RODO Aktualności

Data publikacji: 13.10.2026

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. Irlandzki organ ochrony danych nałożył 645 000 euro kary na służbę zdrowia
2. Wyciek danych klientów Wakacje.pl. Wyciekły w szczególności dane paszportowe
3. Kara pieniężna nałożona za niewykonanie decyzji Prezesa UODO
4. Włoski organ ochrony danych nałożył 7 mln euro kary na firmę analizującą dane zdrowotne
5. Fakturownia ujawniła, jak doszło do wycieku danych. Incydent dotyczy każdego konta
6. WSA w Łodzi: przedawnienie opłaty nie wydłuża retencji danych
7. Nie każde naruszenie ochrony danych wymaga zgłoszenia do Prezesa UODO
8. NSA: 1,97 mln zł kary za brak regularnych testów bezpieczeństwa
9. Rekordowo niski odsetek uwzględniania skarg na decyzje Prezesa UODO
10. WSA w Warszawie: wcześniejsza wiedza nie legalizuje ujawnienia danych

Irlandzki organ ochrony danych nałożył 645 000 euro kary na służbę zdrowia

- **Kontekst:** artykuł opisuje decyzję irlandzkiego organu ochrony danych (Data Protection Commission) dotyczącą **ochrony papierowej dokumentacji medycznej** przechowywanej poza placówkami publicznej służby zdrowia. Organ uznał, że złe warunki składowania akt naruszały wymogi RODO.
- **Główne ustalenie:** obowiązki z RODO (m.in. art. 5 i 32) dotyczą nie tylko systemów IT, ale także **archiwów papierowych** – trzeba zapewnić ich integralność, poufność i dostępność.
- **Czego dotyczyła sprawa:** postępowanie wszczęto po zgłoszeniach i materiałach (m.in. nagraniach w mediach społecznościowych) wskazujących na ryzyko nieuprawnionego dostępu do akt medycznych przechowywanych w **dawnych, nieużytkowanych szpitalach psychiatrycznych**.
- **Skala i weryfikacja problemu:** organ przeprowadził **12 inspekcji** w różnych częściach kraju, aby sprawdzić, czy problem ma charakter incydentalny, czy systemowy.
- **Co wykryto w praktyce:** dokumenty były m.in. **zniszczone przez pleśń**, zabrudzone (np. odchodami zwierząt), zasypane gruzem, gnijące lub uszkodzone przez wodę; akta przechowywano też w miejscach skrajnie nieadekwatnych (np. **nieużywane łazienki**, kontener transportowy, pomieszczenia bez ogrzewania/oświetlenia, opuszczone budynki).
- **Teza 1 – bezpieczeństwo papierowej dokumentacji:** przy przechowywaniu w obiektach zewnętrznych administrator musi wdrożyć **adekwatne do ryzyka środki techniczne i organizacyjne** oraz procesy i kontrole zarządzania dokumentacją; ich brak narusza zasadę integralności i poufności oraz **art. 32 ust. 1 RODO**.
- **Dlaczego to ważne:** brak uporządkowanego systemu **lokalizowania i śledzenia akt** zwiększa ryzyko dostępu osób nieuprawnionych i utrudnia zapewnienie dostępności dokumentacji (np. na potrzeby leczenia, wymogów prawnych lub regulacyjnych).
- **Teza 2 – ograniczenie okresu przechowywania:** dane nie mogą być przechowywane w formie pozwalającej identyfikować osoby **dłużej, niż jest to niezbędne**; przechowywanie „na wszelki wypadek" narusza zasadę ograniczenia przechowywania (**art. 5 ust. 1 lit. e RODO**).
- **Wniosek organu:** przechowywanie dokumentacji w niezabezpieczony sposób po okresie, gdy powinna zostać usunięta, powoduje **ciągłe, istotne ryzyko** ujawnienia wrażliwych informacji medycznych osobom trzecim.
- **Teza 3 – obowiązki po naruszeniu:** naruszenia należy zgłaszać **bez zbędnej zwłoki**, w miarę możliwości w ciągu **72 godzin** od stwierdzenia (art. 33), a w określonych sytuacjach trzeba także **powiadomić osoby, których dane dotyczą** (art. 34).
- **Co zakwestionowano w zgłoszeniach:** część naruszeń nie została zgłoszona w terminie (St. Loman's Hospital), a część osób nie została powiadomiona o naruszeniu (St. Loman's Hospital i St. Conal's Hospital).
- **Teza 4 – audyt i naprawa zabezpieczeń:** doprowadzenie zgodności może wymagać m.in. **pełnego audytu** wszystkich lokalizacji, wdrożenia **systemu rejestrowania i śledzenia dokumentów**, **bezpiecznego i szybkiego niszczenia** akt zbędnych oraz **przeniesienia** dokumentacji z miejsc nieodpowiednich.
- **Środki naprawcze:** oprócz uporządkowania zasobów HSE ma też **regularnie testować, oceniać i weryfikować** zgodność z własnymi zasadami retencji (przechowywania).
- **Decyzja i sankcje:** organ stwierdził naruszenia przez irlandzką publiczną służbę zdrowia (Health Service Executive) i nałożył łączną karę **645 000 euro** oraz zastosował upomnienie i szerokie środki naprawcze.
- **Rozbicie kar:**
  - 300 000 euro – za naruszenia związane z bezpieczeństwem (art. 5 ust. 1 lit. f i art. 32 ust. 1 RODO),
  - 300 000 euro – za naruszenie zasady ograniczenia przechowywania (art. 5 ust. 1 lit. e),
  - 30 000 euro – za naruszenia obowiązku zgłoszenia (art. 33 ust. 1),
  - 15 000 euro – za naruszenie obowiązku powiadomienia osób (art. 34 ust. 1).

- **Okoliczność obciążająca:** przy wymiarze kary uwzględniono **wcześniejsze podobne naruszenia** dotyczące braku odpowiednich zabezpieczeń i utraty kontroli nad danymi w papierowej dokumentacji medycznej.
- **Status publikacji:** pełna decyzja ma zostać opublikowana w późniejszym terminie (zgodnie z komunikatem organu).

Źródło: https://judykatura.pl/irlandzki-organ-ochrony-danych-nalozyl-645-000-euro-kary-na-sluzbe-zdrowia/

Wyciek danych klientów Wakacje.pl. Wyciekły w szczególności dane paszportowe

- **Kontekst:** doszło do włamania do Wakacje.pl. Osoby nieuprawnione mogły uzyskać dostęp m.in. do danych paszportowych klientów. Firma ostrzega przed możliwymi próbami wyłudzeń i apeluje o czujność.
- **Co się stało:** Wakacje.pl poinformowały o incydencie bezpieczeństwa, w którym napastnicy uzyskali dostęp do części firmowych skrzynek e-mail oraz systemu wykorzystywanego do obsługi klientów.
- **Kiedy:** do włamania doszło **29 września**.
- **Jakie dane mogły zostać pozyskane (potencjalnie):** adresy e-mail, imiona i nazwiska, numery telefonów, adresy zamieszkania, daty urodzenia oraz **dane paszportowe**.
- **Co firma podkreśla:** przejęte informacje **nie umożliwiają logowania** do Panelu Klienta (ani przez stronę, ani aplikację).
- **Płatności:** według firmy incydent **nie dotyczył systemów płatności** Wakacje.pl.
- **Ryzyko dla klientów:** możliwe są próby **oszustw i wyłudzeń** (np. prośby o dopłatę, zmiany danych rezerwacji) z wykorzystaniem pozyskanych informacji i podszywanie się pod Wakacje.pl.
- **Zalecenia dla klientów:** zachować ostrożność wobec wiadomości dotyczących płatności lub zmian w rezerwacji oraz **weryfikować je u swojego doradcy**.
- **Działania Wakacje.pl po wykryciu incydentu:** wdrożono dodatkowe procedury bezpieczeństwa i uruchomiono wzmożone monitorowanie ruchu w systemach.
- **Zgłoszenia i instytucje:** o sprawie poinformowano **CSIRT NASK** oraz **Urząd Ochrony Danych Osobowych**; zapowiedziano także zgłoszenie do organów ścigania.
- **Dodatkowa rekomendacja:** jeśli potwierdzi się, że dane danej osoby znalazły się wśród przejętych informacji, jednym z pierwszych działań powinno być **zastrzeżenie numeru PESEL**.

Źródło: https://polskieradio24.pl/polska/wyciek-danych-klientow-wakacjepl-firma-wydala-pilne-ostrzezenie

Kara pieniężna nałożona za niewykonanie decyzji Prezesa UODO

- **Kontekst:** Niewykonanie obowiązku nałożonego decyzją Prezesa UODO może skutkować wszczęciem postępowania egzekucyjnego oraz nałożeniem administracyjnej kary pieniężnej. W opisanym przypadku kara wyniosła **29 112 zł**.
- **Czego dotyczyła sprawa:** W 2025 r. Prezes UODO (Mirosław Wróblewski) nakazał warszawskiej spółce **Costalea** spełnienie **obowiązku informacyjnego** wobec osoby skarżącej (czyli przekazanie wymaganych informacji związanych z przetwarzaniem jej danych).
- **Doręczenie decyzji:** Decyzję wysłano na adres siedziby spółki widniejący w **KRS**. Po **dwukrotnej awizacji** przesyłka została zwrócona do UODO.
- **Brak reakcji administratora:** Administrator nie odpowiadał na korespondencję, dlatego UODO sprawdził, czy obowiązek został wykonany i wezwał spółkę do złożenia wyjaśnień oraz przedstawienia dowodów wykonania decyzji.
- **Ustalenia organu:** Ponieważ spółka nadal nie reagowała, a osoba skarżąca oświadczyła, że nie otrzymała wymaganych informacji, Prezes UODO uznał, że **decyzja nie została wykonana**.
- **Upomnienie jako krok do egzekucji:** UODO wysłał **upomnienie** (pismo wymagane przed wszczęciem egzekucji administracyjnej), dając spółce ostatnią szansę na dobrowolne wykonanie obowiązku. Także na to pismo nie było odpowiedzi.
- **Możliwe konsekwencje prawne:** Poza środkami egzekucyjnymi z ustawy o postępowaniu egzekucyjnym w administracji, Prezes UODO może nałożyć karę pieniężną na podstawie **RODO** za niewykonanie decyzji organu nadzorczego.
- **Skala potencjalnych kar w RODO:** Za niewykonanie decyzji organu nadzorczego kara może wynosić do **20 mln euro**, a w przypadku przedsiębiorstwa także do **4% rocznego światowego obrotu** (jeśli to kwota wyższa).
- **Dlaczego nałożono karę i jak ją ustalono:** W tej sprawie Prezes UODO nałożył karę finansową, uwzględniając wyniki finansowe spółki za ostatni rok obrotowy, aby kara była **proporcjonalna**, **odstraszająca** i **skuteczna** (ma skłonić do wykonania obowiązku).
- **Ważne zastrzeżenie:** Zapłata kary **nie zwalnia** administratora z obowiązku wykonania decyzji. UODO nadal będzie dążył do tego, aby spółka spełniła obowiązek informacyjny wobec skarżącej.
- **Sygnatura sprawy:** DKE.561.3.2026

Źródło: https://uodo.gov.pl/pl/138/4594

Włoski organ ochrony danych nałożył 7 mln euro kary na firmę analizującą dane zdrowotne

- **Kontekst:** Decyzja włoskiego organu ochrony danych (Garante) dotyczy budowy dużej bazy danych zdrowotnych. Organ pokazał, że samo deklarowanie „anonimizacji” nie zwalnia z odpowiedzialności za cały proces przetwarzania, jeśli w praktyce dane można (choćby pośrednio) powiązać z pacjentami.
- **Czego dotyczyła sprawa:** Dane pacjentów ok. 800 lekarzy POZ były przekazywane (przez dodatek do programu gabinetowego) do bazy LPD należącej do IQVIA. Baza obejmowała m.in. diagnozy, recepty, badania, wizyty i inne elementy historii zdrowotnej.
- **Stanowisko spółki a ustalenia organu:** IQVIA twierdziła, że otrzymuje wyłącznie dane anonimowe (usunięte identyfikatory, ograniczone informacje, stały identyfikator Pat ID) i nie ma dostępu do komputerów lekarzy ani „klucza” do ustalenia tożsamości pacjentów. Organ uznał jednak, że zastosowane rozwiązania nie dawały skutecznej anonimizacji.
- **Kluczowe ustalenie – kto był administratorem:** Garante uznał IQVIA za administratora całego procesu (od etapu zbierania danych), bo spółka miała realny wpływ na cele i środki przetwarzania: była właścicielem bazy, wykorzystywała dane biznesowo, zawierała umowy z lekarzami i dostawcą oprogramowania oraz wydawała instrukcje dot. „anonimizacji”. Nazwa roli w umowie nie przesądza o odpowiedzialności.
- **Pseudonimizacja to nie anonimizacja:** Dane pseudonimizowane nadal są danymi osobowymi i podlegają RODO. Pseudonimizacja tylko utrudnia przypisanie danych do osoby, ale nie eliminuje tego ryzyka.
- **Dlaczego k-anonimowość nie wystarczyła:** Organ wskazał, że ocenianie k-anonimowości tylko dla tzw. quasi-identyfikatorów to za mało. W praktyce inne elementy rekordu (np. diagnozy, sekwencje hospitalizacji, wzorce lekowe), zwłaszcza obserwowane w czasie, mogą „wyróżniać” pacjenta i umożliwiać jego wyodrębnienie.
- **Stały identyfikator (Pat ID) zwiększa ryzyka:** Pozwala śledzić historię pacjenta w czasie, co w połączeniu z bogatymi danymi medycznymi może ułatwiać identyfikację, nawet jeśli usunięto dane typu imię i nazwisko.
- **„Anonimizacja” też wymaga podstawy prawnej:** Organ podkreślił, że samo przekształcanie danych osobowych w kierunku anonimizacji jest operacją przetwarzania, więc wymaga odpowiedniej podstawy prawnej. Umowa z lekarzami nie wystarcza jako podstawa do przetwarzania danych pacjentów (pacjenci nie są stroną tej umowy).
- **Poważny problem bezpieczeństwa – pola swobodnego tekstu:** Kontrola wykazała, że do bazy trafiały dane wpisane w „wolnym tekście”, zawierające bezpośrednie identyfikatory 3 370 pacjentów, a u 3 080 osób także informacje o zdrowiu. Te dane zostały następnie przekazane stowarzyszeniu SIMG. Organ uznał, że to nie może być sprowadzone wyłącznie do błędu lekarzy – administrator powinien mieć mechanizmy wykrywania takich danych.
- **Obowiązek kontroli i „privacy by design”:** IQVIA powinna była przed wdrożeniem i w trakcie działania systemu weryfikować, czy narzędzie nie pobiera danych identyfikujących (np. z pól tekstowych), oraz regularnie oceniać skuteczność zabezpieczeń. Brak takich działań narusza zasady integralności i poufności oraz ochrony danych w fazie projektowania.
- **Retencja danych – brak zasad usuwania:** Organ stwierdził naruszenie zasady ograniczenia przechowywania, bo spółka nie miała konkretnych procedur usuwania danych i przechowywała je dłużej niż to konieczne. Ogólna polityka dot. dokumentacji (administracyjnej/prawnej/podatkowej) nie zastępuje zasad retencji dla danych osobowych w bazie.
- **Ocena skutków (DPIA) musi być przed startem:** Przy przetwarzaniu na dużą skalę danych o zdrowiu trzeba przeprowadzić ocenę skutków dla ochrony danych przed rozpoczęciem przetwarzania. Samo „rozpoczęcie przygotowań” nie spełnia wymogu z art. 35 RODO.
- **Dlaczego argument z wyroku TSUE nie pomógł:** IQVIA powoływała się na pogląd, że dla konkretnego odbiorcy dane pseudonimizowane mogą nie być danymi osobowymi, jeśli nie ma on realnych środków identyfikacji. Organ uznał jednak, że IQVIA nie była „zwykłym odbiorcą” – była administratorem zaprojektowanego przez siebie procesu, więc nie może zasłaniać się brakiem dostępu do jednego elementu identyfikacji.
- **Skutki decyzji:** Decyzją z 23 września 2026 r. Garante stwierdził naruszenia m.in. legalności, ograniczenia przechowywania, integralności i poufności, rozliczalności oraz „privacy by design”, nałożył karę **7 000 000 euro** i nakazał dostosowanie przetwarzania.
- **Co organ nakazał / dopuścił na przyszłość:** Jeśli IQVIA chce kontynuować model, musi m.in. wskazać podstawę prawną, zrealizować obowiązki informacyjne, wykonać DPIA oraz ułożyć role (np. lekarze jako podmioty przetwarzające). Alternatywnie – organ dopuścił model, w którym to lekarze niezależnie anonimizują dane, a IQVIA nie określa sposobu pseudonimizacji.
- **Najważniejsze wnioski (w skrócie):**
  - Odpowiedzialność administratora wynika z faktów i realnego wpływu na proces, a nie z zapisów umowy.
  - Pseudonimizacja nie jest anonimizacją – RODO nadal ma zastosowanie.
  - Ocena ryzyka identyfikacji musi obejmować cały „bogaty” rekord danych i analizę w konkretnym kontekście (także w czasie), nie tylko wybrane pola.
  - Brak kontroli nad jednym elementem (np. kluczem identyfikacyjnym u lekarza) nie zwalnia administratora z odpowiedzialności za zaprojektowany przepływ danych.

Źródło: https://judykatura.pl/wloski-organ-ochrony-danych-nalozyl-7-mln-euro-kary-na-firme-analizujaca-dane-zdrowotne/

Fakturownia ujawniła, jak doszło do wycieku danych. Incydent dotyczy każdego konta

- **Kontekst:** Pod koniec września serwis do fakturowania Fakturownia padł ofiarą ataku cyberprzestępców. Firma opisała przebieg incydentu i zakres wycieku. **Kluczowa informacja:** w mniejszym lub większym stopniu wyciek dotknął **każde konto** w serwisie.
- **Kiedy doszło do naruszenia:** wykrycie naruszenia ochrony danych osobowych nastąpiło **28 września**.
- **Jak długo atakujący mieli dostęp:** od ok. **3:20 (27 września)** do ok. **17:45 (28 września)**.
- **Co się wydarzyło:** osoba nieuprawniona uzyskała dostęp do systemów Fakturowni i **skopiowała dużą część bazy danych** na własne serwery.
- **Działania podjęte przez firmę po wykryciu ataku:**
  - usunięto nieuprawniony dostęp,
  - zmieniono klucze aplikacji oraz hasła do usług,
  - przeniesiono ruch na **nowe serwery zbudowane od zera**,
  - stare serwery zostały wyłączone.

- **Zgłoszenia incydentu: 29 września** Fakturownia zgłosiła naruszenie do **UODO**, **CERT Polska** i **Policji**. Tego samego dnia o sprawie informował także wicepremier i minister cyfryzacji **Krzysztof Gawkowski**.
- **Jakie dane mogły zostać skradzione (przykłady z listy firmy):**
  - pełne dane firm i użytkowników (m.in. nazwy, NIP, adresy, imiona i nazwiska, e-mail, telefon),
  - dane działów (m.in. adresy, NIP, nazwy banków, numery rachunków, IBAN/SWIFT),
  - **zaszyfrowane hasła** użytkowników,
  - **tokeny API** i klucze integracji zapisane w ustawieniach konta,
  - kwoty z faktur oraz salda rachunków bankowych (w zakresie zapisanym w systemie),
  - dane kontrahentów (np. nazwa/dane osobowe, NIP, adres, telefon, numer rachunku) – o ile kontrahent został dodany **przed 16 października 2024 r.**,
  - pełna treść faktur (sprzedawca, nabywca, kwoty) – ale tylko dla dokumentów wystawionych **przed 22 marca 2021 r.**,
  - dane o płatnościach, produktach i cennikach.

- **Zakres wycieku zależał od wieku danych:** według firmy pobieranie największych zbiorów zaczęło się od **najstarszych rekordów** i zostało przerwane, zanim dotarło do nowszych.
- **Ważny szczegół dot. faktur po 22 marca 2021 r.:** dla faktur wystawionych od tej daty **nie pobrano** nazwy nabywcy ani numeru faktury (wg wyjaśnień firmy).
- **Konta o szczególnie dużej skali wycieku:** z blisko **2250 kont** pobrano wszystkie dostępne w systemie dane z lat **2022–2026**; właściciele tych kont mają dostać osobną informację.
- **Czego atakującym nie udało się pozyskać (wg Fakturowni):**
  - certyfikatów KSeF,
  - loginów i haseł do banków,
  - danych kart płatniczych,
  - treści faktur wystawionych **po 22 marca 2021 r.**,
  - danych kontrahentów dodanych **po 16 października 2024 r.**.

- **Czy dane są publicznie dostępne:** firma podaje, że wg jej wiedzy dane **nie zostały dotąd upublicznione**; sytuacja ma być monitorowana wspólnie z CERT Polska.
- **Zalecenia dla użytkowników:**
  - zmienić hasło w Fakturowni (oraz w innych usługach, jeśli było takie samo),
  - wygenerować i wpisać **nowe klucze API**,
  - zachować szczególną ostrożność wobec podejrzanych wiadomości i prób kontaktu (ryzyko phishingu i podszywania się).

- **Kim jest Fakturownia:** internetowy program do fakturowania i uproszczonego zarządzania sprzedażą w chmurze; działa w Polsce oraz m.in. na Słowacji, w Czechach, we Francji i Hiszpanii.

Źródło: https://xyz.pl/dzieje-sie/fakturownia-ujawnila-jak-doszlo-do-wycieku-danych-incydent-dotyczy-kazdego-konta-4785

WSA w Łodzi: przedawnienie opłaty nie wydłuża retencji danych

- **Kontekst sprawy:** Wojewódzki Sąd Administracyjny (WSA) w Łodzi skierował do Trybunału Sprawiedliwości UE pytania o to, gdzie przebiegają granice wykorzystywania danych z systemu poboru opłat drogowych po upływie ustawowego terminu ich przechowywania (retencji). Spór dotyczy rozróżnienia między:
  - okresem, w którym państwo może dochodzić należności (przedawnienie), a
  - okresem, w którym organ może legalnie przechowywać dane osobowe identyfikujące przejazd (retencja).

- **O co chodziło w praktyce:** sprawa dotyczyła opłaty dodatkowej za przejazd płatnym odcinkiem autostrady. Organ oparł się na danych takich jak numer rejestracyjny, data, godzina i miejsce przejazdu oraz informacje pozwalające porównać przejazd z wykupionym biletem.
- **Kluczowe terminy z prawa krajowego:**
  - co do zasady dane w systemie poboru opłat miały być przechowywane maksymalnie **24 miesiące od końca roku**, w którym doszło do przejazdu (z wyjątkami, gdy wcześniej podjęto określone działania, np. wystawiono wezwanie),
  - natomiast sama opłata dodatkowa przedawniała się dopiero po **5 latach**.

- **Teza 1: retencja to nie przedawnienie**
  - WSA podkreślił, że termin przedawnienia mówi, jak długo można dochodzić należności publicznoprawnej.
  - Nie oznacza to automatycznie, że przez cały ten czas wolno przechowywać dane osobowe potrzebne do udowodnienia przejazdu.
  - Sąd zaznaczył, że nie można „z automatu" uznać, iż dłuższy termin przedawnienia znosi krótszy limit retencji.

- **Teza 2: o reżimie retencji może decydować cel i sposób użycia danych**
  - Wątpliwość dotyczy tego, czy o czasie przechowywania danych ma decydować ich **źródło techniczne** (np. system rozpoznawania tablic, rejestry, aplikacje), czy **funkcja**, jaką pełnią po włączeniu do systemu poboru opłat.
  - Jeśli dane z różnych źródeł są zintegrowane i służą temu samemu celowi (identyfikacja przejazdu i dochodzenie opłaty), mogą podlegać jednemu, wspólnemu reżimowi retencji.
  - Sąd zwrócił uwagę, że podejście „liczy się tylko źródło danych" mogłoby ułatwiać omijanie limitów retencji i zmniejszać przewidywalność dla kierowców.

- **Teza 3: dalsze przechowywanie danych wymaga wykazania konkretnej potrzeby**
  - Samo to, że organ ma prawo dochodzić opłaty przez 5 lat, nie przesądza jeszcze, że przez 5 lat wolno przechowywać dane osobowe (z punktu widzenia RODO).
  - Należy ocenić **niezbędność** przetwarzania danych w odniesieniu do konkretnego celu i ograniczeń ustanowionych w prawie krajowym (np. limit 24 miesięcy).

- **Teza 4: otwarte pytanie o skutki dowodowe**
  - WSA zapytał, czy dane przechowywane lub użyte po upływie dopuszczalnego terminu retencji mogą być wystarczającą podstawą do utrzymania decyzji nakładającej opłatę dodatkową.
  - Sąd nie przesądził, czy doszło do naruszenia RODO ani jakie miałyby być skutki takiego naruszenia dla decyzji administracyjnej.
  - Postępowanie w sprawie zostało zawieszone do czasu odpowiedzi Trybunału Sprawiedliwości UE.

- **Najważniejsze wnioski z pytań do TSUE (w skrócie):**
  - Retencja danych i przedawnienie należności to dwie różne instytucje i pełnią różne funkcje.
  - Nie można automatycznie uzasadniać przechowywania danych przez cały okres przedawnienia – potrzebna jest ocena niezbędności w świetle RODO i przepisów krajowych.
  - Znaczenie może mieć to, **jak** dane są wykorzystywane po ich zintegrowaniu w systemie poboru opłat (cel przetwarzania), a nie tylko to, **skąd** pierwotnie pochodzą.
  - TSUE ma też rozstrzygnąć, jakie konsekwencje może mieć oparcie decyzji o opłacie na danych użytych po upływie ustawowego limitu retencji.

Źródło: https://judykatura.pl/wsa-w-lodzi-przedawnienie-oplaty-nie-wydluza-retencji-danych/

Nie każde naruszenie ochrony danych wymaga zgłoszenia do Prezesa UODO

- **Kontekst:** Po serii ostatnich incydentów (m.in. nieuprawniony dostęp do baz kontrahentów i systemów fakturowych) Prezes UODO przypomina zasady z RODO dotyczące zgłaszania naruszeń ochrony danych osobowych.
- **Zasada ogólna (art. 33 ust. 1 RODO):** Administrator powinien zgłosić naruszenie do organu nadzorczego (Prezesa UODO) **bez zbędnej zwłoki**, chyba że **mało prawdopodobne** jest, aby naruszenie powodowało ryzyko naruszenia praw lub wolności osób fizycznych.
- **Kluczowy obowiązek:** Administrator musi **za każdym razem rzetelnie ocenić ryzyko** związane z naruszeniem – to wynik tej oceny decyduje, czy zgłoszenie jest konieczne.
- **Kiedy zgłoszenie może nie być wymagane:** Zwykle wtedy, gdy ujawniono dane przedsiębiorców, które są **powszechnie dostępne** w jawnych rejestrach (np. CEIDG), takie jak: imię i nazwisko, nazwa firmy, NIP, oficjalny adres działalności – ponieważ ujawnienie takich informacji co do zasady nie daje nowych możliwości działania na szkodę osoby.
- **Kiedy zgłoszenie jest wymagane:** Gdy naruszenie **może powodować ryzyko** dla praw lub wolności osób fizycznych, zwłaszcza jeśli oprócz danych publicznych ujawniono też informacje, które mogą ułatwić nadużycia (np. oszustwa, kradzież tożsamości, profilowanie, działania socjotechniczne).
- **Przykłady danych podnoszących ryzyko:**
  - **PESEL** – ryzyko kradzieży tożsamości, wyłudzeń, zaciągania zobowiązań finansowych.
  - **Szczegóły zakupów/usług wskazujące na stan zdrowia** lub inne dane wrażliwe – ryzyko naruszenia prywatności, dyskryminacji, nieuprawnionego profilowania.
  - **Informacje finansowe** – ryzyko oszustw finansowych, przygotowywania fałszywych faktur lub płatności.

- **Dodatkowy obowiązek (art. 34 RODO):** Jeśli analiza wykaże **wysokie ryzyko**, administrator powinien także **zawiadomić osoby**, których dane dotyczą.
- **Ważne:** Nawet jeśli administrator uzna, że nie musi zgłaszać naruszenia do UODO, nadal ma obowiązek:
  - **przeprowadzić i udokumentować** ocenę ryzyka,
  - wpisać naruszenie do **wewnętrznego rejestru naruszeń** wraz z uzasadnieniem, dlaczego nie doszło do zgłoszenia.

- **Wniosek praktyczny:** Dokumentowanie i ocena ryzyka są obowiązkowe w każdym przypadku, a zgłoszenie do UODO zależy od tego, czy naruszenie realnie może zaszkodzić osobom, których dane dotyczą.

Źródło: https://uodo.gov.pl/pl/138/4596

NSA: 1,97 mln zł kary za brak regularnych testów bezpieczeństwa

- **Kontekst sprawy:** Naczelny Sąd Administracyjny (NSA) rozpatrywał skargę kasacyjną spółki – następcy prawnego operatora telekomunikacyjnego – w sprawie **administracyjnej kary pieniężnej nałożonej przez Prezesa UODO** za niewdrożenie środków bezpieczeństwa adekwatnych do ryzyka (RODO).
- **Rozstrzygnięcie:** NSA **oddalił skargę kasacyjną**, utrzymując w mocy wcześniejsze orzeczenia akceptujące nałożenie kary.

- **Co się wydarzyło (incydent):** W systemie rejestracji abonentów usług przedpłaconych wykorzystano podatność, co umożliwiło osobie nieuprawnionej dostęp do **142 222 rekordów** potwierdzeń rejestracji dotyczących **114 963 klientów**.
- **Jakie dane wyciekły:** m.in. **imię i nazwisko, PESEL, dane dokumentu tożsamości, numer telefonu**.
- **Kara:** Prezes UODO nałożył **1 968 524 zł** administracyjnej kary pieniężnej (wymierzonej następcy prawnemu spółki).

- **Kluczowy powód odpowiedzialności:** system ochrony danych **nie obejmował regularnego testowania, mierzenia i oceniania skuteczności zabezpieczeń**. Sąd podkreślił, że bezpieczeństwo nie może polegać tylko na jednorazowej analizie ryzyka lub doraźnych działaniach.
- **Dlaczego zastosowane zabezpieczenia uznano za niewystarczające:** system weryfikował dane jedynie po **numerze identyfikacyjnym wniosku**, bez dodatkowej walidacji (np. identyfikatora punktu sprzedaży), co umożliwiło dostęp nieuprawniony.
- **Regularność ma znaczenie:** przeglądy wykonywane tylko „przy okazji" zmian organizacyjnych lub prawnych **nie spełniają wymogu regularności** wynikającego z RODO.

- **Teza 1 – zgłoszenie naruszenia nie obniża automatycznie kary:** samo zgłoszenie incydentu do UODO jest realizacją obowiązku z art. 33 RODO. Organ ma to **rozważyć** przy wymiarze kary, ale co do zasady jest to okoliczność **neutralna**, a nie łagodząca.
- **Teza 2 – naruszenie trwa do potwierdzenia usunięcia uchybień:** samo rozpoczęcie działań (np. procesu zgodności/certyfikacji) **nie dowodzi**, że braki zostały skutecznie usunięte.
- **Teza 3 – obowiązek testowania dotyczy także „normalnego działania", nie tylko projektu:** wymogi RODO odnoszą się nie tylko do fazy projektowania rozwiązań, ale również do **bieżącego przetwarzania danych** i utrzymywania zabezpieczeń w stanie umożliwiającym ich weryfikację.
- **Teza 4 – sąd był związany wcześniejszym wyrokiem:** NSA wskazał, że wcześniejsza prawomocna ocena prawna w tej samej sprawie wiąże kolejne rozstrzygnięcia. Nie można skutecznie „od nowa" podważać ustaleń już przesądzonych (m.in. nieadekwatności zabezpieczeń oraz możliwości uwzględnienia szkody niemajątkowej, np. obaw osób, których dane wyciekły).

- **Kiedy – zdaniem sądu – ustało naruszenie:** spółka twierdziła, że wcześniej (po raporcie audytowym z lutego 2020 r.), ale sąd uznał, że raport wciąż wskazywał braki (m.in. brak zasad regularnych testów). Przyjęto więc, że naruszenie trwało **do uzyskania certyfikacji** zgodności z normami **ISO/IEC 27001:2013** oraz **ISO/IEC 27701:2019** (jako dowodu zakończenia procesu usuwania uchybień).
- **Wniosek praktyczny dla organizacji:** przy przetwarzaniu danych na dużą skalę trzeba umieć wykazać nie tylko wdrożenie zabezpieczeń, ale też ich **regularne, rzeczywiste sprawdzanie**. Jednorazowa analiza ryzyka, rozpoczęty proces certyfikacji lub samo zgłoszenie incydentu **nie zwalniają z odpowiedzialności** za wcześniejsze braki w bezpieczeństwie.

Źródło: https://judykatura.pl/nsa-197-mln-zl-kary-za-brak-regularnych-testow-bezpieczenstwa/

Rekordowo niski odsetek uwzględniania skarg na decyzje Prezesa UODO

- **Kontekst:** artykuł analizuje, jak często sądy administracyjne zmieniają (uchylają) decyzje Prezesa UODO w sprawach dotyczących ochrony danych osobowych (RODO) oraz jak zmieniała się liczba i skuteczność skarg w ostatnich latach.
- **2025 r. – niski odsetek uchyleń decyzji UODO:** Wojewódzki Sąd Administracyjny uchylił **39 z 205** rozpoznanych skarg na decyzje administracyjne Prezesa UODO, czyli **19,02%**.
- **Porównanie do 2023 r.:** w 2023 r. uwzględniono **37 z 189** skarg na decyzje Prezesa UODO, czyli **19,58%** (minimalnie więcej niż w 2025 r.).
- **Wniosek autora dotyczący jakości pracy urzędu:** mimo rekordowej liczby decyzji w 2025 r. (ponad **2 tys.**) odsetek skutecznych skarg pozostaje niski, co ma świadczyć o **wysokiej jakości merytorycznej** decyzji Prezesa UODO oraz **większej sprawności** urzędu (ok. **25% więcej decyzji** niż rok wcześniej).
- **Liczba skarg w 2025 r.:** do sądów administracyjnych wpłynęły **334** skargi na różne działania Prezesa UODO (głównie na decyzje) – to prawie tyle samo co w rekordowym 2023 r. (różnica **1** skargi).
- **2024 r. – wyższy odsetek uwzględnionych skarg:** sądy rozpoznały **296** skarg (więcej niż wpłynęło w tym roku: **225**) i uwzględniły **70**, czyli **23,65%**.
- **2022 r. – podobnie do 2024 r.:** wniesiono **289** skarg, rozpoznano **254**, uwzględniono **63**, czyli **24,8%**.
- **2021 r. – najwyższa skuteczność skarg:** uwzględniono **72 z 192** rozpoznanych skarg, czyli **37,5%** (wpłynęły **302** skargi).
- **Wpływ pandemii:** wysoka liczba skarg w okolicach 2021 r. była wiązana z pandemią i zamieszaniem wokół przetwarzania danych (m.in. praca zdalna), ale też ze wzrostem świadomości praw – od tego czasu liczba skarg utrzymuje się blisko **300 rocznie**.
- **Wcześniej po wejściu RODO skarg było mniej:** w pierwszych latach po rozpoczęciu stosowania RODO liczba skarg była wyraźnie niższa i **nie przekraczała 200**.
- **2020 r.:** wniesiono **177** skarg, rozpoznano **107**, uwzględniono **23** (**21,5%**).
- **2019 r.:** wpłynęło **161** skarg, rozpoznano **68**, uwzględniono **15** (**22,06%**).
- **2018 r. (start stosowania RODO):** wpłynęło **56** skarg; rozpoznano **81** (z uwzględnieniem skarg na rozstrzygnięcia GIODO); uwzględniono **18**. Autor wskazuje, że mimo specyfiki tego roku odsetek był **zbliżony** do kolejnych lat (ok. **22%**).
- **Ogólny obraz z danych:** w ostatnich latach tylko część skarg jest uwzględniana (zwykle ok. **19–25%**, z wyjątkiem 2021 r.), a jednocześnie liczba skarg po pandemii utrzymuje się na podwyższonym poziomie.

