URZĄD OCHRONY DANYCH OSOBOWYCH

# BIULETYN UODO
# Nr 06/06/24

www.uodo.gov.pl

# SPIS TREŚCI

**Szanowni Państwo,**

najważniejszym wydarzeniem dla Urzędu Ochrony Danych Osobowych w czerwcu było powołanie Społecznego Zespołu Ekspertów.

Członkiniami i członkami są osoby, które wyrobiły sobie wielką zawodową markę w dziedzinie, która nas wszystkich interesuje. Zgodziły się nas wspierać.

Powołanie Zespołu jest kolejnym dowodem na to, jak uspołeczniamy pracę Urzędu i sięgamy po wiedzę oraz diagnozy zebrane przez ekspertów i aktywistów.

Kontynuuję spotkania z przedstawicielami środowiska IOD. Miałem przyjemność rozmawiać z inspektorami danych osobowych w kościołach i związkach wyznaniowych. Zaczynamy też cykl spotkań z inspektorami ochrony danych osobowych w instytucjach samorządowych.

W czerwcu zakończyliśmy też zbieranie uwag do pierwszej partii poradników UODO porządkujących wiedzę w różnych dziedzinach wiedzy o danych osobowych. Chcemy, by nasze materiały były zrozumiałe i odpowiadały na kluczowe problemy naszych partnerów, a także przedstawicieli biznesu, instytucji, organizacji społecznych i społeczeństwa.

Do dwóch pierwszych poradników (o przetwarzaniu danych przy zatrudnianiu i o reagowaniu na naruszenia danych osobowych) dostaliśmy mnóstwo cennych uwag. Potwierdza to, jak wiele możemy osiągnąć wspólnie, wykorzystując wiedzę, którą mają sieci społeczne Urzędu. Wkrótce wszystkie nadesłane uwagi zostaną udostępnione na naszej stronie. Już pracujemy nad aktualizacją poradników.

Będziemy konsultowali kolejne poradniki UODO. Korzystając z tej okazji chciałbym Państwa zachęcić do zgłaszania uwag. Będziemy też wykorzystywać mechanizm konsultacji społecznych przy okazji innych projektów.

***Mirosław Wróblewski***
*Prezes UODO*

## Drodzy Czytelnicy!

Dzisiejszy wstęp ograniczę do jednego tematu. Jest on bardzo ważny i chcę aby wybrzmiał odpowiednio wyraźnie.

Mam nadzieję, że Biuletyn UODO jest dla Was cennym źródłem informacji w dziedzinie przetwarzania danych osobowych. Rozsyłanie Biuletynu jest jednak także przetwarzaniem danych osobowych w praktyce. By być w zgodzie z zasadą prawidłowości danych, musimy zaktualizować dane abonentów.

**Dlatego od września 2024 r. Biuletyn trafi tylko do tych z Państwa, którzy potwierdzą chęć otrzymywania go**.

To ważny ruch. W czasie wakacji będziemy o tym Państwu przypominali. Od września lista dystrybucyjna Biuletynu zostanie już zmieniona, a dane osób, które nie potwierdzą chęci dalszego utrzymywania kontaktu z nami, usunięte.

Pamiętajcie! Czekamy na Was – jesteście dla nas bardzo Ważni. To dzięki Wam, naszym Czytelniczkom i Czytelnikom, wiedza o przetwarzaniu i ochronie danych osobowych szerzy się w Polsce.

***Karol Witowski***
*p.o. Rzecznika Prasowego UODO*

URZĄD OCHRONY DANYCH OSOBOWYCH

**Drodzy Subskrybenci „Biuletynu UODO”,**

jedną z zasad ogólnych przetwarzania danych osobowych, jest zasada prawidłowości danych.

Dziś baza subskrybentów „Biuletynu UODO” liczy kilka tysięcy osób, zauważyliśmy jednak, że wiele adresów e-mail, na który wysyłamy Biuletyn, jest już nieaktualnych.

Od dziś zbieramy zapisy do subskrypcji od nowa. Ci z Państwa, którzy nie zapiszą się do nowej bazy danych do 31 sierpnia 2024 r., od **1 września** przestaną otrzymywać Biuletyn.

Dlatego, jeśli tematy dotyczące ochrony danych osobowych są Wam bliskie, serdecznie zachęcamy do ponownej subskrypcji już teraz.

*Robert Miętkowski,*
Inspektor Ochrony Danych w UODO

**Zapisz się!**

# 1 ROZMOWA Z EKSPERTEM

## ZAWSZE JESTEM OTWARTY, ŻEBY PODSUNĄĆ ROZWIĄZANIE, KTÓRE UWAŻAM ZA NAJLEPSZE W DANEJ SPRAWIE

**Z Robertem Miętkowskim, zatrudnionym na samodzielnym stanowisku Inspektora Ochrony Danych w UODO rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO**

**Od 1 września br. zaczynamy od podstaw proces gromadzenia nowych adresów mailowych subskrybentów „Biuletynu UODO". Skąd taka decyzja?**

Jedną z zasad ogólnych przetwarzania danych osobowych jest zasada prawidłowości. Przepisy rozporządzenia 2016/679 wymagają, by dane osobowe były prawidłowe i w razie potrzeby uaktualniane.

Baza danych subskrybentów „Biuletynu UODO" to kilka tysięcy adresów poczty elektronicznej. Wiele z nich zawiera imię, nazwisko, a domena wskazuje na nazwę organizacji.

Musimy sprawdzić, czy wszystkie adresy mailowe, do których dociera biuletyn są aktualne. Nie chcemy przetwarzać nieaktualnych adresów e-mail, więc prosimy czytelników o ponowne zapisanie się do subskrypcji.

**IOD w UODO zajmuje się sprawami dotyczącymi przetwarzania danych obywateli przez UODO, w tym sprawami dotyczącymi realizacji ich praw w zakresie dostępu do sprostowania, usuwania, ograniczenia przetwarzania czy sprzeciwu na przetwarzanie danych. Czego najczęściej dotyczą sprawy, które do Pana wpływają?**

Większość spraw dotyczy przetwarzania danych osobowych w toku postępowań administracyjnych. Wielu obywatelom nie podobają się decyzje administracyjne i liczą, że jako IOD mam wpływ na ich treść. Oczywiście tak nie jest. Zdarzają się przypadki, w których klienci instytucji publicznych chcą przepisy Kodeksu postępowania administracyjnego obchodzić przepisami o ochronie danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych jest organem właściwym w sprawie ochrony danych osobowych oraz jednocześnie administratorem. Do Prezesa UODO jako administratora wpływają

również wnioski dotyczące realizacji praw osób, których dane dotyczą. Prezes UODO, jako organ właściwy w sprawie ochrony danych, działa na podstawie i w granicach przepisów prawa, tymczasem wiele osób kieruje do administratora informację o wycofaniu zgody na przetwarzanie ich danych osobowych oraz żądanie ich usunięcia po zakończonym postępowaniu administracyjnym.

Przetwarzanie danych osobowych, w toku prowadzonych przez Prezesa UODO postępowań, jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Dodatkowo po zakończeniu czynności w sprawie, wszelaka dokumentacja wytworzona w czasie jej trwania musi zostać zarchiwizowana zgodnie z przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz obowiązującym w Urzędzie Ochrony Danych Osobowych Jednolitym Rzeczowym Wykazem Akt. Dlatego też żądanie usunięcia danych osobowych nie może być zrealizowane.

Do Prezesa UODO jako administratora wpływają również wnioski na podstawie art. 16 rozporządzenia 2016/679, od stron postępowania administracyjnego, o sprostowanie danych osobowych, w toku trwających postępowań, zawartych w treści zgromadzonego w sprawie materiału dowodowego. Na postawie art. 58 ust. 1 lit. a) i e) rozporządzenia 2016/679, Prezes UODO w zakresie prowadzonych postępowań może nakazać administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań oraz ma prawo uzyskać od administratora lub podmiotu przetwarzającego dostęp do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań.

Natomiast zgodnie z art. 7 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, w postępowaniach w sprawie naruszeń przepisów o ochronie danych, prowadzonych przez Prezesa UODO, stosuje się ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Zgodnie z przepisami kpa organ prowadzący postępowanie zobowiązany jest do podejmowania wszelakich czynności niezbędnych do ustalenia stanu faktycznego sprawy zgodnego z rzeczywistością, w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy, a także ocenić na podstawie całokształtu zebranego materiału dowodowego, czy dana okoliczność została udowodniona. Nie jest więc możliwe sprostowanie danych osobowych, które stanowią materiał dowodowy zawarty w aktach postępowania administracyjnego.

Zdarzają się również wnioski, skierowane do administratora na podstawie art. 15 ust. 3 rozporządzenia 2016/679, o dostarczenie kopii akt lub dokumentów zawartych w aktach postępowania administracyjnego.

# 1 ROZMOWA Z EKSPERTEM

Tymczasem prawa do otrzymania kopii danych osobowych na podstawie art. 15 ust. 3 rozporządzenia 2016/679 nie należy utożsamiać z uregulowanym w art. 73 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, prawem strony postępowania administracyjnego dotyczącym wglądu w akta sprawy i sporządzania z nich notatek, kopii lub odpisów, żądania uwierzytelnienia odpisów lub kopii akt sprawy lub wydania z akt sprawy uwierzytelnionych odpisów, o ile jest to uzasadnione ważnym interesem strony. Są to bowiem dwa różne prawa i służą różnym celom. Prawo dostępu do akt postępowania nie może być dochodzone na mocy rozporządzenia 2016/679, w trybie realizacji prawa do otrzymania kopii danych osobowych.

Chciałbym też obalić mit zgody jako jedynej podstawy przetwarzania danych. Wciąż wielu obywateli powołuje się na przesłankę zgody, niezależnie od przedmiotu, jakiego dotyczy sprawa. Często muszę tłumaczyć, że przetwarzanie danych osobowych w celu realizacji kompetencji władczych Prezesa UODO nie wymaga zgody osoby, której dane dotyczą.

**Jakie są najtrudniejsze sprawy, którymi zajmuje się IOD w krajowym organie nadzorczym do spraw ochrony danych osobowych?**

Wbrew pozorom najtrudniejsze wcale nie są sprawy zgłaszane przez obywateli. Dla mnie największe wyzwanie stanowi docieranie się stanowisk w danej sprawie przez departamenty wewnątrz Urzędu. Sami potrafimy patrzeć z różnych punktów widzenia na daną kwestię. Inne problemy wychodzą na pierwszy plan, gdy analizuje je IOD, a inne, gdy przedstawiciel Departamentu Kontroli i Naruszeń czy Departamentu Orzecznictwa i Legislacji.

Dlatego poddajemy propozycje rozwiązań pod dyskusję, by razem wypracować takie, które wspólnie uznajemy za najbardziej adekwatne. Droga ku temu nie należy do najłatwiejszych, ale warto się docierać, bo wtedy powstają najlepsze rozwiązania. W rezultacie chcemy przedstawić takie, które są spójne z opiniami wydanymi przez poszczególne departamenty.

**Pracownicy Infolinii UODO codziennie odbierają dziesiątki, a nawet setki telefonów od obywateli. Czy eksperci infolinii konsultują z Panem problemy, z jakimi borykają się nasi klienci, którzy często spodziewają się wydania jasnego stanowiska Urzędu w danej sprawie?**

Zdarzają się takie konsultacje. Zawsze jestem otwarty, żeby podsunąć rozwiązanie, które uważam za najlepsze w danej sprawie. Szczególnie, że chodzi tu o konkretną osobę, której chcemy pomóc. Zagadnienia poruszane przez infolinię na pewno są dużym motorem do zmian, przyczyniają się do wydawania konkretnych stanowisk, jednak moja opinia, podobnie jak pomoc udzielona przez infolinię nie ma mocy wiążącej.

# 1 ROZMOWA Z EKSPERTEM

Osoby ze wszystkich departamentów są u mnie zawsze mile widziane. Lubię słuchać opinii innych i dzielić się własnym zdaniem. Choć podkreślę, że na pytania z niektórych sektorów np. zdrowia, pewnie niewiele mam do powiedzenia, z innych – np. z sektora publicznego – dużo więcej.

**RODO wymaga systematycznych działań zwiększających świadomość kadry samego Urzędu. Nową inicjatywą w tym zakresie ma być stworzenie wygaszacza ekranu ze slajdami – prostymi komunikatami, przypominającymi o tym jak pracownicy Urzędu powinni dbać o bezpieczeństwo danych.**

Mam nadzieję, że już niedługo pracownicy UODO zobaczą na wygaszaczach ekranów swoich komputerów slajdy przypominające im o podstawowych zasadach bezpieczeństwa przetwarzania danych osobowych, podstawach cyberbezpieczeństwa oraz bezpieczeństwa fizycznego. Ma to na celu podniesienie świadomości pracowników, ponieważ przyczyną wielu incydentów bezpieczeństwa, mimo wdrożonych zabezpieczeń technicznych jest błąd ludzki.

Na razie powstało 25 slajdów, jest to baza otwarta, być może będzie ich więcej. Uznaję to za pewną dodatkową formę szkolenia kadry UODO. Przykładowe treści slajdów to: „Nie zapisuj haseł w przeglądarkach internetowych, nie zapisuj haseł na kartkach, nie używaj tych samych haseł w różnych systemach informatycznych oraz nie udostępniaj swojego loginu i hasła innym osobom.” Albo: „Przewozisz dokumenty papierowe między piętrami budynku, włóż je w teczkę”, „Odchodząc od komputera zablokuj urządzenie (klawisze „WIN” + „L” albo „⊞” + „L” albo „CTRL” + „ALT” + „DEL” na klawiaturze komputera)”.

Te slajdy tworzą vademecum pracownika UODO. Oczywiście haseł możemy utworzyć bardzo wiele, a podane przeze mnie tutaj treści mogą ulec małym modyfikacjom.

Dla kadry Urzędu treść haseł ze slajdów jest oczywista, jednak również o oczywistościach warto przypominać, by teoria mogła się zamienić w praktyczne działania.

**Stoi Pan – podobnie jak nasi prezesi – na stanowisku, że język należy upraszczać. Co może zrobić IOD w tym zakresie?**

Z uwagi na fakt, że Pan Mirosław Wróblewski, prezes UODO zwraca szczególną uwagę na prosty i zrozumiały język, to, czym możemy się pochwalić, to że napisaliśmy informację o przetwarzaniu danych osobowych skierowaną dla dzieci. Bardzo staraliśmy się, by była ona dla naszych odbiorców zrozumiała.

By wyjaśnić dzieciom czym są dane osobowe informowaliśmy, że dane osobowe to nie tylko imię i nazwisko, ale również nazwa szkoły i klasa do której chodzą.

# 1 ROZMOWA Z EKSPERTEM

Zastanawialiśmy się również jak wytłumaczyć dzieciom, kim jest administrator danych. Dziś nawet wielu dorosłym osobom, administrator kojarzy się przede wszystkim ze spółdzielnią mieszkaniową, użytkownikiem forum internetowego lub gry posiadającym najwyższe uprawnienia.

Ponieważ pisany przez nas obowiązek informacyjny dotyczył udziału w konkursie, zaczynał się od zdania: „Cieszymy się, że bierzesz udział w konkursie. Zanim przekażesz nam swoją pracę, która będzie zawierać między innymi Twoje dane osobowe, czyli imię, nazwisko, klasę i nazwę szkoły, mamy dla Ciebie parę informacji, o tym jak je wykorzystamy. Twoje dane osobowe są nam potrzebne, abyśmy mieli pewność, że to Ty jesteś autorem/ką pracy. Chcemy nagrodzić autorów/ki najlepszych prac, a także jeżeli się na to zgodzisz opublikujemy listę laureatów/ek konkursu na stronie internetowej Urzędu Ochrony Danych Osobowych. Po zakończeniu konkursu dane, które nam przekazałeś/łaś zostaną zarchiwizowane. Gdybyś miał/miała więcej pytań, o to jak Organizator wykorzysta Twoje dane osobowe, w pierwszej kolejności zapytaj swoich rodziców. Dla nich przygotowaliśmy szczegółowe informacje.”

To początek zmian. Bardzo nam zależy, by przekaz dla poszczególnych grup był łatwy do zrozumienia, a jednocześnie uwzględniający ich podmiotowość. Mam pomysły nowych rozwiązań, jednak by w praktyce je wprowadzić, potrzebne są większe konsultacje, rozmowy i nieustanne tłumaczenie, dlaczego te zmiany są tak ważne.

Chciałbym aby klauzule informacyjne które wykorzystuje UODO, zaczynały się od zdania: „Administratorem Twoich danych jest…, Twoje dane będziemy przetwarzać…”, jednak póki co wciąż funkcjonuje poprzednia wersja: „Państwa dane osobowe będą przetwarzane…”. Chciałbym wprowadzić stronę czynną, a unikać biernej – bo jest trudniejsza do zrozumienia.

Wprowadzenie łatwego języka jest wbrew pozorom trudne. Przywykliśmy do niektórych sformułowań i ciężko je zamienić na inne. Jak np. innymi słowami powiadomić dzieci o archiwizacji danych?

**Obecny prezes UODO bardzo dużo uwagi poświęca ochronie danych dzieci. W dużej mierze z Pana inicjatywy usunęliśmy ze strony internetowej Urzędu, dane osobowe dzieci oraz ich wizerunki. Mówimy o materiałach starszych niż 3 lata, które zostały umieszczone na stronie Urzędu po wyrażeniu zgody przez rodziców.**

Wielu administratorów zapomina o materiałach, które zamieścili na swojej stronie internetowej. Bardzo często materiały te zawierają dane osobowe. Od lat zabiegałem o wzmocnienie ochrony danych osobowych dzieci. Prezes UODO podjął decyzję, że materiały, które w swojej treści zawierają dane osobowe dzieci, opublikowane będą na stronie internetowej UODO maksymalnie przez 3 lata.

# 1 ROZMOWA Z EKSPERTEM

Jeśli chodzi o zdjęcia robione dzieciom, chciałem zwrócić uwagę na liczne zagrożenia dla dzieci, dziś nie trzeba znać obsługi skomplikowanych, zaawansowanych programów graficznych, by przerobić czyjeś zdjęcie, by np. stało się memem. Oczywiście najlepiej robić zdjęcia, na których nie ma wizerunku dzieci. Szczególnie że z dziećmi mamy często kontakt, chociażby z uwagi na prowadzony przez Urząd program skierowany do młodych uczestników – „Twoje dane – Twoja sprawa".

Obserwuję też działania innych organów nadzorczych w zakresie rozpowszechniania wizerunku.

Bardzo trudno jest znaleźć na stronie francuskiego urzędu ds. danych CNIL (Commission Nationale de l'Informatique et des Libertés) zdjęcia innych osób, niż kierownictwo francuskiego organu nadzorczego. Królują tam starannie dobrane piktogramy i grafiki, ułatwiające przekaz informacji.

Z kolei brytyjski odpowiednik naszego Urzędu – ICO (Information Commissioner's Office) – stworzył klauzulę informacyjną o przetwarzaniu danych w formie krótkiego rysunkowego filmu. Chciałbym przenieść podobne rozwiązania na nasz krajowy grunt, jednak z uwagi na ograniczony budżet nie jest to łatwe. Podobne środki pokazują, że jest wiele możliwości, by ułatwić odbiorcom szybki odczyt wizualny. Są starannie projektowane, tak aby były na nich tylko elementy niosące informacje.

Mam nadzieję, że i nasz Urząd będzie mógł wcielić w życie zbliżone koncepcje. Widzę, że dla obecnego prezesa bardzo ważnym aspektem jest upowszechnianie wiedzy o ochronie danych osobowych oraz czerpanie ze wzorców i dobrych praktyk innych regulatorów, tak by rozporządzenie zaczęło być postrzegane jako realne narzędzie skutecznej ochrony danych osobowych, a nie – jak niestety często się dotychczas zdarzało – biurokratyczne obciążenie.

**Dziękuję za rozmowę.**

# DANE NADMIAROWE W OŚWIADCZENIACH MAJĄTKOWYCH

**Podmiot zobowiązany do publikacji oświadczenia majątkowego w BIP musi czuwać nad tym, aby realizacja tego obowiązku odbywała się w sposób zgodny z RODO, w tym z poszanowaniem zasady legalizmu i minimalizacji danych.**

Dość często zdarza się, że osoby zobligowane w jednostkach samorządu terytorialnego do złożenia oświadczenia majątkowego w jego części A (część jawna) podają dane wykraczające poza ustawowy katalog. Wpisują tam np.: numer rachunku bankowego, numer rejestracyjny pojazdu, wysokość dochodów współmałżonka, mienie należące do współmałżonka, numery ksiąg wieczystych.

**Jakie dane publikować w BIP**

Skoro przepisy ustaw: o samorządzie gminnym, o samorządzie powiatowym oraz o samorządzie województwa określają zakres informacji, jakie osoby zobowiązane do złożenia oświadczeń majątkowych zobowiązane są zawrzeć w tym dokumencie, to nie ma podstaw prawnych do udostępniania danych w zakresie szerszym niż wynikający z tych przepisów.

**Odpowiedzialność administratora**

Podmiot zobowiązany do przyjęcia i publikacji oświadczenia majątkowego w BIP jako administrator danych w rozumieniu art. 4 pkt 7 RODO musi czuwać nad tym, aby realizacja obowiązku publikacji przebiegała w sposób prawidłowy, tj. zgodny z zasadami ochrony danych osobowych, m.in. legalizmu (art. 5 ust. 1 lit. a w zw. z art. 6 ust. 1 lit. c) oraz minimalizacji danych (art. 5 ust.1 lit. c RODO).

Potwierdza to również wyrok Trybunału Sprawiedliwości UE z 11 stycznia 2024 r. w sprawie C-252/21 État belge przeciwko Autorité de protection des données podkreślający odpowiedzialność administratora za dane, które publikuje (pkt 17, 32 i 52 wyroku).

**Warto przeciwdziałać**

Problem podawania danych nadmiarowych w oświadczeniach majątkowych mógłby zostać ograniczony poprzez przeprowadzenie przez administratora analizy ryzyka i wprowadzenie rozwiązań minimalizujących wykryte ryzyka związane z przetwarzaniem danych osobowych.

Do takich działań można zaliczyć:

- prowadzenie szkoleń dotyczących poprawnego wypełniania oświadczeń majątkowych,
- wprowadzenie procesów anonimizacji danych,
- czy też prowadzenie wewnętrznych audytów i kontroli związanych z przetwarzaniem danych.

Działania takie mogą i powinny być prowadzone przy wsparciu inspektora ochrony danych, do którego zadań (zgodnie z art. 39 ust. 1 lit. b RODO) należy m.in. monitorowanie stosowania RODO u danego administratora oraz prowadzenie działań zwiększających świadomość w obszarze ochrony danych osobowych.

Fot. pixabay

# OKRES PRZECHOWYWANIA PRZEZ PRACODAWCĘ DANYCH ZAWARTYCH W ORZECZENIACH O NIEPEŁNOSPRAWNOŚCI

**Pracodawcy zatrudniający osoby z niepełnosprawnością przynajmniej raz na 5 lat powinni przeprowadzić przegląd przydatności przetwarzania danych osobowych. Muszą przy tym ocenić ich niezbędność dla osiągnięcia określonych i uzasadnionych celów.**

Takich wskazówek UODO udzielił, odpowiadając na prośbę jednego z IOD o pomoc w ustaleniu okresu przechowywania przez pracodawcę danych osobowych zawartych w orzeczeniach o niepełnosprawności przekazywanych mu dobrowolnie przez pracowników chcących korzystać z uprawnień dla osób z niepełnosprawnością (np. dodatkowe urlopy, skrócony dzień pracy itp.).

Wątpliwości wynikały m.in. z tego, że część orzeczeń o niepełnosprawności jest orzeczeniami terminowymi (np. wydanymi na 5 lat). Po upływie okresu ich ważności pracownicy dostarczają nowe orzeczenia. W tej sytuacji co do zasady cel, dla którego stare orzeczenie było przetwarzane (dodatkowe uprawnienia pracownika), ustał i należałoby usunąć lub zanonimizować dane osobowe zawarte w poprzednim orzeczeniu. Co jednak w przypadku kontroli np. Państwowej Inspekcji Pracy – pytał IOD. Inspektorzy pracy mogą bowiem chcieć skontrolować akta pracownicze (które są przechowywane 50 lub 10 lat w zależności od daty zatrudnienia pracownika) i podstawę np. udzielania pracownikowi dodatkowego urlopu na podstawie orzeczenia, którego termin, na który zostało wydane, już upłynął.

Odpowiadając na tę korespondencję, UODO wskazał, że do przechowywania przez pracodawcę danych osobowych zawartych w orzeczeniach o niepełnosprawności odnoszą się szczególne przepisy prawa krajowego – ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych. Zgodnie z jej art. 2b ust. 7 pracodawcy, podmioty i osoby realizujące zadania wynikające z ustawy przechowują dane osobowe wyłącznie przez okres nie dłuższy niż jest to niezbędne i w zakresie koniecznym do realizacji celów przetwarzania danych osobowych oraz dokonują przeglądu przydatności przetwarzania danych osobowych nie rzadziej niż co 5 lat.

Jednocześnie UODO przypomniał, że zgodnie z zasadą ograniczenia przechowywania (retencji) (sformułowaną w art. 5 ust. 1 lit. e RODO), dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których są one przetwarzane.

Konkludując UODO podniósł, że nie ma sztywnego, ustalonego odgórnie okresu przetwarzania ww. danych. Przepisy wskazują jedynie, że okres ten powinien być determinowany celem, w jakim dane osobowe są konieczne do ich przetwarzania. Niemniej stanowią dla administratora wskazówkę, którą ma się kierować w przypadku dokonywania oceny (przynajmniej raz na 5 lat), czy przetwarzanie danych osobowych o niepełnosprawności jest nadal konieczne (niezbędne) dla określonych i uzasadnionych celów.

Jeśli zatem uzasadnionym celem administratora będzie konieczność udokumentowania dodatkowych uprawnień pracownika wynikających z niepełnosprawności (np. w przypadku kontroli z PIP), to administrator powinien to wykazać w swoim raporcie z przeprowadzonego przeglądu przydatności przetwarzania danych, o którym mowa w powołanym wyżej przepisie ustawy. Jednocześnie należy uwzględnić także przepisy prawa, na podstawie których taka kontrola może być przeprowadzona, w tym okres, w jakim może się ona odbywać. Przykładowo okres taki jest wskazany w art. 30 ust. 3c ustawy o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych. Zgodnie z tym przepisem Państwowa Inspekcja Pracy przeprowadza, nie rzadziej niż co trzy lata, kontrolę w zakładach pracy chronionej i w zakładach aktywności zawodowej w zakresie przestrzegania przepisów ustawy, w szczególności art. 28 ust. 1 pkt 2.

Fot. pixabay

# CZY CANAL+ UJAWNIŁ DANE KLIENTA OSOBOM TRZECIM? PREZES UODO UMARZA SPRAWĘ

**Obywatel poskarżył się UODO, że nieznana osoba korzystając z jego danych zmieniła ustawienia jego konta w serwisie Canal+, a on nawet nie został powiadomiony przez spółkę, że ma płacić więcej za abonament. Skarżący sądził, że Canal+ ujawniła jego dane osobom trzecim.**

Okazało się jednak, że padł on ofiarą ataku credential stuffing: hakerzy zalogowali się na konta wielu użytkowników Canal+ używając loginów i haseł wykradzionych z innych serwisów – były bowiem niestety takie same. W ten sposób weszli w posiadanie danych osobowych, które użytkownicy przekazali spółce Canal+.

Zatem problem nie polegał na zmianie wysokości abonamentu, ale na przejęciu przez hakerów danych takich jak: imię i nazwisko, numer PESEL, numer i seria dowodu osobistego, adres zamieszkania, adres e-mail, numer telefonu stacjonarnego, numer telefonu komórkowego.

Spółka Canal+ po zgłoszeniu od klienta zwróciła pieniądze pobrane na podstawie sfałszowanej umowy, powiadomiła skarżącego, jakie jego dane zostały przejęte, a o ataku credential stuffing powiadomiła UODO.

Ustaliwszy te fakty Prezes UODO umorzył sprawę ze skargi obywatela: owszem, nieuprawniona osoba weszła w posiadanie danych obywatela, ale pochodziły one ze źródeł innych niż Canal+. Niezależnie zatem od tego, czy doszło do naruszenia ochrony danych osobowych, w realiach niniejszej sprawy nie doszło równocześnie do przetwarzania danych osobowych Skarżącego przez Spółkę polegającego na ich udostępnieniu bez podstawy prawnej. Zdarzenie, którego dotyczy niniejsza sprawa, nie stanowiło bowiem działania ani też zaniechania Spółki jako administratora danych. Skarżony proces przetwarzania danych osobowych nie zaistniał, więc niniejsze postępowanie stało się bezprzedmiotowe.

**Sygnatura sprawy: DS.523.507.2021**

# OCHRONA DANYCH OSOBOWYCH W PROCESIE WYBORCZYM

**Kandydaci w wyborach wykorzystujący dane osobowe przetwarzane w ich pracy (w szkole, lecznicy)? Listy poparcia dla kandydatów pozostawiane np. na ladach sklepowych? Wykorzystywanie danych osobowych w kampaniach wyborczych często odbywa się bez świadomości, jak ważny to proces. Dowodem tego są liczne zgłoszenia nieprawidłowości w przetwarzaniu danych osobowych. UODO przypomina, że aby do tych naruszeń nie dochodziło, konieczne jest przeprowadzenie stosownej analizy ryzyka na każdym etapie procesu wyborczego przez wszystkie podmioty, które uznawane są za administratorów danych.**

Wieloetapowy proces wyborczy przewiduje istnienie wielu administratorów. Ich role i obowiązki kształtują się odmiennie w zależności od typu prowadzonej kampanii wyborczej. Kodeks wyborczy wskazuje różnice w prowadzeniu kampanii w wyborach do Sejmu, Senatu, Parlamentu Europejskiego, Prezydenta Rzeczypospolitej Polskiej oraz w wyborach do organów stanowiących jednostek samorządu terytorialnego i w wyborach wójta, burmistrza i prezydenta miasta. Zasady dotyczące przetwarzania danych osobowych pozostają jednak tożsame niezależnie od typu prowadzonej kampanii.

Wśród wskazanych w Kodeksie wyborczym podmiotów przetwarzających dane osobowe można wyróżnić administratorów, którzy odpowiadają za przetwarzanie danych w ramach przyznanych im ustawowo kompetencji:

- stałe organy wyborcze, tj. Państwowa Komisja Wyborcza oraz komisarze wyborczy, przy czym każdy z tych organów administruje danymi osobowymi w innym zakresie i celu określonym ściśle w przepisach odrębnych;
- Krajowe Biuro Wyborcze, które przetwarza dane osobowe w zakresie obsługi organizacyjno-administracyjnej oraz finansowej i technicznej organów wyborczych powołanych w związku z zarządzonymi wyborami, w tym okręgowe, rejonowe i terytorialne komisje wyborcze oraz okręgowe komisje wyborcze;
- wójtowie, burmistrzowie, prezydenci miast, starostowie oraz marszałkowie województw przetwarzający dane osobowe w zakresie obsługi i technicznomaterialnych warunków pracy

obwodowych i terytorialnych komisji wyborczych oraz wykonywania zadań związanych z organizacją i przeprowadzaniem wyborów gminy, powiatów lub województwa;

- minister właściwy do spraw informatyzacji oraz minister właściwy do spraw zagranicznych, wójtowie, burmistrzowie, prezydenci miast, Państwowa Komisja Wyborcza, komisarze wyborczy oraz konsulowie w ramach przetwarzania danych osobowych znajdujących się w Centralnym Rejestrze Wyborców;
- komitety wyborcze.

Kwestię przetwarzania danych osobowych należy traktować jednak znacznie szerzej. W procesie przetwarzania bierze udział znacznie większa liczba podmiotów. Konieczne jest zatem przeprowadzenie stosownej analizy ryzyka na każdym etapie procesu wyborczego przez wszystkie podmioty, które uznawane są za administratorów, czy to na podstawie konkretnych przepisów delegujących poszczególne kompetencje tym podmiotom, czy na podstawie przepisów RODO.

**Jakie problemy widzi UODO?**

Departament Kontroli i Naruszeń UODO mierzy się z wieloma przypadkami naruszeń ochrony danych osobowych. Wykorzystywanie danych osobowych w kampaniach wyborczych często odbywa się bez pełnej świadomości dotyczącej wagi ich przetwarzania. Poprzednie wybory wykazały wiele nieprawidłowości w przetwarzaniu danych osobowych przez komitety wyborcze i zaowocowały sporą liczbą zgłoszeń nieprawidłowości w przetwarzaniu danych osobowych na różnych etapach prowadzenia kampanii wyborczych.

**Dane przetwarzane bez podstawy prawnej**

Najczęściej zgłaszane przypadki naruszeń ochrony danych osobowych polegały na przetwarzaniu danych osobowych w ramach prowadzenia agitacji wyborczej bez podstawy prawnej.

Kandydaci, wywodzący się z różnych grup zawodowych, wykorzystywali dane przetwarzane w ramach wykonywania przez nich czynności zawodowych. Dane te pochodziły z baz danych administratorów będących pracodawcami kandydatów. Takie procedery zauważono m.in. w placówkach oświatowych i placówkach służby zdrowia. Podmioty danych zgłaszały się do Urzędu ze skargami na wykorzystanie ich danych osobowych znajdujących się w bazach danych tych podmiotów w celu zachęcania ich do głosowania na określonych kandydatów. Zgłoszone skargi najczęściej dotyczyły pozyskiwania danych osobowych w postaci numerów telefonów i adresów e-mail.

# 4 NARUSZENIA I KONTROLE

Zbieranie i przechowywanie danych osobowych wykorzystywanych w celu prowadzenia agitacji wymaga wskazania podstawy prawnej przetwarzania, np. przesłanki zgody[1] albo wykazania prawnie uzasadnionego interesu administratora[2].

- Przesłanka zgody będzie najczęściej konieczna w przypadku prowadzenia agitacji wyborczej w formie zindywidualizowanej informacji.
- Natomiast realizacją prawnie uzasadnionego interesu administratora będzie pozyskanie danych w sposób inny niż od osoby, której dane dotyczą (np. z powszechnie dostępnych rejestrów publicznych jak KRS, CEiDG, czy też baz danych marketingowych).

Niezależnie od wyboru przesłanki, aby przetwarzanie miało charakter legalny, administrator musi również spełnić obowiązek informacyjny określony w art. 14 RODO wobec osoby, której dane dotyczą. Wiąże się z tym konieczność zapewnienia osobom, których dane dotyczą, możliwości realizacji ich praw, bowiem mają one prawo zgłosić sprzeciw na podstawie art. 21 RODO. Wówczas administrator traci prawo do dalszego przetwarzania danych osobowych w celach nim objętym i powinien je usunąć.

Dane osobowe muszą być przetwarzane jedynie w zakresie niezbędnym do celów, w których są przetwarzane. Numer telefonu czy adres e-mail może zostać podany jedynie opcjonalnie. Bezpieczniejszą alternatywą dla prowadzenia agitacji wyborczej z perspektywy ochrony danych osobowych będzie kierowanie materiałów promocyjnych drogą pocztową w formie przesyłek bezadresowych, na których nie umieszcza się adresu konkretnego odbiorcy. Przesyłki takie rozpowszechniane są na danym obszarze wszystkim osobom, które go zamieszkują. Ten rodzaj marketingu minimalizuje ryzyko wystąpienia naruszeń ochrony danych osobowych.

**Listy poparcia bez nadzoru**

Do Urzędu wpływają również zgłoszenia dotyczące pozostawiania list poparcia dla kandydatów bez nadzoru w różnych miejscach, np. na ladach sklepowych.

Tak pozostawione listy poparcia pozwalają nie tylko na zapoznanie się z danymi osobowymi osób, które wyraziły poparcie konkretnego kandydata, ale także umożliwiają ich skopiowanie czy wyniesienie. Biorąc pod uwagę zakres kategorii danych osobowych, tj. imię oraz nazwisko, numer ewidencyjny PESEL, adres zamieszkania lub pobytu oraz odręczny podpis, należy zakładać, że incydenty bezpieczeństwa związane z ujawnieniem tych danych generują wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ponadto obywatele, wyrażając poparcie dla wybranego kandydata, udostępniają administratorowi także swoje dane dotyczące poglądów politycznych czy światopoglądu.

# 4 NARUSZENIA I KONTROLE

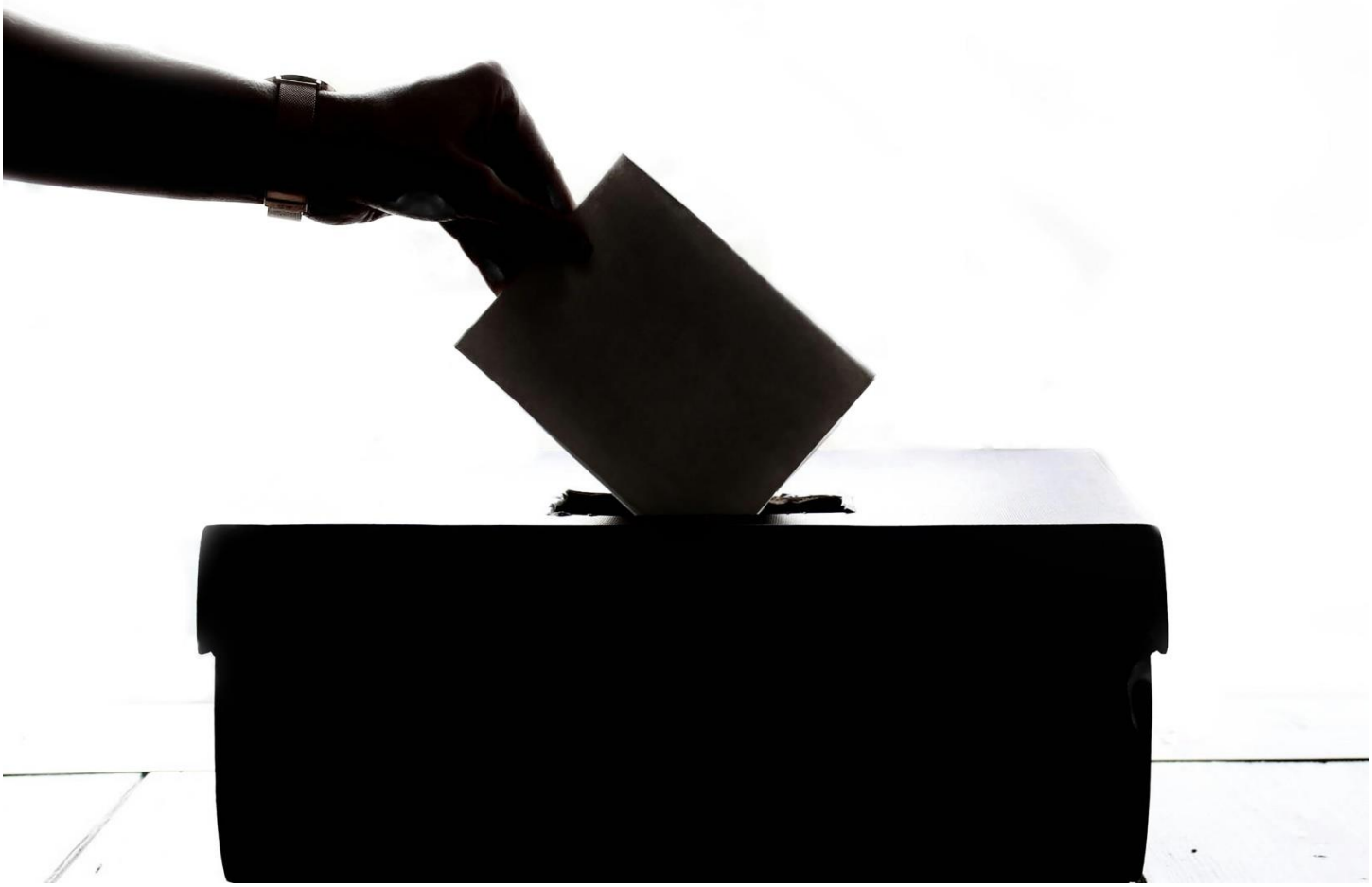
W ostatnim czasie Prezes UODO nałożył na administratora karę pieniężną za brak przestrzegania przez niego przepisów RODO w związku z pozostawieniem list poparcia dla inicjatywy ustawodawczej bez nadzoru w kościele.

Wprawdzie przedmiotowa sprawa nie dotyczy przetwarzania danych w związku z wyborami, ale warto w tym miejscu zwrócić na nią uwagę, gdyż decyzja odnosi się do sytuacji zbierania podpisów pod listami poparcia, tyle tylko, ze w ramach inicjatywy ustawodawczej podjętej przez obywateli. Administrator danych, mimo wielokrotnych sygnałów ze strony Prezesa UODO oraz prowadzonej z nim korespondencji, nie zdecydował się na zgłoszenie naruszenia ochrony danych osobowych, bezskutecznie próbując wykazać, iż wprowadzone przez niego zabezpieczenia były odpowiednie do poziomu ryzyka związanego z przetwarzaniem danych osobowych na listach poparcia.

Analiza przypadku wykazała jednak, iż gromadzenie tak dużych ilości danych osobowych odbywało się bez nadzoru osób uprawnionych do prowadzenia zbiórki, na skutek czego zostało wykonane zdjęcie list poparcia (nieuprawniony dostęp) oraz skopiowanie znajdujących się na listach poparcia danych osobowych przez co najmniej jedną osobę, która zgłosiła nieprawidłowości Prezesowi UODO. Z prowadzonej korespondencji wynikało, iż zbiórka podpisów odbywała się bez jakiejkolwiek kontroli ze strony administratora. Listy poparcia udostępnione były na stronie internetowej administratora, a udział w zbiórce podpisów mógł wziąć każdy zainteresowany wsparciem inicjatywy ustawodawczej. Pomimo posiadanej instrukcji zbierania podpisów administrator nie był w stanie wskazać, czy każdy wolontariusz zapoznał się z jej treścią. Biorąc pod uwagę zasadę rozliczalności określoną w RODO, niedopuszczalne jest działanie administratora, które jedynie pozornie wskazuje na przestrzeganie przepisów rozporządzenia. Nie może bowiem mieć miejsca sytuacja, w której administrator nie jest w stanie wskazać, ilu wolontariuszy zbiera dane osobowe, w jakich miejscach oraz czy wolontariusze znają zasady bezpiecznego zbierania podpisów. Można stwierdzić, iż takie podejście administratora może prowadzić do samowoli wśród zbierających podpisy. W takim przypadku obywatele mogą bać się, że ich dane trafią w ręce przestępców.

Na koniec należy zauważyć, iż większość sygnałów o tych incydentach nie pochodzi od administratorów, na których RODO nakłada obowiązek zgłaszania do organu nadzorczego naruszeń ochrony danych osobowych, a od sygnalistów. Tym bardziej podkreślenia wymaga, że wszystkie podmioty będące administratorami w kampanii wyborczej – na każdym jej etapie – muszą przestrzegać wszystkich obowiązujących przepisów dotyczących ochrony danych osobowych i muszą być świadome swojej odpowiedzialności z tym związanej. Zrozumienie i przestrzeganie zasad

zgodnego z prawem i bezpiecznego przetwarzania danych osobowych jest nie tylko ich obowiązkiem prawnym, ale także kluczem do budowania zaufania wśród wyborców i zapewnienia skutecznej i uczciwej kampanii wyborczej.



Fot. pexels

[1] art. 6 ust. 1 lit. a rozporządzenia 2016/679

[2] art. 6 ust. 1 lit. f rozporządzenia 2016/679

# BEZPIECZNE PODRÓŻOWANIE W DOBIE CYFRYZACJI: JAK CHRONIĆ DANE OSOBOWE I FINANSOWE PODCZAS KORZYSTANIA Z APLIKACJI PODRÓŻNYCH?

**Żeby zadbać o ich bezpieczeństwo i cieszyć się udanym i spokojnym wyjazdem, kiedy już decydujemy się na konkretne aplikacje np. do rezerwacji hoteli czy kupowania biletów, musimy pamiętać o kilku istotnych kwestiach.**

W dobie cyfryzacji, kiedy nasze telefony stały się nieodłącznym towarzyszem podróży, ważne jest, abyśmy korzystali z tych narzędzi w sposób świadomy i bezpieczny. Tym bardziej, że planowanie podróży często wiąże się z koniecznością podawania wielu danych osobowych. Dzięki racjonalnym wyborom i odpowiednim zabezpieczeniom możemy cieszyć się komfortem i wygodą, jaką oferują nam nowoczesne technologie, jednocześnie chroniąc nasze dane osobowe i finansowe.

**Bezpieczne aplikacje podróżne – na co zwrócić uwagę?**

Podróżowanie, choć ekscytujące, może być także źródłem stresu, jeśli nie jesteśmy odpowiednio przygotowani. Jednym z kluczowych elementów przygotowań jest wybór aplikacji podróżnych, które mogą znacznie ułatwić organizację wyjazdu. Oto kilka aspektów, na które warto zwrócić uwagę przy pobieraniu aplikacji podróżnych:

1. **Źródło pobierania:**

- Pobieraj aplikacje tylko z oficjalnych sklepów takich jak Google Play czy Apple App Store. Unikaj pobierania aplikacji z niezaufanych źródeł, które mogą zawierać złośliwe oprogramowanie.

- Weryfikacja dewelopera: Sprawdź, kto jest deweloperem aplikacji. Rekomendowane firmy i popularne aplikacje, które mają tysiące pozytywnych opinii, mogą okazać się bezpieczniejsze.

**2. Opinie i oceny:**

- Recenzje użytkowników: Przeczytaj recenzje innych użytkowników. Zwróć uwagę na wszelkie wzmianki o problemach z bezpieczeństwem czy prywatnością.

- Oceny: Wysoka ocena często świadczy o niezawodności aplikacji, ale ważne jest także, aby sprawdzić liczbę ocen – im więcej, tym lepiej.

**3. Uprawnienia aplikacji:**

• Przegląd uprawnień: Przed zainstalowaniem aplikacji, sprawdź, jakie uprawnienia są wymagane. Upewnij się, że są one adekwatne do funkcji aplikacji. Na przykład, aplikacja do rezerwacji hoteli nie powinna potrzebować dostępu do Twoich kontaktów.

**Ochrona danych osobowych podczas planowania podróży**

Bez względu na to, czy planujesz krótki wypad za miasto, czy dłuższą podróż zagraniczną, bezpieczeństwo Twoich danych powinno być priorytetem. Jak o to zadbać?

**1. Silne hasła:**

• Unikalne hasła: Używaj silnych, nietypowych haseł do różnych kont w aplikacjach podróżnych. Unikaj stosowania tych samych haseł w różnych miejscach.

• Menadżer haseł: Rozważ korzystanie z menadżera haseł, który pomoże Ci przechowywać i zarządzać hasłami w bezpieczny sposób.

**2. Dwuetapowa weryfikacja:**

• Aktywacja 2FA: Włącz dwuetapową weryfikację (2FA) wszędzie, gdzie to możliwe. To dodatkowe zabezpieczenie znacznie utrudnia potencjalnym atakującym dostęp do Twoich kont.

**3. Bezpieczne połączenie internetowe:**

• VPN: Korzystaj z sieci VPN (Virtual Private Network) podczas łączenia się z internetem w miejscach publicznych, takich jak lotniska czy hotele. VPN szyfruje Twoje połączenie, chroniąc Twoje dane przed nieautoryzowanym dostępem.

• Zaufane sieci: Unikaj korzystania z niezabezpieczonych, publicznych sieci Wi-Fi do logowania się na swoje konta w aplikacjach podróżnych.

**Rezerwacja hoteli i kupowanie biletów**

Kiedy już zdecydujesz się na konkretne aplikacje do rezerwacji hoteli i kupowania biletów, pamiętaj również o kilku dodatkowych kwestiach:

**1. Bezpieczne płatności:**

• Metody płatności: Wybieraj aplikacje, które oferują bezpieczne metody płatności, takie jak PayPal czy karty kredytowe z funkcją weryfikacji transakcji.

• Oszustwa płatnicze: Bądź czujny na potencjalne oszustwa. Nigdy nie podawaj danych swojej karty w odpowiedzi na podejrzane wiadomości e-mail czy SMS-y.

**2. Ochrona prywatności:**

Polityka prywatności: Przeczytaj politykę prywatności aplikacji, aby dowiedzieć się, w jaki sposób Twoje dane są przechowywane i wykorzystywane. Upewnij się, że aplikacja nie udostępnia Twoich danych stronom trzecim bez Twojej zgody.

• Anonimizacja danych: Tam, gdzie to możliwe, korzystaj z opcji anonimizacji danych – na przykład, używając pseudonimów zamiast pełnych imion i nazwisk.

**3. Aktualizacje aplikacji:**

• Regularne aktualizacje: Systematycznie aktualizuj swoje aplikacje podróżne, aby mieć pewność, że korzystasz z najnowszych zabezpieczeń. Aktualizacje często zawierają poprawki bezpieczeństwa, które chronią przed nowymi zagrożeniami.

**Uważaj na atrakcyjne oferty!**

Aplikacje turystyczne ułatwiają dostęp do korzystnych ofert cenowych na bilety wstępu do różnych atrakcji turystycznych. Jednak bardzo korzystne na pierwszy rzut oka oferty mogą skrywać pewne zagrożenia.

Zaleca się porównywanie cen z kilku źródeł przed dokonaniem zakupu, aby upewnić się, że oferta jest wiarygodna i pochodzi z zaufanego źródła. Warto również sprawdzać opinie innych użytkowników oraz rankingi sprzedawcy, ponieważ zaufane strony często cieszą się pozytywnymi recenzjami i wysokimi ocenami.

**Nawigacja, lokalizowanie miejsc, planowanie tras…**

Najczęściej korzystamy z map online, które oferują aktualizowane na bieżąco informacje. Mają one również swoje ciemne strony, o których rzadko myślimy. Korzystanie z map online często wiąże się z koniecznością udostępniania danych osobowych i lokalizacyjnych. Każda nasza trasa, każde miejsce, które odwiedzamy, mogą być śledzone i analizowane przez dostawców usług. Warto w takiej sytuacji wziąć pod uwagę alternatywę, jaką są mapy offline.

# 5 NOWE TECHNOLOGIE

Po pierwsze, korzystając z map offline, nie musimy udostępniać naszej lokalizacji w czasie rzeczywistym. Dzięki temu minimalizujemy ryzyko, że nasze dane zostaną wykorzystane bez naszej wiedzy lub zgody. To daje nam większą kontrolę nad tym, kto i w jakim zakresie ma dostęp do informacji o naszych podróżach.

Po drugie, mapy offline nie wymagają połączenia z internetem, co nie tylko zwiększa nasze bezpieczeństwo, ale również jest praktyczne w miejscach o słabym zasięgu.

Nawet korzystając z map offline, powinniśmy zwracać uwagę na źródła, z których je pobieramy. Ważne jest, aby wybierać rekomendowane aplikacje i serwisy, które zapewniają regularne aktualizacje i wysoką jakość map. Tylko wtedy możemy mieć pewność, że nasze dane są bezpieczne, a my sami nie narażamy się na dodatkowe zagrożenia.

Bezpieczeństwo w sieci to nie tylko kwestia technologii, ale także naszych nawyków i podejścia do korzystania z nowoczesnych narzędzi. Przez świadome wybory i odpowiednie zabezpieczenia, możemy cieszyć się komfortem i wygodą, jaką oferują nam nowoczesne technologie, jednocześnie chroniąc nasze dane osobowe i finansowe.

Fot. pixabay

# WERYFIKACJA WIEKU ONLINE – CZY TO W OGÓLE MOŻLIWE?

**Czy istnieją technologie pozwalające na weryfikacje wieku użytkowników w Internecie? Jakie dane osobowe są wykorzystywane do takiej weryfikacji i jakie ryzyka są z tym związane? Co w tym temacie robi ostatnio Unia Europejska?**

Ochrona dzieci w Internecie nabiera coraz większego znaczenia. Do tej pory dostępne były tylko ograniczone metody weryfikacji wieku online, które miały na celu zabezpieczenie dzieci przed dostępem do treści nieodpowiednich dla ich wieku. Wiele krajów wprowadza obecnie przepisy lub kodeksy postępowania, aby zaradzić temu problemowi. Również na poziomie UE podejmowane są coraz większe starania w tym zakresie. Wyzwaniami pozostają kwestie związane z prywatnością, ochroną danych osobowych, monitorowaniem oraz koniecznością poprawy kompetencji cyfrowych zarówno rodziców, jak i dzieci.

Dzieci są bardzo liczną grupą użytkowników Internetu, a pandemia koronawirusa tylko wzmocniła ten trend, ponieważ przyzwyczaiły się do spędzania większej ilości czasu online podczas lockdownów. Ogromna część najmłodszych funkcjonuje w Internecie i zaczyna się to w coraz młodszym wieku. Najczęściej jednak środowiska internetowe, do których uzyskują dostęp, nie były pierwotnie dla nich zaprojektowane. Dzieci też z łatwością omijają wymogi wiekowe, czy to przy korzystaniu z mediów społecznościowych, czy przy wchodzeniu na strony przeznaczone dla dorosłych. Dostawcy usług cyfrowych często nie stosują odpowiednich metod weryfikacji wieku lub zgody rodziców.

**Metody weryfikacji**

Ze względu na duże poczucie anonimowości w Internecie może się wydawać, że sprawdzenie wieku użytkownika nie jest możliwe albo że może być łatwe do sfałszowania. Jeśli opieramy się na popularnych metodach, takich jak deklaracja użytkownika, czy to, że ma ukończony 18. rok życia, czy poprzez podanie daty urodzenia, może być to prawda. Jest to też metoda, która nie zapewnia w zasadzie żadnej gwarancji bezpieczeństwa, bo nawet młodsze dzieci bez problemu są w stanie podać potrzebną datę urodzenia, aby wejść na stronę internetową. Istnieją jednak inne, bardziej zaawansowane metody weryfikacji wieku:

- Biometria – oparcie się na technologii rozpoznawania biometrycznego, np. analiza rysów twarzy po zrobieniu selfie czy nagraniu krótkiego filmiku, aby upewnić się, że osoba wnioskująca o dostęp ma ukończone 18 lat, jednak ustalenie wieku użytkownika z taką dokładnością jest podatne na błędy.

• Karty kredytowe – weryfikacja za pomocą potwierdzenia ważności karty bankowej, na przykład dokonując płatności lub logując się do serwisu banku, najczęściej jest stosowana przez witryny handlu elektronicznego i aplikacje sprzedające produkty, takie jak alkohol, wyroby tytoniowe lub treści pornograficzne.

• Analiza wzorców korzystania z Internetu – wnioskowanie o „dojrzałości" użytkownika poprzez analizę historii przeglądania Internetu i jego zachowań.

• Zgoda rodzica – niektóre aplikacje i usługi wymagają zgody rodziców na rejestrację dziecka na platformie, władza rodzicielska rzadko jest jednak w pełni weryfikowana.

• Tożsamość cyfrowa – oparcie się na narzędziach oferowanych przez państwo w celu weryfikacji tożsamości i wieku osób przed przyznaniem im dostępu do usługi cyfrowej.

• Weryfikacja za pomocą specjalnej aplikacji – uzyskanie dostępu, np. do treści pornograficznych, po zainstalowaniu licencjonowanej aplikacji do certyfikacji cyfrowej[1].

**Ryzyka związane z ochroną danych**

Istnieje więc sporo metod weryfikacji wieku, jednak łączy je to, że wszystkie opierają się na przetwarzaniu jakiegoś rodzaju danych osobowych. Największe ryzyko pojawia się podczas przetwarzania danych biometrycznych ze względu na to, że jest to szczególna kategoria danych osobowych i w sposób szczególny chroniona przez RODO[2]. Korzystanie z aplikacji wykorzystujących technologie biometryczne grozi więc nadmiernym przetwarzaniem bardzo wrażliwych danych i profilowaniem użytkownika, zwłaszcza jeśli poszerzy się taką technologię o sztuczną inteligencję.

W przypadku weryfikacji za pomocą usług bankowych istnieje wysokie ryzyko phishingu, podania danych osobowych w miejscu, które może nie być oficjalną stroną dostawcy usług bankowych. Kolejnym problemem jest sytuacja, w której z karty bankowej korzysta osoba niebędąca jej prawowitym właścicielem. Ponadto wiek uprawniający do posiadania karty kredytowej różni się w zależności od kraju. Analiza wzorców korzystania z Internetu, po pierwsze, nie wydaje się mieć dużej skuteczności, a po drugie, polega na zbieraniu danych behawioralnych użytkowników. Stanowi to kolejne zagrożenie i łatwą okazję do nadużywania profilowania, np. w celu wyświetlania spersonalizowanych reklam.

[1] AT A GLANCE Digital issues in focus - Online age verification methods for children, European Parliament EPRS_ATA(2023)739350_EN.pdf

[2] Dz.U.UE.L.2016.119.1 z dnia 2016.05.04, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Po analizie poprzednich metod najbezpieczniejsza wydaje się być weryfikacja za pomocą tożsamości cyfrowej. Narzędzia w przypadku tej metody są oferowane przez państwo i właśnie też organ państwowy będzie wtedy administratorem danych przetwarzanych na potrzeby przyznania użytkownikowi tożsamości cyfrowej.

**Co obecnie robi w tym temacie Unia Europejska?**

Przed przyjęciem RODO, w Unii Europejskiej nie było konkretnych ograniczeń dotyczących przetwarzania danych dzieci w Internecie. RODO wymaga stosowania weryfikacji wieku i zgody rodziców. Nowa europejska strategia na rzecz lepszego Internetu dla dzieci przewiduje opracowanie kompleksowego kodeksu postępowania dotyczącego projektowania dostosowanego do wieku, opierającego się na nowych przepisach w akcie o usługach cyfrowych (DSA)[3] i zgodnego z AVMSD[4] oraz RODO.

Komisja Europejska zamierza wzmocnić metody weryfikacji wieku poprzez solidne ramy certyfikacji i interoperacyjności. Dodatkowo, propozycja regulacji, mającej na celu zwalczanie wykorzystywania seksualnego dzieci w Internecie, przewiduje udoskonaloną weryfikację wieku online. Podobnie, lepsze metody weryfikacji wieku w celu ochrony dzieci online są częścią proponowanej przez Komisję Europejską Europejskiej deklaracji o prawach cyfrowych i zasadach na rzecz cyfrowej dekady oraz Deklaracji Organizacji Współpracy Gospodarczej i Rozwoju na rzecz zaufanej, zrównoważonej i inkluzywnej przyszłości cyfrowej[5].

Również Europejska Rada Ochrony Danych (EROD) w swojej strategii na lata 2024-2027 podkreśla rolę tworzenia bezpiecznych i skutecznych metod weryfikacji wieku, ze szczególnym uwzględnieniem roli nowego rozporządzenia dotyczącego ustanowienia europejskich ram tożsamości cyfrowej. Częścią tej większej strategii są plany tworzenia europejskich portfeli cyfrowych, pozwalających na weryfikację wieku użytkowników. EROD chce dostarczać wskazówki w wytycznych dotyczących kluczowych kwestii, takich jak stosowanie RODO wobec dzieci oraz stosowanie szczególnie istotnych przepisów, takich jak uzasadniony interes przetwarzania.

