





RODO - aktualności

Data publikacji: 26.09.2025

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

WSA: nie każda Spółdzielnia Mieszkaniowa jest przedsiębiorcą, co skutkuje uchynieniem kary ponad 51 000 zł

02

WSA: prawidłowe 1,4 mln zł kary za brak tzw. obrony przed ransomware

03

Rekordowa kara za wyciek danych w Korei Południowej (ok. 97,2 mln USD)

04

PUODO: Upomnienie za brak prowadzenia rejestru kategorii czynności przetwarzania

05

WSA oddalił skargę Toyota Bank Polska SA na decyzję karową Prezesa UODO

O naszej książce: poznaj **RODOLOGIĘ**

- ✔ 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 WSA: nie każda Spółdzielnia Mieszkaniowa jest przedsiębiorcą, co skutkuje uchyleniem kary ponad 51 000 zł

- W marcu 2023 r. Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył karę pieniężną na spółdzielnię mieszkaniową za naruszenie przepisów RODO poprzez niezgłoszenie naruszenia ochrony danych osobowych oraz brak poinformowania osoby, której dane wyciekły. Sprawa dotyczyła udostępnienia bez zgody danych osobowych członkini spółdzielni osobie trzeciej – dziennikarce.
- Spółdzielnia Mieszkaniowa w O. udostępniła dane (imię, nazwisko, PESEL, adres) członkini spółdzielni osobie trzeciej – dziennikarce – bez odpowiednich uprawnień.
- Dziennikarka oświadczyła, że otrzymała dokument z danymi z inicjatywy wiceprezesa zarządu spółdzielni, sama o nie nie zabiegała.
- Spółdzielnia tłumaczyła swoje działania chęcią przedstawienia opinii publicznej „prawdziwego stanu rzeczy” w odpowiedzi na rzekomą negatywną kampanię osoby, której dane upubliczniono.
- Administrator danych uważał, że ryzyko naruszenia praw tej osoby było niskie, ponieważ wcześniej sama je upubliczniła – jednak nie zgłosił naruszenia zarówno do UODO, jak i do samej osoby poszkodowanej.
- Prezes UODO zwrócił uwagę, że brak zgłoszenia naruszenia:
 - pozbawił osobę fizyczną możliwości reakcji na wyciek danych,
 - uniemożliwił organowi nadzorcemu ocenę skali naruszenia oraz działań naprawczych administratora.
- Na spółdzielnię została nałożona kara administracyjna w wysokości 51 876 zł.

Źródło: <https://judykatura.pl/wsa-nie-kazda-spoldzielnia-mieszkaniowa-jest-przedsiębiorca-co-skutkuje-uchyleniem-kary-ponad-51-000-zl/>

01 cd. WSA: nie każda Spółdzielnia Mieszkaniowa jest przedsiębiorcą, co skutkuje uchynieniem kary ponad 51 000 zł

- Wojewódzki Sąd Administracyjny (WSA) w Warszawie wytknął Prezesowi UODO błędy proceduralne:
 - organ nie uzasadnił dlaczego uznał spółdzielnię za przedsiębiorcę, według którego przeliczono wysokość kary,
 - nie odniesiono się do specyfiki statusu prawnego spółdzielni mieszkaniowej w polskim systemie prawnym,
 - brak wystarczającego uzasadnienia proporcjonalności nałożonej kary oraz oceny ryzyka dla osoby, której dane wyciekły.
- WSA wskazał, że pomijanie specyfiki prawnej spółdzielni mieszkaniowych może prowadzić do nieprawidłowego określania wysokości kar, które finalnie obciążają ich członków.
- **Wnioski:**
 - Administratorzy danych muszą zgłaszać naruszenia ochrony danych osobowych zarówno organowi nadzorcemu, jak i osobom, których dane dotyczą, jeśli ryzyko ich naruszenia jest wysokie.
 - Przekazanie danych osobowych osobie trzeciej bez podstawy prawnej może stanowić poważne naruszenie przepisów RODO.
 - Organ nadzorczy ma obowiązek rzetelnie uzasadniać nałożenie kar, uwzględniając charakter prawny podmiotów, wobec których są stosowane.
 - Błędna kwalifikacja prawna spółdzielni jako przedsiębiorcy może skutkować zawyżeniem kary administracyjnej.

Źródło: <https://judykatura.pl/wsa-nie-kazda-spoldzielnia-mieszkaniowa-jest-przedsiębiorca-co-skutkuje-uchynieniem-kary-ponad-51-000-zl/>

02 WSA: prawidłowe 1,4 mln zł kary za brak tzw. obrony przed ransomware

- Wojewódzki Sąd Administracyjny (WSA) w Warszawie potwierdził decyzję Prezesa Urzędu Ochrony Danych Osobowych (UODO) z maja 2024 r., dotyczącą naruszeń przepisów RODO przez prywatny szpital A. S.A. w związku z atakiem hakerskim i niewystarczającą ochroną danych osobowych.
- WSA oddalił skargę szpitala na decyzję Prezesa UODO, podtrzymując nałożoną karę administracyjną w wysokości 1.440.549 zł.
- Incydent dotyczył ataku hakerskiego, w wyniku którego grupa cyberprzestępców uzyskała dostęp do danych osobowych 21.569 osób – pacjentów i pracowników – oraz rozpowszechniła je w darknetcie.
- Przetwarzane dane zawierały między innymi: dane identyfikacyjne, kontaktowe, finansowe oraz dane wrażliwe dotyczące zdrowia.
- UODO stwierdził, że szpital nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych, mimo przeprowadzanych cyklicznie analiz ryzyka.
- Sąd uznał, że błędna była przeprowadzona przez szpital analiza ryzyka – nie doszacowano realnego ryzyka wystąpienia zagrożeń, takich jak działanie szkodliwego oprogramowania czy brak odpowiedniego wsparcia informatycznego.
- Spółka nie prowadziła też regularnych testów, pomiarów oraz ocen skuteczności zastosowanych zabezpieczeń.
- Chociaż szpital po incydencie wdrożył pewne działania naprawcze, nie zmienia to oceny, że wcześniejsze uchybienia były poważne i miały wpływ na naruszenie zasad integralności, poufności i rozliczalności danych.
- Sąd uznał, że Prezes UODO słusznie ocenił wszystkie przesłanki przy ustalaniu wysokości kary oraz zastosował aktualne wytyczne Europejskiej Rady Ochrony Danych (EROD).

Źródło: <https://judykatura.pl/wsa-prawidlowe-14-mln-zl-kary-za-brak-obrony-przed-ransomware/>

02 cd. WSA: prawidłowe 1,4 mln zł kary za brak tzw. obrony przed ransomware

- Wyrok potwierdza szerokie kompetencje organu nadzorczego w zakresie oceny środków ochrony danych osobowych oraz konieczność ich dostosowania do rzeczywistego poziomu ryzyka.
- **Wniosek:** Sprawa podkreśla znaczenie właściwej oceny ryzyka i ciągłego monitorowania skuteczności zabezpieczeń systemów informatycznych, szczególnie w obszarze ochrony danych zdrowotnych i innych danych wrażliwych.

Źródło: <https://judykatura.pl/wsa-prawidlowe-14-mln-zl-kary-za-brak-obrony-przed-ransomware/>

03 Rekordowa kara za wyciek danych w Korei Południowej (ok. 97,2 mln USD)

- **Kontekst:** Artykuł dotyczy rekordowej kary nałożonej na SK Telecom przez południowokoreański urząd ochrony danych osobowych (PIPC), co podkreśla rosnące znaczenie bezpieczeństwa danych osobowych na świecie.
- **Wysokość kary:** SK Telecom został ukarany kwotą 134,8 miliarda wonów (około 97,2 mln USD) za poważny wyciek danych ponad 23 milionów użytkowników usług telekomunikacyjnych.
- **Przyczyny naruszenia:** Dochodzenie wykazało, że serwery zarządzające były połączone z internetem bez odpowiednich zabezpieczeń, klucze SIM nie były szyfrowane, systemy były przestarzałe i nie były monitorowane pod kątem ataków.
- **Poważne zaniedbania:** Nawet znane od 2016 roku luki w oprogramowaniu nie zostały załatane. Osoby odpowiedzialne za ochronę danych odpowiadały wyłącznie za serwisy internetowe i aplikacje, ignorując kluczową infrastrukturę telekomunikacyjną.
- **Reakcja firmy:** SK Telecom zaoferował klientom bezpłatną wymianę kart SIM, rekompensaty finansowe, zniżki na usługi oraz dodatkowe pakiety danych.
- **Stanowisko regulatora:** PIPC zaznaczył, że działania naprawcze nie mogą zastąpić odpowiedzialności za brak zabezpieczeń. Firmy mają obowiązek chronić dane osobowe jako podstawowe prawo obywateli.
- **Znaczenie kary:** Jest to najwyższa kara w historii Korei Południowej za naruszenia ochrony danych osobowych i ma stanowić przykład dla innych firm, by traktowały tę kwestię priorytetowo.
- **Szerszy wniosek:** Przypadek SK Telecom jest ostrzeżeniem dla globalnych firm technologicznych i operatorów telekomunikacyjnych – lekceważenie kwestii bezpieczeństwa danych może prowadzić do poważnych konsekwencji finansowych i reputacyjnych.

