RODO Aktualności

Data publikacji: 27.10.2026

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. Weto Prezydenta nie wpływa na kompetencje Prezesa UODO w zakresie przejrzystości i targetowania reklamy politycznej
2. Prezes UODO z propozycją nowych przepisów chroniących prawa pacjentów
3. Reklamami na Google infekowali telefony i komputery na całym świecie. Operacja AdFection
4. Oszuści podszywają się pod UODO i chcą wyłudzić dane
5. Uwagi Prezesa UODO do projektu zmian rozporządzenia o systemach pomiarowych zużycia energii
6. Sąd Unii Europejskiej zbada skargę na nadzór nad danymi
7. Europejski Inspektor Ochrony Danych zalecił ochronę wymienianych danych
8. Sąd Hiszpański obniżył do 80 tys. euro karę firmy kurierskiej
9. Wolność badań naukowych a ochrona danych osobowych – konferencja
10. Rada UE za uproszczeniem przepisów RODO i cyberbezpieczeństwa

Weto Prezydenta nie wpływa na kompetencje Prezesa UODO w zakresie przejrzystości i targetowania reklamy politycznej

- **Kontekst:** Prezydent Karol Nawrocki zawetował ustawę z 4 września 2026 r., która miała uzupełniać i wspierać stosowanie unijnego rozporządzenia (UE) 2024/900 dotyczącego **przejrzystości i targetowania reklamy politycznej** (zwłaszcza w internecie).
- **Cel zawetowanej ustawy:** wskazanie krajowych organów odpowiedzialnych za wykonywanie zadań i nadzór wynikający z rozporządzenia (UE) 2024/900, określenie procedur postępowań przed tymi organami oraz wprowadzenie sankcji za naruszenia.
- **Dlaczego wątek UODO jest szczególny:** w odniesieniu do Prezesa UODO przepisy zawetowanej ustawy miały głównie charakter **porządkujący**, ponieważ kluczowe kompetencje UODO wynikają **bezpośrednio** z rozporządzenia (UE) 2024/900 (a nie z prawa krajowego).
- **Bezpośrednie stosowanie prawa UE:** rozporządzenie (UE) 2024/900 obowiązuje bezpośrednio we wszystkich państwach UE od **10 października 2025 r.**
- **Zakres kompetencji organów ochrony danych (w tym Prezesa UODO):** art. 22 ust. 1 rozporządzenia (UE) 2024/900 przesądza, że organy ochrony danych monitorują przestrzeganie wymogów z **art. 18 i 19** dotyczących technik **targetowania** i **dostarczania** reklamy politycznej online oraz dodatkowych wymogów przejrzystości związanych z tymi technikami.
- **Powiązanie z RODO:** w tym obszarze przewidziano odpowiednie stosowanie **art. 58 RODO** oraz pełne stosowanie przepisów **rozdziału VII RODO** (współpraca i mechanizm spójności między organami w UE).
- **Kary finansowe:** Prezes UODO, w zakresie swoich kompetencji wynikających z rozporządzenia (UE) 2024/900, może nakładać **administracyjne kary pieniężne** zgodnie z **art. 83 RODO** (art. 25 ust. 6 rozporządzenia 2024/900).
- **Nie wszystko należy do UODO:** rozporządzenie (UE) 2024/900 wprowadza także **szerszy zakres obowiązków**, z których część pozostaje **poza właściwością** Prezesa UODO.
- **Dalsze prace na poziomie UE:** Europejska Rada Ochrony Danych (EROD) przygotowuje wytyczne dotyczące art. 18 i 19 rozporządzenia (UE) 2024/900; **27 marca 2026 r.** przeprowadzono konsultacje publiczne, a dostępne jest sprawozdanie z konsultacji.

