

LEX  ARTIST



BLOG-DANEOSOBOWE.PL

RODO Aktualności

Data publikacji: 24.03.2026

UWAGA!

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

Spis treści

1. Działania UODO w 2025 roku w ujęciu statystycznym
2. Francuski organ ochrony danych CNIL nałożył łącznie 42 mln euro kary na spółki FREE MOBILE i FREE
3. Nie można kopiować dokumentów bez podstawy prawnej - kara dla Glovo
4. Prezes UODO i SZE omówili bieżące problemy
5. AEPD nakłada karę 80 000 euro na firmę za zmuszanie pracowników do używania prywatnych smartfonów do 2FA
6. RODO daje podstawę prawną do kierowania zaproszeń na badania przesiewowe

Działania UODO w 2025 roku w ujęciu statystycznym

- **Kontekst:** Sprawozdanie Prezesa UODO za 2025 r. nie zostało jeszcze opublikowane. Autor wystąpił więc o informacje publiczne, aby sprawdzić, jakie działania podejmował Urząd Ochrony Danych Osobowych w 2025 r.
- **Ogólny wniosek:** Dane za 2025 r. sugerują, że UODO działa coraz intensywniej, mimo tylko niewielkiego wzmocnienia kadrowego.
- **Skargi od osób (podmiotów danych):** 12 986.
- **Zgłoszone naruszenia ochrony danych:** 22 029.
- **Kontrole przeprowadzone przez UODO:** 56.
- **Udzielone upomnienia:** 872.
- **Nałożone administracyjne kary pieniężne:** 32.
- **Łączna wartość nałożonych kar:** 64 436 940,25 zł.
- **Możliwa przyczyna wzrostu liczby zgłaszanych naruszeń:** rynek mógł zacząć zgłaszać znacznie więcej incydentów po publikacji poradnika UODO dot. naruszeń, interpretując go jako konieczność zgłaszania niemal każdego przypadku.
- **Dlaczego łączna kwota kar jest wysoka:** duży wpływ miały pojedyncze wysokie kary nałożone w 2025 r., m.in. na:
 - Poczta Polska S.A. – 27 000 000 zł (decyzja została uchylona),
 - McDonald's Polska – ok. 17 000 000 zł,
 - ING Bank Śląski – 18 400 000 zł.
- **Źródło danych:** informacje publiczne udzielone przez Prezesa UODO na wniosek.

Źródło: https://www.linkedin.com/posts/pluczynski_na-sprawozdanie-prezesa-uodo-za-2025-r-przyjdzie-ugcPost-7436892944005062656-EHp6?utm_source=share&utm_medium=member_desktop&rcm=ACoAAA9q6N4BN-DgkoP627n1-9JQZ-KmCRaOtlA

Francuski organ ochrony danych CNIL nałożył łącznie 42 mln euro kary na spółki FREE MOBILE i FREE

- **Kontekst:** Francuski regulator ochrony danych osobowych (CNIL) nałożył wysoką karę na grupę telekomunikacyjną Free (należącą do Iliad) po dużym wycieku danych klientów w wyniku cyberataku.
- **Wysokość kary:** łącznie **42 mln euro** – **27 mln euro** dla Free Mobile oraz **15 mln euro** dla Free (decyzja opublikowana 14 stycznia w Journal officiel).
- **Skala incydentu:** atak z października 2024 r. miał dotknąć **24,6 mln klientów**, co CNIL porównuje do ok. **1/3 populacji Francji**.
- **Powód sankcji:** CNIL wskazała na „**uchybień**” w zakresie bezpieczeństwa danych abonentów oraz ocenioną jako **poważną** skalę zaniedbań.
- **Co szczególnie obciążało firmę (wg CNIL):**
 - bezprecedensowa liczba osób, których dane zostały **pozyskane i wyprowadzone** z systemów,
 - **brak wdrożenia podstawowych, powszechnie stosowanych zabezpieczeń**, które mogły utrudnić lub zablokować działania hakerów,
 - **duże zasoby** grupy telekomunikacyjnej, które – zdaniem CNIL – powinny umożliwić zastosowanie odpowiednich środków ochrony.
- **Wątek śledczy:** w styczniu 2025 r. **16-letni** podejrzany o dokonanie włamania miał usłyszeć zarzuty (został formalnie objęty postępowaniem).
- **Stanowisko Free:** firma **kwestionuje decyzję**, twierdząc, że jest to sankcja o **bezprecedensowej surowości** na tle wcześniejszych spraw dotyczących cyberataków.
- **Dalsze kroki prawne:** Free złożył **odwołanie do Rady Stanu** (Conseil d'Etat), domagając się rewizji decyzji.
- **Działania po incydencie (wg Free):** spółka deklaruje, że po ataku **wzmocniła bezpieczeństwo, kontrole dostępu** oraz wdrożyła **wzmocniony monitoring w czasie rzeczywistym**.
- **Szerszy przekaz firmy:** Free podkreśla, że nawet bardzo dobrze zabezpieczone organizacje mogą paść ofiarą **zaawansowanych cyberataków**.