Źródło: https://www.linkedin.com/posts/adam-szkur%C5%82at_ochronadanych-cybersecurity-pipa-activity-7375785174506221569-UeLs?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLzLMFC01FENWMw0oL_z0rPX_x8

04 PUODO: Upomnienie za brak prowadzenia rejestru kategorii czynności przetwarzania

- **Kontekst:** Artykuł dotyczy decyzji polskiego Urzędu Ochrony Danych Osobowych (UODO) w sprawie naruszenia ochrony danych osobowych po włamaniu do sklepu internetowego za pomocą konta zewnętrznego dostawcy usług (podmiotu przetwarzającego dane).
- **Opis naruszenia:**
 - Do incydentu doszło w 2021 roku, gdy osoby nieuprawnione załogowały się do systemu za pośrednictwem konta resellerskiego zewnętrznej firmy świadczącej usługi SEO.
 - Atakujący wyeksportował dane tysięcy klientów – w tym: imiona i nazwiska, adresy e-mail, numery telefonów i adresy zamieszkania.
- **Wyniki kontroli UODO:**
 - Brak formalnych upoważnień do przetwarzania danych dla pracowników i współpracowników podmiotu przetwarzającego.
 - Nieprowadzenie obowiązkowego rejestru czynności przetwarzania (zgodnie z art. 30 RODO) – rejestr ten wprowadzono dopiero po incydencie.
 - Zidentyfikowano problemy strukturalne w zakresie zarządzania bezpieczeństwem danych i rozliczalności.
- **Decyzja UODO:**
 - UODO ograniczył się do wydania upomnienia, biorąc pod uwagę brak szkód, naprawienie naruszenia oraz współpracę ze strony podmiotu przetwarzającego.

Źródło: https://www.linkedin.com/posts/mateusz-kupiec-fip-cipp-e-cipm-289700121_the-polish-dpa-has-recently-published-activity-7371928075367981059-KbQR?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLIzLMFC01FFENWMw0oL_z0rPX_x8

04 cd. PUODO: Upomnienie za brak prowadzenia rejestru kategorii czynności przetwarzania

- Organ zapowiedział surowsze kary przy ewentualnych przyszłych naruszeniach.
- Wnioski i zalecenia:
 - Administratorzy danych muszą nie tylko zawierać umowy powierzenia, ale także kontrolować zgodność działań przetwórców z RODO.
 - Podmioty przetwarzające muszą prowadzić udokumentowaną politykę nadawania upoważnień, prowadzić rejestr czynności przetwarzania oraz utrzymywać mechanizmy audytowe – także w przypadku małych firm.
 - W przypadku współpracy z firmami zewnętrznymi (np. SEO), konieczna jest regularna weryfikacja ich praktyk w zakresie ochrony danych.

Źródło: https://www.linkedin.com/posts/mateusz-kupiec-fip-cipp-e-cipm-289700121_the-polish-dpa-has-recently-published-activity-7371928075367981059-KbQR?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUJLzLMFC01FENWMw0oL_z0rPX_x8

05 WSA oddalił skargę Toyota Bank Polska SA na decyzję karową Prezesa UODO

- **Kontekst:** Artykuł dotyczy decyzji Prezesa Urzędu Ochrony Danych Osobowych (UODO) w sprawie naruszeń przepisów RODO przez Toyota Bank Polska S.A., co skutkowało nałożeniem dwóch kar pieniężnych o łącznej wartości 576 220 zł.
- **Brak niezależności inspektora ochrony danych (IOD):** Bank powierzył obowiązki IOD osobie, która jednocześnie pracowała jako specjalista ds. bezpieczeństwa IT i podlegała dyrektorowi departamentu odpowiedzialnemu za przetwarzanie danych. To naruszyło przepisy RODO dotyczące niezależności IOD.
- **Kara za nieprawidłowe usytuowanie IOD:** Z tego tytułu Prezes UODO nałożył karę w wysokości 261 918 zł.
- **Profilowanie danych osobowych:** Bank stosował profilowanie danych klientów przy analizie zdolności kredytowej (m.in. scoring, nadawanie kategorii ryzyka), ale nie uwzględnił tych działań w wymaganej dokumentacji.
- **Kara za brak uwzględnienia profilowania:** Za brak uwzględnienia profilowania w rejestrze czynności przetwarzania oraz brak oceny jego skutków dla ochrony danych, nałożono drugą karę w wysokości 314 302 zł.
- **Wyniki kontroli UODO:** Ujawniono szereg uchybień w zakresie zasad przetwarzania danych osobowych, w tym brak zapewnienia niezależności IOD oraz nieprzestrzeganie obowiązków dokumentacyjnych dotyczących profilowania.
- **Stanowisko sądu (WSA):** Wojewódzki Sąd Administracyjny w ustnych motywach wyroku z 18 września 2025 r. poparł decyzję UODO, uznając, że bank naruszył przepisy RODO m.in. co do usytuowania IOD i obowiązku wykazywania operacji profilowania w dokumentacji przetwarzania danych.

Źródło: <https://uodo.gov.pl/pl/138/3889>

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