URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 03/03/25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

w marcu podjąłem kilka decyzji ważnych dla bezpieczeństwa naszych danych osobowych. Były to też decyzje o karach dla organów władzy publicznej. Organ nadzorczy właściwy do spraw ochrony danych osobowych musi bowiem jednoznacznie sprzeciwić się sytuacjom, w których przedstawiciele państwa bez uzasadnienia przetwarzają lub ujawniają dane obywateli i je wykorzystują.

Dlatego zdecydowałem się złożyć do Prokuratury Rejonowej Warszawa-Śródmieście zawiadomienie o uzasadnionym podejrzeniu popełnienia przestępstwa polegającego na przetwarzaniu danych osobowych, choć ich przetwarzanie nie jest dopuszczalne. Chodzi o wpisy w portalu X, w których kilku użytkowników opublikowało dane z kwestionariuszy paszportowych prokurator Ewy Wrzosek, byłego ministra, a obecnie posła do Parlamentu Europejskiego Mariusza Kamińskiego, posła na Sejm X kadencji Marka Jakubiaka, a także matki Mariusza Kamińskiego oraz matki obecnego ministra sprawiedliwości Adama Bodnara.

Najważniejsza decyzja o pieniężnej karze administracyjnej dotyczyła Poczty Polskiej i Ministra Cyfryzacji, którzy w kwietniu i maju 2020 r. bez podstawy prawnej przetwarzali dane 30 mln polskich obywateli z bazy PESEL. Sprawa ta dotknęła 80 procent obywateli Rzeczypospolitej. Stąd wysokość obu kar – przy czym wymiar kary dla Poczty Polskiej został znacząco obniżony ze względu na trudną sytuację spółki świadczącej ważne usługi publiczne. Niektórzy twierdzą, że średnio 80 groszy za naruszenie danych jednej osoby to rażąco niska kara, jednak moim zdaniem kara musi być nie tylko skuteczna i odstraszająca, ale także proporcjonalna.

W marcu nałożyłem także karę na Komendanta Głównego Policji za ujawnienie na konferencji prasowej danych kobiety, która poddała się aborcji farmakologicznej. Komendant zrobił to bez podstawy prawnej, na konferencji prasowej bronił swoich podkomendnych przed zarzutem brutalnego i okrutnego potraktowania kobiety, która poprosiła pogotowie o pomoc, ujawniając, że jej złe samopoczucie może mieć związek z dokonaną aborcją. Ujawnienie danych o stanie zdrowia stanowiło bardzo poważne naruszenie przepisów o ochronie danych, dlatego kara była konieczna.

Nałożyłem również karę pieniężną na Polskie Radio Szczecin – za to, że nie miało procedur uniemożliwiających bezprawne ujawnianie danych osobowych w serwisie stacji. Kontrola w radiu została przeprowadzona w wyniku doniesień dotyczących sprawy ujawnienia danych dziecka,

które miało paść ofiarą pedofila. Sprawa miała tragiczny finał, dziecko popełniło samobójstwo. Okazało się, że mamy do czynienia z wieloletnimi systemowymi zaniedbaniami w ochronie danych, co spowodowało konieczność nałożenia wspomnianej kary.

Chciałbym też zwrócić Państwa uwagę na pismo skierowane do Prokuratora Krajowego. Poprosiłem w nim o uczulenie prokuratorów, że dane medyczne pobrane w gabinecie lekarskim nie mogą tak po prostu służyć do oskarżania lekarza. Pismo to powstało na kanwie sprawy lekarki, którą prokuratura oskarżyła o pomoc w aborcjach na podstawie danych o pacjentkach, zebranych w czasie przeszukania gabinetu. Chodzi tu o dane zdrowotne – ich wykorzystanie ze względu na ich wagę podlega szczególnym obostrzeniom. Prokuratura nie spełniła tu warunków pozwalających jej na korzystanie z tych danych.

Uczymy się znaczenia danych osobowych

Jak co miesiąc Prezes UODO angażuje się w szerzenie wiedzy o roli danych osobowych we współczesnym świecie i ich znaczeniu dla ludzi. Uczymy się wspólnie, jak rozumieć nowe regulacje i jak wdrażać nowoczesne techniki zarządcze, w tym analizę ryzyka dla danych. Dlatego m.in. promowaliśmy nasz najnowszy poradnik dla administratorów i IOD dotyczący naruszeń danych osobowych.

W marcu w ramach „UODO rusza w kraj" byliśmy w Rzeszowie. Kolejna odsłona naszej akcji potwierdziła słuszność założeń i pokazała, jak ważne są spotkania z różnymi środowiskami, nie tylko na szczeblu centralnym. Zarówno konferencja, jak i pozostałe spotkania cieszyły się dużym zainteresowaniem i udowodniły, jak potrzebne są nasze wyjazdy. Następnym razem odwiedzimy województwo wielkopolskie.

Angażowaliśmy się także w ochronę praw dzieci jako szczególnie narażonych na niebezpieczeństwa w sieci. Polecam Państwa uwadze ważny raport „Internet dzieci", który pokazuje m.in., skąd dzieci czerpią informacje w sieci i jak się po niej poruszają. W żaden sposób nie przypomina to doświadczeń dzisiejszych dorosłych.

Wiedząc o tym, jak wielkie są dziś różnice pokoleniowe w wyszukiwaniu informacji, poprosiłem Minister Edukacji Narodowej, by rozporządzenie o edukacji zdrowotnej uwzględniało podstawy wiedzy o znaczeniu danych o zdrowiu. Wiedza dzieci o tym, jak chronić swoje dane osobowe, informacje prywatne – często odnoszące się do stanu zdrowia fizycznego i psychicznego – a także o zagrożeniach, jakie wiążą się z naruszeniem bezpieczeństwa tych danych – jest niezbędna do tego, aby bezpiecznie poruszać się w świecie rozwijających się technologii. Z satysfakcją odnotowuję, że takie treści o ochronie danych znalazły się w nowych przepisach. Pragnę za to serdecznie podziękować Pani Minister i całemu Ministerstwu Edukacji Narodowej.

26 marca, w dniu wejścia w życie rozporządzenia unijnego o Europejskiej Przestrzeni Danych Dotyczących Zdrowia (EHDS), zorganizowaliśmy wraz z Wydziałem Prawa i Administracji Uniwersytetu Warszawskiego, Wydziałem Medycznym UW, Instytutem Nauk Prawnych Polskiej Akademii Nauk oraz Naczelną Izbą Lekarską konferencję naukową na temat EHDS, wdrażania rozwiązań w erze AI, Big Data i medycyny spersonalizowanej.

Tego dnia podpisałem też porozumienie o współpracy z Naczelną Izbą Lekarską.

W miesiącu, w którym działo się tak wiele, warto wspomnieć jeszcze o:

• upomnieniu nałożonym na jedną z uczelni (z opóźnieniem wprowadziła regulacje gwarantujące spełnienie wymogów RODO dotyczących zasad współpracy administratora z inspektorem ochrony danych).

• fakcie, że Meta Platforms Ireland Limited cofnęła skargi na postanowienia Prezesa Urzędu Ochrony Danych Osobowych z 5 sierpnia 2024 r. w sprawie Państwa Rafała Brzoski oraz Ammy Omeny Mensah.

• potwierdzeniu przez NSA naszej interpretacji art. 105a ust. 3 Prawa bankowego, że kiedy umowa kredytowa wygasa, bank może przetwarzać dane klienta zalegającego ze spłatą, o ile wcześniej skutecznie powiadomi go o tym zamiarze i odczeka 30 dni.

• interwencji u Ministra Rozwoju i Technologii, w której poprosiłem o zmianę przepisów tak, by numery z ksiąg wieczystych nie były podawane we wnioskach o ustalenie lokalizacji inwestycji oraz w podejmowanych w tych sprawach uchwałach rady gminy. Bo w ten sposób są one następnie publicznie ujawniane na BIP gminy.

I na koniec istotna wiadomość: w lipcu 2025 r. UODO zmienia siedzibę. Wyprowadzamy się z biurowca Intraco przy ul. Stawki 2, który zostanie poddany remontowi.

Przeprowadzamy się do budynku przy ul. Moniuszki w Warszawie, w pobliżu Placu Powstańców.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W tym numerze przyglądamy się ważnym zmianom jakie zaszły po styczniowej reorganizacji Urzędu. Wgląd w działania niedawno utworzonego Departamentu Wstępnej Kontroli Skarg i Naruszeń daje nam rozmowa z jego dyrektorem – Adamem Furmańczukiem. Doświadczony praktyk opowiada nam m.in. czym zajmuje się departament, którym kieruje, o tym jak trudno odseparować zgodnie z procedurą administracyjną bezzasadne skargi i czy po publikacji poradnika dot. naruszeń spodziewa się większej liczby zgłoszeń naruszeń do UODO.

Aktualizacja poradnika wywołała ogromne zainteresowanie ekspertów, które obserwowaliśmy w najważniejszych polskich mediach. Ponieważ w przestrzeni publicznej pojawiły się głosy wskazujące na zaostrzenie stanowiska Prezesa UODO m.in. w sprawie rozumienia naruszeń ochrony danych osobowych, wymogu ich zgłaszania czy też roli inspektora ochrony danych przy ich obsłudze, w marcowym wydaniu „Biuletynu UODO" pokazujemy, że w rzeczywistości aktualizacja poradnika nie przyniosła fundamentalnych zmian w podejściu Prezesa UODO do poruszonych w nim zagadnień.

W związku z rozwojem nowych technologii popularność na rynku zyskują długopisy cyfrowe. Przypominamy, że każda decyzja administratora o pozyskiwaniu danych klienta opartych na biometrii powinna być poprzedzona szczególnie wnikliwą analizą. Przetwarzanie takich danych powinno odbywać się nie tylko z poszanowaniem zasady legalności, ale także być działaniem adekwatnym oraz stosownym i ograniczonym z punktu widzenia realizacji zakładanego celu.

Pliki cookies odgrywają istotną rolę w prawidłowym działaniu współczesnych stron internetowych, jednak ich niekontrolowane wykorzystanie może stanowić poważne zagrożenie dla prywatności użytkowników. Przestrzegamy przed akceptowaniem ich bez zastanowienia i sygnalizujemy, że zgodnie z wytycznymi EROD zgoda na pliki cookies musi być dobrowolna, świadoma, jednoznaczna i poprzedzona aktywnym działaniem użytkownika.

Donosimy też o niedawnych działaniach Komisji Europejskiej:

• Unia Europejska reaguje na zagrożenia związane z importem produktów kupowanych na platformach elektronicznych. W tym celu Komisja Europejska opracowała pakiet na rzecz bezpiecznego i zrównoważonego handlu elektronicznego.

• Komisja Europejska i Europejska Rada Usług Cyfrowych poparły integrację dobrowolnego Kodeksu postępowania w zakresie dezinformacji w ramach Aktu o usługach cyfrowych (DSA). Integracja ta uczyni Kodeks punktem odniesienia przy określaniu zgodności platform z DSA.

• Na szczycie poświęconym działaniom na rzecz sztucznej inteligencji w Paryżu przewodnicząca Komisji Ursula von der Leyen uruchomiła InvestAI – inicjatywę mającą na celu zmobilizowanie 200 miliardów euro na inwestycje w AI, w tym w nowy europejski fundusz w wysokości 20 miliardów euro na gigafabryki AI. Tak duża infrastruktura AI jest potrzebna, aby umożliwić otwarty, wspólny rozwój najbardziej złożonych modeli sztucznej inteligencji.

Przybliżamy sprawę, w której opiekunowie dziecka poskarżyli się do PUODO, że radny miasta udostępnił na Facebooku jego zdjęcia, zrobione podczas publicznej imprezy charytatywnej. Prezes UODO wskazał, że do zamieszczenia zdjęcia dziecka radny nie miał podstaw i nakazał jego usunięcie z prywatnego profilu polityka.

Zwracanie uwagi na zagrożenia związane z naruszeniem prywatności w mediach społecznościowych jest dla UODO bardzo ważne. Dlatego w ramach obecnie trwającej XV edycji ogólnopolskiego programu edukacyjnego Prezesa UODO „Twoje dane – Twoja sprawa" zorganizowaliśmy lekcję dla uczniów „Naruszenie prywatności w mediach społecznościowych – mediacje jako sposób rozwiązywania konfliktów". Prowadząca webinarium opowiedziała uczestnikom o mediacji oraz o sposobach radzenia sobie z trudnymi sytuacjami, tak aby mogli skutecznie rozwiązywać konflikty i budować lepsze relacje.

Niestety przekonanie o anonimowości w sieci potrafi prowadzić do nadużyć, nieodpowiedzialnych działań, a nawet naruszeń prywatności. Dlatego tak ważna jest refleksja nad tym, co publikujemy w internecie, szczególnie jeśli treści, które udostępniamy, dotyczą dzieci.

Na koniec chciałbym przypomnieć, że 31 marca 2025 r. nastąpi wyłączenie archiwalnych stron internetowych UODO (archiwum.uodo.gov.pl oraz archiwum.giodo.gov.pl). To konieczne ze względów bezpieczeństwa.

Karol Witowski
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

TO POMYSŁY PRACOWNIKÓW STAŁY SIĘ PIERWSZYM I NAJWAŻNIEJSZYM ELEMENTEM, KTÓRY OBECNIE WDRAŻAMY

Z Adamem Furmańczukiem, dyrektorem Departamentu Wstępnej Kontroli Skarg i Naruszeń rozmawiał Karol Witowski, Rzecznik Prasowy UODO.

1 stycznia 2025 roku prezes Mirosław Wróblewski wprowadził w UODO zmiany organizacyjne, które mają usprawnić działanie Urzędu. Ważnym krokiem w kierunku skrócenia czasu rozpatrywania spraw przez Urząd było utworzenie Departamentu Wstępnej Kontroli Skarg i Naruszeń, którego jest pan dyrektorem. To właśnie tu w pierwszej kolejności wpływają skargi i zgłoszenia naruszeń ochrony danych osobowych, w celu ich weryfikacji pod kątem formalnym oraz oceny wagi problemu. Jak to wygląda w praktyce?

W praktyce nasza działalność, mówiąc pokrótce, to nic innego jak wstępne badanie skarg i zgłoszeń naruszeń ochrony danych osobowych, oparte na analizie ich treści, potem podejmowanie czynności w celu uzupełnienia ich braków formalnych, czy też brakujących informacji, aby sprawy mogły być merytorycznie załatwione.

Nasza działalność to też niepopularne wśród skarżących odmowy wszczęcia postępowania i, ewentualnie, w wyniku ich zaskarżenia, przygotowywanie odpowiedzi urzędu w tych sprawach dla sądu administracyjnego. Skrócenie czasu rozpatrywania skarg jest celem, dla którego staramy się stale poprawiać metody działania dla lepszej efektywności. Nawet czynności prawnicze można parametryzować, sprawiać, by były powtarzalne, a choćby w tym celu wypracowywać wzory. Cóż, to tak pokrótce…

O tym, że czekają nas zmiany organizacyjne w UODO, szczególnie te, które pozwolą na usprawnienie procesu rozpatrywania skarg i naruszeń, wiedzieliśmy od dawna. Prezes UODO komunikował to zarówno w mediach, jak i wewnątrz Urzędu. Wprowadzone zmiany są efektem wielu rozmów z dyrektorami, pracownikami, interesariuszami Urzędu. Reorganizacja wynika z zaobserwowanych potrzeb oraz zmieniającego się otoczenia Urzędu. Sądzę, że wyjdą wszystkim – przede wszystkim obywatelom – na lepsze.

1 ROZMOWA Z EKSPERTEM

Minęły ponad dwa miesiące, od kiedy funkcjonuje nowy Departament. Czy po tak krótkim czasie jego działania, można już zauważyć pozytywne zmiany, które są efektem pracy jego zespołu?

Mam nadzieję że tak, chociaż nie skupiam się na obserwowaniu pozytywnych zmian, o których pewnie, jeśli są, mogą powiedzieć departamenty, z którymi współpracujemy najczęściej: Departament Skarg oraz Departament Kontroli i Naruszeń. Na pewno pozytywną zmianą dla nich jest to, że mogą skupić się na merytorycznych rozstrzygnięciach spraw, które prowadzą. Teraz to my zajmujemy się selekcją przypadków, które nie rodzą konieczności prowadzenia dalszych postępowań, dzięki czemu pozostałe dwa departamenty mogą przejść do tych spraw, które wymagają kolejnych działań ze strony UODO.

Praktyczne funkcjonowanie nowej struktury pokaże, czy kierunek zmian przynosi zamierzony efekt i służy obywatelom.

Ile procentowo spraw ze wstępnej kontroli jest przekazywanych do innych departamentów, a ile można zakończyć w Departamencie Wstępnej Kontroli Skarg i Naruszeń?

Przekazujemy mniej niż 20 procent spraw dot. zgłaszanych naruszeń ochrony danych osobowych. W przypadku skarg jeszcze za wcześnie na obiektywne dane. Proces uzupełniania braków formalnych skarg trwa często dłużej, chociażby z uwagi na czas, który potrzebują skarżący na odpowiadanie na nasze wezwania. Wciąż też rozbudowujemy Wydział Wstępnej Kontroli Skarg.

Pracuje Pan w UODO (wcześniej w GIODO) od wielu lat. Zawsze pełnił Pan wysokie funkcje w Urzędzie…

Wolę określenie „skromny urzędnik państwowy”. Zaczynałem pracę w 2007 r. jako zwykły pracownik i tak było do 2015 r.…

Przed objęciem obecnego stanowiska, był Pan naczelnikiem Wydziału ds. Sektora Prywatnego w Departamencie Skarg. Jak to doświadczenie przekłada się na Pana obecną funkcję?

Bardzo i jeszcze bardziej pewne wzorce, które zaczęliśmy wypracowywać jeszcze i od 2018 r., gdy zaczął funkcjonować Zespół Wstępnej Oceny Skarg, którego byłem skromnym szefem. Dotyczyło to np. metod komunikacji wewnętrznej w urzędzie. Stała się ona bardziej bezpośrednia. Mail czy telefon stał się wiodącą formą zamiast pism wewnętrznych. Zaczęliśmy stosować zasady prostej polszczyzny w pismach do obywateli. Poznaliśmy dobrodziejstwa Excela, ukonkretniliśmy formy raportowania,

ewidencjonowania spraw… ale przede wszystkim poznałem pracowników, z którymi teraz pracuję. Potem byliśmy wszyscy pracownikami Departamentu Skarg. Już wtedy więc rozmawialiśmy, czy istnienie takiej komórki jak nasza obecna ma sens, co i jak moglibyśmy robić, aby pomóc w funkcjonowaniu urzędu. I, to muszę podkreślić, to pomysły pracowników stały się pierwszym i najważniejszym elementem, który obecnie wdrażamy.

Jak na przestrzeni lat zmieniały się wyzwania w zakresie wstępnego rozpoznania skarg i naruszeń?

Zmienia się ich liczba. To jest prawdziwe wyzwanie. Zasoby urzędu zawsze będą pozostawały nieco w tyle za jego potrzebami. Poza tym nie zmieniło się wiele od wejścia w życie RODO, no, może więcej jest takich skarg, w których wcale nie chodzi o ochronę danych osobowych… To też sprawa dla Departamentu Wstępnej Kontroli Skarg i Naruszeń, ponieważ możemy przekierować obywatela do innej, bardziej odpowiedniej w danej sprawie instytucji jak Rzecznik Praw Obywatelskich czy Urząd Ochrony Konkurencji i Konsumenta.

Czy do UODO wpływa wiele bezzasadnych skarg? Czy łatwo i szybko można je odseparować od tych, które wymagają większej uwagi Urzędu?

Niestety wpływa ich wiele, ale na szczęście procentowo jest ich stanowcza mniejszość. Łatwo je zauważyć, trudniej odseparować zgodnie z procedurą administracyjną. Są to skargi pracochłonne, roszczeniowe, często stresujące. Skargi w rodzaju: wędkarz skarżący innego wędkarza, a jako dane go identyfikujące podaje kolor wędki. Inny przykład: matka, którą pozbawiono praw rodzicielskich, skarżąca szkołę językową, do której dziecko zapisał ojciec, z którą ona sama nie ma nic wspólnego. Po co tę szkołę skarży? Mamy przypadki bezzasadnych skarg nierzetelnych dłużników żądających prawa do bycia zapomnianym wobec wierzycieli. Piszą do nas również sąsiedzi zaglądający nawzajem kamerkami w swoje podwórka…

Są osoby, które skarżą hurtowo dowolnie przez nich wybrane podmioty, a ze skarg wycofują się, gdy otrzymają jakiś bonus, bon, profit, od tych podmiotów, i wprost tego przed złożeniem skargi żądają. Każdą odmowę wszczęcia postępowania trzeba bardzo dobrze uzasadnić.

Cokolwiek powiedzieliby twórcy doktryny prawniczej ochrony danych osobowych, że każdy zasługuje na ochronę swoich danych osobowych, z czym się zgadzam, nam po prostu często jest przykro, że mamy obowiązek poświęcania czasu i środków takim sprawom, gdy naprawdę potrzebujący naszej pomocy „Kowalski” musi czekać.

1 ROZMOWA Z EKSPERTEM

Czy po niedawnej publikacji zaktualizowanego poradnika dotyczącego naruszeń ochrony danych osobowych spodziewa się Pan większej liczby zgłoszeń naruszeń do UODO?

Nie spodziewam się. Administratorzy danych osobowych mają równie zdroworozsądkowe podejście jak urząd. Poradnik nie zmienił przepisów prawa, które dotąd i ciągle wszyscy stosujemy. Sam poradnik też jest jak najbardziej zdroworozsądkowy. Proszę tylko zauważyć, jest pisany dla administratorów danych osobowych, ale przez organ, którego obowiązkiem jest te dane chronić.

Obecny jeszcze wzrost liczby zgłoszeń jest zgodny z trendami obserwowanymi w poprzednich latach i świadczy o skrupulatności firm w raportowaniu naruszeń ze względu na ryzyko związane z potencjalnymi konsekwencjami: postępowaniami, karami finansowymi czy odszkodowaniami. Ten trend nie został jeszcze zatrzymany. Mamy jednak nadzieję, że dzięki rosnącej profesjonalizacji procesów przetwarzania danych osobowych u ich administratorów i z pomocą działań urzędu to się uda. Póki co jednak, zgodnie ze styczniowym raportem „GDPR Fines and Data Breach Survey" DLA Piper (Badanie kar za naruszenie RODO oraz naruszeń danych) Polska kolejny rok z rzędu znalazła się w czołówce krajów z największą liczbą zgłoszeń naruszenia RODO.

W prowadzonym przez Pana Departamencie działa również infolinia, która przed reorganizacją była częścią Departamentu Komunikacji Społecznej. Jak zmieniły się jej zadania?

Infolinia może obecnie bardziej czerpać z doświadczeń osób, które rozpatrują skargi, a osoby, które rozpatrują skargi z wiedzy infolinii. Jesteśmy jedną komórką. Komunikacja jest prostsza, informacje uzyskujemy szybciej i możemy się nimi szybciej wymieniać, czy też zapełniać wspólne, robocze bazy danych. Dzięki temu pracochłonność zdobywania wiedzy przez pracowników infolinii jest mniejsza. Dzięki temu z kolei infolinia może wspierać zespół rozpatrywania skarg w realizacji bieżących działań.

Zauważam przy tym, że pomysł, by ekspertów z infolinii włączyć w rozpatrywanie skarg prezes Wróblewski miał na długo zanim objął powyższe stanowisko. O usprawnieniu rozpatrywania skarg i roli infolinii w tym zakresie, mówił już podczas konferencji dla kandydatów na funkcję Prezesa UODO. Teraz jest duża szansa, by infolinia bardziej mogła wspomóc działalność urzędu.

Choć cały Urząd ma bardzo dużo pracy, od zawsze słyszymy, że to właśnie kadra zajmująca się skargami, jest najbardziej obciążona obowiązkami. Czego Pan sobie i osobom, z którymi współpracuje życzy, co mogłoby sprawić, że praca w departamencie będzie mniej stresująca?

1 ROZMOWA Z EKSPERTEM

Tak, w naszym urzędzie wszyscy mamy dużo pracy. U nas, w naszym departamencie sama ilość spraw rodzi ilość dylematów z nimi związanych. Rozpatrujemy skargi, naruszenia ochrony danych osobowych, zgłoszenia sygnalistów zewnętrznych, prowadzimy infolinię. Każdy z nas ma swoje dylematy merytoryczne, a kadra chce i powinna być pomocna każdemu pracownikowi, naszym koleżankom i kolegom.

Czego im życzyć? Ja życzyłbym im tego, żeby dalej byli sobą. A sobie i im też oczywiście… może zmian legislacyjnych, które pozwoliłyby na odformalizowanie postępowań.

Dziękuję za rozmowę.

fot. zasoby własne UODO. Na zdjęciu Adam Furmańczuk, dyrektor Departamentu Wstępnej Kontroli Skarg i Naruszeń

PODPIS BIOMETRYCZNY KLIENTA NA UMOWIE

Każda decyzja administratora o pozyskiwaniu danych klienta opartych na biometrii powinna być poprzedzona szczególnie wnikliwą analizą. Przetwarzanie takich danych powinno się odbywać nie tylko z poszanowaniem zasady legalności, ale także być działaniem adekwatnym oraz stosownym i ograniczonym z punktu widzenia realizacji zakładanego celu. Jest to istotne tym bardziej, że w świetle art. 9 ust. 1 RODO zasadą jest zakaz przetwarzania takich danych, a odstępstwo od niego powinno mieć wyraźne oparcie w jednym z wyjątków wprost wymienionych w ust. 2 tego przepisu. Przesłanką legalizującą przetwarzanie takich danych mogłaby być więc np. zgoda klienta, o ile zostaną spełnione wszystkie określone w RODO warunki jej wyrażania.

W związku z rozwojem nowych technologii popularność na rynku zyskują długopisy cyfrowe. Umożliwiają one podpisanie umowy lub innego dokumentu własnoręcznym podpisem zapisywanym jednocześnie w formie cyfrowej. Dzięki wykorzystaniu takiego narzędzia możliwe jest powstawanie zarówno wersji papierowej dokumentów, jak i ich elektronicznych odpowiedników.

Wątpliwości administratorów i inspektorów ochrony danych (IOD) budzi jednak kwestia kwalifikacji danych zbieranych przy tworzeniu cyfrowej wersji podpisu odręcznego. Czy takie dane należy uznać za dane biometryczne? Jak powinno wyglądać pozyskiwanie i wycofywanie zgody na ich przetwarzanie? Jakie środki ich ochrony przyjąć?

Kiedy cyfrowy podpis to dane biometryczne?

Wyjaśniając te wątpliwości, w pierwszej kolejności pod uwagę należy wziąć definicję danych biometrycznych zawartą w art. 4 ust. 14 RODO. Stanowi on, że dane te oznaczają „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech (…) behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby.”

2 UODO SYGNALIZUJE

Europejska Rada Ochrony Danych (EROD) w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo wskazała, że aby uznać określone dane za dane biometryczne, pod uwagę należy wziąć trzy elementy:

• charakter danych – dane dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej,

• środki i sposób przetwarzania – wynikają z użycia odpowiedniej technologii,

• cel przetwarzania – dane muszą być przetwarzane w celu jednoznacznej identyfikacji osoby.

Ponadto Grupa Robocza Art. 29 w Opinii 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych zaznaczyła, że jedną z kategorii technik biometrycznych są techniki behawioralne, które obejmują mierzenie zachowania danej osoby na podstawie podpisu odręcznego. Dodano, że „typowymi cechami dynamicznymi mierzonymi przez system biometrii podpisu odręcznego (taki jak tablet graficzny) są: stopień nacisku, kąt nachylenia pisma, prędkość i przyśpieszenie narzędzia pisarskiego, kształt liter, kierunek pisma oraz inne niepowtarzalne cechy dynamiczne".

Zatem biorąc po uwagę powyższe wskazówki uznać należy, że podpis złożony przy pomocy cyfrowego długopisu, który odczytuje i zapisuje kształt pisma, siłę nacisku, czas zapisu oraz szybkość ruchu ręki składającego podpis, można uznać za „dane biometryczne" w rozumieniu art. 4 ust. 1 i art. 9 RODO, jeżeli administrator używa określonych środków technicznych umożliwiających jednoznaczne zidentyfikowanie osoby fizycznej.

Szczególny reżim

Należy też pamiętać, że stosownie do art. 9 ust. 1 RODO „dane biometryczne" należą do szczególnych kategorii danych osobowych, których przetwarzanie co do zasady jest zakazane. Odstępstwo od tego zakazu jest możliwe, o ile spełniony jest jeden z warunków określonych w art. 9 ust. 2 RODO. W przypadku relacji firmy z klientem w grę wchodzi przesłanka, o której mowa w art. 9 ust. 2 lit. a RODO, tj. „osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1." Ponadto motyw 51 RODO określa, że „dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności". Z tego powodu techniczne i organizacyjne środki ochrony danych osobowych wprowadzone przez administratora muszą ograniczyć czynniki ryzyka dla ochrony praw i wolności jego klientów.

Potrzebna ocena skutków dla ochrony danych

W związku z tym administrator przed wprowadzeniem stosowania technologii cyfrowego długopisu powinien przeprowadzić ocenę skutków dla ochrony danych (tzw. Data Protection Impact Assessment). RODO (art. 35) ustanawia taki obowiązek w sytuacji, gdy „dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych".

Dodać należy, że polski organ nadzorczy „przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu" wskazał jako jeden z rodzajów operacji wskazujących na potrzebę przeprowadzenia takiej oceny (patrz wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków dla ochrony danych; dostępny pod linkiem https://monitorpolski.gov.pl/MP/2019/666).

Częścią takiej oceny (zgodnie z powołaną Opinią Grupy Roboczej 3/2012) powinna być analiza tego, czy technologia cyfrowego długopisu i związane z nią przetwarzanie danych biometrycznych są niezbędne do świadczenia określonej usługi, czy nie jest to tylko rozwiązanie najdogodniejsze lub najbardziej opłacalne dla administratora.

Właściwe zabezpieczenia

Po przeprowadzeniu oceny ryzyka, administrator jest zobowiązany do wprowadzenia odpowiednich środków bezpieczeństwa danych osobowych, odpowiadających stopniowi zagrożenia (art. 32 RODO). Administrator powinien rozważyć odpowiednio:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2 UODO SYGNALIZUJE

Grupa Robocza Art. 29 w Opinii 3/2012 oraz EROD w Wytycznych 3/2019, w celu zapewnienia wysokiego poziomu ochrony technicznej przy przetwarzaniu danych biometrycznych, zalecają m.in.:

• wprowadzenie mechanizmu automatycznego usuwania danych, aby zapobiec zbyt długiemu okresowi przechowywania danych biometrycznych,

• wprowadzenie systemów weryfikujących autentyczność podpisującego,

• przechowywanie informacji biometrycznych w postaci zaszyfrowanej oraz w oddzielnej bazie danych,

• kategoryzacje danych w trakcie ich przesyłania i przechowywania.

Co więcej, administrator powinien uwzględnić już w procesie projektowania wdrożenie odpowiednich środków technicznych i organizacyjnych oraz domyślną ochronę, które zapewnią odpowiednią ochronę praw i wolności podmiotów (tzw. privacy by design oraz privacy by default) (art. 25 RODO). Pomocne może być zaznajomienie się z Wytycznymi EROD 4/2019 dotyczącymi artykułu 25 uwzględniającego ochronę danych w fazie projektowania oraz domyślną ochronę danych (dostępne pod linkiem: https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_pl.pdf.

Odpowiednie poinformowanie o zastosowaniu danych biometrycznych

Poza tym Grupa Robocza Art. 29 w Opinii 3/2012 zwraca uwagę, iż przetwarzanie danych na podstawie zgody jest ważne, jeżeli podmiotowi, którego dane będą przetwarzane, udzielona została wystarczająca ilość informacji o zastosowaniu danych biometrycznych. Informacje te są opisane w art. 13 ust. 1 i 2 RODO. Ze względu na szczególny charakter danych biometrycznych, należy zwrócić uwagę na podanie okresu przechowywania danych osobowych oraz informacje o prawie do cofnięcia zgody na ich przetwarzanie. Administrator powinien mieć również na względzie zasady: minimalizacji, ograniczenia przechowywania, integralności i poufności danych (art. 5 RODO).

Warunki pozyskiwania zgody klientów

Należy podkreślić, że według art. 4 ust. 11 RODO, „zgoda" oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie jej danych osobowych, w tym danych biometrycznych.

Żeby można było mówić o wyrażeniu zgody wyraźnej, konieczne jest, by administrator poinformował ją o ryzykach związanych z przetwarzaniem takich danych, zasadach ich przetwarzania, stosowanych zabezpieczeniach i przysługujących jej uprawnieniach. Zgoda powinna także wyraźnie precyzować cel

przetwarzania w momencie jej odbierania. Istotne jest, aby klient, udzielając zgody, znał jej zakres i cel i wiedział, na czym konkretnie będzie polegało przetwarzanie jego danych.

Powinna istnieć również alternatywna metoda, z której podmiot danych mógłby skorzystać w przypadku braku zgody na przetwarzanie danych biometrycznych, tak, aby nie zostać pozbawionym możliwości skorzystania z konkretnej usługi. Należy więc rozważyć, czy klient ma możliwość zawarcia umowy także składając inny niż biometryczny rodzaj podpisu.

Motyw 43 RODO stanowi, że „zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych". W motywie 32 doprecyzowano, że „zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele."

Ponadto, Wytyczne EROD 5/2020 dotyczące zgody na mocy rozporządzenia 2016/679 (dostępne pod linkiem https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf stanowią, że „usługa może obejmować wiele operacji przetwarzania w więcej niż jednym celu. W takich przypadkach osobom, których dane dotyczą, powinna przysługiwać swoboda wyboru celu, który akceptują, zamiast obowiązku wyrażenia zgody na szereg celów przetwarzania. W danym przypadku zgodnie z RODO uzasadnione może być wyrażenie kilku zgód w celu rozpoczęcia oferowania usługi." W związku z tym, administrator powinien umożliwić osobie, której dane dotyczą, wyrażenie zgody/zgód na przetwarzanie danych osobowych, w tym danych biometrycznych, na dokładnie określone cele doprecyzowane w zależności od umowy.

Administrator powinien również pamiętać, że jeżeli chce przetwarzać dane osobowe w innym celu niż oznajmiono osobie, której dane dotyczą, musi poprosić o zgodę tej osoby na nowy cel albo znaleźć inną podstawę prawną zgodną z art. 6 lub art. 9 RODO.

Co ważne, art. 7 ust. 4 RODO oraz Wytyczne 5/2020 podkreślają, że „łączenie zgody z akceptacją warunków lub uzależnianie wykonania umowy lub świadczenia usługi od uwzględnienia wniosku o wyrażenie zgody na przetwarzanie danych osobowych, które nie jest konieczne w celu wykonania umowy lub świadczenia usługi", jest działaniem niepożądanym i podważającym dobrowolność zgody.

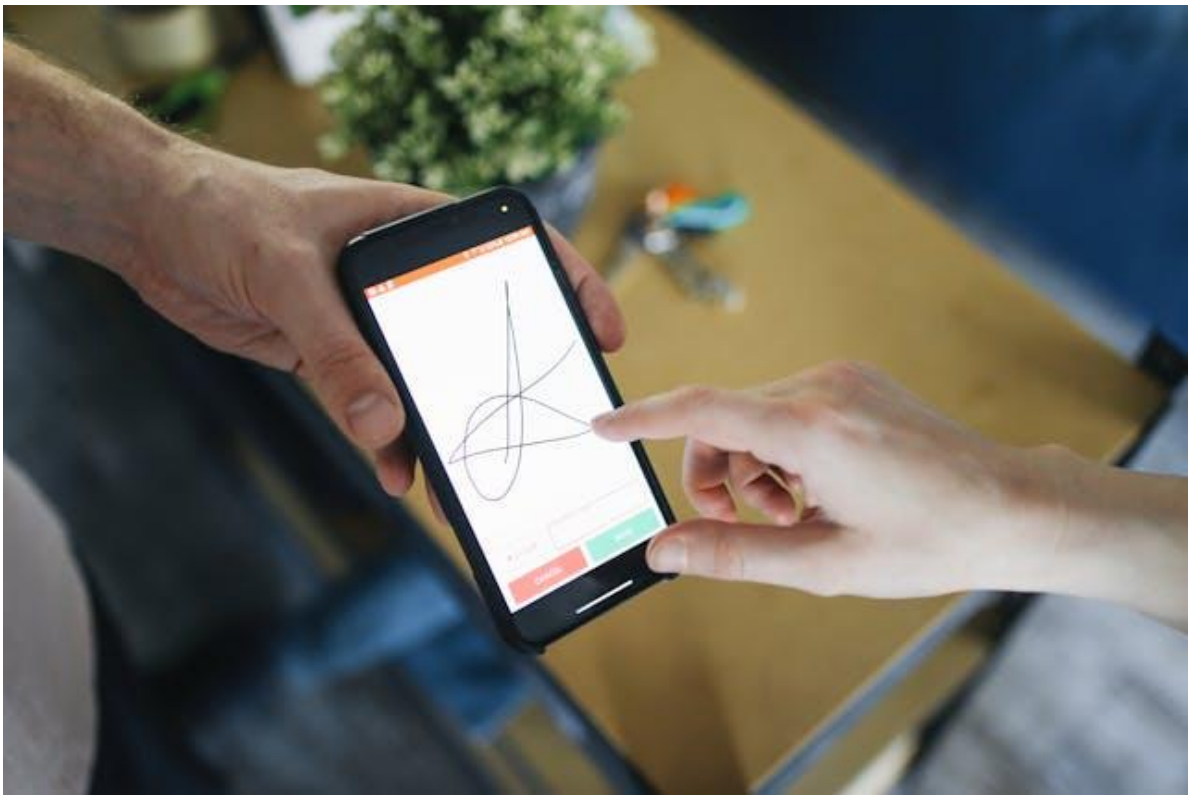
Ponadto administrator, stosownie do art. 7 ust. 3 RODO, jest zobowiązany zapewnić, aby osoba, której dane są przetwarzane, mogła wycofać zgodę w dowolnym momencie oraz z taką samą łatwością, jak jej udzieliła.

Administrator już w momencie pozyskiwania danych osobowych ma także obowiązek poinformowania osoby o prawie do wycofania zgody oraz o tym, jak tego dokonać. Zobowiązuje go do tego art. 13 ust. 2 lit. c RODO. Co więcej, Wytyczne EROD 5/2020 precyzują, że wycofanie zgody nie powinno przynieść żadnych niekorzystnych konsekwencji dla osoby, której dane są przetwarzane.

Biometria w sektorze finansowym

Jednocześnie warto przypomnieć, że w Biuletynie UODO Nr 04/04/24 w materiale „Biometryczna weryfikacja tożsamości klientów usług płatniczych" omówiona została kwestia stosowania przez instytucje finansowe analizy behawioralnej (np. sposobu pisania na klawiaturze czy sposobu poruszania myszą komputera) i tworzenia na podstawie cech charakterystycznych dla danego użytkownika jego unikalnego profilu oraz późniejsze wykorzystywanie tych danych w celu uwierzytelniania klientów usług płatniczych, co w opinii przedstawicieli środowiska finansowego ma umożliwiać ograniczanie transakcji oszukańczych w płatnościach bezgotówkowych.

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



fot. pexels

PREZES UODO NAKAZUJE USUNIĘCIE ZDJĘCIA DZIECKA Z PRYWATNEGO PROFILU POLITYKA

Radny miasta Ś. nie miał prawa udostępniać na swoim profilu na Facebooku zdjęcia dziecka uczestniczącego w samorządowej imprezie.

Opiekunowie dziecka poskarżyli się do PUODO, że radny miasta Ś. udostępnił na Facebooku jego zdjęcia. Na kilku wizerunek jest wystarczająco wyraźny, by możliwa była jego identyfikacja. Ojciec wskazał w skardze, że nie udzielał na to zgody i nie chce, by to zdjęcie było wykorzystywane przez radnego, ponieważ należy do opcji politycznej, której skarżący nie popiera.

Zdjęcia, jak ustalił PUODO, zostały zrobione podczas publicznej imprezy charytatywnej. Radny wziął w niej udział i pochwalił się tym na Facebooku. Nie był jednak organizatorem tej imprezy.

Prezes UODO wskazał, że do zamieszczenia zdjęcia dziecka radny nie miał podstaw.

• Przetwarzanie danych jest zgodne z prawem, gdy jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO). Na tę przesłankę powołał się radny odnosząc się do zarzutów skargi.

• Prezes UODO nie zgodził się jednak z tym twierdzeniem wskazując, że radny nie jest organem publicznym, po drugie, brak jest przepisu, w oparciu o który radny mógłby w sposób przedmiotowy przetwarzać wizerunek dziecka i dla realizacji którego przetwarzanie to byłoby jednocześnie niezbędne. W tej sytuacji radny mógłby upublicznić zdjęcie dziecka za zgodą jego rodziców (przedstawicieli ustawowych). Ale takiej zgody nie miał.

Sygnatura sprawy: DS.523.5859.2023

PORADNIK DOTYCZĄCY NARUSZEŃ OCHRONY DANYCH OSOBOWYCH: STARE CZY NOWE PODEJŚCIE UODO?

Nowa wersja poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" spotkała się z ogromnym zainteresowaniem. Aktualizacja stała się okazją do ożywienia dyskusji wokół omawianych w tekście zagadnień.

Wersja 2.0

W ubiegłym miesiącu Prezes UODO opublikował zaktualizowaną wersję poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych". Odświeżony materiał opracowano we współpracy ze Społecznym Zespołem Ekspertów przy Prezesie UODO. Uwzględniono w nim uwagi zgłoszone w ramach konsultacji społecznych oraz doświadczenia gromadzone w ciągu ponad 6 lat obowiązywania RODO.

Nowa wersja poradnika powstała z myślą o szerokim gronie odbiorców. Jego celem było **przekazanie podstawowej wiedzy o naruszeniach ochrony danych osobowych także tym osobom, które z przepisami RODO zetknęły się po raz pierwszy.** Dlatego podczas pracy nad tekstem szczególnie zadbano, aby został on przygotowany zgodnie z zasadami prostego języka.

Przypomnijmy, że pierwszy materiał na ten temat ukazał się w czerwcu 2019 r. O jego znaczeniu oraz powodach zmian pisaliśmy już w „Biuletynie UODO".

Czy Prezes UODO zmienił podejście?

Aktualizacja poradnika wywołała ogromne zainteresowanie. Ostatnie tygodnie obfitowały w analizy, komentarze oraz ożywione dyskusje na temat naruszeń ochrony danych osobowych i związanych z nimi obowiązków. Reakcje te potwierdziły, że **otwarty dialog w tym obszarze jest potrzebny.**

W przestrzeni publicznej pojawiły się głosy wskazujące na zaostrzenie stanowiska Prezesa UODO m.in. w sprawie rozumienia naruszeń ochrony danych osobowych, wymogu ich zgłaszania czy też roli inspektora ochrony danych przy ich obsłudze. Na przestrzeni lat z pewnością ewoluował sposób, w jaki organ nadzorczy komunikuje swoje oczekiwania czy też formułuje wskazówki dotyczące prawidłowego stosowania przepisów RODO. W rzeczywistości **aktualizacja poradnika nie przyniosła jednak żadnych fundamentalnych zmian w podejściu Prezesa UODO do poruszonych w nim kwestii.**

4 NARUSZENIA I KONTROLE

Definicja naruszenia ochrony danych osobowych

Jednym z szeroko komentowanych tematów jest sposób, w jaki poradnik odnosi się do pojęcia „naruszenia ochrony danych osobowych". Zaznaczmy, że **materiał nie zastępuje przepisów RODO ani wytycznych EROD.** Przeciwnie, jego celem jest przybliżenie źródeł prawa i oficjalnych stanowisk tym administratorom, którzy nie dysponują profesjonalnym wsparciem prawnym, a także wskazanie im kierunków postępowania na wypadek zagrożeń.

Zagadnienia podjęte w poradniku zostały jednocześnie przedstawione w szerszym kontekście, uwzględniającym cele omawianych regulacji oraz misję Prezesa UODO, w tym przede wszystkim – **skuteczną ochronę osób, których dane dotyczą.** Z tej perspektywy wyczulanie administratorów na konieczność zachowania czujności i reagowania na potencjalne zakłócenia bezpieczeństwa danych osobowych na odpowiednio wczesnym etapie jest szczególnie uzasadnione.

Wyjątki od obowiązku notyfikacji

Jedną z ogólnych zasad dotyczących naruszeń ochrony danych osobowych jest konieczność zgłaszania ich organowi nadzorczemu. Wyjątki w tym zakresie zostały omówione w poradniku, jednak spotkały się z pewnymi obawami dotyczącymi potencjalnej „zmiany podejścia".

Pragniemy podkreślić, że **stanowisko Prezesa UODO w tej sprawie również pozostaje niezmienne** i w podobnym brzmieniu wyrażone zostało już w pierwotnym tekście z 2019 r. Na przestrzeni lat organ nadzorczy skutecznie powoływał się na nie w ramach licznych decyzji administracyjnych, a także precyzował je na łamach „Biuletynu UODO". Jego słuszność potwierdzona została w orzecznictwie i praktyce innych organów europejskich. Motywacją dla wprowadzonych zmian było zaś m.in. dostosowanie treści poradnika do nowych wytycznych EROD (np. 01/2021, 9/2022) oraz standardów prostego języka.

Zgłoszeniu nadal podlegają więc naruszenia ochrony danych osobowych generujące ryzyko dla praw lub wolności osób fizycznych. **Zwolnienie z obowiązku następuje wyłącznie w sytuacji, gdy ryzyko takie prawdopodobnie nie wystąpi** („brak ryzyka").

Rola inspektora ochrony danych

Choć znaczenie inspektora ochrony danych to temat wykraczający poza tematykę poradnika, jego rola w obsłudze naruszeń ochrony danych osobowych jest szczególnie istotna. Zagadnienie to było wielokrotnie podejmowane w ramach licznych wystąpień przedstawicieli organu nadzorczego, w tym także w „Biuletynie UODO" (czy też szerzej w niedawnym wydaniu specjalnym).

4 NARUSZENIA I KONTROLE

Wskazówki zaprezentowane w materiale stanowią **naturalną konsekwencję stanowiska wyrażanego przez Prezesa UODO w ostatnich latach.** Również i w tym obszarze tekst nie wprowadził zatem zmian w podejściu organu. Jego istotą jest poszanowanie uregulowanego prawem statusu inspektorów oraz dbałość o przejrzysty i właściwy podział ról.

Świadomość administratorów

Ogromne zainteresowanie i wysoka aktywność w dyskusjach toczących się wokół poradnika to niezwykle pozytywny sygnał świadczący o **rosnącej świadomości administratorów i inspektorów ochrony danych na temat bezpieczeństwa przetwarzania oraz prawidłowego stosowania RODO.**

Cieszymy się, że opublikowany przez Prezesa UODO materiał stał się impulsem do wymiany poglądów, wspólnego poszerzenia wiedzy oraz wyrażenia obaw i wątpliwości dotyczących interpretacji przepisów.

Liczymy na to, że poradnik okaże się dla Państwa przydatny, a nadchodzące wydarzenia przyczynią się do dalszego budowania otwartej komunikacji i przede wszystkim – **sprawnego systemu ochrony danych osobowych.**

fot. Okładka poradnika Obowiązki administratorów związane z naruszeniami ochrony danych osobowych. Wersja 2.0

PROBLEMATYKA OCHRONY DANYCH OSOBOWYCH A PLIKI COOKIES

W erze postępującej cyfryzacji i powszechnego korzystania z internetu, zagadnienia związane z ochroną danych osobowych zyskują fundamentalne znaczenie. Jednym z kluczowych elementów wpływających na prywatność użytkowników w przestrzeni cyfrowej są pliki cookies. Wielu internautów akceptuje je bez zastanowienia, głównie ze względu na wygodę, gdyż odrzucenie tych plików wymaga zazwyczaj większego nakładu czasu niż szybka akceptacja. Znacząca część użytkowników nie jest jednak świadoma, jak obszerne informacje o ich zachowaniach online mogą być gromadzone i przetwarzane przez witryny internetowe za pośrednictwem tzw. „ciasteczek".

Charakterystyka plików cookies

Pliki cookies to niewielkie pliki tekstowe zapisywane na urządzeniu użytkownika podczas przeglądania stron internetowych. Pełnią one różnorodne funkcje – od optymalizacji działania witryny, przez personalizację treści, po monitorowanie aktywności użytkownika w celach analitycznych i marketingowych. W ramach tej kategorii wyróżnia się kilka podstawowych typów:

- **Pliki sesyjne (session cookies):**
  - umożliwiają stronom gromadzenie informacji o użytkowniku w trakcie sesji;
  - są automatycznie usuwane po zakończeniu sesji przeglądania (wylogowaniu lub zamknięciu strony);
  - nie posiadają daty ważności, co umożliwia przeglądarce ich automatyczne usunięcie.

- **Pliki trwałe (persistent cookies):**
  - pozostają w przeglądarce przez określony, zdefiniowany czas;
  - posiadają precyzyjnie określoną datę wygaśnięcia, po której są automatycznie usuwane.

- **Pliki autoryzacyjne (authentication cookies):**
  - usprawniają proces logowania, zwiększając poziom bezpieczeństwa;
  - są generowane podczas procesu uwierzytelniania, zapewniając bezpieczne przekazywanie informacji do konkretnego użytkownika.

- **Pliki typu zombie (zombie cookies):**
  - posiadają zdolność regeneracji po usunięciu, tworząc kopie zapasowe poza przeglądarką;
  - mogą zostać odtworzone po skasowaniu, co stanowi potencjalne zagrożenie, szczególnie w kontekście cyberataków.

- **Pliki śledzące (tracking cookies):**
  - są generowane przez systemy monitorujące aktywność użytkownika;
  - gromadzą dane o zachowaniach w celu dostosowania treści, reklam czy rekomendacji produktowych do preferencji użytkownika.

Pliki cookies w kontekście ochrony danych osobowych

Ciasteczka same w sobie nie zawierają bezpośrednio danych osobowych, jednak mogą umożliwiać identyfikację użytkownika poprzez systematyczne gromadzenie informacji o jego aktywności w sieci. W szczególności cookies wykorzystywane do celów reklamowych i analitycznych mogą prowadzić do profilowania użytkowników oraz łączenia zebranych danych z innymi informacjami, co stanowi istotne ryzyko dla prywatności. Z tego względu stosowanie cookies musi pozostawać w zgodzie z zasadami ochrony danych osobowych określonymi w Rozporządzeniu o Ochronie Danych Osobowych (RODO), w tym z zasadami minimalizacji danych, przejrzystości oraz świadomej zgody.

Obligatoryjne obowiązki administratora:

• Obowiązek informacyjny – administratorzy są zobowiązani do jasnego i przejrzystego informowania użytkowników o stosowanych plikach cookies oraz celach ich przetwarzania.

• Obowiązek uzyskania zgody – użytkownik musi wyrazić świadomą i jednoznaczną zgodę na stosowanie plików cookies, w szczególności tych wykorzystywanych w celach marketingowych i analitycznych.

• Zapewnienie możliwości zarządzania zgodą – użytkownik powinien mieć zagwarantowaną możliwość efektywnego wycofania zgody na przetwarzanie plików cookies.

• Zasada minimalizacji danych – stosowanie cookies powinno być ograniczone do niezbędnego minimum, a dane gromadzone za ich pośrednictwem muszą być odpowiednio zabezpieczone.

Strategie ochrony prywatności – rekomendacje:

• świadome zarządzanie zgodą na cookies – selektywne akceptowanie tylko niezbędnych plików cookies;

• stosowanie trybu incognito – ograniczanie zakresu zapisywanych plików cookies;

• regularne czyszczenie przeglądarki z plików cookies i danych przeglądania;

• implementacja specjalistycznych narzędzi blokujących mechanizmy śledzenia.

Wytyczne EROD na temat ważnej zgody

Europejska Rada Ochrony Danych (EROD) wydała wytyczne dotyczące zgody na pliki cookies na podstawie rozporządzenia 2016/679. **Zgodnie z tymi zasadami zgoda użytkownika musi być dobrowolna, świadoma, jednoznaczna i poprzedzona wyraźnym działaniem potwierdzającym.** Nie można stosować domyślnie zaznaczonych pól wyboru, ponieważ nie spełniają one wymogu aktywnego wyrażenia zgody.

Dodatkowo, stosowanie tzw. ,,cookie walls” (czyli blokowanie dostępu do strony bez akceptacji plików cookies) jest niezgodne z RODO. Administratorzy serwisów muszą umożliwić użytkownikom łatwe wycofanie zgody w taki sam sposób, w jaki została udzielona.

Zgodnie z Wytycznymi EROD 05/2020, zgoda na pliki cookies powinna być świadoma, co oznacza, że użytkownicy muszą mieć jasne i przejrzyste informacje o tym, jakie dane są zbierane i w jakim celu.

Zasada przejrzystości

Administratorzy stron internetowych są zobowiązani do przekazywania użytkownikom jasnych, zrozumiałych i łatwo dostępnych informacji o działaniu plików cookies, aby mogli oni dokonać świadomego wyboru. Informacje te muszą być dostarczone przed uzyskaniem zgody – użytkownik powinien wiedzieć, jakie dane będą przetwarzane, przez kogo i w jakim celu.

Orzecznictwo TSUE

Trybunał Sprawiedliwości Unii Europejskiej w sprawie C-673/17 (Planet49) orzekł, że zgoda na pliki cookies nie może być uznana za ważną, jeśli została udzielona poprzez domyślnie zaznaczone pola wyboru. Natomiast w sprawie C-61/19 (Orange Romania SA) TSUE uznał, że zgoda musi być świadoma i wymaga wcześniejszego przekazywania użytkownikowi jasnych i dostępnych informacji.

5 NOWE TECHNOLOGIE

Powyższe regulacje oraz orzecznictwo potwierdzają konieczność przestrzegania danych osobowych w kontekście stosowania plików cookies. Dzięki temu użytkownicy powinni mieć realną kontrolę nad swoją prywatnością w sieci.

Dodatkowo warto zwrócić uwagę na sprawozdanie z prac grupy zadaniowej EROD dotyczące banerów cookie, w którym podkreślono potrzebę zapewnienia użytkownikom możliwości łatwego odrzucenia plików cookies i unikania nieuczciwych praktyk, takich jak ,,cookie walls" czy domyślnie zaznaczone zgody.

Podsumowanie

Pliki cookies pełnią istotną funkcję w prawidłowym funkcjonowaniu współczesnych stron internetowych, jednakże ich niekontrolowane wykorzystanie może stanowić poważne zagrożenie dla prywatności użytkowników. Dzięki regulacjom prawnym, takim jak RODO, użytkownicy uzyskali większą kontrolę nad swoimi danymi. Niemniej jednak, kluczowe znaczenie ma systematyczne podnoszenie świadomości społecznej dotyczącej mechanizmów śledzenia oraz aktywne zarządzanie ustawieniami prywatności w przeglądarkach internetowych.

Zgodnie z wytycznymi EROD zgoda na pliki cookies musi być dobrowolna, świadoma, jednoznaczna i poprzedzona aktywnym działaniem użytkownika. Nie można stosować domyślnie zaznaczonych pól wyboru ani wymuszać zgody poprzez ,,cookie walls". Ponadto, TSUE w sprawie Planet49 orzekł, że domyślne zgody nie są prawnie wiążące, a użytkownicy muszą otrzymać pełne informacje przed wyrażeniem zgody.

Odpowiedzialność za ochronę danych spoczywa zarówno na administratorach witryn internetowych, jak i na użytkownikach, którzy powinni podejmować świadome decyzje dotyczące własnej prywatności w przestrzeni cyfrowej.

UE REAGUJE NA ZAGROŻENIA ZWIĄZANE Z IMPORTEM PRODUKTÓW KUPOWANYCH NA PLATFORMACH ELEKTRONICZNYCH

W 2024 r. na rynek UE dotarło z innych krajów około 4,6 mld przesyłek o niskiej wartości (do 150 euro). Oznacza to średnio 12 mln paczek dziennie, a w porównaniu z rokiem poprzednim – jest ich dwa razy więcej. Wiele z produktów w tych przesyłkach było niezgodnych z przepisami UE. Importowane do UE produkty mogą być szkodliwe, ich sprzedaż może stanowić nieuczciwą konkurencję z punktu widzenia unijnych sprzedawców, którzy przestrzegają przepisów, a masowy przepływ towarów może negatywnie wpływać na środowisko.

Komisja Europejska opracowała **pakiet na rzecz bezpiecznego i zrównoważonego handlu elektronicznego,** który zawiera następujące propozycje:

• **Reforma celna**: szybkie zatwierdzenie reform unii celnej i zniesienie zwolnienia z cła dla przesyłek o niskiej wartości, aby umożliwić szybkie wdrożenie nowych przepisów i chronić uczciwą konkurencję;

• **Surowsza kontrola towarów importowanych**: wprowadzenie skoordynowanych kontroli realizowanych przez organy celne i organy nadzoru rynku oraz zorganizowanych kontroli bezpieczeństwa produktów;

• **Ochrona klientów internetowych platform handlowych**: egzekwowanie aktu o usługach cyfrowych, aktu o rynkach cyfrowych, rozporządzenia w sprawie ogólnego bezpieczeństwa produktów i rozporządzenia w sprawie współpracy w dziedzinie ochrony konsumentów;

• **Stosowanie narzędzi cyfrowych**: nadzorowanie handlu elektronicznego za pomocą cyfrowego paszportu produktu i nowych narzędzi opartych na sztucznej inteligencji;

• **Ostrzejsze metody ochrony środowiska**: przyjęcie planu działania dotyczącego rozporządzenia w sprawie ekoprojektu dla zrównoważonych produktów i poparcie zmian w dyrektywie ramowej w sprawie odpadów;

• **Działania informacyjne**: informowanie konsumentów i przedsiębiorców o ich prawach, uczulanie ich na zagrożenia związane z handlem elektronicznym;

6 SPRAWY MIĘDZYNARODOWE

• **Ściślejsza współpraca międzynarodowa i wymiana handlowa**: szkolenia z unijnych przepisów bezpieczeństwa produktów dla partnerów spoza UE oraz przeciwdziałanie dumpingowi i subsydiowaniu.

Komisja zachęca kraje UE, współprawodawców i zainteresowane strony do współpracy i wdrożenia tych środków. W ciągu roku Komisja oceni skuteczność działań i w razie potrzeby może zaproponować kolejne.

Około 70 proc. Europejczyków regularnie robi zakupy przez internet, również na platformach handlu elektronicznego poza UE. Handel elektroniczny daje konsumentom, firmom i gospodarce UE wiele korzyści, ale wiąże się również z określonymi wyzwaniami. Nowa inicjatywa ma w równym stopniu chronić konsumentów, uczciwą konkurencję i zrównoważony rozwój, a jednocześnie promować bezpieczny i sprzyjający wysokiej jakości produktów rynek e-handlu w UE.

Więcej informacji

Komunikat prasowy: Komisja ogłasza działania na rzecz bezpiecznego i zrównoważonego importu w handlu elektronicznym

Komunikat w sprawie kompleksowego unijnego pakietu na rzecz bezpiecznego i zrównoważonego handlu elektronicznego

Ulotka z podsumowaniem komunikatu

Pytania i odpowiedzi na temat komunikatu

Safety Gate: unijny system wczesnego ostrzegania o niebezpiecznych produktach niespożywczych

Źródło: artykuł Komisji Europejskiej

KOMISJA POPIERA WŁĄCZENIE DOBROWOLNEGO KODEKSU POSTĘPOWANIA W ZAKRESIE DEZINFORMACJI DO AKTU O USŁUGACH CYFROWYCH

Komisja Europejska i Europejska Rada Usług Cyfrowych poparły integrację dobrowolnego Kodeksu postępowania w zakresie dezinformacji w ramach Aktu o usługach cyfrowych (DSA). Integracja ta uczyni Kodeks punktem odniesienia przy określaniu zgodności platform z DSA.

W styczniu 2025 r. sygnatariusze Kodeksu – w tym firmy wyznaczone w ramach DSA jako bardzo duże platformy internetowe i wyszukiwarki (VLOPE), takie jak Google, Meta, Microsoft i TikTok – złożyli wszystkie niezbędne dokumenty popierające ich wniosek o przekształcenie go w Kodeks postępowania w ramach DSA.

Aby zostać uznanym za dobrowolny kodeks postępowania DSA, Kodeks musi spełniać kryteria określone w ustawie o usługach cyfrowych. Komisja i Rada przyjęły w tym względzie oddzielne pozytywne oceny, popierając oficjalną integrację Kodeksu z ramami DSA.

Dzięki integracji pełne przestrzeganie Kodeksu może być uważane za odpowiedni środek łagodzenia ryzyka dla sygnatariuszy wyznaczonych jako VLOP i VLOSE w ramach DSA. W związku z tym Kodeks stanie się istotnym i znaczącym punktem odniesienia przy określaniu zgodności z DSA. Zgodność ze zobowiązaniami wynikającymi z Kodeksu będzie również częścią corocznego niezależnego audytu, któremu podlegają te platformy na mocy DSA.

Kodeks postępowania w sprawie dezinformacji

Kodeks jest powszechnie uznawanym, solidnym zestawem zobowiązań, które razem stanowią silny zestaw środków łagodzących dla zgodności z DSA. Wartość tych zobowiązań polega na tym, że są one wynikiem porozumienia między szeroką grupą podmiotów, opartego na istniejących najlepszych praktykach branżowych. Biorąc pod uwagę złożoność i wyzwania związane z walką z rozprzestrzenianiem się dezinformacji, Kodeks zawiera różne, ale powiązane ze sobą obszary:

• Demonetyzacja: ograniczenie zachęt finansowych dla dostawców dezinformacji;

• Przejrzystość reklam politycznych: skuteczniejsze etykietowanie dla użytkowników w celu rozpoznawania reklam politycznych;

• Zapewnienie integralności usług: ograniczenie fałszywych kont, wzmocnienia napędzanego przez boty, złośliwych deepfake'ów i innych manipulacyjnych zachowań wykorzystywanych do rozprzestrzeniania dezinformacji;

• Wzmocnienie pozycji użytkowników, badaczy i społeczności weryfikującej fakty: lepsze narzędzia dla użytkowników do identyfikacji dezinformacji, szerszy dostęp do danych, zasięg weryfikacji faktów w całej UE.

Środki te zwalczają ryzyko dezinformacji, jednocześnie w pełni chroniąc wolność słowa i zwiększając przejrzystość.

Zalecenia dotyczące wdrożenia Kodeksu

W ramach odpowiednich ocen, czy Kodeks spełnia kryteria określone w artykule 45 DSA, Komisja i Europejska Rada Usług Cyfrowych zachęcają platformy sygnatariuszy do uwzględnienia kilku zaleceń podczas wdrażania Kodeksu postępowania w zakresie dezinformacji.

Obejmuje to szybkie sfinalizowanie Systemu szybkiego reagowania obejmującego wszystkie wybory krajowe i kryzysy oraz jego skuteczne wdrożenie; szybką dyskusję Zespołu zadaniowego i konkretne działania następcze dotyczące ich zobowiązań w kluczowych obszarach wymienionych powyżej; oraz dostarczenie wszystkich niezbędnych danych w celu uzupełnienia luk w ich sprawozdawczości i umożliwienia dalszego rozwoju i efektywnego pomiaru wskaźników strukturalnych – w tym nowych.

Kolejne kroki

Konwersja Kodeksu wejdzie w życie 1 lipca 2025 r., dzięki czemu jego zobowiązania będą podlegać audytowi od tej daty. Ten czas pozwoli na synchronizację audytu zobowiązań Kodeksu z audytem DSA dla odpowiednich dostawców VLOP i VLOSE.

Komisja i Rada będą monitorować i oceniać realizację celów Kodeksu zgodnie z artykułem 45 DSA.

Kontekst

W 2018 r. po raz pierwszy przedstawiciele platform internetowych, wiodących firm technologicznych i podmiotów z branży reklamowej połączyli siły, aby zwalczać dezinformację na zasadzie dobrowolności i samoregulacji. Poprzez zestaw zobowiązań sygnatariusze przedstawili pierwszą wersję Kodeksu postępowania w zakresie dezinformacji.

6 SPRAWY MIĘDZYNARODOWE

Na podstawie wytycznych Komisji Kodeks został znacznie wzmocniony w czerwcu 2022 r., kiedy został przedstawiony i podpisany przez 34 sygnatariuszy. Od tego czasu Kodeks ma rosnącą bazę sygnatariuszy, z 42 sygnatariuszami do tej pory.

W ramach Kodeksu na rok 2022 sygnatariusze zgodzili się ustanowić ramy ścisłej współpracy za pośrednictwem Stałej Grupy Zadaniowej. Kodeks i jego Grupa Zadaniowa udowodniły swoją skuteczność w wymianie informacji i współpracy między sygnatariuszami. W szczególności System Szybkiego Reagowania Kodeksu okazał się bardzo skutecznym narzędziem, zwłaszcza podczas wyborów europejskich, i pozwala organizacjom społeczeństwa obywatelskiego, weryfikatorom faktów i platformom internetowym współpracować w zakresie treści wrażliwych na czas, które ich zdaniem stanowią zagrożenie dla integralności procesu wyborczego.

Źródło: informacja prasowa Komisji Europejskiej

fot. pixabay

UE URUCHAMIA INICJATYWĘ INVESTAI MAJĄCĄ NA CELU PRZEZNACZENIE 200 MILIARDÓW EURO INWESTYCJI W SZTUCZNĄ INTELIGENCJĘ

Na szczycie poświęconym działaniom na rzecz sztucznej inteligencji (AI) w Paryżu przewodnicząca Komisji Ursula von der Leyen uruchomiła InvestAI, inicjatywę mającą na celu zmobilizowanie 200 miliardów euro na inwestycje w AI, w tym nowy europejski fundusz w wysokości 20 miliardów euro na gigafabryki AI. Tak duża infrastruktura AI jest potrzebna, aby umożliwić otwarty, wspólny rozwój najbardziej złożonych modeli sztucznej inteligencji.

Przewodnicząca Komisji Ursula von der Leyen powiedziała: „AI poprawi naszą opiekę zdrowotną, pobudzi nasze badania i innowacje oraz zwiększy naszą konkurencyjność. Chcemy, aby AI była siłą napędową dobra i wzrostu. Robimy to poprzez nasze własne europejskie podejście – oparte na otwartości, współpracy i doskonałych talentach. Jednak nasze podejście nadal musi zostać doładowane. Dlatego też wspólnie z państwami członkowskimi i partnerami zmobilizujemy bezprecedensowy kapitał za pośrednictwem InvestAI na rzecz europejskich gigafabryk AI.
To wyjątkowe partnerstwo publiczno-prywatne, podobne do CERN dla AI, umożliwi wszystkim naszym naukowcom i firmom – nie tylko największym – opracowanie najbardziej zaawansowanych, bardzo dużych modeli potrzebnych do uczynienia z Europy kontynentu AI”.

Prezes Europejskiego Banku Inwestycyjnego, Nadia Calviño, powiedziała: „Wspólnie z Komisją Europejską Grupa EBI zwiększa wsparcie dla sztucznej inteligencji, kluczowego czynnika napędzającego innowacyjność i produktywność w Europie”.

Fundusz InvestAI UE sfinansuje cztery przyszłe gigafabryki AI w całej UE. Nowe gigafabryki AI będą specjalizować się w szkoleniu najbardziej złożonych, bardzo dużych modeli AI. Takie modele nowej generacji wymagają rozległej infrastruktury obliczeniowej do przełomów w określonych dziedzinach, takich jak medycyna czy nauka. Gigafabryki będą miały około 100 000 chipów AI ostatniej generacji, około cztery razy więcej niż fabryki AI, które są obecnie zakładane.

Gigafabryki finansowane przez InvestAI będą największym partnerstwem publiczno-prywatnym na świecie na rzecz rozwoju godnej zaufania AI. Będą one służyć europejskiemu modelowi kooperatywnej, otwartej innowacji, ze szczególnym uwzględnieniem złożonych zastosowań

przemysłowych i misji krytycznych. Celem jest, aby każda firma, nie tylko najwięksi gracze, miała dostęp do mocy obliczeniowej na dużą skalę, aby móc budować przyszłość.

InvestAI będzie obejmować fundusz warstwowy z udziałami o różnych profilach ryzyka i zwrotu. Budżet UE ograniczy ryzyko inwestycji innych partnerów. Początkowe finansowanie Komisji dla InvestAI będzie pochodzić z istniejących programów finansowania UE, które mają komponent cyfrowy, takich jak Program Cyfrowa Europa i Horyzont Europa oraz InvestEU. Państwa członkowskie mogą również wnieść swój wkład, programując fundusze ze swoich kopert spójności. Finansowanie gigafabryk AI za pomocą mieszanki dotacji i kapitału własnego będzie stanowić jeden z przypadków pilotażowych dla strategicznych technologii ogłoszonych w Kompas konkurencyjności.

Komisja ogłosiła już budowę siedmiu fabryk AI w grudniu i wkrótce ogłosi budowę kolejnych pięciu. Obecne wsparcie dla fabryk AI w wysokości 10 miliardów euro, współfinansowane przez UE i państwa członkowskie, jest już największą publiczną inwestycją w AI na świecie i odblokuje ponad dziesięciokrotnie więcej prywatnych inwestycji. Zapewnia już ogromny dostęp start-upów i przemysłu do superkomputerów.

Kontekst

Oprócz funduszu InvestAI, Komisja podejmuje wiele działań w różnych dziedzinach, aby wspierać innowacje w zakresie AI w Europie. Fabryki AI są najważniejszym elementem pakietu Komisji dotyczącego innowacji w zakresie AI przedstawionego w styczniu 2024 r., wraz z:

• Wsparciem finansowym za pośrednictwem programu Horyzont Europa i programu Cyfrowa Europa poświęconego generatywnej AI;

• Towarzyszącymi inicjatywami mającymi na celu wzmocnienie unijnej puli talentów w zakresie generatywnej AI poprzez działania edukacyjne, szkoleniowe, umiejętności i przekwalifikowanie;

• Dalszym zachęcaniem do publicznych i prywatnych inwestycji w start-upy i scale-upy AI, w tym poprzez kapitał wysokiego ryzyka lub wsparcie kapitałowe;

• Przyspieszeniem rozwoju i wdrażania wspólnych europejskich przestrzeni danych, udostępnionych społeczności AI, dla której dane są kluczowym zasobem do szkolenia i ulepszania ich modeli.

Celem inicjatywy „GenAI4EU” jest wspieranie rozwoju nowych przypadków użycia i powstających aplikacji w 14 ekosystemach przemysłowych Europy, a także w sektorze publicznym. Obszary zastosowań obejmują robotykę, zdrowie, biotechnologię, produkcję, mobilność, klimat i światy wirtualne.

6 SPRAWY MIĘDZYNARODOWE

Komisja utworzy również Europejską Radę ds. Badań nad AI, w ramach której Europa będzie mogła łączyć zasoby i badać, w jaki sposób może wykorzystać potencjał danych do wspierania AI i innych technologii. W dalszej części roku Komisja uruchomi inicjatywę „Apply AI", aby napędzać przemysłową adopcję sztucznej inteligencji w kluczowych sektorach.

Źródło: informacja prasowa Komisji Europejskiej

fot. pexels

WEBINARIUM „NARUSZENIE PRYWATNOŚCI W MEDIACH SPOŁECZNOŚCIOWYCH – MEDIACJE JAKO SPOSÓB ROZWIĄZYWANIA KONFLIKTÓW”

5 marca zorganizowaliśmy lekcję dla uczniów, którzy biorą udział w Programie „Twoje dane – Twoja sprawa”. Prowadząca spotkanie zwróciła uwagę młodych ludzi na zagrożenia związane z naruszeniem prywatności w mediach społecznościowych oraz przedstawiła mediację, jako skuteczną metodę rozwiązywania konfliktów wynikających z niewłaściwego z nich korzystania.

Obecnie trwa XV edycja ogólnopolskiego programu edukacyjnego Prezesa Urzędu Ochrony Danych Osobowych „Twoje dane – Twoja sprawa”, którego celem jest upowszechnienie wiedzy o ochronie danych osobowych wśród uczniów i nauczycieli poprzez poszerzenie oferty edukacyjnej szkół oraz placówek doskonalenia zawodowego nauczycieli o treści związane z ochroną danych osobowych i prawem do prywatności. W ramach Programu systematycznie organizowane są różnorodne działania edukacyjne, takie jak lekcje online obejmujące zagadnienia związane z ochroną danych osobowych oraz prawem do prywatności. Nagrania webinariów wzbogacają platformę edukacyjną dostępną dla uczestników realizujących Program.

Spotkania z uczniami wzmacniają kompetencje bezpiecznego funkcjonowania dzieci i młodzieży w świecie nowych technologii oraz podkreślają wartości ochrony prywatności i danych osobowych w życiu każdego człowieka.

Lekcje są realizowane z udziałem ekspertów Urzędu Ochrony Danych Osobowych oraz liderów Programu, czyli nauczycieli - koordynatorów, którzy wyróżniają się szczególnym zaangażowaniem w realizację założeń „Twoje dane – Twoja sprawa”, jakimi są edukacja i propagowanie odpowiednich postaw związanych z ochroną danych osobowych i prywatności wśród społeczności szkolnych i lokalnych.

I tak w marcu została zorganizowana lekcja online dla uczniów „Naruszenie prywatności w mediach społecznościowych – mediacje jako sposób rozwiązywania konfliktów”, którą poprowadziła Pani Aleksandra Czarnobaj – nauczycielka i koordynatorka Programu w Zespole Szkół nr 1 im. Stanisława Staszica w Kwidzynie. Szkoła scenariuszem pt. „Mediacja rówieśnicza jako metoda rozwiązywania konfliktu wynikającego z niewłaściwego postępowania w mediach społecznościowych” zajęła

7 EDUKACJA

II miejsce w ogólnopolskim konkursie Prezesa UODO „Inicjatywa edukacyjna roku 2023/2024" organizowanego w ramach XIV edycji programu „Twoje dane – Twoja sprawa".

Prowadząca pokazała, że mediacja to nie tylko sposób na rozwiązanie konfliktu, ale także szansa na budowanie empatii i odpowiedzialności za swoje działania w sieci oraz w realnym, codziennym życiu. Pomaga również w zrozumieniu perspektywy drugiej osoby i uczy szacunku dla prywatności innych.

Podstawą mediacji jest komunikacja. Skuteczna komunikacja to klucz do rozwiązania wielu sporów, a umiejętność prowadzenia konstruktywnej rozmowy jest bardzo cenna. Jest to proces wymiany informacji, w którym nadawca przekazuje wiadomość w sposób jasny i zrozumiały, a odbiorca właściwie ją interpretuje i rozumie jej treść. Obejmuje nie tylko słowa, ale także ton głosu, mowę ciała oraz umiejętność aktywnego słuchania.

Celem skutecznej komunikacji jest osiągnięcie wzajemnego porozumienia między stronami. Ma ona ogromny wpływ na wiele aspektów życia, w tym na relacje międzyludzkie, sukcesy osobiste i zawodowe. To, jak postrzegają nas inni, w dużej mierze zależy od tego, jak się komunikujemy. Podczas webinarium słuchacze mogli dowiedzieć się jakie bariery mogą utrudniać komunikację oraz jak rozwijać umiejętność aktywnego słuchania.

Uczestnicy dowiedzieli się również, że naturalnym elementem relacji międzyludzkich są konflikty, które mogą wynikać z różnic w sposobie myślenia, odczuwania i reagowania. Niestety nawet najlepsza komunikacja nie jest w stanie ich całkowicie wyeliminować. Bardzo często przekonanie o anonimowości w sieci prowadzi do licznych przypadków nadużyć, nieodpowiedzialnych działań, a nawet naruszeń prywatności, które mogą mieć poważne konsekwencje prowadzące do konfliktów i napięć.

Przeprowadzona lekcja wyposażyła uczestników w wiedzę na temat mediacji oraz sposobów radzenia sobie z trudnymi sytuacjami, tak aby mogli skutecznie rozwiązywać konflikty i budować lepsze relacje.

W każdej edycji programu, UODO dokłada wszelkich starań, aby przygotowywane materiały edukacyjne, cechowały się adekwatną tematyką do realiów społeczeństwa informacyjnego, a zakres merytoryczny zajęć online był przydatny w codziennym funkcjonowaniu uczniów.

Nieocenione staje się wsparcie nauczycieli uczestniczących w Programie – ambasadorów ochrony danych osobowych, dzięki którym możliwe staje się podkreślanie wagi ochrony danych osobowych w szkołach, podczas prowadzonych przez nich zajęć i realizacji innych inicjatyw w ich placówkach. Dzięki naszym szkolnym ambasadorom ochrony danych osobowych wiemy, jakie są rzeczywiste

potrzeby szkół, tak aby proponowane inicjatywy oraz przygotowywane materiały stanowiły przydatne źródło wiedzy i dobrych praktyk dla nauczycieli w zakresie ochrony danych osobowych, w związku z realizacją obowiązków wynikających z RODO w sektorze oświaty. Rezultatem podejmowanych działań w ramach Programu, staje się odpowiednia wiedza i umiejętności uczniów w zakresie ochrony ich prywatności.

fot. pexels

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl