

COMPLIANCE INSIGHTS

Vol. 73

Niezależność IOD
to nie formalność
– kara PUODO dla
Poczty Polskiej



1. Niezależność IOD pod lupą organu nadzorczego

Prezes UODO nałożył na Poczta Polska S.A. administracyjną karę pieniężną w wysokości 978 tys. zł.

Powodem było niezapewnienie Inspektorowi Ochrony Danych warunków pozwalających na niezależne sprawowanie funkcji i wykonywanie zadań IOD w sposób niepowodujący konfliktu interesów.

Decyzja jasno pokazuje, że rola IOD nie może być traktowana wyłącznie formalnie ani „na papierze” – powinna znaleźć praktyczne odzwierciedlenie w organizacji.



2. Postępowanie wyjaśniające z urzędu

Postępowanie zostało wszczęte przez PUODO z urzędu po zgłoszeniu naruszenia ochrony danych osobowych, polegającego na uzyskaniu przez osobę nieuprawnioną dostępu do danych osobowych zawartych w PIT-11.

Analiza Urzędu wykazała jednak, że problem nie dotyczył wyłącznie jednego incydentu, lecz szerszego sposobu ułożenia w organizacji nadzoru nad ochroną danych osobowych. Zgłoszenie naruszenia ochrony danych ujawniło zatem szerszy problem systemowy w spółce.



3. Konflikt interesów – IOD w wielu rolach jednocześnie

PUODO ustalił, że IOD pełnił równoległe inne funkcje o charakterze kierowniczym i operacyjnym, w tym związane z bezpieczeństwem informacji.

Taka kumulacja ról prowadziła do konfliktu interesów i podważała obiektywizm IOD w ocenie zgodności procesów przetwarzania danych z RODO. Funkcję IOD sprawowała osoba, która jednocześnie odpowiadała za obszar przetwarzania danych związany z działalnością administratora. IOD był zatem jednocześnie kontrolowanym i kontrolującym.



4. Gwarancja niezależności IOD

RODO wymaga, aby IOD wykonywał swoje zadania w sposób niezależny, bez instrukcji dotyczących treści opinii czy decyzji. Oznacza to realną autonomię, brak presji organizacyjnej oraz możliwość krytycznej oceny działań administratora. PUODO podkreślił, że niezależność musi mieć charakter faktyczny, a nie wyłącznie deklaracyjny. Taka interpretacja od lat wynika z unijnych wytycznych, które wskazują, że wymóg unikania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań przez IOD w sposób niezależny.



5. Brak analizy konfliktu interesów

Spółka nie przeprowadziła rzetelnej analizy potencjalnych konfliktów interesów związanych z łączeniem funkcji IOD z innymi obowiązkami. Nie wdrożono również mechanizmów organizacyjnych, które ograniczałyby wpływ innych ról na sposób wykonywania zadań inspektora. Żaden akt wewnętrzny spółki nie wskazywał pierwszeństwa sprawowanej funkcji przez IOD w przypadku zaistnienia konfliktu interesów. Zdaniem PUODO był to istotny błąd systemowy.



6. Wyodrębnienie funkcji IOD w strukturze organizacji

Organ nadzorczy zwrócił uwagę, że IOD powinien być wyraźnie wyodrębniony w strukturze organizacyjnej i raportować bezpośrednio do najwyższego kierownictwa.

Tylko takie umiejscowienie zapewnia skuteczny nadzór nad przestrzeganiem RODO i pozwala inspektorowi działać bez obawy o konsekwencje organizacyjne.

Gwarancje niezależności, skuteczności oraz obiektywizmu IOD zostały określone w przepisach RODO.



7. Charakter naruszeń

UODO uznał, że stwierdzone uchybienia miały charakter długotrwały i systemowy.

Niezapewnienie niezależności IOD nie było jednorazowym przeoczeniem, lecz elementem stałego modelu funkcjonowania spółki. To właśnie ten aspekt w istotny sposób wpłynął na ocenę wagi naruszenia przepisów RODO.

PUODO już wielokrotnie upominał spółkę, nakazując jej dostosowanie operacji przetwarzania danych do przepisów RODO – do tej pory bezskutecznie.



8. Wymiar kary

Przy ustalaniu wysokości kary organ wziął pod uwagę m.in. skalę działalności spółki, czas trwania naruszeń oraz znaczenie funkcji IOD dla całego systemu ochrony danych. Podkreślono, że brak niezależności inspektora realnie ogranicza skuteczność wdrażania i monitorowania zgodności z RODO.

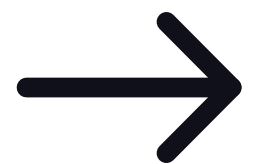
Na wymiar kary wpływ miało także dokonanie przez spółkę zmian w zakresie umiejscowienia IOD w strukturze i określeniu jego bezpośredniej relacji z zarządem spółki, przy czym zmiana została dokonana w toku sprawy, jeszcze przed wydaniem ostatecznej decyzji przez PUODO.



9. Wnioski praktyczne

Decyzja Prezesa UODO to ważne ostrzeżenie dla administratorów danych – IOD musi mieć zapewnioną niezależność organizacyjną, funkcjonalną i decyzyjną.

Niezależność IOD to element ładu organizacyjnego administratora danych. IOD nie może pełnić roli symbolicznej ani być podporządkowany interesom operacyjnym organizacji. Łączenie tej roli z innymi funkcjami wymaga rzetelnej analizy ryzyk i oceny potencjalnych konfliktów interesów. W przeciwnym razie nawet dobrze opisane procedury nie ochronią przed sankcjami.



Kontakt



Mariusz Purgał

Partner

mariusz.purgal@kwkr.pl



Alicja Łopacińska

Associate

alicja.lopacinska@kwkr.pl

Zespół Compliance KWKR



**Anna
Bartosiak**



**Justyna
Staszkiwicz-Maj**



**Katarzyna
Kanik**

KWKR

Behind Your **Growth**