Źródło: https://www.lemonde.fr/economie/article/2026/01/14/le-groupe-free-ecope-d-une-amende-de-42-millions-d-euros-pour-vol-de-donnees_6662130_3234.html

Nie można kopiować dokumentów bez podstawy prawnej - kara dla Glovo

- **Kontekst:** Spółka Restaurant Partner Polska (platforma Glovo) pozyskiwała od części użytkowników aplikacji skany lub zdjęcia dowodów osobistych/paszportów w ramach procedur antyfraudowych. Prezes UODO uznał, że odbywało się to **bez odpowiedniej podstawy prawnej** i nałożył karę **5 898 064 zł**.
- **Skąd wzięta się sprawa:** Decyzja była następstwem kontroli Prezesa UODO dotyczącej sposobu przetwarzania danych użytkowników aplikacji „Glovo – dostawa jedzenie i inne”, w tym podstaw prawnych, celów i zakresu zbieranych danych.
- **Kiedy Glovo żądało dokumentów:** Spółka przewidywała dodatkową weryfikację tożsamości m.in. w sytuacjach podejrzenia oszustwa, np.:
 - zgłoszenie przez kuriera próby kradzieży zamówienia,
 - użycie fałszywych pieniędzy,
 - niezgodność danych karty płatniczej z danymi użytkownika,
 - podejrzenie, że przesyłka może zawierać nielegalne substancje.
- **Stanowisko spółki:** Glovo wskazywało jako podstawę prawną **art. 6 ust. 1 lit. f RODO** (uzasadniony interes administratora) i argumentowało, że:
 - żądania dokumentów były wyjątkowe,
 - przetwarzanie poprzedzono oceną skutków dla ochrony danych oraz tzw. testem równowagi.
- **Ocena Prezesa UODO:** Organ nie zgodził się z tą argumentacją i uznał, że w tym przypadku powołanie się na „uzasadniony interes” było **niewystarczające**, bo skany dokumentów tożsamości zawierają **bardzo szeroki zakres danych**.
- **Dlaczego to było problematyczne prawnie:**
 - Kopiowanie/utrwalanie dokumentów tożsamości powinno być dopuszczalne tylko w **wyjątkowych** sytuacjach i zwykle dla podmiotów **wyraźnie upoważnionych ustawą**.
 - Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (AML) daje takie uprawnienia tylko wskazanym instytucjom – **Restaurant Partner Polska nie należy** do tej grupy.
 - Ustawa o świadczeniu usług drogą elektroniczną również **nie dawała podstawy** do przetwarzania pełnych skanów dokumentów tożsamości w opisanym celu.
 - UODO uznał, że żądanie takich danych **nie było niezbędne** do zawarcia, wykonania lub rozwiązania umowy z użytkownikiem.
- **Minimalizacja danych:** Prezes UODO podkreślił, że przeciwdziałanie oszustwom nie może odbywać się kosztem naruszenia zasady **minimalizacji danych** – nie należy zbierać danych „na zapas” ani w zakresie szerszym niż konieczny.
- **Dodatkowy aspekt:** UODO uwzględnił również ustawę o dokumentach publicznych, która przewiduje szczególną ochronę dokumentów takich jak **dowód osobisty i paszport** (dokumenty publiczne pierwszej kategorii).
- **Jakie dane były zbierane:** Zakres danych z dokumentów był bardzo szeroki i obejmował m.in. imię i nazwisko, nazwisko rodowe, imiona rodziców, datę i miejsce urodzenia, PESEL, serię i numer dokumentu, daty wydania i ważności, adres zamieszkania, wizerunek oraz inne informacje widoczne na dokumencie.
- **Jakie naruszenia stwierdzono:** UODO uznał naruszenie m.in.:
 - **art. 6 ust. 1 RODO** – brak odpowiedniej podstawy prawnej do przetwarzania,
 - **art. 5 ust. 1 lit. a i c RODO** – naruszenie zasad zgodności z prawem/rzetelności/przejrzystości oraz minimalizacji danych,
 - **art. 5 ust. 2 RODO** – naruszenie zasady rozliczalności (skoro przetwarzanie było nielegalne, administrator nie wykazał prawidłowości działania).
- **Dlaczego kara była wysoka:** UODO wskazał na:
 - charakter i wagę naruszenia (dotyczyło podstawowych zasad RODO),
 - **długi okres trwania** – od lipca 2019 r.,
 - potencjalnie szeroką skalę oddziaływania – ponad **3,4 mln aktywnych użytkowników** w Polsce,
 - realne ryzyko szkód niemajątkowych, np. obawa przed utratą kontroli nad danymi i **kradzieżą tożsamości**.
- **Najważniejszy wniosek praktyczny:** Nawet przy podejrzeniu oszustwa firma musi działać w granicach prawa, a procedury antyfraudowe nie mogą prowadzić do zbierania skanów dokumentów tożsamości bez jednoznacznej podstawy prawnej.
- **Nakazy UODO:** Organ nakazał spółce:
 - zaprzestanie pozyskiwania i dalszego przetwarzania skanów/zdjęć dowodów osobistych i paszportów użytkowników,
 - **usunięcie** danych zebranych w ten sposób w terminie **30 dni** od doręczenia decyzji.
- **Sygnatura sprawy:** DKN.5112.33.2022

