RODO Aktualności

Data publikacji: 03.11.2026

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. Włoski organ ochrony danych nałożył 33 tys. euro kary na bank
2. Włoski organ ochrony danych nałożył 48 tys. euro kary na operatora pocztowego
3. Digital Omnibus: mandat Rady UE. Co zmienia we wniosku Komisji w RODO i cookies
4. Nieudzielanie informacji Prezesowi UODO kończy się karą pieniężną
5. WSA w Warszawie: tajemnicy bankowej nie powierza się dowolnie
6. Austriacki Sąd Federalny uznał, że żądanie danych dla zwrotu opłat jest nadmierne
7. Uwagi Prezesa UODO do projektu zmian w Prawie oświatowym
8. Mniej zgłoszeń naruszeń, więcej danych dla AI. Gdzie Rada UE stawia granice?
9. Pozyskiwanie zgody na przetwarzanie danych o zdrowiu - wyrok NSA potwierdzający decyzję Prezesa UODO
10. 825 mln euro kary dla Ubera za algorytmy

Włoski organ ochrony danych nałożył 33 tys. euro kary na bank

- **Kontekst (o czym jest artykuł):** Sprawa pokazuje, że samo nazwanie w umowie uczestnika procesu „podmiotem przetwarzającym" nie wystarcza. O roli decyduje to, **kto w praktyce określa cele i sposoby przetwarzania danych** oraz **kto ponosi realną odpowiedzialność**.
- **Czego dotyczyła sprawa:** W modelu współpracy banku z pośrednikiem (obsługującym klientów ubiegających się o pożyczkę) doszło do sytuacji, w której po odmowie finansowania w systemie dostępnym dla wybranych pracowników pośrednika znalazły się informacje o zobowiązaniach finansowych i dochodzie netto klientki (pracownicy operatora pocztowego).
- **Jak działał proces:**
  - **Pośrednik** zbierał i weryfikował dane klientów (i ewentualnych współzobowiązanych), przekazywał je bankowi oraz komunikował klientowi wynik postępowania.
  - **Bank** oceniał zdolność kredytową i samodzielnie podejmował decyzję o udzieleniu albo odmowie finansowania.

- **Stanowisko organu (Włochy):** Włoski organ ochrony danych uznał, że bank i pośrednik w tym układzie działali jako **odrębni administratorzy danych** (a nie jako wzajemne „podmioty przetwarzające").
- **Teza 1 — liczą się faktyczne role:** Status administratora/podmiotu przetwarzającego trzeba ustalać **na podstawie rzeczywistych działań** w danej sytuacji, a nie wyłącznie na podstawie zapisów umowy.
- **Teza 2 — „wzajemne powierzenie" to za mało:** Nie można zgodnie z prawem przyjąć, że strony są wzajemnie podmiotami przetwarzającymi, jeśli **żadna z nich nie przetwarza danych wyłącznie w interesie drugiej** i nie działa jedynie według jej instrukcji.
- **Dlaczego organ uznał ich za odrębnych administratorów:**
  - Bank **ustalał cele i kluczowe środki** przetwarzania potrzebnego do oceny zdolności kredytowej oraz podejmował decyzję wobec klienta.
  - Pośrednik miał **własną relację z klientem** i mógł wykorzystywać proces pośrednictwa także do **proponowania innych rozwiązań** (np. ofert innych banków), czyli działał również we własnym celu.

- **Podstawa przekazania danych a role stron:** Organ przyjął, że wymiana danych mogła być uzasadniona wykonaniem odrębnych relacji umownych (lub działań przedumownych na żądanie klienta), ale to **nie oznacza**, że jedna strona automatycznie staje się „procesorem" drugiej. Każdy administrator odpowiada za zgodność swojego przetwarzania z prawem.
- **Kluczowy problem: obowiązek informacyjny wobec klientów:** Błędne określenie ról przełożyło się na nieprawidłową informację dla osób składających wnioski. Informacja powinna:
  - wskazywać **odbiorców lub kategorie odbiorców** danych,
  - odzwierciedlać rzeczywistą rolę pośrednika jako **odrębnego administratora**.

- **Naruszenia wskazane przez organ:** Bank naruszył zasadę **rzetelności i przejrzystości** oraz obowiązki informacyjne (art. 5 ust. 1 lit. a i art. 13 RODO).
- **Skutki decyzji:**
  - Nałożono na Deutsche Bank karę administracyjną **33 000 euro** (decyzja z **7 października 2026 r.**).
  - Nakazano przygotowanie (w ciągu **6 miesięcy**) nowej informacji dla klientów, uwzględniającej rolę pośrednika jako odrębnego administratora oraz wskazującej odbiorców/kategorie odbiorców danych.

- **Znaczenie praktyczne dla firm:** Dla wieloetapowych procesów (np. bank + pośrednik) samo „umowne" wpisanie roli procesora nie wystarcza. Trzeba przeanalizować m.in.:
  - kto określa **cele** przetwarzania,
  - kto ustala **zasadnicze środki** (jak i po co przetwarza dane),
  - kto podejmuje **decyzje merytoryczne** wobec klienta,
  - czy dane są używane **wyłącznie** dla drugiej strony, czy również dla **własnych celów**.

Źródło: https://judykatura.pl/wloski-organ-ochrony-danych-nalozyl-33-tys-euro-kary-na-bank/

Włoski organ ochrony danych nałożył 48 tys. euro kary na operatora pocztowego

- **Kontekst:** artykuł opisuje decyzję włoskiego organu ochrony danych (ODO) w sprawie tego, jak firmy powinny informować klientów o przetwarzaniu danych w procesie kredytowym. Sedno sporu: informacja może być zwięzła, ale nie może pomijać elementów potrzebnych, by klient realnie zrozumiał, **kto** i **w jakim celu** używa jego danych oraz **komu** są one przekazywane.
- **Decyzja i konsekwencje:** 7 października 2026 r. organ stwierdził naruszenie zasad **rzetelności** i **przejrzystości** oraz nałożył na operatora pocztowego karę **48 000 euro**.
- **Co uruchomiło postępowanie:** skarga pracownicy operatora pocztowego, która wnioskowała o finansowanie przez portal pracowniczy; po odmowie w systemie kadrowym widoczne były dane o jej zobowiązaniach finansowych, ich wysokości i dochodzie netto.
- **Jak wyglądał proces przetwarzania danych:**
  - operator pocztowy zbierał i weryfikował dane wnioskodawcy, a potem przekazywał je bankowi,
  - w niektórych przypadkach przekazywał też zagregowane wskaźniki oparte o relacje finansowe z klientem,
  - bank oceniał zdolność kredytową i sam decydował o przyznaniu lub odmowie finansowania,
  - pośrednik (operator) przekazywał klientowi wynik oraz mógł zaproponować inne rozwiązania finansowe.

- **Kluczowa zasada nr 1 – przejrzystość to realne zrozumienie:** organ podkreślił, że przejrzystość nie jest „formalnością". Klient ma mieć możliwość jasnego zrozumienia celów przetwarzania, ryzyk, zabezpieczeń i tego, jak kontrolowany jest przepływ danych.
- **Zwięzłość nie usprawiedliwia braków:** operator tłumaczył, że zastosował syntetyczną informację, by nie przeciążać odbiorcy. Organ zgodził się, że komunikat powinien być klarowny i uporządkowany, ale wskazał, że **„zwięzłość i kompletność nie są alternatywne"** — nie wolno skracać kosztem pominięcia kluczowych treści.
- **Kluczowa zasada nr 2 – role wynikają z faktów, nie z umowy:** status „administratora" lub „podmiotu przetwarzającego" ocenia się według tego, co podmiot faktycznie robi (cele i zasadnicze środki przetwarzania), a nie według etykiety wpisanej w dokumentach. Organ odwołał się do wytycznych EROD.
- **Ocena ról w tej sprawie:** organ uznał, że bank i operator byli **odrębnymi administratorami**, bo:
  - bank samodzielnie prowadził ocenę zdolności kredytowej i sam decydował o przyznaniu/odmowie,
  - operator prowadził własne działania pośrednictwa, miał odrębną relację z klientem i mógł proponować alternatywne produkty,
  - obie strony działały dla własnych celów wynikających z odrębnych relacji z klientem, a nie „wyłącznie na rzecz" drugiej strony.

- **Dlaczego błędne role uderzyły w obowiązek informacyjny:** strony wzajemnie wskazały się jako podmioty przetwarzające przy przekazywaniu danych, co (zdaniem organu) nie odpowiadało rzeczywistości. To przełożyło się na **nieprawidłową/niepełną informację** dla klientów, m.in. w zakresie wskazania **odbiorców danych** lub **kategorii odbiorców** oraz innych elementów potrzebnych dla przejrzystości.
- **Działania naprawcze uwzględnione przy karze:** usunięcie danych skarżącej, aktualizacja informacji, rozpoczęcie prac nad zmianą ustaleń z bankiem, współpraca z organem, brak wcześniejszych podobnych rozstrzygnięć; organ odnotował też nieumyślny charakter błędnej interpretacji ról.
- **Najważniejsze wnioski praktyczne:**
  - nie można opierać się wyłącznie na zapisach umownych — trzeba sprawdzić, kto faktycznie ustala cele i kluczowe sposoby przetwarzania,
  - jeśli podmioty mają odrębne cele i odrębne relacje z klientem oraz podejmują samodzielne decyzje, zwykle będą **odrębnymi administratorami**,
  - informacja dla klienta ma być prosta i krótka, ale jednocześnie **kompletna na tyle**, by wyjaśniała przepływ danych (w tym: komu dane są przekazywane),
  - błędne określenie ról często powoduje „efekt domina": wadliwą kwalifikację + wadliwy obowiązek informacyjny.

Źródło: https://judykatura.pl/wloski-organ-ochrony-danych-nalozyl-48-tys-euro-kary-na-operatora-pocztowego/

Digital Omnibus: mandat Rady UE. Co zmienia we wniosku Komisji w RODO i cookies

- **Kontekst (co się wydarzyło i czego dotyczy temat):**
  21 października 2026 r. Komitet Stałych Przedstawicieli (Coreper) uzgodnił mandat Rady UE do negocjacji z Parlamentem Europejskim w sprawie pakietu **Digital Omnibus**, który zmienia m.in. **RODO**, **dyrektywę ePrivacy** oraz **Data Act**. Tekst mandatu przekazano delegacjom 22 października. Teraz rozpoczną się **trilogi** (negocjacje Rada–Parlament–Komisja), a ostateczne brzmienie przepisów może się jeszcze zmienić.
- **RODO: definicja „danych osobowych" bez zmian**
  Rada usunęła proponowane przez Komisję doprecyzowanie, że informacja „nie jest daną osobową" dla podmiotu, który nie może zidentyfikować osoby przy użyciu środków „rozsądnie prawdopodobnych". Skreślenia dotyczą zarówno RODO, jak i rozporządzenia 2018/1725 (dla instytucji UE).
- **RODO: nowa, węższa zasada dla pseudonimizacji**
  Pojawia się nowy art. 25a: **dane spseudonimizowane** nie są danymi osobowymi **dla osoby trzeciej**, jeśli ta osoba trzecia nie jest w stanie zidentyfikować osoby, której dane dotyczą. Jeżeli jednak dane trafią dalej do podmiotu mającego środki identyfikacji, to zarówno przekazanie, jak i dalsze użycie będzie traktowane jako **przetwarzanie danych osobowych**. Stosowanie pseudonimizacji ma wymagać odpowiednich środków technicznych i organizacyjnych (w tym bezpieczeństwa), a EROD ma wydać opinię nt. pseudonimizacji i anonimizacji.
- **Cookies: zostają w dyrektywie ePrivacy (nie przechodzą do RODO)**
  Rada skreśliła pomysł przeniesienia zasad dot. cookies do RODO (w tym obowiązku respektowania zautomatyzowanych sygnałów zgody z przeglądarki). Zamiast tego zmienia art. 5 ust. 3 dyrektywy ePrivacy.
- **ePrivacy: łatwiejsza odmowa cookies i „cisza" po odmowie**
  Odmowa zgody ma być możliwa łatwo (np. jednym kliknięciem). Po odmowie dostawca nie może ponownie pytać o zgodę w tym samym celu przez co najmniej **4 miesiące**.
- **ePrivacy: więcej wyjątków bez zgody – ale bez profilowania**
  Bez zgody dopuszczone mają być m.in.: tworzenie anonimowych, zagregowanych statystyk oglądalności przez dostawcę usługi, pomiar widowni mediów (bez śledzenia poza mierzonym serwisem) oraz pomiar wyświetleń i skuteczności reklamy kontekstowej – **bez profilowania**. Komisja ma w 12 miesięcy przygotować raport o technologiach chroniących prywatność.
- **Decyzje zautomatyzowane: utrzymanie ochrony (nie „liberalizacja")**
  Rada wraca do obecnej logiki art. 22 RODO: osoba ma prawo **nie podlegać** decyzji opartej wyłącznie na automatycznym przetwarzaniu, chyba że zachodzi wyjątek (umowa, prawo, wyraźna zgoda). Usunięto też propozycję Komisji wzmacniającą wyjątek umowny („nawet jeśli dałoby się podjąć decyzję inaczej").
- **AI: „uzasadniony interes" nie z automatu**
  Motyw 33a wskazuje, że sam rozwój i eksploatacja systemu/modelu AI **nie są same w sobie** uzasadnionym interesem. Legalność przetwarzania na podstawie uzasadnionego interesu (art. 6 ust. 1 lit. f) ma być oceniana **indywidualnie** w zależności od celu. Dodatkowo nowe przepisy mają podkreślać zabezpieczenia, w tym **prawo sprzeciwu** (art. 21).
- **Mniej obowiązków informacyjnych – ale tylko przy spełnieniu warunków**
  W art. 13 ust. 5 Rada proponuje zwolnienie z przekazywania informacji, jeśli **łącznie**: (1) są uzasadnione podstawy, by sądzić, że osoba już zna tożsamość administratora i cele przetwarzania oraz (2) przetwarzanie **nie wiąże się z wysokim ryzykiem**. Zwolnienie nie ma dotyczyć m.in. złożonych operacji, dużych ilości danych oraz danych wrażliwych (art. 9) i danych o wyrokach/naruszeniach (art. 10).
- **Przegląd obowiązków pod kątem MŚP i organizacji niekomercyjnych**
  Komisja ma w ciągu 6 miesięcy od wejścia zmian w życie przygotować raport z rekomendacjami dot. obowiązków administratorów i podmiotów przetwarzających – ze szczególnym uwzględnieniem **MŚP** oraz organizacji niekomercyjnych prowadzących przetwarzanie **niskiego ryzyka** – i ocenić, czy obowiązki powinny zostać zmienione.
- **Data Act: silniejsza ochrona tajemnic przedsiębiorstwa**
  Rada wzmacnia możliwość odmowy dostępu do danych, gdy ujawnienie grozi **poważną szkodą gospodarczą** albo istotnym ryzykiem przejęcia tajemnic przez podmioty z państw trzecich (wprost wskazano m.in. przemysłowe know-how sektorów krytycznych z dyrektywy NIS2). Tajemnice mogą być ujawniane osobie trzeciej tylko wtedy, gdy jest to **ściśle niezbędne** do celu uzgodnionego z użytkownikiem.
- **Co dalej i dlaczego to ważne:**
  Mandat Rady otwiera trilogi; przepisy mogą się jeszcze zmienić. W praktyce duże znaczenie będzie miało też to, jak nowe zasady będą interpretowane i egzekwowane przez organy nadzorcze oraz sądy.

Źródło: https://judykatura.pl/digital-omnibus-mandat-rady-ue-co-zmienia-we-wniosku-komisji-w-rodo-i-cookies/

Nieudzielanie informacji Prezesowi UODO kończy się karą pieniężną

- **Kontekst:** Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył na Stowarzyszenie RKW – Ruch Kontroli Wyborów – Ruch Kontroli Władzy karę **10 082 zł** za **brak współpracy** i ignorowanie wezwań do przekazania informacji. Ponieważ kara się uprawomocniła, UODO złożył **wniosek o wszczęcie egzekucji administracyjnej** do **Urzędu Skarbowego**.
- **Skąd wzięła się sprawa:** Do UODO wpłynęła informacja o możliwych nieprawidłowościach w przetwarzaniu danych osobowych podczas **wyborów prezydenckich 2025**.
- **Główny wątek podejrzeń:** Według zawiadomienia członkowie obwodowych komisji wyborczych mieli weryfikować uprawnienia osób głosujących na podstawie zaświadczeń, używając **mobilnej aplikacji Stowarzyszenia RKW**, która miała **nie być autoryzowana przez Krajowe Biuro Wyborcze**.
- **Cel działań UODO:** UODO prowadził postępowanie wyjaśniające, aby ustalić m.in.:
  - czy opisywane zdarzenia rzeczywiście miały miejsce,
  - jakie dane osobowe mogły być zbierane/przetwarzane,
  - kto był odpowiedzialny za przetwarzanie danych,
  - gdzie dane były przechowywane (EOG/poza EOG/chmura),
  - jakie zastosowano zabezpieczenia (np. szyfrowanie, ochrona przed nieautoryzowanym dostępem),
  - jaki był cel przetwarzania, okres przechowywania i możliwość usunięcia danych,
  - czy dane mogły być używane do innych celów (np. analitycznych, marketingowych, profilowania).

- **Wezwania do wyjaśnień:** Prezes UODO wysłał do Stowarzyszenia **dwa wezwania** (czerwiec i lipiec 2025 r.) o przekazanie informacji m.in. o danych zbieranych przez formularz internetowy i ewentualnie automatycznie (np. IP, dane urządzenia, lokalizacja).
- **Brak reakcji Stowarzyszenia:** Oba wezwania wróciły z adnotacją „nie podjęto w terminie", ale zgodnie z przepisami zostały uznane za skutecznie doręczone. Stowarzyszenie nie odpowiedziało.
- **Dodatkowa próba kontaktu:** W październiku 2025 r. pracownik UODO skontaktował się telefonicznie z prezesem Stowarzyszenia. Na prośbę Stowarzyszenia UODO ponownie przesłał korespondencję (tym razem została odebrana), jednak **nadal nie udzielono odpowiedzi**.
- **Osobne postępowanie o karę:** Z powodu braku współpracy UODO wszczął odrębne postępowanie w sprawie kary (poinformowano o tym w grudniu 2025 r.). UODO prosił też o dane finansowe za 2024 r. potrzebne do ustalenia wysokości kary, ale Stowarzyszenie również nie odpowiedziało.
- **Podstawa prawna naruszenia według UODO:** UODO uznał naruszenie **art. 58 ust. 1 lit. a oraz lit. e RODO**, czyli obowiązku dostarczenia informacji potrzebnych organowi oraz umożliwienia dostępu do danych i informacji niezbędnych do prowadzenia postępowań.
- **Dlaczego UODO uznał to za poważne:** Według UODO odmowa informacji:
  - uniemożliwiła pełną ocenę roli Stowarzyszenia i sposobu przetwarzania danych,
  - wydłużyła postępowanie wyjaśniające,
  - mogła opóźnić reakcję organu w sprawie osób, których dane mogły być przetwarzane.

- **Okoliczności obciążające:** UODO wskazał m.in.:
  - charakter, wagę i długi czas trwania naruszenia,
  - umyślny charakter (świadomość żądań),
  - całkowity brak współpracy.

- **Czas trwania naruszenia:** UODO przyjął, że naruszenie trwało ponad **10 miesięcy** – od 15 lipca 2025 r. (po terminie na odpowiedź na pierwsze wezwanie) do decyzji z **18 maja 2026 r.**
- **Co nie zadziałało łagodząco:** UODO odnotował brak wcześniejszych naruszeń i brak ustalonych korzyści finansowych po stronie Stowarzyszenia, ale **nie potraktował tego jako okoliczności łagodzących**.
- **Ustalanie wysokości kary:** Ponieważ Stowarzyszenie nie przekazało danych finansowych, UODO dokonał **szacunkowej oceny skali działalności** (określonej jako średnia) i ustalił karę na **10 082 zł**.
- **Argument UODO o proporcjonalności:** UODO wskazał, że jest to **0,012% maksymalnej kary** możliwej w tego typu naruszeniu oraz że sankcja ma być skuteczna, proporcjonalna i odstraszająca.
- **Egzekucja kary:** Po uprawomocnieniu się decyzji UODO rozpoczął działania egzekucyjne – wniosek trafił do **Urzędu Skarbowego**, który prowadzi egzekucję administracyjną.
- **Ważne zastrzeżenie:** Nałożona kara dotyczy **wyłącznie odmowy przekazania informacji** (braku współpracy) i **nie rozstrzyga** merytorycznie, czy w samej aplikacji doszło do naruszeń ochrony danych. Postępowanie w sprawie głównej może trwać dalej.
- **Możliwe dalsze konsekwencje:** Jeśli Stowarzyszenie nadal będzie odmawiało współpracy, UODO może nałożyć **kolejne administracyjne kary pieniężne**.

Źródło: https://uodo.gov.pl/pl/138/4638

WSA w Warszawie: tajemnicy bankowej nie powierza się dowolnie

- **Kontekst:** Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z **14 kwietnia 2026 r.** potwierdza, że **umowa powierzenia przetwarzania (art. 28 RODO) nie może „obejść" ograniczeń** wynikających z przepisów o **tajemnicy bankowej**. Sąd wskazał też, że **błąd systemu nie usprawiedliwia bezpodstawnego marketingu**, a **prawo dostępu do danych** wymaga odpowiedzi **kompletnej i w terminie**.

- **Wynik sprawy:** Sąd **oddalił skargę spółki** na decyzję Prezesa UODO. Utrzymano:
  - upomnienia za **bezpodstawne udostępnienie danych** podmiotowi przetwarzającemu,
  - upomnienie za **marketingowe wykorzystanie adresu e-mail** bez podstawy prawnej,
  - **nakaz przekazania pełnej kopii danych**,
  - upomnienie za **opóźnioną realizację prawa dostępu**.

- **Czego dotyczyła sprawa (w skrócie):**
  - Spółka przekazywała dane osoby wnioskującej o kredyt konsumencki do podmiotu utrzymującego platformę wymiany informacji (w tym dane używane do oceny zdolności kredytowej, także objęte **tajemnicą bankową**).
  - Spółka powoływała się na **zgody** udzielane przy wnioskach kredytowych oraz na **umowę powierzenia** z tym podmiotem.
  - Osobny wątek: wysłano **e-mail marketingowy** do osoby, która wcześniej **wycofała zgody marketingowe** i zgłosiła **sprzeciw wobec marketingu**.
  - Trzeci wątek: realizacja **prawa dostępu** – pierwsza odpowiedź była **niepełna** (pominięto m.in. informację o obywatelstwie), a dodatkowe informacje przekazano **po terminie**.

- **Najważniejsze wnioski z wyroku:**
  - **Umowa powierzenia nie legalizuje dostępu do tajemnicy bankowej:** nawet jeśli spółka ma umowę z procesorem, to **nie może przekazać danych objętych tajemnicą bankową** do podmiotu, który **nie jest wymieniony** w katalogu uprawnionych podmiotów z **art. 105 ust. 4 Prawa bankowego**.
  - **Zgoda nie działa „na wszystkich":** zgoda pożyczkobiorcy mogła uprawniać do pozyskania/udostępnienia informacji w relacji z instytucjami wskazanymi w ustawie, ale **nie była podstawą do przekazania tych danych dowolnemu podmiotowi** spoza ustawowego katalogu.
  - **Relacja RODO do przepisów sektorowych:** art. 28 RODO określa zasady powierzenia, ale **nie znosi szczególnych ograniczeń** wynikających np. z tajemnicy bankowej. Jeśli przepisy branżowe nie dają podmiotowi uprawnienia do przetwarzania takich danych, to **sama umowa powierzenia nie tworzy takiego uprawnienia**.
  - **Błąd systemu nie zwalnia z odpowiedzialności:** wysłanie marketingu do osoby po **wycofaniu zgód** i zgłoszeniu **sprzeciwu** jest **przetwarzaniem bez podstawy prawnej**. Tłumaczenie, że to „wina systemu", nie eliminuje naruszenia – administrator ma obowiązek tak skonfigurować narzędzia, aby do tego nie dochodziło (odpowiedzialność za środki techniczne i organizacyjne).
  - **Prawo dostępu = kompletna informacja:** przekazana „kopia danych" i odpowiedź na żądanie z art. 15 RODO muszą być **pełne**. Pominięcie części danych faktycznie przetwarzanych (np. obywatelstwa) może **wprowadzać w błąd** co do skali przetwarzania i utrudniać korzystanie z dalszych praw.
  - **Liczy się termin i formalne przedłużenie:** jeśli administrator **uzupełnia odpowiedź dopiero po miesiącu** i nie poinformował w terminie o skorzystaniu z przedłużenia, narusza **art. 12 ust. 3 RODO**. Późniejsze dosłanie informacji traktowane jest jako uzupełnienie wcześniejszej, niepełnej odpowiedzi – nie „naprawia" uchybienia terminowi.

- **Znaczenie praktyczne (dla nie-ekspertów):**
  - Nie każdą operację na danych da się „zalegalizować" umową z podwykonawcą – przy danych wrażliwych sektorowo (np. bankowych) decydują też **przepisy szczególne**.
  - Marketing po cofnięciu zgody/sprzeciwie to naruszenie, nawet jeśli „system się pomylił" – firma odpowiada za to, jak działa jej automatyzacja.
  - Osoba pytająca o swoje dane ma dostać **pełną** odpowiedź **na czas**, a jeśli potrzeba więcej czasu – firma musi to formalnie i terminowo zakomunikować.

Źródło: https://judykatura.pl/wsa-w-warszawie-tajemnicy-bankowej-nie-powierza-sie-dowolnie/

Austriacki Sąd Federalny uznał, że żądanie danych dla zwrotu opłat jest nadmierne

- **Kontekst:** Artykuł omawia wyrok austriackiego Federalnego Sądu Administracyjnego, który pokazuje **granice prawa dostępu do danych z art. 15 RODO**, zwłaszcza gdy wniosek ma w praktyce służyć **zdobyciu materiału do roszczeń cywilnych** (np. o zwrot opłat), a nie sprawdzeniu, jak przetwarzane są dane.

- **Czego dotyczyła sprawa:** Połączono **42 skargi**. Wnioski o dostęp do danych złożył **adwokat** w imieniu osób fizycznych wobec operatora telekomunikacyjnego. Żądania obejmowały m.in. **dane rozliczeniowe** oraz informacje o **pobranych opłatach serwisowych**.
- **Co zrobił operator:** Nie udzielił odpowiedzi na wnioski, domagał się **odrębnych pełnomocnictw** i twierdził, że celem wniosków jest uzyskanie danych do **procesów cywilnych o zwrot opłat**.
- **Co ustalono co do osób:** Sąd rozdzielił sytuację **31 obecnych/byłych klientów** operatora oraz **11 osób, które nigdy nie były jego klientami**.

- **Teza 1 – pełnomocnictwo i tożsamość:** Administrator **nie może rutynowo** żądać dowodu tożsamości lub umocowania (np. pełnomocnictwa) już na etapie złożenia wniosku. Może prosić o dodatkowe informacje **tylko gdy ma uzasadnione wątpliwości** co do tożsamości osoby składającej żądanie.
- **W tej sprawie:** Do wniosków dołączono **dokumenty tożsamości** osób, których dane dotyczyły, więc sąd uznał, że operator **nie miał podstaw**, by blokować wnioski wyłącznie z powodu braku osobnego dokumentu pełnomocnictwa.

- **Teza 2 – odpowiedź negatywna dla nieklienta:** Prawo dostępu obejmuje też prawo do informacji, **czy administrator w ogóle przetwarza dane danej osoby**. Jeśli nie przetwarza, powinien udzielić **odpowiedzi negatywnej**.
- **W tej sprawie (11 nieklientów):** Operator nadal miał obowiązek zareagować i przekazać informację, czy dane są przetwarzane (a jeśli nie – odpowiedź negatywną). Nie mógł odmówić odpowiedzi tylko dlatego, że „zakłada", iż ktoś nie był klientem.

- **Teza 3 – kiedy pierwszy wniosek może być „nadmierny":** Sąd wskazał, że **nawet pierwszy wniosek** o dostęp może wyjątkowo zostać uznany za **nadmierny** (art. 12 ust. 5 RODO), ale administrator musi to **dobrze udowodnić**.
- **Wymagany wysoki próg dowodowy:** Administrator powinien wykazać jednocześnie:
  - **obiektywnie** – że cel prawa dostępu (uzyskanie wiedzy o przetwarzaniu danych i możliwość kontroli zgodności z prawem) nie jest w praktyce realizowany, oraz
  - **subiektywnie** – że wnioskodawca działa z **zamiarem nadużycia** (uzyskania korzyści sztucznie powiązanej z regulacją).

- **Podstawa podejścia sądu:** Sąd powołał się na najnowszy standard wynikający z orzecznictwa TSUE (w artykule wskazano wyrok z **19 marca 2026 r., C-526/24**).

- **Teza 4 – wyłącznie cywilny cel jako nadużycie (w konkretnych okolicznościach):** Wnioski **31 klientów** uznano za nadmierne/nadużywające, ponieważ sąd ustalił, że miały one **wyłącznie** na celu uzyskanie danych o opłatach potrzebnych do **dochodzenia roszczeń cywilnych**, a nie kontrolę przetwarzania danych.
- **Na czym oparto ustalenia:** Sąd brał pod uwagę m.in. **treść żądań**, materiały publikowane przez kancelarię i podmiot współpracujący oraz **liczne podobne postępowania**.

- **Co sąd przesądził w praktyce:**
  - Wobec **31 klientów** sąd **uchylił** ustalenie naruszenia prawa dostępu oraz **nakaz udzielenia informacji** (uznając wnioski za nadmierne/nadużywające w tych realiach).
  - Wobec **11 nieklientów** utrzymał obowiązek udzielenia **odpowiedzi negatywnej**, jeżeli operator ich danych nie przetwarza.

- **Co pozostaje otwarte:** Sąd **nie stwierdził**, że cel cywilny **zawsze** wyklucza ochronę z art. 15 RODO. Wskazał, że dopiero **wyłącznie cywilny** cel, potwierdzony dowodami w konkretnej sprawie, może oznaczać nadużycie.
- **Dalszy bieg sprawy:** Wyrok jest z **2 października 2026 r.** i dopuszcza wniesienie rewizji; sąd zauważył też, że w austriackim orzecznictwie administracyjnym pozostają sporne pytania m.in. o zakres obowiązku udzielania odpowiedzi negatywnej i odmowę realizacji żądania przy motywach niezwiązanych z ochroną danych.

Źródło: https://judykatura.pl/austriacki-sad-federalny-uznal-ze-zadanie-danych-dla-zwrotu-oplat-jest-nadmierne/

Uwagi Prezesa UODO do projektu zmian w Prawie oświatowym

- **Kontekst:** Poselski projekt nowelizacji przepisów oświatowych dotyczący szkolnych e-dzienników jest nieprecyzyjny i wymaga doprecyzowania. W obecnym kształcie nie rozstrzyga kluczowych kwestii i nie tworzy kompleksowych ram prawnych, szczególnie w obszarze ochrony danych i cyberbezpieczeństwa cyfrowej dokumentacji szkolnej.
- **Stanowisko UODO:** Prezes Urzędu Ochrony Danych Osobowych (UODO) Mirosław Wróblewski przekazał uwagi do projektu na ręce Dariusza Salomończyka (zastępcy Szefa Kancelarii Sejmu RP).
- **Co obejmuje projekt:** Proponowane zmiany dotyczą głównie **nieodpłatnego zapewnienia uczniom i rodzicom** dostępu do cyfrowej dokumentacji szkolnej (w tym e-dzienników).
- **Brak kompleksowości:** UODO wskazuje, że projekt w praktyce **utrzymuje obecny model**, w którym komercyjne firmy są dostawcami systemów cyfrowej dokumentacji szkolnej, bez stworzenia pełnych, spójnych zasad działania całego systemu.
- **Ochrona danych osobowych – podejście fragmentaryczne:** Zdaniem organu nadzorczego regulacje dotyczące ochrony danych w e-dokumentacji są **niepełne** i nie odpowiadają na wszystkie ryzyka związane z przetwarzaniem danych.
- **Potrzeba oceny skutków regulacji:** UODO podkreśla, że zmiany wpływające na przetwarzanie danych w cyfrowej dokumentacji szkolnej powinny być poprzedzone **oceną skutków regulacji** (w tym „testem prywatności"), aby system był spójny i zgodny z zasadami przetwarzania danych osobowych.
- **Podstawa prawna przetwarzania danych:** W ustawach dotyczących edukacji muszą być jasno spełnione i umocowane **dwie przesłanki jednocześnie**:
  - przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
  - przetwarzanie jest niezbędne do wykonania zadania w interesie publicznym lub w ramach sprawowania władzy publicznej.

  Obie powinny wynikać z przepisów, zwłaszcza z **Prawa oświatowego**.
- **Cyberbezpieczeństwo jako kluczowe wyzwanie:** Skala przetwarzania danych w e-dokumentacji szkolnej w całym kraju oznacza wysoką wagę bezpieczeństwa. UODO wskazuje, że regulacje należy projektować także pod kątem realnych cyberzagrożeń.
- **Proponowane kierunki wzmocnienia bezpieczeństwa:** Dla dużych platform obsługujących szkoły warto rozważyć:
  - wprowadzenie **standardów bezpieczeństwa IT** dla systemów teleinformatycznych,
  - ustanowienie **systemu certyfikacji** platform, gdzie gwarantem wiarygodności byłyby podmioty publiczne.

- **Rekomendacje dot. certyfikacji i nadzoru:** Należy rozważyć:
  - nałożenie na podmioty przetwarzające danych obowiązku uzyskania **dodatkowej certyfikacji**,
  - przyznanie właściwemu ministrowi kompetencji do prowadzenia **publicznej bazy podmiotów certyfikowanych**.

- **Wniosek ogólny:** Rozwiązania dotyczące e-dzienników i cyfrowej dokumentacji szkolnej powinny zostać zaprojektowane jako **spójny, kompleksowy system**, obejmujący jednocześnie kwestie prawne, ochronę danych osobowych oraz cyberbezpieczeństwo.

Źródło: https://uodo.gov.pl/pl/138/4640

Mniej zgłoszeń naruszeń, więcej danych dla AI. Gdzie Rada UE stawia granice?

- **Kontekst:** Unia Europejska chce zwiększyć konkurencyjność firm i uprościć przepisy dotyczące ochrony danych osobowych, prywatności i cyberbezpieczeństwa, aby ułatwić rozwój nowych technologii (w tym sztucznej inteligencji).
- Rada UE uzgodniła swoje stanowisko w sprawie pakietu **Digital Omnibus**, którego celem jest **ograniczenie obowiązków przedsiębiorstw** i zmniejszenie obciążeń regulacyjnych.
- Rada UE **odrzuciła** propozycję zmiany **definicji danych osobowych** w RODO.
- Jednocześnie Rada chce **zmienić niektóre zasady dotyczące danych pseudonimizowanych** (czyli takich, które są „ukryte"/przetworzone w sposób utrudniający identyfikację osoby, ale nie wykluczający jej całkowicie).
- Proponowane zmiany w zgłaszaniu naruszeń danych:
  - obowiązek zgłoszenia miałby dotyczyć **tylko przypadków wysokiego ryzyka** dla osób, których dane dotyczą,
  - **termin zgłaszania naruszeń** miałby zostać **wydłużony**.

- Uproszczone mają być także zasady **zgłaszania cyberataków**, co ma zmniejszyć biurokrację po stronie firm.
- Zmiany obejmują również **trenowanie modeli AI**:
  - w określonych sytuacjach **dane osobowe mogłyby być użyte** do trenowania bez konieczności uzyskania zgody **od każdej osoby**,
  - przewidziano **dodatkowe zabezpieczenia** dotyczące **danych wrażliwych**, jeśli znalazłyby się w zbiorach treningowych.

- **Co dalej:** to jeszcze nie są ostateczne przepisy — końcowy kształt zmian będzie przedmiotem **negocjacji w Parlamencie Europejskim**.

Źródło: https://edgp.gazetaprawna.pl/prawo/prawo-internetu-i-ochrony-danych/artykuly/11336322,mniej-zgloszen-naruszen-wiecej-danych-dla-ai-gdzie-rada-ue-stawia-gr.html

Pozyskiwanie zgody na przetwarzanie danych o zdrowiu - wyrok NSA potwierdzający decyzję Prezesa UODO

- **Kontekst sprawy:** wspólnicy spółki cywilnej przetwarzali dane osobowe potencjalnych klientów (w tym **dane o zdrowiu**), twierdząc, że uzyskali **ustną zgodę** jeszcze przed zawarciem umowy. Nie przedstawili jednak dowodów, że klienci rzeczywiście **żądali podjęcia działań** przed podpisaniem umowy.
- **Finał przed sądami: 6 października 2026 r.** NSA oddalił skargę kasacyjną wspólników Kancelarii Pionier, utrzymując wyrok WSA w Warszawie i decyzję Prezesa UODO o karze **45 697 zł**.
- **Jak zaczęła się sprawa:** Prezes UODO wszczął postępowanie po wniosku Komendanta Powiatowego Policji o przeprowadzenie czynności kontrolnych wobec wskazanych administratorów danych.
- **Brak współpracy z UODO:** wspólnicy zwlekali z odpowiedziami na wezwania organu albo przekazywali **niepełne wyjaśnienia**, co doprowadziło do decyzji o kontroli w przedsiębiorstwie.
- **Ustalenia kontroli – skąd brano dane:** dane potencjalnych klientów pozyskiwano m.in. z **internetu**, **mediów społecznościowych** oraz z **wywiadu środowiskowego**.
- **Zakres zbieranych informacji:** po nawiązaniu wstępnej relacji ponownie kontaktowano się z klientami i zbierano **dodatkowe informacje, w tym o stanie zdrowia** (dane wrażliwe).
- **Co z danymi, gdy nie było umowy:** jeśli nie doszło do zawarcia umowy, dane przechowywano zwykle **3–5 dni**.
- **To nie był „marketing bezpośredni”:** Prezes UODO nie uznał tej praktyki za marketing bezpośredni w rozumieniu motywu 47 RODO.
- **Decyzja Prezesa UODO:** organ stwierdził przetwarzanie **bez podstawy prawnej**, nakazał zaprzestanie takiego przetwarzania oraz nałożył **karę pieniężną**.
- **Argumenty wspólników w skardze:** twierdzili m.in., że skoro klienci przekazywali dane, to „gdyby nie chcieli umowy, to by tego nie zrobili”, oraz że sam kontakt potencjalnego klienta był równoznaczny ze zgodą.
- **Stanowisko WSA:** sąd uznał, że przetwarzanie danych potencjalnych klientów:
  - nie było **niezbędne** do wykonania umowy ani do działań na żądanie osoby przed zawarciem umowy,
  - służyło głównie ocenie **opłacalności** i „upewnieniu się”, czy dojdzie do umowy,
  - było **nieproporcjonalne** i nie było konieczne, zwłaszcza że dotyczyło **danych o zdrowiu**.

- **Ustna zgoda – ważna, ale trzeba ją udowodnić:** WSA wskazał, że ustna zgoda może być wystarczająca (zwłaszcza dla danych zwykłych), ale w praktyce powinna iść za nią możliwość wykazania jej udzielenia (np. rejestr zgód/rozmów). W tej sprawie brakowało podstawy prawnej w RODO.
- **Kluczowe stanowisko NSA:** RODO nie wymaga, by zgoda była pisemna ani by rozmowa była nagrana, ale administrator musi **być w stanie wykazać**, że zgoda została udzielona (art. 7 ust. 1 RODO) – to element zasady **rozliczalności**.
- **Dlaczego „praktyka pytania o zgodę” nie wystarczyła:** NSA uznał, że ogólne deklaracje pracowników nie pozwalały ustalić:
  - kto konkretnie wyraził zgodę,
  - kiedy i w jakich okolicznościach,
  - jakie informacje przekazano osobie,
  - jaki był dokładny **zakres zgody**, w tym czy wyraźnie obejmowała **dane o zdrowiu** i ponowny kontakt.

- **Brak sprzeciwu to nie zgoda:** NSA podkreślił, że **zgoda** i **sprzeciw** to różne instytucje. Milczenie, brak skargi czy brak sprzeciwu **nie oznaczają** świadomego, aktywnego przyzwolenia wymaganego przez RODO.
- **Zainteresowanie usługą nie dowodzi zgody:** samo zainicjowanie rozmowy lub przekazanie dokumentów medycznych może świadczyć o zainteresowaniu, ale **nie potwierdza** jeszcze wyraźnej zgody na konkretny cel, zakres i czas przetwarzania danych.
- **Najważniejszy wniosek praktyczny:** jeśli firma przetwarza dane (szczególnie **wrażliwe**, jak dane o zdrowiu) na podstawie zgody, musi mieć realne możliwości **udowodnienia**, że zgoda była świadoma, konkretna i wyraźna – a ciężaru tego nie da się przerzucić na UODO ani na klientów.

Źródło: https://uodo.gov.pl/pl/138/4645

825 mln euro kary dla Ubera za algorytmy

- **Kontekst sprawy:** Holenderski organ ochrony danych (Autoriteit Persoonsgegevens) nałożył na Ubera karę **825 mln euro** za praktykę, w której **konta kierowców były automatycznie dezaktywowane** (czasowo lub na stałe) na podstawie podejrzeń oszustwa lub niskich ocen. Dla kierowców oznaczało to często **natychmiastową utratę możliwości zarobkowania**. Sprawa pokazuje, że „człowiek na etapie reklamacji" nie zawsze daje realny nadzór nad decyzjami algorytmu.
- **Co uznano za problem:** nie sama automatyzacja, ale **oddanie systemowi decyzji**, która może w jednej chwili pozbawić człowieka źródła dochodu, bez wcześniejszej, rzeczywistej oceny przez człowieka i bez jasnej informacji dla zainteresowanych.
- **Jak działał mechanizm (wg organu):** system monitorował zachowania kierowców, analizował sygnały ryzyka oszustwa oraz oceny klientów; po przekroczeniu progów konto mogło zostać **zablokowane**, a przy dłużej utrzymujących się niskich ocenach – **wyłączone na stałe**.
- **Skutek dla kierowcy:** dezaktywacja to nie „techniczna niedostępność", lecz realne konsekwencje życiowe: **brak zleceń i dochodu**, potencjalne problemy finansowe nawet przy krótkiej blokadzie oraz możliwy wpływ na reputację i pozycję w sporze z platformą.
- **Skąd wzięło się postępowanie:** ruszyło po skargach **171 francuskich kierowców**. Sprawę prowadził regulator holenderski, bo europejska siedziba Ubera jest w Niderlandach (mechanizm **one-stop-shop** w RODO). Badany okres: **2018–2022**.
- **Stanowisko Ubera:** firma zaprzestała kwestionowanych naruszeń, ale **nie zgodziła się z decyzją** i zapowiedziała zaskarżenie.
- **Klucz prawny: art. 22 RODO:** co do zasady **zakazane** są decyzje wobec osoby oparte **wyłącznie** na automatycznym przetwarzaniu (w tym profilowaniu), jeśli wywołują skutki prawne lub **podobnie istotnie wpływają** na osobę.
- **Ważne doprecyzowanie po wyroku TSUE (SCHUFA, C-634/21):** art. 22 RODO to **zakaz co do zasady**, a nie tylko „prawo, z którego trzeba skorzystać". To organizacja ma wcześniej ocenić, czy jej proces nie narusza zakazu – niezależnie od tego, czy ktoś zdążył zaprotestować.
- **Kiedy art. 22 ma zastosowanie:** muszą wystąpić łącznie:
  - jest **decyzja dotycząca konkretnej osoby**,
  - jest oparta **wyłącznie** na automatycznym przetwarzaniu,
  - powoduje **istotny wpływ** (np. utratę możliwości pracy/zarobku).

- **Nie da się „uciec" w nazewnictwo:** liczy się rzeczywisty przebieg procesu. Jeśli wynik systemu automatycznie uruchamia blokadę konta, trudno twierdzić, że decyzję podjął człowiek.
- **Algorytm wspiera vs. algorytm decyduje:** samo generowanie alertów (np. o nietypowych trasach) może być dopuszczalne. Problem zaczyna się, gdy alert **automatycznie** wywołuje skutek albo „zatwierdzający" pracownik nie ma czasu, danych lub uprawnień, by realnie wynik podważyć (nadzór „dekoracyjny").
- **Odwołanie nie zawsze ratuje sytuację:** formularz reklamacyjny nie jest „dodatkowym wyjątkiem" od zakazu. Najpierw musi istnieć podstawa legalizująca automatyczną decyzję, a dopiero potem działają gwarancje (np. interwencja człowieka). Przy odcięciu od dochodu liczy się też **czas** – odpowiedź po tygodniach może nie być skuteczną ochroną.
- **Wyjątki od zakazu (art. 22 ust. 2 RODO):** automatyczna decyzja może być dopuszczalna tylko w określonych sytuacjach (np. niezbędna do wykonania umowy, dopuszczona prawem, oparta na wyraźnej zgodzie). Te wyjątki trzeba interpretować **ściśle** – wygoda, szybkość czy niższy koszt nie wystarczą.
- **Jakość danych to realne ryzyko:** oceny klientów i sygnały „podejrzenia oszustwa" mogą być mylące (np. uprzedzenia, błąd aplikacji, legalna nietypowa trasa). RODO wymaga dbania o **prawidłowość i aktualność danych** oraz sensownego informowania o tym, jak działa automatyczne podejmowanie decyzji i jakie ma konsekwencje (bez konieczności ujawniania kodu, ale z możliwością zrozumienia i zakwestionowania decyzji).
- **Nowe przepisy dla pracy platformowej (dyrektywa 2024/2831):** państwa UE mają wdrożyć ją do **2 grudnia 2026 r.** Wzmacnia ochronę osób pracujących przez aplikacje (nie tylko etatowców) i wymaga większej przejrzystości algorytmów.
- **Najmocniejsza zasada z dyrektywy:** decyzje o **ograniczeniu, zawieszeniu lub zakończeniu** relacji/ konta (albo równoważnej szkodzie) mają być **podejmowane przez człowieka** – nie tylko „do zaskarżenia po fakcie". Uzasadnienie ma być przekazane szybko, najpóźniej w dniu wejścia decyzji w życie.
- **AI Act (akt o sztucznej inteligencji):** nie każdy „algorytm" to AI w rozumieniu AI Act. Jeśli jednak system AI służy decyzjom dotyczącym pracy/dochodu, może być uznany za **wysokiego ryzyka**, co oznacza dodatkowe obowiązki (m.in. zarządzanie ryzykiem, jakość danych, dokumentacja, rejestrowanie zdarzeń, realny nadzór człowieka). Te wymogi dla części systemów zaczną mieć zastosowanie od **2 grudnia 2027 r.**
- **Wniosek praktyczny dla firm:** potrzeba zaprojektować proces tak, by człowiek był **przed** momentem powstania szkody (np. blokady konta), miał dostęp do danych i uzasadnienia, realne uprawnienia do zmiany wyniku oraz czas i zasoby na indywidualną ocenę.
- **Najważniejsza konkluzja:** automatyzacja może pomagać wykrywać ryzyka i porządkować sprawy, ale organizacja nie może przerzucać na system odpowiedzialności za decyzje, które **odcinają człowieka od pracy i dochodu**. Im poważniejsze skutki, tym mniej wystarczające jest stwierdzenie: „zawsze można się odwołać".

Źródło: https://edgp.gazetaprawna.pl/prawo/prawo-internetu-i-ochrony-danych/artykuly/11337941,825-mln-euro-kary-dla-ubera-za-algorytmy.html