





RODO - aktualności

Data publikacji: 17.01.2025

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.

01

PUODO: Numery ksiąg wieczystych stanowią dane osobowe

02

Włoski organ nadzorczy nakłada 15 000 000 euro kary na OpenAI LLC

03

Komisja Europejska upomniana za kampanię w mediach społecznościowych

04

Nowe technologie w ryzach prawnych. Czy w 2025 r. zmierzmy się z przepisami na miarę RODO?

05

Zmiany organizacyjne w Urzędzie Ochrony Danych Osobowych

06

Gawkowski: Do końca stycznia sprawdzanie uprawnień kierowców będzie zautomatyzowane

07

TSUE: Tożsamość płciowa klienta nie należy do danych niezbędnych do zakupu biletu

08

CNIL: 240 000 euro za skopiowanie 160 mln danych kontaktowych z LinkedIn

09

Sąd UE: przyznał zadośćuczynienie za przekazanie danych

10

Największy atak hakerski w historii Słowacji. Przestępcy żądają okupu od rządu

11

Litwiński: Prywatna osoba publikująca w internecie podlega RODO

12

Anonimowość sygnalisty zagrożona przez opłatę skarbową. Co na to ministerstwo?

13

NSA potwierdził - bank nie może przetwarzać danych na zapas

14

Plan kontroli sektorowych UODO na 2025 rok

O naszej książce: poznaj RODOLOGIE

- ✔ Autorska koncepcja pięciu filarów
- ✔ Gotowe sprawdzone rozwiązania
- ✔ Automatyzacja rozwiązań
- ✔ Prosty język, przykłady i schematy
- ✔ Myślenie procesowe by default
- ✔ Ponad 500 stron w pięknej, premium formie



Razem z książką otrzymasz dostęp do aplikacji SODO z Modelowym RCP

01 PUODO: Numery ksiąg wieczystych stanowią dane osobowe.

- **Kontekst sprawy:** Były Główny Geodeta Kraju (GGK) nie zgadza się z decyzją Prezesa Urzędu Ochrony Danych Osobowych (UODO), który zakazał publikowania numerów ksiąg wieczystych w serwisie Geoportal2 i nałożył za to karę.
- **Stanowisko UODO:** Prezes UODO podkreślił, że numery ksiąg wieczystych stanowią dane osobowe zgodnie z przepisami RODO, ponieważ umożliwiają łatwy dostęp do danych takich jak imiona, nazwiska, numery PESEL czy adresy nieruchomości.
- **Potwierdzenie przez sąd:** Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 5 maja 2021 r. (sygn. akt II Sa/Wa 2222/20) potwierdził stanowisko UODO, uznając numery ksiąg wieczystych za dane osobowe.
- **Brak podstaw do zmiany decyzji:** Prezes UODO w odpowiedzi na wniosek byłego GGK zaznaczył, że nie ma przesłanek do uchylenia lub zmiany decyzji w tej sprawie.
- **Uniemożliwienie kontroli:** Były GGK uniemożliwił pracownikom UODO przeprowadzenie kontroli, za co również został ukarany. Wojewódzki Sąd Administracyjny 23 lutego 2021 r. (sygn. akt II Sa/Wa 1746/20) uznał to działanie za brak znajomości obowiązujących przepisów przez organ publiczny.
- **Przypomnienie konsekwencji:** UODO przypomina, że ujawnianie numerów ksiąg wieczystych naraża na ryzyko przypadki, w których można uzyskać poufne dane osobowe właścicieli nieruchomości.

Źródło: <https://uodo.gov.pl/pl/138/3497>

02 Włoski organ nadzorczy nakłada 15 000 000 euro kary na OpenAI LLC.

- **Kontekst:** Włoski organ nadzorczy ds. ochrony danych osobowych (Garante) nałożył na OpenAI, właściciela usługi ChatGPT, administracyjną karę pieniężną w wysokości 15 milionów euro w związku z naruszeniami przepisów RODO.
- **Przyczyna postępowania:** Postępowanie zostało wszczęte po zgłoszeniach o błędzie technicznym (20 marca 2023 r.), który umożliwił użytkownikom dostęp do historii czatów oraz części danych osobowych innych osób, takich jak imię, nazwisko, adres e-mail, a także dane karty kredytowej powiązanej z płatną wersją ChatGPT Plus.
- **Działania organu nadzorczego:**
 - W kwietniu 2023 r. wydano postanowienie o czasowym ograniczeniu przetwarzania danych przez OpenAI, wymagając jednocześnie wdrożenia środków zapewniających zgodność z RODO.
 - Przekazano sprawę do irlandzkiego organu ochrony danych w związku z jurysdykcją po rejestracji OpenAI w Irlandii.
- **Stwierdzone naruszenia:**
 - Brak odpowiedniej analizy adekwatności i podstaw prawnych przetwarzania danych przed uruchomieniem ChatGPT (art. 5 ust. 2 i art. 6 RODO).
 - Brak spełnienia obowiązku informacyjnego wobec użytkowników (art. 12 i 13 RODO).
 - Niepodjęcie odpowiednich technicznych i organizacyjnych środków ochrony danych (art. 24 i 25 RODO).

