

LEX  ARTIST



BLOG-DANEOSOBOWE.PL

RODO Aktualności

Data publikacji: 10.03.2026

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

Spis treści

1. UODO: Fundacja od nieodpłatnej pomocy prawnej ukarana za naruszenia RODO
2. Prezes UODO nakłada karę ponad 15 000 zł za brak niezwłocznej publikacji danych IOD oraz za konflikt interesów
3. Lotniska w Polsce z jednym standardem RODO. Jest list intencyjny PPL i portów regionalnych
4. W ChatGPT pojawią się reklamy. Czy nasze dane będą w niebezpieczeństwie?
5. Komitet Wyborczy Karola Nawrockiego naruszył przepisy RODO publicznie udostępniając dane osobowe
6. Za proces przetwarzania danych osobowych odpowiada administrator oraz podmiot przetwarzający
7. TikTok pod lupą austriackiego organu ochrony danych - skargi dotyczą pozyskiwania i ujawniania informacji o użytkownikach

UODO: Fundacja od nieodpłatnej pomocy prawnej ukarana za naruszenia RODO

- **Kontekst:** Urząd Ochrony Danych Osobowych (UODO) przypomina, że **organizacje pozarządowe realizujące zadania publiczne** (zwłaszcza w obszarach wrażliwych) **muszą stosować te same zasady RODO** co inne podmioty. Misja społeczna ani finansowanie publiczne nie zwalniają z obowiązków w zakresie ochrony danych.
- **Przykład problemu systemowego:** Sprawa Fundacji Lumus (działającej w systemie **nieodpłatnej pomocy prawnej i poradnictwa obywatelskiego – NPP/NPO**) ujawniła brak świadomości i praktyk zgodnych z RODO.
- **Co się stało:** Do organu terenowej administracji rządowej trafił dokument Fundacji dotyczący wpisu na listę organizacji uprawnionych do prowadzenia punktów NPP/NPO, a wraz z nim **załącznik z niezanonimizowanymi danymi**:
 - 29 beneficjentów NPP oraz 4 współpracowników Fundacji,
 - m.in. imiona i nazwiska, **numery PESEL**, adresy, telefony,
 - oraz informacje o sytuacji życiowej, prawnej i **zdrowotnej** (dane szczególnie wrażliwe).
- **Ocena UODO:** Tak szeroki zakres danych **nie był wymagany** przepisami ustawy o nieodpłatnej pomocy prawnej i został uznany za **nadmiarowy**, co doprowadziło do **nieuprawnionego ujawnienia danych**.
- **Brak właściwej reakcji na naruszenie:** Fundacja nie dopełniła kluczowych obowiązków:
 - nie zgłosiła naruszenia do UODO w ciągu **72 godzin** (art. 33 ust. 1 RODO),
 - nie poinformowała bez zbędnej zwłoki osób, których dane dotyczą (art. 34 ust. 1 RODO).
- **Stanowisko UODO ws. ryzyka:** UODO nie zgodził się z argumentem, że ryzyko było „mało prawdopodobne”, bo dane trafiły do instytucji publicznych i w formie papierowej. Sam fakt ujawnienia (zwłaszcza danych wrażliwych) **tworzy ryzyko** i uruchamia obowiązki z RODO — nawet jeśli szkoda ostatecznie nie wystąpi.
- **Spóźnione działania:** Osoby, których dane ujawniono, zostały poinformowane dopiero po interwencji UODO; organ uznał to za **spóźnione i niewystarczające**.
- **Drugi problem: konflikt interesów przy inspektorze ochrony danych (IOD):** Funkcję IOD pełnił członek zarządu, a następnie prezes zarządu. UODO uznał to za sprzeczne z art. 38 ust. 6 RODO, bo IOD musi być **niezależny** i nie może „nadzorować sam siebie”.
- **Krytyka UODO:** Negatywnie oceniono także, że analiza konfliktu interesów została zatwierdzona przez osobę, której bezpośrednio dotyczyła.
- **Dodatkowe uchybienia formalne:** Fundacja naruszyła art. 37 ust. 7 RODO, ponieważ:
 - nie opublikowała danych kontaktowych IOD,
 - nie zgłosiła wyznaczenia IOD do UODO w terminie **14 dni**.
- **Konsekwencje:**
 - **Kara administracyjna:** 22 920 zł za naruszenia art. 33 ust. 1, art. 37 ust. 7 i art. 38 ust. 6 RODO,
 - **Upomnienie:** za naruszenie art. 34 ust. 1 RODO.
- **Co dalej:** Fundacja w trakcie postępowania dostosowała się do wytycznych UODO, ale organ uznał, że nie jest to wystarczający powód, by całkowicie odstąpić od kary.
- **Wniosek na przyszłość:** Decyzja UODO (sygn. DKN.5131.15.2025) ma podkreślać, że **NGO realizujące zadania publiczne muszą wdrażać realne procedury RODO** (minimalizacja danych, anonimizacja, szybkie zgłaszanie naruszeń, niezależny IOD), a nie traktować wymogów jako formalności.