Źródło: https://uodo.gov.pl/pl/138/4611

Prezes UODO z propozycją nowych przepisów chroniących prawa pacjentów

- **Kontekst:** Po śmierci lekarza prowadzącego indywidualną praktykę pojawia się praktyczny problem: pacjenci mogą mieć trudność z uzyskaniem dostępu do swojej dokumentacji medycznej. Na ten problem zwrócił uwagę Prezes UODO Mirosław Wróblewski, opisując sprawę pacjentki, która nie mogła otrzymać dokumentacji po zgonie lekarza.
- **Dlaczego to ważne:** Dane o zdrowiu są szczególnie chronione (art. 9 RODO). Niewłaściwe lub niejasne procedury przejęcia dokumentacji zwiększają ryzyko naruszeń prywatności i ograniczają prawa pacjentów.
- **Co mówią przepisy dziś:** Zgodnie z art. 30a ust. 3 pkt 3 ustawy o prawach pacjenta – gdy nie ma podmiotu, który przejąłby zadania po zmarłym lekarzu prowadzącym praktykę – za **przechowywanie i udostępnianie dokumentacji** odpowiada właściwa **okręgowa izba lekarska**.
- **Główny problem:** Przepisy nakładają obowiązek na okręgowe izby lekarskie, ale **nie precyzują w ustawie** trybu i sposobu jego realizacji. To powoduje **niepewność prawną** i różne praktyki w kraju.
- **Co dzieje się w praktyce:** Okręgowe izby lekarskie, próbując uzupełnić braki, wydają **wewnętrzne uchwały/instrukcje** dotyczące przejmowania dokumentacji (np. wymagające złożenia wniosku przez osobę posiadającą dokumentację, czasem przez spadkobiercę lekarza). Inne izby mogą działać inaczej.
- **Zastrzeżenia Prezesa UODO:** UODO ocenia, że tworzenie zasad przetwarzania danych wrażliwych w drodze **aktów wewnętrznych** izb budzi poważne wątpliwości z perspektywy legalności przetwarzania danych (wymogi art. 6 i art. 9 RODO). Takie kwestie powinny wynikać z jasnych przepisów prawa.
- **Brak „automatycznego" działania po śmierci lekarza:** Prezes UODO wskazuje, że śmierć lekarza skutkuje m.in. skreśleniem z rejestrów, co powinno uruchamiać działania samorządu w sprawie dokumentacji. Jednak bez wyraźnych obowiązków ustawowych w praktyce często do tego nie dochodzi.
- **Stanowisko Naczelnej Rady Lekarskiej (NRL):** W odpowiedzi na wcześniejsze sygnały, NRL wskazała, że brakuje przepisów dotyczących **poszukiwania i pozyskiwania** dokumentacji medycznej w celu jej przechowywania.
- **Prawa pacjenta:** UODO podkreśla, że prawo pacjenta do **dostępu do dokumentacji** i informacji o zdrowiu jest chronione przez RODO oraz przepisy prawa cywilnego.
- **Kto jest administratorem danych:** Okręgowe izby lekarskie mają status **administratora** w odniesieniu do przejętej dokumentacji, co – zdaniem UODO – powinno umożliwiać im podejmowanie działań niezbędnych do zabezpieczenia danych i realizacji praw pacjentów, ale nadal brakuje przejrzystych reguł „jak to robić".
- **Wniosek do Ministerstwa Zdrowia:** Prezes UODO zwrócił się do minister zdrowia Jolanty Sobierańskiej-Grendy o rozważenie **działań legislacyjnych**, które kompleksowo uregulują procedurę przejmowania dokumentacji po zmarłym lekarzu.
- **Co powinno zostać doprecyzowane w prawie (postulaty UODO):**
  - jak ustalać, **kto** po śmierci lekarza posiada dokumentację i jak przetwarzać te informacje,
  - jasne zasady i kroki **przejmowania dokumentacji** przez samorząd lekarski,
  - nałożenie obowiązku na osoby posiadające dokumentację (np. spadkobierców) do jej **przekazania** właściwej izbie,
  - mechanizmy **egzekwowania** obowiązku przekazania dokumentacji, gdy ktoś go nie wykonuje.

- **Możliwe sankcje:** UODO postuluje także rozważenie **sankcji karnych** za niewywiązywanie się z obowiązków związanych z przekazaniem/przejęciem dokumentacji po zmarłym lekarzu.
- **Najważniejszy wniosek:** Obecne przepisy tworzą lukę: obowiązek przejęcia dokumentacji istnieje, ale brakuje jednolitej, ustawowej procedury. Zdaniem UODO nie powinno być tak, że luki w ochronie danych o zdrowiu „łata się" wyłącznie wewnętrznymi uchwałami izb – potrzebne są jasne, ogólnokrajowe regulacje ustawowe.

