Warszawa, 19.03.2025 r.

Niezależny inspektor ochrony danych, czyli jaki?

Od ponad roku Urząd Ochrony Danych Osobowych (UODO) sporo mówi o niezależności inspektora ochrony danych (IOD). W kwietniu 2024 r. zorganizował nawet specjalne wydarzenie połączone z transmisją on-line, które w całości poświęcone było temu zagadnieniu. A jeszcze wcześniej byliśmy świadkami kilku kontroli, których wspólnym mianownikiem było tzw. 27 pytań, których celem było zweryfikowanie przez UODO stopnia przestrzegania przez administratorów danych przepisów dotyczących IOD. Obecnie można już zaobserwować pierwsze decyzje administracyjne, gdzie ten wątek przejawia się albo jako motyw przewodni (decyzja wraz z karą finansową nałożoną na Toyota Bank) albo niejako przy okazji np. zgłaszania naruszeń ochrony danych.

Niezależny… Czyli co?

Nie sposób nie zacząć rozważań na interesujący mnie temat od przywołania definicji słowa „niezależny". W tym celu oczywiście najlepiej sięgnąć do Słownika Języka Polskiego PWN. A zatem: niezależny to inaczej „niepodporządkowany komuś, czemuś, decydujący o sobie; też: świadczący o braku podporządkowania komuś lub czemuś"[1].
Teraz rzućmy okiem do RODO. Na początek fragment motywu 97, gdzie jest mowa o tym, że „inspektorzy ochrony danych - bez względu na to, czy są pracownikami administratora - powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny".

Atrybuty niezależności w RODO

Tu przede wszystkim z pomocą przychodzi nam art. 38 RODO, gdzie wskazuje się na to, że zarówno administrator danych jak i podmiot przetwarzający muszą:

- zapewnić, żeby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania (swoich) zadań,
- nie odwoływać ani nie karać IOD za wypełnianie swoich zadań,
- zapewnić bezpośrednią podległość IOD najwyższemu kierownictwu administratora lub podmiotu przetwarzającego,
- zapewnić zasoby niezbędne do wykonania zadań IOD oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania wiedzy fachowej IOD,
- w przypadku zlecania innych zadań i nakładania dodatkowych obowiązków na IOD – zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów,

Ponadto IOD jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego, co moim zdaniem również wpisuje się w niezależność inspektora ochrony danych.

[1] Źródło: https://sjp.pwn.pl/slowniki/niezale%C5%BCny.html

Przypadek Toyota Bank

W styczniu 2025 r. światło dzienne ujrzała decyzja PUODO dotycząca Toyota Bank[2]. To bardzo interesujący materiał do analizy właśnie pod kątem niezależnego IOD, ponieważ jeden z dwóch wątków poruszonych w tej decyzji dotyczył właśnie IOD.

W toku czynności prowadzonych przez Prezesa UODO okazało się, że powołany w Toyota Bank inspektor ochrony danych nie podlegał bezpośrednio najwyższemu kierownictwu ww. Banku (tj. jego zarządowi). Ponadto IOD jednocześnie pracował na stanowisku IT audytora/specjalisty ds. bezpieczeństwa w zespole ds. bezpieczeństwa, a następnie w departamencie bezpieczeństwa, podlegając bezpośrednio dyrektorowi tego departamentu. Dalej PUODO wskazał, że obowiązki tego dyrektora polegały również na zarządzaniu procesami przetwarzania danych.

Nie trzeba tu robić pogłębionej analizy przepisów RODO, zwłaszcza zaś przytaczanego wcześniej art. 38, by zauważyć, że w powyższym przypadku doszło do naruszenia tychże przepisów. Co ciekawe, Toyota Bank argumentował PUODO, że usytuowanie IOD w departamencie bezpieczeństwa „ma jedynie wymiar administracyjny (np. akceptacja urlopów oraz ustalenie warunków finansowych)", natomiast sam inspektor ochrony danych w zakresie swoich obowiązków (jako IOD) był całkowicie niezależny.

Najwyraźniej powyższa argumentacja nie przekonała PUODO, ponieważ Toyota Bank został ukarany m.in. za niewłaściwe usytuowanie IOD.

Przypadek Toyota Banku wydaje mi się dość oczywisty i – o ile mogę sobie pozwolić na tego typu komentarz – PUODO, w moim przekonaniu, podjął słuszną decyzję.

IOD z pełnomocnictwem – czy tak można?

Przez naprawdę długi czas temat dokonywania pewnych czynności przez IOD na bazie pełnomocnictwa (konkretnie chodzi tu o dokonanie zgłoszenia wyznaczenia IOD a także zgłaszania naruszeń) nie był w ogóle kwestionowany przez organ nadzorczy.

Pierwsze pisma z UODO, które poruszały tę kwestię zaczęły pojawiać się w 2024 r. Zobaczymy co UODO wskazywał w tego typu korespondencji:

„Udzielenie inspektorowi ochrony danych pełnomocnictwa do występowania w imieniu administratora (reprezentowania administratora) przed organem nadzorczym w sprawach z zakresu ochrony danych osobowych stoi w kolizji z nakazem nienakładania na IOD zadań powodujących konflikt interesów. Zadaniem IOD jest informowanie administratora o obowiązkach spoczywających na nim na mocy RODO, doradzanie mu w tym zakresie oraz monitorowanie wykonania tych obowiązków (art. 39 ust. 1 lit. a i b RODO). Występowanie w roli pełnomocnika administratora w zakresie obowiązków nałożonych na administratora może istotnie utrudniać lub uniemożliwiać inspektorowi niezależną ocenę, czy obowiązki administratora są wykonywane i czy są wykonywane prawidłowo.

Warto nadmienić, że zgodnie z art. 83 ust 4 lit a RODO za naruszenie art. 38 ust. 6 RODO, tj. nałożenie na IOD zadania powodującego konflikt interesów, organ nadzorczy może nałożyć na administratora karę pieniężną. Karą administracyjną obwarowano zatem obowiązki administratorów dotyczące nie tylko wyznaczania inspektora ochrony danych, posiadania przez niego właściwych kwalifikacji i gwarancji niezależności, ale też zapewnienia, aby wyznaczony inspektor mógł prawidłowo realizować swoje zadania".

[2] Źródło: https://uodo.gov.pl/pl/138/3519

Jak widać na bazie powyższego cytatu (jest to fragment korespondencji z jednym z naszych klientów, dlatego dokładnego źródła ani szczegółów podać nie mogę) PUODO postawił sprawę jasno. IOD nie powinien być pełnomocnikiem. I o ile jestem w stanie zrozumieć to w kontekście zgłaszania naruszeń (IOD jest związany pełnomocnictwem, a zatem nie bardzo może wyjść poza to co w nim zostało wskazane, więc można to uznać za naruszenie jego niezależności albo konflikt interesów), o tyle tak prosta czynność (właściwie można ją określić jako „techniczną") jak zgłoszenie wyznaczenia IOD budzi już pewne wątpliwości, czy aby takie stanowisko nie jest zbyt daleko idące, żeby nie powiedzieć restrykcyjne.

Rola IOD przy naruszeniach ochrony danych

Obecnie jesteśmy w tej komfortowej sytuacji, że PUODO dość jasno wyartykułowało swoje stanowisko w zaktualizowanym poradniku dotyczącym naruszeń (jego publikacja nastąpiła 20 lutego 2025 r.). Jego lektura pozwala wymienić te obszary, które zdaniem organu nadzorczego, mogą zagrażać niezależności IOD oraz powodować konflikt interesów. Są to:

- zgłaszanie naruszeń ochrony danych w imieniu administratora danych,
- zawiadamianie w imieniu administratora danych osób, których dane objęte zostały naruszeniem,
- dokumentowanie naruszeń,
- podejmowanie zobowiązań odnoszących się do bezpieczeństwa przetwarzania danych w imieniu administratorów danych lub podmiotów przetwarzających,
- działania na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych.

W przestrzeni pojawiły się już różne głosy, ale chyba nie było takich, które by w 100% zgadzały się z prezentowanym wyżej podejściem[3].
Nie wchodzący w szczegóły, zastanówmy się przez chwilę, czy rzeczywiście dokumentowanie naruszeń może powodować ryzyko dla niezależności IOD czy też generować sytuację, która sprawi, że dojdzie tu do konfliktu interesów. Otóż nawet sam wyżej wskazany poradnik UODO wskazuje, że IOD musi otrzymać informację o tym, że doszło do naruszenia. Nawet, żeby tym jakoś sprawnie zarządzać, tak by mógł realizować wpisane do RODO zadanie mówiące o tym, że jego obowiązkiem jest „monitorowanie przestrzegania niniejszego rozporządzenia (tj. RODO), 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" niezbędnym wydaje się prowadzenie dokumentacji takiego naruszenia, czy też jego rejestrowanie. Pytanie zatem, czy tego typu czynności mogłyby zostać zakwestionowane przez PUODO.

Podsumowanie

Niestety ciężko pokusić się o jakąś sensowną puentę dla wywodu zawartego w tym artykule, ponieważ na naszych oczach dochodzi do sporej zmiany podejścia PUODO do kwestii związanych z funkcjonowaniem inspektorów ochrony danych. Na razie wszystko wskazuje na to, że organ nadzorczy idzie w kierunku IOD – doradcy, który w zasadzie ma przede wszystkim być… No

[3] Zobacz np.: https://www.prawo.pl/biznes/iod-a-naruszenie-danych-osobowych-uodo-zmienia-stanowisko,531724.html

właśnie, głosem doradczym dla administratora danych. Tylko czy administratorzy danych rzeczywiście potrzebują takiego IOD, zwłaszcza w sytuacji, gdy nie są zobligowani do jego powołania? Moim zdaniem nie i pójdzie to raczej w tym kierunku, że tam, gdzie IOD jest fakultatywny, dojdzie do zmian na poziomie nomenklatury związanej z nazwą stanowiska. IOD przestanie być już IOD, a stanie się doradcą ds. ochrony danych osobowych albo po prostu specjalistą / pełnomocnikiem ds. ochrony danych.
Czyli mówiąc nieco żartobliwie (podziękowania dla Pawła Wojciechowskiego!) - do tej pory IOD był widywanym przez wszystkich supermanem, teraz będzie nim nadal, ale już nie jako superman tylko jako Clark Kent dla niepoznaki zakładający okulary, ale nadal dysponujący tą samą mocą. Innymi słowy inspektora nie będzie, bo to oznacza niepotrzebne ryzyko, ale ktoś i tak przecież musi pomóc administratorowi danych przy wdrażaniu obowiązków wynikających z RODO.

Michał Sztąberek – ekspert ds. ochrony danych osobowych, CEO w iSecure Sp. z o.o.