Jakie są zadania Inspektora Ochrony Danych w organizacji?

Status i rola IOD nie są w RODO określone sztywno. Taka ogólność i brak szczegółowych wytycznych generują wiele pytań i wątpliwości. W swoim artykule chciałbym udzielić Ci odpowiedzi na najczęściej zadawane pytania związane z funkcją Inspektora Ochrony Danych.

Wskazówki dla siebie znajdą również przedstawiciele administratora danych, którzy współpracują z IOD. Aby relacja IOD – ADO funkcjonowała dobrze, wymaga szczerości, otwartości i precyzyjnego wyznaczenia granic.

Zapraszam do lektury artykułu opartego na doświadczeniach moich oraz zespołu Lex Artist w zakresie wykonywania funkcji Administratora Bezpieczeństwa Informacji, a następnie Inspektora Ochrony Danych.

Pamiętaj, że na naszym blogu znajdziesz również inne artykuły poświęcone funkcji IOD:

- Jak poprawnie zawiadomić Prezesa UODO o wyznaczeniu IDO?
- Lista lektur prawniczych Inspektora Ochrony Danych.

A to jeszcze nie wszystko! W naszych kolejnych tekstach zajmiemy się innymi ważnymi elementami związanymi z funkcją IOD, takimi jak:

- niezależność i konflikty interesów w pracy IOD – jak ich uniknąć,
- wynagrodzenie IOD, czyli jak IOD rozlicza swoją pracę,
- odpowiedzialność IOD, czyli za co IOD może odpowiadać.

IOD następcą Administratora Bezpieczeństwa Informacji?

Instytucja Inspektora Ochrony Danych, wywodzi się z ustawodawstwa niemieckiego i została uwzględniona przez prawodawcę europejskiego już w Dyrektywie 95/46/WE z 1995 r.

Regulacja zawarta w art. 18 tej Dyrektywy miała jednak charakter szczątkowy, wiążąc tę funkcję z możliwością wprowadzenia zwolnień z obowiązku zgłoszenia organom nadzorczym operacji przetwarzania danych osobowych. Administrator danych mógł zostać zwolniony z obowiązku zawiadamiania, jeżeli powołał **urzędnika do spraw ochrony danych osobowych**, który był odpowiedzialny, w szczególności za:

- zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy Dyrektywy,
- prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających określone Dyrektywą informacje.

W Polsce, takim urzędnikiem był Administrator Bezpieczeństwa Informacji, który oficjalnie w polskim porządku prawnym pojawił się dopiero w 2004 r., tj. po nowelizacji Ustawy o ochronie danych osobowych z 1997 r. Zgodnie z ówczesnym brzmieniem art. 36 ust. 3 tej Ustawy, administrator danych osobowych wyznaczał ABI nadzorującego przestrzeganie zasad ochrony danych osobowych, chyba, że sam wykonywał te czynności.

Jeśli więc ktoś narzeka na to, że RODO nie reguluje funkcji IOD zbyt precyzyjnie, niech spojrzy na pierwsze europejskie i polskie regulacje w tym zakresie.

Z biegiem czasu, w różnych państwach Unii Europejskiej, zaczęły pojawiać się bardziej szczegółowe przepisy, mówiące o obowiązku lub dobrowolności wyznaczenia urzędnika do spraw ochrony danych osobowych, a także jego zadaniach. Pisaliśmy już o tym kiedyś na łamach naszego bloga.

W Polsce, prawdziwa rewolucja w wykonywaniu funkcji ABI miała miejsce w 2015 r., kiedy to nowelizacja ustawy o ochronie danych osobowych istotnie zmieniła model jego funkcjonowania.

Nowe przepisy wprowadziły dobrowolność powołania Administratora Bezpieczeństwa Informacji. Wskazały wymogi wobec osób pełniących tę funkcję i określiły ich usytuowanie w strukturze administratora danych. Wyczerpująco zdefiniowały zadania ABI, do których przede wszystkim należało zapewnienie przestrzegania przepisów o ochronie danych osobowych.

Takie zmiany, dały wówczas funkcjonującym ABI, a także administratorom danych, możliwość przygotowania się do nowych wymogów określonych przez RODO.

Poniższa tabela prezentuje ewolucję funkcji ABI w Polsce:

Okres:	**Historia instytucji ABI / IOD:**
1997 - 2004	Funkcja ABI w ogóle **nie istnieje** w polskim porządku prawnym, mimo obowiązywania ustawy o ochronie danych osobowych z 1997 r.
2004 - 2015	Wyznaczenie ABI jest **obowiązkowe**, chyba że przypisane mu czynności administrator danych realizuje samodzielnie.
2015 - 2018	Wyznaczenie ABI **nie jest obowiązkowe**, a w przypadku jego niepowołania, czynności wymienione w ustawie o ochronie danych osobowych z 1997 r. wykonuje administrator danych.
2018 – do teraz	Funkcja IOD jest **obowiązkowa dla niektórych administratorów** danych.

Tabela obrazuje postęp i dążenie do porządkowania tych kwestii. RODO w końcu dało czytelną i zdroworozsądkową odpowiedź w zakresie obowiązku powołania specjalnej osoby zajmującej się ochroną danych osobowych. Powołanie IOD jest obowiązkowe, ale tylko w niektórych sytuacjach.

Dzięki temu unikamy prawnego absurdu, polegającego na obowiązku wyznaczeniu IOD w zakładzie fryzjerskim czy niewielkiej restauracji.

W Polsce, IOD jest następcą Administratora Bezpieczeństwa Informacji. Poza samą ciągłością historyczną, osoby, które przed 25 maja 2018 r. pełniły funkcję ABI, automatycznie stały się Inspektorami Ochrony

Danych na okres od 25 maja 2018 r. do 31 sierpnia 2018 r. Po 1 września 2018 r. osoby te nadal pełniły funkcję IOD, o ile administrator danych zawiadomił o tym Prezesa UODO.

Oczywiście nie możemy powiedzieć, że IOD i ABI są tym samym. Diabeł tkwi w szczegółach, a o nich więcej w kolejnych akapitach tekstu.

Czy moja organizacja potrzebuje IOD?

Powołanie Inspektora Ochrony Danych **jest obowiązkowe dla wskazanych w RODO grup administratorów danych** (i podmiotów przetwarzających). IOD muszą wyznaczyć:

1. **Organy lub podmioty publiczne**, czyli jednostki sektora finansów publicznych, np. jednostki samorządu terytorialnego, uczelnie publiczne.
2. Przedsiębiorcy, których **główna działalność** polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają **regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę**, np. banki i firmy ubezpieczeniowe, firmy przetwarzające dane do celów reklamy behawioralnej przez wyszukiwarki, dostawcy usług telekomunikacyjnych lub internetowych.
3. Przedsiębiorcy, których **główna działalność** polega na przetwarzaniu na **dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i czynów zabronionych**, np. firmy świadczące usługi medyczne.

Przepisy zostały skonstruowane w taki sposób, aby IOD był obowiązkowy wszędzie tam, gdzie danych osobowych jest dużo i są one szczególnie chronione.

Oczywiście powyższy podział nie jest idealnie precyzyjny. Wciąż mogą pojawić się sytuacje graniczne. Pamiętaj również o tym, że czasami IOD powołać po prostu warto, nawet jeśli jego powołanie nie jest obowiązkowe.

Jeśli jesteś osobą reprezentującą ADO, wyznaczenie IOD możesz potraktować jako dodatkową przewagę konkurencyjną i korzyść marketingową.

Formalnie powołując na stanowisko IOD osobę, z którą współpracujesz w zakresie ochrony danych osobowych, podnosisz również jej status wśród innych współpracowników.

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Firma produkcyjna, która zatrudnia tysiące pracowników, nie będzie zobowiązana do powołania Inspektora Ochrony Danych. Nie jest bowiem podmiotem publicznym, a jej główna działalność (produkcja) w ogólne nie wiąże się z przetwarzaniem danych osobowych. Powinna ona jednak poważnie zastanowić się nad uwzględnieniem w swojej strukturze organizacyjnej funkcji IOD. Będzie to miało pozytywny wydźwięk przede wszystkim wśród jej pracowników. Ich dane osobowe, mimo, że nie w zakresie głównej działalności administratora, są przetwarzane na szeroką skalę. Dodatkowo, nie sposób w tym zakresie, pominąć wydarzeń ostatnich miesięcy. Wielu administratorów mierzyło (i nadal mierzy) się z wyzwaniami związanymi z przeciwdziałaniem pandemii COVID-19. Są to również wyzwania w zakresie gromadzenia dodatkowych danych osobowych (pomiary temperatury, odpytywanie o kierunki

wyjazdów, etc.). W tym zakresie zatem, pomoc i wsparcie IOD będą dla każdego administratora bezcenne.

Marcin Szkutnik, radca prawny, ekspert ds. ochrony danych osobowych

Powoływanie IOD jest częstą praktyką wśród dużych przedsiębiorstw, gdzie głównych argumentem dla ich powołania jest duża ilość danych w takich firmach (np. danych kadrowych) lub występowanie licznych i złożonych procesów przetwarzania danych. W grupach kapitałowych, popularnym rozwiązaniem jest wyznaczanie jednej osoby pełniącej funkcję IOD dla całej grupy, co pozwala utrzymać jednolite standardy ochrony danych osobowych w ramach grupy. Z drugiej strony, na powoływanie IOD decydują się także małe firmy, szczególnie z branży technologicznej i marketingowej, które na co dzień przetwarzają duże ilości danych swoich klientów.

Jakie są zadania IOD w praktyce?

Każdemu IOD zdarzyło się wykonywać różne zadania i obowiązki w ramach pełnienia swojej funkcji.

Stanowisko IOD zostało celowo opisane w RODO w sposób dość ogólny. Zakres zadań IOD, zawsze po części będzie zależał od tego na co konkretnie umówią się obie strony. Dlatego tak **ważny jest początek sprawowania funkcji IOD**. To najlepszy moment na ustalenie konkretnego zakresu obowiązków dla obu stron. Podkreślam – obu stron, ponieważ to również administrator danych ma pewne obowiązki względem Inspektora Ochrony Danych.

Jeśli nawiązujemy współpracę z IOD zewnętrznym, sprawa będzie nieco prostsza. Podpisana zostanie umowa, w której wskazany zostanie zakres obowiązków każdej z jej stron.

Jeśli IOD będzie nasz pracownik, potrzebna może być zmiana treści umowy w ramach, której z nim współpracujemy lub przynajmniej zakresu obowiązków.

W praktyce zdarza się, że IOD – pracownik nie podpisuje aneksu do umowy, ani nie otrzymuje nowego zakresu obowiązków. Taka sytuacja nie powinna mieć miejsca, bo zawsze będzie szkodliwa dla organizacji. IOD do swoich obowiązków może zaliczyć jedynie to co wskazane jest wprost w RODO, a administrator danych będzie oczekiwał znacznie więcej. Kto będzie miał rację w takim sporze? Trudno powiedzieć… bo same obowiązki wymienione w RODO nie są precyzyjne. Na pewno jednak sytuacja będzie szkodliwa i ryzykowna dla samej organizacji.

Co zrobić, aby zapobiec takim sytuacjom? Zacznijmy od precyzyjnego podziału obowiązków IOD. W kolejnych akapitach napiszę o tym, co IOD:

- musi robić,
- może robić,
- czego robić nie powinien.

Co IOD robić powinien?

Obowiązki IOD zostały opisane w art. 39 ust. 1 RODO. Artykuł ten zawiera katalog, który określa minimalny zakres zadań, do których wykonywania są zobowiązani Inspektorzy Ochrony Danych. Problem

w tym, że np. obowiązek wykonywania szkoleń czy audytów został opisany w sposób bardzo ogólny. Czy chodzi o audyt prowadzony raz na kilka lat, czy może cykliczny audyt sprawdzający stan wdrożenia RODO? Podobnie kwestia szkoleń. Czy wystarczy raz przeprowadzić szkolenie e-learningowe, czy też konieczne będę cykliczne szkolenia stacjonarne? Administrator danych i IOD mogą widzieć te działania w nieco odmienny sposób. Dlatego warto, aby już na etapie rozpoczęcia współpracy, obie strony miały spójną wizję wykonywania zadań przez IOD i formalnie ją opisały (w umowie, porozumieniu, zakresie obowiązków, etc.).

Przyjrzyjmy się zatem bliżej obowiązkom IOD wymienionym w RODO.

Obligatoryjne zadania Inspektora Ochrony Danych
Informowanie o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych.
Doradzanie w zakresie obowiązków wynikających z RODO i innych przepisów.
Monitorowanie przestrzegania RODO, innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych.
Monitorowanie przestrzegania polityk w dziedzinie ochrony danych osobowych.
Doradztwo w zakresie podziału obowiązków (np. między współadministratorami, administratorem a podmiotem przetwarzającym lub pomiędzy członkami personelu).
Prowadzenie działań zwiększających świadomość personelu w zakresie obowiązków wynikających z RODO lub przyjętych polityk.
Przeprowadzanie lub organizowanie szkoleń dla personelu uczestniczącego w operacjach przetwarzania danych.
Przeprowadzanie audytów w zakresie przestrzegania RODO i polityk.
Udzielanie na żądanie administratora zaleceń co do oceny skutków dla ochrony danych.
Monitorowanie wykonania oceny skutków dla ochrony danych.
Współpraca z Prezesem UODO oraz pełnienie funkcji punktu kontaktowego dla Prezesa UODO w kwestiach związanych z przetwarzaniem.
Uczestniczenie w konsultacjach we wszelkich sprawach związanych z ochroną danych osobowych.
Pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Co IOD może, ale nie musi robić?

W praktyce IOD często otrzymuje znacznie więcej zadań, niż te opisane w RODO. Oczekiwania administratora danych w tym zakresie są zrozumiałe… ale nie zawsze dobre dla jego organizacji. Od IOD oczekuje się, że temat RODO weźmie w całości na siebie. Jednak nadmierne wymagania administratora danych, nie zawsze będą możliwe do zrealizowania w praktyce. Przykładowo, IOD wewnętrzny, który wykonuje innego rodzaju pracę, nie zawsze będzie miał czas na szkolenia, audyty i zupełnie samodzielne prowadzenie rejestru czynności przetwarzania. Jeśli dodamy takiemu IOD jeszcze obowiązek analizy prawnej umów powierzenia, odpowiadania na żądania osób, sprawdzania zabezpieczeń IT, to mamy dobry przepis na mniejszą lub większą katastrofę.

W części przypadków, IOD potrzebować może wsparcia innych pracowników przy realizacji zadań fakultatywnych, wymienionych poniżej.:

Fakultatywne zadania Inspektora Ochrony Danych
Koordynowanie całego procesu oceny skutków dla ochrony danych osobowych.
Opracowywanie i aktualizacja polityk ochrony danych
Administrowanie oraz kontrola upoważnień do przetwarzania danych osobowych, w tym prowadzenie rejestru nadanych upoważnień.
Przygotowywanie lub opiniowanie umów powierzenia przetwarzania danych osobowych, w tym prowadzenie ich rejestru zawartych umów.
Udział w procesach związanych z naruszeniami ochrony danych osobowych, w tym prowadzenie rejestru naruszeń, prowadzenie postępowania wyjaśniającego, dokonywanie oceny naruszenia, koordynowanie zgłoszenia naruszenia Prezesowi UODO oraz osobom, których dane dotyczą.
Opracowywanie treści klauzul informacyjnych, klauzul zgód na przetwarzanie danych osobowych, oraz innych klauzul / postanowień związanych z przetwarzaniem danych osobowych (np. postanowień w zakresie współadministrowania).
Prowadzenie rejestru czynności przetwarzania danych osobowych.
Prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu innego administratora danych.
Udział w procesie realizacji praw osób, których dane dotyczą, w tym udzielanie odpowiedzi na zapytania, prowadzenie wszelkiej korespondencji, spotkania z osobami realizującymi swoje prawa.
Reagowanie na skargi osób, których dane dotyczą, w tym prowadzenie korespondencji ze skarżącym, opracowywanie treści pism w toku postepowania.

Udział w postępowaniach administracyjnych oraz sądowych prowadzonych w związku ze skargami osób, których dane dotyczą bądź innymi naruszeniami RODO.
Udział w procesach certyfikacji oraz przystępowania do funkcjonujących kodeksów postępowania.
Kontrola podmiotów przetwarzających.

Powyższe wyliczenie nie ma charakteru zamkniętego. Istotne jest to, aby wykonywanie przez IOD dodatkowych zadań nie powodowało konfliktu interesów, nie naruszało zasady niezależności IOD, a także było możliwe w praktyce.

Dwa modele bycia IOD

Powyższe zadania, te obowiązkowe i fakultatywne, możemy podzielić na zadania związane z zarządzeniem ochroną danych osobowych (IOD manager) oraz bardziej szczegółowe i techniczne (IOD specjalista). Całość obrazuje poniższy schemat:

Który z tych modeli jest prawidłowy? Nie da się odpowiedzieć jednoznacznie na to pytanie. RODO celowo pozostawiło dość szerokie pole do interpretacji przy opisie funkcji IOD.

W praktyce funkcjonują oba modele i w wielu przypadkach sprawdzają się one dobrze. Najważniejsze to oraz wybrać konkretne rozwiązanie odpowiednie dla naszej organizacji za wspólną zgodą obu stron – ADO i IOD.

Nie można zapominać o możliwościach czasowych Inspektora Ochrony Danych. Jeśli decydujesz się na IOD zewnętrznego, to musisz być świadom/a tego, że IOD zajmujący się również szczegółowymi obszarami, będzie kosztował więcej.

Podobnie w przypadku IOD wewnętrznego. Jeśli jest nim Twój pracownik, np. z działu kadr, to musisz liczyć się z tym, że nowe obowiązki obciążą taką osobę. Jak mocno? To już będzie zależało od wzajemnych ustaleń.

Dla celów poglądowych przedstawiłem dwie skrajności. IOD, który w ogólnie nie wchodzi w szczegóły, nie prowadzi rejestru czynności przetwarzania, nie przegląda umów powierzenia, etc. Oraz IOD, który zajmuje się wszystkim w swojej organizacji. Od umów powierzenia po audyty i szkolenia. W praktyce, rola IOD w organizacji najczęściej wpasowuje się gdzieś pośrodku obu tych skrajności.

Czego IOD robić nie powinien

Zakres obowiązków IOD jest dość elastyczny i zależny od tego na co umówiły się strony. Zadania których IOD nie powinien wykonywać, będą łączyły się przede wszystkim z różnego rodzaju konfliktami interesów.

Jednym z głównych zadań IOD oraz ADO, będzie takie ułożenie sobie współpracy, aby konflikty interesów nie występowały.

Tematem konfliktów interesów oraz niezależności IOD, zajmę się w kolejnym artykule cyklu.

A jakie są obowiązki ADO względem IOD?

Pełnienie funkcji IOD ma sens tylko wtedy, kiedy ma on zagwarantowane niezależność i dostęp do informacji. Jeśli reprezentujesz administratora danych i chcesz powołać Inspektora Ochrony Danych, pamiętaj o tym, że po Twojej stronie również leżą pewne obowiązki.

Obowiązki administratora danych wobec Inspektora Ochrony Danych
Zapewnienie, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Twoja organizacja powinna zapewnić m.in., aby: • IOD był zapraszany do regularnego udziału w posiedzeniach kadry kierowniczej oraz uczestniczył w podejmowaniu decyzji mających wpływ na ochronę danych, • wszystkie niezbędne informacje zostały udostępnione IOD odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska, • opinia IOD była zawsze należycie uwzględniana, w przypadku stwierdzenia naruszenia ochrony danych lub innego incydentu, następowała niezwłoczna konsultacja z IOD.
Wspieranie Inspektora Ochrony Danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. W tym zakresie administrator danych powinien wziąć pod uwagę następujące aspekty: • aktywne wsparcie IOD ze strony kadry kierowniczej przy pełnieniu powierzonej mu funkcji (np. na poziomie zarządu), • czas wystarczający do tego, by IOD mógł się wywiązać z przydzielonych mu obowiązków, • w stosownych przypadkach wsparcie w postaci zasobów finansowych, infrastruktury (pomieszczenia, urządzenia, wyposażenie) oraz pracowników, • oficjalne powiadomienie wszystkich pracowników o wyznaczeniu IOD w celu zapewnienia, aby wszyscy w organizacji wiedzieli o jego istnieniu i pełnionej przez niego funkcji, • niezbędny dostęp do innych służb, np. działu zasobów ludzkich, działu prawnego, informatycznego i ochrony, itd., aby IOD mógł otrzymywać niezbędne wsparcie i informacje, • doskonalenie zawodowe, (poszerzanie wiedzy na temat postępów poczynionych w dziedzinie ochrony danych, udział w kursach i innych formach doskonalenia zawodowego, takich jak udział w forach, warsztatach, itp.), • w zależności od rozmiaru i struktury organizacji konieczne może być powołanie zespołu IOD (IOD i jego współpracowników).

Opublikowanie danych kontaktowych Inspektora Ochrony Danych na stronie internetowej, a jeśli jej nie prowadzi w sposób ogólnie dostępny w miejscu prowadzenia działalności, oraz zawiadomienie o nich Prezesa UODO.

Co jeszcze ADO powinien określić, decydując się na powołanie IOD?

Inne kwestie, które administrator danych powinien określić samodzielnie
Wyznaczenie Inspektora Ochrony Danych spośród członków personelu albo nawiązanie współpracy z zewnętrznym IOD na podstawie umowy o świadczenie usług zawartej z daną osobą fizyczną lub organizacją.
Wyznaczenie jednego IOD w ramach grupy przedsiębiorstw (lub grupy organów publicznych), o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.
Możliwość wykonywania przez Inspektora Ochrony Danych innych zadań i obowiązków z zastrzeżeniem, że administrator danych zapewni, by takie zadania i obowiązki nie powodowały konfliktu interesów.
Powołanie zespołu Inspektora Ochrony Danych w zależności od rozmiaru i struktury organizacji. W takich przypadkach należy jasno określić wewnętrzną strukturę zespołu oraz zadania i obowiązki poszczególnych jego członków.

Czego ADO nie może oczekiwać względem IOD?

Czynności, których administrator danych nie może wykonać wobec Inspektora Ochrony Danych
Przekazywanie Inspektorowi Ochrony Danych instrukcji dotyczących wykonywania jego zadań (np. instrukcji dotyczących wyników, jakie należy osiągnąć, sposobu rozpatrywania skargi lub tego, czy należy przeprowadzić konsultacje z organem nadzorczym).
Zobligowanie IOD do przyjęcia określonego stanowiska w sprawie przepisów dotyczących ochrony danych np. określonej wykładni przepisów.
Odwoływanie lub ukaranie Inspektora Ochrony Danych za wypełnianie swoich zadań. Chodzi tu o kary w różnych formach, bezpośrednie albo pośrednie, np. brak albo opóźnienie awansu, utrudnienie rozwoju zawodowego, ograniczenie dostępu do korzyści oferowanych pozostałym pracownikom. Zakaz odwoływania IOD, nie oznacza natomiast, że nie może on zostać odwołany w uzasadnionych sytuacjach, z przyczyn innych niż wykonywanie swoich obowiązków (np. z powodu kradzieży).

Delegowania podległości IOD na inną osobę lub jednostkę organizacyjną, niż najwyższe kierownictwo administratora.
Zobowiązanie Inspektora Ochrony Danych do poniesienia osobistej odpowiedzialności za przypadki naruszenia przepisów RODO.
Uniemożliwianie bądź ograniczanie Inspektorowi Ochrony Danych kontaktu z Prezesem Urzędu Ochrony Danych Osobowych

Podsumowanie

Jak w każdej relacji, początkowe ustalenie wzajemnych oczekiwań jest kluczowe. Jeśli IOD wspólnie z ADO w sposób świadomy dobierze zakres obowiązków, to jest szansa na długą i owocną współpracę – dla obu stron. Lepiej poświęcić nieco więcej czasu na początku, aby ustalić szczegóły, niż zdawać się jedynie na wyobrażenia drugiej strony. To ważna uwaga dla obu stron relacji. Zwłaszcza w obecnej sytuacji, kiedy wyobrażenia o roli IOD mogą być bardzo różne.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu

Źródła:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych)
- Wytyczne dotyczące inspektorów ochrony ('DPO') (przyjęte w dniu 13 grudnia 2016 r. ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.)
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 roku (jako IOD)