Źródło: https://uodo.gov.pl/pl/138/4610

Reklamami na Google infekowali telefony i komputery na całym świecie. Operacja AdFection

- **Kontekst (o co chodziło):** opisana operacja polegała na złośliwych reklamach, które potrafiły zainfekować urządzenie już po samym wyświetleniu reklamy (bez klikania). W części przypadków reklama mogła ładować się „w tle", więc użytkownik mógł nawet nie zauważyć, że coś się wyświetliło.
- **Nie były to masowe ataki:** w kampanii używano zaawansowanego spyware, a ofiary były dobierane selektywnie (atak „wymierzony" w konkretne osoby, a nie przypadkowych użytkowników).
- **Ogromna skala dystrybucji reklam:** reklamy były emitowane na ok. **120 000 stron internetowych** i w ok. **70 000 aplikacjach**, w tym na znanych serwisach jak **BBC** czy **New York Times**.
- **Model „usługi" do infekowania:** firma **Discover-Tech** miała umożliwiać zakup „usługi infekowania urządzeń". Klient dostawał dostęp do **panelu administracyjnego**, z którego mógł uruchamiać operacje.
- **Ciekawostka dot. Polski:** co najmniej jeden użytkownik (klient) platformy logował się z **Polski**, przy czym ten sam użytkownik logował się też z **trzech innych krajów**.
- **Skąd wiadomo o logowaniach:** panel dla klientów Discover-Tech miał podatność – wejście na ścieżkę **/csv-download** pozwalało pobrać **logi połączeń** (w tym adresy IP) **bez logowania**.
- **Nie tylko Google:** poza reklamami w ekosystemie Google wykorzystywano również **Yandex** oraz kilka mniejszych platform reklamowych.
- **Długi czas działania:** operacja mogła trwać nawet od **2020 roku**, a została zablokowana dopiero w **październiku 2026**.
- **Dlaczego mogło to działać tak długo:** Discover-Tech uzyskała w Google status **„Certified External Vendor"**, co mogło ułatwiać publikowanie reklam i ograniczać poziom kontroli (zwłaszcza jeśli współpraca była opłacalna biznesowo).

Źródło: https://sekurak.pl/reklamami-na-google-infekowali-telefony-komputery-na-calym-swiecie-operacja-adfection/

Oszuści podszywają się pod UODO i chcą wyłudzić dane

- **Kontekst:** cyberprzestępcy podszywają się pod **Urząd Ochrony Danych Osobowych (UODO)** i wysyłają do firm (zwłaszcza instalujących monitoring) fałszywe prośby o przekazanie szczegółowych danych dot. systemów monitoringu wizyjnego. **UODO potwierdza, że to nie są wiadomości wysyłane przez Urząd.**
- **Co się wydarzyło:** w poniedziałek **19 października** CSIRT GOV poinformował UODO o kampanii e-mailowej wymierzonej w firmy związane z instalacją monitoringu.
- **Na czym polega oszustwo:** nadawca udaje UODO i żąda przesłania zestawienia instalacji monitoringu z ostatnich 12 miesięcy, sugerując, że jest to „urzędowe wezwanie" oraz wyznaczając termin **7 dni roboczych** na odesłanie pliku (np. **XLSX**).
- **Jakie dane próbują wyłudzić oszuści:**
  - dane kontaktowe użytkownika końcowego,
  - lokalizacje instalacji (nawet z **dokładnymi współrzędnymi geograficznymi**),
  - **adresy IP** urządzeń,
  - **numery seryjne**,
  - wersje **firmware**,
  - informacje o **modelach kamer**.

- **Dlaczego wiadomość może wyglądać wiarygodnie:** zawiera formalny język, przywołuje przepisy RODO (choć wskazane artykuły nie muszą mieć bezpośredniego związku z monitoringiem), podaje prawie poprawne dane teleadresowe oraz dołącza tabelę do wypełnienia.
- **Po co przestępcom te informacje:**
  - mogą ocenić, czy urządzenia mają nieaktualne oprogramowanie i wykorzystać znane podatności,
  - mogą próbować przejąć kontrolę nad urządzeniami, zwłaszcza jeśli pozostały ustawienia fabryczne,
  - zebrane dane mogą ułatwić identyfikację użytkowników końcowych i miejsc instalacji,
  - przejęcie obrazu z kamer może realnie wpływać na **bezpieczeństwo osób i mienia**.

- **Stanowisko UODO:** Urząd podkreśla, że **nie rozsyła takich pism/ankiet** (tym bardziej jako „urzędowe wezwanie") i **nie zbiera** tego typu szczegółowych informacji o konkretnych instalacjach monitoringu.
- **To klasyczny phishing:** czyli próba wyłudzenia wrażliwych danych poprzez podszywanie się pod zaufaną instytucję.
- **Jak zwykle działa UODO (ważne rozróżnienie):**
  - UODO kontroluje przede wszystkim **administratorów danych** (podmioty decydujące o celach i sposobach przetwarzania), a nie instalatorów, dostawców czy serwisy.
  - Jeśli Urząd dopytuje o szczegóły w ramach postępowania, sprawa ma **konkretną sygnaturę** i wskazany jest kontakt do departamentu prowadzącego.
  - Komunikacja urzędowa odbywa się typowo **pocztą tradycyjną** lub przez **eDoręczenia/ePUAP**.
  - Szersze działania (np. zbieranie opinii/ogólnych informacji) są zwykle zapowiadane komunikatem na stronie **uodo.gov.pl**, pytania mają charakter ogólny i często są **dobrowolne**.

- **Zalecenie:** zachować szczególną ostrożność i **zawsze weryfikować**, czy korespondencja rzeczywiście pochodzi od instytucji, za którą się podaje (zwłaszcza jeśli dotyczy przekazywania wrażliwych danych lub zawiera presję czasu).

Źródło: https://uodo.gov.pl/pl/138/4612

Uwagi Prezesa UODO do projektu zmian rozporządzenia o systemach pomiarowych zużycia energii

- **Kontekst:** Prezes Urzędu Ochrony Danych Osobowych (UODO) Mirosław Wróblewski przekazał Ministrowi Energii Miłoszowi Motyce uwagi do planowanych zmian w przepisach dotyczących systemu pomiarowego zużycia energii.
- **Główne ryzyko wskazane przez UODO:** projekt może prowadzić do **nadmiernego gromadzenia danych o konsumentach**, co w praktyce może pozwolić na wnioskowanie o ich **stylu życia i codziennych aktywnościach**.
- **Kontrowersyjna częstotliwość pomiaru:** projekt przewiduje pomiar **nie rzadziej niż co sekundę**. Zdaniem Prezesa UODO tak wysoka częstotliwość:
  - umożliwia pozyskiwanie bardzo szczegółowych danych,
  - zwiększa ryzyko **profilowania** odbiorców energii,
  - może stanowić **nadmierną ingerencję w prywatność**.

- **Problem z dostępem konsumentów do danych:** według UODO projektowane przepisy mogą utrudnić odbiorcom **bezpośredni i przejrzysty dostęp** do informacji o własnym zużyciu energii.
- **Pominięcie wymagań unijnych dla urządzeń pomiarowych:** w załączniku do projektu rozporządzenia mają zostać pominięte wymagania wynikające z prawa UE, co może:
  - ograniczyć prawa konsumentów do **transparentnego odczytu** zużycia energii,
  - sprawić, że odczyt parametrów będzie możliwy dopiero **z użyciem zewnętrznych instrukcji**,
  - pozbawić odbiorców gwarantowanego prawem **dostępu do danych rozliczeniowych bez dodatkowych warunków**.

- **Postulat zasady minimalizacji danych:** Prezes UODO wskazał na konieczność analizy, czy cele regulacji nie mogą być osiągnięte **mniej inwazyjnymi metodami** i przy mniejszym zakresie danych, szczególnie wobec osób **niekorzystających z taryf dynamicznych**.
- **Rekomendacja „testu prywatności”:** z uwagi na ryzyka dla praw i wolności osób UODO postuluje przeprowadzenie w procesie legislacyjnym **oceny skutków dla ochrony danych** (tzw. testu prywatności).

Źródło: https://uodo.gov.pl/pl/138/4608

Sąd Unii Europejskiej zbada skargę na nadzór nad danymi

- **Kontekst:** Sprawa dotyczy sporu o to, jak **Europejski Inspektor Ochrony Danych (EIOD)** rozpatrzył skargę na **Europol** w związku z przetwarzaniem danych osobowych. Skarga jest opisana w bazie Judykatura i zawiera **pięć zarzutów**. Postępowanie przed **Sądem Unii Europejskiej** jest w toku – **wyroku jeszcze nie ma**.

- **O co wnioskuje skarżąca (Natalie Gruber):**
  - o **stwierdzenie nieważności** decyzji EIOD z **8 lipca 2026 r.** (wydanej po jej skardze przeciwko Europolowi),
  - o **zadośćuczynienie** od UE za szkodę niemajątkową w wysokości **130 000 EUR** (lub innej uznanej przez Sąd),
  - o **odsetki** oraz obciążenie EIOD **kosztami postępowania**.

