Warszawa, dn. 29.10.2025 r.

UODO egzekwuje niezależność IOD – jak nie wpaść w pułapkę przerzucania obowiązków na inspektora?

UODO egzekwuje niezależność IOD – jak nie wpaść w pułapkę przerzucania obowiązków na inspektora?

Od dłuższego czasu w środowisku prawników, inspektorów ochrony danych i specjalistów compliance toczy się dyskusja, jak daleko sięga rola IOD w procesie reagowania na naruszenia ochrony danych osobowych. Choć teoretyczne ramy wynikają bezpośrednio z RODO, praktyka wielu organizacji wciąż pokazuje coś innego: inspektorzy stają się osobami faktycznie obsługującymi incydenty, zamiast doradzającymi administratorowi.

Tymczasem UODO coraz wyraźniej i konsekwentniej egzekwuje rozdzielenie ról między administratorem a inspektorem. W jednym z pism z **pierwszej połowy października 2025 r.** organ nadzorczy sformułował **jedno z najbardziej precyzyjnych stanowisk, jakie jak dotąd widzieliśmy** w naszej praktyce a dotyczące właśnie interpretacji art. 38 ust. 6 RODO i obowiązków IOD w postępowaniu związanym z naruszeniem danych osobowych.

UODO twardo: inspektor nie może działać w imieniu administratora

W piśmie z pierwszej połowy października 2025 r. Prezes Urzędu Ochrony Danych Osobowych jednoznacznie wskazał, że powierzanie inspektorowi ochrony danych (IOD) czynności, które należą do administratora danych, stanowi naruszenie zakazu konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

Organ podkreślił, że w wielu organizacjach obserwuje się praktykę, w której to właśnie IOD — z uwagi na swoją wiedzę i doświadczenie — faktycznie realizuje obowiązki spoczywające na administratorze, w tym w szczególności:

- przygotowuje i podpisuje zgłoszenia naruszeń kierowane do UODO,
- samodzielnie wysyła zawiadomienia do osób, których dane dotyczą,
- prowadzi dokumentację incydentów oraz proponuje działania naprawcze.

Jak wskazano w piśmie, takie działanie jest niedopuszczalne, ponieważ inspektor ochrony danych pełni funkcję doradczą i nadzorczą – a nie wykonawczą. UODO wyraźnie zaakcentował, że inspektor nie może być jednocześnie doradcą, wykonawcą i kontrolerem w tym samym procesie, gdyż rodzi to bezpośredni konflikt interesów i prowadzi do utraty niezależności roli.

Organ szczegółowo wyjaśnił, że w sytuacji, gdy inspektor sam dokonuje zgłoszenia naruszenia do UODO lub kontaktuje się z osobami, których dane dotyczą, a następnie – w ramach swoich obowiązków – ma monitorować prawidłowość przebiegu tego procesu, dochodzi do wewnętrznej sprzeczności funkcji. IOD staje się wówczas podmiotem, który kontroluje samego siebie, co jest nie do pogodzenia z zasadą bezstronności i niezależności funkcji inspektora wynikającą z art. 38 ust. 3 RODO.

W uzasadnieniu UODO przypomniał, że **administrator danych ponosi wyłączną odpowiedzialność za realizację obowiązków z art. 33 i 34 RODO**, tj. za dokonanie oceny ryzyka, podjęcie decyzji o zgłoszeniu naruszenia, przygotowanie dokumentacji, a także za poinformowanie organu nadzorczego i osób, których dane dotyczą. Inspektor może wspierać administratora, ale nie może go zastępować w wykonywaniu tych obowiązków.

W piśmie znalazły się też odwołania do wcześniejszych materiałów edukacyjnych Urzędu, w tym biuletynów *„Niezależność IOD musi być standardem”* oraz *„Rola IOD przy naruszeniach ochrony danych*

osobowych". W obu publikacjach organ podkreślał, że nakładanie na inspektora ochrony danych obowiązków należących do administratora lub podmiotu przetwarzającego prowadzi do utraty obiektywizmu oraz wewnętrznego konfliktu interesów.
To stanowisko wydaje się być teraz wzmocnione i jednoznacznie przeniesione z poziomu zaleceń do poziomu praktycznej egzekucji.
W praktyce oznacza to, że inspektor:

- nie podpisuje zgłoszeń naruszeń kierowanych do UODO, nawet jeśli brał udział w ich opracowaniu;
- nie wysyła zawiadomień do osób, których dane dotyczą, choć może opiniować ich treść;
- nie prowadzi rejestru naruszeń w imieniu administratora – obowiązek dokumentowania incydentów należy do administratora;
- nie podejmuje działań naprawczych ani nie wdraża środków bezpieczeństwa, a jedynie doradza w zakresie ich doboru i adekwatności.

UODO wskazał przy tym, że w praktyce dopuszczalne jest, by IOD wspierał administratora merytorycznie w opracowaniu zgłoszenia lub zawiadomienia, ale ostateczne decyzje, podpisy i komunikacja z organem muszą być realizowane przez osoby działające z upoważnienia administratora.
Organ podsumował, że utrzymanie jasnej granicy między funkcją doradczą a wykonawczą jest niezbędne dla zachowania wiarygodności i skuteczności systemu ochrony danych w organizacji. W przeciwnym razie administrator naraża się nie tylko na zarzut naruszenia art. 38 RODO, lecz także na ryzyko, że jego zgłoszenie zostanie uznane za nieprawidłowe, a proces monitorowania – za pozbawiony niezależności.

Powszechny błąd: „Skoro IOD zna RODO, to niech się tym zajmie"
W wielu organizacjach IOD zostaje „operacyjnym właścicielem" incydentu: przygotowuje zgłoszenie do UODO, podpisuje je, wysyła zawiadomienia do osób, prowadzi rejestr naruszeń i nadzoruje wdrożenie środków zaradczych. **To wygodne organizacyjnie, ale jak widać sprzeczne z RODO**.
Powstaje pytanie jak to „ułożyć prawidłowo – na początek rozdział ról (segregation of duties) – matryca „*RACI*"

- **Responsible (R)**: właściciel procesu/incydentu po stronie biznesu/IT (zwykle Security/IT + właściciel systemu).
- **Accountable (A)**: **administrator danych** (zarząd/członek zarządu/pełnomocnik/koordynator ODO) – podejmuje decyzje, zatwierdza treści i **podpisuje** zgłoszenia oraz zawiadomienia.
- **Consulted (C)**: **IOD** (opinie, rekomendacje, konsultacje treści, kwalifikacja, ocena ryzyka).
- **Informed (I)**: PR/komunikacja, HR, Legal, Risk.

a w dalszej kolejności zmiana / dostosowanie dokumentacja i upoważnień np.: poprzez wyraźne wskazanie, że IOD nie podpisuje zgłoszeń ani zawiadomień i nie działa jako pełnomocnik administratora przed UODO. Wprowadzenie zasady we wzorach pism w zakresie miejsca na podpis osoby działającej w imieniu administratora (nie IOD), z dołączonym zakresem umocowania (pełnomocnictwo wewn./ZK). Ponadto, możliwa jest checklista art. 33–34: decyzja o zgłoszeniu, termin 72h, sposób zawiadomienia osób, opis środków zaradczych – z polami na akcept administratora. Na zakończenie rejestr naruszeń (art. 33 ust. 5) ma być prowadzony przez administratora a IOD ma wyłącznie wgląd i dokonuje ewentualnych adnotacji, uwag.

Jak wyjść z tej pułapki braku kompetencji po stronie administratora?
UODO, akcentując zakaz powierzania IOD zadań należących do administratora, pośrednio wskazuje na szerszy problem – **niedostateczne przygotowanie organizacji do samodzielnej obsługi incydentów**. W wielu podmiotach brak jest odpowiednich procedur, zespołów czy narzędzi, które umożliwiałyby administratorowi skuteczne wypełnienie obowiązków z art. 33 i 34 RODO. W efekcie, nawet przy najlepszych intencjach, ciężar obsługi incydentu spada na IOD, co prowadzi do opisanych przez UODO konfliktów funkcji.
W takich sytuacjach konieczne staje się **usystematyzowanie procesu reagowania na naruszenia** – zarówno poprzez szkolenie personelu i wyznaczenie wewnętrznych koordynatorów, jak i przez zapewnienie dostępu do zewnętrznego wsparcia merytorycznego. Nie chodzi tu o „oddanie" obowiązków inspektora, ale o stworzenie modelu, w którym administrator ma realne zaplecze do wykonywania własnych zadań, a IOD może pełnić funkcję doradczą i kontrolną w sposób niezależny.

Outsourcing i model hybrydowy
Coraz częściej organizacje decydują się na **model mieszany**, łączący wewnętrzną odpowiedzialność administratora z zewnętrznym wsparciem specjalistycznym. Taki model może obejmować m.in.:

- pomoc w analizie ryzyka i kwalifikacji incydentów,
- wsparcie przy przygotowaniu dokumentacji zgłoszeniowej,
- opracowanie wzorcowych komunikatów i rekomendacji środków naprawczych.

Rozwiązanie to pozwala zachować **niezależność IOD**, który nadal doradza i monitoruje działania administratora, ale nie wykonuje ich w jego imieniu.
W praktyce model hybrydowy stanowi odpowiedź na rzeczywiste potrzeby organizacji – pozwala na zapewnienie zgodności z RODO, bez naruszania strukturalnego rozdziału ról pomiędzy administratorem a inspektorem.

Podsumowanie
UODO od dawna zapowiadał, że rola IOD wymaga uporządkowania. Dziś widać, że te zapowiedzi stają się rzeczywistością – organ **aktywnie egzekwuje zasadę niezależności IOD i odpowiedzialność administratora za obsługę incydentów**. To sygnał dla każdej organizacji: czas na przegląd procedur, szkolenia i jasne przypisanie obowiązków. IOD ma doradzać i nadzorować, administrator – działać i odpowiadać. Świadomy rozdział ról to nie tylko wymóg RODO, ale też sposób na realne bezpieczeństwo danych i uniknięcie konfliktu interesów, który coraz częściej znajduje się w centrum zainteresowania UODO.

Paweł Wojciechowski – adwokat, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.