



AKTUALNE WYZWANIA W PRACY INSPEKTORÓW OCHRONY DANYCH

Warto wspierać inspektorów ochrony danych w wykonywaniu ich funkcji i chronić ich niezależność. Kluczowe w tej pracy jest właściwe rozumienie roli inspektora i zapewnienie mu właściwych warunków funkcjonowania i gwarancji niezależności. Czy w przyszłości czeka nas jednak większa specjalizacja wśród inspektorów?

O kompetencjach i wyzwaniach stojących przed inspektorami ochrony danych wypowiedzieli się Monika Młotkiewicz, naczelnik Wydziału Współpracy z Inspektorami Ochrony Danych w UODO, oraz prof. Grzegorz Sibiga z Instytutu Nauk Prawnych Polskiej Akademii Nauk w rozmowie z Adamem Sanockim, rzecznikiem Prasowym UODO.

Adam Sanocki: Jakie są obecnie najistotniejsze kompetencje IOD?



Monika Młotkiewicz
Naczelnik Wydziału Współpracy
z Inspektorami Ochrony Danych
w UODO

Monika Młotkiewicz: Kompetencje inspektorów ochrony danych – odkąd zaczęliśmy stosować RODO – są niezmiennie i wynikają one wprost z treści tej regulacji – są to fachowa wiedza i fachowe umiejętności, czyli znajomość prawa i praktyk w dziedzinie ochrony danych osobowych i umiejętność ich zastosowania w praktyce przy realizacji zadań inspektorów ochrony danych.

Przy czym ostatni czas był pod tym względem dość trudny. Pandemia przeniosła nas niemal z dnia na dzień prawie całkowicie w świat cyfrowy, narzuciła nam zupełnie nowe warunki funkcjonowania, za którymi zupełnie nie nadążały procesy prawne. Znaleźliśmy się tak naprawdę w sytuacji deficytu

norm prawnych oraz braku jednoznacznych i niebudzących wątpliwości podstaw przetwarzania danych, w tym danych wrażliwych.

W takiej sytuacji bardzo trudno być doradcą, wskazywać w swoich organizacjach właściwe rozwiązania. I tutaj przewagę mieli ci inspektorzy, którzy mieli duże doświadczenie w swojej pracy, są biegli w wykonywaniu swoich zadań. Ci, którzy potrafili szybko reagować na tą nową sytuację, którzy mieli wiedzę w zakresie elektronicznych środków przekazu, funkcjonowania dużych platform internetowych, pracy zdalnej czy zagrożeń w cyberprzestrzeni. Dużą sztuką było szybkie dostosowanie obowiązujących procedur do nowej sytuacji i skuteczne zaznajomienie z nimi pracowników.

Grzegorz Sibiga: Inspektor ochrony danych potrzebuje różnego rodzaju kompetencji. Nie wystarczą tylko i wyłącznie kompetencje prawnicze, które były wymagane na początkowym etapie wdrożenia RODO i związane były przede wszystkim z nowym stanem prawnym. Natomiast wraz z upływem czasu okazuje się, że są potrzebne również innego rodzaju kompetencje – związane nie tylko z zarządzaniem bezpieczeństwem informacji, ale również kompetencje miękkie związane ze znajomością kultury organizacyjnej danej jednostki, jej specyfiki, związane ze znajomością zadań publicznych lub też biznesów, w ramach których dochodzi do przetwarzania danych osobowych.

Adam Sanocki: Jakie są najważniejsze aspekty związane z pracą IOD w administracji publicznej, a jakie w sektorze prywatnym?



prof. Grzegorz Sibiga
Instytut Nauk Prawnych
Polskiej Akademii Nauk

Grzegorz Sibiga: Faktycznie zauważalna jest różnica pomiędzy wykonywaniem funkcji IOD w sektorze publicznym i w szeroko rozumianym sektorze prywatnym. W sektorze publicznym wymaga się znajomości całej gamy różnego typu uregulowań dotyczących prawa administracyjnego oraz procedur, w jakich działa administracja publiczna. Natomiast gdy chodzi o działalność gospodarczą, występują tutaj pewne aspekty, które w sposób naturalny nie istnieją w administracji publicznej, takie jak choćby kwestia marketingu usług i produktów, czy też kwestia przekazywania danych wewnątrz grupy kapitałowej. Kwestie te są związane ze specyfiką działalności gospodarczej. Trzeba jednak podkreślić, że wspólnym mianownikiem dla pracy inspektora ochrony danych zarówno w sferze publicznej, jak i w sektorze prywatnym są przede wszystkim te przepisy ogólnego rozporządzenia o ochronie danych osobowych, a także ustawy o ochronie danych osobowych, które w takim samym stopniu dotyczą zarówno sektora publicznego, jak i sektora prywatnego.

Monika Młotkiewicz: Kwalifikacje inspektora ochrony danych są ściśle związane ze specyfiką administratora, z branżą, w której on funkcjonuje, niezależnie od tego, czy mówimy o sektorze publicznym, czy prywatnym. Praca inspektora ochrony danych wymaga bardzo dobrej orientacji w przepisach prawa, ale też w całym dorobku, który wiąże się z tymi przepisami. Chodzi tutaj o orzecznictwo sądowe, piśmiennictwo, rozstrzygnięcia organów nadzorczych. Czasem jest to bardzo rozległa specjalizacja branżowa, bo rzeczywiście w niektórych dziedzinach przepisy prawa, rekomendacje, wytyczne są bardzo szczegółowe. Mam na myśli takie dziedziny, jak działalność lecznicza, edukacja, sektor pracy, czyli takie dziedziny, które dotyczą zarówno podmiotów prywatnych, jak i publicznych. Takie szczegółowe, rozbudowane regulacje dotyczą również innych sektorów – sektora bankowego, ubezpieczeniowego, telekomunikacyjnego, farmaceutycznego, pomocy społecznej czy też sektora sądownictwa. Oczywiście sektor publiczny, posiada, co do zasady, np. odmienne podstawy przetwarzania danych, inne niż w sektorze prywatnym, czy też pewne specyficzne problemy specjalne wspólne zagadnienia, jak chociażby dostęp do informacji publicznej czy tworzenie narodowego zasobu archi-

walnego. Niemniej jednak obserwujemy, że wiedza i doświadczenie sektorowe jest coraz bardziej cenione.

Adam Sanocki: Czy zatem warto rozdzielać te kompetencje na sektor publiczny i prywatny, czy może istotne są inne czynniki?

Grzegorz Sibiga: Bazując na swoim doświadczeniu uzyskanym z pracy naukowej, pracy kancelaryjnej jak i kierownika studiów podyplomowych dla inspektorów ochrony danych, przyznaję, że potrzebne są pewne specyficzne kompetencje dla każdego z rodzajów tych działalności. W administracji publicznej jest to przede wszystkim potrzeba znajomości szczególnych przepisów, czy też uregulowań dotyczących administracji publicznej, takich jak choćby prawo zamówień publicznych, znajomości procedur, które występują w administracji publicznej czy też znajomości archiwizacji, która jest bardzo specyficzna w administracji publicznej i różni się od tego, co występuje w przedsiębiorstwach. Natomiast gdy chodzi o sektor prywatny, kompetencje powinny podążać za biznesem, za samym przedmiotem działalności gospodarczej. W obu tych rodzajach działalności wydaje się, że potrzebne są też w coraz większym stopniu kompetencje miękkie, związane z potrzebą niezależności inspektora, komunikacji inspektora z pozostałymi osobami w jednostce organizacyjnej, jak również unikania konfliktów interesu. Miękkie kompetencje, które na początku obowiązywania RODO były mniej zauważalne, teraz w praktyce mają coraz większe znaczenie.

Monika Młotkiewicz: Na pewno warto wspierać inspektorów w wykonywaniu ich funkcji i chronić ich niezależność. Kluczowe jest właściwe rozumienie roli inspektora i zapewnienie mu właściwych warunków funkcjonowania i gwarancji niezależności. Niestety mimo że RODO stosujemy już od ponad 3 lat nie wszędzie jest to respektowane. Do UODO zgłaszane są problemy związane chociażby z powołaniem inspektora ochrony danych. Nie zawsze rozumie się, że musi to być fachowiec, że wiedza i bezpieczeństwo danych kosztuje, że nie można w tę rolę ubrać swojego pracownika zupełnie nieprzygotowanego do tej funkcji albo przeciążonego innymi obowiązkami albo też nowej wykwalifikowanej osoby, ale za najniższe możliwe wynagrodzenie.

Nie tylko polski organ do spraw ochrony danych osobowych, ale i inne organy nadzorcze w Unii Europejskiej pokazują w wydawanych decyzjach, że wysokie standardy, które są przyjęte w odniesieniu

do inspektora i jego niezależności muszą być respektowane. Organy reagują również wtedy, kiedy zadania inspektora nie są wykonywane w sposób prawidłowy, a odpowiedzialność za to ponosi administrator. Przykładem takiej reakcji była decyzja Prezesa Urzędu Ochrony Danych Osobowych w sprawie Szkoły Głównej Gospodarstwa Wiejskiego, gdzie naruszenie i kara dotyczyły m.in. niewłączenia inspektora w sprawy ochrony danych osobowych i nieprawidłowe wykonywanie przez niego zadań. Innym przykładem decyzji jest nałożenie upomnienia na administratora, który przerzucał na inspektora swoje obowiązki.

Adam Sanocki: Jakie wyzwania w związku z tym czekają z jednej strony samych IOD, a jakie ich pracodawców?

Grzegorz Sibiga: Bardzo ważny jest wybór właściwego IOD przez administratora lub podmiot przetwarzający, bo to do nich należy obowiązek wybrania inspektora, który posiada właściwe kompetencje. Administrator czy podmiot przetwarzający powinni zwracać uwagę na doświadczenie i wiedzę inspektora ochrony danych osobowych w tym sektorze, w którym działają. Zatem, odnosząc się do podziału na sektor publiczny i prywatny, administrator z sektora publicznego, organ administracji publicznej, powinien poszukiwać przede wszystkim inspektorów ochrony danych osobowych, którzy mają doświadczenie i znają specyfikę administracji publicznej, bądź też są wyedukowani właśnie w tym kierunku. Natomiast pracodawcy w sektorze prywatnym, w przedsiębiorstwach, w naturalny sposób poszukują inspektorów, którzy mają doświadczenie w sektorze prywatnym, w biznesie, w działalności gospodarczej, a nawet w ściśle określonym rodzaju działalności gospodarczej, przykładowo w sektorze zdrowotnym, gdzie występuje bardzo duża specyfika. Z kolei ze strony inspektorów ochrony danych osobowych wymaga to jednak pewnej specjalizacji. Nie mówię, że jest to specjalizacja raz na zawsze w określonym sektorze, ale chcąc prawidłowo wykonywać swoją

funkcję w administracji publicznej trzeba znać i rozumieć jej specyfikę, znać szczególne uregulowania prawne dotyczące sektora publicznego i tak samo w sektorze prywatnym. Bez tego, jak się wydaje niemożliwe jest już prawidłowe wykonywanie tej funkcji.

Monika Młotkiewicz: W pracy inspektora niezwykle ważna jest wiedza i wsparcie ze strony administratora oraz ze strony wszystkich osób, które przetwarzają dane w określonej organizacji. Takie osoby muszą współdziałać z inspektorem. Wiedza inspektora musi być ciągle aktualizowana. Co oznacza nie tylko stały wysiłek po stronie samych inspektorów w zakresie poszerzania tej wiedzy, korzystania z wiarygodnych źródeł informacji na temat prawa i praktyk, ale też stałe pozycje na ten cel w budżetach organizacji. W wiedzę inspektora trzeba systematycznie inwestować i taki obowiązek jest wprost zapisany w przepisach rozporządzenia ogólnego o ochronie danych osobowych.

Praca inspektora polega na tym, żeby informować o obowiązkach, wskazywać zauważone nieprawidłowości, zagrożenia związane z przetwarzaniem danych osobowych, ale ważne jest, aby za tymi rekomendacjami szły od strony pracodawców i zlecniodawców inspektorów ochrony danych konkretne decyzje, zarządzenia, przypisywanie odpowiednich zadań odpowiednim osobom w odpowiednich terminach i potem te decyzje muszą być egzekwowane. Tylko wtedy praca inspektora ma sens, przyczynia się do przestrzegania przepisów prawa i do rozwijania skutecznego systemu ochrony danych osobowych w takiej organizacji.

Zapis całej rozmowy z Moniką Młotkiewicz, naczelnik Wydziału Współpracy z Inspektorami Ochrony Danych w UODO, oraz prof. Grzegorzem Sibigą z Instytutu Nauk Prawnych Polskiej Akademii Nauk znajduje się w materiale wideo dostępnym pod linkiem:
<https://video.uodo.gov.pl/video/rola-iod.mp4>