Źródło: <https://www.prawo.pl/biznes/uodo-ukaral-fundacje-lumus-za-naruszenie-rod0,1539576.html>

Prezes UODO nakłada karę ponad 15 000 zł za brak niezwłocznej publikacji danych IOD oraz za konflikt interesów

- **Kontekst sprawy:** Prezes UODO (organ nadzorczy ds. ochrony danych) przeprowadził postępowanie po sygnale od **Wojewody**, który wskazał na możliwe naruszenie ochrony danych. Chodziło o przesłanie do Urzędu Wojewódzkiego **25 kart potwierdzających udzielenie pomocy prawnej** zawierających dane beneficjentów, w tym numery PESEL.
- **Co się wydarzyło (sedno incydentu):** do ujawnienia danych doszło **przez pomyłkę pracownika** – do przesyłki dołączono **niezanonimizowane** kopie kart, mimo wydania polecenia anonimizacji dokumentów.
- **Skutek naruszenia:** ujawniono dane osobowe **29 osób** podmiotom nieuprawnionym (w tym beneficjentów pomocy prawnej oraz – jak wskazano – dane współpracowników).
- **Ważne tło prawne:** w obszarze nieodpłatnej pomocy prawnej obowiązują dodatkowe wymogi zachowania **poufności** przy udzielaniu pomocy i dokumentowaniu działań (wynikające z ustawy z 5 sierpnia 2015 r.).
- **Wynik postępowania:** Prezes UODO stwierdził **cztery odrębne naruszenia** przepisów RODO i ustawy o ochronie danych osobowych, które łącznie pokazały „szerokie skutki” kontroli.
- **Naruszenie 1 – spóźnione zgłoszenie naruszenia do UODO:** administrator nie zgłosił naruszenia ochrony danych **bez zbędnej zwłoki**.
 - **Sankcja:** administracyjna kara pieniężna **6 700 zł**.
- **Naruszenie 2 – brak zawiadomienia osób, których dane ujawniono:** administrator nie poinformował osób, których dane zostały ujawnione w sposób nieuprawniony.
 - **Sankcja:** **upomnienie** (bez kary finansowej).
- **Naruszenie 3 – obowiązki dot. Inspektora Ochrony Danych (IOD):** brak niezwłocznej publikacji danych kontaktowych IOD na stronie internetowej oraz brak terminowego/formalnie poprawnego zawiadomienia organu o wyznaczeniu IOD.
 - **Sankcja:** administracyjna kara pieniężna **6 091 zł**.
 - **Ustalenia szczegółowe:** organ wskazał, że zawiadomienie o wyznaczeniu IOD zostało skutecznie dokonane dopiero **25 sierpnia 2025 r.**, co oznaczało uchybienie terminom (wskazano m.in. opóźnienie rzędu **ok. 6 miesięcy** w jednym z przypadków).
 - **Wymogi formalne:** zgłoszenie IOD powinno być dokonane elektronicznie z kwalifikowanym podpisem lub przez profil zaufany ePUAP (zgodnie z ustawą z 10 maja 2018 r.).
- **Naruszenie 4 – konflikt interesów IOD:** Prezes UODO uznał za nieakceptowalne pełnienie funkcji IOD przez osobę, która jednocześnie jest **członkiem zarządu**, a następnie także **prezesem zarządu** (poziom zarządzający).
 - **Kluczowe uzasadnienie:** IOD musi działać **niezależnie** i mieć warunki do efektywnej realizacji zadań; łączenie funkcji kontrolnej (IOD) z zarządczą rodzi konflikt interesów i podważa fundamenty roli IOD (odwołania m.in. do zasad z art. 38–39 RODO oraz podejścia Grupy Roboczej Art. 29).
 - **Praktyczny wniosek:** nawet jeśli organizacja uważa, że „charakter projektów” zapewnia niezależność, organ może uznać, że sam fakt łączenia ról zarządczych z funkcją IOD jest sprzeczny z wymaganiami braku konfliktu interesów.
- **Informacje o skali kar:** wskazano, że jedna z nałożonych kar stanowiła ok. **0,16% obrotu** organizacji za 2024 r., a jednocześnie jedynie ok. **0,015% maksymalnej możliwej kary** przewidzianej w art. 83 ust. 4 RODO dla tego typu naruszeń.
- **Najważniejsze wnioski dla organizacji (w prostych słowach):**
 - Incydent może zacząć się od pojedynczej pomyłki (np. brak anonimizacji), ale konsekwencje obejmują też to, **jak organizacja reaguje** (zgłoszenie, powiadomienie osób, dokumentacja).
 - Obowiązki związane z IOD są realnie kontrolowane: trzeba **terminowo zgłosić** IOD do UODO i **opublikować** dane kontaktowe.
 - Nie należy łączyć funkcji IOD z rolami zarządczymi – ryzyko **konfliktu interesów** może samo w sobie zostać uznane za naruszenie.
 - Ochrona danych w obszarze pomocy prawnej wymaga szczególnej dbałości o **poufność** oraz właściwe przygotowanie i sprawdzenie dokumentów przed wysyłką.

