Grant Thornton

Kto płaci za brak ochrony danych osobowych?

Analiza administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2025 r.

Edycja II: Luty 2026

~64 mln zł

Wyniosły łącznie administracyjne kary pieniężne nałożone w opublikowanych decyzjach Prezesa UODO w 2025 r.

Wprowadzenie

Kary za RODO mogą być wysokie! Jak jest w praktyce?

Rozporządzenie o ochronie danych osobowych (RODO) jest podstawowym aktem prawnym regulującym zasady przetwarzania danych osobowych w Unii Europejskiej. Określa ono obowiązki podmiotów przetwarzających dane oraz prawa osób, których dane dotyczą. W dobie dynamicznego rozwoju technologii i powszechnego wykorzystania danych w działalności gospodarczej ich właściwa ochrona ma kluczowe znaczenie.

Nadzór nad przestrzeganiem przepisów RODO w Polsce sprawuje Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO). Organ ten jest uprawniony nie tylko do kontrolowania zgodności działań z przepisami, ale także do nakładania administracyjnych kar pieniężnych w przypadku stwierdzenia naruszeń.

Kary te mogą być bardzo dotkliwe — w skrajnych sytuacjach sięgać nawet 20 mln euro lub, w przypadku przedsiębiorstw, do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (w zależności od tego, która kwota jest wyższa). W przypadku podmiotów publicznych maksymalna kara może wynosić 100 tys. złotych.

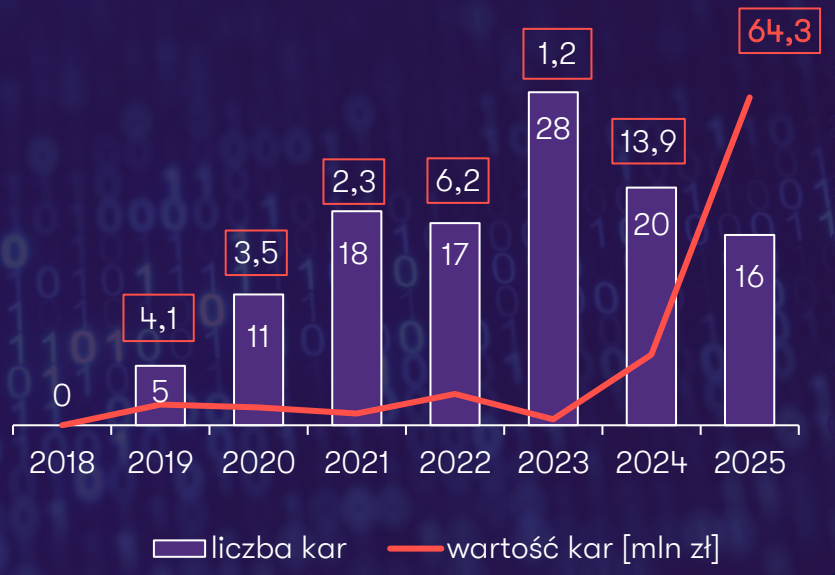
W niniejszym Raporcie analizujemy decyzje Prezesa UODO wydane i opublikowane w 2025 r., w których nałożono administracyjne kary pieniężne. Przedstawiamy najważniejsze wnioski z tych rozstrzygnięć, wskazując, jakie naruszenia występowały najczęściej, kogo dotyczyły oraz na co administratorzy i podmioty przetwarzające powinni zwrócić szczególną uwagę. Zapraszamy do lektury!

Rekordowe kary w RODO

Rok 2025 stanowi punkt przełomowy w dotychczasowej praktyce Prezesa UODO. Choć liczba nałożonych kar była niższa niż w poprzednich latach, ich łączna wartość wzrosła w sposób bezprecedensowy, osiągając ponad 64 mln zł.

Od wejścia w życie RODO w 2018 r. praktyka nakładania kar przez PUODO stopniowo dojrzewała. Początkowo (2018) był to okres przejściowy bez kar finansowych, służący adaptacji do nowych przepisów. Od 2019 r. zaczęły pojawiać się pierwsze kary, a w latach 2020–2022 ich liczba rosła, choć pozostawały one niskie wartościowo. W latach 2023–2024 odnotowano wyraźny wzrost liczby kar, przy nadal umiarkowanej wysokości sankcji.

Przełom nastąpił w 2025 r., gdy mimo mniejszej liczby decyzji, łączna wysokość kar przekroczyła 64 mln zł. Oznacza to przejście od licznych ale niskich sankcji do mniejszej liczby kar o bardzo wysokiej wartości, nakładanych głównie na duże podmioty dopuszczające się poważnych naruszeń. Trend ten potwierdza rosnącą rolę wysokich kar jako kluczowego narzędzia egzekwowania przepisów o ochronie danych.



Grant Thornton

Część 1.

Kto zapłacił najwięcej?

Analiza administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2025 r.

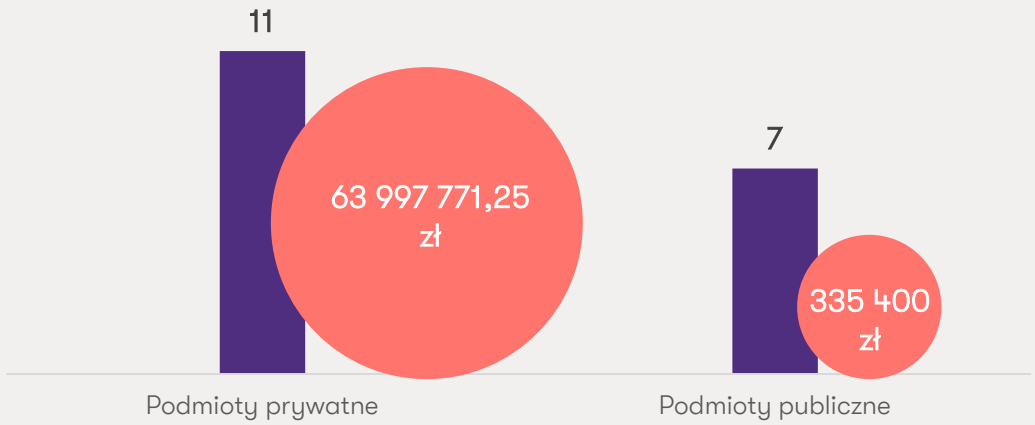
Grant Thornton

Podmioty prywatne płacą częściej za błędy w RODO

W 2025 r. Prezes UODO wydał 16 opublikowanych decyzji nakładających administracyjne kary pieniężne na 18 podmiotów. Łączna wartość nałożonych kar wyniosła 64 333 171,25 zł.

W analizowanym okresie większość stanowiły kary nałożone na podmioty prywatne. Nałożono na nie łącznie 11 administracyjnych kar pieniężnych (68,75% wszystkich decyzji), których całkowita wartość wyniosła 63 997 771,25 zł (99,48% wartości wszystkich kar). Dla porównania, na podmioty publiczne nałożono 7 administracyjnych kar pieniężnych, o łącznej wartości 335 400 zł (0,52% wartości wszystkich kar).

Wykres 1. Rodzaje podmiotów, na które zostały nałożone administracyjne kary pieniężne w 2025 r. oraz wysokość nałożonych kar



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Najwyższa administracyjna kara pieniężna wynosiła 27 124 816,00 zł (42,16% wartości wszystkich kar) i została nałożona przez Prezesa UODO na Pocztę Polską S.A w związku z naruszeniami RODO podczas organizacji wyborów kopertowych. Jednocześnie w ramach tej samej decyzji najwyższą karą nałożoną na podmiot publiczny była kara w wysokości 100 000 zł wymierzona Ministrowi Cyfryzacji.

Najniższa kara natomiast wynosiła 5 000,00 zł i została nałożona na Gminny Ośrodek Pomocy Społecznej w Aleksandrowie za brak wdrożenia wystarczających środków bezpieczeństwa oraz przeprowadzenia analizy ryzyka, które doprowadziły do ataku hackerskiego.

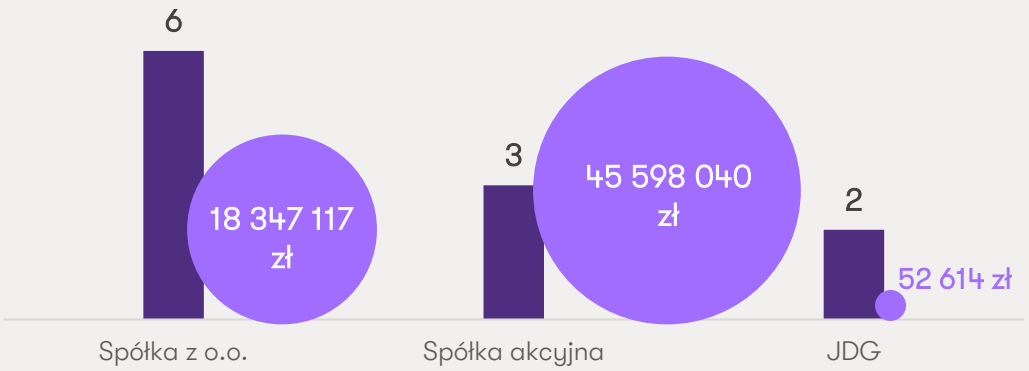
Spółki kapitałowe na celowniku

Administracyjne kary pieniężne nałożone na przedsiębiorstwa w 2025 r. koncentrowały się na spółkach kapitałowych, które odpowiadały za niemal całą kwotę zastosowanych kar.

Spółki akcyjne oraz spółki z ograniczoną odpowiedzialnością, mimo że stanowiły łącznie tylko 9 ukaranych podmiotów prywatnych, odpowiadały za 63,9 mln zł, czyli niemal całą kwotę kar nałożonych na sektor prywatny. Dominacja spółek kapitałowych wynika przede wszystkim ze skali prowadzonej działalności, a co za tym idzie - złożoności procesów przetwarzania danych osobowych oraz wysokich obrotów, które wpływają na maksymalny wymiar kary. W porównaniu z nimi jednoosobowe działalności gospodarcze (JDG) otrzymały łącznie 52 614 zł, co stanowi zaledwie 0,08% wszystkich kar nałożonych na podmioty prywatne.

Pokazuje to bardzo wyraźnie, że w 2025 r. – w odróżnieniu od lat poprzednich – prawie cała wartość finansowa kar dla sektora prywatnego koncentrowała się w spółkach kapitałowych, a kary wobec mniejszych form działalności miały charakter marginalny zarówno pod względem liczby, jak i wysokości. Taka koncentracja kar w spółkach kapitałowych nie powinna być jednak interpretowana jako trwały trend. Dane za 2025 r. odzwierciedlają strukturę zakończonych postępowań i skalę naruszeń, a nie zmianę podejścia organu nadzorczego wobec mniejszych podmiotów.

Wykres 2. Rodzaje podmiotów w ramach sektora prywatnego, na które zostały nałożone administracyjne kary pieniężne w 2025 r. oraz wysokość nałożonych kar



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Administrator sam bije się w piersi

W 2025 r. Prezes UODO wszczął postępowania głównie przez zgłoszenia incydentów ochrony danych osobowych przez administratorów. Ta przyczyna stanowiła 50% wszystkich spraw i przyniosła 18,45 mln zł kar.

