



Zasady współpracy audytora wewnętrznego i inspektora ochrony danych przy realizacji zadań w jednostce sektora finansów publicznych

Jednostki sektora publicznego od 25 maja 2018 r., tj. od dnia, obowiązywania *Rozporządzenia 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 (RODO)*, są zobowiązane do wyznaczenia inspektora ochrony danych¹.

Obowiązkiem kierownika jednostki jest zapewnienie odpowiedniego wsparcia IOD, w wypełnianiu przez niego zadań, oraz zapewnienie warunków niezależnego i skutecznego wykonywania tych zadań, tj.:

- bezpośrednią podległość kierownikowi jednostki,
- udział we wszystkich sprawach związanych z ochroną danych osobowych,
- nieotrzymywanie instrukcji dotyczących wykonywania zadań,
- brak możliwości odwołania lub ukarania za wypełnianie przez IOD jego zadań,
- nieotrzymywanie innych zadań i obowiązków, które mogłyby powodować konflikt interesów.

Jednocześnie w jednostkach sektora finansów publicznych, w których prowadzony jest audyt wewnętrzny funkcjonuje audytor wewnętrzny dokonujący systematycznej oceny kontroli zarządczej, obejmując zasięgiem swojego działania wszystkie obszary jednostki.

Na podstawie art. 282 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych², kierownik jednostki jest odpowiedzialny za zapewnienie warunków niezbędnych do niezależnego, obiektywnego i efektywnego prowadzenia audytu wewnętrznego, w tym organizacyjnej odrębności komórki audytu wewnętrznego oraz ciągłości prowadzenia audytu wewnętrznego w jednostce.

Warunki niezależności audytora wewnętrznego wynikające z *ustawy* to:

- bezpośrednia podległość kierownika komórki audytu wewnętrznego kierownikowi jednostki,
- ochrona stosunku pracy poprzez konieczność uzyskania zgody właściwego komitetu audytu na rozwiązanie stosunku pracy lub zmiana warunków płacy i pracy kierownika komórki audytu wewnętrznego ministerstwa oraz jednostki w dziale,

¹ Dalej jako: IOD.

² Dz. U. z 2017 r. poz. 2077, z późn. zm., dalej jako: *ustawa*.

- prawo wstępu do pomieszczeń jednostki oraz wglądu do wszelkich dokumentów, informacji i danych oraz do innych materiałów związanych z funkcjonowaniem jednostki, w tym utrwalonych na elektronicznych nośnikach danych, jak również do sporządzania ich kopii, odpisów, wyciągów, zestawień lub wydruków, z zachowaniem przepisów o tajemnicy ustawowo chronionej,
- zobowiązanie pracowników jednostki do udzielania informacji i wyjaśnień, a także sporządzania i potwierdzania kopii, odpisów, wyciągów lub zestawień niezbędnych do realizacji audytu.

Dodatkowo, zgodnie ze standardami audytu wewnętrznego dla jednostek sektora finansów publicznych³, audytor wewnętrzny nie powinien być narażony na jakiegokolwiek próby ingerowania w zakres realizowanego audytu, wpływania na sposób wykonywania pracy i informowania o jej wynikach. Jednocześnie audytor powinien unikać konfliktu interesów.

Ze względu na charakter zadań realizowanych w jednostce przez IOD i audytora wewnętrznego oraz w celu zapewnienia ich niezależności zostały wypracowane przez Ministerstwo Finansów i Urząd Ochrony Danych Osobowych zasady współpracy dotyczące audytu wewnętrznego w obszarze ochrony danych osobowych.

Obowiązkiem każdej jednostki sektora publicznego jako administratora danych jest czuwanie nad zgodnym z prawem przetwarzaniem danych osobowych i właściwą organizacją bezpieczeństwa informacji. W osiągnięciu tego celu jednostka powinna korzystać zarówno z pomocy audytorów, jak i inspektorów ochrony danych.

Zarówno IOD, jak i audytor wewnętrzny wspierają kierownika jednostki sektora finansów publicznych w realizacji celów i zadań tej jednostki. Jednostki sektora finansów publicznych będące administratorami danych ponoszą bowiem odpowiedzialność za pełną i całościową zgodność przetwarzania danych osobowych z przepisami prawa. Do zadań IOD należy monitorowanie zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa. Natomiast do zadań audytora wewnętrznego należy m.in. ocena zgodności działalności jednostki z przepisami prawa (a zatem również przepisami prawa o ochronie danych osobowych) oraz procedurami wewnętrznymi, a także skuteczności i efektywności działania, ochrony zasobów oraz zarządzania ryzykiem.

W związku z tym działania audytorów wewnętrznych i inspektorów ochrony danych powinny być komplementarne. W celu wsparcia prawidłowego funkcjonowania jednostki powinni oni wymieniać informacje i dokumenty niezbędne dla prawidłowej realizacji swoich zadań. Zarówno inspektorzy ochrony danych, jak i audytorzy podlegają bezpośrednio kierownikowi jednostki, a ich praca może podlegać jego kontroli, w tym kontroli zleconej przez kierownika podmiotom wewnętrznym lub zewnętrznym.

Zarówno w przypadku audytora wewnętrznego jak i inspektora ochrony danych kluczową rolę odgrywa niezależność w realizowaniu zadań. Stąd audytorzy i inspektorzy muszą w swojej pracy

³ Komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz. U. poz. 28).

uwzględniać wzajemną niezależność i nie wpływać na jej ograniczanie. Sposób przeprowadzania audytu wewnętrznego został określony w przepisach *rozporządzenia z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu*⁴. W przypadku gdy audyt obejmuje zadania realizowane przez IOD audytor wewnętrzny powinien odnosić się do badanego obszaru, nie formułując wniosków dotyczących bezpośrednich działań IOD. W tym zakresie ostateczne decyzje podejmuje kierownik jednostki. Jeżeli IOD nie zgadza się ze stanowiskiem kierownika jednostki sektora finansów publicznych, powinien mieć możliwość przedstawienia swojego stanowiska, które powinno zostać uzasadnione i udokumentowane. Materiał ten może być przydatny w celach dowodowych w przypadkach oceny prawidłowości wykonywania funkcji IOD w kontekście jego odpowiedzialności na gruncie przepisów prawa pracy lub Kodeksu cywilnego (odpowiedzialności kontraktowej) przez właściwe organy.

Inspektor ochrony danych i audytor wewnętrzny posiadają gwarancje niezależności kształtujące ich status. Każdy z nich działa też w celu zapewnienia zgodności działań jednostki sektora finansów publicznych z prawem. Dlatego w osiągnięciu tego celu potrzebna jest ich efektywna współpraca oraz wzajemne wspieranie się w tym zakresie wiedzą i doświadczeniem.

⁴ Dz. U. poz. 1480, z późn. zm.