Źródło: <https://judykatura.pl/prezes-uodo-naklada-kare-ponad-15-000-zl-za-brak-niezwlocznej-publicacji-danych-iod-oraz-za-konflikt-interesow/>

Lotniska w Polsce z jednym standardem RODO. Jest list intencyjny PPL i portów regionalnych

- **Kontekst:** Polskie lotniska przetwarzają bardzo dużo danych osobowych pasażerów i pracowników (m.in. w systemach bezpieczeństwa i monitoringu). Dotąd każde lotnisko stosowało przepisy RODO na własnych zasadach.
- Polskie Porty Lotnicze (PPL) oraz Związek Regionalnych Portów Lotniczych podpisały **list intencyjny** w sprawie przygotowania **wspólnego kodeksu postępowania RODO** dla podmiotów zarządzających infrastrukturą lotniskową.
- **Cel inicjatywy:** stworzenie **jednolitego** kodeksu, który doprecyzuje ogólne wymagania RODO do realiów funkcjonowania lotnisk i ułatwi ich praktyczne stosowanie.
- Kodeks ma stanowić podstawę do **certyfikacji** – czyli formalnego potwierdzenia, że dane lotnisko działa zgodnie z ustalonymi zasadami ochrony danych.
- Powstanie **zespół roboczy** z ekspertów PPL i przedstawicieli portów regionalnych, który ma opisać i uporządkować procesy przetwarzania danych na lotniskach.
- Mapowanie procesów obejmie m.in. obszary: **bezpieczeństwo, marketing, HR** oraz **operacje lotnicze**.
- **Zakres danych:** lotniska przetwarzają dane pasażerów, osób towarzyszących, pracowników, personelu firm obsługi naziemnej oraz podmiotów świadczących usługi na terenie lotniska – również poprzez **monitoring**.
- **Oczekiwany efekt dla lotnisk:** większa **pewność prawna** i bardziej przejrzyste, jednolite zasady działania w całej branży.
- **Oczekiwany efekt dla pasażerów:** gwarancja, że niezależnie od tego, z którego lotniska w Polsce korzystają, ich dane będą chronione według **tych samych wysokich standardów**.
- Wiceminister infrastruktury Maciej Lasek podkreślił, że lotniska są **infrastrukturą krytyczną**, a bezpieczeństwo fizyczne pasażerów jest powiązane z **bezpieczeństwem cyfrowym**.
- Inicjatywę poparł Prezes Urzędu Ochrony Danych Osobowych (PUODO) Mirosław Wróblewski, wskazując na korzyści: większą **transparentność** i łatwiejsze przestrzeganie przepisów dla administratorów oraz **realny wzrost ochrony prywatności** dla osób, których dane dotyczą.
- **Dalsze kroki:** projekt kodeksu ma przejść **konsultacje społeczne**, a następnie trafi do **zatwierdzenia przez Prezesa UODO**.
- Uzyskanie certyfikatu ma sprawić, że stosowanie kodeksu będzie **oficjalnym potwierdzeniem zgodności z RODO**, uznawanym przez organy nadzorcze w Unii Europejskiej.

