RAPORT 2025

Stosowanie RODO w Polsce. Analiza decyzji UODO

Statystyki, kluczowe obszary ryzyka i prognozy

Autorzy raportu:
r. pr. Karolina Kukielska
Tomasz Ochocki

Z Raportu dowiesz się...

Raport „Stosowanie RODO w Polsce – 2025. Analiza decyzji UODO” stanowi przekrojowe podsumowanie praktyki nadzorczej Prezesa Urzędu Ochrony Danych Osobowych w 2025 r.

Z Raportu dowiesz się, jak RODO było faktycznie stosowane w Polsce, za jakie naruszenia organ nakładał administracyjne kary pieniężne oraz które obszary przetwarzania danych generowały największe ryzyka dla administratorów i podmiotów przetwarzających.

Podstawą raportu są opublikowane decyzje Prezesa UODO dotyczące nałożenia administracyjnych kar pieniężnych (dane aktualne na dzień: 10.02.2026 r.; faktyczna liczba decyzji może się różnić, albowiem nie wszystkie mogły zostać opublikowane), uzupełnione danymi statystycznymi, porównaniami rok do roku oraz odniesieniami do praktyki innych państw UE. Analiza koncentruje się nie na interpretacji przepisów, lecz na konkretnych błędach, zaniedbaniach i schematach naruszeń, które realnie skutkowały sankcjami finansowymi.

URZĄD OCHRONY DANYCH OSOBOWYCH

W raporcie znajdziesz

W raporcie znajdziesz m.in.:

- statystyki dotyczące liczby i wysokości kar nakładanych przez Prezesa UODO w 2025 r.,
- **najczęściej naruszane przepisy RODO** oraz obszary, na których w minionym roku koncentrował się organ nadzorczy,
- **przegląd najciekawszych i najistotniejszych decyzji Prezesa UODO** wraz z praktycznymi wnioskami do wykorzystania w codziennej pracy,
- czynniki łagodzące i obciążające, które miały realny wpływ na wymiar administracyjnych kar pieniężnych,
- **rekomendacje**, pomagające ograniczyć ryzyko naruszeń i odpowiedzialności,
- **prognozy na 2026 r.**, wskazujące obszary, które – w świetle decyzji i sygnałów płynących z praktyki nadzorczej – mogą znaleźć się w centrum zainteresowania UODO.

Raport został przygotowany przez praktyków ochrony danych. Jego celem jest dostarczenie konkretnej i użytecznej wiedzy, którą możesz bezpośrednio wykorzystać w audytach zgodności, projektowaniu procesów, zarządzaniu ryzykiem oraz bieżącej pracy z RODO.

Spis treści

1 Struktura podmiotów ukaranych przez UODO w 2025 r.

2 Różnice w karach na przestrzeni lat 2023–2025

3 Za co UODO nakładał kary w 2025 r.

4 Polska na tle Europy

5 Przegląd najciekawszych kar

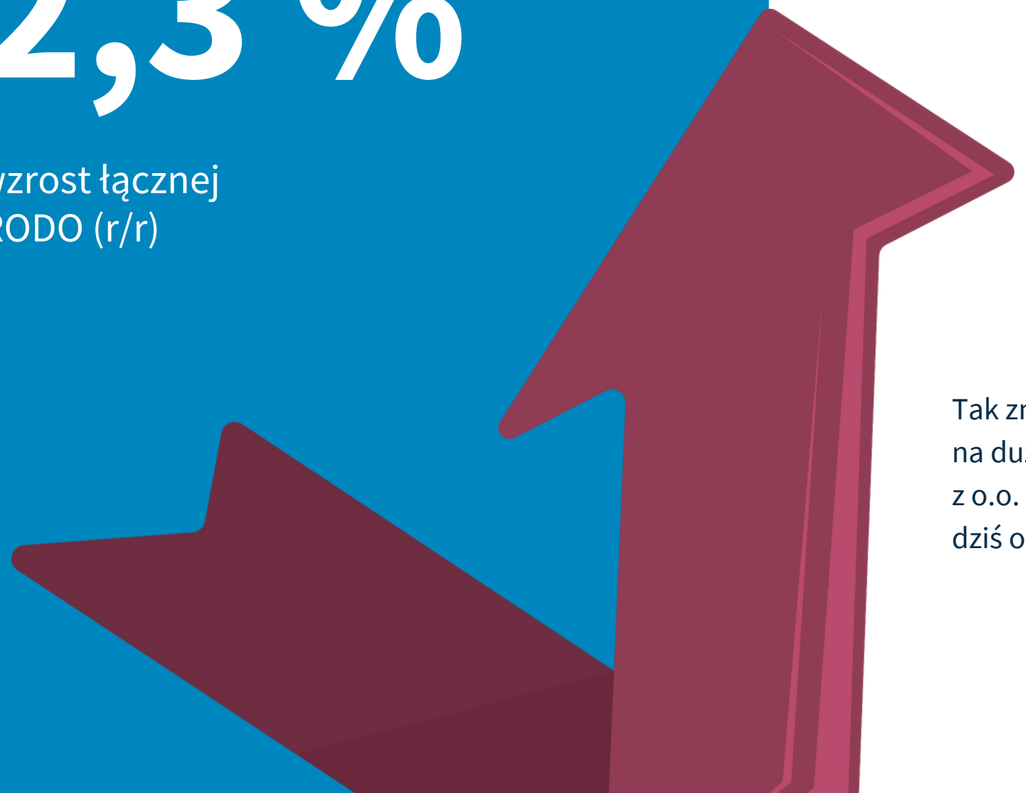
6 Jak organ ustala wysokość kary

7 Prognoza na 2026 r.

Wzrost wartości kar RODO

362,3 %

Procentowy wzrost łącznej wartości kar RODO (r/r)



Rok 2025 okazał się **rekordowy pod względem wysokości kar nakładanych przez Prezesa UODO**. Choć liczba decyzji nie wzrosła (na dzień wydania Raportu, organ opublikował ich jedynie 19), łączna kwota kar zwiększyła się niemal pięciokrotnie w porównaniu z rokiem poprzednim i osiągnęła:

64 291 471,25 zł.

Tak znaczący wzrost to **efekt kilku głośnych, wielomilionowych kar**, nałożonych na duże podmioty: Pocztę Polską SA, ING Bank Śląski oraz McDonald’s Polska sp. z o.o. Każda z tych spraw istotnie wpłynęła na roczny bilans i dobrze pokazuje, że dziś o „rekordowym” roku mogą przesądzić pojedyncze decyzje.

Wartości graniczne kar RODO w 2025 r.

5000,00 zł

Najniższa kara

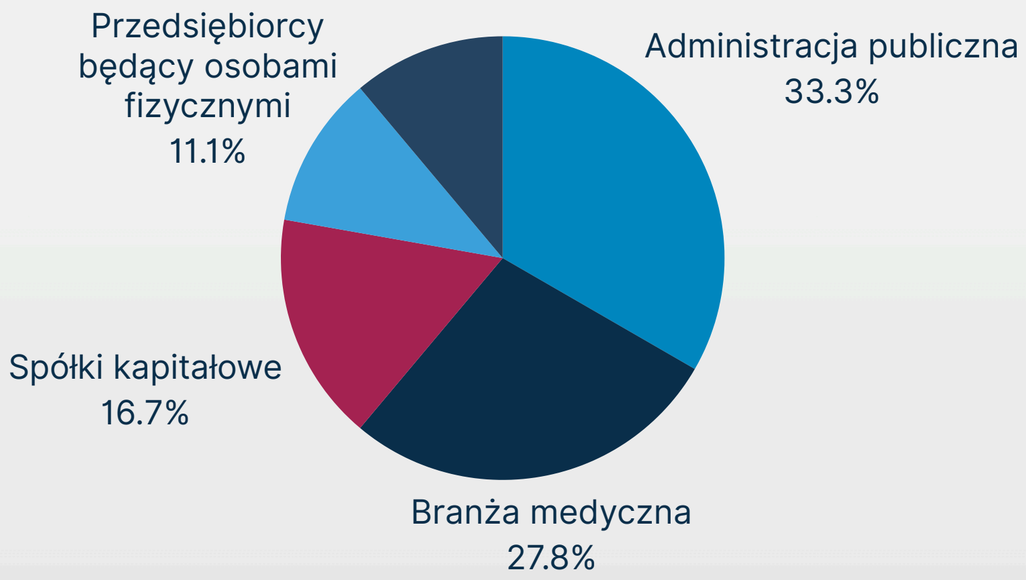
na Gminny Ośrodek Pomocy Społecznej w Aleksandrowie

