestie wdrożeniowe, które są równie ważne.

Zapraszamy do zapoznania się z raportem Komisji Europejskiej, oferującym bardziej szczegółowy opis badania i jego implikacji dla przyszłości zarządzania sztuczną inteligencją.

Przeczytaj raport

Dołącz do Komisji w przemyśleniu roli ludzkiego nadzoru w sztucznej inteligencji. Dzięki odpowiednim regulacjom i wytycznym możemy upewnić się, że UE może czerpać korzyści z nowych technologii, zapewniając jednocześnie sprawiedliwe i odpowiedzialne podejmowanie decyzji w erze cyfrowej.

Jeśli chcesz dowiedzieć się więcej o tym projekcie, zapoznaj się z niektórymi zastosowanymi w nim metodami: Uczciwe podejmowanie decyzji: Czy ludzie mogą uchronić nas przed stronniczą sztuczną inteligencją? - Komisja Europejska

Źródło: artykuł Komisji Europejskiej

OCENY INTEROPERACYJNOŚCI SĄ TERAZ OBOWIĄZKOWE

Od 12 stycznia 2025 r. administracje publiczne w całej Unii Europejskiej muszą przeprowadzać oceny interoperacyjności przy wprowadzaniu nowych lub zmienionych wymogów dotyczących transeuropejskich cyfrowych usług publicznych.

Oceny interoperacyjności są jednym z najważniejszych obowiązków wynikających z Aktu w sprawie Interoperacyjnej Europy, służąc jako proces odkrywania dla administracji publicznych w celu zidentyfikowania barier i możliwości w zakresie interoperacyjności transgranicznej. Dzięki uwzględnieniu tych czynników na wczesnym etapie procesu projektowania i kształtowania polityki, oceny ułatwiają wdrażanie cyfrowych usług publicznych opartych na płynnej transgranicznej wymianie danych.

Kogo to dotyczy?

Oceny interoperacyjności mają zastosowanie do podmiotów unijnych i organów sektora publicznego planujących wprowadzenie wiążących wymogów, które mają wpływ na transgraniczne cyfrowe usługi publiczne. Przykłady takich usług obejmują wzajemne uznawanie kwalifikacji akademickich, dostęp do informacji dotyczących zabezpieczenia społecznego i cyfrową dokumentację medyczną – usługi, które opierają się na płynnej wymianie danych między państwami członkowskimi UE.
W przeciwieństwie do tego, oceny te zazwyczaj nie mają zastosowania do ściśle lokalnych usług publicznych, które nie obejmują transgranicznej wymiany informacji, takich jak aplikacje parkingowe opracowane do użytku w jednej gminie.

Wytyczne i wsparcie ze strony Komisji Europejskiej

Rada Interoperacyjnej Europy, podczas swojego pierwszego posiedzenia w grudniu 2024 r., przyjęła wytyczne w celu standaryzacji wdrażania ocen interoperacyjności. Wytyczne te zapewniają jasność co do tego, w jaki sposób organy publiczne mogą oceniać prawny, semantyczny, techniczny i organizacyjny wymiar interoperacyjności. Krok ten odzwierciedla zaangażowanie Rady w uczynienie interoperacyjności kluczowym aspektem polityki cyfrowej UE.

Aby wesprzeć oceny, Komisja Europejska zaoferuje narzędzie online zintegrowane z portalem Interoperacyjna Europa. Narzędzie to uprości proces raportowania poprzez generowanie nadających

się do odczytu maszynowego, wielojęzycznych raportów, które będą publicznie dostępne. Komisja będzie również oferować materiały szkoleniowe i okresowo organizować warsztaty na ten temat. Udostępnione zasoby mają na celu podniesienie kwalifikacji pracowników sektora publicznego i zapewnienie płynnej integracji rozwiązań interoperacyjnych w całej UE.

Jeśli chcesz dowiedzieć się więcej o procesie stojącym za wytycznymi dotyczącymi oceny interoperacyjności, przeczytaj broszurę Komisji Europejskiej Science for Policy Brief.

Akt w sprawie Interoperacyjnej Europy

Akt w sprawie Interoperacyjnej Europy wszedł w życie w kwietniu 2024 roku. Rozporządzenie ustanawia ramy zarządzania w celu zwiększenia interoperacyjności usług cyfrowych sektora publicznego. Stanowi ono podstawę szerszej wizji UE dotyczącej połączonego jednolitego rynku cyfrowego, zapewniając dostępność i inkluzywność ponad granicami.

Aby uzyskać więcej informacji, odwiedź stronę Interoperable Europe Act Regulation i bądź na bieżąco za pośrednictwem portalu Interoperable Europe Portal.

