



## Inspektor Ochrony Danych (IOD) w sektorze medycznym – ochrona danych zdrowotnych w praktyce podmiotów leczniczych.

Numer usługi 2026/03/24/175921/3433351

2 337,00 PLN brutto

1 900,00 PLN netto

389,50 PLN brutto/h

316,67 PLN netto/h

177,78 PLN cena rynkowa ⓘ

Centrum

Szkoleniowe LDM

Roksana Michalska

★★★★★ 4,8 / 5

10 ocen

🏠 Usługa szkoleniowa

📺 zdalna

🕒 06:00 h

📅 08.05.2026 do 22.05.2026

## Informacje podstawowe

Kategoria

Prawo i administracja / Prawo ogólne

Grupa docelowa usługi

Grupa docelowa:

- Inspektorzy Ochrony Danych pełniący funkcję w podmiotach leczniczych lub planujący wejście do sektora medycznego
- Dyrektorzy szpitali, przychodni, centrów medycznych i innych podmiotów leczniczych
- Kadra zarządzająca i administracyjna ochrony zdrowia (kierownicy rejestracji, działu kadr, IT, compliance)
- Personel IT i specjaliści ds. bezpieczeństwa w placówkach medycznych
- Osoby przygotowujące się do objęcia funkcji IOD w sektorze ochrony zdrowia

Szkolenie skierowane zarówno do klientów indywidualnych, jak i do firm oraz instytucji (podmioty lecznicze, szpitale, przychodnie, centra medyczne).

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

06-05-2026

Forma prowadzenia usługi

zdalna

Liczba godzin usługi

6

Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

# Cel

## Cel edukacyjny

Celem szkolenia jest kompleksowe przygotowanie uczestników do samodzielnego i skutecznego pełnienia funkcji Inspektora Ochrony Danych w podmiotach leczniczych – szpitalach, przychodniach, centrach medycznych oraz innych jednostkach systemu ochrony zdrowia.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<b>WIEDZA:</b> Uczestnik zna przepisy RODO w kontekście przetwarzania danych zdrowotnych oraz regulacje sektorowe (ustawa o prawach pacjenta, ustawa o działalności leczniczej, ustawa o systemie informacji w ochronie zdrowia)	Uczestnik wskazuje właściwe przepisy dla konkretnych scenariuszy przetwarzania danych w podmiocie leczniczym, rozróżnia podstawy prawne z art. 6 i art. 9 RODO oraz identyfikuje przepisy krajowe uzupełniające	Test teoretyczny
<b>WIEDZA:</b> Uczestnik rozumie specyfikę danych szczególnych kategorii (dane zdrowotne, genetyczne, biometryczne) i zasady ich przetwarzania w placówkach medycznych	Uczestnik poprawnie klasyfikuje rodzaje danych przetwarzanych w podmiocie leczniczym, wskazuje dopuszczalne podstawy z art. 9 ust. 2 RODO oraz opisuje obowiązki wynikające z ich przetwarzania	Test teoretyczny
<b>WIEDZA:</b> Uczestnik zna zasady prowadzenia elektronicznej dokumentacji medycznej (EDM) oraz wymogi prawne dotyczące jej przechowywania, udostępniania i zabezpieczenia	Uczestnik opisuje wymagany okres retencji dokumentacji medycznej, wskazuje zasady dostępu do EDM, formy udostępniania uprawnionym podmiotom oraz obowiązki wynikające z ustawy o prawach pacjenta	Test teoretyczny
<b>WIEDZA:</b> Uczestnik zna obowiązki IOD w podmiocie leczniczym, w tym zakres współpracy z PUODO, NFZ oraz innymi organami nadzorczymi systemu ochrony zdrowia	Uczestnik wymienia zadania IOD z art. 39 RODO, opisuje zakres niezależności funkcji IOD w podmiocie medycznym oraz wskazuje sytuacje wymagające zgłoszenia do organu nadzorczego	Test teoretyczny
<b>WIEDZA:</b> Uczestnik zna zasady korzystania z systemów teleinformatycznych w ochronie zdrowia (HIS, LIS, PACS, e-recepta, e-skierowanie, platforma P1) pod kątem ochrony danych osobowych	Uczestnik wskazuje ryzyka związane z poszczególnymi systemami, opisuje wymagania dla umów powierzenia z dostawcami IT oraz zna zasady zarządzania dostępem do systemów klinicznych	Test teoretyczny
<b>WIEDZA:</b> Uczestnik zna procedury zgłaszania naruszeń ochrony danych osobowych w podmiocie leczniczym, w tym incydentów dotyczących dokumentacji medycznej	Uczestnik opisuje terminy i kryteria zgłaszania naruszeń do PUODO (72h), wskazuje obowiązek powiadomienia pacjentów w przypadku naruszeń wysokiego ryzyka oraz zna wewnętrzne procedury rejestracji incydentów	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p><b>UMIEJĘTNOŚCI:</b>            Uczestnik potrafi przygotować i wdrożyć dokumentację RODO dostosowaną do podmiotu leczniczego (polityka ochrony danych, rejestr czynności przetwarzania, klauzule informacyjne dla pacjentów)</p>	<p>Uczestnik opracowuje dokumenty uwzględniające specyfikę medyczną: właściwe podstawy z art. 9 RODO, okresy przechowywania dokumentacji medycznej, prawa pacjentów wynikające z ustawy o prawach pacjenta</p>	<p>Wywiad swobodny</p>
<p><b>UMIEJĘTNOŚCI:</b>            Uczestnik potrafi wdrożyć procedury obsługi praw pacjentów w zakresie ochrony danych (dostęp, sprostowanie, usunięcie, ograniczenie, sprzeciw) z uwzględnieniem ograniczeń prawa medycznego</p> <p><b>UMIEJĘTNOŚCI:</b>            Uczestnik potrafi weryfikować umowy powierzenia z podmiotami zewnętrznymi (laboratoria, firmy IT, podmioty lecznicze współpracujące) i identyfikować relacje powierzenia vs. udostępnienia danych</p>	<p>Uczestnik rozróżnia prawa z RODO od praw z ustawy o prawach pacjenta, wskazuje przypadki, gdy realizacja praw jest ograniczona przepisami sektorowymi (np. zakaz usunięcia dokumentacji medycznej)</p> <p>Uczestnik ocenia, kiedy relacja z podmiotem zewnętrznym wymaga umowy powierzenia (art. 28 RODO), a kiedy stanowi udostępnienie; wskazuje obowiązkowe elementy umów w kontekście medycznym</p>	<p>Wywiad swobodny</p> <p>Wywiad swobodny</p>
<p><b>KOMPETENCJE SPOŁECZNE:</b>            Uczestnik potrafi skutecznie komunikować wymagania RODO personelowi medycznemu, administracyjnemu i kierownictwu podmiotu leczniczego</p> <p><b>KOMPETENCJE SPOŁECZNE:</b>            Uczestnik wykazuje zdolność do zachowania niezależności IOD i zarządzania konfliktami interesów w środowisku podmiotu leczniczego, gdzie presja operacyjna może kolidować z wymogami ochrony danych</p>	<p>Uczestnik formułuje zalecenia w języku zrozumiałym dla lekarzy, pielęgniarek i rejestratorek, potrafi wyjaśnić konsekwencje naruszeń bez wywoływania nieuzasadnionego lęku i buduje kulturę ochrony danych w organizacji</p> <p>Uczestnik wskazuje sytuacje potencjalnych konfliktów interesów w placówce medycznej oraz opisuje sposoby zachowania niezależności IOD przy jednoczesnym wspieraniu działalności leczniczej, nie blokując procesów niezbędnych dla bezpieczeństwa pacjentów</p>	<p>Wywiad swobodny</p> <p>Wywiad swobodny</p>
<p><b>KOMPETENCJE SPOŁECZNE:</b>            Uczestnik potrafi śledzić zmiany prawne i technologiczne istotne dla ochrony danych w ochronie zdrowia (dyrektywa NIS2, rozporządzenie EHDS) i aktualizować wiedzę</p>	<p>Uczestnik identyfikuje kluczowe źródła informacji o zmianach prawnych (UODO, EDPB, MZ), potrafi ocenić wpływ nowych regulacji na funkcjonowanie podmiotu leczniczego i zaplanować działania dostosowawcze</p>	<p>Wywiad swobodny</p>