Źródło: <https://judykatura.pl/wloski-organ-nadzorczy-naklada-15-000-000-euro-kary-na-openai-llc/>

02 cd. Włoski organ nadzorczy nakłada 15 000 000 euro kary na OpenAI LLC.

- **Argumentacja decyzji:** Uruchomienie usługi przetwarzającej dane osobowe na dużą skalę bez minimalnych środków ochrony danych zostało uznane za poważne naruszenie zasad RODO.
- **Kwota kary:** Kara administracyjna wyniosła 15 milionów euro, co stanowi około 1,58% całkowitego rocznego światowego obrotu OpenAI za rok 2023 (948,5 mln euro).
- **Kolejny etap:** Irlandzki organ nadzorczy ma ocenić, czy europejska jednostka OpenAI posiada odpowiednią podstawę prawną do przetwarzania danych osobowych, w tym uzasadniony interes.

Źródło: <https://judykatura.pl/wloski-organ-nadzorczy-naklada-15-000-000-euro-kary-na-openai-llc/>

03 Komisja Europejska upomniana za kampanię w mediach społecznościowych.

- **Kontekst sprawy:** Komisja Europejska (KE) została upomniana przez Europejskiego Inspektora Ochrony Danych (EIOD) za naruszenie przepisów RODO w trakcie kampanii reklamowej w mediach społecznościowych.
- **Cel kampanii:** Promowanie projektu rozporządzenia dotyczącego zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczania (CSAM).
- **Zakres kampanii:**
 - Reklamy były mikrotargetowane do użytkowników serwisu X (dawniej Twitter) z Holandii, mówiących po niderlandzku i mających powyżej 18 lat.
 - Profilowanie użytkowników oparto na 44 kryteriach, z których 36 dotyczyło opinii politycznych lub partii politycznych, a 6 – przekonań religijnych.
 - Kampania była prowadzona od 18 do 27 września 2023 r. i wyświetlono ją ponad 600 tys. razy.
- **Skarga NOYB:**
 - Organizacja obrońców prywatności NOYB zgłosiła, że KE naruszyła art. 10 RODO, który zabrania przetwarzania szczególnych kategorii danych osobowych (np. dotyczących opinii politycznych i przekonań religijnych).
 - Zarzuty dotyczyły również naruszenia art. 4 i 5 RODO poprzez brak odpowiedniej podstawy prawnej do przetwarzania danych.
- **Obrona KE:** KE wskazała, że kampanię prowadził zewnętrzny wykonawca, który miał działać zgodnie z przepisami prawa. Komisja nie dostarczyła jednak dowodów na legalność przetwarzania danych.

Źródło: <https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/9695490,komisja-europejska-upomniana-za-kampanie-w-mediach-spolecznosciowych.html>

03 cd. Komisja Europejska upomniana za kampanię w mediach społecznościowych.

- Decyzja EIOD:
 - EIOD stwierdził, że KE nie wykazała podstawy do prawnego przetwarzania danych, w tym danych szczególnych kategorii.
 - Nałożono na KE upomnienie, uznając je za proporcjonalną odpowiedź – m.in. z powodu zaprzestania kampanii.
- **Dalsze kroki:** NOYB złożyło osobną skargę przeciwko platformie X do holenderskiego organu ochrony danych.

Źródło: <https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/9695490.komisja-europejska-upomniana-za-kampanie-w-mediach-spolecznosciowych.html>

04 Nowe technologie w ryzach prawnych. Czy w 2025 r. zmierzmy się z przepisami na miarę RODO?

- **Kontekst:** Od 2023 roku mamy do czynienia z intensywnym „regulacyjnym tsunami” w prawie nowych technologii, które obejmuje takie obszary jak cyberbezpieczeństwo, moderowanie treści w internecie i sztuczna inteligencja. Unia Europejska dąży do wyznaczenia międzynarodowych standardów w tym zakresie, podobnie jak miało to miejsce w przypadku RODO.
- **Polska prezydencja w UE (2025):** Cyberbezpieczeństwo, AI, zarządzanie internetem oraz wdrażanie regulacji cyfrowych zostały określone jako kluczowe priorytety Polski w kontekście prezydencji w UE.
- **Kluczowe akty prawne:**
 - **Digital Services Act (DSA):** Wprowadza nowe obowiązki dla pośredników internetowych, takie jak ujednoczone zasady usuwania treści nielegalnych i możliwość odwoływania się od decyzji o takim usunięciu. Obowiązuje wobec wszystkich od 17 lutego 2024 r. Polska pracuje nad implementacją przepisów.
 - **Dyrektywa NIS2:** Dotyczy krajowego systemu cyberbezpieczeństwa i uznawania dostawców za podmioty wysokiego ryzyka. Wymusi na operatorach wymianę sprzętu i oprogramowania w określonych terminach.
 - **AI Act:** Pierwsza kompleksowa regulacja AI na świecie. Obligacje takie jak analiza ryzyka systemów AI i szkolenia personelu (AI Literacy) wejdą w życie w lutym 2025 r. Przepisy o karach z kolei od sierpnia. To regulacja dotycząca przede wszystkim systemów o wysokim ryzyku, np. rekrutacyjnych czy nadzoru w pracy.
 - **Akt o danych (Data Act):** Wprowadzi zasady ułatwiające zmianę dostawców usług IT, w tym chmury, oraz rozszerzy prawa konsumentów do danych generowanych przez nowe technologie. Będzie obowiązywał od września 2025 r.

Źródło: <https://www.rp.pl/prawo-w-polsce/art41610321-nowe-technologie-w-ryzach-prawnych-czy-w-2025-r-zmierzmy-sie-z-przepisami-na-miare-rod>

04 cd. Nowe technologie w ryzach prawnych. Czy w 2025 r. zmierzmy się z przepisami na miarę RODO?

- **Nowe obowiązki i wyzwania:**
 - Organy krajowe będą odpowiadały za przestrzeganie unijnych przepisów i nakładanie kar. Przykład: Prezes UKE będzie nadzorował internetowych pośredników.
 - Wdrażanie regulacji wiąże się z wysokimi kosztami i czasochłonnymi procesami, szczególnie dla operatorów i mniejszych firm.
- **Ochrona grup wrażliwych:**
 - **Dostępność:** Implementacja Europejskiego Aktu o dostępności od czerwca 2025 r. zobowiąże np. branżę e-commerce do ułatwień dla osób niepełnosprawnych.
 - **Ochrona dzieci:** Przepisy DSA nakładają zakaz profilowania dzieci w reklamach. Polska planuje wprowadzić dodatkowe regulacje dotyczące skutecznej weryfikacji wieku na stronach z treściami szkodliwymi.
- **Rekomendacje:**
 - Zastanów się nad wcześniejszym przygotowaniem do wdrożenia nowych regulacji, szczególnie dot. AI, np. poprzez szkolenia i mapowanie procesów w organizacjach.
 - Świadome podejście do nowych obowiązków pozwoli uniknąć kar, które w niektórych przypadkach będą wyższe niż te przewidziane w RODO.

Źródło: <https://www.rp.pl/prawo-w-polsce/art41610321-nowe-technologie-w-ryzach-prawnych-czy-w-2025-r-zmierzmy-sie-z-przepisami-na-miare-rodou>

05 Zmiany organizacyjne w Urzędzie Ochrony Danych Osobowych.

- **Kontekst:** Prezes Mirosław Wróblewski wprowadził zmiany organizacyjne w Urzędzie Ochrony Danych Osobowych (UODO), które mają na celu usprawnienie działania Urzędu oraz skrócenie czasu rozpatrywania spraw.
- **Cel zmian:** Zwiększenie skuteczności działań UODO, podnoszenie świadomości społeczeństwa na temat ochrony danych osobowych oraz intensyfikacja współpracy międzynarodowej.
- **Data obowiązywania:** Zmiany weszły w życie 1 stycznia 2025 roku.
- **Nowe departamenty i ich zadania:**
 - Departament Wstępnej Kontroli Skarg i Naruszeń – zajmuje się wstępną weryfikacją skarg i zgłoszeń oraz prowadzeniem infolinii.
 - Departament Współpracy Międzynarodowej – odpowiedzialny za współpracę na forum międzynarodowym, postępowania transgraniczne, transfery danych oraz certyfikacje.
 - Departament Inicjatyw Edukacyjnych – skoncentrowany na edukacji w zakresie ochrony danych, organizacji szkoleń, konferencji oraz popularyzacji wiedzy.
 - Departament Projektów Społecznych i Zrównoważonego Rozwoju – rozwija współpracę z organizacjami społecznymi i realizuje regionalne inicjatywy w ramach programu "UODO rusza w kraj".
 - Departament Prawa i Nowych Technologii – zajmuje się analizą nowych technologii i ich wpływu na ochronę danych osobowych oraz oceną stanowionego prawa.

Źródło: <https://uodo.gov.pl/pl/138/3498>

05 Zmiany organizacyjne w Urzędzie Ochrony Danych Osobowych.

- **Powód zmian:** Podjęto je na podstawie analizy działania UODO oraz rozmów z pracownikami, aby dostosować jednostki do nowych wyzwań i wymogów prawnych.
- **Przyszłość UODO:** Wdrażanie nowych zadań związanych z unijnym Aktem o zarządzaniu danymi wymaga dalszego wzmocnienia Urzędu i jego zasobów.

Źródło: <https://uodo.gov.pl/pl/138/3498>

06 Gawkowski: Do końca stycznia sprawdzanie uprawnień kierowców będzie zautomatyzowane.

- **Kontekst:** Ministerstwo cyfryzacji wprowadza zmiany w procesie weryfikacji uprawnień kierowców, co ma na celu zwiększenie bezpieczeństwa na drogach oraz poprawę nadzoru nad pracownikami branży transportowej.
- **Automatyzacja procesu:** Zautomatyzowany system weryfikacji uprawnień będzie dostępny dla przedsiębiorców do końca stycznia. Informacje na temat działania systemu zamieści wicepremier i minister cyfryzacji Krzysztof Gawkowski na stronie resortu.
- **Funkcjonalność systemu:** Zmieniona Centralna Ewidencja Pojazdów i Kierowców (CEPIK) pozwoli przedsiębiorcom codziennie monitorować uprawnienia kierowców pracujących dla ich firm.
- **Udostępniane narzędzia:** Przedsiębiorstwa otrzymają tzw. "wtyczkę" umożliwiającą integrację i monitorowanie uprawnień w czasie rzeczywistym. Proces instalacji tego rozwiązania ma być szybki, zajmując zaledwie kilkadziesiąt minut.
- **Skala wykorzystania danych:** Co roku CEPIK obsługuje 25-30 mln zapytań od firm i instytucji, co podkreśla znaczenie tych danych dla administracji i przedsiębiorstw.
- **Dedykacja dla dużych firm:** Nowe rozwiązania mają szczególnie wspierać duże przedsiębiorstwa transportowe, podczas gdy małe firmy mogą już teraz samodzielnie weryfikować swoich kierowców.
- **Bezkompromisowe egzekwowanie prawa:** Ministerstwo, we współpracy z prokuraturą, policją i służbami specjalnymi, zapewnia, że zmiany umożliwią skuteczną walkę z naruszaniem przepisów drogowych.

Źródło: <https://www.bankier.pl/wiadomosc/Gawkowski-Do-konca-stycznia-sprawdzanie-uprawnien-kierowcow-bedzie-zautomatyzowane-8870459.html>

06 Gawkowski: Do końca stycznia sprawdzanie uprawnień kierowców będzie zautomatyzowane.

- **Reakcja na tragiczny wypadek:** Decyzja ministerstwa to odpowiedź na piątkowy wypadek w Warszawie, podczas którego kierowca z sądowym zakazem prowadzenia pojazdów śmiertelnie potrącił pieszą na pasach.
- **Brak zmian w ustawie:** Wprowadzane udoskonalenia w CEPIK-u nie wymagają żadnych zmian legislacyjnych, co przyspiesza ich wdrożenie.

Źródło: <https://www.bankier.pl/wiadomosc/Gawkowski-Do-konca-stycznia-sprawdzanie-uprawnien-kierowcow-bedzie-zautomatyzowane-8870459.html>

07 TSUE: Tożsamość płciowa klienta nie należy do danych niezbędnych do zakupu biletu.

- **Kontekst sprawy:** Trybunał Sprawiedliwości Unii Europejskiej (TSUE) podkreślił, że zbieranie danych osobowych, takich jak forma grzecznościowa („Pan” lub „Pani”), musi być zgodne z zasadą minimalizacji danych wynikającą z RODO. Sprawa dotyczyła praktyki przedsiębiorstwa kolejowego SNCF Connect we Francji.
- **Stanowisko Trybunału:** Personalizacja komunikacji handlowej na podstawie form grzecznościowych nie jest obiektywnie konieczna do zawarcia i realizacji umowy na zakup biletu kolejowego.
- **Alternatywa:** Trybunał wskazał, że wystarczającym i mniej inwazyjnym rozwiązaniem mogłaby być komunikacja oparta na neutralnych i ogólnych zwrotach grzecznościowych, bez konieczności odniesienia do tożsamości płciowej klientów.
- **Zasada minimalizacji danych:** Dane gromadzone przez przedsiębiorstwa muszą być adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane.
- **Zgodność z RODO:** Zgodne z prawem przetwarzanie danych wymaga, aby realizowany „prawnie uzasadniony interes” był komunikowany klientom, oraz aby dane były przetwarzane wyłącznie w granicach niezbędnych do realizacji tego interesu, z uwzględnieniem ochrony praw klientów.
- **Ochrona praw podstawowych:** TSUE podkreślił, że prawa i wolności osób, których dane dotyczą, mogą mieć nadrzędne znaczenie w przypadku ryzyka dyskryminacji, np. ze względu na tożsamość płciową.
- **Konsekwencje wyroku:** Orzeczenie TSUE w sprawie C-394/23 (Mousse) ma znaczenie nie tylko dla Francji, ale również dla innych krajów UE, w tym Polski. Może ono wpłynąć na praktyki dotyczące przetwarzania danych osobowych w sektorze usług.

Źródło: <https://www.prawo.pl/prawo/tozsamosc-plciowa-klienta-nie-nalezy-do-danych-niezbednych-do-zakupu-biletu-tsue-c-39423,530864.html>

08 CNIL: 240 000 euro za skopiowanie 160 mln danych kontaktowych z LinkedIn.

- **Kontekst:** Decyzja francuskiego organu nadzorczego (CNIL) dotyczy działań firmy KASPR, założonej w 2018 roku w Paryżu. Firma oferuje rozszerzenie przeglądarki umożliwiające uzyskanie zawodowych danych kontaktowych użytkowników serwisu LinkedIn.
- **Cel rozszerzenia KASPR:** Oprogramowanie pozwala użytkownikom (klientom firmy) na odwiedzanie profili w serwisie LinkedIn oraz uzyskiwanie danych takich jak:
 - adres e-mail,
 - numer telefonu,
 - pracodawca, stanowisko, umiejętności, zainteresowania zawodowe, kariera, i inne szczegóły zawodowe.
- **Zakres zebrania danych:** Firma KASPR zebrała dane dotyczące ponad 160 milionów kontaktów z serwisu LinkedIn, przetwarzając dane dwóch grup osób:
 - Osób docelowych, których dane zawodowe zostały zebrane.
 - Użytkowników rozszerzenia, czyli klientów firmy.
- **Prawna podstawa przetwarzania:**
 - KASPR uzasadnia zbieranie danych „uzasadnionym interesem” działalności komercyjnej firmy.
 - CNIL zauważył, że ten interes nie może przeważać nad prawami i wolnościami osób, których dane dotyczą.

Źródło: <https://judykatura.pl/cnil-240-000-euro-za-skopiowanie-160-mln-danych-kontaktowych-z-linkedin/>

08 cd. CNIL: 240 000 euro za skopiowanie 160 mln danych kontaktowych z LinkedIn.

- **Zastrzeżenia organu nadzorczego:**
 - Osoby, które ograniczyły widoczność swoich danych na LinkedIn, mają prawo oczekiwać, że ich dane nie będą pozyskiwane przez podmioty zewnętrzne.
 - KASPR nie poinformował odpowiednio osób docelowych o zbieraniu ich danych ani nie podjął wystarczających działań, aby zmniejszyć ryzyko naruszenia ich praw.
 - Zbieranie danych bez zgody osób docelowych narusza art. 6 RODO, ponieważ nie ma uzasadnionej prawnej podstawy.
- **Wnioski:** CNIL uznał, że działalność firmy KASPR w zakresie zbierania danych kontaktowych osób, które zdecydowały się ograniczyć widoczność swoich danych, nie spełnia wymogów RODO oraz odpowiednich regulacji dotyczących ochrony danych osobowych.

Źródło: <https://judykatura.pl/cnil-240-000-euro-za-skopiowanie-160-mln-danych-kontaktowych-z-linkedin/>

09 Sąd UE: przyznał zadośćuczynienie za przekazanie danych.

- **Kontekst sprawy:** Sąd Unii Europejskiej wydał wyrok obowiązujący Komisję Europejską do zapłaty 400 euro zadośćuczynienia za naruszenie prawa w przetwarzaniu danych osobowych obywatela Niemiec. Podstawą przetwarzania danych były przepisy Rozporządzenia (UE) 2018/1725, analogicznego do RODO.
- **Skarżący obywatel Niemiec:** Podważył legalność przekazania swoich danych osobowych do podmiotów w państwach trzecich niewystarczająco chroniących dane. Domagał się także wyjaśnień w sprawie podstaw prawnych przetwarzania jego danych oraz ich przekazywania.
- **Chronologia działań skarżącego:** Wielokrotnie korzystał ze strony internetowej Komisji Europejskiej, rejestrując się na wydarzenia oraz zauważając połączenia z zewnętrznymi dostawcami, m.in. Amazon Web Services. W listopadzie 2021 r. zwrócił się z formalnym żądaniem informacji na temat przetwarzania swoich danych.
- **Zarzuty bezczynności Komisji:** Skarżący wskazał, że Komisja nie odpowiedziała na jego żądania dotyczące dostępu do informacji oraz zaniechała podjęcia działań w terminie. Komisja uznała część zarzutów za bezprzedmiotowe po udzieleniu odpowiedzi.
- **Kryteria odpowiedzialności Unii:** Unia Europejska jest odpowiedzialna za naruszenia prawa, jeśli spełnione zostaną trzy warunki: bezprawność działania instytucji, powstanie rzeczywistej szkody oraz związek przyczynowy między tym działaniem a szkodą.
- **Rozstrzygnięcie Sądu UE:** Sąd uznał zasadność części skargi skarżącego i przyznał mu 400 euro odszkodowania. Komisja została zobowiązana do zadośćuczynienia za to, że dopuściła się naruszeń podczas przetwarzania danych osobowych.

Źródło: <https://judykatura.pl/sad-ue-przyznal-zadoscuczynienie-za-przekazanie-danych/>

10 Największy atak hakerski w historii Słowacji. Przestępcy żądają okupu od rządu.

- **Kontekst ataku:** Słowacki Urząd Geodezji, Kartografii i Katastru padł ofiarą bezprecedensowego ataku typu ransomware, który doprowadził do paraliżu systemu ewidencji nieruchomości. Hakerzy zaszyfrowali dane i zażądali wielomilionowego okupu w dolarach.
- **Skutki dla obywateli i administracji:**
 - Brak dostępu do rejestru nieruchomości uniemożliwia zaciąganie kredytów hipotecznych, dokonywanie zmian meldunkowych i uzyskiwanie pozwoleń na budowę.
 - Problemy w systemie administracyjnym i bankowym wywołały efekt domina, wpływając na codzienne funkcjonowanie obywateli.
 - Brak kompleksowych kopii zapasowych danych może wydłużyć proces przywracania systemu, a część danych może być nieodwracalnie utracona.
- **Stan techniczny urzędu:** Były szef urzędu wskazał na przestarzałą infrastrukturę informatyczną – komputery z 2008 roku i niedobór ekspertów IT.
- **Spekulacje na temat sprawców:**
 - Premier Robert Fico sugeruje, że atak może pochodzić z terytorium Ukrainy lub być wynikiem działań wewnętrznych pracowników urzędu.
 - Według słowackiej Rady Bezpieczeństwa, napastnicy żądają siedmiocyfrowej kwoty w dolarach za przywrócenie dostępu do danych.
 - Zdarzenie porównano do podobnego incydentu w Rosji, co może świadczyć o działaniu tej samej grupy przestępczej.

Źródło: <https://www.money.pl/gospodarka/najwiekszy-cyberatak-w-historii-slowacji-sparalizowane-banki-i-urzedysprawcy-zadaja-okupu-7112808333286112a.html>

10 cd. Największy atak hakerski w historii Słowacji. Przestępcy żądają okupu od rządu.

- **Działania władz:**
 - Minister rolnictwa zapewnia, że urzędowe kopie zapasowe minimalizują ryzyko utraty majątków obywateli, choć proces odzyskiwania danych może być długotrwały.
 - Władze zapowiedziały stopniowe przywracanie funkcjonalności systemu od przyszłego tygodnia, z regionalnymi urzędami działającymi jako niezależne jednostki.
 - Biuro ds. Zwalczania Przemoczości Zorganizowanej prowadzi śledztwo w sprawie nieuprawnionej ingerencji w system komputerowy.
- **Możliwe konsekwencje w dłuższym terminie:**
 - Wstrzymanie transakcji nieruchomościowych.
 - Pojawienie się sporów prawnych dotyczących własności.
 - Długoterminowy chaos w rejestrach nieruchomości.
- **Eksperska opinia:** Łukasz Olejnik, ekspert ds. cyberbezpieczeństwa, ocenia incydent jako znaczący problem dla funkcjonowania całego państwa, wskazując na niedostateczne zabezpieczenia systemowe.

Źródło: <https://www.money.pl/gospodarka/najwiekszy-cyberatak-w-historii-slowacji-sparalizowane-banki-i-urzedysprawcy-zadaja-okupu-7112808333286112a.html>

11

Litwiński: Prywatna osoba publikująca w internecie podlega RODO.

- **Kontekst:** Wyrok Naczelnego Sądu Administracyjnego (sygn. akt III OSK 4984/21) oraz jego uzasadnienie przypominają, że każdy, kto publikuje dane osobowe w internecie, staje się ich administratorem zgodnie z RODO, nawet w przypadku działalności prywatnej.
- **Zasadnicza kwestia:** RODO nie ogranicza obowiązków dotyczących przetwarzania danych wyłącznie do celów zarobkowych czy działalności gospodarczej – dotyczy także działań prywatnych, takich jak publikowanie zdjęć w internecie, na których można rozpoznać osoby.
- **Obowiązki administratora danych:**
 - Teoretycznie, administrator powinien spełniać obowiązek informacyjny wobec osób, których dane przetwarza, np. na zdjęciach.
 - W praktyce, jeśli obowiązek ten jest niemożliwy do spełnienia (np. brak danych kontaktowych przypadkowych osób), nie jest wymagany.
- **Przykłady:**
 - Wrzucenie zdjęcia z jarmarku, na którym są przypadkowe osoby w tle, jest możliwe dzięki przepisom prawa autorskiego. RODO pozwala na takie publikacje, ale należy być świadomym potencjalnego żądania usunięcia danych przez osoby rozpoznawalne.
 - Jeśli osoba na zdjęciu zgłosi sprzeciw wobec publikacji, administrator musi ocenić konflikt interesów – swoją potrzebę publikacji wobec prawa do ochrony prywatności tej osoby.
- **Ważne wyjątki:**
 - Publikowanie danych w zamkniętych grupach internetowych (np. wyłącznie w gronie znajomych) może podlegać wyłączeniu z zakresu stosowania RODO.

Źródło: <https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/9707452.litwinski-prywatna-osoba-publikujaca-w-internecie-podlega-rod0-wywia.html>

11

cd. Litwiński: Prywatna osoba publikująca w internecie podlega RODO.

- Publikowanie w szerszym, nieograniczonym kręgu odbiorców (np. publiczne posty na Facebooku) skutkuje jednak stosowaniem przepisów RODO.
- **Praktyczny wymiar:** Większość przypadków publikowania danych przez osoby prywatne nie powoduje automatycznego naruszenia RODO, a znaczące zaangażowanie w przepisy rozporządzenia dotyczy głównie konfliktów (np. sąsiedzkich lub rodzinnych).
- **Podsumowanie:** Wyrok NSA przypomina, że prawie każdy z nas w pewnym momencie staje się administratorem danych osobowych. Jednak w większości przypadków nie wiąże się to z dodatkowymi obowiązkami, a przepisy RODO są stosowane z umiarem.

Źródło: <https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/9707452,litwinski-privatna-osoba-publikujaca-w-internecie-podlega-rodow-wywia.html>

12 Anonimowość sygnalisty zagrożona przez opłatę skarbową. Co na to ministerstwo?

- **Kontekst:** Przepisy o ochronie sygnalistów weszły w życie 25 września zeszłego roku, a mechanizmy zewnętrzne umożliwiające zgłaszanie nieprawidłowości uruchomiono 25 grudnia. Przepisy te mają zapewnić sygnalistom poufność i bezpieczeństwo.
- **Problem:** Luka w przepisach może prowadzić do ujawnienia danych sygnalisty w trakcie procedury związanej z wydaniem zaświadczenia potwierdzającego ochronę. Tożsamość sygnalisty staje się znana organom podatkowym w związku z wymogiem uiszczenia opłaty skarbowej.
- **Obowiązek opłaty skarbowej:** W celu wydania zaświadczenia sygnalista musi podać swoje dane osobowe (PESEL, imię, nazwisko, adres) i dowód zapłaty opłaty skarbowej. W przypadku braku wniesienia opłaty, dane są przekazywane organom podatkowym, co może ujawnić tożsamość sygnalisty.
- **Apel prawników:** Ekspertki postulują nowelizację przepisów, w tym zwolnienie zaświadczeń dla sygnalistów z opłat skarbowych, aby zapewnić pełną ochronę danych osobowych i poufność.
- **Stanowisko Ministerstwa Rodziny:** Resort zaleca interpretację przepisów zakładającą, że zaświadczenie wydane w interesie publicznym powinno być zwolnione z opłaty skarbowej. Jednak taka wykładnia budzi wątpliwości natury prawnej.
- **Przyszłe zmiany:** Prezes UODO zapowiada prace legislacyjne mające na celu poprawę przepisów dotyczących przetwarzania danych osobowych, co może pomóc rozwiązać problem ochrony tożsamości sygnalistów.
- **Kluczowy wniosek:** Konieczna jest szybka interwencja ustawodawcza, aby ochronić sygnalistów przed potencjalnym naruszeniem poufności i prywatności w ramach obecnie istniejących procedur.

Źródło: <https://www.rp.pl/dane-osobowe/art41666161-anonimowosc-sygnalisty-zagrozona-przez-oplate-skarbowa-co-na-to-ministerstwo>

13 NSA potwierdził - bank nie może przetwarzać danych na zapas.

- **Kontekst:** Naczelny Sąd Administracyjny (NSA) w Warszawie podtrzymał decyzję Prezesa Urzędu Ochrony Danych Osobowych (UODO) w sprawie niezgodnego z prawem przetwarzania danych osobowych przez Bank Millennium.
- **Główna decyzja:** Sąd uznał, że bank nie może przetwarzać danych byłych klientów na podstawie art. 6 ust. 1 lit. f RODO w celu „zabezpieczenia się” przed ewentualnymi i niepewnymi roszczeniami w przyszłości.
- **Kluczowe argumenty:**
 - Przetwarzanie danych musi opierać się na istniejącym i uzasadnionym interesie prawnym, a nie na hipotetycznych sytuacjach mogących wystąpić w przyszłości.
 - Bank Millennium nie wykazał, że istnieje jakikolwiek spór czy roszczenie ze strony byłych klientów, które uzasadniałoby dalsze przetwarzanie ich danych.
- **Stanowisko Prezesa UODO:** Decyzja organu nadzorczego nakazała bankowi usunięcie danych byłych klientów, gdyż przetwarzano je „na zapas”, co mogłoby prowadzić do ich permanentnego przetwarzania.
- **Przypadek byłych klientów:** Bank Millennium przetwarzał dane osobowe osób, które zamknęły swoje konta i wyraziły sprzeciw wobec działań marketingowych banku, mimo braku podstaw prawnych.
- **Zasady przetwarzania:** NSA przypomniał, że art. 6 ust. 1 lit. f RODO wymaga spełnienia trzech warunków, w tym nadrzędności interesu administratora nad prawami osoby, której dane dotyczą - w tej sprawie warunki te nie zostały spełnione.

Źródło: <https://uodo.gov.pl/pl/138/3510>

13 cd. NSA potwierdził - bank nie może przetwarzać danych na zapas.

- **Obowiązki administratora:** Zgodnie z zasadą rozliczalności, administrator danych (bank) odpowiada za przedstawienie podstaw prawnych przetwarzania danych i udowodnienia zgodności swoich działań z przepisami.
- **Podsumowanie:** Naczelny Sąd Administracyjny potwierdził, że ewentualne, przyszłe roszczenia nie mogą stanowić podstawy do trwałego przechowywania danych osobowych. Bank Millennium został zobowiązany usunąć dane klientów, a wyrok NSA podkreśla ważność przestrzegania zasad RODO, w szczególności rozliczalności i ochrony praw osób, których dane dotyczą.

Źródło: <https://uodo.gov.pl/pl/138/3510>

14 Plan kontroli sektorowych UODO na 2025 rok.

- **Kontekst:** Urząd Ochrony Danych Osobowych (UODO) w 2025 roku skupi swoją działalność kontrolną na obszarach szczególnie istotnych z punktu widzenia bezpieczeństwa danych osobowych. Wybrano sektory, gdzie istnieje ryzyko naruszeń lub które budzą silne zainteresowanie społeczne.
- **Główne obszary kontroli:**
 - **Wielkoskalowe Systemy Unii Europejskiej:** Przetwarzanie danych w systemach takich jak Schengen Information System (SIS) i Visa Information System (VIS), zgodnie z przepisami krajowymi i unijnymi.
 - **Dane o stanie zdrowia:** Ocena sposobów zapewnienia bezpieczeństwa danych osobowych przetwarzanych przez podmioty medyczne.
 - **Dane dzieci:** Kontrola przetwarzania wizerunku dzieci, szczególnie w sytuacjach wymagających zgody rodziców lub opiekunów prawnych.
 - **Dokumentowanie naruszeń danych:** Sprawdzanie, czy administratorzy realizują obowiązek dokumentowania naruszeń danych, ich okoliczności oraz podejmowanych działań zaradczych.
- **Cel kontroli:** Ochrona prywatności i bezpieczeństwa danych osobowych w wybranych sektorach, ze szczególnym uwzględnieniem aktualnych zagrożeń i społecznych oczekiwań.
- Plan UODO na 2025 rok jest odpowiedzią na nowe wyzwania związane z ochroną danych w szybko zmieniającym się otoczeniu prawnym i technologicznym.

Źródło: <https://uodo.gov.pl/pl/138/3513>

*Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,
w szczególności rozpowszechniany i kopiowany.*