Webinarium „Interoperacyjność w działaniu: Akt i oceny”

Aby wesprzeć administracje publiczne i zainteresowane strony w poruszaniu się po nowych wymaganiach, Komisja Europejska zorganizowała webinarium zatytułowane „Interoperacyjność w działaniu: Działaj i oceniaj”. Sesja ta dostarczyła praktycznych informacji na temat przeprowadzania ocen interoperacyjności i wdrażania transgranicznych cyfrowych usług publicznych.

KOMISJA ZWRACA SIĘ O INFORMACJE ZWROTNE NA TEMAT ŚRODKÓW, KTÓRE APPLE POWINNO PODJĄĆ W CELU ZAPEWNIENIA INTEROPERACYJNOŚCI NA PODSTAWIE AKTU O RYNKACH CYFROWYCH

Komisja przesłała Apple wstępne ustalenia w kontekście dwóch postępowań w sprawie specyfikacji, które wszczęła w dniu 19 września 2024 r. Ustalenia te wskazują na proponowane środki dla Apple w celu zapewnienia interoperacyjności urządzeń podłączonych do internetu z telefonami iPhone oraz zwiększenia przewidywalności i przejrzystości interoperacyjności ze strony stron trzecich, zgodnie z wymogami aktu o rynkach cyfrowych.

Zgodnie z DMA Apple musi zapewnić programistom i firmom bezpłatną i skuteczną interoperacyjność z funkcjami sprzętu i oprogramowania kontrolowanymi przez jego systemy operacyjne iOS i iPadOS, które są podstawowymi usługami platformowymi, dla których Apple został wyznaczony jako strażnik dostępu.

Postępowanie w sprawie specyfikacji urządzeń podłączonych do internetu

We wstępnych ustaleniach pierwszego postępowania w sprawie **specyfikacji** przedstawiono proponowane środki, które zdaniem Komisji Apple powinno wdrożyć, aby skutecznie wywiązać się ze swoich obowiązków w zakresie interoperacyjności w odniesieniu do kilku funkcji łączności **z systemem iOS, wykorzystywanych** głównie do urządzeń **podłączonych do internetu i przez takie urządzenia.** Mogą to być powiadomienia, automatyczne połączenie Wi-Fi, AirPlay, AirDrop lub automatyczne przełączanie dźwięku Bluetooth.

Otwarcie funkcji łączności iOS i umożliwienie interoperacyjności z urządzeniami innych firm doprowadzi do zwiększenia innowacji na rynku i zwiększy wybór dla użytkowników iOS fizycznych podłączonych urządzeń, takich jak smartwatche lub słuchawki.

6 SPRAWY MIĘDZYNARODOWE

Postępowanie w sprawie specyfikacji dotyczące procesu składania wniosków o interoperacyjność

We wstępnych ustaleniach drugiego postępowania w sprawie **specyfikacji** przedstawiono proponowane środki, które zdaniem Komisji Apple powinno wdrożyć w odniesieniu do procesu opartego na wnioskach, który twórcy procesów muszą przejść, aby uzyskać interoperacyjność z konkretną funkcją iOS lub iPadOS. Proponowane środki obejmują zwiększoną przejrzystość z góry wewnętrznych funkcji iOS i iPadOS, terminową komunikację i aktualizację, sprawiedliwą i przejrzystą obsługę odrzuceń oraz bardziej przewidywalny harmonogram.

Aby zapewnić skuteczną interoperacyjność proponowanych środków zgodnie z aktem o rynkach cyfrowych, Komisja rozpoczęła **dwie konsultacje publiczne:**

• Środki istotne dla urządzeń podłączonych do internetu, które dążą do interoperacyjności z systemem iOS.

• Proces składania przez Apple wniosków o interoperacyjność w odniesieniu do stron trzecich.

Zainteresowane strony miały czas **do 9 stycznia 2025 r.** na przedstawienie opinii na temat każdego z dwóch zestawów środków.

Nieopatrzone **klauzulą poufności streszczenia obu postępowań i planowanych środków** są również dostępne na stronach poświęconych konsultacjom.

Kolejne kroki

Komisja dokładnie oceni informacje zwrotne przekazane przez zainteresowane strony i Apple. Otrzymane informacje mogą spowodować dostosowanie środków, które zostaną uwzględnione w dwóch ostatecznych wiążących decyzjach.

Komisja ma sześć miesięcy od wszczęcia dwóch postępowań w sprawie specyfikacji na przyjęcie ostatecznych decyzji.

Kontekst

Zgodnie z aktem o rynkach cyfrowych Komisja może przyjąć decyzję, w której określi środki, które strażnik dostępu musi wdrożyć w celu wypełnienia obowiązków określonych w art. 6 i 7 aktu o rynkach cyfrowych. Postępowanie w sprawie specyfikacji ma na celu dostarczenie szczegółowych informacji na temat obowiązku, a nie ocenę przestrzegania go przez strażnika dostępu. Przyjęcie wstępnych ustaleń jest etapem pośrednim, który umożliwia danemu strażnikowi dostępu i osobom trzecim przekazanie informacji zwrotnych na temat środków, które Komisja zamierza określić.

6 SPRAWY MIĘDZYNARODOWE

Postępowania w sprawie specyfikacji i przypadki niezgodności to dwa odrębne narzędzia, którymi dysponuje Komisja i które służą różnym celom. W przeciwieństwie do przypadków niezgodności postępowania w sprawie specyfikacji dotyczą szczegółów zgodności z samym obowiązkiem.

Aby uzyskać więcej informacji:

Konsultacje publiczne w sprawie proponowanych środków specyfikacji dla urządzeń podłączonych do internetu

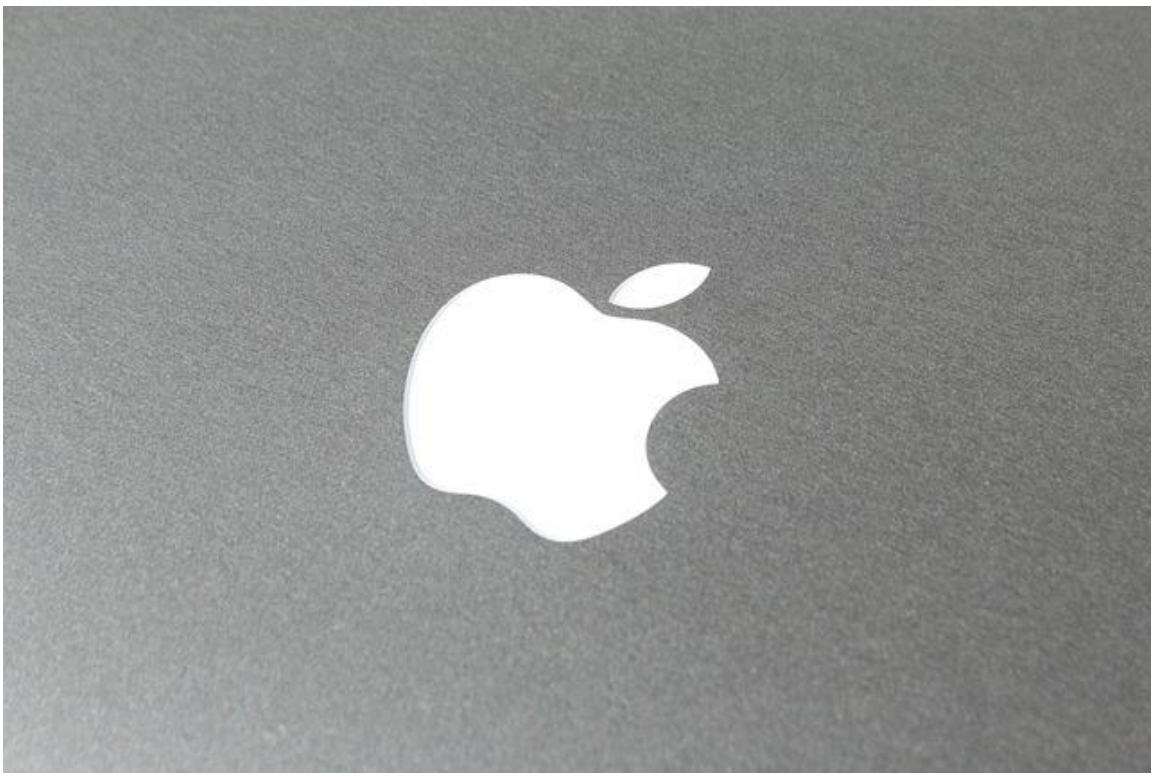
DMA.100203 – Apple – Systemy operacyjne – iOS – Artykuł 6 ust. 7 – SP – Funkcje podłączonych urządzeń fizycznych

Konsultacje społeczne w sprawie proponowanych środków specyfikacji procesu

DMA.100204 – Apple – Systemy operacyjne – iOS i iPadOS – Artykuł 6 ust. 7 – SP – Proces

Commission seeks feedback on the measures Apple should take to ensure interoperability under the Digital Markets Act

Źródło: materiał Komisji Europejskiej



fot. pixabay

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl