# RODO Aktualności

Data publikacji: 06.10.2026

**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. Kamera nagrywa cudzą działkę? NSA: zaczernienie obrazu nie wystarczy
2. Przejrzystość, skuteczność i codzienność. Ochrona danych w zamówieniach publicznych
3. Austriacki Sąd Najwyższy pyta o przekazanie procesorowi
4. TSUE: pytanie o granice systemu zdrowotnego
5. Szwedzki Organ Ochrony Danych nałożył 1,8 mln koron kary na dostawcę systemów kadrowych
6. Skarbówka kontra prywatność obywateli. Poselski projekt zgodny z postulatami Prezesa UODO
7. Miliony Polaków poszkodowane. Po nowym wycieku danych medycznych PUODO zapowiada kontrolę
8. Niezapewnienie dostępu do danych osobowych i informacji może skutkować nałożeniem kary
9. NSA: prywatny komputer nie zwalnia administratora
10. Po karze dla hurtowni leków UODO pyta o dane pacjentów z aptek

# Kamera nagrywa cudzą działkę? NSA: zaczernienie obrazu nie wystarczy

- **Kontekst:** Artykuł dotyczy sporu sąsiedzkiego o monitoring wizyjny. **Naczelny Sąd Administracyjny (NSA) uznał, że objęcie kamerą cudzej nieruchomości (lub drogi prowadzącej do niej) jest przetwarzaniem danych osobowych w rozumieniu RODO** – **nawet jeśli zastosowano tzw. „maskę prywatności" (cyfrowe zaczernienie fragmentu obrazu)**.
- **Co było przedmiotem skargi:** Kobieta zarzuciła, że kamery z sąsiedniej posesji rejestrują jej bramę i furtkę oraz fragment działki i drogi dojazdowej, przez co mogą utrwalać m.in. **wizerunek domowników, tablice rejestracyjne oraz tabliczkę adresową**.
- **Reakcja właścicieli kamer:** Kobieta wielokrotnie prosiła o przestawienie kamer tak, aby obejmowały tylko nieruchomość sąsiadów, ale bezskutecznie.
- **Decyzja Prezesa UODO:** Organ przyznał rację skarżącej i **nakazał zaprzestanie przetwarzania jej danych osobowych** za pomocą monitoringu.
- **Ustalenia UODO o monitoringu:**
  - system miał **dysk twardy** i umożliwiał **ciągłe nagrywanie** oraz przechowywanie nagrań przez **48 godzin**;
  - **pole widzenia kamer** obejmowało także **prywatną drogę dojazdową** i **fragment posesji** skarżącej.

- **„Maska prywatności" nie przekonała UODO:** Właściciel kamer twierdził, że zastosował zaczernienie, ale **nie wykazał, że było ono stałe i skutecznie chroniło prywatność**.
- **Wyrok WSA w Warszawie:** Sąd utrzymał decyzję UODO. Wskazał, że właściciel monitoringu nie zastosował **wystarczających i pewnych środków technicznych i fizycznych**, by nie pozyskiwać danych osób przebywających na obszarach, które nie powinny być monitorowane (np. wspólna droga dojazdowa).
- **Brak podstawy prawnej:** WSA podkreślił, że właściciel kamer **nie wskazał podstawy prawnej** uzasadniającej przetwarzanie danych osób z sąsiedniej nieruchomości.
- **Argument o bezpieczeństwie rodziców:** Właściciel kamer tłumaczył monitoring potrzebą ochrony rodziców. Sądy uznały jednak, że **ten argument nie wystarcza**, jeśli naruszane są prawa innych osób (w tym osoby, która **nie wyraziła zgody** na taki sposób „zapewniania bezpieczeństwa").
- **Stanowisko NSA:** NSA oddalił skargę właściciela kamer i wskazał, że **prawa do prywatności, ochrony wizerunku, danych osobowych i życia rodzinnego** są w tej sprawie **ważniejsze niż hipotetyczne zagrożenie**, na które powoływał się skarżący.
- **Proporcjonalność działań:** NSA podkreślił, że ograniczanie wolności i prywatności wymaga spełnienia **rygorystycznych wymogów proporcjonalności**, które w tej sprawie nie zostały zachowane.
- **Kluczowy wniosek NSA o „masce prywatności":** Zastosowanie cyfrowego zaczernienia **nie wyłącza faktu przetwarzania danych**. Istotne jest to, że **kamera obejmuje zasięgiem cudzą nieruchomość** (czyli potencjalnie ją rejestruje), a zaczernienie jest jedynie **operacją na obrazie**.
- **Dlaczego to nadal jest „przetwarzanie" wg RODO:** NSA wskazał, że w takim przypadku dochodzi do operacji takich jak **utrwalanie obrazu**, jego **modyfikacja** (zaczernienie) i **zapis**. To spełnia definicję przetwarzania danych z art. 4 RODO.
- **Nie ma znaczenia techniczny szczegół zaczernienia:** Według NSA bez znaczenia pozostaje, czy zaczernienie jest **odwracalne** czy **nieodwracalne**, trwałe czy chwilowe – jeśli zasięg kamery obejmuje cudzy teren, wchodzi w grę przetwarzanie danych osobowych.
- **Sygnatura i data:** Wyrok NSA z **8 września 2026 r.**, sygn. akt **III OSK 649/24**.