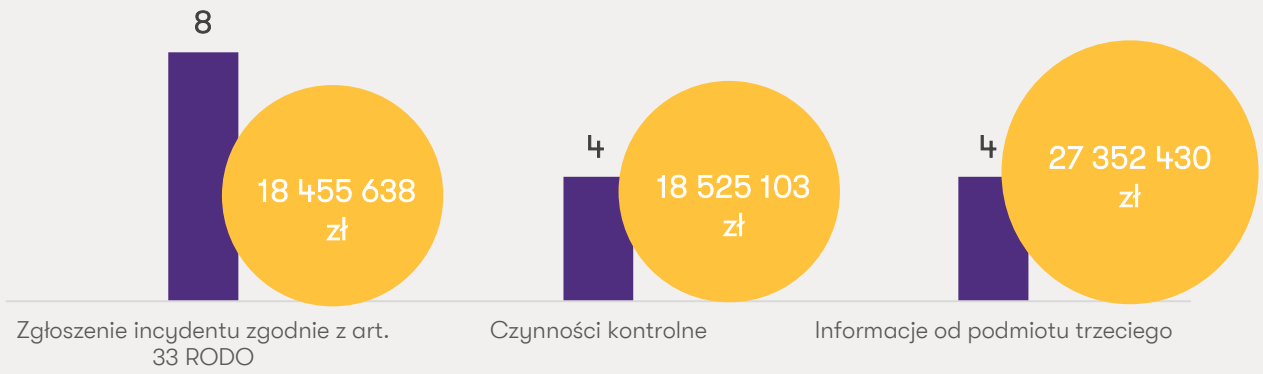
Pokazuje to, że zgłoszenie naruszenia, mimo że jest obowiązkiem administratora wynikającym z art. 33 RODO może wiązać się z potencjalnym ujawnieniem uchybień w zakresie zabezpieczeń technicznych i organizacyjnych. W takich przypadkach podmiot może otrzymać karę nie dlatego, że dokonał zgłoszenia naruszenia lub, że miało ono miejsce, ale dlatego, że wcześniej nie wprowadził adekwatnych i rozsądnych działań, które takim naruszeniom miały zapobiec. Istotną grupę stanowią również sprawy wszczęte na podstawie informacji od podmiotu trzeciego, które obejmowały 25% wszystkich postępowań. To właśnie ta kategoria generowała najwyższe kary finansowe – ponad 27,35 mln zł, w tym najwyższą karę roku nałożoną na Pocztę Polską S.A.

Brak zgłoszenia naruszenia przez administratora, a jednocześnie ujawnienie naruszenia przez osoby trzecie, jest przez Prezesa UODO oceniane bardzo surowo, zwłaszcza gdy naruszenia mają charakter systemowy lub umyślny.

Kolejną przyczyną wszczęcia postępowań były czynności kontrolne prowadzone przez Prezesa UODO, które stanowiły również 25% spraw i zakończyły się nałożeniem kar o łącznej wartości 18,52 mln zł. Kontrole te dotyczyły głównie dużych organizacji, gdzie stwierdzono systemowe uchybienia, m.in. przetwarzanie danych bez podstawy prawnej, brak nadzoru nad procesami przetwarzania czy niewłaściwe środki zabezpieczające.

Warto podkreślić, że w 2025 r. nie wystąpił ani jeden przypadek wszczęcia postępowania z powodu braku udzielenia informacji na wezwanie Prezesa UODO. Nie oznacza to jednak, że obowiązek współpracy z organem nadzorczym traci znaczenie, wręcz przeciwnie, brak reakcji administratora nadal pozostaje obszarem szczególnej uwagi Prezesa UODO.

Wykres 3. Przyczyna wszczęcia postępowania administracyjnego przez Prezesa UODO w 2025 r. oraz wysokość nałożonych kar



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

3 tys. czy 30 mln poszkodowanych?

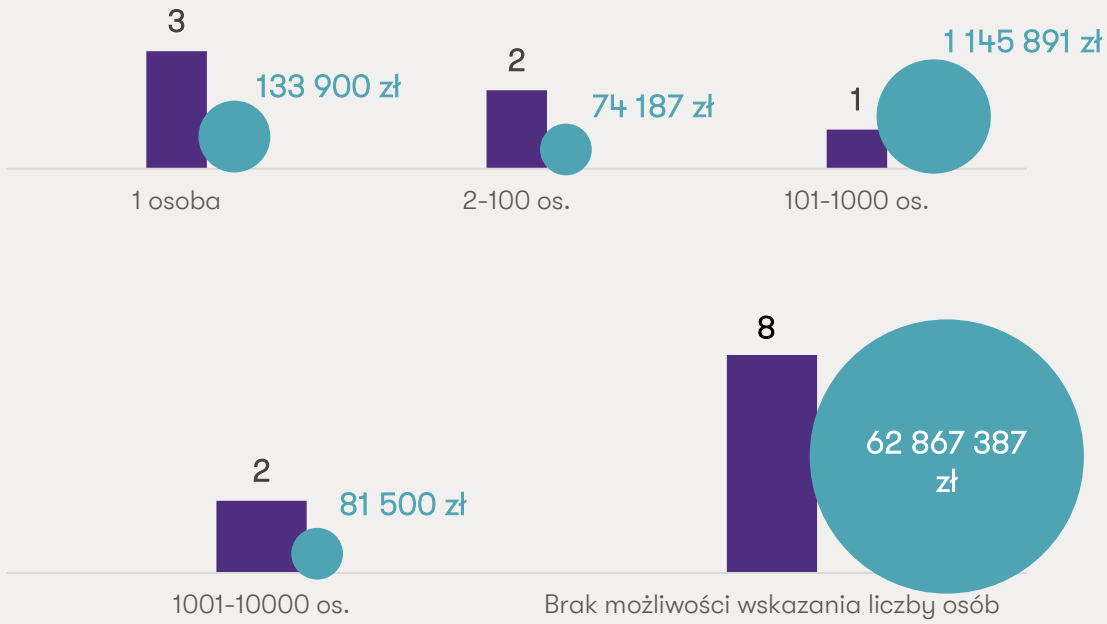
Łączna liczba osób, których dotyczą naruszenia powstałe w wyniku działań lub zaniechań ukaranych podmiotów, wynosi co najmniej 3,8 tys.

