

COMPLIANCE INSIGHTS

Vol. 61

IOD bez
niezależności to
realne ryzyko
prawne



1. Inspektor Ochrony Danych musi być niezależny

Zgodnie z art. 38 ust. 3 RODO administrator ma obowiązek zapewnić, by IOD nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. IOD powinien również bezpośrednio podlegać najwyższemu kierownictwu administratora.

Niezależność IOD to nie formalność – to jeden z fundamentów skutecznej ochrony danych osobowych w organizacji. Brak tej niezależności stanowi naruszenie RODO. A to oznacza ryzyko prawne wynikające z nieprawidłowej ochrony danych osobowych.



2. PUODO vs. Toyota Bank Polska S.A.

Prezes UODO uznał, że Toyota Bank Polska S.A. jako administrator danych doprowadziła do sytuacji, w której IOD nie był w pełni niezależny. Nie podlegał on bezpośrednio najwyższemu kierownictwu banku, tj. zarządowi, pracując na stanowisku IT audytora/specjalisty ds. bezpieczeństwa, a następnie w departamencie bezpieczeństwa.

IOD podlegał bezpośrednio dyrektorowi tego departamentu. Obowiązki dyrektora polegały także na zarządzaniu procesami przetwarzania danych i kontrolowaniu zabezpieczeń przetwarzania.



3. Konsekwencje finansowe i wyrok WSA

W konsekwencji PUODO nałożył na bank karę pieniężną w wysokości 261 918 zł.

Bank odwołał się do sądu, ale przegrał. W wyroku z 18 września 2025 r. WSA podzielił stanowisko PUODO stwierdzając, że zatrudnienie IOD było sprzeczne z przepisami prawa.

Administrator nie zapewnił odpowiednich środków do tego, by IOD nie otrzymywał instrukcji co do sposobu wykonywania swoich obowiązków. WSA oddalił więc skargę banku.



4. Inspektor Ochrony Danych w zarządzie

W drugiej sprawie PUODO prowadził postępowanie przeciwko spółce z branży usług medycznych, w której funkcję IOD pełnił prezes zarządu.

Spółka uznała, że powyższa sytuacja nie zagraża niezależności IOD. Według niej, działalność objęta tajemnicą lekarską wyklucza konflikt interesów, a prezes spółki najlepiej zadba o dane pacjentów. PUODO uznał tę interpretację art. 38 ust. 6 RODO za błędną.



5. Inspektor Ochrony Danych a konflikt interesów

Zgodnie z art. 38 ust. 6 RODO, IOD może wykonywać inne zadania i obowiązki. Administrator ma natomiast obowiązek zapewnić, że takie zadania i obowiązki nie powodują konfliktu interesów.

Konflikt interesów to nic innego jak sytuacja, w której istnieje obawa negatywnego wpływu określonych okoliczności na bezstronne oraz niezależne wykonywanie obowiązków przez IOD.



6. Decyzja PUODO

Zdaniem PUODO spółka naruszyła przepisy, bowiem prezes zarządu nie może być jednocześnie IOD. Takie rozwiązanie organizacyjne jest sprzeczne z RODO i nie daje gwarancji, że obowiązki związane z ochroną danych osobowych będą wykonywane w sposób niezależny i obiektywny.

Spółka może dbać organizacyjnie i technicznie o bezpieczeństwo danych osobowych tylko wtedy, gdy niezależny od kierownictwa IOD może informować je o problemach i wskazywać, co i jak należy poprawić. PUODO zdecydował się nałożyć na spółkę karę w wysokości 11.365 zł.



7. Konflikt interesów w praktyce

IOD musi być niezależny od osób, które kontroluje. Tę zasadę potwierdzają decyzje Prezesa UODO, w których podkreśla się, że tylko niezależny IOD może skutecznie dbać o ochronę danych zgodnie z RODO.

W praktyce konflikt interesów i brak niezależności najczęściej dotyczy pełnienia przez IOD jednocześnie funkcji członka zarządu, dyrektora IT lub bezpieczeństwa, czy też audytora odpowiedzialnego za systemy przetwarzające dane.



8. Wnioski dla administratora lub procesora danych

Jako administrator lub procesor danych, powołujący w swojej organizacji IOD:

- Sprawdź organizacyjne usytuowanie IOD – czy podlega bezpośrednio najwyższemu kierownictwu?
- Zidentyfikuj potencjalne konflikty interesów – IOD nie może pełnić funkcji, które sam powinien nadzorować.
- Zapewnij realną niezależność – unikaj sytuacji, w których IOD działa pod wpływem zależności służbowych lub decyzyjnych.
- Nie traktuj IOD-a fasadowo – jego rola to nie formalność, ale kluczowy element systemu ochrony danych i zgodności z RODO.



Kontakt



Mariusz Purgał

Partner

mariusz.purgal@kwkr.pl



Agata Baca

Associate

agata.baca@kwkr.pl

Zespół Compliance KWKR



**Paweł
Zyskowski**



**Katarzyna
Kanik**



**Bartosz
Bogusławski**



**Anna
Bartosiak**



**Alicja
Łopacińska**



**Justyna
Staszkievicz-Maj**