Źródło: https://edgp.gazetaprawna.pl/prawo/prawo-internetu-i-ochrony-danych/artykuly/11316278,kamera-nagrywa-cudza-dzialke-naczelny-sad-administracyjny-zaczernien.html

# Przejrzystość, skuteczność i codzienność. Ochrona danych w zamówieniach publicznych

- **Kontekst:** 18 września odbyła się druga konferencja z cyklu „Ochrona danych w zamówieniach publicznych”, zorganizowana wspólnie przez Urząd Zamówień Publicznych (UZP) oraz Urząd Ochrony Danych Osobowych (UODO).
- **Temat przewodni spotkania:** jak łączyć wymogi przejrzystości w zamówieniach publicznych z obowiązkami wynikającymi z przepisów o ochronie danych osobowych.
- **Wystąpienie UODO:** Monika Krasińska (dyrektor Departamentu Prawa i Nowych Technologii w UODO) wygłosiła wykład „Przejrzystość w zamówieniach publicznych w świetle przepisów o ochronie danych osobowych”.
- **Cel konferencji:** wzmocnienie kompetencji uczestników w zakresie prawa i strategii udzielania zamówień publicznych oraz praktycznych aspektów ochrony danych osobowych w tym obszarze.
- **Privacy by design w zamówieniach:** Natalia Bender (UZP) omówiła „Model ochrony danych osobowych w zamówieniach publicznych w oparciu o zasadę privacy by design”, czyli podejście zakładające uwzględnianie ochrony danych już na etapie projektowania procesu i dokumentacji zamówienia.
- **Orzecznictwo KIO:** Aldona Kowalczyk (4K Legal Kowalczyk Kuchnio Królak sp. k) przedstawiła przegląd orzecznictwa Krajowej Izby Odwoławczej dotyczącego ochrony danych w zamówieniach publicznych.
- **Od RODO do NIS2:** przedstawiciele Open Nexus poruszyli temat zarządzania bezpieczeństwem danych w zamówieniach publicznych w kontekście wymagań RODO oraz dyrektywy NIS2:
  - Eryk Brodnicki – „Od RODO do NIS2 - jak skutecznie zarządzać bezpieczeństwem danych w zamówieniach publicznych”.
  - Mateusz Bartosiewicz – „RODO dla każdego urzędnika. Jak małe zamówienia kształtują codzienną świadomość bezpieczeństwa danych?”.

- **Szerszy kontekst cyklu:** Monika Krasińska była również prelegentką pierwszej konferencji z tego cyklu („Projektowanie ochrony danych w zamówieniach publicznych. Wyzwania w świetle rozwoju nowych technologii”), która odbyła się 17 kwietnia w siedzibie UODO.
- **Wniosek z pierwszego spotkania:** wskazano, że prawo zamówień publicznych ma wiele cech wspólnych z regulacjami o ochronie danych osobowych, co wymaga spójnego podejścia do przejrzystości, obowiązków informacyjnych i bezpieczeństwa danych.
- **Dodatkowe informacje:** szczegóły i wszystkie wystąpienia z pierwszej konferencji są dostępne w relacji na stronie UODO (sekcja „Konferencje i webinaria”).

Źródło: https://uodo.gov.pl/pl/531/4582

# Austriacki Sąd Najwyższy pyta o przekazanie procesorowi

- **Kontekst:** sprawa dotyczy zasad przekazywania danych osobowych (tu: adresu e-mail) do podmiotu przetwarzającego mającego siedzibę poza UE (w USA). Austriacki Sąd Najwyższy zwrócił się do Trybunału Sprawiedliwości UE (TSUE) z pytaniami, które mogą wpłynąć na to, jak firmy legalnie zlecają przetwarzanie danych dostawcom w państwach trzecich.
- **O co pyta sąd TSUE (dwa kluczowe problemy):**
  - **Czy do samego przekazania danych procesorowi w państwie trzecim** potrzebna jest **osobna podstawa prawna** z art. 6 ust. 1 RODO (niezależnie od spełnienia wymogów transferu z art. 44 i nast. RODO)?
  - **Czy zgoda na newsletter jest „świadoma”**, jeśli osoba zapisująca się **nie wiedziała wcześniej**, że wysyłka będzie powierzona procesorowi w państwie trzecim (USA)?

- **Stan sprawy:** to **odesłanie prejudycjalne** – na tym etapie sąd austriacki **nie przesądził**, czy transfer był legalny, czy zgoda była ważna ani czy administrator ponosi odpowiedzialność za szkodę. Ustalono jedynie, że potrzebna jest wykładnia prawa UE.
- **Co się wydarzyło (fakty):**
  - Klient kupił portfel sprzętowy do przechowywania kryptoaktywów i korzystał z oprogramowania spółki.
  - Spółka korzystała z amerykańskiej platformy jako **podmiotu przetwarzającego** do obsługi i wysyłki newslettera.
  - Po potwierdzeniu subskrypcji adres e-mail klienta został przekazany do tego podmiotu w USA.
  - Informacja o przekazaniu była w wiadomości potwierdzającej, **drobny druk** i **po angielsku**; klient twierdził, że jej nie przeczytał i nie wiedział o przetwarzaniu w USA.
  - Później doszło do **ataku phishingowego** na konta amerykańskiego dostawcy; wykradziono m.in. adres e-mail i IP klienta, a następnie klient – po otrzymaniu phishingu – ujawnił kod dający dostęp do kryptoaktywów.

- **Spór prawny nr 1 – czy potrzebna jest osobna podstawa z art. 6 RODO:**
  - Sąd przyjął, że transfer do państwa trzeciego podlega rozdziałowi V RODO (art. 44 i nast.), ale powziął wątpliwość, czy to wystarcza, czy trzeba jeszcze „dodatkowej” podstawy z art. 6.
  - **Dominujący pogląd** w doktrynie: korzystanie z procesora reguluje art. 28 RODO, a przy transferze – art. 44+; procesor nie jest „stroną trzecią”, działa na polecenie administratora, więc nie trzeba osobnej podstawy z art. 6 tylko „na przekazanie do procesora”.
  - **Pogląd przeciwny**: przekazanie danych do procesora może być traktowane jako osobna operacja przetwarzania, którą także trzeba oprzeć o art. 6 RODO.
  - W tej sprawie sąd wskazał, że według dotychczasowych ocen sądów niższych **nie zachodziły** przesłanki, na które powoływała się spółka (zgoda, wykonanie umowy ani uzasadniony interes – art. 6 ust. 1 lit. a, b, f). Jeśli TSUE uzna, że osobna podstawa jest wymagana, może to mieć kluczowe znaczenie dla legalności transferu.

- **Spór prawny nr 2 – czy zgoda na newsletter była świadoma:**
  - Klient potwierdził zapis, ale (wg założeń przyjętych na potrzeby pytań do TSUE) **nie wiedział**, że dane będą przetwarzane na serwerach w USA.
  - Sąd przypomniał ogólną zasadę: zgoda musi być oparta o informację przekazaną w sposób zrozumiały, łatwo dostępny i prostym językiem, tak aby osoba rozumiała konsekwencje zgody.
  - Jednocześnie zwrócono uwagę, że wytyczne EROD dot. zgody **nie wymagają wprost**, aby dla samej ważności zgody podawać wszystkie elementy z art. 13 ust. 1 RODO; procesorzy nie muszą być „zawsze” wymieniani jako warunek zgody, choć administrator ma obowiązki informacyjne dot. odbiorców/kategorii odbiorców.
  - Sedno wątpliwości: czy informacja o korzystaniu z procesora w państwie trzecim to **minimum konieczne** do „świadomej zgody”, czy raczej element szerszego obowiązku informacyjnego administratora.

- **Dlaczego to ważne praktycznie:** odpowiedź TSUE może doprecyzować relację między:
  - podstawą legalności przetwarzania (art. 6 RODO),
  - zasadami korzystania z procesorów (art. 28 RODO),
  - oraz wymogami transferu danych poza UE (art. 44 i nast. RODO),

  co wpłynie na to, jakie zgody/informacje i jakie podstawy prawne firmy muszą zapewnić, gdy zlecają obsługę np. newsletterów dostawcom spoza UE.

Źródło: https://judykatura.pl/austriacki-sad-najwyzszy-pyta-o-przekazanie-procesorowi/

# TSUE: pytanie o granice systemu zdrowotnego

- **Kontekst:** Najwyższy Sąd Administracyjny Bułgarii zwrócił się do Trybunału Sprawiedliwości UE (TSUE) z pytaniami o to, jakie **prawne i techniczne zabezpieczenia** muszą spełniać krajowe systemy, które **centralnie i obowiązkowo** gromadzą oraz udostępniają dane o zdrowiu pacjentów (szczególnie wrażliwe dane).
- **To nie jest jeszcze wyrok TSUE** – tekst streszcza tzw. **odesłanie prejudycjalne**, czyli pytania sądu bułgarskiego, które mają dopiero zostać rozstrzygnięte przez TSUE.

- **Czego dotyczy bułgarski system:** utworzono krajowy system informacji zdrowotnej, w którym powstaje elektroniczna dokumentacja medyczna obejmująca m.in. dane identyfikacyjne, badania, skierowania, wyniki, hospitalizacje, szczepienia, recepty, informacje o chorobach przewlekłych, alergiach, leczeniu i wyrobach medycznych.
- **Kto może mieć dostęp:** przede wszystkim personel medyczny, a w określonych sytuacjach także **ubezpieczyciele**, **organy ścigania**, **sądy** i **biegli**.
- **Istota sporu:** skarżący kwestionują m.in. **brak wyraźnej zgody** na gromadzenie danych oraz **zbyt słabe mechanizmy kontroli** tego, kto i do jakich informacji zagląda.

- **Kluczowy problem prawny (Teza 1):** sąd ma wątpliwość, czy najważniejsze elementy takiego systemu mogą być regulowane głównie **rozporządzeniem** (aktem niższego rzędu), a nie **ustawą**.
- **Co uznaje się za „istotne elementy", które powinny być jasno określone:**
  - jakie **kategorie danych** są zbierane,
  - jakie są **cele przetwarzania**,
  - jakie są **kategorie odbiorców** danych,
  - na jakich **warunkach** następuje dostęp,
  - jak długo dane są **przechowywane**,
  - jakie istnieją **gwarancje ochrony** (zabezpieczenia).

- **Obawa sądu:** jeśli te kwestie określa głównie organ wykonawczy, to może to oznaczać zbyt małą „stabilność" i przewidywalność reguł ingerujących w prawa podstawowe.

- **Kluczowy problem praktyczny (Teza 2):** sama deklaracja, że dostęp do danych jest ograniczony do „niezbędnego minimum", **nie wystarcza**, jeśli system nie ma mechanizmów, które realnie to wymuszą.
- **Na czym polega ryzyko:** w części przypadków dostęp może obejmować **całą dokumentację**, a decyzję „co jest potrzebne" podejmuje osoba uzyskująca dostęp (np. lekarz, ubezpieczyciel, organ), bez technicznego filtra ograniczającego zakres danych.
- **Jakie mechanizmy (przykładowo) powinny istnieć, by minimalizacja była egzekwowalna:**
  - **role i profile dostępu** (kto do czego ma prawo),
  - **ograniczenia czasowe** dostępu,
  - **z góry określone zestawy danych** dla konkretnych zadań,
  - **automatyczne filtry** ograniczające wgląd,
  - **obowiązek uzasadnienia** dostępu,
  - **skuteczne informowanie** osoby, której dane dotyczą.

- **Zgoda pacjenta a zakres dostępu:** jedno z pytań dotyczy modelu zgody, której pacjent nie może „dawkować" (np. tylko do części danych, na określony czas lub cel).
- **Wątpliwość sądu:** czy taka zgoda może być uznana za rzeczywiście **dobrowolną, konkretną, świadomą i jednoznaczną**, jeśli w praktyce działa jak ogólne pozwolenie na szeroki wgląd.
- **Ważny akcent:** zgoda nie powinna być formalnym „otwarciem" całej dokumentacji, gdy do konkretnej czynności (badania/lecznia) potrzebny jest tylko wycinek danych.

- **Protokół dostępu i informowanie (Teza 3):** rejestrowanie kto i kiedy miał dostęp (logi) jest ważne, ale **nie zapobiega** nadmiernemu dostępowi – umożliwia głównie **kontrolę po fakcie**.
- **Problem z informowaniem „w razie konieczności":** sąd ma wątpliwość, czy taki model realnie zapewnia pacjentowi skuteczne korzystanie z praw (np. wiedzy o tym, kto przeglądał dane).
- **Pytanie do TSUE:** czy pacjent powinien być informowany w sposób systematyczny i skuteczny o tym **kto, kiedy, na jakiej podstawie i do jakich danych** uzyskał dostęp.

- **Co jest przed TSUE:** wykładnia przepisów RODO (w szczególności art. 9 o danych wrażliwych) w powiązaniu z prawami podstawowymi do **prywatności i ochrony danych** (Karta Praw Podstawowych UE).
- **Najważniejszy wniosek z opisu sprawy:** przy masowym, obowiązkowym i scentralizowanym przetwarzaniu danych o zdrowiu może nie wystarczyć:
  - ogólne upoważnienie w prawie,
  - oraz sama deklaracja „minimalizacji danych".

  Potrzebne mogą być **konkretne, przewidywalne reguły** i **technicznie egzekwowalne ograniczenia dostępu**, a nie tylko rozliczalność po fakcie.

# Szwedzki Organ Ochrony Danych nałożył 1,8 mln koron kary na dostawcę systemów kadrowych

- **Kontekst:** Decyzja szwedzkiego organu ochrony danych (IMY) pokazuje, że przy przetwarzaniu danych zdrowotnych i kadrowych nie wystarczy mieć „formalnie wdrożone" zabezpieczenia. Organ oczekuje także **sprawdzania aktualności komponentów bezpieczeństwa** oraz **zdolności do szybkiego wykrywania ataku**.
- **Co się wydarzyło:** W sierpniu 2025 r. doszło do **ataku ransomware** na dostawcę internetowych systemów wspierających m.in. absencję chorobową, rehabilitację oraz zdarzenia w pracy.
- **Skala i rodzaj danych:** Incydent dotyczył ok. **2 200 000 osób**. Przetwarzano m.in. dane identyfikacyjne i kontaktowe, dane o zatrudnieniu i absencji oraz **dane o zdrowiu**, dane dzieci, numery identyfikacyjne i (w pewnym zakresie) dane objęte szczególną ochroną. Część danych trafiła do **Darknetu**.
- **Dlaczego wymagano wysokiego poziomu ochrony:** IMY połączył **bardzo dużą skalę przetwarzania** z **wrażliwym charakterem danych**. Organ wskazał, że nieuprawniony dostęp/ujawnienie mogły prowadzić do poważnych konsekwencji dla osób, których dane dotyczą.
- **Główna przyczyna techniczna:** Atakujący wykorzystał **znaną krytyczną podatność** w komponencie wspierającym rozwiązanie zapory sieciowej. Uzyskał dostęp do środowiska, podniósł uprawnienia, przemieszczał się między serwerami, szyfrował je i wyprowadzał dane.
- **Wniosek 1 – kontrola wersji to podstawa:** IMY uznał, że **sprawdzenie, czy instalowana jest właściwa (aktualna) wersja komponentu bezpieczeństwa**, było podstawowym środkiem bezpieczeństwa – zwłaszcza że:
  - komponent instalowano na **serwerze dostępnym z internetu**,
  - nie był wcześniej testowany w **środowisku testowym**,
  - podatność przestarzałej wersji była **publicznie znana od ponad roku**.

- **Wniosek 2 – „renomowany dostawca" nie zwalnia z obowiązków:** Spółka tłumaczyła, że zaufała producentowi. IMY podkreślił jednak, że to podmiot świadczący usługę/administrujący środowiskiem technicznym odpowiada za zapewnienie odpowiedniej ochrony danych.
- **Wniosek 3 – monitoring wydajności nie wystarcza:** Stosowane narzędzia nadzoru były nastawione głównie na **dostępność i wydajność**, przez co nie wykryły wczesnych etapów ataku, ruchów atakującego, szyfrowania serwerów ani transferu danych.
- **Wniosek 4 – potrzebny monitoring bezpieczeństwa w czasie rzeczywistym:** Organ wskazał, że przy tak wysokim ryzyku podstawowym środkiem powinien być **automatyczny monitoring w czasie rzeczywistym**, zdolny do identyfikacji podejrzanej aktywności oraz prób włamań. W tej sprawie incydent wykryto dopiero po ok. **3 dniach**.
- **Skutek prawny:** IMY uznał naruszenie **art. 32 ust. 1 RODO** (niewystarczające środki techniczne i organizacyjne adekwatne do ryzyka) i ocenił działanie spółki jako **nieostrożne** oraz naruszenie jako **poważne**.
- **Kara:** Decyzją z **22 września 2026 r.** IMY nałożył administracyjną karę pieniężną **1 800 000 koron**.
- **Co nie zostało uznane za wystarczające „złagodzenie":** Organ nie uznał za wystarczające m.in. faktu szyfrowania części danych oraz działań naprawczych po incydencie (szyfrowanie nie dowodziło skutecznej ochrony przed nieuprawnionym dostępem w trakcie ataku).
- **Najważniejsze praktyczne wnioski:**
  - Przy danych zdrowotnych i kadrowych **nie można zastąpić weryfikacji aktualności i bezpieczeństwa komponentów** samym zaufaniem do dostawcy.
  - **Monitoring ciągłości działania** (wydajność/dostępność) nie spełnia sam w sobie wymogu **wykrywania zagrożeń dla poufności danych** – potrzebne są narzędzia bezpieczeństwa działające w czasie rzeczywistym.

Źródło: https://judykatura.pl/szwedzki-organ-ochrony-danych-nalozyl-18-mln-koron-kary-na-dostawce-systemow-kadrowych/

# Skarbówka kontra prywatność obywateli. Poselski projekt zgodny z postulatami Prezesa UODO

- **Kontekst:** artykuł dotyczy planów ograniczenia dostępu Krajowej Administracji Skarbowej (KAS) do informacji o rachunkach bankowych. Obecnie skarbówka ma – zdaniem autorów projektu zmian oraz Prezesa UODO – zbyt dużą swobodę w sięganiu po dane bankowe, co może naruszać tajemnicę bankową i prywatność obywateli.
- **Jak jest dziś:** na podstawie obecnych przepisów KAS może żądać od banków szerokiego zakresu danych o rachunkach, m.in. dat i kwot wpływów oraz obciążeń, danych nadawcy i odbiorcy przelewów, a także informacji o pożyczkach i kredytach.
- **Co ma się zmienić:** projekt nowelizacji zakłada, że organy skarbowe będą mogły pozyskiwać dane z kont bankowych **bez dodatkowej zgody** tylko w przypadku osób mających **status podejrzanego**. W innych przypadkach dostęp do danych miałby być możliwy **wyłącznie za zgodą sądu**.
- **Etap prac:** 16 września sejmowa Komisja Finansów Publicznych zajęła się projektem nowelizacji dotyczącym art. 48. Ostateczny kształt przepisów zależy od dalszych prac parlamentarnych.
- **Gdzie zostanie wpisana zmiana:** według projektu modyfikacja ma się znaleźć nie w ustawie o KAS, lecz w ustawie **Prawo bankowe**.
- **Rola Prezesa UODO:** Prezes UODO Mirosław Wróblewski od dłuższego czasu postuluje doprecyzowanie i ograniczenie przepisów, wskazując na ryzyka dla prywatności i ochrony danych osobowych.
- **Argumenty prawne (RODO i Konstytucja):** w lipcu 2024 Prezes UODO zwrócił się do Ministra Finansów o dostosowanie przepisów do wymogów Konstytucji RP, RODO (rozporządzenie 2016/679) oraz standardów wynikających z orzecznictwa międzynarodowego.
- **Ryzyka wskazywane przez UODO:** Prezes UODO zwraca uwagę, że tak szerokie kompetencje KAS (w tym przetwarzanie danych także w sposób zautomatyzowany i poprzez profilowanie) mogą generować istotne ryzyka naruszeń prywatności.
- **Celowość i ograniczenie użycia danych:** UODO podkreśla, że dane zebrane przez KAS do konkretnych celów nie powinny być łączone z innymi danymi ani wykorzystywane do celów nieprzewidzianych w prawie (np. szeroko rozumianych analiz), bo może to być sprzeczne z RODO.
- **Największe zastrzeżenia:** szczególne wątpliwości UODO budzą przepisy art. 46a i 48 ustawy o KAS, oceniane jako mechanizmy ingerujące w prywatność w sposób **nieproporcjonalny**.
- **Ocena projektu zmian:** w sierpniu 2024 Prezes UODO pozytywnie ocenił kierunek zawężenia art. 48 (dostęp do danych bankowych ma dotyczyć podejrzanych, a nie „każdej osoby fizycznej"), jednocześnie wskazując potrzebę **szerszego, kompleksowego** przeglądu przepisów o przetwarzaniu danych w KAS.
- **Wątek wymiany danych z obszaru zdrowia (art. 46a):** w grudniu 2024 Prezes UODO zwrócił uwagę na problem związany z wymianą informacji między Ministrem Zdrowia a KAS. Jego zdaniem przepis jest sformułowany na tyle ogólnie, że może pozwalać na przetwarzanie także tzw. **szczególnych kategorii danych** (np. danych o zdrowiu), mimo że takie dane podlegają wyższej ochronie.
- **Postulat doprecyzowania zakazów:** UODO wskazuje, że jeśli dane wrażliwe mają być wyłączone, powinno to wynikać jasno z przepisów (podobnie jak w regulacjach dotyczących NIK, gdzie kontrolerom wprost zabrania się przetwarzania danych szczególnych kategorii w trakcie kontroli).
- **Dane do analiz:** Prezes UODO postuluje, aby przetwarzanie danych przez KAS do celów analitycznych odbywało się **wyłącznie na danych zanonimizowanych** i by zostało to jednoznacznie zapisane w prawie.
- **Spór o rozszerzenie z 2022 r.:** UODO wskazuje, że poszerzenie w 2022 r. zakresu danych przetwarzanych na podstawie art. 48 (podmiotowo i przedmiotowo) nie zostało odpowiednio uzasadnione pod kątem niezbędności; podobne zastrzeżenia zgłaszał też Rzecznik Praw Obywatelskich.
- **Wniosek ogólny:** projektowane zmiany mają wzmocnić ochronę prywatności i tajemnicy bankowej, wprowadzając zasadę: dostęp do danych bankowych ma być co do zasady ograniczony (podejrzany) lub kontrolowany przez sąd (pozostałe osoby), ale jednocześnie – według UODO – potrzebne są także dalsze doprecyzowania i szersze zmiany w przepisach o danych osobowych w KAS.

Źródło: https://uodo.gov.pl/pl/138/4588

## Miliony Polaków poszkodowane. Po nowym wycieku danych medycznych PUODO zapowiada kontrolę

- **Kontekst:** Media informują o nowym, potencjalnym wycieku danych, który może obejmować **dane medyczne nawet 5 mln Polaków**. Sprawą zajmuje się **Centralne Biuro Zwalczania Cyberprzestępczości (CBZC)**, a **Prezes UODO** zapowiada kontrolę firmy odpowiedzialnej za oprogramowanie **Medyc**.
- **Źródło zagrożenia:** Incydent ma być skutkiem **ataku na aplikację Medyc**, tworzoną przez firmę **Qbusoft Sp. z o.o.**.
- **Działania służb:** Wicepremier i minister cyfryzacji **Krzysztof Gawkowski** przekazał, że CBZC prowadzi działania w ramach **szerszego śledztwa** dotyczącego incydentów cyberbezpieczeństwa, obejmującego m.in. oprogramowanie Medyc.
- **Zalecenia bezpieczeństwa: CSiRT CeZ** oraz **Ministerstwo Zdrowia**, w związku z rosnącą liczbą ataków na podmioty medyczne i dostawców oprogramowania, przygotowały **zalecenia bezpieczeństwa** dla dostawców oprogramowania w ochronie zdrowia i przekazały je do wdrożenia (w tekście wskazano datę **16 września 2026 r.**).
- **Brak zgłoszenia incydentu:** Według komunikatu ministra cyfryzacji firma **Qbusoft** do tej pory **nie zgłosiła incydentu** do **CERT Polska** ani do **CSiRT CeZ**.
- **Zapowiedź konsekwencji:** Minister cyfryzacji zapowiedział, że w przypadku naruszenia procedur bezpieczeństwa przez prywatną firmę zostaną wyciągnięte **surowe konsekwencje**.
- **Reakcja UODO: Prezes UODO Mirosław Wróblewski** zapowiedział **kontrolę** w firmie Qbusoft, m.in. pod kątem zastosowanych środków technicznych i organizacyjnych oraz analizy ryzyka.
- **Szersze tło – wcześniejszy incydent MyDr:** Artykuł przypomina wyciek danych z **MyDr**, który miał dotyczyć **19 mln Polaków**. Do **17 września** UODO otrzymał **ponad 50 skarg i sygnałów** oraz **ponad 2 tys. zawiadomień** od administratorów danych w związku z tym zdarzeniem.
- **Kontrole na większą skalę:** 16 września Prezes UODO zdecydował, że potrzebne są **szersze kontrole** w obszarze przetwarzania danych o zdrowiu (nie tylko w związku z MyDr, ale też innymi naruszeniami) oraz zapowiedział **dodatkowe kontrole do końca 2026 roku**.

Źródło: https://uodo.gov.pl/pl/138/4585

## Niezapewnienie dostępu do danych osobowych i informacji może skutkować nałożeniem kary

- **Kontekst:** Prezes UODO Mirosław Wróblewski nałożył na krakowskiego przedsiębiorcę **karę 31 507 zł** za brak współpracy i nieprzekazanie informacji potrzebnych w postępowaniu dotyczącym przetwarzania danych osobowych w prowadzonych przez niego serwisach internetowych.
- Postępowanie dotyczyło możliwych nieprawidłowości w funkcjonowaniu portali **lexspace.pl** oraz **adwokatura.info**.
- Serwisy służyły przetwarzaniu danych osobowych:
  - **prawników** (radców prawnych i adwokatów),
  - **osób szukających porad prawnych**.

- Na stronach internetowych **nie zamieszczono danych kontaktowych administratora**, co utrudniało użytkownikom skuteczne korzystanie z praw związanych z ochroną prywatności i danych osobowych.
- UODO ustalił, że oba serwisy są powiązane z działalnością gospodarczą **jednego przedsiębiorcy z Krakowa**, który następnie potwierdził, że jest **administratorem danych** przetwarzanych w tych serwisach.
- Administrator początkowo współpracował z organem nadzorczym, jednak ostatecznie **nie udzielił informacji niezbędnych do rozstrzygnięcia sprawy**.
- Wyjaśnienia przekazane przez przedsiębiorcę były **niewystarczające** – nie odniósł się w odpowiednim zakresie do pytań UODO i nie umożliwił dokonania koniecznych ustaleń.
- UODO **wielokrotnie wzywał** administratora do uzupełnienia wyjaśnień oraz informował, że brak przekazania wymaganych informacji może skutkować **administracyjną karą pieniężną**.
- Mimo ponawianych prób kontaktu (telefonicznie i mailowo) administrator **nie zareagował** na wezwania.
- Zdaniem UODO taka bierna postawa **uniemożliwiła obiektywne i wszechstronne rozpatrzenie sprawy**, co przesądziło o konieczności nałożenia kary.
- **Sygnatura sprawy:** DKE.561.7.2026

Źródło: https://uodo.gov.pl/pl/138/4590

# NSA: prywatny komputer nie zwalnia administratora

- **Kontekst:** Wyrok NSA z 8 września 2026 r. wyznacza praktyczną granicę odpowiedzialności administratora danych przy telepracy i korzystaniu z prywatnych urządzeń. Sąd potwierdził, że administrator nie może „przerzucić" na pracownika odpowiedzialności za zaprojektowanie, wdrożenie i wykazanie adekwatnych zabezpieczeń (RODO).
- **O co chodziło w sprawie:** Prezes UODO udzielił upomnienia Rzecznikowi Finansowemu po kradzieży prywatnego komputera byłego pracownika, na którym znajdowały się skopiowane dokumenty ze służbowej skrzynki (pozostały tam także po zakończeniu pracy).
- **Skala naruszenia:** Sprawa dotyczyła danych **1334 osób**, w tym m.in. numerów PESEL, informacji finansowych, danych z dokumentów tożsamości oraz informacji o prowadzonych sprawach.
- **Kluczowy wniosek NSA (telepraca na prywatnym sprzęcie):** Obowiązki administratora z art. 24 i 32 RODO aktualizują się już w momencie, gdy administrator **dopuszcza** model pracy zdalnej z użyciem prywatnych komputerów. Późniejsze przekroczenie upoważnienia przez pracownika nie zwalnia administratora z obowiązku wcześniejszego zaprojektowania bezpiecznego środowiska pracy.
- **Teza 1 – Administrator odpowiada także za prywatny sprzęt używany do pracy:** Administrator powinien z góry tak zorganizować telepracę, aby ograniczać niekontrolowane kopiowanie danych oraz zapewnić sprawdzalny proces:
  - odebrania dostępu po zakończeniu pracy,
  - potwierdzenia trwałego usunięcia lokalnych kopii danych.

- **Teza 2 – Kto jest administratorem, zależy od realnej roli, a nie tytułu:** O statusie administratora nie decyduje nazwa stanowiska, kwalifikacje (np. radca prawny), tajemnica zawodowa ani to, czy urządzenie jest prywatne. Liczy się to, kto faktycznie ustala **cele** i **zasadnicze sposoby** przetwarzania – w tej sprawie robił to Rzecznik Finansowy jako organizacja/pracodawca.
- **Teza 3 – Sam incydent nie oznacza automatycznie, że zabezpieczenia były złe:** NSA podkreślił, że RODO nie wprowadza odpowiedzialności „za każdy incydent". Adekwatność środków ocenia się w konkretnej sytuacji, biorąc pod uwagę m.in. ryzyka, kontekst, stan wiedzy technicznej, koszty wdrożenia oraz prawdopodobieństwo i wagę skutków.
- **Dlaczego w tej sprawie uznano braki po stronie administratora:** Wskazano na skumulowane problemy systemowe, m.in.:
  - brak wcześniejszej analizy ryzyka dotyczącej telepracy na prywatnych komputerach,
  - brak wymogu szyfrowania całego dysku (lub rozwiązania równoważnego) na prywatnym sprzęcie,
  - brak technicznej weryfikacji, czy zabezpieczenia na prywatnym urządzeniu są faktycznie zainstalowane i skuteczne,
  - brak kontroli/ograniczeń kopiowania dokumentów ze służbowej poczty na lokalny dysk,
  - brak sprawdzalnego mechanizmu potwierdzającego trwałe usunięcie kopii danych po zakończeniu zatrudnienia.

- **Ważne doprecyzowanie (czego nie wymaga wyrok):** Administrator nie musiał zapobiec samej **kradzieży** urządzenia. Miał natomiast obowiązek tak dobrać środki, aby w razie przewidywalnego zdarzenia (utrata/kradzież) **ograniczyć możliwość dostępu do danych**.
- **Dlaczego VPN/hasło/szyfrowanie archiwów uznano za niewystarczające:** NSA wskazał, że:
  - VPN chroni kanał połączenia, a nie dane już zapisane lokalnie na dysku,
  - szyfrowanie archiwów chroni tylko te pliki, które zostały objęte szyfrowaniem,
  - hasło do konta użytkownika nie jest równoważne szyfrowaniu danych na nośniku.

- **Teza 4 – Upomnienie to nie kara pieniężna:** Upomnienie z art. 58 ust. 2 lit. b RODO jest środkiem władczym, ale nie jest administracyjną karą pieniężną. W tej sprawie utrzymano upomnienie m.in. ze względu na jednorazowy charakter zdarzenia, działania naprawcze i brak przesłanek, że nadal występuje systematyczne zaniechanie stwarzające poważne ryzyko.
- **Najważniejsza konsekwencja praktyczna:** Dopuszczenie prywatnego sprzętu do przetwarzania danych **nie zmniejsza** odpowiedzialności administratora. Wymaga wdrożenia rozliczalnego modelu bezpieczeństwa: analizy ryzyka, weryfikowalnych zabezpieczeń urządzeń, ograniczeń kopiowania danych oraz kontrolowanego zakończenia dostępu i usunięcia danych.

