



WSPÓŁPRACA AUDYTORA WEWNĘTRZNEGO I INSPEKTORA OCHRONY DANYCH - PERSPEKTYWA URZĘDU OCHRONY DANYCH OSOBOWYCH

R.PR. MONIKA MŁOTKIEWICZ
DYREKTOR ZESPOŁU WSPÓŁPRACY Z ADMINISTRATORAMI DANYCH
UODO



Czy możliwe jest łączenie funkcji audytora i inspektora ochrony danych?



**Dlaczego możliwe jest łączenie funkcji
audytora i inspektora ochrony danych?**



Cechy wspólne obu funkcji.



OBOWIĄZEK WYZNACZENIA IOD

- art. 37 ust 1 RODO przewiduje

obowiązek wyznaczenia inspektora dla organów lub podmiotów publicznych, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości (sądy i trybunały mają obowiązek wyznaczenia IOD, jednakże w przypadku sądów ze względu na ochronę niezawisłości sędziowskiej z zakresu kompetencji inspektora wyłączone są operacje przetwarzania danych mieszczące się w czynnościach orzeczniczych (sprawowania wymiaru sprawiedliwości).

- art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Przez organy i podmioty publiczne obowiązane do wyznaczenia IOD, o których mowa w art. 37 ust. 1 lit. a RODO, rozumie się **jednostki sektora finansów publicznych** (np. jednostki samorządu terytorialnego, uczelnie publiczne), **instytuty badawcze oraz Narodowy Bank Polski**.

USTAWA Z DNIA 14 GRUDNIA 2018 R. O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH

Art. 46. ust 1. Administrator wyznacza inspektora ochrony danych.

Ust 2. Inspektorem ochrony danych może być osoba, która:

- 1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
- 2) posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;
- 3) nie była skazana prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

Art. 4. Ilekroć w ustawie jest mowa o:

administratorze - rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych,
podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie,
albo podmiot wskazany przez prawo Unii Europejskiej albo prawo państwa członkowskiego Unii Europejskiej lub podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa;

USTAWA Z DNIA 14 GRUDNIA 2018 R.

O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU
Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI



O osobowych

KTO MA OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH
na podstawie ustawy z dnia 14 grudnia 2018 r.?

Policja

Straż Graniczna

Służba Więzienna

Żandarmeria Wojskowa

Służba Ochrony Państwa

Generalny Inspektor Informacji

Finansowej

Krajowa Administracja Skarbowa

Sądy

Prokuratury

Straż gminna / miejska

Inspekcja Drogowa

Minister Środowiska

Główny Inspektorat Ochrony Środowiska

Straż Rybacka

Główny Inspektor Straży Leśnej

Państwowa Straż Łowiecka

Urząd Żeglugi Śródlądowej

urzędy morskie

Państwowa Inspekcja Sanitarna

Podmioty odpowiedzialne za

bezpieczeństwo imprez masowych

Przewoźnicy lotniczy (dane PNR)

OBOWIĄZEK PROWADZENIA AUDYTU WEWNĘTRZNEGO

Urząd
Ochrony
Danych
Osobowych



- **Ustawa o finansach publicznych** wymienia wprost jednostki **zobowiązane** do prowadzenia audytu wewnętrznego. Kancelaria Prezesa Rady Ministrów, ministerstwa, urzędy wojewódzkie, izby celne, izby skarbowe, ZUS, KRUS, NFZ, państwowe jednostki budżetowe, uczelnie publiczne, samodzielne publiczne ZOZ, jednostki samorządu terytorialnego i sektora finansów publicznych (z pewnymi założeniami).
- Kierownicy **innych jednostek samodzielnie podejmują decyzję** o tym, czy zamierzają skorzystać ze wsparcia w zarządzaniu jednostką w postaci audytu wewnętrznego.

WYKONYWANIE ZADAŃ JAKO CZŁONEK PERSONELU LUB NA PODSTAWIE UMOWY O WYKONYWANIE USŁUG

Urząd
Ochrony
Danych
Osobowych



Art. 275 ufp

Audyt wewnętrzny prowadzi:

- 1) audytor wewnętrzny **zatrudniony w jednostce** albo
- 2) usługodawca **niezatrudniony w jednostce**, zwany dalej "usługodawcą",

Zewnętrzny usługodawca tylko przy zachowaniu określonych warunków – może nim być:

- **osoba fizyczna**, spełniająca warunki wymienione w ustawie, np. posiadająca określone certyfikaty kwalifikacji, w tym także biegły rewident,
- **spółka cywilna, spółka jawna, spółka partnerska, spółka komandytowa, spółka komandytowo-akcyjna lub osoba prawna**, która zatrudnia do prowadzenia audytu wewnętrznego w jednostce osoby z odpowiednimi uprawnieniami.

art. 37 ust. 6 RODO:

Inspektor ochrony danych może być **członkiem personelu administratora danych** lub przetwarzającego lub **wykonywać zadania na podstawie umowy o świadczenie usług.**

NIEZALEŻNOŚĆ IOD

Urząd
Ochrony
Danych
Osobowych



Motyw 97 RODO inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób **niezależny**.

NIEZALEŻNOŚĆ AUDYTORA WEWNĘTRZNEGO

Urząd
Ochrony
Danych
Osobowych



art. 282 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,

kierownik jednostki musi zapewnić audytorowi wewnętrznemu warunki niezbędne do niezależnego, obiektywnego i efektywnego prowadzenia audytu wewnętrznego,

w tym organizacyjnej odrębności komórki audytu wewnętrznego oraz ciągłości prowadzenia audytu wewnętrznego w jednostce.

UMIEJSCOWIENIE W STRUKTURZE ORGANIZACYJNEJ

Urząd
Ochrony
Danych
Osobowych



Art. 280. ufp **Kierownik komórki audytu wewnętrznego podlega bezpośrednio kierownikowi jednostki**, a w urzędzie administracji rządowej, w którym tworzy się stanowisko dyrektora generalnego urzędu - dyrektorowi generalnemu w zakresie określonym odrębnymi ustawami.

Art. 38 ust. 3 RODO **Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.**

DOSTĘP DO INFORMACJI



Art. 282 ust. 2 ufp Audytor wewnętrzny **ma 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.

ust. 3 **Pracownicy jednostki są obowiązani udzielać informacji i wyjaśnień**, a także sporządzać i potwierdzać kopie, odpisy, wyciągi lub zestawienia, o których mowa w ust. 2.

DOSTĘP DO INFORMACJI



Art. 38 ust 1 RODO Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był **właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.**

Art. 38 ust 2 RODO Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, 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.

WARUNKI DO PEŁNIENIA FUNKCJI, W TYM ODPOWIEDNIE KWALIFIKACJE ZAWODOWE (WIEDZA)

Urząd
Ochrony
Danych
Osobowych



Art. 286 ufp

1. Audytorem wewnętrznym może być osoba, która:

- 1) ma **obywatelstwo państwa członkowskiego Unii Europejskiej** lub **innego państwa**, którego **obywatelom**, na podstawie umów międzynarodowych lub przepisów prawa wspólnotowego, przysługuje prawo **podjęcia zatrudnienia na terytorium Rzeczypospolitej Polskiej**;
- 2) ma pełną **zdolność do czynności** prawnych oraz korzysta z pełni praw publicznych;
- 3) **nie była karana za umyślne przestępstwo lub umyślne przestępstwo skarbowe**;
- 4) posiada **wyższe wykształcenie**;

C.D. ODPOWIEDNIE KWALIFIKACJE ZAWODOWE (WIEDZA) ART. 286 UFP

Urząd
Ochrony
Danych
Osobowych



5) posiada następujące kwalifikacje do przeprowadzania audytu wewnętrznego:

a) **jeden z certyfikatów:** Certified Internal Auditor (CIA), Certified Government Auditing Professional (CGAP), Certified Information Systems Auditor (CISA), Association of Chartered Certified Accountants (ACCA), Certified Fraud Examiner (CFE), Certification in Control Self Assessment (CCSA), Certified Financial Services Auditor (CFSA) lub Chartered Financial Analyst (CFA), lub

b) złożyła, **w latach 2003-2006**, z wynikiem pozytywnym **egzamin na audytora wewnętrznego** przed Komisją Egzaminacyjną powołaną przez Ministra Finansów,

c) **uprawnienia biegłego rewidenta,**

d) **dwuletnią praktykę w zakresie audytu wewnętrznego i legitymuje się dyplomem ukończenia studiów podyplomowych w zakresie audytu wewnętrznego**, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi ustawami, do nadawania stopnia naukowego doktora nauk ekonomicznych lub prawnych.

KWALIFIKACJE DO PEŁNIENIA FUNKCJI -KRYTERIA WYBORU ODPOWIEDNIEGO IOD

Urząd
Ochrony
Danych
Osobowych



Art. 37 ust. 5 RODO **Inspektor ochrony danych** jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności **wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.**

Wytyczne Grupy Roboczej art. 29 dotyczące inspektorów ochrony danych
Istotne jest, by IOD posiadał odpowiednią wiedzę z zakresu krajowych, europejskich oraz sektorowych **przepisów oraz praktyk** w zakresie ochrony danych osobowych oraz **dogłębną znajomość RODO.**

Jednocześnie powinien posiadać odpowiednią wiedzę na temat:

- procesów przetwarzania, systemów informatycznych oraz zabezpieczeń stosowanych u administratora,
- sektora, w którym działa administrator,
- procedur administracyjnych i funkcjonowania jednostki.



OCHRONA TRWAŁOŚCI STOSUNKU PRACY

art. 38 ust. 3 RODO

Inspektor **nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.**

Art. 281 ufp [Ochrona stosunku pracy kierownika komórki audytu wewnętrznego]

Rozwiązanie stosunku pracy ani zmiana warunków płacy i pracy kierownika komórki audytu wewnętrznego ministerstwa oraz jednostki w dziale nie może nastąpić bez zgody właściwego komitetu audytu.

USTAWA Z DNIA 14 GRUDNIA 2018 R. WYZNACZENIE IOD - JAKI WARUNKI MUSI SPEŁNIAĆ OSOBA WYZNACZONA?

Art. 46 ust. 2

Inspektorem ochrony danych może być osoba, która:

- 1) **ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;**
- 2) posiada odpowiednie kwalifikacje zawodowe, w szczególności **wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych**, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;
- 3) **nie była skazana prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.**

USTAWA Z DNIA 14 GRUDNIA 2018 R. WYZNACZENIE IOD - JAKI WARUNKI MUSI SPEŁNIAĆ OSOBA WYZNACZONA? – WIEDZA I UMIEJĘTNOŚCI

Co oznacza że IOD ma posiadać odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;

Poziom wiedzy fachowej należy ustalać zwłaszcza **w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora (motyw 63 dyrektywy)**.

IOD wyznaczeni przez administratorów podlegających dyrektywie policyjnej powinny zatem posiadać wiedzę w zakresie ochrony, której wymagają dane osobowe przetwarzane w związku z zapobieganiem i zwalczaniem przestępczości.

ZAKAZ WYDAWANIA INSTRUKCJI ORAZ NAKŁADANIA NA IOD ZADAŃ MOGĄCYCH PROWADZIĆ DO KONFLIKTU INTERESÓW

Urząd
Ochrony
Danych
Osobowych



Art. 38 ust. 3 RODO Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych **nie otrzymywał instrukcji dotyczących wykonywania tych zadań.**

Wytyczne grupy Roboczej art. 29 dotyczące inspektorów ochrony danych
Zakaz ten odnosi się np. do poleceń dotyczących sposobu załatwienia sprawy, środków jakie mają zostać podjęte, czy też celu jaki powinien zostać osiągnięty.

Art. 38 ust 6 RODO Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały **konfliktu interesów.**

ROZPORZĄDZENIE MF W SPRAWIE AUDYTU WEWNĘTRZNEGO ORAZ INFORMACJI O PRACY I WYNIKACH TEGO AUDYTU

Urząd
Ochrony
Danych
Osobowych



§ 23. Audytor wewnętrzny **powstrzymuje się od wykonywania czynności doradczych, które prowadziłyby do przyjęcia przez niego obowiązków, odpowiedzialności lub uprawnień wchodzących w zakres zarządzania jednostką, i informuje o tym kierownika jednostki.**

**CELEM DZIAŁALNOŚCI CZYNNOŚCI DORADCZE
I SYSTEMATYCZNA OCENA (MONITOROWANIE)
DZIAŁALNOŚCI PODMIOTU
I UWZGLĘDNIANIE RYZYKA**

Urząd
Ochrony
Danych
Osobowych



Art. 39 ust 1

Inspektor ochrony danych ma następujące zadania:

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

2. Inspektor ochrony danych wypełnia swoje zadania **z należytym uwzględnieniem ryzyka** związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

ART. 272 UFP POJĘCIE AUDYTU WEWNĘTRZNEGO

Urząd
Ochrony
Danych
Osobowych



1. Audyt wewnętrzny jest działalnością **niezależną i obiektywną**, której celem jest **wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań** przez systematyczną **ocenę kontroli zarządczej oraz czynności doradcze**.
2. **Ocena**, o której mowa w ust. 1, **dotyczy w szczególności adekwatności, skuteczności i efektywności kontroli zarządczej** w dziale administracji rządowej lub jednostce.

ART. 68. POJĘCIE I CELE KONTROLI ZARZĄDCZEJ



1. Kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy.
2. Celem kontroli zarządczej jest zapewnienie w szczególności:
 - 1) **zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;**
 - 2) **skuteczności i efektywności** działania;
 - 3) wiarygodności sprawozdań;
 - 4) **ochrony zasobów;**
 - 5) przestrzegania i promowania zasad **etycznego postępowania;**
 - 6) **efektywności i skuteczności przepływu informacji;**
 - 7) **zarządzania ryzykiem.**

CECHY WSPÓLNE



- obowiązek wyznaczenia dla jednostek sektora finansów publicznych
- wykonywanie zadań jako członek personelu lub na podstawie umowy o wykonywanie usług
- niezależność (*gwarancje niezależności*)
- bezpośrednia podległość najwyższemu kierownictwu
- dostęp do informacji
- odpowiednie kwalifikacje zawodowe (wiedza)
- celem działalności czynności doradcze i systematyczna ocena (monitorowanie) działalności podmiotu
- kryteriami oceny jest m.in. zgodność z prawem i efektywność
- wykonywanie zadań z uwzględnieniem ryzyka



Dlaczego warto łączyć funkcję audytora wewnętrznego i inspektora ochrony danych?



- deficyt fachowych kadr – potrzeby administratorów
- wysokie kwalifikacje i doświadczenie audytorów wewnętrznych
- w wielu jednostkach może się to okazać racjonalnym, mniej kosztownym rozwiązaniem (mniejsze jednostki)
- podejście systemowe - spójność i efektywność systemu zapewniania zgodności z prawem
- skupienie obu podobnych obszarów w jednym ręku może się przyczyniać do bardziej efektywnego wykonywania tych funkcji
- co do zasady brak konfliktu interesów (ryzyko przeciążenia!)
- perspektywy rozwoju doświadczenia i kwalifikacji
- brak rywalizacji



Co może przemawiać za rozdzieleniem funkcji audytora wewnętrznego i inspektora ochrony danych?

ROZDZIELENIE FUNKCJI IOD I AUDYTORA WEWNĘTRZNEGO



- Rozmiary jednostki oraz złożoność jej struktury organizacyjnej
- Ilość zadań (konflikt interesów)



Rozważając wyznaczenie na IOD kierownika komórki w organizacji lub innej osoby, powinno się uwzględnić, co najmniej trzy kryteria:

- **organizacyjne** (IOD powinien podlegać bezpośrednio najwyższemu kierownictwu jednostki organizacyjnej),
- **merytoryczne** (inne obowiązki nie powinny negatywnie wpływać na niezależne wykonywanie zadań IOD),
- **czasowe** (IOD powinien dysponować czasem wystarczającym do wykonywania swoich zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania).

KRYTERIUM CZASOWE



- Należy przemyśleć ilość czasu potrzebnego na wykonywanie **poszczególnych obowiązków** (w tym na współpracę z innymi służbami kontrolnymi), **stopień skomplikowania i ważności zadań**, rezerwę czasową na **nieplanowane zadania**, **ilość i rodzaj danych osobowych** oraz **procesów i systemów informatycznych** służących do ich przetwarzania, **obszary ryzyka**, związane z tymi procesami. Pod rozwagę należy brać również wiele innych czynników, takich jak np. **struktura, wielkość i zasoby kadrowe danego podmiotu** (w tym również pod kątem obowiązku prowadzenia szkoleń personelu).
- W szczególności, w **przypadku IOD zatrudnionego w niepełnym wymiarze czasu pracy, albo łączącego obowiązki IOD z innymi zadaniami**, priorytetem powinno być zapewnienie IOD odpowiedniej ilości czasu na wykonywanie powierzonych zadań.



Współpraca inspektorów z audytorami wewnętrznymi jednostek sektora finansów publicznych



SIERPIEŃ 2018 R.

» Aktualności

Zasady współpracy audytora wewnętrznego i IOD określone przez Ministerstwo Finansów i Prezesa UODO

Zadaniem zarówno inspektora ochrony danych, jak i audytora wewnętrznego jest wspieranie kierownika jednostki sektora finansów publicznych w zgodnej z prawem realizacji celów i zadań tej jednostki. Dlatego działania audytorów wewnętrznych i inspektorów ochrony danych powinny być komplementarne.

Działający w jednostkach sektora finansów publicznych inspektor ochrony danych (IOD) i audytor wewnętrzny to dwie ważne osoby wspierające kierownictwo jednostki w zgodnej z prawem realizacji jej celów i zadań. Obie są niezależne w wykonywaniu swoich obowiązków, które niekiedy są zbieżne. Dlatego tak ważne jest, by właściwie rozumieć ich rolę i odpowiednio ułożyć wzajemne relacje.





- Obie funkcje są niezależne w wykonywaniu swoich obowiązków, które niekiedy są zbieżne.
- Dlatego tak ważne jest, by **właściwie rozumieć ich rolę i odpowiednio ułożyć wzajemne relacje.**

KONIECZNOŚĆ ZAPEWNIENIA NIEZALEŻNEGO WYKONYWANIA ZADAŃ



- bezpośrednia 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.

- bezpośrednią podległość kierownika komórki audytu wewnętrznego kierownikowi jednostki,
- ochronę stosunku pracy
- prawo wstępu do pomieszczeń jednostki oraz wglądu do wszelkich dokumentów, informacji i danych
- zobowiązanie pracowników jednostki do udzielania informacji i wyjaśnień, a także sporządzania i potwierdzania kopii, odpisów, wyciągów lub zestawień niezbędnych do realizacji audytu.

KONIECZNOŚĆ ZAPEWNIENIA NIEZALEŻNEGO WYKONYWANIA ZADAŃ



Zgodnie ze standardami audytu wewnętrznego dla jednostek sektora finansów publicznych, określonymi w [Komunikacie Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych](#), **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.

WSPÓŁPRACA JEST NIEZBĘDNA – PODOBNE CELE OBU FUNKCJI

Urząd
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 jej celów i zadań w zakresie” **oceny (monitorowania) 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.**

WYMIANA INFORMACJI I POSZANOWANIE NIEZALEŻNOŚCI



- 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. **Ich praca może podlegać jego kontroli, w tym tej zleconej 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 uwzględniać wzajemną niezależność i nie wpływać na jej ograniczanie**.

GDY AUDYT OBEJMUJE ZADANIA REALIZOWANE PRZEZ IOD - OSTATECZNA DECYZJA NALEŻY DO KIEROWNIKA JEDNOSTKI



- Sposób przeprowadzania audytu wewnętrznego został określony w przepisach rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu. **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.

PODSUMOWANIE



- 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.
- W osiągnięciu tego celu potrzebna jest ich efektywna współpraca oraz wzajemne wspieranie się w tym zakresie wiedzą i doświadczeniem.

Urząd
Ochrony
Danych
Osobowych



Dziękuję za uwagę!

Urząd Ochrony Danych
Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl