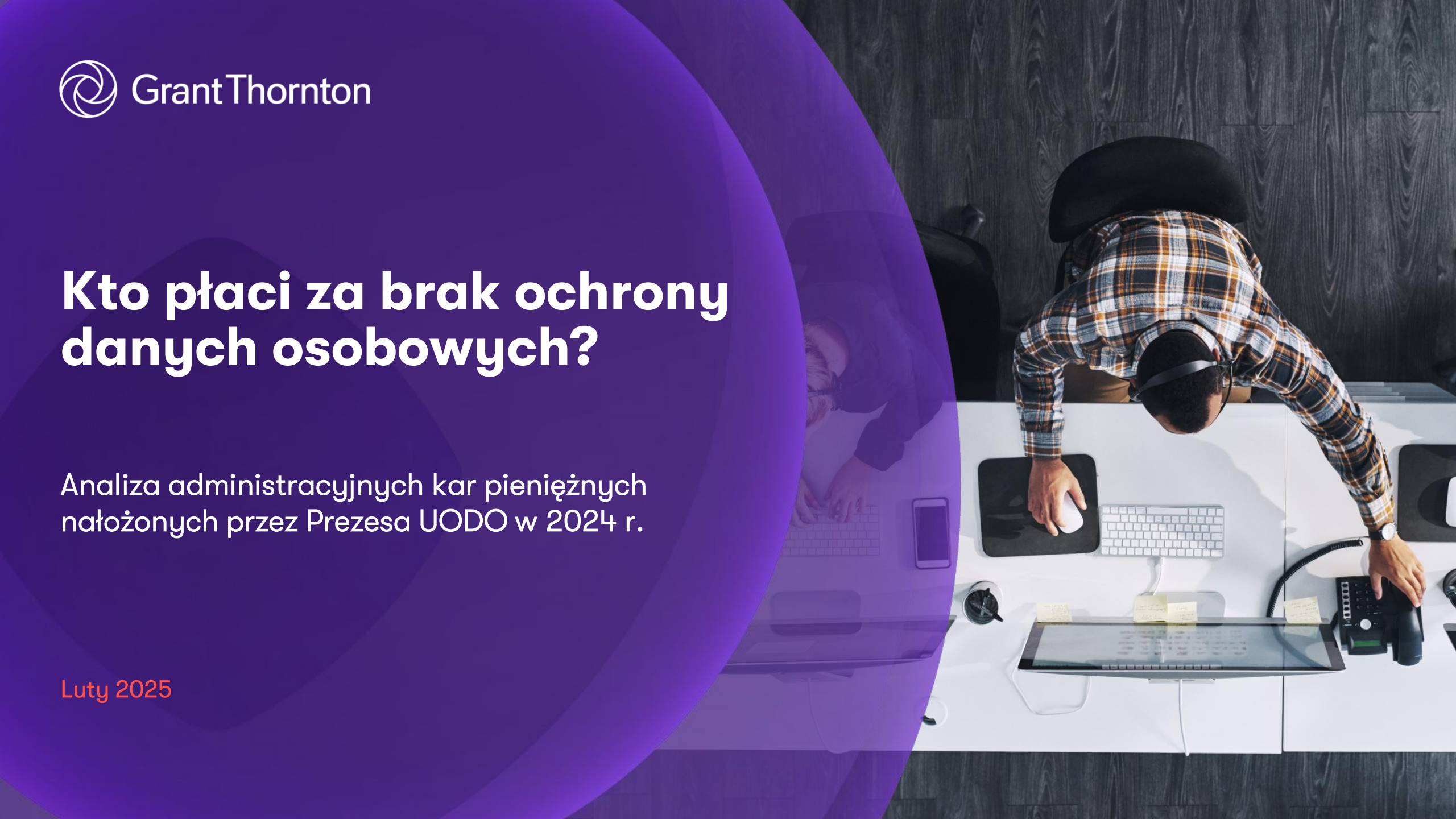
Grant Thornton

Kto płaci za brak ochrony danych osobowych?

Analiza administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2024 r.

Luty 2025



~14 mln zł

Wyniosły łącznie administracyjne kary pieniężne nałożone w opublikowanych decyzjach Prezesa UODO w 2024 r.

Wprowadzenie

Kary za RODO w teorii i w praktyce

Rozporządzenie o ochronie danych osobowych (czyli RODO) stanowi fundamentalny element współczesnego systemu ochrony tych danych w Unii Europejskiej, wprowadzając szereg praw i obowiązków na podmioty, które biorą udział w operacjach przetwarzania danych. W obliczu dynamicznego rozwoju technologii i globalizacji, w której dane osobowe stały się cennym zasobem, konieczność ich odpowiedniej ochrony jest kwestią kluczową.

Bardzo ważną rolę w zapewnianiu przestrzegania przepisów dotyczących ochrony danych osobowych odgrywa organ nadzorczy, którym w przypadku Polski jest Prezes Urzędu Ochrony Danych Osobowych. Oprócz monitorowania stosowania RODO, Prezes UODO ma również możliwość nakładania administracyjnych kar pieniężnych na podmioty, które dopuściły się naruszeń przepisów. Warto przy tym wspomnieć, że kara za naruszenia może wynieść nawet do 20 mln 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 ramach niniejszego Raportu postanowiliśmy przeanalizować najważniejsze wnioski, jakie płyną z analizy decyzji wydanych i opublikowanych przez Prezesa UODO w 2024 r., w ramach których zostały nałożone administracyjne kary pieniężne. Jaki jest stan przestrzegania przepisów ochrony danych osobowych w ubiegłym roku? Na kogo zostały nałożone kary pieniężne? Czego dotyczyły naruszenia przepisów? O czym powinni pamiętać administratorzy oraz podmioty przetwarzające, przeprowadzając operacje na danych osobowych?

Zapraszamy do lektury!

Część 1.

Kto zapłacił najwięcej?

Analiza administracyjnych kar pieniężnych nałożonych przez Prezesa UODO w 2024 r.

