



PRAKTYCZNE
ROZWIĄZANIA

Praktyczny kurs IOD

kompleksowe przygotowanie do pełnienia
funkcji inspektora ochrony danych
(stacjonarnie lub online)



[SPRAWDŹ SZCZEGÓŁY LOKALIZACJI](#)

Kompleksowe usługi z zakresu ochrony danych osobowych
i bezpieczeństwa informacji (str. nr 11)

SZANOWNI PAŃSTWO,

Praktyczny kurs IOD daje gruntowną wiedzę i praktyczne rozwiązania, dzięki którym będziesz mógł skutecznie sprawować funkcję inspektora ochrony danych. Każdy dzień kursu poświęcony został innemu zagadnieniu, które stopniowo budują kompetencje IOD.

Co ważne, podczas kursu naprzemiennie łączymy teorię z praktyką, dzięki czemu opracowana przez nas metodyka jest użyteczna dla kursantów. Wierzymy w to, że nie ma lepszego sposobu, żeby przygotować siebie i swoją organizację do wymogów prawa w zakresie ochrony danych osobowych.

DZIĘKI KURSOWI DOWIESZ SIĘ:

- Jak krok po kroku zbudować system ochrony danych osobowych.
- Jak skutecznie i rzetelnie wywiązać się z powierzonych Tobie obowiązków.
- Jak przeprowadzić audyt zgodności z przepisami o ochronie danych osobowych.
- Jakie polityki ochrony danych osobowych powinna zastosować Twoja organizacja.
- Jak zabezpieczyć system informatyczny.
- Jak szacować ryzyko i dokonać oceny skutków dla ochrony danych.
- Jak wdrożyć i stosować RODO, aby przepisy o ochronie danych osobowych przyczyniły się do rozwoju Twojej organizacji a nie pozostawały irytującym ciężarem

PRAKTYCZNY KURS IOD W CENIE 2 400 Zł + VAT

- Wybierając materiały w wersji elektronicznej oszczędzisz 200 zł.
- Korzystając z promocji First minute otrzymasz 200 zł upustu lub
- 3 książki o łącznej wartości 360zł.
- Każdy kolejny uczestnik z tego samego podmiotu otrzyma 10% upustu!
- Dla uczestników naszych poprzednich szkoleń dodatkowo oferujemy 25% upustu.

KAŻDY UCZESTNIK OTRZYMUJE

- Certyfikat IOD - wydrukowany lub w wersji elektronicznej.
- Poszkoleniowe wsparcie - Pomoc ODO 24.
- Skrypty prezentacji - wydrukowane lub w wersji elektronicznej.
- Poradniki RODO - wydrukowane lub w wersji elektronicznej.
- Dostęp do nagrań cyklicznie odbywających się webinarów.
- Wzory dokumentacji pozwalającej wykazać zgodność z RODO:

ZAKRES KURSU

RODO od podstaw

- Zgodność z RODO - co to oznacza?
- Wyjaśnienie najważniejszych pojęć określonych w RODO.
- Zasady przetwarzania danych osobowych i sposoby ich realizacji.
- Status inspektora ochrony danych.
- Prawa osób, których dane dotyczą i sposoby ich realizacji.
- Obowiązki administratora danych.
- Dokumentacja RODO.
- Obowiązki podmiotu przetwarzającego.
- Przekazywanie danych do państw trzecich i organizacji międzynarodowych.
- Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

IOD w praktyce

- Jak zarządzać systemem ochrony danych?
- Pozycja, praca i kwalifikacje inspektora ochrony danych (IOD).
- Inwentaryzacja i zrozumienie organizacji.
- Przygotowanie działań audytowych.
- Przygotowanie i przeprowadzenie audytu zgodności.
- Utrzymanie i zarządzaniem systemem „na co dzień”.
- Jak osiągnąć gotowość do kontroli organu nadzorczego?