Źródło: https://uodo.gov.pl/pl/138/4597

WSA w Warszawie: wcześniejsza wiedza nie legalizuje ujawnienia danych

- **Kontekst sprawy:** Artykuł omawia wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie (8 kwietnia 2026 r., wyrok nieprawomocny) dotyczący tego, kiedy bank może legalnie udostępnić dane osobowe oraz czy wcześniejsza znajomość informacji przez odbiorcę „usprawiedliwia” ich ponowne potwierdzenie i przekazanie.
- **O co chodziło:** Bank wydał osobie trzeciej (córce klientki) zaświadczenie zawierające dane klientki oraz informację o zawarciu przez nią umów najmu konkretnych skrytek sejfowych.
- **Reakcja organu i sądu:** Prezes UODO uznał to za naruszenie art. 6 ust. 1 RODO (brak wykazanej podstawy prawnej) i udzielił bankowi upomnienia; WSA oddalił skargę banku na to rozstrzygnięcie.
- **Kluczowy wniosek 1 – wcześniejsza wiedza odbiorcy nie legalizuje udostępnienia:** To, że odbiorca już wcześniej znał dane (np. z wcześniejszych relacji lub umów), nie ma znaczenia dla oceny, czy bank mógł je później ponownie ujawnić. Samo „potwierdzenie” informacji przez administratora jest przetwarzaniem danych i musi mieć podstawę z art. 6 ust. 1 RODO.
- **Kluczowy wniosek 2 – bank musi wykazać konkretną podstawę z art. 6 ust. 1 RODO:** Sąd podzielił ocenę, że bank nie udowodnił m.in. istnienia zgody klientki, niezbędności do wykonania umowy ani niezbędności do spełnienia obowiązku prawnego. Nie potwierdzono też, aby odbiorczyni była uprawniona do uzyskania tych informacji.
- **Kluczowy wniosek 3 – umowy najmu skrytek traktuje się jako odrębne zdarzenia:** Brak dokumentów potwierdzających „trójstronne” przejęcie skrytek (bank + klientka + córka) spowodował, że sąd nie uznał, iż osoba trzecia miała prawo do informacji o umowie zawartej przez inną osobę. Rozwiązanie jednej umowy i zawarcie tego samego dnia nowej umowy przez inną osobę uznano za dwa niezależne zdarzenia.
- **Kluczowy wniosek 4 – spór cywilny o tajemnicę bankową nie przesądza o RODO:** Oddalenie powództwa cywilnego (dotyczącego tajemnicy bankowej/dóbr osobistych) nie oznacza automatycznie, że przetwarzanie danych było legalne w rozumieniu RODO. To dwa różne reżimy prawne (prawo prywatne vs publiczne) i wymagają odrębnej oceny.
- **Kluczowy wniosek 5 – Prezes UODO ocenia sprawę autonomicznie:** Organ nadzorczy ma prawo samodzielnie ustalać okoliczności istotne dla legalności przetwarzania danych. Nie rozstrzyga roszczeń cywilnych, ale niezależnie ocenia zgodność działań administratora z RODO.
- **Kluczowy wniosek 6 – wiąże sentencja wyroku, nie uzasadnienie:** Sąd przypomniał, że moc wiążąca prawomocnego orzeczenia dotyczy przede wszystkim sentencji (rozstrzygnięcia), a nie argumentów w uzasadnieniu. Dodatkowo roszczenia cywilne i uprawnienia wynikające z RODO nie są tożsame.
- **Znaczenie praktyczne dla organizacji (administratorów danych):** Każde ujawnienie/udostępnienie danych trzeba umieć uzasadnić i udokumentować właściwą podstawą prawną z art. 6 ust. 1 RODO — nawet jeśli odbiorca „już to wie”. Znajomość informacji przez odbiorcę nie zastępuje zgody, obowiązku prawnego ani innej przesłanki legalności.