Źródło: https://judykatura.pl/nsa-prywatny-komputer-nie-zwalnia-administratora/

# Po karze dla hurtowni leków UODO pyta o dane pacjentów z aptek

- **Kontekst:** Prezes Urzędu Ochrony Danych Osobowych (UODO) chce ustalić, czy w ramach programów partnerskich hurtowni farmaceutycznych z aptek mogło dochodzić do **wycieku danych pacjentów** (np. numerów PESEL i informacji o zdrowiu). W związku z tym zwrócił się o stanowisko i współpracę do **Głównego Inspektora Farmaceutycznego (GIF)**.
- **Pismo UODO do GIF:** 30 września prezes UODO Mirosław Wróblewski skierował pismo do GIF Łukasza Pietrzaka, prosząc o pilne informacje pozwalające na **wstępne ustalenia dotyczące bezpieczeństwa danych pacjentów**.
- **Co było wcześniej (UOKiK):** UODO powołuje się na **decyzję UOKiK z 21 września**, według której grupa Neuca, spółki z grupy Farmacol i Polska Grupa Farmaceutyczna miały **wymieniać się informacjami handlowymi** (m.in. o cenach dla konkretnych aptek), a dane o zakupach aptek pozyskiwać przez narzędzia IT w programach partnerskich.
- **Kary i status decyzji:** Łączne kary UOKiK przekroczyły **904 mln zł**; PGF uniknęła sankcji dzięki programowi łagodzenia kar. **Decyzja jest nieprawomocna.**
- **Ważne zastrzeżenie:** UOKiK badał **informacje handlowe**; w decyzji nie opisano kwestii danych osobowych pacjentów.
- **Główne ryzyko wskazane przez UODO:** według doniesień medialnych hurtownie mogły korzystać z tzw. **„nakładek”** (modułów w oprogramowaniu aptecznym), które automatycznie raportowały dane o sprzedaży. Problem polega na tym, że w tych samych systemach aptecznych przetwarzane są też **dane bardzo wrażliwe**, m.in. PESEL oraz informacje o zdrowiu i historii recept (dane szczególnie chronione na mocy art. 9 RODO).
- **Pytania UODO do GIF:** czy w kontrolach sprawdzano, **jakie dane pobierają „nakładki”**; czy GIF ma wiedzę o przypadkach **przekazania danych pacjentów hurtowniom**; oraz czy planowane są **doraźne kontrole**.
- **Skala potencjalnego problemu:** UODO wskazuje, że hurtownie wymienione przez UOKiK miały ponad **70% udziału w rynku**, a z programów partnerskich korzysta łącznie ponad **4 tys. aptek** (ok. **40% rynku**). To może oznaczać ryzyko **systemowego naruszenia prywatności milionów pacjentów**.
- **UODO nie przesądza naruszeń:** pismo mówi o **wstępnych ustaleniach** i potrzebie wyjaśnienia sprawy; nie stwierdza wprost, że do przekazywania danych pacjentów doszło.
- **Niejasne dalsze kroki UODO:** redakcja zapytała 23 września, czy UODO wszcznie postępowanie z urzędu, ale **do czasu publikacji nie było odpowiedzi**.
- **Głosy ekspertów:**
  - Aneta Sieradzka ocenia działania UODO jako potrzebne, bo sprawa dotyczy nie tylko konkurencji na rynku, ale **potencjalnie także bezpieczeństwa danych pacjentów**.
  - Dr Łukasz Fijałkowski podkreśla, że proceder mógł trwać **około 10 lat** i że przez „nakładki” **mogły** przepływać dane milionów pacjentów (z zastrzeżeniem, że nie przesądza, czy faktycznie trafiały do hurtowni).
  - Wskazywana jest wartość **współpracy urzędów**: GIF może weryfikować praktyki w aptekach, a UODO – zgodność z przepisami o ochronie danych.

- **Tło regulacyjne i rynek:** ekspert przypomina, że prawo farmaceutyczne nie pozwala temu samemu podmiotowi prowadzić jednocześnie hurtowni i apteki, a po zmianach z 2023 r. kontrole hurtowni mają odbywać się **raz na pięć lat**. Wskazuje też na ryzyko zbyt ścisłej współpracy, gdy apteki muszą zamawiać **80% lub więcej** produktów z jednej hurtowni (możliwy wpływ na konkurencję i monopolizację).
- **Co powinno być kontrolowane (wg ekspertów):** kontrola ochrony danych w aptekach powinna być **kompleksowa i regularna** – nie tylko IT, ale też: jakie dane są gromadzone, kto ma dostęp, na jakiej podstawie i w jakim celu są przetwarzane, komu i w jakim zakresie są przekazywane, czy działa zasada minimalizacji danych; dodatkowo warto kontrolować dostawców oprogramowania, prowadzić audyty, weryfikować uprawnienia i rejestrować dostęp.
- **Porozumienie UODO–GIF:** przypomniano, że 7 grudnia 2023 r. UODO i GIF podpisały porozumienie o współpracy przy ujawnianiu i eliminowaniu naruszeń w przetwarzaniu danych pacjentów i pracowników aptek, w tym o **wzajemnym przekazywaniu informacji**.
- **Szersza perspektywa:** według ekspertów ocena rynku aptecznego powinna uwzględniać punkt widzenia pacjenta: **bezpieczeństwo danych, dostęp do leków i usług, obecność farmaceutów oraz ceny**. Pada też ocena, że decyzja UOKiK może być jedynie **„czubkiem góry lodowej”**, a inne instytucje mogą badać głębsze aspekty problemu.

Źródło: https://edgp.gazetaprawna.pl/prawo/prawo-internetu-i-ochrony-danych/artykuly/11322852,po-karze-dla-hurtowni-lekow-uodo-pyta-o-dane-pacjentow-z-aptek.html