[3] Dz.U.UE.L.2022.277.1 z dnia 2022.10.27, Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)

[4] Dz.U.UE.OJ L 95, 15.4.2010, Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych)

[5] AT A GLANCE Digital issues in focus - Online age verification methods for children, European Parliament

Podkreśla swój cel, aby takie wskazówki były praktyczne, w tym zawierały przykłady tam, gdzie jest to odpowiednie, oraz były opracowane w sposób dostępny dla odpowiedniej grupy odbiorców i pomagały prawidłowo wdrażać przepisy[6].

Można więc zastanawiać się, czy w pełni skuteczna weryfikacja wieku online będzie kiedykolwiek możliwa. Jednak strategia Unii Europejskiej wydaje się słuszna – dąży do stworzenia bezpiecznej przestrzeni w Internecie dla dzieci poprzez zapewnienie najwyższych standardów technicznych i legislacyjnych. Istotne jest także zwrócenie uwagi na edukację rodziców, aby potrafili zapewnić swoim dzieciom bezpieczeństwo w sieci. Warto również podnosić świadomość najmłodszych na temat potencjalnych zagrożeń, jakie mogą napotkać w Internecie, uwzględniając ich specyficzne podejście, które często traktuje to środowisko jako równoległą rzeczywistość.

**Artykuł powstał w ramach cyklu, w którym zapraszamy pracowników Urzędu do dzielenia się swoimi przemyśleniami. Jego autorką jest Julia Rak, referentka w Departamencie Nowych Technologii.**

Fot. pexels

[6] Strategia Europejskiej Rady Ochrony Danych na lata 2024-2027 edpb_strategy_2024-2027_en.pdf

# STANY ZJEDNOCZONE ZAPEWNIAJĄ ODPOWIEDNI POZIOM OCHRONY DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UE DO ORGANIZACJI W USA. JAK WYGLĄDAJĄ PROCEDURY?

**Europejska Rada Ochrony Danych przyjęła notę informacyjną na temat mechanizmu dochodzenia roszczeń przez osoby fizyczne z UE/EOG w związku z domniemanymi naruszeniami prawa Stanów Zjednoczonych w odniesieniu do ich danych gromadzonych przez organy Stanów Zjednoczonych właściwe do spraw bezpieczeństwa narodowego.**

10 lipca 2023 r. Komisja Europejska przyjęła decyzję wykonawczą C(2023) 4745 w sprawie odpowiedniego poziomu ochrony danych osobowych na mocy ram ochrony prywatności danych UE-USA („decyzja w sprawie adekwatności"). W ten sposób Komisja zdecydowała, że Stany Zjednoczone, zgodnie z art. 45 RODO, zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z UE do organizacji w USA.

Ważnym elementem amerykańskich ram prawnych, na których opiera się decyzja o adekwatności, jest rozporządzenie wykonawcze 14086 w sprawie „wzmocnienia zabezpieczeń dla działań wywiadu Stanów Zjednoczonych" („E.O. 14086"), które zostało podpisane przez prezydenta USA Bidena 7 października 2022 r. i któremu towarzyszą przepisy przyjęte przez Prokuratora Generalnego USA, a także odpowiednie polityki i procedury przyjęte przez Biuro Dyrektora Wywiadu Narodowego i agencje wywiadowcze USA.

E.O. 14086 ustanowiło nowy mechanizm dochodzenia roszczeń w dziedzinie bezpieczeństwa narodowego w celu rozpatrywania i rozstrzygania skarg osób, których dane dotyczą, w UE i EOG. Zarzucają one bezprawny dostęp i wykorzystanie danych przez amerykańskie służby wywiadu sygnałowego do danych osobowych, które zostały przekazane z UE i EOG do USA. Ten mechanizm dochodzenia roszczeń ma zastosowanie niezależnie od narzędzia przekazywania danych wykorzystanego do przekazania danych osobowych skarżących do USA (tj. decyzji w sprawie adekwatności, standardowych klauzul umownych lub klauzul umownych ad hoc, wiążących reguł korporacyjnych, kodeksów postępowania, mechanizmów certyfikacji, odstępstw. Mechanizm ten ma jednak zastosowanie wyłącznie do danych przekazanych po 10 lipca 2023 r.

Należy pamiętać, że informacje na temat możliwości złożenia skargi dotyczącej naruszenia przez podmiot prywatny w USA obowiązujących zasad określonych w Data Privacy Framework można znaleźć na stronie EROD.

**Jak złożyć skargę?**

Skargi należy przesyłać do krajowego organu ochrony danych UE/EOG właściwego dla danej osoby. Listę organów ochrony danych w państwach członkowskich UE/EOG można znaleźć tutaj.

EROD przyjęła regulamin, aby zapewnić organom ochrony danych wytyczne dotyczące ich zadań i obowiązków. Ustanowiono unijny formularz skargi indywidualnej w celu składania skarg do Biura Dyrektora Wywiadu Narodowego („CLPO") przez osoby fizyczne z UE/EOG.

**W jaki sposób organ ochrony danych rozpatrzy skargę?**

Krajowy organ ochrony danych UE/EOG zweryfikuje tożsamość skarżących i sprawdzi, czy skarga jest kompletna i spełnia warunki określone w prawie amerykańskim.

W szczególności organ ochrony danych zweryfikuje:

- tożsamość osoby składającej skargę oraz to, że działa ona wyłącznie we własnym imieniu, a nie jako przedstawiciel organizacji rządowej, pozarządowej lub międzyrządowej;
- czy skarżący uważa, że doszło do naruszenia jednego lub więcej przepisów prawa Stanów Zjednoczonych, jeśli dane osobowe skarżącego lub jego dotyczące zostały bezprawnie udostępnione amerykańskim agencjom wywiadowczym po przekazaniu jego danych osobowych z UE do Stanów Zjednoczonych;
- czy skarga zawiera na piśmie (również za pośrednictwem poczty elektronicznej) wszystkie istotne informacje (które nie muszą wykazywać, że dane skarżącego były faktycznie przedmiotem działań amerykańskiego wywiadu):
  - wszelkie informacje stanowiące podstawę skargi, w tym szczegóły dotyczące konta internetowego lub transferu danych osobowych, do których prawdopodobnie uzyskano dostęp;
  - charakter żądanego zadośćuczynienia;
  - konkretne środki, za pomocą których dane osobowe skarżących lub ich dotyczące zostały przekazane do USA;
  - który podmiot lub podmioty rządu USA były zaangażowane w uzyskanie dostępu do danych

- osobowych skarżącego lub o nim (jeśli są znane);
- oraz wszelkie inne środki podjęte przez skarżącego w celu uzyskania żądanych informacji lub zadośćuczynienia, a także odpowiedź otrzymana za pomocą tych innych środków;
- dotyczy danych osobowych skarżących lub ich dotyczących, które prawdopodobnie zostały przekazane do Stanów Zjednoczonych po 10 lipca 2023 r;
- czy skarga nie jest niepoważna, dokuczliwa ani złożona w złej wierze.

Po tej weryfikacji – i jeśli skarga zostanie uznana za kompletną – organ ochrony danych przekaże ją w zaszyfrowanym formacie do Sekretariatu Europejskiej Rady Ochrony Danych. Ta ostatnia dostarczy ją również w zaszyfrowanym formacie organowi USA, właściwemu do rozpatrzenia skargi – urzędnikowi ds. ochrony swobód obywatelskich w CLPO.

**Jaka jest rola CLPO?**

CLPO jest odpowiedzialny za przeprowadzenie postępowania wyjaśniającego w sprawie skargi w celu ustalenia, czy doszło do naruszenia zabezpieczeń przewidzianych w E.O. 14086 lub innych obowiązujących przepisach prawa USA, a jeśli tak, to w celu ustalenia odpowiednich wiążących środków zaradczych.

CLPO dostarczy odpowiedź do organu ochrony danych, za pośrednictwem Sekretariatu EROD, w odpowiednim czasie. Odpowiedź ta potwierdzi, że:

(1) „Przegląd albo nie wykazał żadnych naruszeń, albo Urzędnik ds. Ochrony Swobód Obywatelskich Biura Dyrektora Wywiadu Narodowego (ODNI) wydał decyzję wymagającą odpowiednich środków zaradczych. W swojej standardowej odpowiedzi ODNI nie potwierdzi ani nie zaprzeczy, czy skarżący był celem inwigilacji, ani nie potwierdzi konkretnego zastosowanego środka zaradczego;

(2) Skarżący lub element amerykańskiej wspólnoty wywiadowczej może złożyć wniosek o ponowne rozpatrzenie decyzji CLPO, składając odwołanie do Sądu Kontroli Ochrony Danych („DPRC”); oraz

(3) Jeśli skarżący lub członek Wspólnoty Wywiadowczej złoży wniosek o ponowne rozpatrzenie sprawy przez DPRC, DPRC wybierze tzw. „Specjalnego Rzecznika”, który będzie reprezentował interesy skarżącego w tej sprawie.

**Decyzja CLPO jest wiążąca dla elementów Społeczności Wywiadowczej**

CLPO wysyła odpowiedź do Sekretariatu EROD w zaszyfrowanym formacie. Ten następnie przekazuje ją, również w zaszyfrowanym formacie, do krajowego organu ochrony danych, który pierwotnie otrzymał skargę. Z kolei organ ochrony danych informuje skarżącego o odpowiedzi CLPO (w tym o tłumaczeniu z języka angielskiego, jeśli i w niezbędnym zakresie).

**Jak odwołać się od decyzji CLPO?**
Skarżący mają możliwość odwołania się od decyzji CLPO do Sądu Ochrony Danych („DPRC") w ciągu 60 dni od otrzymania powiadomienia od krajowego organu ochrony danych o odpowiedzi CLPO.

W celu złożenia odwołania skarżący może złożyć wniosek do swojego organu ochrony danych w ciągu 60 dni. DPRC może badać skargi od osób fizycznych w UE/EOG, w tym uzyskiwać odpowiednie informacje od elementów społeczności wywiadowczej USA i podejmować wiążące decyzje naprawcze.

Procedura odwoławcza będzie przebiegać w podobny sposób i zgodnie z podobną procedurą, jak w przypadku pierwotnej skargi: organ ochrony danych przekaże odwołanie do Sekretariatu EDPB w zaszyfrowanym formacie, który z kolei przekaże je w zaszyfrowanym formacie do Biura Prywatności i Swobód Obywatelskich Departamentu Sprawiedliwości Stanów Zjednoczonych („OPCL"), które zapewnia wsparcie dla DPRC, tak aby DPRC mogło rozpatrzyć odwołanie.

W szczególności DPRC dokona przeglądu ustaleń dokonanych przez CLPO (zarówno w odniesieniu do tego, czy doszło do naruszenia obowiązującego prawa amerykańskiego, jak i w odniesieniu do odpowiednich środków zaradczych) w oparciu, co najmniej, o zapisy dochodzenia CLPO, a także wszelkie informacje i oświadczenia dostarczone przez skarżącego, Specjalnego Rzecznika lub element Społeczności Wywiadowczej.

Zespół DPRC ma dostęp do wszystkich informacji niezbędnych do przeprowadzenia przeglądu, które może uzyskać za pośrednictwem CLPO (np. zespół może zwrócić się do CLPO o uzupełnienie dokumentacji o dodatkowe informacje lub ustalenia faktyczne, jeśli jest to konieczne do przeprowadzenia przeglądu). Specjalny Rzecznik ma również dostęp do wszystkich informacji niezbędnych do wypełnienia swojej roli polegającej na wspieraniu zespołu DPRC w rozpatrywaniu wniosku, w tym poprzez reprezentowanie interesów skarżącego w sprawie i zapewnienie, że zespół DPRC jest dobrze poinformowany o kwestiach i przepisach prawa w odniesieniu do sprawy.

Kończąc swój przegląd, DPRC może:

(1) zdecydować, że nie ma dowodów wskazujących na to, że działania wywiadu dotyczyły danych osobowych skarżącego;

(2) zdecydować, że ustalenia CLPO były poprawne pod względem prawnym i poparte istotnymi dowodami; lub

(3) wydać własne ustalenia, jeśli nie zgadza się z ustaleniami CLPO (czy doszło do naruszenia obowiązującego prawa USA lub odpowiednich środków naprawczych).