## Kwalifikacje

### Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

## Program

### Program ramowy szkolenia

Temat szkolenia / moduł
Przepisy RODO – zastosowanie w ochronie zdrowia (art. 6, art. 9, art. 35, art. 37–39)
Ustawy sektorowe: ustawa o prawach pacjenta, o działalności leczniczej, o systemie informacji w ochronie zdrowia
Tajemnica lekarska, zawodowa i bankowa a RODO – kolizje norm i sposoby ich rozwiązywania
Odpowiedzialność cywilna, administracyjna i karna za naruszenia danych w ochronie zdrowia
Obowiązek wyznaczenia IOD – kiedy jest obowiązkowy, a kiedy dobrowolny
Pozycja IOD w strukturze organizacyjnej: niezależność, konflikt interesów, dostęp do zasobów
Plan pracy IOD, audyty, przeglądy ryzyka i raportowanie do kierownictwa podmiotu
Matryca ról w placówce medycznej: administrator, podmiot przetwarzający, współadministrator
Polityka ochrony danych i polityki szczegółowe dla podmiotu leczniczego
Rejestr Czynności Przetwarzania Danych (RCPD) i Rejestr Kategorii Czynności Przetwarzania (RKCP)

Podstawy prawne przetwarzania, zgody pacjentów i klauzule informacyjne

Dokumentacja medyczna – udostępnianie, retencja (okresy przechowywania) i zabezpieczenie

Prawa pacjenta w świetle RODO i ustawy o prawach pacjenta – realizacja żądań

Standardy nazewnictwa, klasyfikacja informacji i komitet ds. prywatności i bezpieczeństwa

Metodologia analizy ryzyka dla podmiotów leczniczych – aktywna i procesowa ocena zagrożeń

Ocena skutków dla ochrony danych (DPIA) – obowiązek, metodyka, dokumentowanie

Systemy IT i integracje w ochronie zdrowia: HIS, LIS, PACS, RIS – specyfika i ryzyka

Platforma e-Zdrowie (P1) i CeZ: e-recepta, e-skierowanie, EDM – obowiązki IOD

Telemedycyna i opieka zdalna – specyfika przetwarzania danych, wymogi prawne

Sztuczna inteligencja i algorytmy diagnostyczne w medycynie – DPIA i przejrzystość

Cyberbezpieczeństwo i ciągłość działania w podmiocie leczniczym (NIS2)

Bezpieczeństwo fizyczne i monitoring w szpitalu/przychodni

Dostawcy i umowy powierzenia – weryfikacja, klauzule RODO, rejestr umów

Współadministracja i grupy kapitałowe w ochronie zdrowia

HR w placówce medycznej – dane pracowników, badania medycyny pracy, upoważnienia

Badania naukowe i dydaktyka – przetwarzanie danych w celach naukowych (art. 89 RODO)

Komunikacja i PR – wizerunek placówki, media społecznościowe, dane pracowników publicznych

Front desk i operacje kliniczne – punkty wycieku danych w codziennej pracy rejestracji

Incydenty i naruszenia ochrony danych – procedura reagowania (72h), rejestr, powiadomienia

Audyty i kontrole PUODO, NFZ i kontrole wewnętrzne – przygotowanie i obsługa

Retencja, minimalizacja i porządek organizacyjny – praktyczne wdrożenie

Metryki i dashboard IOD – raportowanie skuteczności ochrony danych

Warsztaty praktyczne – case studies i ćwiczenia na dokumentach (klauzule, RCP, DPIA)

Szkolenie opracowane przez: Mariusza Kanię – eksperta z 10-letnim doświadczeniem jako czynny Inspektor Ochrony Danych

Kwalifikacje i certyfikaty:

- CIPP/E (Certified Information Privacy Professional/Europe) – międzynarodowy certyfikat potwierdzający zaawansowaną wiedzę z zakresu europejskiego prawa ochrony danych
- CIPT (Certified Information Privacy Technologist) – certyfikat potwierdzający kompetencje w zakresie technicznych aspektów ochrony prywatności
- CIPM (Certified Information Privacy Manager) – certyfikat specjalisty ds. zarządzania programami ochrony prywatności

Doświadczenie praktyczne:

- 10 lat pracy jako IOD w jednostkach samorządowych, placówkach oświatowych oraz podmiotach medycznych
- Kompleksowa obsługa zgodności z RODO dla dziesiątek organizacji z sektora publicznego i prywatnego
- Przeprowadzanie audytów RODO, wdrażanie systemów ochrony danych, szkolenia dla kadry zarządzającej i pracowników
- Specjalizacja w obszarze ISO 27001, audytów dostępności cyfrowej oraz cyberbezpieczeństwa
- Prowadzenie szkoleń dla pracowników samorządów terytorialnych z zakresu wykorzystania AI w administracji publicznej
- Współpraca z Polskim Centrum Bezpieczeństwa i Prewencji jako trener i konsultant ds. RODO

Mariusz Kania łączy wiedzę prawniczą z praktycznym doświadczeniem wdrożeniowym, dzięki czemu szkolenie ma charakter aplikacyjny – uczestnicy otrzymują nie tylko teorię, ale przede wszystkim narzędzia i procedury gotowe do wdrożenia w swoich organizacjach.

**Szczegółowe cele szkolenia:**

- Przekazanie specjalistycznej wiedzy z zakresu RODO i przepisów sektorowych regulujących przetwarzanie danych zdrowotnych (ustawa o prawach pacjenta, ustawa o działalności leczniczej, ustawa o systemie informacji w ochronie zdrowia)
- Wykształcenie umiejętności zaprojektowania i prowadzenia systemu ochrony danych osobowych dostosowanego do specyfiki podmiotów leczniczych
- Przygotowanie do przeprowadzania analizy ryzyka i oceny skutków dla ochrony danych (DPIA) w procesach medycznych i klinicznych
- Nabycie praktycznych umiejętności w zakresie zarządzania dokumentacją medyczną (EDM) pod kątem RODO: udostępnianie, retencja, zabezpieczenie
- Przygotowanie do reagowania na incydenty bezpieczeństwa i naruszenia ochrony danych w środowisku klinicznym
- Zrozumienie relacji IOD z organami nadzorczymi (PUODO, NFZ), pacjentami i personelem medycznym
- Zapoznanie z nowoczesnymi wyzwaniami technologicznymi (telemedycyna, platforma e-Zdrowie P1, sztuczna inteligencja w medycynie)

## Cennik

**Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT**

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 337,00 PLN
Koszt przypadający na 1 uczestnika netto	1 900,00 PLN
Koszt osobogodziny brutto	389,50 PLN

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

- Materiały wideo z lektorem – 35 modułów (ponad 220 slajdów), dostęp 24/7
- Nielimitowana liczba odtworzeń przez cały okres dostępu (6 miesięcy)
- Możliwość pauzowania, wznawiania i powtarzania każdego modułu
- Nauka w dowolnym miejscu i czasie (komputer, tablet, telefon)
- Certyfikat oraz komplet dokumentacji RODO po ukończeniu szkolenia
- Miesięczny dostęp do platformy wsparcia dla IOD z ekspertami PCBiP

### Warunki uczestnictwa

Brak formalnych wymagań. Szkolenie dedykowane jest przede wszystkim osobom posiadającym podstawową znajomość przepisów RODO (np. po szkoleniu ogólnym z zakresu IOD). Dla osób bez wcześniejszego doświadczenia zalecane jest ukończenie kursu „Zostań IOD – od podstaw” przed przystąpieniem do niniejszego szkolenia specjalistycznego.

### Informacje dodatkowe

**Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT.**

Szkolenie prowadzone jest w formie kursu e-learningowego na platformie internetowej. Uczestnicy uzyskują dostęp do 35 modułów tematycznych z lektorem przez 6 miesięcy od aktywacji.

## Warunki techniczne

Każdy uczestnik szkolenia musi mieć możliwość korzystania z komputera z dostępem do Internetu.

## Kontakt



**ROKSANA MICHALSKA**

**E-mail** [r.michalska@ldmszkolenia.pl](mailto:r.michalska@ldmszkolenia.pl)

**Telefon** (+48) 660 079 541