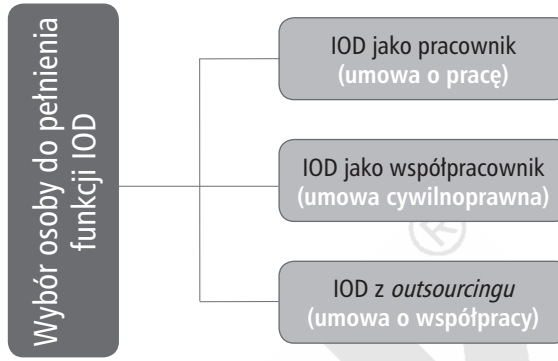
Rozdział 5.
Wybór IOD – pracownik, freelancer, outsourcing

Założenie przewidujące, że nadzór nad wszystkimi procesami przetwarzania danych osobowych w całej organizacji (w przypadku średnich i dużych organizacji) ma pełnić jedna osoba, wydaje się wyjątkowo nietrafione. Jednak właśnie w taki sposób ustawodawca postanowił ukształtować funkcję IOD.

Niezależnie od liczby procesów i osób w nie zaangażowanych odpowiedzialność za ich zgodność z regulacjami prawnymi ponosi zawsze jedna osoba. Warto zaznaczyć, że ponoszenie odpowiedzialności za konkretny proces wcale nie oznacza jego osobistego wykonania. Innymi słowy, nie ma żadnych ograniczeń, by poszczególne czynności w ramach pełnienia nadzoru nad przetwarzaniem danych osobowych wykonywały inne osoby. Tu pojawia się furtka, która pozwala na tworzenie całych komórek organizacyjnych, których celem jest szeroko rozumiany *compliance*, czyli badanie zgodności konkretnych procesów z normami wewnętrznymi lub powszechnie obowiązującymi. Jednak ważne jest, aby w ramach bardziej złożonej struktury organizacyjnej nadzoru nie dochodziło do wspomnianego wcześniej konfliktu interesów, tj. weryfikacji podmiotu audytowanego przez ten sam podmiot przeprowadzający audyt. Zarówno w przypadku średnich, jak i dużych organizacji warto, już na etapie samego wyboru osoby na funkcję IOD, rozważyć stworzenie bardziej złożonej struktury nadzoru.

Kolejnym pytaniem, z którym należy się zmierzyć, jest wybór formy współpracy z IOD. Przepisy prawa dopuszczają praktycznie każdą formę współpracy, choć zastrzeżenia może budzić forma wolontariatu w przypadku pełnienia funkcji IOD (ze względu na brak środków utrzymania przez samego IOD). Najczęściej występującą formą współpracy z IOD jest umowa o pracę. Kolejno niemal równorzędnie występują umowy cywilnoprawne i tzw. outsourcing funkcji IOD, czyli zapew-

nienie IOD z firmy zewnętrznej, profesjonalnie zajmującej się ochroną danych osobowych i bezpieczeństwem informacji.



Rys. 9. Opcje wyboru modelu współpracy z IOD
Źródło: oprac. autora.

Warto zaznaczyć, że nie ma żadnych ograniczeń prawnych co do wybranego modelu współpracy z IOD. Przepisy pozostawiają tę decyzję do dyspozycji administratora danych. Bardzo często najwyższe kierownictwo w organizacji nie jest świadome możliwości, jakie są dopuszczalne, dlatego dobrym pomysłem jest zapoznanie najwyższego kierownictwa ze specyfiką wybranego modelu, tak aby decyzja o jego wyborze nie była przypadkowa, lecz przemyślana i przede wszystkim możliwa do zastosowania w praktyce.

IOD jako pracownik administratora danych

Sytuacja, w której IOD jest pracownikiem administratora danych, jest najczęściej wybieraną opcją ze względu na najniższe (pozornie!) koszty jej wyboru. Zwykle administrator danych wychodzi bowiem z założenia, że skoro przepisy na to pozwalają, wystarczy rozszerzyć zakres obowiązków pracownika (kadr, IT lub administracji) o obowiązki IOD, i sądzi, że problem jest rozwiązany. Zapomina jednak, że w wyniku pobieżnej analizy powołał IOD, który ze względu na obowiązki pracownicze ani nie ma wystarczająco dużo czasu, ani nie dysponuje właściwą wiedzą czy doświadczeniem, by pełnić taką funkcję. Na ogół kolejnym krokiem administratora jest więc skierowanie pracownika na specjali-

styczne szkolenie w zakresie pełnienia funkcji IOD, w celu uzupełnienia braków. Na szkoleniu pracownik przydzielony do pełnienia funkcji IOD poznaje od strony praktycznej, na czym ma polegać jego nowa funkcja. Łatwo orientuje się, że nie będzie w stanie realizować dotychczasowych obowiązków pracowniczych, gdyż zakres zadań IOD jest zbyt szeroki. Ale dla administratora danych jest to często moment, gdy w wyborze modelu współpracy zabrnął już dość daleko (np. poniósł koszty szkolenia swojego IOD, przyznał dodatek funkcyjny wybranemu pracownikowi itp.). W takiej sytuacji administrator może uznać, że zmiana wybranego modelu będzie się wiązała ze zbyt dużymi kosztami i w rezultacie niczego już nie zmieni.

Opisany scenariusz pozwala dostrzec, gdzie tkwi przyczyna nawarstwiających się problemów, prowadzących do wielu frustracji, które stają się udziałem przede wszystkim osoby pełniącej funkcję IOD. Mnóstwo obowiązków i brak czasu na ich realizację to konsekwencja błędnego podejścia do pełnienia nadzoru przez IOD już na samym początku pełnienia tej funkcji. W rezultacie pracownik stanie przed niełatwym wyborem pomiędzy obowiązkami, które przynoszą realnie wysokie wynagrodzenie, a unikaniem odpowiedzialności z tytułu pełnienia funkcji IOD. Mówiąc wprost, przeciążony pracownik pełniący dodatkową funkcję IOD będzie dbał głównie o to, by jego obowiązki były spełnione *stricte* od strony formalnej, ale nie przeprowadzi już z właściwym zaangażowaniem poszczególnych czynności, aby osiągnąć zamierzony efekt, jakim jest zgodność przetwarzania danych osobowych w organizacji, bo siłą rzeczy nie będzie miał na to czasu.

Aby uniknąć powyższego scenariusza, przy wyborze modelu IOD jako pracownika należałoby od razu założyć, że będzie to kolejny etat, to znaczy, że wybrana osoba będzie przede wszystkim IOD, a dopiero w kolejnym kroku można dodawać jej inne obowiązki pracownicze. Powyższy stan rzeczy powoduje, że pracownik zawsze w pierwszej kolejności będzie IOD, co jest niezbędnym założeniem, jeżeli organizacja wybiera model ochrony danych osobowych z IOD (lub musi powołać IOD). Jeżeli administrator danych uważa, że w jego organizacji zakres zadań IOD jest zbyt wąski, aby poświęcić mu cały etat, to powinien

rozważyć wybór modelu systemu ochrony danych osobowych bez IOD (jeżeli przepisy mu na to pozwalają).

Powołując IOD jako pracownika, warto pamiętać o tym, że podstawa prawna współpracy, jaką w tym przypadku będzie umowa o pracę, nie zawsze jest podstawą prawną pełnienia funkcji IOD. IOD musi zostać powołany do pełnienia funkcji i może to się stać w treści umowy o pracę, jednak jeżeli tak nie jest, a IOD zostaje powołany na przykład uchwałą zarządu lub treścią wewnętrznej dokumentacji ochrony danych osobowych, to rozwiązanie umowy o pracę nie spowoduje zaprzestania pełnienia przez tę osobę funkcji IOD. Warto pamiętać, że prawo pracy nie reguluje wprost funkcji IOD, czyni to natomiast RODO i ustawa o ochronie danych osobowych. Podobnie jak w sytuacji upoważnień do przetwarzania danych osobowych, które należy odebrać w przypadku zakończenia stosunku pracy, chyba że ich wygaśnięcie wynika wprost z ich treści, tak samo należy odwołać IOD z pełnionej funkcji w przypadku jego zwolnienia z pracy.

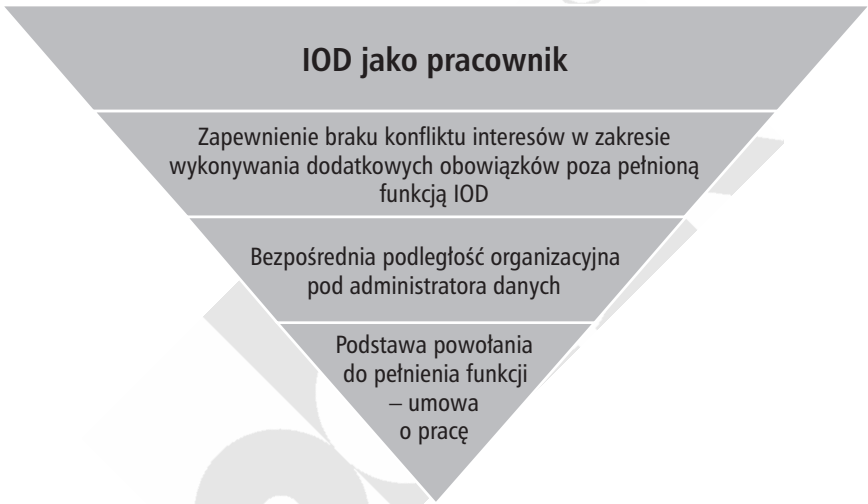
Kolejnym aspektem, który należy wziąć pod uwagę, jest usytuowanie IOD w strukturze organizacyjnej. Pełnić funkcji IOD nie może na przykład członek zarządu organizacji, a to ze względu na ewidentny konflikt interesów, gdyż osoba występująca w imieniu administratora danych (lub w niektórych sytuacjach mogąca występować, na przykład, gdy pełni funkcję wiceprezesa zarządu) nie może pełnić funkcji IOD[41]. W powyższej kwestii głos również zabrała Grupa robocza art. 29 ds. ochrony danych osobowych.

> „Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. I choć DPO mogą posiadać inne zadania i obowiązki, to jednak te nie mogą powodować konfliktu interesów. Oznacza to, że DPO nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych.
>
> Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu. Co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu

[41] Zob. http://www.giodo.gov.pl/1520228/id_art/8527/j/pl/ (dostęp: 28.12.2016 r.).

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, gdy zewnętrzny DPO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych"[42].

W związku z powyższym w strukturze organizacyjnej IOD podlega bezpośrednio pod administratora danych, czyli w praktyce pod osoby występujące w imieniu administratora danych, np. prezesa zarządu spółki kapitałowej lub wójta w gminie.



Rys. 10. Najważniejsze zagadnienia powołania IOD jako pracownika
Źródło: oprac. autora.

Na samym końcu warto zwrócić uwagę na rzeczywiste koszty zatrudnienia specjalisty, który ma pełnić funkcję IOD. Jak pokazują statystyki, jest to średnio kwota ok. 8000 zł brutto[43] (należy brać pod uwagę region, wielkość oraz branżę administratora danych).

[42] Zob. https://uodo.gov.pl/data/filemanager_pl/15.pdf (dostęp: 11.06.2018 r.).
[43] Zob. http://wynagrodzenia.pl/moja-placa/ile-zarabia-specjalista-ds-bezpieczenstwa-informatycznego (dostęp: 24.06.2018 r.).