Warto jednak zaznaczyć, że w rzeczywistości ta liczba może być znacznie wyższa (nawet 30 mln, w przypadku osób, których dane wykorzystano do próby organizacji wyborów kopertowych), ponieważ część administratorów nie była w stanie dokładnie określić liczby osób dotkniętych incydentami lub informacja ta nie była wskazana w uzasadnieniu decyzji Prezes UODO.

W 2025 r. naruszenia obejmowały zarówno pojedyncze osoby, jak i zdarzenia dotyczące kilku tysięcy osób, m.in. w wyniku ataków ransomware czy ujawnienia danych pracowników jednostek publicznych. Pokazuje to, że administratorzy muszą dbać o bezpieczeństwo zarówno dużych zbiorów danych, jak i danych jednostkowych, ponieważ każde naruszenie niesie ryzyko konsekwencji administracyjnych i reputacyjnych.

Zakres naruszonych danych był bardzo szeroki - od podstawowych danych kontaktowych i identyfikacyjnych, po dane szczególnych kategorii.
W 11 przypadkach kary dotyczyły danych zwykłych o wysokim wpływie na osobę (np. numer PESEL, dane z dokumentu tożsamości), co skutkowało surowszymi sankcjami. Osiem decyzji odnosiło się natomiast do danych wrażliwych, głównie dotyczących zdrowia oraz orientacji seksualnej.

Wykres 4. Liczba osób, których dotyczyło naruszenie w 2025 r. oraz nałożone w wyniku wykrycia naruszenia kary pieniężne



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Naruszenia umyślne ostrzej karane

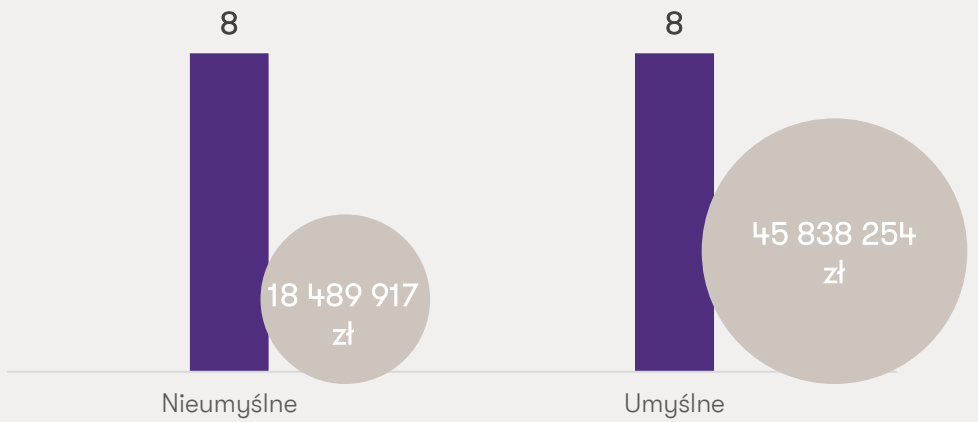
W odróżnieniu od poprzednich lat, w roku 2025 liczba naruszeń umyślnych i nieumyślnych była taka sama, czyli po 8 przypadków każdego typu.

Rozbieżność pojawiła się natomiast pod względem wysokości kar. Kary za naruszenia umyślne były ponad dwukrotnie wyższe niż kary za naruszenia nieumyślne. Naruszenia umyślne w decyzjach Prezesa UODO z 2025 r. obejmowały przede wszystkim sytuacje, w których administrator w sposób świadomy zaniechał realizacji swoich obowiązków lub podjął działania, które wprost naruszały przepisy o ochronie danych osobowych.

Do tego rodzaju naruszeń zaliczały się przypadki niezgłoszenia naruszenia ochrony danych w ustawowym terminie 72 godzin, sytuacje, w których dochodziło do celowego lub rażąco nieodpowiedzialnego ujawnienia danych osobowych, np. podczas konferencji prasowych. W tej kategorii znalazły się również przypadki przetwarzania danych bez wymaganej podstawy prawnej oraz naruszenia związane z niewłaściwym funkcjonowaniem Inspektora Ochrony Danych.

Naruszenia nieumyślne wynikały natomiast z błędów, zaniedbań lub niewystarczającej staranności w procesach przetwarzania danych. Do tej kategorii należały między innymi incydenty spowodowane błędem ludzkim, takie jak przypadkowe ujawnienie dokumentów, przesłanie korespondencji do niewłaściwego odbiorcy czy zagubienie nośników danych, w szczególności pendrive'ów lub dokumentacji papierowej. Znaczącą część naruszeń nieumyślnych stanowiły również skutki ataków ransomware, którym administrator nie był w stanie zapobiec z uwagi na niewdrożenie adekwatnych środków technicznych i organizacyjnych.