Decyzja DPRC jest wiążąca i ostateczna w odniesieniu do złożonej skargi.

W przypadkach, w których przegląd DPRC został zainicjowany wnioskiem skarżącego, jest on powiadamiany o decyzji DPRC. Po zakończeniu przeglądu przez DPRC przekaże on skarżącemu standardowe oświadczenie wskazujące, że zakończył przegląd i stwierdzające, że „przegląd albo nie wykazał żadnych objętych nim naruszeń, albo Trybunał Kontroli Ochrony Danych wydał orzeczenie wymagające odpowiednich środków zaradczych".

DPRC przekaże takie oświadczenie w zaszyfrowanym formacie do Sekretariatu EROD, który z kolei przekaże je do organu ochrony danych w zaszyfrowanym formacie. Organ ochrony danych powiadomi skarżącego o oświadczeniu DPRC (w tym o tłumaczeniu z języka angielskiego, jeśli i w niezbędnym zakresie). Oświadczenie to nie potwierdzi ani nie zaprzeczy, czy skarżący był celem nadzoru, ani nie potwierdzi konkretnego zastosowanego środka zaradczego.
Każda decyzja DPRC jest również przekazywana do CLPO.

**Jaka jest rola Departamentu Handlu USA w odniesieniu do odtajnionych informacji?**

Departament Handlu USA („DoC") będzie okresowo kontaktował się z odpowiednimi elementami społeczności wywiadowczej w sprawie tego, czy informacje dotyczące przeglądu skargi przez CLPO lub DPRC zostały odtajnione. Jeśli wywiad poinformuje DoC, że informacje dotyczące przeglądu skargi przez CLPO lub DPRC zostały odtajnione, DoC powiadomi skarżącego, za pośrednictwem Sekretariatu EROD. Ten z kolei przekaże go do organu ochrony danych, że informacje dotyczące przeglądu ich skargi przez CLPO lub DPRC, w zależności od przypadku, mogą być dostępne dla skarżącego na mocy obowiązującego prawa USA.

Jednym z takich przepisów jest amerykańska ustawa o wolności informacji („FOIA"), zgodnie z którą skarżący może złożyć wniosek FOIA bezpośrednio do ODNI, do odpowiedniego elementu Społeczności Wywiadowczej lub do Departamentu Sprawiedliwości (tj. bez przechodzenia przez DPA i Sekretariat EROD) w celu uzyskania odtajnionych informacji na temat swojej skargi.

Instrukcje dotyczące składania wniosków FOIA są dostępne na odpowiednich publicznych stronach internetowych oraz elementów Społeczności Wywiadowczej i DPRC.

Należy zauważyć, że skargi od osób, których dane dotyczą w UE/EOG, dotyczące pewnych naruszeń prawa Stanów Zjednoczonych w zakresie działań amerykańskiego wywiadu, które mają negatywny wpływ na ich prywatność i swobody obywatelskie, oraz odnoszące się do ich danych osobowych, przekazanych z UE/EOG do Stanów Zjednoczonych, powinny być składane wyłącznie do CLPO, a nie do wyżej wymienionych biur FOIA.

**Źródła:** **Nota informacyjna EROD**
**Nota informacyjna EROD**

Fot. pixabay

# DWUSTRONNA, ŚCISŁA WSPÓŁPRACA POMIĘDZY WŁOSKIM I NIEMIECKIM ORGANEM NADZORCZYM

**Włoski i niemiecki organ nadzorczy podjęły dwustronną, ścisłą współpracę. W dniach 18-20 kwietnia w Akademii Konrada Adenauera nad jeziorem Como odbyło się spotkanie przedstawicieli tych dwóch instytucji.**

Rozmowy dotyczyły wyzwań związanych ze sztuczną inteligencją i roli organów ochrony danych, od promowania działań na poziomie EROD, po ściślejszą współpracę między obydwoma organami w różnych unijnych i międzynarodowych grupach roboczych.

Przedstawiciele obu instytucji wymienili poglądy i doświadczenia na tematy, które znajdą się w programie spotkania „G7 Privacy", zaplanowanego na październik 2024 r. we Włoszech. Rozmawiali też o ochronie danych osobowych dzieci, analizując przy tym ramy regulacyjne i inicjatywy podejmowane przez różne instytucje. Zastanawiali się nad tym, kiedy można wprowadzić skuteczne mechanizmy weryfikacji wieku i jakie kryteria powinny one spełniać.

Wreszcie przeanalizowali opinię przyjętą przez EROD w kwestii modeli „zgoda lub zapłata" w kontekście dużych platform internetowych.

**Źródło:** komunikat włoskiego organu nadzorczego

# ROZPOZNAWANIE TWARZY W RZYMIE. WŁOSKI ORGAN NADZORCZY WSZCZYNA POSTĘPOWANIE

**Włoski organ nadzorczy wystąpił z wnioskiem o udzielenie informacji przez Roma Capitale w sprawie projektu nadzoru wideo na stacjach metra.**

Z doniesień prasowych wynika, że w Rzymie planowane jest zainstalowanie kamer z funkcją rozpoznawania twarzy, „zdolnych do weryfikacji działań osób zakłócających porządek" wewnątrz wagonów i na peronach. Kamery te mają na celu monitorowanie osób, które w przeszłości dokonały „czynów niezgodnych z przepisami".

Roma Capitale ma 15 dni na udzielenie odpowiedzi i dostarczenie między innymi technicznego opisu funkcji rozpoznawania twarzy, celu i podstawy prawnej takiego przetwarzania danych biometrycznych oraz kopii oceny skutków dla ochrony danych.

Włoski organ nadzorczy przypomina, że do końca 2025 r. obowiązuje ograniczenie na instalowanie systemów nadzoru wideo z systemami rozpoznawania twarzy w miejscach publicznych lub ogólnodostępnych. Takie przetwarzanie danych jest dozwolone wyłącznie organom sądowym w ramach wykonywania ich funkcji jurysdykcyjnych oraz organom publicznym w celu zapobiegania i zwalczania przestępstw, po uzyskaniu pozytywnej opinii włoskiego organu nadzorczego.

**Źródło:** komunikat włoskiego organu nadzorczego

# KOMISJA EUROPEJSKA WSZCZĘŁA FORMALNE POSTĘPOWANIE PRZECIWKO FACEBOOKOWI I INSTAGRAMOWI NA MOCY AKTU O USŁUGACH CYFROWYCH

**30 kwietnia 2024 r. Komisja Europejska wszczęła formalne postępowanie w celu oceny, czy Meta, dostawca Facebooka i Instagrama, mógł naruszyć akt o usługach cyfrowych.**

Chodzi o politykę i praktyki Meta związane z oszukańczymi reklamami i treściami politycznymi. Dotyczą one również niedostępności skutecznego, zewnętrznego narzędzia do prowadzenia dyskursu obywatelskiego w czasie rzeczywistym i monitorowania wyborów przed wyborami do Parlamentu Europejskiego, w kontekście wycofania przez Meta narzędzia CrowdTangle do publicznego wglądu w czasie rzeczywistym bez odpowiedniego zamiennika.

Ponadto Komisja podejrzewa, że mechanizm oznaczania nielegalnych treści w usługach („zawiadomienie i działanie"), a także mechanizm dochodzenia roszczeń przez użytkowników i wewnętrzne mechanizmy rozpatrywania skarg nie są zgodne z wymogami aktu o usługach cyfrowych oraz że istnieją niedociągnięcia w zapewnianiu przez Meta dostępu do publicznie dostępnych danych dla naukowców. Wszczęcie postępowania opiera się na wstępnej analizie sprawozdania z oceny ryzyka przesłanego przez Meta we wrześniu 2023 r., odpowiedziach Mety na formalne wnioski Komisji o udzielenie informacji (dotyczące nielegalnych treści i dezinformacji, dostępu do danych, subskrypcji polityki „noad-ads" i generatywnej sztucznej inteligencji), publicznie dostępnych sprawozdaniach oraz własnej analizie Komisji.

Przewodnicząca Komisji Ursula von der Leyen powiedziała: „Komisja stworzyła środki ochrony obywateli europejskich przed ukierunkowaną dezinformacją i manipulacją ze strony państw trzecich. Jeżeli podejrzewamy, że doszło do naruszenia przepisów, działamy. Ma to miejsce przez cały czas, ale zwłaszcza w czasie demokratycznych wyborów. Duże platformy cyfrowe muszą wywiązać się ze swoich zobowiązań, aby przeznaczyć na ten cel wystarczające zasoby, a dzisiejsza decyzja pokazuje, że poważnie przestrzegamy przepisów. Ochrona naszych demokracji to wspólna walka z państwami członkowskimi. Dziś w Pradze pragnę podziękować premierowi Fiali za jego aktywną rolę w poruszaniu tej kwestii na szczeblu europejskim, a także za uruchomienie przez Belgię nadzwyczajnego mechanizmu wymiany informacji między państwami członkowskimi".

# 6 SPRAWY MIĘDZYNARODOWE

Obecne postępowania skupią się na następujących obszarach:

- **Wprowadzające w błąd reklamy i dezinformacja.** Komisja podejrzewa, że Meta nie wypełnia obowiązków wynikających z aktu o usługach cyfrowych, związanych z przeciwdziałaniem rozpowszechnianiu zwodniczych reklam, kampanii dezinformacyjnych i skoordynowanych nieautentycznych zachowań w UE. Rozprzestrzenianie się takich treści może stanowić zagrożenie dla dyskursu obywatelskiego, procesów wyborczych i praw podstawowych, a także dla ochrony konsumentów.

- **Widoczność treści politycznych.** Komisja podejrzewa, że polityka Meta związana z „podejściem do treści politycznych", która obniża rangę treści politycznych w systemach rekomendacji Instagrama i Facebooka, w tym w ich kanałach, nie jest zgodna z obowiązkami aktu o usługach cyfrowych. Dochodzenie skoncentruje się na zgodności tej polityki z obowiązkami w zakresie przejrzystości i dochodzenia roszczeń przez użytkowników, a także wymogach oceny i ograniczania zagrożeń dla dyskursu obywatelskiego i procesów wyborczych.

- **Niedostępność skutecznego zewnętrznego narzędzia do dyskursu obywatelskiego i monitorowania wyborów w czasie rzeczywistym.** Meta jest w trakcie wycofywania „CrowdTangle", publicznego narzędzia umożliwiającego monitorowanie wyborów w czasie rzeczywistym przez badaczy, dziennikarzy i społeczeństwo obywatelskie, w tym za pomocą wizualnych pulpitów nawigacyjnych na żywo, bez odpowiedniego zamiennika. Jak jednak wynika z niedawnych wytycznych Komisji dla dostawców bardzo dużych platform internetowych w sprawie ryzyka systemowego dla procesów wyborczych, w czasie wyborów należy raczej rozszerzyć dostęp do takich narzędzi. W związku z tym Komisja podejrzewa, że biorąc pod uwagę wycofanie i planowane zaprzestanie działalności CrowdTangle przez Meta, Meta nie zdołała starannie ocenić i odpowiednio złagodzić ryzyka związanego z wpływem Facebooka i Instagrama na dyskurs obywatelski i procesy wyborcze oraz innych zagrożeń systemowych. Komisja zastrzega sobie prawo do oceny charakteru i bezpośredniości szkód i oczekuje, że Meta będzie z nią współpracować. Oczekuje również, że Meta podejmie szybko wszelkie niezbędne działania w celu zapewnienia skutecznej kontroli publicznej w czasie rzeczywistym swoich usług poprzez zapewnienie odpowiedniego dostępu badaczom, dziennikarzom i urzędnikom wyborczym do narzędzi monitorowania w czasie rzeczywistym treści hostowanych w jej usługach.