- **Ram czasowy:** skargę wniesiono **7 września 2026 r.**, a ogłoszenie o jej wniesieniu opublikowano **19 października 2026 r.**

- **Najważniejsze zarzuty (5 tez skargi):**
  - **1) Niewystarczające uzasadnienie decyzji EIOD:** skarżąca twierdzi, że EIOD naruszył obowiązek uzasadnienia (m.in. art. 296 TFUE) oraz prawa procesowe, w tym **prawo do bycia wysłuchaną** i **prawo do obrony**. Sąd ma ocenić, czy uzasadnienie pozwalało zrozumieć tok rozumowania oraz czy skarżąca realnie mogła przedstawić swoje stanowisko.
  - **2) Granice nadzoru EIOD nad Europolem:** skarżąca zarzuca **nadużycie uprawnień nadzorczych i dochodzeniowych** – jej zdaniem EIOD nie przeprowadził niezależnej kontroli, tylko w praktyce „zrekompensował" Europolowi braki w wypełnianiu obowiązków.
  - **3) Legalność przetwarzania danych przez Europol:** skarżąca kwestionuje, czy Europol miał podstawy do przechowywania i przetwarzania jej danych. Twierdzi, że dane miały związek z działaniem, które **nie było przestępstwem** i **nie mieściło się w kompetencjach Europolu** (chodzi o aktywność opisaną jako nakłanianie organów granicznych i bezpieczeństwa do ratowania migrantów).
  - **4) Brak samodzielnej oceny (oparcie się na ocenach krajowych):** skarżąca twierdzi, że EIOD **nie powinien opierać się wyłącznie** na stanowiskach krajowych organów ochrony danych, bez własnej analizy zgodności przetwarzania z prawem. Spór obejmuje też ocenę, czy Europol prawidłowo odpowiedział na **wniosek o dostęp do danych**.
  - **5) Zadośćuczynienie za przewlekłość postępowania:** skarżąca wskazuje na **zbyt długi czas** rozpatrywania sprawy i domaga się rekompensaty za szkodę niemajątkową. Podnosi, że długotrwała niepewność co do tego, **jakie dane** są przetwarzane, **skąd pochodzą**, **w jakim celu**, **gdzie** i **jak długo**, utrudniała jej skuteczne korzystanie z praw osoby, której dane dotyczą.

- **Dlaczego ta sprawa jest istotna (szersze znaczenie):**
  - Nie przesądza jeszcze niczego o tym, czy Europol lub EIOD działali niezgodnie z prawem, ale stawia ważne pytanie o **standard i „intensywność" nadzoru** nad przetwarzaniem danych przez unijną agencję policyjną.
  - Spór dotyczy nie tylko wyniku postępowania, ale też **sposobu prowadzenia kontroli** (samodzielność, rzetelność, terminowość).

- **Co pozostaje otwarte na tym etapie:**
  - Ogłoszenie o skardze przedstawia **stanowisko skarżącej**.
  - Sąd UE dopiero oceni: (1) czy decyzja EIOD była wadliwa, (2) czy przetwarzanie danych przez Europol było legalne, oraz (3) czy są podstawy do **odpowiedzialności odszkodowawczej UE**.
  - Nie można jeszcze wyciągać wniosków, jakie będzie stanowisko Sądu co do zasadności zarzutów.

Źródło: https://judykatura.pl/sad-unii-europejskiej-zbada-skarge-na-nadzor-nad-danymi/

Europejski Inspektor Ochrony Danych zalecił ochronę wymienianych danych

- **Kontekst:** Artykuł dotyczy zmian w zasadach działania unijnego repozytorium informacji o lotnictwie cywilnym. Repozytorium ma służyć nie tylko do **przechowywania** danych, ale też do ich **wymiany** (także bez trwałego zapisu) oraz do **analizy** informacji. Europejski Inspektor Ochrony Danych (EIOD) wskazuje, że ochrona danych nie może zależeć wyłącznie od tego, czy dane są w repozytorium „zapisane na stałe".

- **Główna teza 1 (wymiana danych):** Jeśli interfejs systemu ma umożliwiać dostęp nie tylko do danych przechowywanych, ale też do danych **wymienianych bez przechowywania**, to przepisy o ochronie danych osobowych powinny obejmować oba te sposoby przetwarzania.
- **Główna teza 2 (analiza danych):** Gdy Agencja UE ds. Bezpieczeństwa Lotniczego (EASA) analizuje informacje zawierające dane osobowe, musi stosować **rozporządzenie (UE) 2018/1725** (zasady ochrony danych dla instytucji i organów UE).

- **Czego dotyczą uwagi EIOD:** formalnych uwag z **19 października 2026 r.** do projektu zmieniającego zasady funkcjonowania repozytorium informacji w lotnictwie cywilnym.
- **Co zmienia projekt:** repozytorium, które dotąd służyło głównie do **przechowywania** danych przekazywanych przez krajowe organy, ma być też używane do **wymiany** wybranych informacji bez ich utrwalania w systemie.
- **Zidentyfikowany problem:** planowana funkcja interfejsu (dostęp online do danych również „wymienianych") jest szersza niż obecne brzmienie przepisów, które mówią o danych osobowych **przechowywanych** w repozytorium.
- **Rekomendacja legislacyjna:** EIOD zalecił zmianę art. 12 rozporządzenia wykonawczego (UE) 2023/2117 tak, aby obejmował dane osobowe **przechowywane w repozytorium lub wymieniane za jego pośrednictwem**.
- **Analiza informacji przez EASA:** projekt ma wyraźnie dopuścić analizowanie danych z repozytorium w celu wsparcia zadań związanych z **certyfikacją, nadzorem i egzekwowaniem** (dla EASA i organów krajowych).
- **Podkreślenie obowiązków prawnych:** dopuszczenie analizy nie znosi obowiązków wynikających z przepisów o ochronie danych — jeśli w analizowanych informacjach są dane osobowe, muszą być chronione zgodnie z właściwymi regulacjami.
- **Charakter stanowiska EIOD:** nie jest to stwierdzenie naruszenia, lecz **zalecenie** dla Komisji Europejskiej w ramach konsultacji projektu; EIOD oddzielił tę opinię od ewentualnych przyszłych działań nadzorczych.

- **Najważniejsze wnioski „wprost" z uwag EIOD:**
  - Ochrona danych powinna obejmować również dane **wymieniane** przez repozytorium, nawet jeśli nie są tam przechowywane.
  - EASA, analizując informacje zawierające dane osobowe, musi przestrzegać **rozporządzenia (UE) 2018/1725**.
  - Zmiana roli repozytorium (od przechowywania do wymiany i analizy) powinna być w pełni odzwierciedlona w przepisach dotyczących ochrony danych.

Źródło: https://judykatura.pl/europejski-inspektor-ochrony-danych-zalecil-ochrone-wymienianych-danych/

Sąd Hiszpański obniżył do 80 tys. euro karę firmy kurierskiej

- **Kontekst:** Artykuł opisuje wyrok hiszpańskiego sądu, z którego wynika, że **wadliwa weryfikacja tożsamości odbiorcy przesyłki** może prowadzić do **nielegalnego przetwarzania danych osobowych** (bez podstawy prawnej), gdy paczka trafia do osoby nieuprawnionej.
- **O co chodziło w sprawie:** Dwóch klientów kupiło telefony komórkowe z dostawą do domu, ale **przesyłki zostały wydane w placówce firmy kurierskiej osobom trzecim**, a nie faktycznym nabywcom.
- **Jak doszło do błędu (niedbała weryfikacja):**
  - W jednym przypadku osoba odbierająca podała tylko **imię i numer dokumentu** – **bez okazania dokumentu**.
  - W drugim przypadku przyjęto dokument, którego **dane i zdjęcie nie odpowiadały** prawdziwemu dokumentowi odbiorcy.

- **Dlaczego sąd potwierdził naruszenie RODO:** Sąd uznał, że to **firma kurierska** przetwarzała dane osobowe przy wydaniu przesyłek (w jej placówkach) i że z powodu braku należytej staranności doszło do użycia danych odbiorców oraz wydania telefonów osobom nieuprawnionym. W efekcie naruszono **art. 6 RODO** (brak legalnej podstawy przetwarzania).
- **Argument firmy kurierskiej nie pomógł:** Spółka twierdziła, że działała według instrukcji podmiotu zlecającego oraz że zmiana sposobu doręczenia była możliwa dla osoby znającej numer przesyłki i kod pocztowy. **Sąd nie uznał tego za zwolnienie z odpowiedzialności**.
- **Decyzja i kary:**
  - Organ ochrony danych nałożył początkowo **2 kary po 70 000 euro** (łącznie 140 000 euro) – po jednej za każdego poszkodowanego.
  - Sąd (wyrok z **1 października 2026 r.**, Audiencia Nacional) **utrzymał stwierdzenie naruszenia**, ale **obniżył łączną karę do 80 000 euro** (po 40 000 euro za każdy przypadek).

