



PRAKTYCZNE
ROZWIĄZANIA

Akredytowany kurs IOD (4-dniowy) kompleksowe przygotowanie do pełnienia funkcji inspektora ochrony danych



Gdańsk

13 – 16 VII 2020r.

10 – 13 VIII 2020r.

Katowice

20 – 23 VII 2020r.

17 – 20 VIII 2020r.

Poznań

27 – 30 VII 2020r.

24 – 27 VIII 2020r.

Warszawa

13 – 16 VII 2020r.

27 – 30 VII 2020r.

10 – 13 VIII 2020r.

24 – 27 VIII 2020r.

[SPRAWDŹ SZCZEGÓŁY LOKALIZACJI](#)

Kompleksowe usługi z zakresu ochrony danych osobowych
i bezpieczeństwa informacji (str. nr 13)

SZANOWNI PAŃSTWO,

Akredytowany kurs IOD stanowi element kształcenia ustawicznego w formach pozaszkolnych zgodnie z rozporządzeniem Ministra Edukacji Narodowej i Sportu z dnia 20 grudnia 2003 r. w sprawie akredytacji placówek i ośrodków prowadzących kształcenie ustawiczne w formach pozaszkolnych (Dz. U. z 2003 roku nr 227, poz. 2247 ze zm.)

ZAKRES KURSU

WPROWADZENIE DO OCHRONY DANYCH OSOBOWYCH (ZASADY, PROCEDURY I DOKUMENTACJA PRZETWARZANIA)

- 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).

AUDYT ZGODNOŚCI

- Wyjaśnienie najważniejszych pojęć związanych z audytem.
- Zasady audytowania rodzaje audytów na gruncie RODO/GDPR.
- Ustalanie struktury odpowiedzialnej za przeprowadzanie audytu.
- Przygotowanie działań audytowych.
- Działania audytowe.
- Działania po audytowe.

OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA) ORAZ 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 ŚRODOWISKA TELEINFORMATYCZNEGO

- 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.

KAŻDY UCZESTNIK OTRZYMUJE

Certyfikat IOD potwierdzający udział w kursie, wydrukowane skrypty prezentacji, poradnik „Jak przetwarzać dane osobowe? RODO poradnik dla przedsiębiorców” – wydrukowany [RODO Nawigator](#) oraz dostęp na okres 12 miesięcy do aplikacji [ODO Nawigator](#) wraz z trzema szkoleniami e-learningowymi „[meritum](#)„ dla pracowników Twojej organizacji oraz wzory dokumentacji pozwalającej wykazać zgodność z RODO:

- Analizę zasadności prowadzenia rejestru czynności przetwarzania.
- Analizę zasadności wyznaczenia inspektora ochrony danych.
- Arkusz audytowy RODO.
- Arkusz oceny skutków dla ochrony danych (DPIA).
- Dekalog ochrony danych osobowych.
- Dokumentację naruszenia ochrony danych osobowych.
- Instrukcję zarządzania zasobami informatycznymi.
- Listę kontrolną podstawowych funkcjonalności systemów informatycznych.
- Listę uczestników audytu.
- Listę przykładowych procesów przetwarzania.
- Notatkę z oględzin.
- Plan audytu RODO.
- Politykę ochrony danych osobowych.
- Politykę privacy by design and by default
- Politykę realizacji praw osób, których dane dotyczą (w tym przykładowe klauzule zgody na przetwarzanie danych osobowych, profilowanie oraz klauzule informacyjne).
- Prezentację na podstawowe szkolenie RODO.
- Procedurę oceny skutków przetwarzania dla ochrony danych (DPIA).
- Raport z audytu RODO.
- Rejestr czynności przetwarzania (administrator danych).
- Rejestr czynności przetwarzania (podmiot przetwarzający).
- Rejestr incydentów ochrony danych osobowych.
- Rejestr tworzenia kopii zapasowych.
- Uchwałę w sprawie wyznaczenia IOD.
- Uchwałę ws. przyjęcia dokumentacji RODO.
- Umowę o powierzeniu przetwarzania danych osobowych.
- Upoważnienie do przetwarzania danych osobowych.
- Upoważnienie do przetwarzania danych osobowych.
- Wniosek o nadanie, modyfikację, odebranie uprawnień do systemu informatycznego.
- Wykaz członków zespołu wdrożeniowego.
- Wykaz oprogramowania wspierającego wdrożenie i utrzymanie RODO (w języku angielskim).
- Wyniki oceny skutków dla ochrony danych (DPIA).