27 124 816,00 zł

Najwyższa kara

nałożona na Pocztę Polską SA.

Struktura podmiotów ukaranych



Struktura podmiotów ukaranych przez UODO w 2025 r. pokazuje, że działania organu nadzorczego obejmują **szerokie spektrum administratorów danych** – z sektora zarówno publicznego, jak i prywatnego.

Największy udział mają **instytucje publiczne i samorządowe** (33%), co potwierdza, że obowiązki wynikające z RODO są egzekwowane także wobec podmiotów realizujących zadania publiczne.

Istotną grupę stanowią również **podmioty z branży medycznej** (28%). Wynika to bezpośrednio z przetwarzania danych szczególnych kategorii oraz z podwyższonych wymogów w zakresie bezpieczeństwa i legalności przetwarzania. W tym kontekście sektor ochrony zdrowia pozostaje obszarem podwyższonego ryzyka regulacyjnego.

Pozostałe kategorie – **spółki kapitałowe, spółki Skarbu Państwa oraz przedsiębiorcy prowadzący działalność jednoosobową** – łącznie odpowiadają za niemal 40% ukaranych podmiotów. To jasno pokazuje, że skala działalności ani forma prawna nie stanowią ochrony przed odpowiedzialnością administracyjną.

Wnioski z wykresu potwierdzają uniwersalny charakter egzekwowania RODO oraz rosnącą potrzebę wdrażania adekwatnych mechanizmów compliance we wszystkich sektorach, niezależnie od profilu działalności.

Różnice w karach na przestrzeni lat 2023–2025

	2023	2024	2025
Liczba ukaranych podmiotów	31	27	22
Łączna wysokość kar	1 230 331,28 PLN	13 907 740, 96 PLN	64 291 471,25 PLN
Najwyższa kara	282 960,00 PLN	4 053 174,00 PLN	27 124 816,00 PLN
Najniższa kara	472 PLN	916,71 PLN	5000,00 PLN

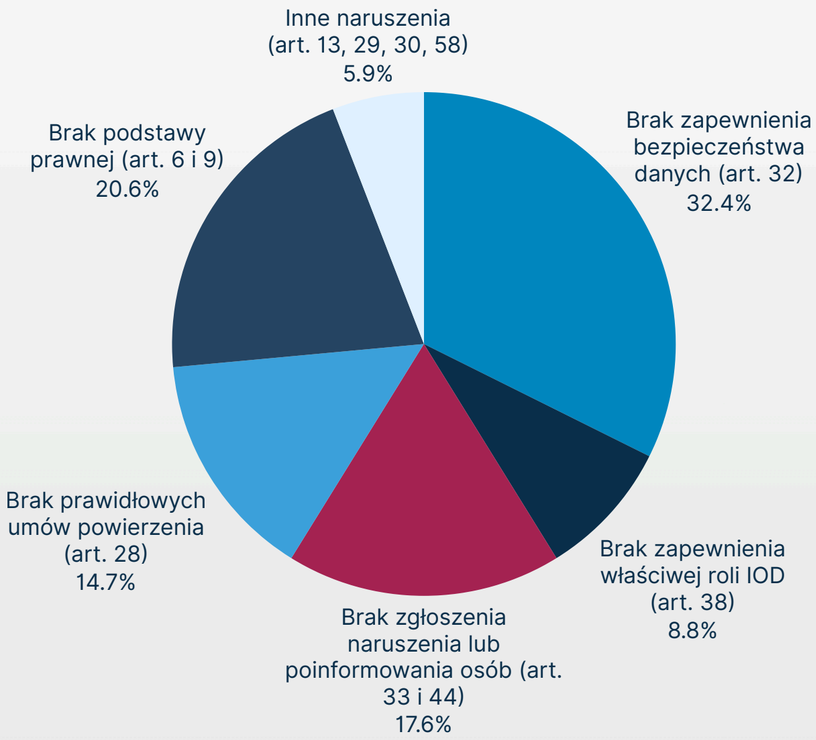
Dane za lata 2023–2025 wskazują na **wyraźny i dynamiczny wzrost restrykcyjności polityki sankcyjnej** przy jednoczesnym spadku liczby ukaranych podmiotów w 2025 r. (dane niepełne).

Najbardziej zauważalny jest **skokowy wzrost łącznej wysokości kar**: od ok. 1,23 mln zł w 2023 r., przez 13,9 mln zł w 2024 r., aż do ponad 64 mln zł w 2025 r. Oznacza to ponad **50-krotny wzrost w porównaniu z 2023 r.**, co sugeruje zmianę podejścia organu nadzorczego: z nakładania sankcji o charakterze głównie dyscyplinującym na wymierzanie kar o realnym, dotkliwym wymiarze finansowym.

Jednocześnie widoczny jest **spadek liczby ukaranych podmiotów (**wedle dostępnych danych: 31 – w 2023 r., 27 – w 2024 r., 22 – w 2025 r.). W połączeniu ze wzrostem łącznej kwoty kar wskazuje to na koncentrację na mniejszej liczbie spraw, lecz mających większą wagę i potencjalnie dotyczących poważnych lub poważnych lub systemowych naruszeń.

Z perspektywy podmiotów objętych regulacją oznacza to rosnące ryzyko finansowe i konieczność realnego, a nie tylko formalnego wdrażania mechanizmów zgodności i bezpieczeństwa przetwarzanych danych.

Za co UODO nakładał kary w 2025 r.



Całościowo wykres pokazuje, że Prezes UODO koncentruje się przede wszystkim na egzekwowaniu fundamentalnych obowiązków systemowych, a nie wyłącznie na reakcji na pojedyncze incydenty. Dominują naruszenia, które świadczą o braku dojrzałości organizacyjnej, a nie jedynie o popełnieniu błędów technicznych.

Naruszenia art. 32 RODO stanowią 30% wszystkich przypadków, co wskazuje na utrzymujące się problemy z adekwatnością środków technicznych i organizacyjnych oraz z oceną ryzyka po stronie administratorów.

Drugą najczęściej sankcjonowaną kategorią jest brak podstawy prawnej przetwarzania (art. 6 i 9 RODO). Odpowiada ona za 21% naruszeń. Wysoki udział tej kategorii dowodzi, że mimo kilkuletniego obowiązywania RODO w praktyce nadal dochodzi do błędów na poziomie fundamentalnych zasad legalności przetwarzania.

Na szczególną uwagę zasługuje połączona kategoria: brak zgłoszenia naruszenia lub poinformowania osób, których dane dotyczą (art. 33 i 34 RODO). Stanowi ona 18% przypadków. Oznacza to, że niemal co piąta kara jest związana z nieprawidłową reakcją na incydent, a nie z samym jego wystąpieniem. Wskazuje to na istotne braki zarówno w procedurach zarządzania naruszeniami, jak i w gotowości organizacyjnej do działania pod presją czasu.

Kolejne istotne grupy naruszeń mają charakter organizacyjno-kontraktowy:

- niewypełnianie obowiązków związanych z powierzeniem przetwarzania (art. 28 RODO)– 15%,
- brak zapewnienia właściwej roli inspektora ochrony danych (art. 38 RODO) – 9%.

Relatywnie niewielki udział kategorii: inne naruszenia (6%) sugeruje, że praktyka egzekucyjna koncentruje się na najważniejszych obowiązkach RODO, mających bezpośredni wpływ na prawa i wolności osób fizycznych.

Polska na tle Europy

Liczba decyzji

Kraje	2023	2024
Niemcy (wszystkie landy)	469	416
Hiszpania	367	281
Włochy	146	140
Polska	30	22

Analiza porównawcza praktyki w państwach UE pokazuje istotne zróżnicowanie aktywności organów nadzorczych w zakresie nakładania administracyjnych kar pieniężnych. **Niemcy, Hiszpania i Włochy** konsekwentnie pozostają w ścisłej czołówce krajów o najwyższej liczbie decyzji sankcyjnych, co odzwierciedla zarówno skalę rynku, jak i dojrzałość oraz intensywność działań nadzorczych.

Polska na tle Europy

Wysokość kar vs. liczba decyzji

Kraje	Wysokość kary	Liczba decyzji
2023		
Irlandia	1 551 782 500 €	6
Holandia	243 160 000 €	8
Włochy	79 164 500 €	37
2024		
Irlandia	652 029 500 €	7
Holandia	328 030 000 €	16
Francja	145 332 449 €	140

Na tym tle Polska zajmuje pozycję umiarkowaną. Liczba decyzji Prezesa UODO jest wyraźnie niższa niż w największych jurysdykcjach, ale jednocześnie wyższa niż w państwach, w których sankcje mają charakter incydentalny (np. w Danii, Finlandii, Luksemburgu czy na Malcie).

Spadek liczby decyzji Prezesa UODO w 2024 r. w porównaniu z 2023 r. wpisuje się w obserwowany trend selektywności, czyli koncentracji na mniejszej liczbie spraw o większym ciężarze gatunkowym.

Z perspektywy europejskiej Polska nie jest ani „liderem sankcji”, ani jurysdykcją pasywną – pozostaje krajem o stabilnej, lecz ewoluującej praktyce nadzorczej

Przegląd najciekawszych kar

Poczta Polska S.A. (DKN.5131.1.2025)

ING Bank Śląski (DKN.5112.6.2020)

McDonald’s Polska + 24/7 Communication (DKN.5130.4179.2020)

Centrum Medyczne Ujastek (DKN.5131.4.2024)

Poczta Polska S.A.

Prezes UODO nałożył na Pocztę Polską rekordową karę w wysokości 27 124 816 zł za bezpodstawne przetwarzanie danych z rejestru PESEL ok. 30 mln obywateli. Dane zostały udostępnione spółce przez Ministra Cyfryzacji w związku z przygotowaniami do wyborów korespondencyjnych w 2020 r., które ostatecznie się nie odbyły.

Prezes UODO uznał, że **Poczta Polska przetwarzała dane bez podstawy prawnej**, z naruszeniem zasad zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a oraz art. 6 ust. 1 RODO). Kluczowe było to, że spółka – mimo działania na podstawie decyzji administracyjnej – **nie zweryfikowała samodzielnie legalności pozyskania i dalszego przetwarzania danych.**

Organ podkreślił, że od spółki Skarbu Państwa realizującej zadania publiczne oczekuje się szczególnie wysokiego standardu staranności i zgodności z prawem. **W tej sprawie ukarany został także Minister Cyfryzacji** (karą w wysokości 100 000 zł – maksymalną dla podmiotu publicznego).

Wnioski praktyczne

- Każdy administrator danych ma obowiązek samodzielnie ocenić podstawę prawną przetwarzania – nawet gdy działa na polecenie organu władzy publicznej.
- Otrzymanie danych od innego podmiotu (w tym państwowego) nie zwalnia z odpowiedzialności za zgodność z RODO.
- Decyzja administracyjna nie zastępuje analizy legalności przetwarzania danych osobowych.

URZĄD OCHRONY DANYCH OSOBOWYCH

ING Bank Śląski

Prezes UODO nałożył na ING Bank Śląski karę w wysokości 18 416 400 zł za bezpodstawne kopiowanie (skanowanie) dokumentów tożsamości klientów i potencjalnych klientów. Naruszenia dotyczyły okresu od kwietnia 2019 r. do września 2020 r. i obejmowały sytuacje niezwiązane z realizacją obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (AML), w tym obsługę reklamacji.

Prezes UODO ustalił, że bank przyjął w swoich procedurach **zbyt szeroki katalog przypadków**, w których uznawał skan dokumentu tożsamości za konieczny, a w praktyce uzależniał wykonanie czynności na rzecz klienta od przekazania kopii dokumentu. Bank nie weryfikował, czy w danym przypadku skan był rzeczywiście niezbędny ani nie dokonywał indywidualnej oceny ryzyka. Organ stwierdził przetwarzanie bez podstawy prawnej oraz naruszenie zasad zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu oraz minimalizacji danych (art. 5 ust. 1 lit. a–c oraz art. 6 ust. 1 RODO). Naruszenie uznano za poważne ze względu na masowy charakter przetwarzania.

Wnioski praktyczne

- Uprawnienia ustawowe (np. wynikające z przepisów AML) nie mogą być interpretowane rozszerzająco – kopiowanie dokumentów tożsamości jest dopuszczalne wyłącznie w sytuacjach wyraźnie przewidzianych przepisami.
- Każdorazowo należy ocenić niezbędność danych w kontekście konkretnej czynności i celu przetwarzania.
- Procedury wewnętrzne nie legalizują przetwarzania danych sprzecznego z RODO.
- Masowe przetwarzanie danych zwiększa poziom odpowiedzialności administratora i wymaga podwyższonego standardu staranności.

URZĄD OCHRONY DANYCH OSOBOWYCH

McDonald’s Polska i 24/7 Communication

23 czerwca 2025 r. Prezes UODO nałożył na McDonald’s Polska (administrator) karę w wysokości 16 932 657 zł, a na 24/7 Communication (procesor) – 183 858 zł. Sprawa dotyczyła obsługi grafików pracy. Dane pracowników i franczyzobiorców znalazły się w publicznie dostępnym katalogu, co umożliwiało nieuprawnionym osobom pobranie plików i uzyskanie dostępu do danych (m.in. imion i nazwisk, numerów PESEL, numerów paszportów). Przyczyną była błędna konfiguracja serwera, za którą odpowiadał procesor.

URZĄD OCHRONY DANYCH OSOBOWYCH

Prezes UODO wskazał na braki po obu stronach: niewdrożenie adekwatnych środków bezpieczeństwa, brak analizy ryzyka oraz brak regularnego testowania i oceny skuteczności zabezpieczeń. Administrator dodatkowo nie zweryfikował należycie procesora przed powierzeniem danych i w trakcie współpracy. Nie sprawował też realnego nadzoru ani nie ocenił minimalizacji – zakres powierzanych danych był nadmiarowy (w szczególności w zakresie identyfikacji pracowników przez PESEL lub paszport). Procesor korzystał z podwykonawcy bez umowy dalszego powierzenia. W procesie nie zapewniono udziału IOD.

Wnioski praktyczne

- Odpowiedzialność jest po obu stronach – administrator i procesor odpowiadają za bezpieczeństwo, a outsourcing nie zwalnia z obowiązków.
- Analiza ryzyka oraz testowanie zabezpieczeń to podstawa – zarówno po stronie administratora, jak i po stronie procesora.
- Weryfikacja procesora musi być realna i udokumentowana – same „oświadczenia o bezpieczeństwie” nie wystarczą.
- Nadzór nad procesorem musi być ciągły.
- Zasada minimalizacji danych oznacza, że powierzane mogą być wyłącznie dane niezbędne do realizacji celu (wykorzystywanie numeru PESEL lub paszportu do identyfikacji pracownika zwykle będzie ryzykowne).
- Dalsze powierzenie wymaga umowy – jej brak stanowi odrębne naruszenie.
- IOD musi być włączany także w procesy w pełni outsourcowane.

Centrum Medyczne Ujastek

Prezes UODO nałożył na Centrum Medyczne Ujastek karę w wysokości 1 145 891,25 zł za bezprawne stosowanie monitoringu wizyjnego oraz za rażące braki w zabezpieczeniu danych. Placówka prowadziła ukryty monitoring w salach szpitalnych oddziału neonatologii, rejestrujący matki i noworodki – także w sytuacjach intymnych. Kamery były zamaskowane w zegarach i rejestrowały obraz bez wiedzy pacjentów, bez podstawy prawnej i bez spełnienia obowiązku informacyjnego.

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowo doszło do **zagubienia lub kradzieży kart pamięci** z nagraniami z tych kamer. Dane nie były szyfrowane ani właściwie zabezpieczone, co Prezes UODO uznał za dowód poważnych uchybień w zarządzaniu ryzykiem i ochronie danych. Uchybienia te były szczególnie dotkliwe ze względu na charakter danych oraz sytuację osób, których dotyczyły (dane wrażliwe, pacjenci w szczególnie chronionej sytuacji).

Wnioski praktyczne

- Monitoring wizyjny wymaga uprzedniej, udokumentowanej analizy niezbędności i proporcjonalności – należy wykazać, że nie istnieją mniej inwazyjne środki.
- Podstawa prawna przetwarzania musi być jasno określona przed uruchomieniem monitoringu i zgodna z RODO.
- Obowiązek informacyjny musi być realizowany w sposób konkretny i zrozumiały – ogólne sformułowania typu „kluczowe pomieszczenia” są niewystarczające.
- Ukryty monitoring jest co do zasady niedopuszczalny i zastrzeżony wyłącznie dla uprawnionych służb na podstawie przepisów szczególnych.
- Nagrania muszą być odpowiednio zabezpieczone (m.in. przez szyfrowanie i kontrolę nośników) – ich utrata znacząco zwiększa odpowiedzialność administratora.
- W sektorze ochrony zdrowia standard należytej staranności powinien być szczególnie wysoki ze względu na godność, intymność i wrażliwość danych pacjentów.

Jak organ ustala wysokość kary

Przy wymierzaniu administracyjnej kary pieniężnej organ zawsze analizuje okoliczności konkretnej sprawy. W szczególności bierze pod uwagę:

- charakter naruszenia (jego wagę, czas trwania, zakres i cel przetwarzania, liczbę osób dotkniętych naruszeniem oraz rozmiar szkody),
- umyślność lub nieumyślność działania,
- działania naprawcze i próby ograniczenia skutków naruszenia,
- poziom odpowiedzialności administratora lub procesora, w tym wdrożone środki techniczne i organizacyjne,
- wcześniejsze naruszenia i historię zgodności,
- stopień współpracy z organem,
- kategorię naruszonych danych (np. dane szczególnych kategorii),
- sposób ujawnienia naruszenia (samodzielne zgłoszenie czy ujawnienie przez osoby trzecie),
- przestrzeganie wcześniejszych środków naprawczych (jeżeli były stosowane),
- stosowanie kodeksów postępowania lub mechanizmów certyfikacji,
- inne czynniki łagodzące lub obciążające, w tym ewentualne korzyści osiągnięte w związku z naruszeniem.

Organ może:

- nałożyć jedną łączną karę za kilka naruszeń albo
- wymierzyć odrębne kary za każde naruszenie, jeżeli dotyczą one niezależnych operacji przetwarzania.

Ostatecznym celem jest kara skuteczna, proporcjonalna i odstraszająca, a nie automatyczna lub wyłącznie represyjna.

Przykłady czynników mogących wpłynąć łagodząco na wymiar kary

1. Aktywne działania podjęte po incydencie, ukierunkowane na podniesienie poziomu bezpieczeństwa.

2. Usunięcie stanu niezgodności z RODO.

3. Przyjęcie i stosowanie np. zatwierdzonego przez PUODO kodeksu postępowania jako środka gwarantującego wyższy niż standardowy poziom ochrony przetwarzania danych osobowych.

4. Działania zmierzające do zminimalizowania szkody poniesionej przez osoby, których dane dotyczą.

Uwaga: Samo przekazanie informacji o zaistniałym zdarzeniu nie może być uznane za takie działanie (stanowi wykonanie obowiązku RODO) i nie będzie interpretowane jako czynnik łagodzący wysokość kary.

Przykłady czynników wpływających obciążająco na wymiar kary

1. Znaczna waga i poważny charakter naruszenia, które stwarzają wysokie ryzyko negatywnych skutków dla osób, których dane dotyczą, w tym ryzyko braku możliwości realizacji ich praw.

2. Dalsze utrzymywanie stanu niezgodności z RODO po zgłoszonym incydencie, co niesie poważne ryzyko naruszenia praw lub wolności wszystkich osób, których dane osobowe są przetwarzane przez administratora.

3. Profil działalności administratora (np. szpital przetwarzający dane osobowe dotyczące dzieci, w tym dane objęte tajemnicą lekarską – od takich podmiotów szczególnie oczekuje się wysokich standardów bezpieczeństwa).

4. Kategorie ujawnionych danych i wynikające z tego ryzyko – UODO (za EROD) przyjmuje, że „im większej liczby takich kategorii danych dotyczy naruszenie lub im bardziej wrażliwe są dane, tym większą wagę organ nadzorczy może przypisać temu czynnikowi”.

Prognoza na 2026 r.

W 2026 r. należy spodziewać się dalszego **wzrostu aktywności organów nadzorczych w obszarze nowych technologii**, w szczególności w zakresie cyberbezpieczeństwa oraz wykorzystywania systemów sztucznej inteligencji. Praktyka Prezesa UODO oraz projektowane i wchodzące w życie przepisy prawa potwierdzają, że zgodność z RODO pozostaje kluczowym elementem oceny legalności przetwarzania danych – również w kontekście AI. Coraz większe znaczenie będą miały także takie zagadnienia, jak privacy by design i by default, ocena skutków dla ochrony danych, właściwe określenie podstaw prawnychprzetwarzania oraz przejrzyste obowiązki informacyjne.

Równolegle obserwowany jest **wzrost wymagań w obszarze cyberbezpieczeństwa**, w szczególności na styku RODO i dyrektywy NIS 2. Znajduje to odzwierciedlenie zarówno w praktyce nadzorczej, jak i w projektowanych zmianach legislacyjnych. Zapewnienie adekwatnych zabezpieczeń technicznych i organizacyjnych, a także prawidłowe uregulowanie relacji z kontrahentami, w tym w zakresie powierzeń przetwarzania danych, będzie miało istotne znaczenie dla oceny zgodności regulacyjnej.

Wnioski płynące z projektowanych oraz wchodzących w życie aktów prawnych UE i prawa polskiego wskazują jednocześnie na **stopniowe rozszerzanie zakresu obowiązków nakładanych na podmioty wykorzystujące technologie cyfrowe**. Dotyczy to w szczególności regulacji związanych z dostępem do danych (Data Act), ze sztuczną inteligencją (AI Act), z cyberbezpieczeństwem (NIS 2, CRA), z rynkiem kryptoaktywów (MiCA) oraz z funkcjonowaniem usług cyfrowych i handlu elektronicznego. Część z tych regulacji zacznie być stosowana bezpośrednio w 2026 r., natomiast pozostałe będą wymagały przygotowań organizacyjnych i technicznych już na etapie projektowania nowych produktów i usług.

Trzymaj rękę na pulsie

Zapisz się na bezpłatny biuletyn informacyjny

Raz w miesiącu możesz otrzymywać merytoryczną esencję
z obszaru ochrony danych osobowych i cyberbezpieczeństwa.
Bez spamowania. Sprawdź, zanim się zapiszesz.

ODO24.pl/biuletyn

Zapytania ofertowe

Cezary Lutyński
Doradca ds. ochrony danych
tel. 22 740 99 96, +48 690 957 609
oferty@odo24.pl

Marcin Kuźniak
Doradca ds. ochrony danych
tel. 22 740 99 96, +48 690 957 665
oferty@odo24.pl