Warszawa, 12.02.2025 r.

Rola Inspektora Ochrony Danych w organizacji. Co IOD może, a czego nie powinien robić?

WSTĘP

Niezależność Inspektora Ochrony Danych (IOD) jest jednym z najważniejszych elementów skutecznej ochrony danych osobowych. Przepisy RODO, a w szczególności artykuł 38, gwarantują inspektorowi autonomię, dzięki której może on wypełniać swoje zadania zgodnie z artykułem 39. Niezależność ta oznacza, że IOD powinien mieć możliwość samodzielnego dostarczania analiz i zaleceń dotyczących przetwarzania danych oraz podejmowania decyzji bez wpływu innych osób czy podmiotów w organizacji. Ważnym aspektem niezależności jest również brak konfliktu interesów – inspektor nie może weryfikować decyzji, które sam podejmuje wspólnie z administratorem danych, ani działać pod wpływem osób, które mogłyby ograniczać jego swobodę działania.

NIEZALEŻNOŚĆ IOD

Warto więc zwrócić szczególną uwagę na postanowienia RODO, które gwarantują niezależność IOD. Art. 38 wskazuje w:

Ust.3: „*Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.*”

Ust. 6: „*Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.*”

Grupa Robocza art. 29 w wytycznych dotyczących inspektorów ochrony danych (DPO)[1] wskazuje na praktyczne przykłady działalności IOD. GR29 podkreśla konieczność zaangażowania IOD lub jego zespołu od najwcześniejszego etapu we wszystkich kwestiach związanych z ochroną danych osobowych. Zaangażowanie IOD w każdy proces biznesowy powinno być normą. Zaangażowanie te powinno przejawiać się m.in.: w udziale IOD w spotkaniach średniego i wyższego szczebla pracowników, zajmowanie stanowiska przez IOD w każdej decyzji dotyczącej przetwarzania danych, czy natychmiastowa konsultacja z IOD w sprawach dot. naruszenia ochrony danych osobowych.

Niezależność IOD ma się objawiać tym, że to na końcu administrator i podmiot przetwarzający są odpowiedzialni za przestrzeganie przepisów RODO i to te podmioty muszą być w stanie wykazać ich przestrzeganie. IOD ma prawo zgłoszenia swoich uwag i rekomendacji i przedstawienie ich najwyższemu kierownictwu, ale ostateczną decyzję na końcu podejmuje dana organizacja (w zasadzie organ zarządzający organizacją). UODO w swoich stanowiskach[2] podkreśla, że zadania IOD charakteryzują się tym, że jest to osoba, która monitoruje przestrzeganie przepisów RODO i wewnętrznych polityk danego administratora, przy jednoczesnym nadzorze nad realizacją obowiązków. IOD nie może wykonywać obowiązków administratora „za niego". IOD ma być ciałem doradczym, wspierającym, wydającym rekomendacje, a nie osobą, która będzie realizować te rekomendacje. Takie rozumienie i realizacja funkcji IOD została bardzo dobrze pokazana w jednej z decyzji PUODO o sygn. ZWAD.405.31.331.2019. Urząd upomniał w nim administratora danych, ponieważ w jego organizacji IOD odpowiedzialny był za nadawanie upoważnień do przetwarzania danych pracownikom. PUODO podkreśliło w decyzji[3], że: „(…)*Podstawowy zakres zadań IOD, wśród których na próżno szukać jednak tych związanych z nadawaniem pracownikom administratora upoważnień do przetwarzania danych osobowych, określony został przez unijnego ustawodawcę w art. 39 ust. 1 RODO, niemniej jednak zgodnie z art. 38 ust. 6 RODO IOD może wykonywać też inne zadania i obowiązki, o ile administrator lub podmiot przetwarzający zapewni, aby te zadania i obowiązki nie powodowały konfliktu interesów. Należy jednak przyjąć, że z uwagi na specyfikę zadań IOD ogniskujących się na doradzaniu oraz kontrolowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, administrator*

[1] https://uodo.gov.pl/data/filemanager_pl/15.pdf
[2] https://uodo.gov.pl/pl/p/archiwum-biuletynu-dla-iod
[3] https://uodo.gov.pl/decyzje/ZWAD.405.31.331.2019

nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych, pozostawiając IOD w procedurze wydawania upoważnień do przetwarzania danych osobowych sprawowanie funkcji doradczej i nadzorczej. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za przeprowadzenie tej procedury, a jednocześnie miałby monitorować jej zgodność z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b) RODO, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 RODO. Wyraźnego podkreślenia wymaga fakt, iż IOD, cechujący się szczególnym statusem w dziedzinie zapewniania właściwego przestrzegania przepisów o ochronie danych osobowych, musi mieć dla tego celu zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację obowiązków wynikających z przepisów prawa, co wynika z art. 38 ust. 2 i 3 RODO."

Jedna z najnowszych decyzji administracyjnych PUODO (DKN.5112.14.2022)[4] nałożył administracyjną karę pieniężną na Toyota Bank Polska S.A. m.in., że Inspektor Ochrony Danych nie posiadał odpowiedniej niezależności. IOD nie odpowiada bezpośrednio organom zarządzającym, a zatrudniony był w jednym z Departamentów, w którym to podlegał pod Dyrektora tegoż Departamentu. Jednocześnie osoba będąca IOD pełniła również inne obowiązki, które PUODO określiło jako czynności związane z kreowaniem procesów przetwarzania danych. Osoba ta „raportowała" dyrektorowi Departamentu również kwestie, które bezpośrednio dotyczyły celów i sposobów przetwarzania danych osobowych. Jak wskazano w decyzji to obowiązków tej osoby należało m.in. tworzenie i wdrożenie polityk, kontrola stosowania procedur i polityk, a także określenie wymogów funkcjonowania systemów informatycznych. Dodatkowo w zakresie wykonywania funkcji IOD osoba ta zobowiązana była m.in. obsługa naruszeń ochrony danych osobowych. PUODO w uzasadnieniu decyzji stwierdził, że stan faktyczny jasno wskakuje, że IOD nie podlegał bezpośrednio najwyższego kierownictwa, co nie spełnia wymogów art. 38 ust. 3 RODO. PUODO zwróciło wyraźnie uwagę, że: „ *nie może dochodzić do sytuacji, jak w przedmiotowej sprawie, że administrator, tj. C. S.A., wprowadza określone środki organizacyjne, takie np. jak polityka (…), w których deklaruje niezależność IOD w wykonywaniu jego obowiązków, w tym jego podległość wyłącznie i bezpośrednio najwyższemu kierownictwu (tj. w przedmiotowej*

[4] https://uodo.gov.pl/decyzje/DKN.5112.14.2022

sprawie zarządowi C. S.A.), a jednocześnie faktycznie stosuje rozwiązania organizacyjno-prawne, takie jak umowy o pracę wraz z określeniem w nich zakresu obowiązków, z których wynika, że stoją one w sprzeczności z postanowieniami polityki, a w konsekwencji z treścią art. 38 ust. 3 rozporządzenia 2016/679."

Co ciekawe, zdaniem PUODO konflikt interesów mógłby wystąpić również w przypadku, gdyby IOD odpowiedzialny byłby za sporządzanie projektów umów powierzenia. Konflikt ten polegałby jednocześnie na tym, że z jednej strony IOD kształtowałby prawa i obowiązki administratora/podmiotu przetwarzającego wskazane w umowie, a z drugiej strony zobowiązany byłby do weryfikacji i oceny tych obowiązków w zakresie sprawowania funkcji doradczej. Przez konflikt interesów można rozumieć, że IOD nie może jednocześnie pełnić funkcji kierowniczych lub funkcji niższego szczebla w organizacji, która to funkcja bierze udział w określaniu celów i sposobów przetwarzania danych. PUODO wskazał, że zajmowanie stanowisk kierowniczych przez IOD jest sytuacją powodującą konflikt interesów tj. „*dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych. Ponadto konflikt interesów może powstać wówczas, gdy zewnętrzny IOD zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych.*"

PUODO dalej wskazuje, że opracowanie wewnętrznej dokumentacji ochrony danych osobowych to rola administratora. IOD ma za zadanie dokonywać oceny przyjętych polityk i wskazywać na ewentualne braki lub niezgodności. Prowadzenie Rejestru Czynności Przetwarzania także jest obowiązkiem po stronie administratora/podmiotu przetwarzającego. Natomiast Grupa Robocza art. 29 wskazuje w swoich wytycznych, że administrator może powierzyć IOD prowadzenie Rejestru Czynności Przetwarzania: „*Artykuł 39(1) określa minimalną listę zakresu obowiązków DPO. W związku z tym nic nie stoi na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył DPO prowadzenie, w imieniu administratora albo podmiotu przetwarzającego, rejestru czynności przetwarzania danych.*"

CO IOD MOŻE?

Zadania jakie wprost może realizować Inspektor Ochrony Danych także wprost wskazuje w Rozporządzeniu. Art. 39 ust. 1 stanowi, że IOD ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35,

d) współpraca z organem nadzorczym,

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego.

RODO zapewnia inspektorowi ochronę i odpowiednie warunki pracy. Administrator danych lub podmiot przetwarzający zobowiązani są do wspierania IOD poprzez zapewnienie mu zasobów, takich jak dostęp do danych, operacji przetwarzania oraz możliwość rozwijania wiedzy fachowej. IOD powinien bezpośrednio podlegać najwyższemu kierownictwu organizacji, co zapobiega nadmiernej ingerencji ze strony niższych szczebli zarządzania. Jednocześnie inspektor musi być na bieżąco angażowany we wszystkie sprawy związane z przetwarzaniem danych, aby mógł skutecznie nadzorować zgodność procesów z przepisami.

Przepisy te chronią IOD również przed instrukcjami ze strony administratora danych. Inspektor nie może otrzymywać poleceń, które wpływałyby na jego niezależne decyzje. Oprócz tego, zgodnie z przepisami, inspektor nie może być odwoływany ani karany za realizację swoich zadań, co zapewnia mu swobodę podejmowania obiektywnych decyzji bez obawy o konsekwencje zawodowe. Ważnym elementem jest także unikanie sytuacji, w których inne obowiązki mogłyby wpływać na obiektywizm IOD. Dlatego nie może on pełnić ról w organizacji, które powodowałyby konflikt interesów, takich jak podejmowanie decyzji dotyczących operacji przetwarzania danych.

ROLA IOD PRZY NARUSZENIACH

W ostatnich pismach kierowanych przez Urząd Ochrony Danych Osobowych (UODO) do administratorów danych podkreślono, że inspektor nie powinien wykonywać pewnych zadań, które mogłyby wpływać na jego niezależność. Należy do nich zgłaszanie naruszeń ochrony danych osobowych, podpisywanie pism i formularzy związanych z tymi zgłoszeniami, a także wysyłanie zawiadomień do osób, których dane dotyczą. IOD nie powinien również odpowiadać za dokumentowanie naruszeń zgodnie z art. 33 ust. 5 RODO. Te działania powinny być przypisane innym jednostkom organizacyjnym, aby uniknąć sytuacji, w której inspektor traci swoją niezależność poprzez angażowanie się w zadania wykonawcze.

Administrator danych jest zobowiązany do aktywnego wspierania IOD poprzez zapewnienie mu zasobów, pełnej informacji oraz przestrzegania zasad, które gwarantują jego niezależność. Inspektor musi mieć przestrzeń do obiektywnego działania oraz możliwość wcześniejszego identyfikowania i sygnalizowania zagrożeń związanych z ochroną danych osobowych. Administratorzy, a także sami inspektorzy oraz organy nadzorcze, mają obowiązek współpracować na rzecz ochrony prywatności i praw osób, których dane są przetwarzane.

Wyznaczenie inspektora ochrony danych jest obowiązkowe w określonych sytuacjach. Dotyczy to organizacji, które regularnie i na dużą skalę monitorują osoby fizyczne lub przetwarzają szczególne kategorie danych, takie jak informacje o stanie zdrowia czy wyroki skazujące. Obowiązek ten dotyczy również organów i podmiotów publicznych. Choć IOD odgrywa kluczową rolę w monitorowaniu zgodności z przepisami, nie ponosi on osobistej odpowiedzialności za ewentualne naruszenia ochrony danych – odpowiedzialność ta spoczywa na administratorze danych.

PODSUMOWANIE

Podsumowując, niezależność Inspektora Ochrony Danych jest kluczowa dla skutecznego zarządzania danymi osobowymi i ochrony prywatności. Zasady tej niezależności określone w RODO mają na celu umożliwienie inspektorowi pełnego wykonywania jego funkcji w sposób obiektywny, niezależny od wpływów zewnętrznych. Organizacje muszą dbać o przestrzeganie tych przepisów, by zapewnić zgodność przetwarzania danych z

obowiązującymi regulacjami prawnymi. Ostatnie wytyczne
PUODO w zakresie niezależności i obowiązków IOD, zwłaszcza w zakresie roli IOD przy zgłaszaniu naruszeń mogą wpłynąć na dotychczasowe obowiązki Inspektorów w organizacji administratora/podmiotu przetwarzającego.

Maciej Łukaszewicz - Radca prawny, specjalista ds. ochrony danych osobowych