Uczestnikom gwarantujemy merytoryczne wsparcie zarówno w trakcie kursu, jak i po jego zakończeniu w formie usługi [Pomoc ODO 24](#).

FIRST MINUTE

Każda osoba, która dokona wpłaty za kurs na 14 dni przed planowanym terminem, w ramach prezentu otrzyma po szkoleniu komplet [książek](#).



ZGŁOSZEŃ NALEŻY DOKONYWAĆ

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

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

Koszt uczestnictwa 1 osoby w warsztatach wynosi:

- ~~2950~~ **2212,50 zł (25% rabatu do 31.08.2020 r.)**
zw. z VAT na podstawie art. 43 ust. 1 pkt 29 lit. b

Wpłat należy dokonywać na konto: Bank Citi Handlowy 23 1030 0019 0109 8533 0003 5356, nie później niż 2 dni robocze przed planowanym terminem kursu.

Więcej informacji (w tym sylwetki prowadzących) znajduje się na naszej stronie [\[link\]](#)

SZCZEGÓŁOWY HARMONOGRAM KURSU

DZIEŃ I

WPROWADZENIE DO OCHRONY DANYCH OSOBOWYCH (ZASADY, PROCEDURY I DOKUMENTACJA PRZETWARZANIA)	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 w dniu rozpoczęcia kursu	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 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, • prawo do niepodlegania profilowaniu, • zasada przejrzystości. 	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 powiadomienia Prezesa UODO, • zawiadamianie osób, których dane dotyczą o naruszeniach. • ocena skutków dla ochrony danych (DPIA). <p>II. Dokumentacja RODO</p> <ul style="list-style-type: none"> • polityka ochrony danych osobowych, • instrukcja zarządzania zasobami informatycznymi, 	13.30 – 15.30

<ul style="list-style-type: none"> ocena skutków dla ochrony danych i analiza ryzyka dla zasobów biorących udział w operacjach przetwarzania, polityka zgłaszania naruszenia i zarządzania incydemem, procedura realizacji praw osób, których dane dotyczą, i udzielania odpowiedzi na żądania, rejestr czynności przetwarzania. 	
Przerwa kawowa	15.30 – 15.45
I. Obowiązki podmiotu przetwarzającego. II. Przekazywanie danych do państw trzecich i organizacji międzynarodowych III. Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) <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, w tym kryteria ustalenia wysokości kar. 	15.45 – 17.15
Indywidualne konsultacje	17.10 – 17.30

DZIEŃ II

AUDYT ZGODNOŚCI	GODZINY
MODUŁ I	
I. Wyjaśnienie najważniejszych pojęć związanych z audytem (m.in.): <ul style="list-style-type: none"> audyt i jego rodzaje, kryterium audytu, dowód z audytu, kompetencje, zespół audytowy, plan audytu, zakres podmiotowy oraz przedmiotowy audytu, ustalenia z audytu, stopień spełnienia kryterium audytu (ćwiczenie), wnioski z audytu, działania korekcyjne i korygujące. II. Zasady audytowania: <ul style="list-style-type: none"> rzetelność, uczciwe przedstawienie wyników, należyta staranność zawodowa, poufność, niezależność, podejście oparte na dowodach. 	9.00 – 11.00

Przerwa kawowa	11.00 – 11.15
MODUŁ II	
<p>I. Ustalanie struktury odpowiedzialnej za przeprowadzanie audytu</p> <ul style="list-style-type: none"> • ustalenia proceduralne, • wybór członków zespołu audytującego, • harmonogram prac. <p>II. Przygotowanie działań audytowych</p> <ul style="list-style-type: none"> • określenie wykonalności audytu, • przygotowanie planu audytowego (omówienie wzoru), • przydzielenie pracy zespołowi audytującemu, • przygotowanie dokumentów roboczych, • inicjowanie audytu, • przebieg procesu audytowania. 	11.10 – 13.00
Lunch	13.00 – 13.30
MODUŁ III	
<p>I. Działania audytowe</p> <ul style="list-style-type: none"> • spotkanie otwierające • przegląd dokumentacji podczas przeprowadzania audytu, • komunikowanie się podczas audytu, • wyznaczenie ról i odpowiedzialność przewodników i obserwatorów, • zbieranie i weryfikowanie informacji (ćwiczenie), • badanie dokumentacji przetwarzania danych osobowych (ćwiczenie), • opracowanie ustaleń z audytu, • przygotowanie wniosków z audytu (ćwiczenie), • spotkanie zamykające. 	13.30 – 15.30
Przerwa kawowa	15.30 – 15.45
<p>II. Działania po audytowe</p> <ul style="list-style-type: none"> • przygotowanie raportu z audytu (omówienie wzoru). • rozpowszechnienie raportu z audytu. 	15.45 – 17.15
Indywidualne konsultacje	17.15 – 17.35