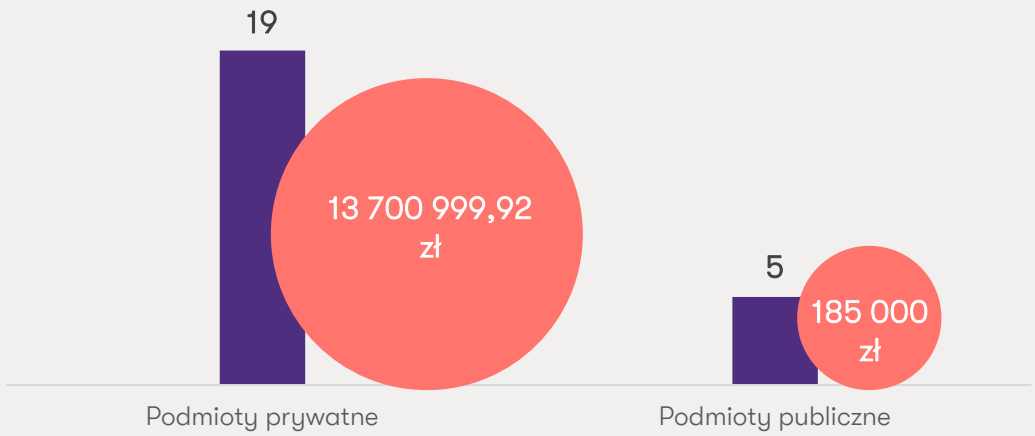
Grant Thornton

Podmioty prywatne płacą częściej za błędy w RODO

W 2024 r. Prezes UODO wydał 20 opublikowanych decyzji nakładających administracyjne kary pieniężne na 24 podmioty. Łączna wartość nałożonych kar wyniosła 13 885 999,92 zł.

W analizowanym okresie kary nałożone na podmioty prywatne stanowiły zdecydowaną większość - nałożono na nie łącznie 19 administracyjnych kar pieniężnych, czyli blisko 80 % wszystkich kar. Ich całkowita wartość wyniosła 13 700 999,92 zł, co oznacza 98,7% wartości wszystkich kar. Z kolei na podmioty publiczne nałożono w tym okresie jedynie 5 administracyjnych kar pieniężnych, co stanowiło nieco ponad 20% wszystkich kar o łącznej wartości 185 000 zł, czyli 1,3 % wartości wszystkich kar.

Wykres 1. Rodzaje podmiotów, na które zostały nałożone administracyjne kary pieniężne w 2024 r. oraz wysokość nałożonych kar



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Najwyższa nałożona w 2024 r. przez Prezesa UODO administracyjna kara pieniężna wynosiła 4 053 173 zł (29,2% wartości wszystkich kar), najniższa natomiast 916,71 zł (co stanowi 0,007% wartości wszystkich kar). Obydwie kary zostały nałożone na podmioty prywatne.

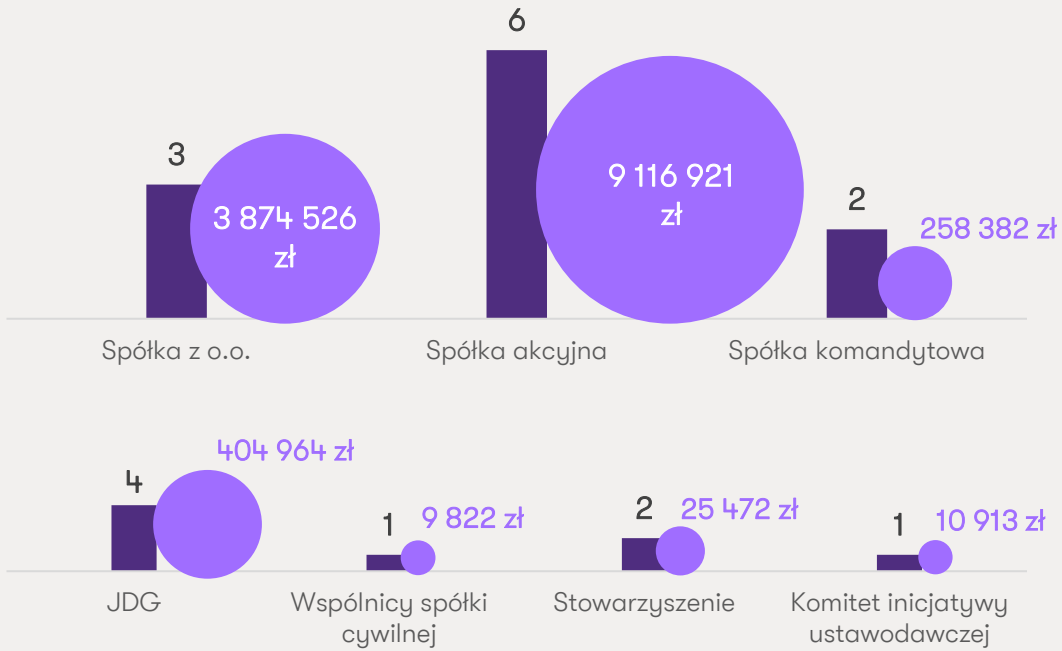
Spółki kapitałowe na celowniku

Administracyjne kary pieniężne nałożone na przedsiębiorstwa skupiały się przede wszystkim na spółkach kapitałowych, które odpowiadały za blisko 94% całkowitej wartości kar.

Za taki stan rzeczy może odpowiadać z jednej strony fakt, że wysokość administracyjnej kary pieniężnej nakładanej przez Prezesa UODO jest związana zarówno z obrotem, jak i specyfiką oraz skalą prowadzonej działalności. Ponadto, spółki kapitałowe cechują się bardziej złożonymi i rozbudowanymi procesami przetwarzania danych osobowych, co zwiększa ich podatność na potencjalne naruszenia.

Mimo mniejszej liczby przypadków naruszeń, inne formy działalności, takie jak spółki osobowe, jednoosobowe działalności gospodarcze czy wspólnicy spółki cywilnej, stowarzyszenia oraz komitet inicjatywy ustawodawczej, również zostały w minionym roku ukarane, choć wysokość tych kar była znacząco niższa i odpowiadała za ok. 6% wartości wszystkich kar.

Wykres 2. Rodzaje podmiotów w ramach sektora prywatnego, na które zostały nałożone administracyjne kary pieniężne w 2024 r. oraz wysokość nałożonych kar



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Administrator sam bije się w piersi

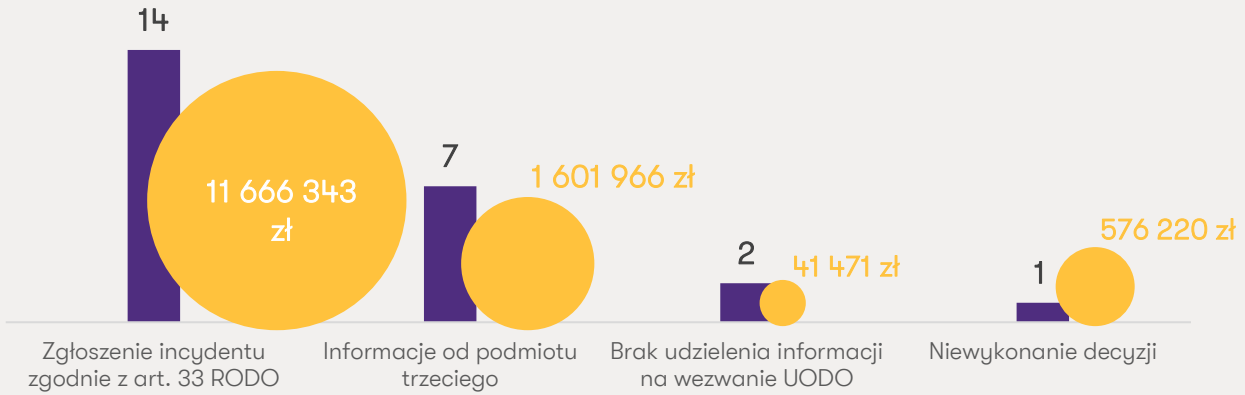
W ponad połowie przypadków to administrator danych osobowych informuje o naruszeniu przepisów dotyczących ich ochrony.

Prezes UODO wszczął postępowanie w związku ze zgłoszeniem naruszenia ochrony danych osobowych (dalej incydent) przez administratora w ok. 55% przypadków , co skutkowała nałożeniem łącznie ponad 11,5 mln zł kar pieniężnych. Oznacza to, że Prezes UODO zwraca szczególną uwagę na zgłoszenie organowi nadzorczemu incydentu bez zbędnej zwłoki. Pojawiły się również przypadki, gdy postępowanie zostało wszczęte z uwagi na informację od podmiotu trzeciego (bez stosowanego zgłoszenia incydentu ze strony administratora).

Stanowi to ważną wskazówkę dla administratorów, żeby nie ukrywali ewentualnych incydentów w obszarze ochrony danych osobowych. Administratorzy powinni także natychmiast podjąć niezbędne działania mające na celu ocenę powstałego zdarzenia oraz dokonać zgłoszenia do organu nadzorczego zgodnie z przepisami RODO.

Wśród administracyjnych kar pieniężnych są również przypadki kar nałożonych w związku z brakiem udzielania informacji przez administratora na wezwanie Prezesa UODO, a także w związku z czynnościami kontrolnymi. Administratorzy powinni mieć zatem na względzie, że zaniechania w zakresie współpracy z organem nadzorczym (np. w przypadku braku odbioru korespondencji) również mogą wiązać się z konsekwencjami finansowymi. Powinni mieć także świadomość, że zapewnienie zgodności procesów przetwarzania z RODO ma charakter ciągły – dzięki cyklicznym audytom podmioty będą lepiej przygotowane na ewentualne kontrole ze strony pracowników UODO.

Wykres 3. Przyczyna wszczęcia postępowania administracyjnego przez Prezesa UODO w 2024 r. oraz wysokość nałożonych kar



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Wysokość kar rośnie wraz ze skalą incydentu

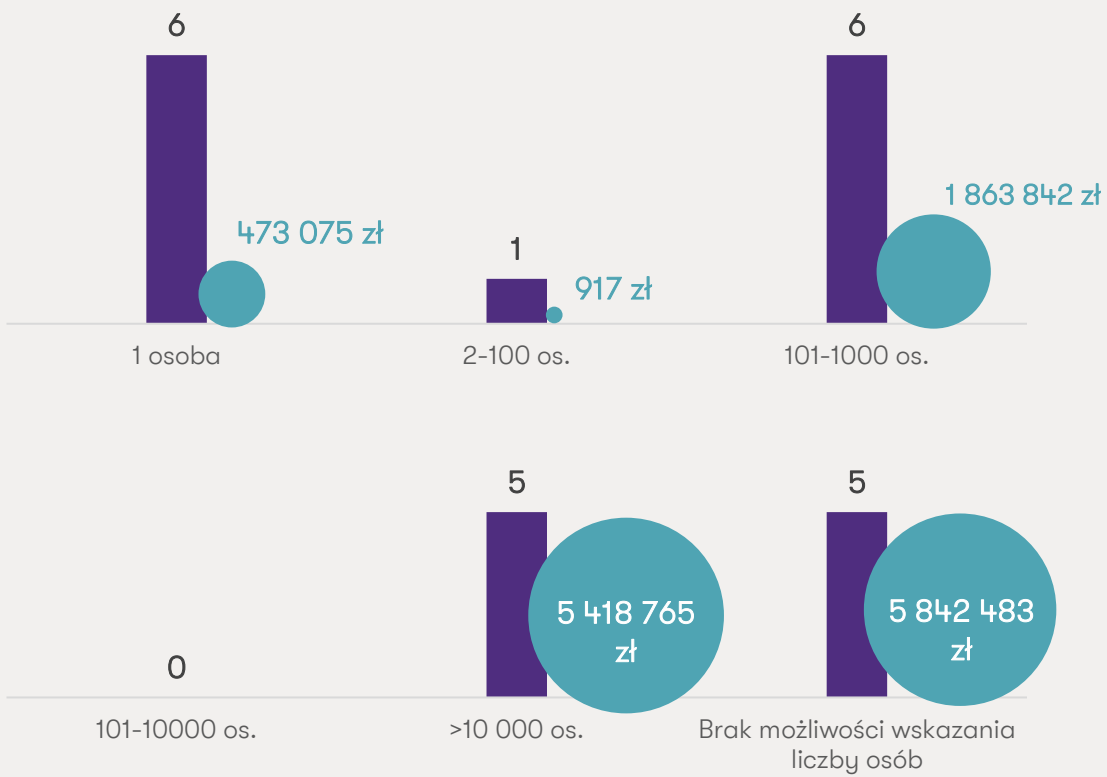
Łączna liczba osób, których dotyczą naruszenia powstałe w wyniku działań lub zaniechań ukaranych podmiotów, wynosi ponad 2,4 mln!

W rzeczywistości liczba ta może być jednak znacznie wyższa, ponieważ część administratorów nie była w stanie dokładnie określić liczby osób dotkniętych incydentami lub informacja ta nie była wskazana w uzasadnieniu decyzji Prezesa UODO.

W jednym przypadku doszło do naruszenia danych osobowych ok. 2,2 mln osób, co w znaczący sposób wpłynęło na wysokość nałożonej administracyjnej kary pieniężnej (3 819 960 zł). Wśród decyzji nakładających kary pojawiły się zarówno przypadki naruszenia danych osobowych jednej osoby, jak i sytuacje, gdy doszło do naruszenia danych osobowych ponad 10 000 osób. Pokazuje to, że administratorzy powinny dbać o odpowiednie bezpieczeństwo danych osobowych przetwarzanych w ramach baz danych, ale również danych osobowych pojedynczych osób.

Warto zwrócić uwagę, iż w 18 przypadkach nałożone kary obejmowały dane osobowe zwykłe, które mają szczególny wpływ na osobę (numer PESEL czy też seria i numer dokumentu tożsamości), co skutkuje surowszymi konsekwencjami finansowymi dla administratora. Co więcej, 9 nałożonych administracyjnych kar pieniężnych dotyczyło sytuacji związanych z danymi osobowymi szczególnej kategorii, związanych głównie ze stanem zdrowia, ale także światopoglądem.

Wykres 4. Liczba osób, których dotyczyło naruszenie w 2024 r. oraz nałożone w wyniku wykrycia naruszenia kary pieniężne



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Administratorzy sami sobie winni?

W analizowanym okresie większość naruszeń stanowiły przypadki spowodowane umyślnym działaniem bądź zaniechaniem ze strony administratora – było ich 14.

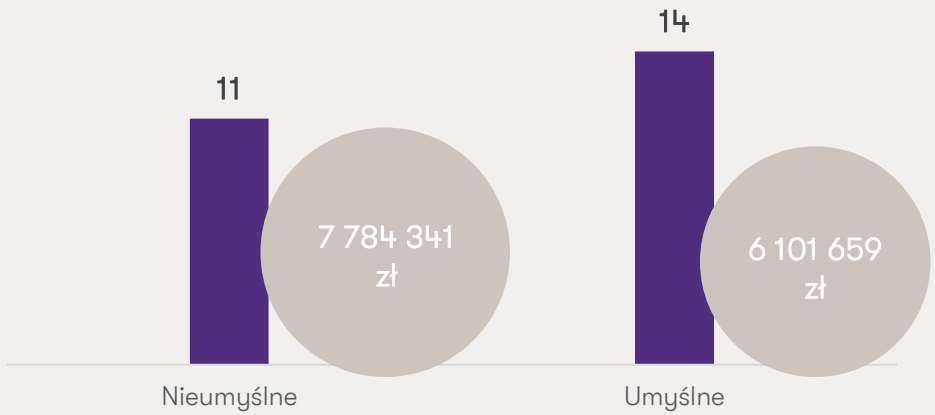
Wśród przypadków naruszenia umyślnego dominowały incydenty związane z brakiem zawiadomienia organu nadzorczego o naruszeniu ochrony danych osobowych oraz z brakiem udzielania odpowiedzi na wezwania Prezesa UODO, ale także świadome wyznaczanie IOD w sposób niezapewniający jego podległości bezpośrednio najwyższemu kierownictwu.

Warto zwrócić uwagę, że większy udział w łącznej wartości wszystkich kar mają administracyjne kary pieniężne nałożone w związku z naruszeniem nieumyślnym. Zatem nawet nieumyślne/nieświadome działanie administratora może skutkować surowymi konsekwencjami finansowymi.

Do nieumyślnych naruszeń Prezes UODO zaliczył niekorzystanie w sposób świadomy z zasobów informatycznych pozbawionych bieżącego wsparcia ich producentów, wynikające z niedbalstwa niedopełnienie obowiązku zastosowania odpowiednich środków bezpieczeństwa skutkujące utartą pendrive'a czy niepodjęcie na skutek niedochowania należytej staranności działań zmierzających do prawidłowego wdrożenia środków bezpieczeństwa, pomimo posiadanej analizy ryzyka.

Warto pamiętać, że brak wdrożenia odpowiednich środków zabezpieczających dane osobowe, w sytuacji w której administrator był świadomy niedostateczności tych środków, jest przyczyną umyślnego naruszenia przepisów RODO.

Wykres 5. Liczba i łączna wartość kar w 2024 r. w podziale na umyśle i nieumyślne naruszenia przepisów



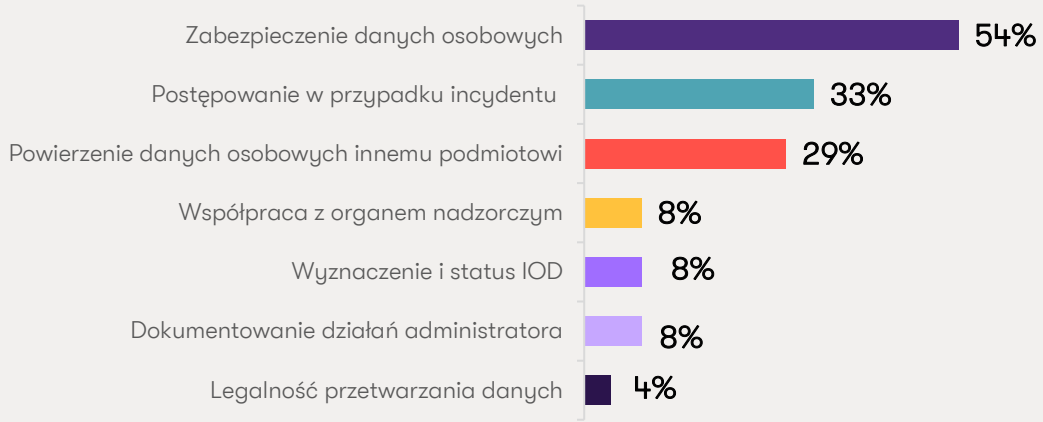
Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Jakie incydenty zdarzają się najczęściej?

Obszary naruszeń przepisów RODO pokazują różnorodność nośników danych i obszarów przetwarzania danych osobowych, które administrator musi brać pod uwagę przy zabezpieczaniu organizacji.

Wśród zdarzeń, które prowadzą do incydentów, występują bowiem: wysłanie do nieuprawnionego adresata wiadomości e-mail zawierającej niezabezpieczoną hasłem bazę danych, upublicznienie dokumentów znajdujących się w porzuconej przesyłce, zgubienie zewnętrznego nośnika danych (pendrive), udostępnienie na profilu listy uczestników, czy ataki złośliwego oprogramowania (w tym ransomware).

Wykres 6. Nakładane przez Prezesa UODO administracyjne kary pieniężne w 2024 r. w podziale na obszary, których dotyczyło naruszenie



Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Ważnym wnioskiem płynącym z naszego badania jest konieczność przeprowadzenia analizy ryzyka oraz wdrożenia odpowiednich środków technicznych i organizacyjnych, które skutecznie zabezpieczą przetwarzane dane osobowe. Istotne jest również przestrzeganie zasady rozliczalności, która wymaga od administratora wykazania zgodności z przepisami RODO oraz wewnętrznego dokumentowania działań związanych z ochroną danych osobowych.

W przypadku powierzenia przetwarzania danych osobowych należy pamiętać nie tylko o zawarciu umowy powierzenia (z wszystkimi wymaganymi elementami), ale również o tym, by podmiot przetwarzający zapewniał wdrożenie odpowiednich środków technicznych i organizacyjnych.

Administratorzy powinni również współpracować z organem nadzorczym – w tym odbierać i terminowo odpowiadać na korespondencję. Co równie ważne administratorzy muszą dbać o prawidłowe wyznaczenie, jak i status inspektora ochrony danych.

Jakie błędy popełnia administrator?

Administratorzy w głównej mierze zaniedbują kwestie wdrożenia odpowiednich środków zabezpieczających dane osobowe.

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

Przepis RODO	Obowiązek administratora	Liczba naruszeń
Art. 32 ust. 1 i 2	Wdrożenie odpowiednich środków zabezpieczających dane osobowe	13
Art. 5 ust. 1 lit. f	Zapewnienie odpowiedniego bezpieczeństwa danych osobowych	10
Art. 5 ust. 2	Zapewnienie zdolności do wykazania przestrzegania zasad RODO	10
Art. 25 ust. 1	Uwzględnienie ochrony danych w fazie projektowania procesu przetwarzania danych	9
Art. 33 ust. 1 i 3	Zgłoszenie naruszenia ochrony danych do organu nadzorczego	8
Art. 34 ust. 1 i 2	Zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych	8
Art. 28 ust. 1 i 3	Powierzanie danych osobowych podmiotom zapewniającym wystarczające gwarancje dla bezpieczeństwa danych osobowych oraz zawarcie umowy powierzenia	7
Art. 24 ust. 1	Wdrożenie środków mających na celu przetwarzanie danych osobowych zgodnie z prawem	5
Art. 58 ust. 1 lit. a) i e) w zw. z art. 31	Współpraca z organem nadzorczym	2
Art. 6 ust. 1	Posiadanie podstawy do przetwarzania danych osobowych	1
Art. 9 ust. 1	Posiadanie podstawy do przetwarzania danych osobowych szczególnej kategorii	1
art. 30 ust. 1	Rejestrowanie czynności przetwarzania	1
Art. 35 ust. 1 I 7	Przeprowadzenie oceny skutków dla ochrony danych	1
Art. 37 ust. 1 i 7	Wyznaczenie i status inspektora ochrony danych	1
Art. 38 ust. 3	Status inspektora ochrony danych	1

Źródło: Opracowanie własne na podstawie decyzji opublikowanych przez UODO

Kary nałożone przez UODO mogą dotknąć każdy podmiot

Obowiązki związane z ochroną danych dotyczą wszystkich przedsiębiorców – niezależnie od wielkości, branży czy sektora działalności. Jednocześnie skala działalności nie zwalnia z odpowiedzialności za zapewnienie zgodności z przepisami. Organizacje powinny zatem dokładnie ocenić, czy ich obecny poziom wdrożenia RODO rzeczywiście chroni je przed najczęściej występującymi problemami, które pojawiają się w decyzjach wydanych przez Prezesa UODO, a więc:

- czy przeprowadzono adekwatną analizę uwzględniającą wszelkie potencjalne ryzyka związane z przetwarzaniem danych osobowych?
- czy wdrożono odpowiednie zabezpieczenia przy przetwarzaniu danych osobowych?
- czy wdrożono odpowiednią ścieżkę postępowania w przypadku incydentów i przeszkolono pracowników w tym zakresie?
- czy w organizacji funkcjonuje dokumentacja potwierdzająca przestrzeganie RODO?
- czy powołano odpowiednie struktury, które odpowiadają za ochronę danych osobowych, w tym również za potencjalną współpracę z UODO?

Różnorodność zagrożeń, z którymi muszą zmagać się organizacje, dodatkowo podkreśla, jak złożone i wieloaspektowe musi być podejście do ochrony danych osobowych. Ataki złośliwego oprogramowania, w tym ransomware, błędy ludzkie, jak omyłkowe wysłanie danych, fizyczne uszkodzenie nośników danych, czy kradzież sprzętu to tylko niektóre z ryzyk, które mogą prowadzić do poważnych incydentów.

W obliczu tych zagrożeń, administratorzy nie mogą ograniczać się tylko do wdrożenia odpowiednich technicznych zabezpieczeń. Niezwykle istotne jest również stworzenie skutecznych procedur operacyjnych, które nie tylko zminimalizują ryzyko wystąpienia incydentów, ale również umożliwią ich szybką identyfikację i reakcję, co ostatecznie może ochronić organizację przed wysoką karą pieniężną.

Emilia Martynowicz-Mamajek
Junior Associate
Kancelaria Prawna
Grant Thornton

Część 2.

Decyzje Prezesa UODO pod lupą!

Na jakie zagadnienia należy zwrócić uwagę?

Grant Thornton

Analiza ryzyka

Nieprawidłowo przeprowadzona analiza ryzyka stanowiła główną przyczynę administracyjnych kar pieniężnych dotyczących braku zapewnienia odpowiedniego poziomu bezpieczeństwa danych.

1. **Przeprowadzenie analizy ryzyka uwzględniającej specyfikę wszystkich procesów przetwarzania danych** – w analizowanych decyzjach organ podkreślał, że wymaga przeprowadzenia analizy m.in. zezwolenia pracownikom na korzystanie z przenośnych komputerów podczas delegacji czy dopuszczenie przetwarzania danych osobowych z wykorzystaniem sprzętu komputerowego umożliwiającego podłączenie przenośnych nośników danych (w szczególności pamięci USB),
2. **Udokumentowanie analizy ryzyka** – organ podkreślał, że analiza musi być udokumentowana lub w inny sposób utrwalona oraz ujęta w postaci ściśle określonych, precyzyjnych formuł wyjaśniających i porządkujących przebieg tego procesu. W ocenie organu taki sposób działania zapewnia należytą kontrolę nad procesem w kontekście zagwarantowania bezpieczeństwa uczestniczących w nim danych osobowych, jak również możliwości wykazania zgodności działań administratora z przepisami RODO,
3. **Metodologia analizy ryzyka** – organ miał zastrzeżenia co do analiz ryzyka, które były przedstawiane bez kompletnej metodyki ich sporządzenia. Zdaniem organu prawidłowa analiza powinna zawierać macierz ryzyka oraz wartości przyjęte do wzoru dla obliczenia ryzyka akceptowalnego. Bez przedstawionej metodologii organ nie może ponownie odtworzyć analizy i ocenić, czy została ona przeprowadzona prawidłowo.
4. **Subiektywna analiza ryzyka** – analiza ryzyka powinna zostać przeprowadzona w oparciu o wewnętrzne i zewnętrzne okoliczności dotyczące w szczególności kontekstu przetwarzania danych w organizacji. Dlatego prawdopodobieństwo wystąpienia naruszenia administrator powinien oceniać nie tylko w kontekście doświadczenia (występowania bądź nie określonych zdarzeń w przeszłości), ale również istniejących zabezpieczeń, ich skuteczności oraz podatności wystąpienia. Ocena dokonana przez administratora wyłącznie na podstawie występowania naruszeń w okresie ostatnich trzech lat została uznana przez organ za dowolną i nieuzasadnioną.
5. **Zastosowanie adekwatnych do zagrożeń środków bezpieczeństwa** – w sytuacji, gdy analiza ryzyka nie została przeprowadzona w sposób prawidłowy (np. nie uwzględnia możliwych zagrożeń związanych z nieuprawnionym dostępem lub odbywa się bez pełnej znajomości struktury wszystkich elementów systemu przetwarzania danych), administrator nie może poprawnie określić oraz zastosować środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa danych osobowych. Poza tym administrator jest zobligowany nie tylko do zapewniania zgodności poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale również do zapewniania ciągłości monitorowania poziomu zagrożeń.

Środki techniczne i organizacyjne

Zagadnienia związane z wdrożeniem odpowiednich środków technicznych i organizacyjnych pojawiały się najczęściej w odniesieniu do nieprawidłowo przeprowadzonej analizy ryzyka, jak i w związku z incydentami.

1. **Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych** – wdrożenie takich środków nie jest działaniem jednorazowym. Powinno ono przybrać postać procesu, w ramach którego administrator dokonuje przeglądu i w razie potrzeby uaktualnia przyjęte wcześniej zabezpieczenia. Regularna ocena zastosowanych środków bezpieczeństwa pozwala, m.in. na weryfikację, czy wprowadzona procedura określająca zakaz użytkowania prywatnych nośników danych lub zasady pracy zdalnej jest skuteczna oraz ewentualne wdrożenie dodatkowych środków.
2. **Zapewnienie aktualnego oprogramowania** – oprogramowanie wykorzystywane do przetwarzania danych osobowych powinno posiadać najnowszą wersję, a same aktualizacje powinny odbywać się na bieżąco. Ponadto, oprogramowanie powinno mieć wsparcie producenta. Ataki złośliwego oprogramowania często polegają na wykorzystaniu podatności w systemie teleinformatycznym. Jeśli administrator regularnie dokonuje aktualizacji oprogramowania, które eliminują takie podatności, to jednocześnie ogranicza ryzyko wystąpienia ataków. Natomiast dalsze wykorzystywanie nieaktualnego oprogramowania, lub takiego, które utraciło wsparcie może zostać uznane za niewywiązanie się przez administratora z obowiązku zapewnienia bezpieczeństwa danych osobowych.
3. **Zabezpieczenie przenośnych nośników** – organ nadzorczy zwraca uwagę, że w przypadku korzystania w organizacji z zewnętrznych nośników danych, administrator w celu skutecznego zabezpieczenia danych na nośniku, powinien nie tylko wprowadzić zabezpieczenia mające na celu ochronę danych na wypadek awarii nośnika, ale także na wypadek ich kradzieży lub zagubienia, tak aby osoba nieuprawniona nie mogła ich odczytać. Organ nadzorczy podkreśla także, że sam fakt wprowadzenia zabezpieczeń będzie niewystarczający jeśli administrator nie będzie regularnie weryfikował czy są one stosowane.
4. **Szkolenia z zakresu ochrony danych osobowych** – przeprowadzanie szkoleń, aby mogło być uznane za adekwatny środek bezpieczeństwa, musi być realizowane w sposób cykliczny, co zapewni stałe przypominanie, a w konsekwencji utrwalanie zasad przetwarzania danych osobowych objętych szkoleniem. Brak przeprowadzania szkoleń we wskazany sposób oznacza, że ten środek w praktyce nie obniża wystąpienia incydentów.
5. **Zasady dotyczące przetwarzania danych osobowych** – bardzo często konsekwencją naruszenia obowiązków przez administratora w zakresie bezpieczeństwa przetwarzania jest naruszenie zasady integralności i poufności poprzez niezastosowanie skutecznych środków technicznych i organizacyjnych, a także zasady rozliczalności. Jak podkreślana Prezes UODO, kwestia zapewnienia poufności danych powinna być traktowana w sposób szczególny i priorytetowy przez administratora. Naruszając zasady przewarzania danych administrator naraża się na najwyższy z możliwych wymiarów administracyjnej kary pieniężnej.

Powierzenie przetwarzania danych osobowych

Administratorzy często współpracują z różnymi podmiotami przetwarzającymi dane, w ramach np. outsourcingu kadrowo-płacowego, księgowego, informatycznego czy w zakresie zarządzania i administracji.

1. **Zawarcie pisemnej umowy powierzenia przetwarzania danych osobowych** – konsekwencją braku zachowania formy pisemnej, w przypadku gdy nie obowiązuje żaden inny odpowiedni instrument prawny, jest naruszenie RODO. Relacja administrator-podmiot przetwarzający nadal istnieje w przypadku braku pisemnej umowy związanej z przetwarzaniem danych. Warto przy tym wspomnieć, że administrator, nie dbając o pisemną formę umowy, pozbawia się de facto możliwości kształtowania działań podmiotu przetwarzającego.
2. **Wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych przez podmiot przetwarzający** –to administrator dokonuje oceny, czy podmiot przetwarzający gwarantuje wdrożenie adekwatnych środków technicznych i organizacyjnych. Często będzie to wymagało wymiany odpowiedniej dokumentacji (np. polityki prywatności, warunków świadczenia usług, polityki bezpieczeństwa informacji, sprawozdań z zewnętrznych audytów ochrony danych, uznanych międzynarodowych certyfikatów, jak np. normy ISO 27001). Poza tym administrator powinien wziąć pod uwagę takie elementy jak, np.: wiedza fachowa (np. wiedza techniczna w zakresie środków bezpieczeństwa), wiarygodność, czy reputacja.
3. **Przeprowadzanie regularnych audytów/inspekcji w organizacji podmiotu przetwarzającego** – weryfikacja, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych jest obowiązkiem ciągłym i nie kończy się w momencie zawarcia umowy powierzenia. W praktyce jest to m.in. konieczności zapewnienia regularnego monitoringu zastosowanych zabezpieczeń oraz prowadzenia stałego nadzoru nad pomiotem przetwarzającym.
4. **Dowolność w działaniu podmiotu przetwarzającego** – brak ustanawiania odpowiednich ram działania dla podmiotu przetwarzającego może doprowadzić do powstania, a następnie długotrwałego kontynuowania stanu dowolności jego działania. Administrator wydając polecenia, powinien je przekazywać wraz z precyzyjną instrukcją co do metod zapewnienia bezpieczeństwa przetwarzania danych (np. w zakresie wprowadzania zmian w systemie informatycznym celem umożliwiania pracownikom realizowania pracy zdalnej). Dowolność wyboru stosowanych rozwiązań przez podmiot przetwarzający w połączeniu z brakiem wdrożonych procedur dotyczących kontroli prawidłowości podejmowanych w tym zakresie czynności, może doprowadzić do incydentu.
5. **Wieloletnia współpraca pomiędzy administratorem a podmiotem przetwarzającym** – dotychczasowa pozytywnie oceniana współpraca może stanowić jedynie punkt wyjścia przy dokonywaniu weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Co więcej, długotrwała współpraca stron, niepodparta okresowym, systematycznym przeprowadzaniem audytów nie gwarantuje, że podmiot przetwarzający zrealizuje prawidłowo zadania wymagane przez RODO.

Naruszenie ochrony danych osobowych (incydent)

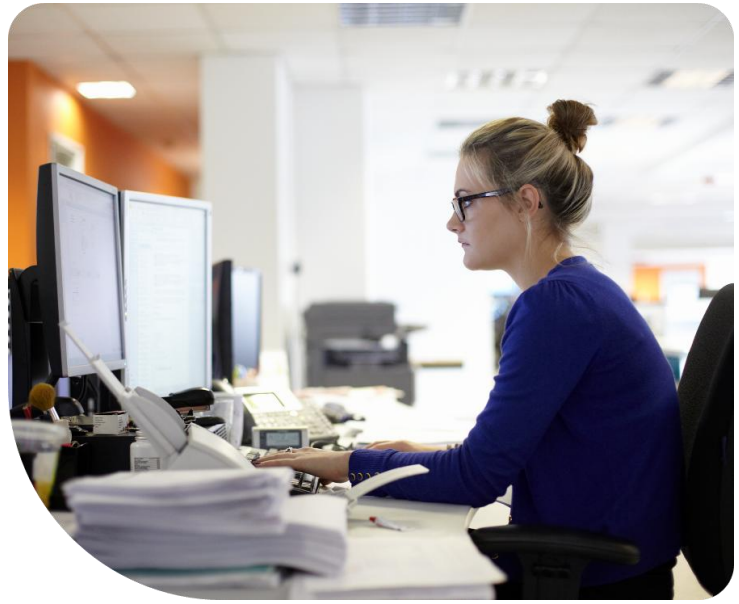
Najbardziej medialne z przyczyn nałożonych administracyjnych kar pieniężnych są przypadki incydentów, jak np. ataki złośliwego oprogramowania (w tym ransomware) czy kradzieże sprzętów lub dokumentów z danymi.

1. **Zgłoszenie naruszenia ochrony danych osobowych (incydentu)** – w przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby okazać się nadmierna. Aby mógł prawidłowo wywiązać się z nałożonych na niego obowiązków, powinien w pierwszej kolejności przeprowadzić stosowną analizę ryzyka w odniesieniu do powstałego incydentu (biorąc pod uwagę np. charakter, wrażliwość i ilość danych osobowych, czy łatwość identyfikacji). Poza tym nie może pominąć okoliczności, że zbiór różnych danych osobowych ma zazwyczaj bardziej wrażliwy charakter niż pojedyncze dane.
2. **Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (incydencie)** – administrator rezygnując z zawiadamiania osób, których dane osobowe podlegały incydentowi, pozbawia te osoby możliwości przeciwdziałania potencjalnym szkodom. Przy braku odpowiedniej i szybkiej reakcji naruszenie może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u podmiotów danych, takich jak utrata kontroli nad własnymi danymi osobowymi, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, naruszenie dobrego imienia. Informacja przekazywana do osób, objętych incydentem powinna być szybka, jasna i przejrzysta.
3. **Odpowiednie środki bezpieczeństwa** – jeśli na skutek incydentu mogą nastąpić szkody administrator jest zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne, by od razu stwierdzić incydent i szybko poinformować organ nadzorczy oraz osoby, których dane osobowe były objęte naruszeniem. Administrator nie może przy tym powoływać się na brak wyczulenia na RODO lub niedostatki w wiedzy z zakresu ochrony danych osobowych.
4. **Ocena ryzyka w przypadku błędnego wysłania korespondencji** – częstym błędem administratorów jest uznawanie osób, które otrzymały korespondencję przez pomyłkę, za zaufanych odbiorców, tj. za osoby, które nie wykorzystają danych w sposób nieuprawniony. Aby uznać taką osobę za zaufaną, administrator powinien utrzymywać z nią stałe relacje, znać jej procedury i mieć pewność, że nie odczyta ona omyłkowo przesłanych danych i zgodnie z poleceniem je odeśle. Błędem jest zatem założenie, że klient, który sam zgłosił incydent lub zwrócił dane, automatycznie staje się zaufanym odbiorcą. Może to prowadzić do błędnej oceny ryzyka i niewykonania obowiązków wynikających z RODO.
5. **Wysokie ryzyko naruszenia w przypadku numeru PESEL** – numer PESEL jest daną identyfikująca każdą osobę i jest powszechnie używany w kontaktach z różnymi instytucjami oraz w obiegu prawnym. Tym samym jego ujawnienie może wiązać się z negatywnymi skutkami takimi jak kradzież tożsamości czy wyłudzenie pożyczki. Dlatego incydent, który dotyczy ujawnienia numeru PESEL nieuprawnionym odbiorcom powinien być traktowany jako powodujący wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Współpraca z organem nadzorczym

Karą pieniężną ukarano przypadki braku współpracy z organem nadzorczym przy wykonywaniu przez niego swoich zadań, jak i niezapewnienia przez administratora dostępu do danych i informacji.

1. **Brak odpowiedzi na wezwania organu nadzorczego** – zdaniem organu nadzorczego obowiązkiem administratorów jest taka organizacja pracy, by doręczanie pism w godzinach pracy i w lokalu ich siedziby było zawsze możliwe. Długotrwałe nieodbieranie pism jest uznawane za rażące niedbalstwo, które utrudnia realizację uprawnień organu nadzorczego. W przypadku, gdy administrator odebrał jedno wezwanie, a później zaprzestał ich odbierania organ uznawał naruszenie za umyślne.
2. **Brak odpowiedzi na zapytanie o wysokość rocznego obrotu** – Prezes UODO często wzywał podmioty do udzielenia informacji o wysokości rocznego obrotu, co stanowi podstawę do ustalenia wysokości ewentualnej kary. W przypadkach, gdy przedsiębiorcy nie odpowiadali na takie wezwania, organ nadzorczy nie wstrzymywał się z nałożeniem kary. W takich sytuacjach organ pozyskiwał informację z innych źródeł (np. rocznych sprawozdań finansowych). Zatem celowe ignorowanie zapytania o dochód nie uchroniło przedsiębiorców przed karą, a także doprowadziło do nałożenia dodatkowej kary.
3. **Brak wystarczającego dowodu na wykonanie nakazu decyzji** – Prezes UODO zwraca uwagę, że zgodnie z zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie. Oznacza to, że w razie sporu z organem nadzorczym, to na administratorze spoczywa ciężar udowodnienia, że przestrzega on zasad RODO.
4. **Nieudostępnianie pełnomocnictwa** – organ nadzorczy podkreśla konieczność, aby odpowiedzi na wezwania były składane przez osoby uprawnione do reprezentacji podmiotu lub posiadające pełnomocnictwo. Dokumenty przedstawiane przez inspektora ochrony danych lub podmioty powiązane z przedsiębiorstwem, bez odpowiednich pełnomocnictw, były uznawane za złożone z brakiem formalnym.
5. **Brak podpisu lub daty na dokumentach** – organ nadzorczy szczególnie zwracał uwagę na formalne elementy dokumentów, takie jak podpis i data, które potwierdzają ich autentyczność i aktualność w kontekście obowiązków spółki.



Jakie wnioski płyną z decyzji Prezesa UODO?

Bez względu na rozmiar organizacji administratora czy podmiotu przetwarzającego, skalę prowadzonej działalności czy liczbę zatrudnianych pracowników każdy podmiot powinien pamiętać, że przetwarzanie danych osobowych musi odbywać się w sposób bezpieczny i zapewniający gwarancje dla osób, których dane dotyczą. Decyzje wydane przez Prezesa UODO nakładające administracyjne kary pieniężne pozwalają na wyciągnięcie ogólnych wniosków dla wszystkich podmiotów, które uczestniczą w operacjach przetwarzania danych osobowych:

1. Analiza ryzyka w kontekście przetwarzania danych osobowych musi być kompleksowa, udokumentowana i oparta na solidnej metodologii. Powinna uwzględniać specyfikę wszystkich procesów przetwarzania danych, być przeprowadzona w oparciu o wewnętrzne i zewnętrzne okoliczności oraz zapewniać zastosowanie adekwatnych środków bezpieczeństwa.
2. Zapewnienie bezpieczeństwa danych osobowych wymaga ciągłego i systematycznego podejścia. Administratorzy muszą regularnie testować, aktualizować i oceniać skuteczność środków technicznych i organizacyjnych, zapewniać aktualność oprogramowania, zabezpieczać przenośne nośniki danych, prowadzić cykliczne szkolenia oraz przestrzegać zasad przetwarzania danych osobowych.
3. Administrator musi zapewnić ścisłą kontrolę i nadzór nad podmiotem przetwarzającym dane. Obejmuje to zawarcie pisemnej umowy, regularne audyty, zapewnienie odpowiednich środków technicznych i organizacyjnych oraz precyzyjne instrukcje dotyczące przetwarzania danych. Długotrwała współpraca nie zwalnia z obowiązku ciągłej weryfikacji i monitorowania działań podmiotu przetwarzającego.
4. Administrator musi być bardzo ostrożny i proaktywny w przypadku naruszeń ochrony danych. Powinien zgłaszać incydenty nawet przy najmniejszych wątpliwościach, informować osoby, których dane dotyczą, wdrażać odpowiednie środki bezpieczeństwa, oraz szczególnie chronić dane takie jak numer PESEL.
5. Administratorzy muszą ściśle przestrzegać formalnych wymogów w komunikacji z organem nadzorczym. Obejmuje to odbieranie pism, udzielanie informacji o rocznym obrocie, dostarczanie dowodów na wykonanie decyzji, udostępnianie pełnomocnictw oraz dbanie o formalne elementy dokumentów, takie jak podpis i data. Zaniedbania w tych obszarach mogą prowadzić do poważnych konsekwencji, w tym nałożenia kar.

Łukasz Jarecki
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

Łukasz Jarecki
Associate
Kancelaria Prawna
Grant Thornton
M +48 885 661 839
E lukasz.jarecki@pl.gt.com

Emilia Martynowicz-Mamajek
Junior Associate
Kancelaria Prawna
Grant Thornton
M +48 667 778 891
E emilia.martynowicz-mamajek@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 147 krajach i zatrudniająca ponad 68 tys. pracowników. W Polsce działamy od 30 lat. Zespół 1000 pracowników wspiera naszych klientów w obszarach takich jak doradztwo podatkowe, prawne, transakcyjne i finansowe, audyt czy outsourcing płac i kadr oraz outsourcing księgowości.

Załącznik

Wykaz opublikowanych decyzji wydanych w 2024 r. przez Prezesa UODO nakładających administracyjne kary pieniężne

Opublikowane decyzje Prezesa UODO nakładające administracyjne kary pieniężne w 2024 r.

Lp.	Podmiot	Data decyzji	Sygnatura	Wysokość kary
1	Morele.net sp. z o.o.	17 stycznia 2024 r.	ZSPR.421.2.2019 oraz ZSPR.405.67.2019	3 819 960 zł
2	B.W. prowadzący działalność gospodarczą pod firmą B.	18 stycznia 2024 r.	DKN.5131.53.2021	9 903,60 zł
3	Santander Bank Polska S.A.	12 marca 2024 r.	DKN.5131.59.2022	1 440 549 zł
4	Toyota Bank Polska S.A.	12 marca 2024 r.	DKN.5131.28.2023	78 575,40 zł
5	Komitet Inicjatywy Ustawodawczej "StopLGBT"	24 kwietnia 2024 r.	DKN.5131.32.2022	10 913 zł
6	Res-Gastro M. Gaweł Sp. k.	29 kwietnia 2024 r.	DKN.5131.29.2023	238 345 zł
7	Stowarzyszenie sportowe „Maraton”	30 kwietnia 2024 r.	DKN.5131.58.2022	916,71 zł
8	American Heart of Poland S.A.	20 maja 2024 r.	DKN.5112.35.2021	1 440 549 zł
9	Samodzielny Publiczny Zespół Opieki Zdrowotnej z siedzibą w P.	13 czerwca 2024 r.	DKN.5131.57.2022	40 000 zł
10	A.Z. prowadząca działalność gospodarczą pod firma B.	10 lipca 2024 r.	DOKE.561.1.2024	21 827 zł
11	mBank S.A.	20 sierpnia 2024 r.	DKN.5131.1.2024	4 053 173 zł
12	A. K. prowadząca działalność gospodarczą pod firmą B.	30 sierpnia 2024 r.	DOKE.561.4.2024	19 644 zł
13	Prokuratura Krajowa	2 września 2024 r.	DKN.5131.33.2023	85 000 zł
14	(1) A.B. prowadzący działalność gospodarczą pod firmą X	9 października 2024 r.	DKN.5131.1.2021	353 589 zł
	(2) CD, EF, GH wspólnicy Y s.c.			9 822 zł
15	(1) X. w K.	10 października 2024 r.	DKN.5131.35.2021	15 000 zł
	(2) Y. w K.			20 000 zł
	(3) Z. sp. z o.o.			25 882,21 zł
16	X.	18 października 2024 r.	DKN.5131.7.2024	25 000 zł
17	X. w Y.	12 listopada 2024 r.	DKN.5131.9.2024	24 555 zł
17	(1) Panek S.A.	12 listopada 2024 r.	DKN.5130.2415.2020	1 527 855 zł
	(2) X. z siedzibą w W.			20 037 zł
19	"Szpital Powiatowy we Wrześni" Sp. z o.o.	26 listopada 2024 r.	DKN.5131.6.2024	29 684 zł
20	Toyota Bank Polska S.A.	18 grudnia 2024 r.	DKN.5112.14.2022	26 1918 zł 314 302 zł

Łączna wartość kar: 13 885 999,92 zł