Źródło: <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/10645110,lotniska-w-polsce-z-jednym-standardem-rod0-jest-list-intencyjny-ppl-i.html>

W ChatGPT pojawią się reklamy. Czy nasze dane będą w niebezpieczeństwie?

- **Kontekst:** W USA dorośli użytkownicy ChatGPT zaczęli otrzymywać reklamy. OpenAI zapowiada, że z czasem podobne rozwiązanie może pojawić się także w innych krajach, w tym potencjalnie w Europie. To rodzi pytania, czy dane użytkowników będą wykorzystywane zgodnie z prawem oraz jak realna będzie kontrola nad personalizacją reklam.
- **Główna obawa:** reklamy w narzędziu takim jak ChatGPT mogą być bardziej wpływowe niż tradycyjne reklamy, bo są powiązane z treścią rozmowy i mogą oddziaływać na decyzje oraz sposób myślenia użytkownika, nie tylko na zakupy.
- **Ryzyko manipulacji i podatności na sugestie:** prawnicy wskazują, że jeśli „asystent” dobrze pozna użytkownika (np. po historii rozmów), rośnie ryzyko manipulowania jego wyborami. Dodatkowym problemem jest to, że użytkownicy mogą nie rozumieć, jak działają algorytmy dobierające reklamy (lub nie dostaną pełnych wyjaśnień).
- **Profilowanie = przetwarzanie danych osobowych:** nawet jeśli reklamodawcy nie mają dostępu do treści czatów, samo dobieranie reklam „pod użytkownika” oznacza profilowanie, a więc przetwarzanie danych osobowych. OpenAI musi mieć do tego odpowiednią podstawę prawną.
- **RODO i zgoda jako kluczowa podstawa prawna:** eksperci podkreślają, że w świetle podejścia organów ochrony danych (m.in. EROD) oraz orzecznictwa TSUE, przy reklamie targetowanej najczęściej wymagana jest **zgoda** użytkownika. Zgoda musi być dobrowolna, konkretna, świadoma i możliwa do wycofania w każdej chwili — oraz zebrana **zanim** zacznie się profilowanie marketingowe.
- **Możliwe ryzyko „zautomatyzowanego podejmowania decyzji” (art. 22 RODO):** ponieważ rozmowy z AI mogą przypominać kontakt z przyjacielem lub ekspertem i dotyczyć wrażliwych spraw, reklamy dopasowane do kontekstu rozmowy mogą (zdaniem jednej z ekspertek) rodzić ryzyko uznania tego mechanizmu za formę zautomatyzowanego oddziaływania na użytkownika.
- **DSA (Akt o usługach cyfrowych) – znaczenie zależy od tego, czym „formalnie” jest ChatGPT:**
 - DSA nakłada szczególne obowiązki reklamowe głównie na **platformy internetowe** (m.in. przejrzystość reklam i ograniczenia profilowania).
 - Według jednego z prawników podstawowa funkcja ChatGPT jest bardziej podobna do **wyszukiwarki** (odpowiedź na prywatne zapytanie), a nie do platformy społecznościowej, bo nie polega na publicznym rozpowszechnianiu treści.
 - ChatGPT może jednak mieć **elementy platformowe** w funkcjach typu *custom GPT*, gdzie użytkownicy mogą tworzyć i udostępniać konfiguracje innym — to może mieć znaczenie dla oceny obowiązków z DSA.
- **Zakaz wykorzystywania danych wrażliwych do profilowania reklam:** jeśli mechanizmy DSA mają zastosowanie, pojawia się m.in. zakaz profilowania reklam w oparciu o szczególne kategorie danych (np. zdrowie, poglądy polityczne) oraz obowiązek wyjaśniania, jakie parametry decydują o doborze reklamy.
- **AI Act (Akt o sztucznej inteligencji):** eksperci wskazują, że może mieć znaczenie poprzez katalog praktyk zakazanych, w tym (w uproszczeniu) zakazy dotyczące manipulacji i wykorzystywania słabości użytkowników. W niektórych przypadkach może też wspierać prawo do informacji lub skargi.
- **Przejrzystość i kontrola użytkownika:** prawnicy podkreślają potrzebę jasnego oznaczania reklam, wyjaśniania zasad ich doboru oraz zapewnienia użytkownikom realnej opcji ograniczenia personalizacji (a nie tylko deklaratywnej).
- **Wątpliwości etyczne:** nawet jeśli formalnie da się spełnić wymogi prawne, pozostaje pytanie, jak dużo informacji firmy technologiczne faktycznie ujawnią o mechanizmach reklamowych i czy bez presji (np. sporów, kontroli regulatorów) użytkownicy uzyskają pełny obraz sytuacji.
- **Potencjalny problem nierówności/dyskryminacji ekonomicznej:** wskazano, że reklamy mają dotyczyć planów Free i Go, a nie subskrypcji płatnych i biznesowych. Może to oznaczać, że osoby mniej zamożne będą bardziej narażone na wpływ reklam i „konsumpcyjne” bodźce.
- **Wniosek końcowy:** o zgodności z prawem w UE nie da się dziś przesądzić, bo nie znamy szczegółów wdrożenia reklam na rynku europejskim. Kluczowe będą konkretne rozwiązania techniczne i organizacyjne OpenAI (zwłaszcza w zakresie zgody, profilowania, przejrzystości oraz możliwości wyłączenia personalizacji).

Źródło: <https://www.gazetaprawna.pl/firma-i-prawo/artykuly/10645906,w-chatgpt-pojawia-sie-reklamy-czy-nasze-dane-beda-w-niebezpieczenstwie.html>

Komitet Wyborczy Karola Nawrockiego naruszył przepisy RODO publicznie udostępniając dane osobowe

- **Kontekst sprawy:** w trakcie kampanii prezydenckiej w 2025 r. publicznie pokazano dokumenty dotyczące sprzedaży mieszkania („kawalerki”) oraz testamentu holograficznego. Prezes UODO Mirosław Wróblewski uznał, że doszło do naruszenia RODO i nałożył na Komitet Wyborczy Kandydata na Prezydenta RP Karola Nawrockiego karę **35 582 zł**.
- **Co się wydarzyło:** 6 maja 2025 r. podczas konferencji prasowej w siedzibie PiS posłowie (m.in. Przemysław Czarnek) zaprezentowali i omawiali dokumenty związane z transakcją. Dokumenty były widoczne dla kamer i mediów, **bez anonimizacji**.
- **Jakie dokumenty ujawniono:** m.in. **umowę przedwstępną sprzedaży mieszkania, pełnomocnictwa oraz testament**.
- **Jakie dane osobowe ujawniono:** m.in. imiona i nazwiska, imiona rodziców, numery PESEL, serie i numery dowodów osobistych, adresy zamieszkania, informacje o sytuacji rodzinnej oraz o rozporządzeniu majątkiem.
- **Kogo dotyczyło ujawnienie:** dane obejmowały kandydata na prezydenta, ale także **dwie osoby niepełniące funkcji publicznych** (właściciela mieszkania i małżonkę kandydata). W ocenie UODO co najmniej jedna z tych osób **na pewno nie wyraziła zgody** na udostępnienie danych.
- **Wyjaśnienia posła:** pełnomocnik wskazywał brak zamiaru ujawnienia danych, a sam poseł Przemysław Czarnek podał, że dokumenty otrzymał od organizatorów konferencji kandydata i działał, by przedstawić „rzeczywiste okoliczności” w odpowiedzi na zarzuty w kampanii.
- **Stanowisko Komitetu Wyborczego:** komitet potwierdził wyjaśnienia posła, ale **nie zgodził się**, że ujawniono dane osób niepublicznych. Twierdził też, że część danych właściciela mieszkania już krążyła w internecie i sprawa była przedmiotem dużego zainteresowania opinii publicznej.
- **Dlaczego UODO uznał naruszenie:** Prezes UODO stwierdził naruszenie m.in. zasad z **art. 5 ust. 1 lit. a** (zgodność z prawem, rzetelność) oraz **art. 6 ust. 1 RODO** (brak podstawy prawnej przetwarzania) w zakresie ujawnienia danych dwóch osób prywatnych.
- **„To już było w sieci” nie wystarczyło:** UODO wskazał, że nawet jeśli w internecie dało się znaleźć np. imię i nazwisko, to nie oznacza to legalności ujawnienia **pozostałych danych**. Nie było dowodu, że właściciel mieszkania sam je publikował lub wyraził na to zgodę.
- **Interes kampanii nie usprawiedliwia wszystkiego:** UODO podkreślił, że ujawnienia danych osób prywatnych **nie można uznać za konieczne** dla prowadzenia kampanii czy odpierania zarzutów. Dokumenty **można i należało zanonimizować**, a dodatkowe dane nie wnosiły istotnej wartości informacyjnej dla celu konferencji.
- **Brak wykazania podstawy prawnej:** komitet jako administrator danych miał obowiązek wykazać legalną podstawę przetwarzania (zasada rozliczalności), ale **nie wykazał** jej ani wobec właściciela mieszkania, ani wobec małżonki kandydata.
- **Naruszenie prywatności:** UODO ocenił, że ujawnienie danych właściciela mieszkania było **bardzo silną i niepotrzebną ingerencją** w jego prawo do prywatności, a komitet nie przeprowadził analizy, która uzasadniałaby nadrzędność interesu kandydata nad interesami tych osób.
- **Wysokość kary:** choć RODO przewiduje kary nawet do 20 mln euro (lub 4% obrotu przedsiębiorstwa), w tej sprawie zastosowano metodykę EROD (Wytyczne 04/2022) i nałożono karę **35 582 zł**, uznaną za adekwatną i sprawiedliwą.
- **Dlaczego nie skończyło się na upomnieniu:** UODO wskazał, że samo upomnienie nie byłoby proporcjonalne, m.in. dlatego, że komitet był już wcześniej adresatem środków nadzorczych w podobnych sprawach.
- **Znaczenie „recydywy”:** obecna kara ma związek z tym, że naruszenie nastąpiło w warunkach powtórzenia naruszeń: wcześniej komitet Karola Nawrockiego został m.in. **upomniany** i zobowiązany do **usunięcia** materiału z YouTube zawierającego wrażliwe informacje o życiu prywatnym właściciela mieszkania (zdrowie, problemy rodzinne i finansowe, problemy z prawem).
- **Powiązane działania wobec innych podmiotów:** temat „kawalerki” wykorzystał też Komitet Wyborczy Rafała Trzaskowskiego – wobec niego również wszczęto postępowanie, zakończone **upomnieniem** za ujawnienie nazwiska właściciela mieszkania oraz danych placówki, w której przebywał.

Źródło: <https://uodo.gov.pl/pl/138/4083>

Za proces przetwarzania danych osobowych odpowiada administrator oraz podmiot przetwarzający

- **Kontekst sprawy:** Naczelny Sąd Administracyjny (NSA) uwzględnił skargę kasacyjną Prezesa UODO i uchylił wyrok Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie w sprawie naruszenia przepisów RODO przez Fortum Marketing and Sales S.A. (administrator danych) oraz Pika Sp. z o.o. (podmiot przetwarzający). Wcześniej WSA uchylił decyzję Prezesa UODO nakładającą kary na obie spółki.
- **Co się wydarzyło (incydent):** Sprawa sięga kwietnia 2020 r., gdy Fortum zgłosiło naruszenie ochrony danych. Incydent był związany ze zmianami w systemie informatycznym pełniącym funkcję cyfrowego archiwum.
- **Przyczyna naruszenia:** Podmiot przetwarzający (Pika), próbując poprawić wydajność systemu, utworzył dodatkową bazę danych i zasilił ją danymi klientów Fortum, ale udostępnił ją w nieprawidłowy sposób, co umożliwiło dostęp osobom nieuprawnionym i skopiowanie danych.
- **Skala i zakres danych:** Naruszenie dotyczyło danych ponad **95 tys. osób**. Ujawnione dane obejmowały m.in. imiona i nazwiska, adresy, numery PESEL, dane dokumentów tożsamości, dane kontaktowe oraz informacje o zawartych umowach.
- **Powiadomienie osób:** Fortum początkowo uznało, że nie ma wysokiego ryzyka dla praw i wolności osób, więc nie poinformowało ich o incydencie. Dopiero po interwencji Prezesa UODO osoby zostały zawiadomione i otrzymały zalecenia ograniczające skutki naruszenia.
- **Ustalenia Prezesa UODO:** Organ nadzorczy uznał, że zarówno Fortum, jak i Pika nie wdrożyły odpowiednich środków technicznych i organizacyjnych wymaganych przez RODO, aby właściwie zabezpieczyć dane.
- **Zarzuty wobec Fortum (administratora):**
 - brak weryfikacji przed zawarciem umowy powierzenia, czy Pika daje wystarczające gwarancje bezpieczeństwa,
 - nieskorzystanie z prawa kontroli/audytu (art. 28 ust. 3 lit. h RODO),
 - brak realnego nadzoru nad wprowadzaniem zmian w systemie.
- **Zarzuty wobec Piki (podmiotu przetwarzającego):**
 - brak testowania zabezpieczeń na etapie prac rozwojowych,
 - używanie rzeczywistych danych osobowych do testów bez pseudonimizacji,
 - niepełna konfiguracja zabezpieczeń technicznych, w tym brak podstawowych rozwiązań (np. firewall).
- **Standardy bezpieczeństwa:** Prezes UODO odwołał się do norm i dobrych praktyk (m.in. ISO/IEC 27001 i 27002), wskazując, że w środowiskach testowych nie powinno się używać realnych danych, a jeśli już – muszą być one chronione jak w środowisku produkcyjnym.
- **Decyzja Prezesa UODO i kary:**
 - dla Fortum: kara **blisko 5 mln zł** (m.in. naruszenia art. 5, 25, 28 i 32 RODO),
 - dla Piki: kara **ponad 250 tys. zł** (naruszenia dotyczące bezpieczeństwa przetwarzania – art. 32 RODO w powiązaniu z obowiązkami z art. 28).
- **Stanowisko WSA (dlaczego uchylił decyzję):** WSA uznał, że Prezes UODO nie wykazał wystarczająco stanu faktycznego i nie przeprowadził pełnej oceny dowodów; sugerował też potrzebę dodatkowych ustaleń (standardy rynkowe, audyty i ich potencjalny wpływ na zapobieżenie incydentowi).
- **Stanowisko NSA (dlaczego uchylił wyrok WSA):** NSA uznał, że Prezes UODO wyjaśnił istotne okoliczności, zebrał i ocenił obszerny materiał dowodowy zgodnie z prawem oraz spójnie uzasadnił decyzję, a WSA błędnie zakwestionował kompletność ustaleń i ocenę dowodów.
- **Kluczowe doprecyzowanie NSA:** NSA za niezrozumiałe uznał rozważania WSA, czy doszło do „wycieku” czy „krótkotrwałej możliwości dostępu”, wskazując, że utrata poufności danych została jednoznacznie ustalona przez Prezesa UODO.
- **Co dalej:** NSA uchylił wyrok WSA i przekazał sprawę do ponownego rozpoznania, wskazując, że WSA powinien uznać kompletność ustaleń faktycznych dokonanych przez organ na podstawie zgromadzonego materiału dowodowego.
- **Najważniejszy wniosek praktyczny:** Artykuł podkreśla, że odpowiedzialność za bezpieczeństwo danych dotyczy zarówno administratora, jak i podmiotu przetwarzającego, a kluczowe są: realny nadzór, weryfikacja zabezpieczeń dostawców, testowanie zmian oraz właściwe zabezpieczenie (lub pseudonimizacja) danych używanych w pracach rozwojowych i testach.