- **Kluczowy powód obniżenia kary:** Sąd uznał, że naruszenie wynikało z **niedbalstwa**, a nie z **działania umyślnego**. Nie było więc podstaw, by traktować sprawę jako „umyślne wykorzystanie danych" (okoliczność obciążająca).
- **Dodatkowe czynniki łagodzące:** Naruszenia nie były **ciągłe** ani **długotrwałe** oraz nie wykazano **wcześniejszych naruszeń** po stronie firmy.
- **Wniosek praktyczny dla firm dostawczych:** Operator wydający przesyłkę **nie może zasłaniać się samą umową** z nadawcą lub pośrednikiem. Jeśli identyfikacja odbiorcy i wydanie paczki dzieją się w jego placówce, musi zapewnić **rzetelną weryfikację tożsamości**.
- **Istotne rozróżnienie z wyroku:** Co innego **odpowiedzialność za naruszenie** (może wynikać z niedbałych procedur), a co innego **ocena winy przy wymiarze kary** (niedbalstwo nie oznacza automatycznie umyślności).

Źródło: https://judykatura.pl/sad-hiszpanski-obnizyl-do-80-tys-euro-kare-firmy-kurierskiej/

Wolność badań naukowych a ochrona danych osobowych – konferencja

- **Kontekst:** 20 listopada 2026 r. w godz. **09:30–13:40** odbędzie się **naukowa konferencja online** pt. „**Dane badawcze, dane osobowe. Wolność badań naukowych a ochrona danych osobowych**". Tematem spotkania będzie to, jak prowadzić badania naukowe z poszanowaniem zasad ochrony danych osobowych.
- **Organizatorzy:** Wydział Prawa i Administracji Uniwersytetu Łódzkiego, Wydział Prawa i Administracji Uniwersytetu Śląskiego, **Urząd Ochrony Danych Osobowych (UODO)** oraz Społeczny Zespół Ekspertów przy Prezesie UODO.
- **Otwarcie konferencji:** dr hab. Marlena Sakowska-Baryła, prof. UŁ oraz dr hab. Mariusz Jagielski, prof. UŚ.
- **Struktura wydarzenia:** konferencja będzie podzielona na **dwa panele tematyczne**.
- **Udział UODO w programie:** w pierwszym panelu wystąpi przedstawicielka UODO **Marta Brzózka** z prezentacją: „**Wyzwania związane z wypełnieniem warunków wyrażenia zgody w kontekście przetwarzania danych osobowych na potrzeby badań naukowych**".
- **Zakres omawianych zagadnień (najważniejsze wątki):**
  - obowiązki badaczy związane z **ochroną danych osobowych** w projektach naukowych,
  - zasady **zarządzania danymi badawczymi**,
  - wyzwania wynikające z wykorzystywania **sztucznej inteligencji** w badaniach naukowych.

- **Dostęp do transmisji:** wydarzenie będzie transmitowane online na stronie internetowej **UODO**; **nie jest wymagana wcześniejsza rejestracja**.

Źródło: https://uodo.gov.pl/pl/531/4633

Rada UE za uproszczeniem przepisów RODO i cyberbezpieczeństwa

- **Kontekst:** Rada Unii Europejskiej uzgodniła stanowisko w sprawie pakietu zmian, które mają **uprościć wybrane przepisy o ochronie danych, prywatności i cyberbezpieczeństwie**, przy zachowaniu wysokiego poziomu ochrony danych osobowych. Celem jest, aby prawo cyfrowe UE było **bardziej przejrzyste i łatwiejsze w stosowaniu** dla firm, administracji i obywateli, co ma wspierać konkurencyjność UE.
- **Skąd wynika inicjatywa:** propozycje są częścią pakietu legislacyjnego **„Omnibus VII"** w ramach unijnej agendy upraszczania prawa (od 2025 r. Komisja przedstawiła łącznie 12 pakietów „Omnibus").
- **Co obejmuje „Omnibus VII":** dwa wnioski – jeden dot. uproszczenia ram prawnych dla technologii cyfrowych (ten omawiany), drugi dot. ułatwień we wdrażaniu zharmonizowanych zasad dotyczących AI (akt dotyczący AI został przyjęty **29 czerwca 2026 r.**).
- **Ogólny cel zmian:** zmniejszenie obciążeń administracyjnych i kosztów zgodności, ułatwienie prowadzenia działalności w całej UE oraz szybsze uzyskanie praktycznych korzyści – bez obniżania standardów ochrony prywatności i praw obywateli.
- **Najważniejsze elementy mandatu Rady (zakres zmian):**
  - zmiany w **RODO** (ułatwienia i doprecyzowania zasad),
  - modernizacja podejścia do **plików cookie** w ramach dyrektywy **ePrivacy**,
  - **uchylenie** przepisów rozporządzenia **Platform-to-Business (P2B)**,
  - uproszczenie i konsolidacja przepisów jednolitego rynku dotyczących danych (**„data acquis"**),
  - mechanizmy usprawniające **zgłaszanie incydentów cyberbezpieczeństwa i incydentów dotyczących danych**.