- **Mechanizm oznaczania nielegalnych treści.** Komisja podejrzewa, że mechanizm powiadamiania i działania firmy Meta, który umożliwia użytkownikom powiadamianie o obecności nielegalnych treści w jej usługach, nie jest zgodny z zobowiązaniami wynikającymi z DSA. Wydaje się, że wymogi, zgodnie z którymi mechanizm ten musi być łatwo dostępny i przyjazny dla użytkownika, nie są spełnione. Komisja podejrzewa też, że Meta nie wdrożyła skutecznego wewnętrznego systemu

rozpatrywania skarg w celu składania skarg na podjęte decyzje dotyczące moderowania treści.

Jeżeli uchybienia te zostaną udowodnione, stanowiłyby naruszenie art. 14 ust. 1, art. 16 ust. 1, art. 16 ust. 5, art. 16 ust. 6, art. 17 ust. 1, art. 20 ust. 1, art. 20 ust. 3, art. 24 ust. 5, art. 25 ust. 1, art. 34 ust. 1, art. 34 ust. 2, art. 35 ust. 1 i art. 40 ust. 12 aktu o usługach cyfrowych. Komisja przeprowadzi teraz szczegółowe dochodzenie w trybie priorytetowym. Wszczęcie formalnego postępowania nie przesądza o jego wyniku.

Obecne wszczęcie postępowania pozostaje bez uszczerbku dla jakiegokolwiek innego postępowania Komisji. Może ona podjąć decyzję o wszczęciu postępowania w sprawie wszelkich innych zachowań, które mogą stanowić naruszenie na mocy aktu o usługach cyfrowych.

**Kolejne kroki**

Po wszczęciu formalnego postępowania Komisja będzie nadal gromadzić dowody, na przykład wysyłając dodatkowe wnioski o udzielenie informacji, przeprowadzając rozmowy lub kontrole.

Wszczęcie formalnego postępowania upoważnia Komisję do podjęcia dalszych kroków egzekucyjnych, takich jak środki tymczasowe i decyzje o braku zgodności. Komisja jest również uprawniona do przyjęcia zobowiązań podjętych przez Metę w celu rozwiązania kwestii poruszonych w postępowaniu. DSA nie określa żadnego prawnego terminu zakończenia formalnego postępowania. Czas trwania szczegółowego dochodzenia zależy od kilku czynników, w tym od złożoności sprawy, zakresu współpracy danego przedsiębiorstwa z Komisją i korzystania z prawa do obrony.

Wszczęcie formalnego postępowania zwalnia koordynatorów ds. usług cyfrowych lub jakikolwiek inny właściwy organ państw członkowskich UE z ich uprawnień do nadzorowania i egzekwowania DSA w związku z podejrzeniem naruszenia art. 14 ust. 1, art. 16 ust. 1, art. 16 ust. 5, art. 16 ust. 6, art. 17 ust. 1, art. 20 ust. 1, art. 20 ust. 3, art. 24 ust. 5, art. 25 ust. 1 i art. 40 ust. 12.

**Kontekst ogólny**

25 kwietnia 2023 r. na mocy unijnego aktu prawnego o usługach cyfrowych Facebook i Instagram zostały wyznaczone jako bardzo duże platformy internetowe, ponieważ w obu tych platformach miesięcznie w UE jest ponad 45 mln aktywnych użytkowników. Jako bardzo duże platformy internetowe cztery miesiące od ich wyznaczenia, tj. pod koniec sierpnia 2023 r., Facebook i Instagram musiały zacząć wypełniać szereg obowiązków określonych w akcie o usługach cyfrowych. Od 17 lutego akt o usługach cyfrowych ma zastosowanie do wszystkich pośredników internetowych w UE.

**Źródło: komunikat Komisji Europejskiej**

# OPINIA RZECZNIKA GENERALNEGO W SPRAWIE C-768/21 LAND HESSEN

**Zdaniem rzecznika generalnego Priita Pikamäe organ nadzorczy jest zobowiązany do interwencji, gdy stwierdzi naruszenie w ramach rozpatrywania skargi. Jednakże decyzja w sprawie środka naprawczego, który należy przyjąć, zależy od konkretnych okoliczności każdego przypadku.**

Klient kasy oszczędnościowej zwrócił się do inspektora ochrony danych i wolności informacji kraju związkowego Hesja (Niemcy) o podjęcie działań przeciwko tej kasie z powodu naruszenia jego danych osobowych. Jedna z pracownic kasy oszczędnościowej wielokrotnie konsultowała jego dane, nie mając do tego upoważnienia.

Inspektor ochrony danych stwierdził naruszenie ogólnego rozporządzenia o ochronie danych (RODO). Doszedł jednak do wniosku, że nie ma potrzeby interweniowania wobec kasy oszczędnościowej, która podjęła już środki dyscyplinarne wobec pracownicy.

Klient zakwestionował tę odmowę przed sądem niemieckim, wnosząc o nakazanie inspektorowi ochrony danych podjęcia działań przeciwko kasie oszczędnościowej. Podnosił w szczególności, że inspektor ochrony danych powinien był nałożyć karę pieniężną na kasę oszczędnościową.

Sąd niemiecki zwrócił się do Trybunału Sprawiedliwości z pytaniem o uprawnienia i obowiązki inspektora ochrony danych jako „organu nadzorczego” w rozumieniu RODO.

Rzecznik generalny Priit Pikamäe uważa, że organ nadzorczy ma obowiązek interweniować w przypadku stwierdzenia naruszenia ochrony danych osobowych w ramach rozpatrywania skargi. W szczególności jest zobowiązany do określenia środków naprawczych najodpowiedniejszych dla zaradzenia naruszeniu i zapewnienia przestrzegania praw osoby, której dane dotyczą.

W tym względzie choć RODO pozostawia pewne uprawnienia dyskrecjonalne organowi nadzorczemu, wymaga ono, aby środki te były odpowiednie, niezbędne i proporcjonalne.

Wynika z tego, że:

- uprawnienia dyskrecjonalne w zakresie wyboru środków są ograniczone, gdy wymagana ochrona może zostać zapewniona jedynie poprzez podjęcie konkretnych środków[1] oraz, że
- organ nadzorczy może pod pewnymi warunkami zrezygnować ze środków wymienionych w RODO, jeżeli jest to uzasadnione szczególnymi okolicznościami danej sprawy.

Może tak być w szczególności w sytuacji, gdy administrator podjął pewne działania z własnej inicjatywy.

W każdym razie zainteresowana osoba nie ma prawa żądania przyjęcia określonego środka[2]. Zasady te mają również zastosowanie do systemu administracyjnych kar pieniężnych[3].

**Źródło: komunikat prasowy TSUE**

Fot. pixabay

[1] Tym samym nie można wykluczyć, że w zależności od szczególnych okoliczności danej sprawy uprawnienia dyskrecjonalne mogą ograniczać się do przyjęcia jednego odpowiedniego środka.

[2] Oprócz ewentualnie sytuacji, gdy uprawnienia dyskrecjonalne będą ograniczać się w zależności od szczególnych okoliczności konkretnego przypadku do przyjęcia jednego odpowiedniego środka. Natomiast co się tyczy nałożenia kary pieniężnej, rzecznik generalny wyklucza kategorycznie prawo podmiotowe osoby, której dane dotyczą, do żądania nałożenia takiej kary, ze względu na jej karny charakter.

[3] W odniesieniu do uprawnień dyskrecjonalnych organu nadzorczego rzecznik generalny zaznacza, że zasada równego traktowania pociąga za sobą konieczność wypracowania praktyki administracyjnej nakładania kar pieniężnych, która traktuje podobne przypadki w porównywalny sposób.

# OPINIA RZECZNIKA GENERALNEGO W SPRAWIE C-446/21 SCHREMS

**Rzecznik generalny Athanasios Rantos w przedmiocie życia prywatnego uznał, że użytkownik sieci społecznościowej, wypowiadając się publicznie na temat własnej orientacji seksualnej „w oczywisty sposób" upublicznia te dane, nie wyrażając jednak zgody na ich przetwarzanie do celów reklamy spersonalizowanej.**

W 2018 r. Meta Platforms Ireland przedstawiła swoim użytkownikom w Unii Europejskiej nowe warunki korzystania z Facebooka. Udzielenie na nie zgody jest wymagane, aby móc się zarejestrować lub uzyskać dostęp do kont i usług świadczonych przez Facebook.

Maximilian Schrems, użytkownik Facebooka i aktywista w dziedzinie ochrony danych, zaakceptował te warunki. Regularnie otrzymywał reklamy kierowane do osób orientacji homoseksualnej i zaproszenia na odpowiednie wydarzenia. Te reklamy nie były oparte bezpośrednio na jego orientacji seksualnej, lecz na przeprowadzonej analizie jego zainteresowań.

M. Schrems, niezadowolony z takiego przetwarzania jego danych, które uważa za niezgodne z prawem, skierował skargę do sądów austriackich. Następnie, podczas dyskusji panelowej, oświadczył publicznie, że jest homoseksualistą, ale nigdy niczego nie opublikował na swoim profilu na Facebooku.

Austriacki sąd najwyższy zastanawia się nad wykładnią, jaką należy nadać ogólnemu rozporządzeniu o ochronie danych osobowych (RODO). Zwrócił się do Trybunału Sprawiedliwości z pytaniem, czy sieć taka jak Facebook może analizować i przetwarzać wszystkie dostępne dla niej dane osobowe dla celów reklamy ukierunkowanej, bez ograniczenia w czasie lub w zależności od charakteru danych. Ponadto zwrócił do Trybunału z pytaniem, czy fakt, że dana osoba wypowiedziała się w ramach dyskusji panelowej w przedmiocie własnej orientacji seksualnej pozwala na przetwarzanie innych danych na ten temat w celu kierowania do niej reklamy spersonalizowanej.

W odniesieniu do pierwszego z tych pytań rzecznik generalny Athanasios Rantos zaproponował Trybunałowi wydanie rozstrzygnięcia, że RODO stoi na przeszkodzie temu, aby dane osobowe mogły być przetwarzane w celu reklamy ukierunkowanej bez ograniczenia w czasie. Sąd krajowy musi być w stanie ocenić, przy zastosowaniu w szczególności zasady proporcjonalności, w jakim zakresie okres przechowywania i ilość przetwarzanych danych są uzasadnione zgodnym z prawem

celem przetwarzania tych danych dla celów reklamy spersonalizowanej.

Jeśli chodzi o drugie z pytań, rzecznik generalny, z zastrzeżeniem dokonania ustaleń faktycznych przez austriacki sąd najwyższy, jest zdania, że okoliczność polegająca na tym, iż M. Schrems podczas otwartej dla publiczności dyskusji panelowej całkowicie świadomie wypowiedział się w przedmiocie własnej orientacji seksualnej może stanowić akt, przez który „w oczywisty sposób upublicznił" on te dane w rozumieniu RODO. Przypomniał, że choć dane dotyczące orientacji seksualnej należą do kategorii szczególnie chronionych, które są objęte zakazem przetwarzania, zakaz ten nie ma zastosowania w sytuacji, gdy osoba, których te dane dotyczą, upublicznia je w oczywisty sposób. Niemniej takie zajęcie stanowiska nie stanowi, jako takie, udzielenia zgody na przetwarzanie tych danych do celów reklamy spersonalizowanej.

**Źródło:** komunikat prasowy TSUE

---

**Uwaga do powyższych opinii:**
Opinia rzecznika generalnego nie wiąże Trybunału Sprawiedliwości. Zadanie rzeczników generalnych polega na przedkładaniu Trybunałowi, przy zachowaniu całkowitej niezależności, propozycji rozstrzygnięć prawnych w sprawach, które rozpatrują. Sędziowie Trybunału rozpoczynają właśnie obrady w tej sprawie. Wyrok zostanie wydany w terminie późniejszym.

Odesłanie prejudycjalne pozwala sądom państw członkowskich, w ramach rozpatrywanego przez nie sporu, zwrócić się do Trybunału z pytaniem o wykładnię prawa Unii lub o ocenę ważności aktu Unii. Trybunał nie rozpoznaje sporu krajowego. Do sądu krajowego należy rozstrzygnięcie sprawy zgodnie z orzeczeniem Trybunału. Orzeczenie to wiąże w ten sam sposób inne sądy krajowe, które spotkają się z podobnym problemem.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl