Wewnętrzny inspektor ochrony danych, a konflikt interesów w organizacji

Zgodnie z RODO obowiązkiem niektórych administratorów i przetwarzających będzie powołanie inspektora ochrony danych (IOD). Taki obowiązek będzie miał miejsce w przypadku wszystkich organów i podmiotów publicznych, jak również w stosunku do podmiotów, które w ramach swojej głównej działalności regularnie i na dużą skalę monitorują osoby lub jeżeli działalność podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych. Nawet jeżeli RODO bezpośrednio nie nakłada obowiązku powołania inspektora ochrony danych, coraz częściej pojawiają się głosy, że podmioty mogą skorzystać na jego powołaniu.

Z RODO wynika, że IOD może być członek personelu lub osoba z zewnątrz, świadcząca usługi związane z ochroną danych osobowych. Nie oznacza to jednak, że można wyznaczyć dowolną osobę do pełnienia funkcji inspektora. Pamiętajmy, że inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji awodowych, wiedzy fachowej z ochrony danych.

Czy członek zarządu albo szef compliance może być inspektorem ochrony danych?

Okazuje się, że nie wszystkie stanowiska, mogą być łączone z funkcją IOD. Tak wskazuje sama Europejska Rada Ochrony Danych, Prezes UODO, a także inne europejskie organy nadzorcze.

Zgodnie z Wytycznymi Grupy Roboczej art. 29, inspektorem ochrony danych nie może być osoba pozostająca w „konflikcie interesów". I zgodnie z tymi wytycznymi, co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze. Na przykład: dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT. Takim stanowiskiem kierowniczym będzie pełnienie funkcji członka zarządu, bez względu na sposób wynagradzania czy zatrudnienia takiego członka zarządu.

Stanowisko wyrażone przez polski organ nadzorczy, jest właściwie powtórzeniem powyższego stanowiska EROD. Prezes UODO rekomenduje również opracowanie wewnętrznej polityki określającej stanowiska będące w konflikcie interesów oraz opracowanie generalnego dokumentu dotyczącego konfliktu interesów.

Aby zrozumieć powyższe, przypomnijmy sobie czym zajmuje się IOD? Zgodnie z **art. 39 ust. 1 RODO**, do zadań IOD należą m.in.:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników o ich obowiązkach,
- doradztwo w sprawie ochrony danych osobowych,
- monitorowanie przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego,

- podejmowanie działań zwiększających świadomość w zakresie ochrony danych osobowych,
- udział w postępowaniach wyjaśniających,
- przeprowadzanie szkoleń i audytów,
- udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- aktywne uczestnictwo w procesach biznesowych związanych z przetwarzaniem danych osobowych,
- współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego.

Nie można również zapomnieć, że do właściwego wykonywania obowiązków przez IOD niezbędne jest:

- zagwarantowanie IOD odpowiedniej pozycji w strukturze organizacji – IOD musi podlegać on bezpośrednio kierownictwu administratora lub podmiotu przetwarzającego.
- wyposażenie IOD w odpowiednie zasoby – IOD powinien być wspierany w swoich działaniach, właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, mieć wystarczającą ilość czasu na wykonywanie zadań, a także odpowiednie wsparcie finansowe, kadrowe i infrastrukturalne.
- zapewnienie, aby funkcja była pełniona w sposób bezstronny i niezależny – IOD nie może być związany otrzymywanymi instrukcjami, a także nie może być odwoływany ani karany za wypełnianie swoich zadań.

Co więcej, Art. 36 ust. 6 RODO wskazuje, że IOD może wykonywać inne zadania i obowiązki, ale jego przełożeni muszą zapewnić, by nie powodowały one konfliktu interesów.

Wymogi prawne stawiane IOD są wysokie, a łączenie tego stanowiska z inną funkcją może wpłynąć na bezstronność i prawidłowość sprawowania powierzonej funkcji. Dodatkowo, łączenie obu funkcji stawia pod znakiem zapytania po pierwsze **możliwość zagwarantowania poufności** działań prowadzonych przez IOD i inne stanowisko oraz **może powodować konflikt interesów** w postaci kontrolowania jednej funkcji przez drugą.

Podobne podejście jest prezentowane:

- w zaleceniach wydanych przez Grupę Roboczą Art. 29, w których wskazano, że IOD **nie może** zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. W zaleceniach zostały wymienione przykładowe stanowiska, których nie należy łączyć z funkcją IOD, a także wskazano dobre praktyki i działania, których podjęcie zmniejszy ryzyko naruszenia przepisów: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT),
- w zaleceniach Grupy Roboczej art. 29 jako dobrą praktykę dla organizacji proponuje się zidentyfikowanie stanowisk niekompatybilnych z funkcją

inspektora ochrony danych oraz opracowanie wewnętrznych zasad uniemożliwiających łączenie stanowisk będących w konflikcie interesów,

- przez Urząd Ochrony Danych Osobowych, który podziela stanowisko Grupy Roboczej Art. 29. UODO i podkreśla także konieczność każdorazowego zbadania konkretnego przypadku oraz spełnienia wszystkich obowiązków wynikających z RODO (np. prawidłowe umiejscowienie IOD w strukturze organizacji oraz zapobieganie powstaniu konfliktu interesów),

Należy pamiętać, iż 28 kwietnia 2019 r. belgijski organ ds. danych osobowych nałożył na firmę Proximus S.A. karę grzywny w wysokości 50 000 EUR w związku z m.in. połączeniem funkcji IOD z innymi stanowiskami, w tym ze stanowiskiem szefa compliance. W uzasadnieniu organ wskazał, że tak obsadzone stanowisko IOD powoduje niewystarczające zaangażowanie w proces przetwarzania danych osobowych oraz zarządzania naruszeniami, a także brak gwarancji pełnej poufności. Podkreślono również wystąpienie konfliktu interesów. Uznano również, że wskutek połączenia stanowisk, IOD określa cele i sposoby przetwarzania danych osobowych, a to jest niezgodne z obowiązującymi przepisami.

W kwietniu 2020 roku, belgijski organ ochrony danych (DPA) ukarał Administratora Danych za powołanie dyrektora ds. zgodności, audytu i ryzyka na Inspektora Ochrony Danych. Według DPA, ta kombinacja ról powoduje konflikt interesów, a zatem stanowi naruszenie art. 38 ust. 6 RODO. Kara wynosi 50 tys. EUR.

Podsumowując, podjęcie decyzji o połączeniu funkcji IOD i połączeniu tej funkcji powinno być poprzedzone analizą pod kątem prawidłowego i efektywnego sprawowania każdej z nich. Mając na uwadze rekomendacje wskazane powyżej oraz podejście europejskich organów nadzorczych, w naszej ocenie bezpieczniejszą opcją z punktu widzenia przedsiębiorcy jest dążenie do rozdzielenia funkcji IOD w celu zapewnienia niepodważalnej bezstronności, niezależności oraz efektywności działań wskazanych osób.

W przypadku IOD zewnętrznego, znacznie łatwiej zadbać o niezależność oraz uniknąć konfliktu interesów wewnątrz organizacji. Łatwiej o niezależność faktyczną i formalną.

Olga Skotnicka – ekspert ds. ochrony danych osobowych w iSecure Sp. z o.o.