IODO: kompetencje nie wystarczą

W interesie kadry menadżerskiej jest prawidłowe określenie zakresu obowiązków Inspektora Ochrony Danych Osobowych i zapewnienie mu niezależności. To ona bowiem ostatecznie odpowiada za naruszenia RODO w firmie.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) obowiązuje w Polsce już od kilku miesięcy. W dalszym ciągu wzbudza jednak wiele niejasności, a nawet kontrowersji. Pomimo upływu znacznej ilości czasu od wejścia w życie przepisów Rozporządzenia, wiele krajowych przepisów wciąż nie jest dostosowanych do RODO. Stwarza to problemy w zakresie właściwej interpretacji przepisów.

W związku z wejściem w życie RODO, przedsiębiorcy często są zobowiązani do dosyć trudnej i czasochłonnej zmiany sposobu organizacji funkcjonowania firmy, nie tylko w zakresie relacji z kontrahentami, ale też z pracownikami. Konieczne jest zarówno opracowanie nowych procedur i wykonanie analizy ryzyka w zakresie bezpieczeństwa danych osobowych, jak również stałe monitorowanie procesów dotyczących danych osobowych. Z tego względu powołanie w strukturze organizacji osoby, która będzie odpowiedzialna za weryfikację obowiązujących procesów, jest z reguły niezbędne (a czasem nawet obowiązkowe), aby zapewnić funkcjonowanie firmy w zgodzie z RODO.

Obowiązek powołania

RODO określa przypadki, kiedy obligatoryjne jest powołanie Inspektora Ochrony Danych Osobowych (IODO). 25 maja 2018 r., tj. w dniu wejścia w życie RODO, każdy przedsiębiorca powinien już znać odpowiedź na pytanie – czy w związku z prowadzoną przez niego działalnością gospodarczą ma obowiązek powołać inspektora na gruncie RODO? Jednak wielu przedsiębiorców nie pochyliło się nad tym tematem do chwili obecnej.

Obowiązek powołania IODO mają przedsiębiorcy, których:

1. główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane w dużej mierze dotyczą, lub
2. główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (tzw. danych wrażliwych) lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych,

- przy czym dotyczy to sytuacji, gdy przedsiębiorca w procesie przetwarzania danych osobowych będzie pełnił funkcję administratora lub procesora.

Niejasne pojęcia

Mimo wskazania w RODO przesłanek, kiedy konieczne jest wyznaczenie IODO, wielu przedsiębiorców wciąż nie wie, czy ciąży na nich ten obowiązek. Brak wyjaśnienia przez

unijnego ustawodawcę takich pojęć jak „regularne czy systematyczne monitorowanie" lub przetwarzanie „na dużą skalę" powoduje, że przedsiębiorcy nadal borykają się z udzieleniem prawidłowej odpowiedzi na pytanie – czy moja firma musi powołać IODO? Pomocne w udzieleniu prawidłowej odpowiedzi na to pytanie mogą się okazać wytyczne dotyczące inspektorów ochrony danych (DPO) wydane przez Grupę Roboczą Art. 29 ds. Ochrony danych (WP 243). Obowiązek powołania takiego inspektora mają m.in.:
- wszystkie podmioty świadczące usługi ochrony mienia, które monitorują przestrzeń publiczną (głównym celem działalności jest ochrona, jednak przetwarzanie danych osobowych – wizerunku – na nagraniach z monitoringu jest bezpośrednio związane z prowadzoną działalnością),
- szpitale, które nie mogą realizować świadczeń medycznych bez przetwarzania danych pacjenta,
- firmy marketingowe, które zajmują się obsługą call center.

Obowiązek powołania IODO mają również organy lub podmioty publiczne. Bez znaczenia pozostaje przy tym wielkość organu, cel przetwarzania danych czy realizowane zadania.

Informacja do urzędu

Samo wyznaczenie inspektora nie wystarczy, aby mógł on skutecznie działać. Polska ustawa o ochronie danych osobowych z 10 maja 2018 r. określa procedurę powołania IODO w strukturze organizacji oraz sposób zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora. Aby skutecznie powołać IODO, przedsiębiorca powinien:

1) powołać inspektora w strukturze wewnętrznej organizacji (np. uchwałą zarządu),
2) zawrzeć umowę o współpracy z IODO (lub umowę o pracę), w której określone zostaną w sposób szczegółowy obowiązki inspektora,
3) w terminie 14 dni od wyznaczenia inspektora zawiadomić o tym Prezesa Urzędu Ochrony Danych Osobowych przy użyciu dedykowanych formularzy udostępnionych przez urząd. Zawiadomienie sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Podmiot powinien umieścić informację o wyznaczeniu IODO na swojej stronie internetowej. Musi też wywiązać się z obowiązków informacyjnych dotyczących przetwarzania danych osobowych – np. przekazując informację pracownikom lub kontrahentom.
Jeżeli przedsiębiorca nie prowadzi strony internetowej, informację o wyznaczeniu IODO powinien umieścić w widoczny sposób w miejscu prowadzonej działalności, np. na tablicy informacyjnej.