DZIEŃ III

OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA) ORAZ ANALIZA RYZYKA	GODZINY
MODUŁ I	
<p>I Wprowadzenie do zarządzania ryzykiem ochrony danych osobowych</p> <ul style="list-style-type: none"> • podstawowe pojęcia, • organizacja procesu szacowania ryzyka, • omówienie wybranych metodyk szacowania ryzyka. niezbędne elementy procesu DPIA, <p>II. Badanie kontekstu przetwarzania danych osobowych.</p> <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. <p>III. Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.</p>	<p>9.00 – 11.00</p>
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> <ul style="list-style-type: none"> • cel szacowania ryzyka, • korzyści z wykonania szacowania ryzyka, • kryteria oceny ryzyka, • szacowanie ryzyka, • poziom ryzyka. 	<p>11.15 – 13.00</p>
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, • identyfikacja 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

DZIEŃ IV

DOSTOSOWANIE ŚRODOWISKA TELEINFORMATYCZNEGO	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 - możliwe sposoby realizacji. 	<p>9.00 – 11.00</p>
Przerwa kawowa	<p>11.00 – 11.15</p>
MODUŁ II	
<p>I. Techniczne środki ochrony danych osobowych</p> <ul style="list-style-type: none"> • kontrola dostępu, • zabezpieczenia sieciowe, • 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>	<p>11.15 – 13.30</p>

Lunch	13.30 – 14.00
MODUŁ III	
I. Zarządzanie ciągłością działania <ul style="list-style-type: none">• plan ciągłości działania,• procedury awaryjno-odtworzeniowe. II. Dokumentacja przetwarzania danych osobowych w obszarze IT <ul style="list-style-type: none">• wymagane polityki ochrony danych w obszarze IT,• przegląd polityk ochrony danych.	14.00 – 15.30
Indywidualne konsultacje	15:30 – 16:00
Test sprawdzający poziom wiedzy uczestników w dniu zakończenia kursu	16:00 – 16:15
Zakończenie szkolenia - wydanie certyfikatów	16.15 - 16.30

NASZE SZKOLENIA

OTWARTE

[Akredytowany Kurs IOD](#)
[DPIA i analiza ryzyka](#)
[DODO od podstaw](#)
[Kontrola UODO](#)
[Monitorowanie zgodności](#)
[RODO w HR](#)
[RODO w IT](#)
[RODO od podstaw](#)
[Spotkanie eksperckie](#)

ZAMKNIĘTE

[Bezpieczeństwo informacji](#)
[Ochrona danych osobowych](#)
[Kontrola UODO](#)

E-LEARNING

[Dedykowany](#)
[DODO](#)
[Meritum](#)
[Premium](#)
[W pigułce](#)

NASZE USŁUGI

OCHRONA DANYCH OSOBOWYCH

[Audyt zgodności](#)
[Bieżące wsparcie](#)
[DPIA i analiza ryzyka](#)
[Kontrola UODO](#)
[Przejęcie funkcji IOD](#)
[Wdrożenie RODO](#)

BEZPIECZEŃSTWO INFORMACJI

[Bezpieczeństwo informacji ISO 27001](#)
[Bezpieczeństwo IT ISO 20000](#)
[Ciągłość działania ISO 22301](#)
[Cyberbezpieczeństwo](#)

BEZPŁATNIE UDOSTĘPNIAMY

[Baza wiedzy](#)
[Biuletyn informacyjny](#)
[RODO Nawigator](#)
[RODO migawka](#)

NARZĘDZIA:

[Kalkulator analizy ryzyka](#)
[Kalkulator wagi naruszeń](#)

PORADNIKI:

[Jak przetwarzać dane osobowe](#)
[Jak przygotować się do kontroli](#)
[Zasady ochrony danych osobowych](#)
[Zasady bezpiecznej pracy zdalnej](#)

ZAPRASZAM DO WSPÓŁPRACY



Dominik Kantorowicz

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

Jesteśmy
inwestorem
społecznym



Patronujemy
fundacji



Wspieramy
finansowo



ODO 24 sp. z o.o. z siedzibą: 03-812 Warszawa, ul. Kamionkowska 45, zarejestrowana w Rejestrze Przedsiębiorców prowadzonym przez Sąd Rejonowy dla m. st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000434350, NIP: 7010353442, kapitał zakładowy: 50 000 zł.