Inspektor to pomoc, a nie kozioł ofiarny

Zgodnie z RODO nie każdy musi wyznaczyć inspektora ochrony danych osobowych (dalej: IODO). 25 maja 2018 r. wielu przedsiębiorców posiadało w swojej strukturze osoby odpowiedzialne za bezpieczeństwo danych, powołane zgodnie z poprzednimi przepisami (ABI), które po tej dacie automatycznie zamieniły się w IODO. Znaczna grupa firm postanowiła wyznaczyć IODO fakultatywnie. W korporacjach i większych organizacjach wsparcia dla inspektora dostarcza najczęściej rozbudowana struktura dedykowana zapewnieniu ochrony danych osobowych.

Do dzisiaj rola IODO dla wielu przedsiębiorców nie jest jednak w pełni zrozumiała. Powoduje to wiele problemów związanych z jego funkcjonowaniem.

Doradca i sygnalista

IODO jest wsparciem dla administratora lub podmiotu przetwarzającego w utrzymaniu i aktualizacji przyjętych przez niego zasad ochrony danych osobowych. Jest on bowiem bardziej doradcą i sygnalistą niż twórcą zasad czy ich egzekutorem. Jego rola sprowadza się przede wszystkim do przekazywania informacji o obowiązkach wynikających z przepisów i weryfikowania, czy stosowane w firmie zasady ochrony danych ich nie naruszają. Pełni również rolę „skrzynki kontaktowej" dla osób, których dane są przetwarzane, lub dla UODO.

Skoro zatem IODO ma za zadanie kontrolować obowiązujące polityki czy procedury, zasadniczo nie powinien ich tworzyć. Nie ponosi on odpowiedzialności za ich wdrożenie, ponieważ jego rola sprowadza się tylko i wyłącznie do poinformowania o nieprawidłowościach kierownictwa, które powinno wymusić na strukturze adekwatne zachowanie.

Wiele firm w dalszym ciągu mylnie zakłada, że IODO zdejmie z kierownictwa całą odpowiedzialność za RODO. Tymczasem trzeba mieć świadomość, że odpowiedzialność spoczywa na administratorze, czyli de facto na zarządzie.

Własne struktury…

Za ochronę danych osobowych na końcu zawsze odpowiada kierownictwo firmy. To na nim ciąży decyzja, czy rolę IODO ma pełnić pracownik firmy, czy zadania te oddelegować na zewnątrz. Każde z tych rozwiązań ma swoje plusy i minusy.

Niewątpliwym plusem "wewnętrznego" inspektora jest dobra znajomość specyfiki firmy i procesów, które mogą wykorzystywać dane osobowe. Jeżeli jednak IODO nie ma do pomocy dodatkowych osób, które wesprą go przy wykonywaniu obowiązków, może się okazać, że system ochrony danych osobowych będzie działał nieprawidłowo. Jednym z powodów może być nieobecność IODO (urlop, choroba), w trakcie której może dojść do naruszenia przepisów RODO, ponieważ administrator nie wykona swoich obowiązków.

… nie zawsze wystarczą

W przypadku wyznaczenia wewnętrznego IODO, podstawowym problemem jest możliwy brak bezstronności. RODO wymaga, aby IODO mógł działać w strukturze organizacyjnej

niezależnie. Oznacza to, że nie powinien łączyć z pełnieniem swojej funkcji zadań związanych z bieżącym przetwarzaniem danych osobowych czy też podlegać organizacyjnie szefowi działu, którego miałby kontrolować. Inspektorem nie może być np. kierownik działu IT odpowiedzialny za zabezpieczenia teleinformatyczne. Dodatkowo inspektor posiada dostęp do wielu – często poufnych – informacji na temat funkcjonowania przedsiębiorstwa. Ta wiedza może negatywnie wpływać na pełnienie innych funkcji.

Obowiązek powołania IODO nie zależy od wielkości przedsiębiorstwa, lecz od procesów, jakie wiążą się z przetwarzaniem danych osobowych. Firma, która zatrudnia 10 pracowników, ale przetwarza dane szczególnej kategorii na dużą skalę, również może być zobowiązana do wyznaczenia IODO – tak samo, jak wielkie korporacje zatrudniające kilka tysięcy pracowników. W tak małej organizacji znalezienie kompetentnej osoby, która byłaby wystarczająco niezależna w strukturze organizacyjnej, może być problemem. Rozwiązaniem może być nowa osoba w zespole, ale z uwagi na znaczne zapotrzebowanie na specjalistów z zakresu ochrony danych osobowych i ich brak na rynku pracy, proces poszukiwań bywa długotrwały. Dlatego często atrakcyjnym rozwiązaniem okazuje się outsourcing.

Konkretna osoba

Z uwagi na swoje zadania, IODO musi posiadać odpowiednią wiedzę oraz kompetencje w zakresie przepisów dotyczących ochrony danych osobowych. W naturalny sposób prowadzi to do wniosku, że IODO powinien być prawnikiem. Nie zawsze musi to oznaczać status adwokata czy radcy prawnego – na rynku funkcjonuje wiele osób posiadających odpowiednie certyfikaty potwierdzające ich kompetencje w zakresie audytu czy też organizacji określonych procesów bezpieczeństwa. Niemniej jednak współpraca z osobą posiadającą odpowiedni tytuł zawodowy na pewno uprości proces oceny kompetencji w zakresie znajomości prawa.

Inspektorem zawsze jest konkretna osoba, na co jasno wskazuje zakres formularzy UODO dedykowanych do zgłoszenia IODO. Przy zleceniu działań IODO firma zewnętrzna powinna zatem ustalić, jaka osoba zostanie formalnie wpisana we wniosku do UODO – odpowiedzialność za prawidłowość realizacji zadań spoczywa nie tylko na podwykonawcy, ale również na osobie, która pełni tę funkcję.

Współpraca z firmą zewnętrzną może polegać na przekazaniu jej w całości obowiązków IODO lub zamówieniu wsparcia dla wewnętrznego inspektora. Pierwszy model pozwala w całości delegować pracę, ale może oznaczać większe koszty. Dlatego firmy często wybierają model mieszany, który pozwala znaleźć złoty środek między zapewnieniem odpowiedniego poziomu merytorycznego a dostępnością inspektora w firmie i jego znajomością specyfiki prowadzonej działalności. Korzystanie z zewnętrznych doradców pozwala na optymalizację kosztów, bo bieżącymi kwestiami z zakresu ochrony danych osobowych będzie zajmować się pracownik na miejscu, natomiast zespół wykwalifikowanych specjalistów zewnętrznych przejmie tylko wybrane, bardziej skomplikowane kwestie. Tacy doradcy są w szczególności pożądani – z uwagi na ich bezstronność – w przypadku przeprowadzania okresowych audytów bezpieczeństwa danych osobowych.

Miejsce w strukturach

Podstawową kwestią – bez względu na model funkcjonowania IODO – jest właściwe określenie miejsca inspektora w strukturze firmy (bezpośrednia podległość pod zarząd) oraz wskazanie zakresu prac, jakie ma wykonywać. W przypadku IODO spoza firmy te kwestie powinny zostać precyzyjnie określone w zawartej z nim umowie, w której jasno ustalone zostaną takie aspekty, jak zachowanie poufności oraz konsekwencje w przypadku niewykonania obowiązków (np. odpowiednio sformułowane kary umowne).

Pracownik, który pełni taką funkcję, powinien być dedykowany tylko i wyłącznie do ochrony danych osobowych. Kluczowe jest także ustalenie właściwych procedur związanych nie tylko z bieżącą pracą IODO, ale również jego powołaniem czy odwołaniem, w celu zapewnienia ciągłości realizacji jego zadań.

Warto przewidzieć zastępstwo

W firmach, które przetwarzają większe ilości danych, istotną kwestią jest wyznaczenie ewentualnego zastępcy IODO lub zbudowanie zespołu specjalistów z odpowiednim podziałem kompetencji. Obowiązek wyznaczenia IODO wynikający z RODO sprowadza się nie tylko do znalezienia kompetentnej osoby i obrania właściwego modelu współpracy, ale również precyzyjnego dostosowania jego zadań do potrzeb administratora czy podmiotu przetwarzającego.

Autorzy:

Monika Bogdał, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.

Anna Hoffmann, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.