Możliwość dofinansowania

Inspektor Ochrony Danych (IOD) - szkolenie kompleksowe od podstaw

Numer usługi 2026/03/24/175921/3431329

5 166,00 PLN brutto
4 200,00 PLN netto
20,66 PLN brutto/h
16,80 PLN netto/h
210,56 PLN cena rynkowa

Centrum Szkoleniowe LDM
Roksana Michalska

4,8 / 5
10 ocen

Usługa szkoleniowa
zdalna
250:00 h
08.06.2026 do 08.06.2027

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo pozostałe
Grupa docelowa usługi	Odbiorcy szkolenia: • Pracownicy administracji publicznej (samorządy, urzędy) • Kadra placówek oświatowych (szkoły, przedszkola, uczelnie) • Pracownicy podmiotów medycznych (szpitale, przychodnie, NZOZ) • Specjaliści z firm prywatnych odpowiedzialni za compliance i ochronę danych • Klienci indywidualni planujący rozwój kariery w obszarze RODO **Szkolenie skierowane jest zarówno do firm, jak i klientów indywidualnych.** **Dla kogo ta forma szkolenia:** Idealna dla osób pracujących, które potrzebują elastyczności w nauce i chcą pogodzić rozwój zawodowy z obowiązkami służbowymi i życiem prywatnym. Szczególnie polecane dla pracowników administracji publicznej, placówek oświatowych i medycznych, którzy mogą uczyć się w dogodnych dla siebie momentach.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	05-06-2026
Forma prowadzenia usługi	zdalna
Liczba godzin usługi	250
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

Usługa szkoleniowa kompleksowo przygotowuje uczestników do samodzielnego wykonywania zadań z zakresu ochrony danych osobowych oraz do pełnienia funkcji Inspektora Ochrony Danych zgodnie z wymogami rozporządzenia RODO oraz polskiej ustawy o ochronie danych osobowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik definiuje przepisy RODO, ustawy o ochronie danych osobowych oraz akty wykonawcze	Uczestnik poprawnie identyfikuje podstawy prawne przetwarzania danych	Test teoretyczny
	Uczestnik definiuje obowiązki administratora i właściwe przepisy dla konkretnych sytuacji	Test teoretyczny
WIEDZA: Uczestnik rozróżnia zasady wyznaczania i funkcjonowania IOD w organizacji	Uczestnik definiuje zakres obowiązków, zadań i pozycję IOD w strukturze organizacyjnej	Test teoretyczny
	Uczestnik definiuje wymogi dotyczące kwalifikacji i niezależności	Test teoretyczny
WIEDZA: Uczestnik charakteryzuje metodologię przeprowadzania audytów zgodności z RODO	Uczestnik rozróżnia etapy audytu	Test teoretyczny
	Uczestnik definiuje obszary wymagające weryfikacji przy pomocy narzędzi audytorskich	Test teoretyczny
WIEDZA: Uczestnik charakteryzuje zasady prowadzenia rejestru czynności przetwarzania i innej dokumentacji RODO	Uczestnik definiuje elementy obowiązkowe rejestru i różnice między dokumentacją administratora oraz podmiotu przetwarzającego	Test teoretyczny
WIEDZA: Uczestnik charakteryzuje procedury zgłaszania naruszeń ochrony danych osobowych	Uczestnik definiuje terminy i wymogi formalne zgłoszeń do UODO oraz informowania osób, których dane dotyczą	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik analizuje zgodności przetwarzania danych z RODO	Uczestnik samodzielnie identyfikuje nieprawidłowości w procesach przetwarzania	Obserwacja w warunkach symulowanych
	Uczestnik proponuje działania naprawcze	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
UMIEJĘTNOŚCI: Uczestnik opracowuje politykę bezpieczeństwa danych i procedury RODO	Uczestnik projektuje dokumenty dostosowane do specyfiki organizacji, uwzględniając jej wielkość, branżę i ryzyko	Obserwacja w warunkach symulowanych
UMIEJĘTNOŚCI: Uczestnik przeprowadza ocenę skutków dla ochrony danych (DPIA)	Uczestnik rozróżnia operacje wymagające DPIA	Test teoretyczny
	Uczestnik analizuje ryzyko	Obserwacja w warunkach symulowanych
	Uczestnik proponuje środki minimalizujące ryzyko	Obserwacja w warunkach symulowanych
UMIEJĘTNOŚCI: Uczestnik obsługuje żądania osób, których dane dotyczą	Uczestnik prawidłowo reaguje na żądania dostępu, sprostowania, usunięcia, ograniczenia przetwarzania i przenoszenia danych	Obserwacja w warunkach symulowanych
UMIEJĘTNOŚCI: Uczestnik prawidłowo reaguje na incydenty bezpieczeństwa i naruszenia danych	Uczestnik stosuje właściwe procedury wykrywania, dokumentowania i zgłaszania naruszeń w wymaganych terminach	Obserwacja w warunkach symulowanych
UMIEJĘTNOŚCI: Uczestnik prowadzi szkolenia z zakresu ochrony danych osobowych	Uczestnik planuje działania szkoleniowe dostosowane do potrzeb różnych grup pracowników	Obserwacja w warunkach symulowanych
	Uczestnik realizuje działania szkoleniowe dostosowane do potrzeb różnych grup pracowników	Obserwacja w warunkach symulowanych
	Uczestnik formułuje jasne zalecenia jako ekspert ds. ochrony danych	Test teoretyczny
KOMPETENCJE SPOŁECZNE: Uczestnik skutecznie komunikuje się z zarządem, pracownikami i podmiotami zewnętrznymi w sprawach RODO	Uczestnik argumentuje stanowisko jako ekspert ds. ochrony danych	Test teoretyczny
	Uczestnik buduje zaufanie jako ekspert ds. ochrony danych	Obserwacja w warunkach symulowanych
KOMPETENCJE SPOŁECZNE: Uczestnik podejmuje samodzielne decyzje w złożonych sytuacjach prawnych	Uczestnik prezentuje pewność w interpretacji przepisów	Obserwacja w warunkach symulowanych
	Uczestnik broni swoje stanowisko merytoryczne	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETENCJE SPOŁECZNE: Uczestnik formułuje znaczenie etyki i odpowiedzialności w pracy IOD	Uczestnik wykazuje świadomość konsekwencji naruszeń prywatności	Test teoretyczny
	Uczestnik dba o prawa osób, których dane dotyczą	Obserwacja w warunkach symulowanych
KOMPETENCJE SPOŁECZNE: Uczestnik współpracuje z organem nadzorczym (UODO)	Uczestnik charakteryzuje zasady komunikacji z UODO	Test teoretyczny
	Uczestnik przygotowuje wyjaśnienia i dokumentację na potrzeby kontroli	Obserwacja w warunkach symulowanych
KOMPETENCJE SPOŁECZNE: Uczestnik planuje swój rozwój poprzez aktualizację wiedzy w dynamicznie zmieniającym się obszarze privacy	Uczestnik analizuje zmiany legislacyjne, orzecznictwo i najlepsze praktyki w ochronie danych osobowych	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

MODUŁ 1: Podstawy prawne ochrony danych osobowych

- - Ewolucja prawa do prywatności i ochrony danych osobowych
  - RODO – struktura, zakres, zasady i definicje kluczowe
  - Ustawa o ochronie danych osobowych – przepisy krajowe
  - Orzecznictwo TSUE i praktyka UODO
  - Relacja RODO z innymi aktami prawnymi (Kodeks pracy, ustawa o świadczeniu usług drogą elektroniczną, itp.)

MODUŁ 2: Zasady przetwarzania danych osobowych

- Sześć zasad przetwarzania danych (art. 5 RODO)
- Podstawy prawne przetwarzania – analiza przypadków
- Zgoda jako podstawa przetwarzania – wymogi i wycofanie
- Prawnie uzasadniony interes administratora (LIA)
- Minimalizacja danych i privacy by design
- Okres przechowywania danych

MODUŁ 3: Rola i obowiązki administratora oraz podmiotu przetwarzającego

- Administrator danych – definicja, obowiązki, odpowiedzialność
- Podmiot przetwarzający – rola i wymogi współpracy
- Współadministrowanie danymi
- Umowy powierzenia przetwarzania danych – analiza klauzul
- Podwykonawstwo w przetwarzaniu danych
- Transfery danych do państw trzecich

MODUŁ 4: Inspektor Ochrony Danych – funkcja i zadania

- Obligatoryjne wyznaczenie IOD – przesłanki
- Zadania IOD zgodnie z art. 39 RODO
- Pozycja IOD w strukturze organizacyjnej
- Wymogi dotyczące kwalifikacji IOD
- Niezależność i zakaz odwołania IOD
- Współpraca IOD z UODO
- Zarządzanie konfliktem interesów

MODUŁ 5: Dokumentacja systemu ochrony danych

- Rejestr czynności przetwarzania – budowa i prowadzenie
- Polityka bezpieczeństwa informacji
- Procedury wewnętrzne (obsługa żądań, zgłaszanie naruszeń, itp.)
- Instrukcje zarządzania systemami IT
- Dokumentacja umów powierzenia
- Accountability – zasada rozliczalności w praktyce

MODUŁ 6: Prawa osób, których dane dotyczą

- Prawo dostępu do danych (art. 15 RODO)
- Prawo do sprostowania i uzupełnienia danych
- Prawo do usunięcia danych („prawo do bycia zapomnianym")
- Prawo do ograniczenia przetwarzania
- Prawo do przenoszenia danych
- Prawo do sprzeciwu wobec przetwarzania
- Obsługa żądań – procedury i terminy

MODUŁ 7: Bezpieczeństwo danych osobowych

- Środki techniczne i organizacyjne zabezpieczeń
- Analiza ryzyka w kontekście ochrony danych
- Zarządzanie dostępem i kontrola uprawnień
- Szyfrowanie i pseudonimizacja
- Zabezpieczenia fizyczne i logiczne
- Bezpieczeństwo systemów IT i baz danych
- Audyty bezpieczeństwa

MODUŁ 8: Ocena skutków dla ochrony danych (DPIA)

- Kiedy DPIA jest obowiązkowa
- Metodologia przeprowadzania DPIA
- Identyfikacja i ocena ryzyka
- Środki minimalizujące ryzyko
- Konsultacje z IOD i UODO
- Dokumentacja DPIA – studia przypadków

MODUŁ 9: Naruszenia ochrony danych osobowych

- Definicja naruszenia (data breach)
- Procedura wykrywania i dokumentowania naruszeń
- Zgłaszanie naruszeń do UODO – terminy i wymogi
- Informowanie osób, których dane dotyczą
- Rejestr naruszeń
- Analiza przypadków naruszeń i ich konsekwencji

MODUŁ 10: Współpraca z organem nadzorczym (UODO)

- Kompetencje i uprawnienia UODO
- Procedury kontrolne prowadzone przez UODO
- Komunikacja z organem – pisma, wyjaśnienia, odwołania
- Decyzje administracyjne i środki naprawcze
- Sankcje administracyjne – katalog i zasady wymierzania
- Postępowania sądowe w sprawach RODO

MODUŁ 11: Praktyczne aspekty pracy IOD

- Planowanie i organizacja pracy IOD
- Narzędzia wspomagające pracę IOD (oprogramowanie, szablony)
- Audyty zgodności z RODO – metodyka i checklisty
- Prowadzenie szkoleń dla pracowników
- Budowanie kultury ochrony danych w organizacji
- Raportowanie do zarządu i monitorowanie zgodności

MODUŁ 12: RODO w różnych sektorach

- Ochrona danych w administracji publicznej
- Specyfika ochrony danych w placówkach medycznych
- RODO w edukacji – szkoły, przedszkola, uczelnie
- Ochrona danych w sektorze finansowym
- E-commerce i marketing a RODO
- Monitoring wizyjny i biometria

MODUŁ 13: Warsztaty i case studies

- Analiza rzeczywistych przypadków naruszeń RODO
- Warsztaty: tworzenie rejestru czynności przetwarzania
- Warsztaty: przeprowadzanie DPIA krok po kroku
- Warsztaty: obsługa skarg i żądań osób, których dane dotyczą
- Symulacja kontroli UODO
- Rozwiązywanie problemów prawnych – sesje Q&A

MODUŁ 14: Przygotowanie do egzaminu i walidacja

- Podsumowanie wiedzy – kluczowe zagadnienia
- Techniki zdawania egzaminów certyfikacyjnych
- Egzamin końcowy (test teoretyczny + case study)
- Omówienie wyników i feedback indywidualny

RAZEM: 250 godzin

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

Usługa skierowana jest do:

- osób fizycznych (początkujących),
- osób zainteresowanych podjęciem pracy jako IOD lub specjalista ds. ochrony danych,
- osób planujących rozwój kompetencji w obszarze ochrony danych osobowych,
- pracowników organizacji, którzy w przyszłości będą wspierać lub już wspierają administratora w realizacji obowiązków RODO.

Łączny czas trwania szkolenia : 249 godzin dydaktycznych + 1h dydaktyczna walidacja. Przerwy nie są wliczone w czas trwania usługi.

Liczba godzin teoretycznych: 200, liczba godzin praktycznych 49 + 1 h walidacja.

Walidacja

Walidacja odbywa się w formie testu teoretycznego i obserwacji w warunkach symulowanych. Kryterium zaliczenia: minimum 70% poprawnych odpowiedzi. Rozdzielność szkolenia od walidacji (rozdzielność osobowa): osoba prowadząca/opracowująca szkolenie nie przeprowadza końcowej walidacji. Wyniki walidacji są dokumentowane protokołem oraz arkuszem oceny/testem.

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	5 166,00 PLN
Koszt przypadający na 1 uczestnika netto	4 200,00 PLN
Koszt osobogodziny brutto	20,66 PLN
Koszt osobogodziny netto	16,80 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- **Materiały wideo**: profesjonalnie nagrane prezentacje z lektorem szczegółowo omawiającym wszystkie zagadnienia programowe
- **12 miesięcy dostępu**: pełny rok na ukończenie szkolenia i wielokrotne powracanie do materiałów

Szkolenie kończy się wydaniem certyfikatu Polskiego Centrum Bezpieczeństwa i Prewencji potwierdzającego ukończenie 250-godzinnego kursu dla Inspektorów Ochrony Danych.

Materiały szkoleniowe udostępniane w formie elektronicznej (prezentacja, skrypt, zestaw szablonów dokumentów: RCP, DSAR, karta incydentu, checklista mini-audytu, karta analizy ryzyka).

Warunki uczestnictwa

- Wykształcenie minimum średnie
- Podstawowa znajomość obsługi komputera i platform online
- Chęć rozwoju w obszarze ochrony danych osobowych

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 Google Classroom**, co zapewnia uczestnikom **pełną elastyczność** w planowaniu nauki zgodnie z własnym tempem i dostępnością czasową.

Charakterystyka formy szkolenia:

- **Materiały wideo**: profesjonalnie nagrane prezentacje z lektorem szczegółowo omawiającym wszystkie zagadnienia programowe
- **Dostęp 24/7**: możliwość nauki o dowolnej porze, z dowolnego miejsca – wymóg tylko dostęp do internetu
- **12 miesięcy dostępu**: pełny rok na ukończenie szkolenia i wielokrotne powracanie do materiałów
- **Uczenie się we własnym tempie**: bez sztywnych terminów realizacji poszczególnych modułów
- **Wsparcie trenera**:
- Kontakt mailowy z możliwością zadawania pytań (odpowiedzi w jak najkrótszym czasie)
- Komunikacja przez platformę Classroom
- Cykliczne webinary Q&A w wyznaczonych terminach (uczestnik w ciągu 12 miesięcy dostępu ma gwarancję znalezienia odpo

Warunki techniczne

Aby uczestniczyć w szkoleniu online wystarczy:

- Komputer stacjonarny/ laptop/ notebook (samodzielne stanowisko komputerowe)
- Stały dostęp do internetu- szybkość pobierania i wysyłania co najmniej 5Mb/s
- Przeglądarka internetowa (np. Google Chrome)

Zalecane są:

- Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy);
- 2GB pamięci RAM (zalecane 4GB lub więcej);
- System operacyjny taki jak Windows 10 (zalecany Windows 11), Mac OS wersja 13 (zalecana najnowsza wersja), Linux, Chrome OS.

Szkolenie realizowane będzie przez platformę Google Clasroom, zalecamy korzystanie z Google Chrome, Mozilla Firefox, Safari, Edge (Chromium), Yandex lub Opera. Należy korzystać z najaktualniejszej oficjalnej wersji wybranej przeglądarki.

Uczestnik powinien posiadać **indywidualne stanowisko komputerowe** pozwalające na samodzielną pracę z materiałami szkoleniowymi, wykonywanie ćwiczeń oraz rozwiązywanie testów wiedzy dostępnych na platformie.

Dostęp do platformy szkoleniowej zostanie przekazany uczestnikowi mailowo po zapisie na szkolenie i sfinalizowaniu płatności. Szkolenie można realizować w dowolnym czasie w okresie jego dostępności.

Kontakt

LDM CENTRUM SZKOLENIOWE

ROKSANA MICHALSKA

E-mail r.michalska@ldmszkolenia.pl

Telefon (+48) 660 079 541