Wykres 5. Liczba i łączna wartość kar w 2025 r. w podziale na umyśle i nieumyślne naruszenia przepisów



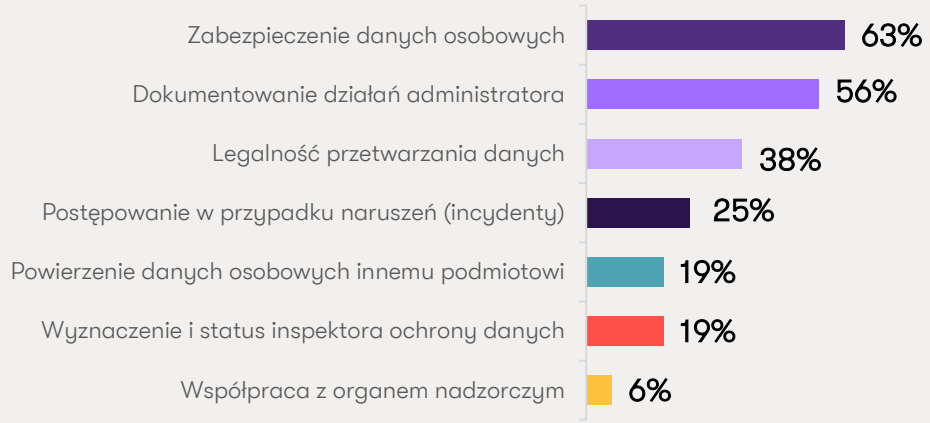
Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Jakie naruszenia zdarzają się najczęściej?

W 2025 r. najczęściej stwierdzane naruszenia, które skutkowały karami administracyjnymi, dotyczyły niewłaściwego zabezpieczenia danych osobowych. Stanowiły ponad 60% incydentów.

Problemy wynikały głównie z braku adekwatnych środków technicznych i organizacyjnych, nieprawidłowych konfiguracji systemów, braku testowania i monitorowania zabezpieczeń oraz stosowania przestarzałych technologii. Istotną część decyzji (56%) stanowiły również naruszenia związane z dokumentowaniem działań administratora – w wielu przypadkach nie można było wykazać faktycznego wdrożenia procedur ani przedstawić dokumentacji potwierdzającej zgodność przetwarzania z RODO.

Wykres 6. Nakładane przez Prezesa UODO administracyjne kary pieniężne w 2025 r. w podziale na obszary, których dotyczyło naruszenie



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Często pojawiały się też naruszenia legalności przetwarzania danych osobowych (38%), obejmujące brak podstawy prawnej, przetwarzanie wykraczające poza cel, nieuprawnione ujawnianie danych podczas konferencji, niewłaściwe wykorzystywanie danych w wyborach korespondencyjnych oraz nadmiarowe kopiowanie dokumentów tożsamości klientów na potrzeby procedur AML.

Naruszenia związane z postępowaniem po incydencie (25%) dotyczyły m.in. przekroczeń terminów zgłoszeń do UODO, opóźnionego powiadamiania osób, których dane dotyczą, i niewłaściwego zarządzania incydentami. Problemy z powierzeniem danych innym podmiotom (19%) wynikały z braku nadzoru nad procesorami, niekompletnych umów powierzenia i niejasnego określenia ról w łańcuchu przetwarzania.

Naruszenia dotyczące wyznaczenia i statusu inspektora ochrony danych (19%) dotyczyły głównie braku niezależności i odpowiedniego umocowania IOD w strukturze organizacyjnej

Jakie błędy popełnia administrator?

Administratorzy w głównej mierze zaniedbują kwestie wdrożenia odpowiednich środków zabezpieczających dane osobowe oraz przeprowadzenia prawidłowej analizy ryzyka.

Tabela 1. Liczba naruszeń obowiązków przez administratora w podziale na przepisy RODO

Przepis RODO	Obowiązek administratora	Liczba naruszeń
Art. 5 ust. 1 lit. a	Zasada legalności, rzetelności i przejrzystości przetwarzania danych	5
Art. 5 ust. 1 lit. f	Zasada integralności i poufności danych	3
Art. 5 ust. 2	Zasada rozliczalności – zdolność wykazania zgodności przetwarzania	3
Art. 6 ust. 1	Legalność przetwarzania danych osobowych	5
Art. 9 ust. 1	Legalność przetwarzania danych szczególnych kategorii	4
Art. 13 ust. 1	Obowiązek informacyjny przy zbieraniu danych	1
Art. 24 ust. 1	Odpowiedzialność administratora za zgodność z RODO oraz wdrażanie właściwych środków	9
Art. 25 ust. 1	Uwzględnienie ochrony danych w fazie projektowania (privacy by design)	9
Art. 28 ust. 1	Powierzenie danych osobowych podmiotom zapewniającym wystarczające gwarancje	2
Art. 28 ust. 3 lit. c	Zapewnienie, aby podmiot przetwarzający wdrażał odpowiednie środki	1
Art. 28 ust. 4	Przetwarzanie przez dalszego procesora (subprocesora)	1
Art. 33 ust. 1	Zgłoszenie naruszenia ochrony danych organowi nadzorczemu	3
Art. 32 ust. 1 i 2	Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych	11
Art. 34 ust. 1	Zawiadomienie osoby, której dane dotyczą, o naruszeniu	3
Art. 38 ust. 1	Zapewnienie wsparcia dla IOD oraz właściwych warunków wykonywania funkcji	2
Art. 38 ust. 6	Zapewnienie braku konfliktu interesów IOD	1
Art. 58 ust. 1 lit. a	Współpraca z organem nadzorczym	1
Art. 58 ust. 1 lit. e	Obowiązek udzielania informacji	1

Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Rekordowe kary sygnałem końca taryfy ulgowej

Rok 2025 i rekordowe kary na łącznym poziomie prawie 65 mln złotych pokazują jasno, że zakończył się okres ulgowy związany z wdrażaniem RODO. Urząd Ochrony Danych Osobowych daje wyraźny sygnał, że po ponad 8 latach obowiązywania przepisów nie ma już miejsca na tłumaczenie się brakiem doświadczenia czy nieświadomością.

Decyzje Prezesa UODO pokazują również wyraźnie, że zapewnienie zgodności z przepisami nie powinno być traktowane jako jednorazowy projekt, a stały element funkcjonowania firmy wpisany we wszystkie jej procesy.

Dlatego nawet najbardziej rozbudowana dokumentacja i komplet procedur nie zagwarantują firmie bezpieczeństwa. Kluczowe jest ich realne stosowanie oraz mechanizmy weryfikujące ich skuteczność. Prezes UODO w decyzjach regularnie podnosi zarzuty dotyczące braku szkoleń podnoszących świadomość pracowników, korzystania z nieaktualnego oprogramowania, nieweryfikowania podmiotów, którym powierzane są dane, czy rozmytej odpowiedzialności w strukturze organizacyjnej.

Dla firm oznacza to konieczność przejścia od „RODO na papierze" do „RODO w działaniu". Wyznaczenie realnie umocowanej osoby odpowiedzialnej za obszar ochrony danych, regularne audyty, podnoszenie świadomości pracowników oraz praktyczne testowanie procedur to dziś nie tylko dobra praktyka, ale również warunek ograniczenia ryzyka finansowego i reputacyjnego dla firm.

Emilia Martynowicz-Mamajek
Associate
Kancelaria Prawna
Grant Thornton

Krzysztof Jeromin
Junior Associate
Kancelaria Prawna
Grant Thornton

Część 2.

CASE STUDY
Czego uczą nas działania Prezesa UODO?

Grant Thornton

#1 Niezależność IOD pod lupą UODO

Litera prawa:
Inspektor Ochrony Danych powinien pełnić swoją funkcję w sposób niezależny, bez konfliktu interesów, aby skutecznie monitorować zgodność działań administratora z RODO. W ostatnich latach Prezes UODO coraz częściej bada, czy organizacje zapewniają IOD realną niezależność, traktując to jako kluczowy element skutecznego systemu ochrony danych.

Opis sprawy:
W sprawie **DKN.5131.7.2025** Prezes UODO w wyniku zgłoszenia naruszenia przez podmiot leczniczy zauważył, że w spółce funkcje IOD przez prawie sześć lat pełniła ta sama osoba, która była jednocześnie prezesem zarządu. W związku z tym organ poprosił spółkę o wyjaśnienia. Spółka argumentowała, że połączenie funkcji nie rodzi konfliktu interesów, powołując się na wewnętrzną analizę oraz względy organizacyjne i finansowe.

Działania organu:
Prezes UODO uznał, że połączenie obu ról uniemożliwia rzeczywiste zachowanie niezależności IOD, ponieważ prezes zarządu decyduje o celach i sposobach przetwarzania danych i nie może bezstronnie monitorować zgodności działań z RODO. Organ podkreślił, że konflikt interesów ma charakter obiektywny i nie może być wyłączony deklaracją administratora ani wewnętrzną analizą zatwierdzoną przez zainteresowaną osobę. W konsekwencji na spółkę nałożono administracyjną karę pieniężną w wysokości **11 365 zł**.

Wnioski

IOD powinien mieć odpowiednie umocowanie w strukturze organizacyjnej, zapewniające niezależność od zarządu i działów operacyjnych.

Nie można łączyć funkcji IOD z rolami decyzyjnymi w zakresie przetwarzania danych.

Wewnętrzne analizy czy deklaracje administratora nie zastępują realnej niezależności IOD.

Niezależność IOD nie tylko na papierze

Niezależność Inspektora Ochrony Danych stanowi jeden z fundamentalnych filarów systemu ochrony danych osobowych przewidziany w RODO. Jak jednoznacznie pokazuje praktyka Prezesa Urzędu Ochrony Danych Osobowych niezależność ta nie może być traktowana w sposób wyłącznie formalny lub deklaratywny. Prezes UODO konsekwentnie podkreśla, że sama czynność wyznaczenia IOD nie jest wystarczająca, jeżeli nie towarzyszy jej realne zapewnienie warunków umożliwiających niezależne, obiektywne i skuteczne wykonywanie tej funkcji.

W decyzjach wydawanych w ostatnich latach organ nadzorczy wielokrotnie wskazywał, że poważnym naruszeniem przepisów RODO jest powierzanie funkcji Inspektora Ochrony Danych osobom zajmującym stanowiska kierownicze lub pełniącym role decyzyjne w zakresie celów i sposobów przetwarzania danych osobowych – przykładem jest najnowsza kara z 2026 r. dla Poczty Polskiej za brak zapewnienia niezależności sprawowania funkcji IOD, która wyniosła 978 tys. zł.

Wynika to z faktu, że tego rodzaju kumulacja kompetencji prowadzi do oczywistego konfliktu interesów, w którym ta sama osoba z jednej strony kształtuje procesy przetwarzania danych, a z drugiej ma je nadzorować i oceniać pod kątem zgodności z RODO. W ocenie Prezes UODO taka konstrukcja organizacyjna podważa sens istnienia funkcji IOD.

Organ nadzorczy zwraca również szczególną uwagę na kwestie podporządkowania służbowego Inspektora Ochrony Danych. Prezes UODO konsekwentnie wskazuje, że brak wyraźnego organizacyjnego i merytorycznego rozdzielenia funkcji decyzyjnych od kontrolnych prowadzi do faktycznego pozbawienia IOD gwarancji niezależności, nawet jeśli formalnie spełnione są wymogi dotyczące jego powołania.

Na szczególne podkreślenie zasługuje fakt, że w sprawach dotyczących niezależności Inspektora Ochrony Danych Prezes UODO coraz częściej sięga po administracyjne kary pieniężne. Naruszenia te są kwalifikowane jako mające charakter systemowy, ponieważ bezpośrednio wpływają na całościowy poziom ochrony danych osobowych w organizacji. Dla administratorów danych oznacza to konieczność krytycznej oceny nie tylko formalnego statusu IOD, lecz także jego faktycznej pozycji w strukturze organizacyjnej, zakresu powierzonych mu obowiązków oraz realnej możliwości działania bez konfliktów interesów.

Krzysztof Jeromin
Junior Associate
Kancelaria Prawna
Grant Thornton

#2 AML a RODO - gdzie kończy się obowiązek, a zaczyna naruszenie?

Opis sprawy:

Od 1 kwietnia 2019 r. do 23 września 2020 r. ING Bank Śląski masowo skanował dokumenty tożsamości klientów i potencjalnych klientów, tłumacząc to koniecznością realizacji obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy (AML). W praktyce kopiowano jednak dokumenty również w sytuacjach teoretycznie niepowiązanych z tymi obowiązkami, np. przy reklamacjach bankomatu. Jednocześnie bank nie przeprowadzał indywidualnej analizy ryzyka ani oceny, czy kopiowanie dokumentów było faktycznie niezbędne do realizacji wymogów prawnych wynikających z ustawy AML.

Działania organu:

Prezes UODO przeprowadził kontrolę w banku, sprawdzając m.in. podstawę prawną przetwarzania danych, zakres i cel zbierania kopii dokumentów tożsamości oraz sposób ich przetwarzania. Organ ustalił, że po zmianie procedur bank zaczął automatycznie wykonywać skany dokumentów w przypadkach przewidzianych w instrukcjach, nie weryfikując przy tym, czy każdorazowo było to konieczne. Prezes UODO podkreślił, że legalne skanowanie dokumentów przez instytucje obowiązane jest dopiero wtedy, gdy wynika z realnej potrzeby stosowania środków przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, opartej na indywidualnej ocenie ryzyka. W związku z tym Prezes UODO nałożył na ING Bank Śląski administracyjną karę pieniężną w wysokości 18 416 400 zł. Organ wskazał, że naruszenie dotyczyło przede wszystkim bezpodstawnego przetwarzania danych osobowych w dużej skali, co stwarzało realne ryzyko dla praw i wolności klientów

Wnioski

Każde przetwarzanie danych pozyskiwanych poprzez skanowanie dokumentów powinno być poprzedzone oceną celowości i ryzyka, aby upewnić się, że jest niezbędne.

Wewnętrzne procedury nie mogą zastępować merytorycznej oceny potrzeby przetwarzania danych.

Nawet jeśli dane nie należą do szczególnych kategorii, ich zakres może rodzić wysokie ryzyko naruszenia praw osób, np. poprzez kradzież tożsamości czy wyłudzenia.

Czy przetwarzasz tylko niezbędne dane osobowe?

Rok 2025 pokazuje wyraźny zwrot w polityce nakładania kar przez Prezesa UODO. W poprzednich latach decyzje organu koncentrowały się głównie na kwestiach związanych z obsługą incydentów czy zabezpieczeniem danych osobowych. W 2025 r. Prezes UODO przesuwa nacisk na wcześniejszy etap - weryfikację, czy administratorzy mają rzeczywistą podstawę do przetwarzania danych osobowych oraz czy nie przetwarzają ich w sposób nadmiarowy.

Oznacza to, że administratorzy powinni szczególnie zwracać uwagę na wszystkie procesy przetwarzania danych, upewniając się, że przetwarzane są wyłącznie dane niezbędne do realizacji celu i że nie dochodzi do nadmiarowego gromadzenia informacji. Dotyczy to w szczególności danych o wysokim ryzyku, takich jak: numery PESEL, dokumenty tożsamości, paszporty, kopie dokumentów, a także danych wrażliwych - np. informacje o stanie zdrowia, dane biometryczne czy zaświadczenia o niekaralności. W przypadku tych szczególnych kategorii danych administratorzy powinni nie tylko zachować wyjątkową ostrożność, ale także upewnić się, że mają odpowiednia podstawę prawną do ich przetwarzania.

Rola Inspektora Ochrony Danych staje się w tym kontekście kluczowa. IOD powinien być włączany we wszystkie procesy przetwarzania danych, aby monitorować ich zgodność z RODO, oceniać ryzyko i wspierać administratora w podejmowaniu decyzji.

Skuteczny nadzór IOD zwiększa szanse na uniknięcie nadmiernego przetwarzania i ryzyka naruszeń, a tym samym zmniejsza ryzyko nakładania kar przez Prezesa UODO.

Emilia Martynowicz-Mamajek
Associate
Kancelaria Prawna
Grant Thornton

Część 3.

Wywiąż się z obowiązków!

Na jakich zasadach nakładane są kary pieniężne w obszarze RODO?

Grant Thornton

Od czego zależy nałożenie kary i jej wysokość?

Administracyjne kary pieniężne nakłada się zależnie od okoliczności każdego indywidualnego przypadku.

Organ nadzorczy - w przypadku Polski jest to Prezes Urzędu Ochrony Danych Osobowych - decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, w każdym przypadku zwraca uwagę na **11 szczegółowo opisanych kryteriów**, m.in. na:

a. charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,
b. umyślny lub nieumyślny charakter naruszenia,
c. działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,
d. stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem wdrożonych środków technicznych i organizacyjnych,
e. kategorie danych osobowych, których dotyczyło naruszenie.

Co więcej administracyjne kary pieniężne powinny być w każdym indywidualnym przypadku **skuteczne, proporcjonalne i odstraszające**.

Pułapy wysokości administracyjnych kar pieniężnych

do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa

w przypadku naruszenia obowiązków administratora i podmiotu przetwarzającego związanych z m.in.:

- uwzględnianiem ochrony danych w fazie projektowania,
- kwestiami związanymi z powierzeniem przetwarzania danych osobowych,
- współpracą z organem nadzorczym,
- zapewnieniem bezpieczeństwa przetwarzania,
- zgłaszaniem naruszenia ochrony danych osobowych organowi nadzorczemu,
- zawiadamianiem osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa

w przypadku naruszenia m.in.:

- zasad dotyczących przetwarzania danych osobowych,
- podstaw prawnych przetwarzania zwykłych danych osobowych,
- podstaw prawnych przetwarzania szczególnych kategorii danych osobowych,
- praw osób, których dane dotyczą,
- przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej,
- nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy

Kara pieniężna może być **ograniczona** do wysokości:

a. **100 000 zł**, w przypadku naruszeń jednostek sektora finansów publicznych, instytutów badawczych, Narodowego Banku Polskiego.
b. **10 000 zł** w przypadku naruszeń państwowych i samorządowych instytucji kultury.

Jeśli administrator lub podmiot przetwarzający narusza kilka przepisów RODO w ramach tych samych lub powiązanych operacji, kara pieniężna **nie może być wyższa niż za najpoważniejsze naruszenie.**

Dodatkowo Europejska Rada Ochrony Danych przyjęła w 2023 r. Wytyczne 04/2022 EROD dotyczące **obliczania** administracyjnych **kar pieniężnych** na podstawie RODO (link).

Zapraszamy do kontaktu

Emilia Martynowicz-Mamajek
Associate
Kancelaria Prawna
Grant Thornton
M +48 667 778 891
E emilia.martynowicz-mamajek@pl.gt.com

Krzysztof Jeromin
Junior Associate
Kancelaria Prawna
Grant Thornton
M +48 785 640 434
E Krzysztof.Jeromin@pl.gt.com

Kontakt dla mediów:

Jacek Kowalczyk
Dyrektor Marketingu i PR
Grant Thornton
T +48 505 024 168
E Jacek.Kowalczyk@pl.gt.com

O nas

Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie, obecna w 156 krajach i zatrudniająca ponad 76 tys. pracowników. W Polsce działamy od 1993 roku. Zespół 1200 pracowników wspiera naszych klientów w obszarach takich jak doradztwo podatkowe, doradztwo transakcyjne, prawne, finansowe, outsourcing płac i kadr oraz outsourcing księgowości, czy audyt.

Załącznik

Wykaz opublikowanych decyzji wydanych w 2025 r. przez Prezesa UODO nakładających administracyjne kary pieniężne

Opublikowane decyzje Prezesa UODO nakładające administracyjne kary pieniężne w 2025 r.

Lp.	Podmiot	Data decyzji	Sygnatura	Wysokość kary
1	Centrum Medyczne Ujastek Sp. z o.o.	17 stycznia 2025 r.	DKN.5131.4.2024	1 145 891,25 zł
2	J. w M. S.A. w likwidacji z siedzibą w M.	6 marca 2025 r.	DKN.5112.10.2024	56 824,00 zł
3	(1) Minister cyfryzacji (2) Poczta Polska S.A.	17 marca 2025 r.	DKN.5131.1.2025	100 000,00 zł 27 124 816,00 zł
4	Komendant Główny Policji z siedzibą w Warszawie	19 marca 2025 r.	DS.523.4750.2023	75 000.00 zł
5	G. M. prowadząca działalność gospodarczą pod firmą U.	01 kwietnia 2024 r.	DKN.5131.10.2023	33 673,00 zł
6	(1) Gminny Ośrodek Pomocy Społecznej w Aleksandrowie (2) Wójt w Aleksandrowie	3 czerwca 2025 r.	DKN.5131.30.2022	5 000,00 zł 10 000,00 zł
7	Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku	17 czerwca 2025 r.	DKN.5131.48.2022	65 500,00 zł
8	(1) Mc Donald's Polska Sp. z o.o. (2) Communication Sp. z o.o.	23 czerwca 2025	DKN.5130.4179.2020	16 932 657,00 zł 183 858,00 zł
9	A. Z., prowadzącego działalność gospodarczą pod firmą „W." z siedzibą w T. przy ul. (...)	23 czerwca 2025	DKE.561.1.2025	18 941,00 zł
10	Niepubliczny Zakład Opieki Zdrowotnej (...) H. Sp. z o.o. z siedzibą w R.	4 lipca 2025	DKN.5131.17.2022	32 832,00 zł
11	ING Bank Śląski S.A.	23 lipca 2025	DKN.5112.6.2020	18 416 400,00 zł
12	Q. Sp. z o.o. (ul. (...), (...)-(...) H.)	12 września 2025	DKN.5131.7.2025	11 365,00 zł
13	B. Sp. z o.o. z siedzibą w M. przy ul. (...)	15 października 2025	DKN.5131.3.2025	40 514,00 zł
14	Komornik Sądowy przy Sądzie Rejonowym w S. B. F. Kancelaria (...) w S. (ul. (...), (...)-(...) S.)	23 października 2025	DKN.5131.17.2024	20 900,00 zł
15	Państwowy Powiatowy Inspektor Sanitarny w Policach	15 listopada 2025	DKN.5131.3.2024	20 000,00 zł
16	Komendant Miejski Policji w Krakowie	29 grudnia 2025	DKN.5131.5.2024	38 000,00 zł

Łączna wartość kar: 64 333 171,25 zł