Prezes UODO i SZE omówili bieżące problemy

- **Kontekst:** 6 marca 2026 r. w siedzibie Urzędu Ochrony Danych Osobowych (UODO) odbyło się spotkanie Prezesa UODO z członkami Społecznego Zespołu Ekspertów (SZE) oraz Grupy roboczej SZE ds. sztucznej inteligencji (AI). Rozmowy dotyczyły bieżących wyzwań w ochronie danych osobowych, w tym w kontekście rozwoju technologii AI.
- **Rola ekspertów:** Prezes UODO Mirosław Wróblewski podkreślił, że SZE odgrywa ważną rolę we wspieraniu działań Urzędu i pomaga ukierunkowywać prace UODO na najpilniejsze problemy związane z ochroną danych.
- **Kongres i kontynuacja działań:** Prezes podziękował członkom SZE za zaangażowanie w organizację Kongresu Ochrony Danych i Nowych Technologii (28 stycznia 2026 r.) oraz zapowiedział kolejną edycję wydarzenia.
- **Plan prac na 2026 r.:** Dr Mirosław Gumularz, przewodniczący SZE, przedstawił harmonogram prac Zespołu na 2026 r.
- **Tematy do pogłębionej analizy:** Omówiono zagadnienia, które w najbliższym czasie wymagają dokładniejszego zbadania i wypracowania stanowisk oraz rekomendacji.
- **Wydarzenia dla środowiska ekspertów:** Przedyskutowano plany organizacji wydarzeń poświęconych problemom i wątpliwościom pojawiającym się w środowisku zajmującym się ochroną danych osobowych.
- **Opiniowanie przepisów prawa:** Rozmawiano o planach UODO dotyczących opiniowania obowiązujących i projektowanych aktów prawnych. Podkreślono wagę tej działalności, zwłaszcza gdy brakuje inicjatywy ustawodawczej.
- **Więcej skarg i zgłoszeń naruszeń:** Zwrócono uwagę na rosnącą liczbę wniosków skargowych oraz zgłoszeń naruszeń ochrony danych. Wzrost ten wiąże się m.in. ze zwiększoną świadomością społeczną dotyczącą roli i kompetencji UODO.
- **Usprawnienie pracy Urzędu:** Dyskutowano o możliwościach przyspieszenia rozpatrywania spraw i usprawnienia pracy UODO przy utrzymaniu wysokich standardów merytorycznych.
- **Oddzielne spotkanie ws. AI:** Tego samego dnia odbyło się spotkanie Grupy roboczej ds. sztucznej inteligencji, poświęcone bieżącym zagadnieniom i planom dalszych działań.
- **Ochrona danych w projektach AI:** Omawiano kwestie, które mogą wymagać interwencji UODO w związku z ochroną danych osobowych przy rozwoju i wdrażaniu rozwiązań AI.
- **Rekomendacje i raport strategiczny:** Pracowano nad rekomendacjami będącymi finalnym elementem dokumentu pt. „Raport Strategiczny - Badanie potrzeb organizacji w zakresie wykorzystania sztucznej inteligencji i ochrony danych osobowych”, dotyczącego wdrażania AI w instytucjach. Raport opracowała Grupa robocza ds. AI działająca w ramach SZE.
- **Wyzwania rynkowe:** Znaczną część dyskusji poświęcono bieżącym wyzwaniom na rynku wynikającym z rosnącego zainteresowania wdrażaniem technologii sztucznej inteligencji.

AEPD nakłada karę 80 000 euro na firmę za zmuszanie pracowników do używania prywatnych smartfonów do 2FA

- **Kontekst:** Hiszpańska Agencja Ochrony Danych (AEPD) ukarała firmę za to, że wymagała od pracowników używania **prywatnych smartfonów i prywatnych numerów telefonów** do uwierzytelniania dwuskładnikowego (2FA) w systemach firmowych.
- Pracownicy, aby uzyskać dostęp do platformy klienta, musieli otrzymywać **kod SMS** na telefon komórkowy.
- Ponieważ nie wszyscy mieli telefony służbowe, firma wymagała podania **prywatnego numeru telefonu**, aby móc otrzymywać SMS-y do logowania.
- W praktyce oznaczało to, że bez rejestracji prywatnego numeru **nie dało się korzystać z platformy**, a więc posiadanie i udostępnienie prywatnego numeru było **warunkiem wykonywania pracy**.
- Firma twierdziła, że przetwarzanie numerów telefonów było niezbędne do realizacji umowy o pracę i świadczenia usług, więc mogło opierać się na **art. 6 ust. 1 lit. b RODO** (niezbędność do wykonania umowy).
- AEPD nie zgodziła się z tym stanowiskiem: uznała, że wykorzystywanie **prywatnych numerów** nie było **obiektywnie konieczne** do wypełnienia obowiązków wynikających z umowy.
- Organ podkreślił, że to **pracodawca** ma obowiązek zapewnić **zasoby niezbędne do wykonywania pracy** (np. służbowe urządzenia lub alternatywną metodę 2FA).
- Wskazano też, że nawet gdyby firma próbowała oprzeć się na **zgodzie pracownika**, mogłaby ona nie być uznana za ważną, bo w relacji pracodawca–pracownik zgoda często **nie jest w pełni dobrowolna** (z powodu zależności służbowej).
- **Kara:** nałożono grzywnę w wysokości **80 000 euro**.
- **Obniżenie kary:** ponieważ firma przyznała się do naruszenia i dobrowolnie zapłaciła, grzywna została zmniejszona do **48 000 euro**.