Jeden inspektor w całej grupie

Znacznym ułatwieniem dla przedsiębiorców działających w szczególności w ramach grup kapitałowych jest możliwość powołania jednego, wspólnego Inspektora Ochrony Danych Osobowych dla wszystkich spółek funkcjonujących w ramach tej grupy.

W przypadku gdy grupa podmiotów – np. spółki wchodzące w skład grupy kapitałowej – chce wspólnie zgłosić IODO, każda z tych spółek musi odrębnie dokonać zgłoszenia inspektora w UODO.

Kto odpowie, gdy nie ma IODO

Jeżeli kadra kierownicza stwierdzi, że podmiot nie ma obowiązku powołania inspektora na podstawie przesłanek wskazanych w RODO, możliwe jest:

1) fakultatywne powołanie IODO i zgłoszenie go do PUODO (tak jak w przypadku, gdyby powołanie inspektora jest obligatoryjne), lub
2) powołanie w strukturze firmy osoby odpowiedzialnej (np. pełnomocnika ds. ochrony danych) za monitorowanie kwestii dotyczących ochrony danych osobowych (bez zgłoszenia jej do PUODO), albo
3) niewyznaczanie w strukturze firmy osoby odpowiedzialnej za ochronę danych osobowych w firmie.

Bez wątpienia warto w ramach wypracowywania dobrej praktyki i prowadzenia działalności w zgodzie z przepisami powołać IODO (pkt 1) lub osobę odpowiedzialną za kwestię zapewnienia zgodności działalności firmy z przepisami o ochronie danych osobowych (pkt 2). Argumentem przemawiającym za wyznaczeniem takiej osoby jest pozytywny wpływ, jaki będzie ona miała na procesy związane z ochroną danych osobowych w organizacji, w szczególności w zakresie poprawy świadomości pracowników w tym temacie. Kolejną pozytywną przesłanką jest fakt, że taka osoba odciąży kadrę kierowniczą od zajmowania się kwestiami dotyczącymi ochrony danych osobowych.

Nadzór i doradztwo

Przepisy Rozporządzenia wprost określają, że IODO zobowiązany jest do:

1. monitorowania prawidłowości przestrzegania RODO i przepisów o ochronie danych osobowych przez przedsiębiorcę,
2. właściwej identyfikacji procesów przetwarzania, jakimi są: zbieranie informacji w celu konkretnego rozpoznania poszczególnych czynności związanych z przetwarzaniem danych osobowych oraz analizowanie i sprawdzanie zgodności tego przetwarzania z prawem (rozstrzyganie, czy czynności związane z przetwarzaniem danych osobowych są zgodne z obowiązującymi przepisami),
3. informowania, doradzania i rekomendowania określonych działań, współpracy z organem nadzorczym i pełnienia punktu kontaktowego.

Oczywiście to od przedsiębiorcy zależy, jakie obowiązki będzie posiadała osoba odpowiedzialna za kwestie zapewnienia działania przedsiębiorstwa zgodnie z przepisami o ochronie danych osobowych. W ramach kompetencji może być ona zobowiązana do przeprowadzania okresowych audytów w celu weryfikacji zgodności z RODO, weryfikacji poprawności działalności systemów IT z RODO, tworzenia i aktualizowania dokumentacji zgodnej z RODO, w tym prowadzenia rejestrów.

Funkcja nie dla każdego

Przedsiębiorca nie może wyznaczyć na IODO dowolnej osoby. Osoba pełniąca tę funkcję powinna:

1) dysponować odpowiednią wiedzą na temat prawa i praktyk w dziedzinie ochrony danych oraz posiadać odpowiednie kwalifikacje zawodowe; przy czym do odpowiednich umiejętności i wiedzy zgodnie z wytycznymi Grupy Roboczej Art. 29 ds. ochrony danych osobowych zalicza się wiedzę na temat krajowych i europejskich przepisów i praktyk w zakresie ochrony danych osobowych, w tym dogłębnego rozumienia RODO. Zrozumienie przeprowadzonych procesów przetwarzania, zrozumienie technologii informacyjnych i bezpieczeństwa danych, znajomość sektora biznesowego i organizacji (odpowiednia znajomość do sektora działalności, w której funkcjonuje dany podmiot na rynku),
2) posiadać możliwość wykonywania zadań poprzez zapewnienie odpowiedniej pozycji w strukturach podmiotu (niezależność IODO),
3) być dostępna i zlokalizowana na terenie UE (zgodnie z wytycznymi Grupy Roboczej art. 29 w tym zakresie).

Funkcję IODO może pełnić zarówno podmiot zewnętrzny, jak i pracownik lub współpracownik przedsiębiorcy. Konieczne jest jednak zapewnienie jego niezależności i odpowiednie ułożenie relacji z kadrą kierowniczą.

Relacje z kadrą kierowniczą

Określenie sposobu, w jaki należy prawidłowo ułożyć relacje kadry kierowniczej z IODO, jest niezwykle trudnym zadaniem. Należy wziąć pod uwagę fakt, że inspektor będzie posiadał dostęp do wielu – często poufnych – informacji na temat funkcjonowania przedsiębiorstwa, a jednocześnie będzie zobowiązany do zapewnienia bezpieczeństwa tych informacji (i danych osobowych). Ponadto musi on być niezależny w strukturze, a żadne organy nie powinny negatywnie wpływać na wykonywaną przez niego pracę.
Właściwe ułożenie relacji kadry kierowniczej z IODO (lub osobą, która zajmie się kwestiami ochrony danych osobowych) dotyczy następujących kwestii:

1) zapewnienia IODO udziału we wszystkich zagadnieniach związanych z ochroną danych osobowych w firmie, np. udziału w spotkaniach, uczestnictwa w podejmowaniu kluczowych decyzji czy umożliwienie zajęcia stanowiska w kwestii danych osobowych,
2) umożliwienia IODO dostępu do niezbędnych informacji, np. o funkcjonowaniu poszczególnych działów,
3) zapewnienie możliwości ciągłego szkolenia,
4) dokumentowania przypadków i powodów postąpienia niezgodnie z zaleceniem IODO,
5) zapewnienia IODO odpowiedniego wsparcia technicznego czy organizacyjnego, np. wsparcia dodatkowych osób w strukturze organizacji ze względu np. na rozległość procesów przetwarzania danych osobowych. Nie ma przeszkód, aby w takim przypadku przedsiębiorca powołał dedykowany zespół, który pod kierownictwem IODO będzie się zajmował kwestią ochrony danych osobowych w firmie.

Niezwykle istotną kwestią jest zagwarantowanie IODO niezależności w działaniach. Chodzi w szczególności o niezależność od instrukcji organów zarządzających

dotyczących sposobu wykonywania zadań przez inspektora czy brak możliwości wpływania przez inne podmioty (np. pracowników) na podejmowane czynności. Oznacza to brak możliwości instruowania IODO przez organy zarządzające w zakresie wypełniania ciążących na nim obowiązków.
Innym fundamentalnym zagadnieniem jest ułożenie relacji pozbawionej konfliktu interesów. Chodzi w głównej mierze o to, żeby IODO nie mógł jednocześnie sprawować własnej funkcji oraz łączyć z nią stanowiska, w którym sam ma wpływ na sprawowaną funkcję inspektora. Przykładowo, funkcji IODO nie powinien sprawować specjalista ds. IT odpowiedzialny za bezpieczeństwo informatyczne w firmie, gdyż podmiot ten nie będzie miał możliwości sam siebie kontrolować.

Samo wyznaczenie IODO i wykonywanie przez niego opisanych działań nie zwalnia organów zarządzających z odpowiedzialności za naruszenie przepisów RODO. Oznacza to, że zarówno w przypadku, gdy wyznaczenie inspektora jest obligatoryjne, jak i wtedy, gdy podmiot wyznaczył go dobrowolnie, za wszelkie ewentualne nieprawidłowości związane z przetwarzaniem danych osobowych odpowiada administrator. Oczywiście w umowie pomiędzy administratorem a tym podmiotem można określić kwestię odpowiedzialności inspektora.

Autorzy:
Anna Hoffmann, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy
Michał Dutkiewicz, prawnik, Kancelaria Prawna Piszcz i Wspólnicy