DPIA i analiza ryzyka

- Wprowadzenie do zarządzania ryzykiem ochrony danych osobowych.
- Badanie kontekstu przetwarzania danych osobowych.
- Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.
- Co to jest ocena skutków dla ochrony danych (DPIA)?
- Wykonanie oceny skutków dla ochrony danych oraz szacowanie ryzyka dla zasobu przetwarzającego dane osobowe.
- Ćwiczenia z zakresu wykonania analizy ryzyka.
- Ćwiczenia z identyfikacji zasobów i zabezpieczeń.
- Przygotowanie planu postępowania z ryzykiem.
- Konsultacje z organem nadzorczym.

Dostosowanie IT

- Systemy informatyczne – funkcjonalności bezpieczeństwa.
- Systemy informatyczne – prawa osób, których dane dotyczą.
- Techniczne środki ochrony danych osobowych.
- Zarządzanie naruszeniami ochrony danych osobowych.
- Zarządzanie ciągłością działania.
- Dokumentacja przetwarzania danych osobowych w obszarze IT.

SZCZEGÓLOWY HARMONOGRAM

RODO OD PODSTAW (1 DZIEŃ)	GODZINY
Rejestracja uczestników	09.00 – 09.05
Zapytamy o państwa oczekiwania wobec szkolenia oraz o zagadnienia, na wyjaśnieniu których szczególnie będzie państwu zależało.	09.05 – 09.15
Test sprawdzający poziom wiedzy uczestników	09.15 – 09.30
MODUŁ I	
<p>I. Zgodność z RODO - co to oznacza?</p> <p>II. Wyjaśnienie najważniejszych pojęć określonych w RODO (m.in.)</p> <ul style="list-style-type: none"> • dane osobowe, • przetwarzanie, • profilowanie, pseudonimizacja, • administrator, • podmiot przetwarzający, • odbiorca danych, • strona trzecia. <p>III. Zasady przetwarzania danych osobowych i sposoby ich realizacji</p> <ul style="list-style-type: none"> • zgodność z prawem i przejrzystość, • ograniczenie celu, • minimalizacja danych, • prawidłowość, • ograniczenie przechowywania, • integralność i poufność, • rozliczalność. 	09.30 – 11.00
PRZERWA KAWOWA	11.00 – 11.10
MODUŁ II	
<p>I. Status inspektora ochrony danych.</p> <ul style="list-style-type: none"> • obligatoryjne wyznaczenie inspektora ochrony danych (IOD), • pozycja IOD, • zadania IOD, • konflikt interesów – jakich zadań nie powinien wykonywać IOD? • odpowiedzialność IOD. <p>II. Prawa osób, których dane dotyczą i sposoby ich realizacji</p> <ul style="list-style-type: none"> • prawo do uzyskania informacji (obowiązek informacyjny), • prawo dostępu do danych, • prawo do sprostowania danych, • prawo do usunięcia danych („prawo do bycia zapomnianym”), • prawo do ograniczenia przetwarzania, • prawo do przenoszenia danych, • prawo do sprzeciwu. 	11.10 – 13.00

LUNCH	13.00 – 13.30
MODUŁ III	
<p>I. Obowiązki administratora danych</p> <ul style="list-style-type: none"> • uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (ang. Privacy by Design, Privacy by Default), • status i obowiązki współadministratorów danych, • przetwarzanie danych z upoważnienia administratora lub podmiotu przetwarzającego, • rejestrowanie czynności przetwarzania, • bezpieczeństwo przetwarzania, <ul style="list-style-type: none"> ○ pseudonimizacja i szyfrowanie danych osobowych, ○ zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, ○ zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, ○ regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, • zgłaszanie naruszeń ochrony danych do organu nadzorczego, w tym omówienie formularza powiadomienie Prezesa UODO, • zawiadamianie osób, których dane dotyczą o naruszeniach. • ocena skutków dla ochrony danych (DPIA). 	13.30 – 15.30
PRZERWA KAWOWA	15.30 – 15.45
<p>I. Obowiązki podmiotu przetwarzającego.</p> <p>II. Przekazywanie danych do państw trzecich i organizacji międzynarodowych</p> <p>III. Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO)</p> <ul style="list-style-type: none"> • status Prezesa UODO, • obowiązki Prezesa UODO, • kontrola i postępowanie w sprawie naruszenia ochrony danych, • uprawnienia naprawcze Prezesa UODO, • certyfikacja i akredytacja, • administracyjne kary pieniężne, kryteria ustalenia wysokości kar. 	15.45 – 17.15
INDYWIDUALNE KONSULTACJE	17.15 – 17.30

IOD W PRAKTYCE (2 DZIEŃ)	GODZINY
MODUŁ I	
<p>I. Jak zarządzać systemem ochrony danych?</p> <ul style="list-style-type: none"> • kiedy system ochrony danych jest efektywny, • rzecznictwo na rzecz ochrony danych i wsparcie kierownictwa, • model i zakres zarządzania systemem ochrony danych, • skompletowanie zespołu ds. prywatności. <p>II. Pozycja, praca i kwalifikacje inspektora ochrony danych (IOD)</p> <ul style="list-style-type: none"> • IOD w organizacji: niezależność, brak konfliktu interesów i zasoby, • kiedy wyznaczyć IOD i kogo wybrać na to stanowisko, • co obejmują, a czego nie obejmują zadania IOD, • kwalifikacje IOD – jak je rozwijać i uwzględnić interdyscyplinarność ochrony danych. 	09.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.10
MODUŁ II	
<p>I. Inwentaryzacja i zrozumienie organizacji.</p> <ul style="list-style-type: none"> • jak zrozumieć i zinwentaryzować przepływy danych, • jak prowadzić przydatny rejestr czynności przetwarzania, • ćwiczenie: jak dobrze zacząć pracę jako iod. <p>II. Przygotowanie i przeprowadzenie audytu zgodności.</p> <ul style="list-style-type: none"> • audyt zgodności a inne analizy z zakresu ochrony danych osobowych, • przygotowanie działań audytowych i ustalenia organizacyjne, • przygotowanie dokumentów roboczych, w tym listy kontrolnej, • jak zachowywać się podczas audytu, • ćwiczenie: jak przeprowadzić rozmowę audytową, • jak ocenić zgodność, przygotować i przedstawić raport z audytu, • jak zaplanować i wpłynąć na realizację rekomendacji. 	11.10 – 13.00
LUNCH	13.00 – 13.30
MODUŁ III	
<p>I. Utrzymanie i zarządzaniem systemu „na co dzień”.</p> <ul style="list-style-type: none"> • jak zapewnić rozliczalność, • co uwzględnić w dokumentacji ochrony danych, • ćwiczenie: jak w praktyce realizować wymóg privacy by design, • świadomość pracowników – klucz do utrzymania zgodności z RODO, • obsługa żądań i realizacja praw osób fizycznych, • jak wybrać i zweryfikować podmiot przetwarzający, • jak zarządzać naruszeniami ochrony danych, • ćwiczenie: ocena wagi naruszenia. 	13.30 – 15.30

PRZERWA KAWOWA	15.30 – 15.45
MODUŁ IV	
I. Jak osiągnąć gotowość do kontroli organu nadzorczego? <ul style="list-style-type: none"> • przygotowanie do kontroli jako najlepszy sposób na zgodność, • jak postępować po otrzymaniu zawiadomienia o kontroli, • jak przygotować dokumenty, lokalizację i pracowników, • formalne i merytoryczne przygotowanie pełnomocników, • ćwiczenie: przygotowanie do kontroli w przykładowym stanie faktycznym, • przebieg kontroli: wyjaśnienia, przesłuchanie pracowników i oględziny, • protokół kontroli, zgłaszanie zastrzeżeń i dalsze kroki. 	15.45 – 17.15
INDYWIDUALNE KONSULTACJE	17.15 – 17.30
DPIA I ANALIZA RYZYKA (3 DZIEŃ)	GODZINY
MODUŁ I	
I Wprowadzenie do zarządzania ryzykiem ochrony danych osobowych <ul style="list-style-type: none"> • podstawowe pojęcia, • organizacja procesu szacowania ryzyka, • omówienie wybranych metodyk szacowania ryzyka. niezbędne elementy procesu DPIA, II. Badanie kontekstu przetwarzania danych osobowych. <ul style="list-style-type: none"> • ćwiczenia z zakresu określania kontekstu procesu szacowania ryzyka: <ul style="list-style-type: none"> ○ ustalanie kontekstu zewnętrznego, ○ ustalanie kontekstu wewnętrznego.. III. Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.15

MODUŁ II	
<p>I. Co to jest ocena skutków dla ochrony danych (DPIA)?</p> <ul style="list-style-type: none"> • cel wykonania DPIA, • sytuacje, w których przeprowadzenie DPIA jest obligatoryjne, • niezbędne elementy procesu DPIA, • inwentaryzacja procesów przetwarzania, • ustalenie zasobów związanych z przetwarzaniem wiążącym się z dużym prawdopodobieństwem spowodowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. <p>II. Wykonanie oceny skutków dla ochrony danych oraz szacowanie ryzyka dla zasobu przetwarzającego dane osobowe.</p>	11.15 – 13.00
LUNCH	13.00 – 13.30
MODUŁ III	
<p>I. Ćwiczenia z zakresu wykonania analizy ryzyka.</p> <ul style="list-style-type: none"> • szacowanie prawdopodobieństwa wystąpienia zagrożenia, • identyfikacja podatności, istniejących zabezpieczeń, • identyfikacja efektywności istniejących zabezpieczeń, • szacowanie następstw, • identyfikacja ryzyka, • określanie poziomu ryzyka, • określanie progu akceptowalności ryzyka. <p>II. Ćwiczenia z identyfikacji zasobów i zabezpieczeń.</p> <ul style="list-style-type: none"> • ustalenie wartości ryzyka procesu dla zasobu, • oszacowanie prawdopodobieństwa wystąpienia zagrożenia, • identyfikacja podatności, • identyfikacja istniejących zabezpieczeń, • identyfikacja efektywności istniejących zabezpieczeń, • szacowanie następstw, • identyfikacja ryzyka, określanie poziomu ryzyka, • określanie progu akceptowalności ryzyka. 	13.30 – 15.30
PRZERWA KAWOWA	15.30 – 15.45
MODUŁ IV	
<p>I. Przygotowanie planu postępowania z ryzykiem.</p> <ul style="list-style-type: none"> • obniżanie ryzyka, redukcja ryzyka, • uniknięcie ryzyka, transfer ryzyka. <p>II. Konsultacje z organem nadzorczym</p> <ul style="list-style-type: none"> • zakres informacji dla organu nadzorczego, • uprawnienia organu nadzorczego. 	15.45 – 17.15
INDYWIDUALNE KONSULTACJE	17.15 – 17.35

DOSTOSOWANIE IT (4 DZIEŃ)	GODZINY
MODUŁ I	
<p>I. Systemy informatyczne – funkcjonalności bezpieczeństwa</p> <ul style="list-style-type: none"> • identyfikacja systemów informatycznych, • zarządzanie dostępem użytkownikami, • kontrola dostępu do systemów i aplikacji, • dostęp do sieci i usług sieciowych, • zarządzanie informacjami uwierzytelniającymi użytkowników, • zabezpieczenia kryptograficzne. <p>II. Systemy informatyczne – prawa osób, których dane dotyczą</p> <ul style="list-style-type: none"> • prawo do bycia zapomnianym – możliwe sposoby realizacji, • prawo do przeniesienia danych – możliwe sposoby realizacji, • prawo dostępu do danych osobowych – możliwe sposoby realizacji, • prawo do ograniczenia przetwarzania – możliwe sposoby realizacji, • domyślna ochrona danych i ochrona danych w fazie projektowania. 	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.15
MODUŁ II	
<p>I. Techniczne środki ochrony danych osobowych</p> <ul style="list-style-type: none"> • kontrola dostępu, • infrastruktura serwerowa, • stacje robocze, urządzenia mobilne, • systemy wydruku, • pozyskiwanie, rozwój i utrzymanie systemów, • zarządzanie zasobami i usługami IT, • relacje z dostawcami. <p>II. Zarządzanie naruszeniami ochrony danych osobowych</p>	11.15 – 13.30
LUNCH	13.30 – 14.00
MODUŁ III	
<p>I. Zarządzanie ciągłością działania</p> <ul style="list-style-type: none"> • plan ciągłości działania, • procedury awaryjno-odtworzeniowe. <p>II. Dokumentacja przetwarzania danych osobowych</p> <ul style="list-style-type: none"> • wymagane polityki ochrony danych,, • przegląd polityk ochrony danych. 	14.00 – 15.30
INDYWIDUALNE KONSULTACJE	15:30 – 16:00
TEST SPRAWDZAJĄCY POZIOM WIEDZY UCZESTNIKÓW	16:00 – 16:15
ZAKOŃCZENIE SZKOLENIA - WYDANIE CERTYFIKATÓW	16.15 - 16.30

FIRST MINUTE

Każda osoba, która dokona wpłaty za kurs na 14 dni przed planowanym terminem, otrzyma **200 zł upustu** lub komplet [książek](#).



ZGŁOSZEŃ NALEŻY DOKONYWAĆ

Za pomocą formularza rejestracji dostępnego na naszej stronie internetowej lub telefonicznie: **22 740 99 96, 690 004 852**

Koszt uczestnictwa 1 osoby w szkoleniu wynosi:

- 2400 zł netto.
- 2400 zł zw. z VAT dla opłacających szkolenie w 70% lub całości ze środków publicznych.

Każdy kolejny uczestnik z tego samego podmiotu otrzyma **10% upustu!**

Dla uczestników naszych szkoleń lub warsztatów otwartych oferujemy **25% upustu** na drugie i każde kolejne.

Wpłat należy dokonywać na konto: Bank Citi Handlowy 23 1030 0019 0109 8533 0003 5356 nie później niż 2 dni robocze przed planowanym terminem szkolenia. W tytule wpłaty należy wpisać miasto, w którym odbywa się szkolenie oraz imię i nazwisko uczestnika.

NASZE SZKOLENIA

OTWARTE

Praktyczny Kurs IOD (32h)
RODO od podstaw (8h)
IOD w praktyce (8h)
DPIA i analiza ryzyka (8h)
RODO w HR (8h)
RODO w IT (8h)
Webinary (1h) - **gratis**

ZAMKNIĘTE

Bezpieczeństwo informacji (ok. 2h)
Ochrona danych osobowych (ok. 2h)
Przygotowanie do kontroli (ok. 2h)

E-LEARNING

W pigułce (30min)
Meritum (45 min) - **najpopularniejszy**
Premium (60 min)
Praca zdalna (20 min)
RODO migawki (15 min) - **gratis**
DODO (45 min)

NASZE USŁUGI

OCHRONA DANYCH OSOBOWYCH

Przejęcie funkcji IOD
Bieżące wsparcie
Audyt zgodności
DPIA i analiza ryzyka
Wdrożenie RODO
Kontrola UODO
Zgodność z DODO
Ochrona sygnalistów

BEZPIECZEŃSTWO INFORMACJI

Bezpieczeństwo informacji ISO 27001
Ciągłość działania ISO 22301
Badanie podatności
Cyberbezpieczeństwo

BEZPŁATNIE UDOSTĘPNIAMY

ABC RODO
Baza Wiedzy
Blog ODO 24
RODO Navigator Online
Poradniki i przewodniki RODO

Ranking aplikacji dla sygnalistów
Kalkulator wagi naruszeń
Kalkulator analizy ryzyka
RODO Migawki - dla pracowników
Bezpłatne porady

ZAPRASZAM DO WSPÓŁPRACY



Dominik Kantorowicz
Koordynator ds. szkoleń
tel. 22 740 99 99
tel. kom. 690 004 852
e-mail: d.kantorowicz@odo24.pl