Źródło: <https://uodo.gov.pl/pl/138/4088>

TikTok pod lupą austriackiego organu ochrony danych - skargi dotyczą pozyskiwania i ujawniania informacji o użytkownikach

- **Kontekst:** po doniesieniach o zbiorowych pozwach przeciwko TikToku w Holandii, artykuł opisuje **skargi złożone na TikToka do austriackiego organu ochrony danych**, dotyczące sposobu pozyskiwania i ujawniania informacji o użytkownikach.
- **Co ustalono:** jeden z użytkowników, korzystając z **prawa dostępu do danych**, odkrył, że TikTok otrzymywał informacje o jego aktywności w **innych aplikacjach mobilnych**.
- **Jakie dane wchodziły w grę:** wśród danych miały znaleźć się informacje o korzystaniu z **Grindr** oraz bardziej szczegółowe dane o działaniach użytkownika w innych usługach (np. **interakcje** czy **aktywność zakupowa**), a nie tylko sam fakt używania aplikacji.
- **Rola pośrednika:** według ustaleń dane mogły być przekazywane za pośrednictwem podmiotu pośredniczącego **AppsFlyer** (czyli mechanizmu/narzędzia, które może ułatwiać przekazywanie danych pomiędzy aplikacjami).
- **Dlaczego to budzi poważne wątpliwości:** tego typu informacje mogą pozwalać na wnioskowanie o życiu prywatnym, w tym o **orientacji seksualnej**, co może oznaczać wejście w zakres **szczególnych kategorii danych** (art. 9 RODO) wymagających spełnienia wyjątkowo rygorystycznych warunków legalności.
- **Brak zgody użytkownika:** skarga wskazuje, że użytkownik **nie wyraził zgody** na przekazywanie takich informacji między aplikacjami ani na ich dalsze wykorzystanie.
- **Problem z realizacją prawa dostępu:** TikTok miał odesłać użytkownika do narzędzia pobierania danych, ale udostępniony zakres informacji był **niepełny**. Dopiero po kolejnych wnioskach platforma potwierdziła, że posiada także **dotychczasowe dane** o aktywności w innych aplikacjach.
- **Potencjalne naruszenia przepisów:** sytuacja rodzi pytania o zgodność z art. **12 i 15 RODO** (pełna, zrozumiała informacja o przetwarzaniu i odbiorcach danych) oraz o istnienie właściwej podstawy prawnej przetwarzania z art. **6 RODO**.
- **Dwie skargi noyb.eu:**
 - pierwsza dotyczy **niepełnej odpowiedzi** na wnioski o dostęp do danych,
 - druga dotyczy **przekazywania danych** pomiędzy TikTok, AppsFlyer i Grindr bez wskazania odpowiedniej podstawy prawnej oraz możliwego naruszenia art. 9 RODO (dane wrażliwe).
- **Szerszy wymiar sprawy:** spór dotyczy nie tylko transparentności, ale też **modelu współdzielenia danych między aplikacjami** oraz roli pośredników w tym przepływie.
- **Pytania, które stawia artykuł:** gdzie leżą granice **profilowania** opartego na danych zbieranych poza daną usługą oraz czy użytkownicy mają **realną kontrolę** nad przepływem swoich danych między różnymi podmiotami.

Źródło: https://www.linkedin.com/posts/adam-szur%C5%82at_rododataprotection-privacy-activity-7434165033216962561-5ym1?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLzLMFC01FENWMw0oL_z0rPX_x8