Źródło: https://www.linkedin.com/posts/tomasz-borys-32725915a_rododaneosobowe-pracownik-share-7440040636625604608-xewp?utm_source=share&utm_medium=member_ios&rcm=ACoAAA9q6N4BN-DgkoP627n1-9JQZ-KmCRaOtlA

RODO daje podstawę prawną do kierowania zaproszeń na badania przesiewowe

- **Kontekst:** artykuł dotyczy tego, czy podmioty medyczne mogą przetwarzać dane osobowe pacjentów (w tym dane wrażliwe o zdrowiu) po to, aby wysyłać im **zaproszenia na badania przesiewowe** w ramach profilaktyki zdrowotnej.
- **Stanowisko Prezesa UODO:** Mirosław Wróblewski wskazał, że przetwarzanie danych pacjentów w celu kierowania zaproszeń na badania przesiewowe może być **legalne bez zgody pacjenta**, jeśli spełnia warunki z **art. 9 ust. 2 lit. h RODO** (cele profilaktyki zdrowotnej, diagnozy lub organizacji opieki zdrowotnej).
- **Warunek bezpieczeństwa:** takie przetwarzanie musi odbywać się **pod nadzorem osób zobowiązanych do zachowania tajemnicy zawodowej** (np. personelu medycznego).
- **Dlaczego powstało pismo:** stanowisko jest efektem spotkania UODO z Narodowym Instytutem Onkologii dotyczącego przetwarzania danych w profilaktyce onkologicznej i w działalności naukowej; po spotkaniu Instytut poprosił o ocenę m.in. legalności wysyłania zaproszeń na badania przesiewowe.
- **Oparcie także w Kodeksie postępowania:** Prezes UODO przypomniał, że w **Kodeksie postępowania dla sektora ochrony zdrowia** wskazano, iż **zgoda pacjenta nie jest wymagana**, gdy przetwarzanie danych służy celom zdrowotnym (w tym profilaktyce).
- **Przykłady działań profilaktycznych:** do takich działań można zaliczyć m.in. **wysyłanie zaproszeń na badania przesiewowe** oraz **szczepienia** realizowane zgodnie z Programem Szczepień Ochronnych.
- **Ograniczenie dotyczące Kodeksu:** kodeks może być argumentem potwierdzającym spełnianie obowiązków przez administratora danych **tylko wtedy, gdy administrator jest członkiem tego kodeksu**.
- **Wątpliwości wokół Internetowego Konta Pacjenta (IKP):** obecne przepisy nie określają jednoznacznie, **w jaki sposób** podmioty medyczne miałyby przekazywać pacjentom informacje profilaktyczne przez IKP, mimo że ustawa przewiduje dostęp pacjenta do informacji o profilaktyce i zdrowym trybie życia.
- **Wniosek dot. IKP:** Prezes UODO wskazał na potrzebę **zmiany przepisów**, aby IKP mogło służyć także podmiotom medycznym jako narzędzie komunikacji profilaktycznej (w tym wysyłania zaproszeń na badania).
- **Wątek badań naukowych i danych pseudonimowych:** Prezes UODO odniósł się też do potrzeby uregulowania przetwarzania **danych pseudonimowych** na potrzeby badań naukowych.
- **Dostosowanie do nowych przepisów UE:** wskazano konieczność dostosowania polskich regulacji do **rozporządzenia 2025/327** o Europejskiej Przestrzeni Danych Dotyczących Zdrowia, które dopuszcza przetwarzanie takich danych w jasno uzasadnionych i niezbędnych przypadkach dla badań naukowych.
- **Ochrona praw pacjentów:** zgodnie z art. 89 RODO przetwarzanie danych do celów naukowych wymaga zabezpieczeń chroniących prawa i wolności osób, których dane dotyczą, w tym wdrożenia środków technicznych i organizacyjnych oraz realizacji zasady **minimalizacji danych**.
- **Działania legislacyjne:** 1 września 2025 r. Prezes UODO wystąpił do Ministra Zdrowia o podjęcie prac nad podstawą prawną umożliwiającą udostępnianie danych medycznych w formacie zabezpieczonym m.in. przez „**klucz kodujący**” (który ma uniemożliwiać odwracalne odkodowanie przez odbiorcę, a pozostaje w posiadaniu podmiotu udostępniającego dane).
- **Odpowiedź Ministerstwa Zdrowia:** Minister Zdrowia zadeklarował **otwartość na współpracę** z UODO w tym zakresie.
- **Dalszy krok:** Prezes UODO oczekuje jeszcze na stanowisko **Ministra Nauki**.

Źródło: <https://uodo.gov.pl/pl/138/4126>