- **RODO – kluczowe proponowane zmiany:**
  - utrzymanie obecnej **definicji danych osobowych**,
  - doprecyzowanie zasad dotyczących **pseudonimizacji** i identyfikacji osoby fizycznej, aby ułatwić spełnianie obowiązków,
  - uprościć obsługę **nieuzasadnionych lub nadmiernych żądań** oraz ograniczyć część **obowiązków informacyjnych** w sytuacjach niskiego ryzyka,
  - wprowadzenie bardziej jednolitego podejścia do przetwarzania danych w **badaniach naukowych** (definicja oparta na zasadach) oraz ukierunkowane wyjątki dla organizacji badawczych,
  - dodatkowe zabezpieczenia dla odstępstw dotyczących przetwarzania **danych wrażliwych** m.in. na potrzeby **weryfikacji biometrycznej** i w kontekście **systemów AI**,
  - wsparcie innowacji i rozwoju AI przez doprecyzowanie podstaw prawnych przetwarzania danych oraz wymogu stosowania zabezpieczeń,
  - poparcie dla wydłużenia terminu na **zgłaszanie naruszeń ochrony danych**,
  - większa spójność w UE dzięki m.in. wspólnemu wykazowi operacji wysokiego ryzyka oraz **wspólnym wzorom dokumentów** ułatwiającym wypełnianie obowiązków.

- **„Data acquis" i tajemnice przedsiębiorstwa – co ma się zmienić:**
  - uproszczenie zasad dotyczących **altruizmu danych** oraz **usług pośrednictwa danych**, aby łatwiej było stosować przepisy w praktyce (mniej rozbieżności interpretacyjnych i obciążeń administracyjnych),
  - możliwość ustalania przez sektor publiczny **innych warunków i wyższych opłat** za ponowne wykorzystywanie danych przez **bardzo duże przedsiębiorstwa**, w tym tzw. **gatekeepers**,
  - wzmocnienie ochrony przed ryzykiem ujawnienia **tajemnic przedsiębiorstwa** państwom trzecim – ujawnienie ma być możliwe dopiero po podjęciu wszystkich niezbędnych działań zapewniających poufność.

- **ePrivacy i pliki cookie – najważniejsze założenia:**
  - utrzymanie zasad dot. technologii śledzenia (cookie i podobne),
  - aktualizacja poprzez doprecyzowanie **jasnych celów**, dla których **zgoda użytkownika nie byłaby wymagana**, co ma ograniczyć liczbę banerów cookie,
  - przykładowe sytuacje bez konieczności zgody: cookie niezbędne do świadczenia usługi, **pomiaru odbiorców**, zapewnienia **bezpieczeństwa urządzenia**.

- **Zgłaszanie incydentów cyberbezpieczeństwa i danych:**
  - zamiast jednego punktu zgłoszeniowego na poziomie UE – **krajowy punkt zgłoszeniowy** w każdym państwie członkowskim (ma ułatwiać raportowanie na podstawie różnych przepisów UE),
  - na poziomie UE ma powstać **punkt informacyjny** dotyczący zgłaszania incydentów,
  - planowane są przepisy mające stworzyć **bardziej zharmonizowane ramy** raportowania, w tym dla incydentów transgranicznych.

- **Co dalej:** po zatwierdzeniu mandatu Rady prezydencja rozpocznie negocjacje z Parlamentem Europejskim, gdy Parlament przyjmie własne stanowisko. Celem jest szybkie osiągnięcie porozumienia.
- **Szersze tło polityczne:** działania wpisują się w plan **„One Europe, One Market"** (podpisany 24 kwietnia 2026 r.), który zakłada zakończenie prac nad pakietami upraszczającymi do **końca 2027 r.**; impuls do przyspieszenia uproszczeń wynika m.in. z dyskusji o konkurencyjności UE po raportach Letty i Draghiego oraz wezwania Rady Europejskiej z października 2024 r.

Źródło: https://www.consilium.europa.eu/en/press/press-releases/2026/10/21/digital-rulebook-council-agrees-position-to-simplify-data-protection-privacy-and-cyber-reporting-rules/?trk=public_post_comment-text