PRAKTYCZNE
ROZWIĄZANIA

Akredytowany kurs IOD (4-dniowy)

kompleksowe przygotowanie do pełnienia funkcji inspektora ochrony danych

Gdańsk	Katowice	Poznań	Warszawa
07 – 10.09.2020 r.	17 – 20.08.2020 r.	24 – 27.08.2020 r.	24 – 27.08.2020 r.
05 – 08.10.2020 r.	14 – 17.09.2020 r.	21 – 24.09.2020 r.	07 – 10.09.2020 r.
02 – 05.11.2020 r.	12 – 15.10.2020 r.	19 – 22.10. 2020 r.	21 – 24.09.2020 r.
30.11.– 3.12.2020 r.	23 – 26.11.2020 r.	16 – 19.11. 2020 r.	05 – 08.10.2020 r.
	07 – 10.12.2020 r.	14 – 17.12. 2020 r.	19 – 22.10.2020 r.
			02 – 05.11.2020 r.
			16 – 19.11.2020 r.
			30.11 – 3.12.2020 r.
			14 – 17.12.2020 r.

SPRAWDŹ SZCZEGÓŁY LOKALIZACJI

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

SZANOWNI PAŃSTWO,

Akredytowany kurs IOD stanowi element kształcenia ustawicznego w formach pozaszkolnych zgodnie z rozporządzeniem Ministra Edukacji Narodowej i Sportu z dnia 20.12.2003 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

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 systemu „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.

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**.

SZCZEGÓŁOWY 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	
I. Zgodność z RODO - co to oznacza? II. Wyjaśnienie najważniejszych pojęć określonych w RODO (m.in.) • dane osobowe, • przetwarzanie, • profilowanie, pseudominizacja, • administrator, • podmiot przetwarzający, • odbiorca danych, • strona trzecia. III. Zasady przetwarzania danych osobowych i sposoby ich realizacji • 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	
I. Status inspektora ochrony danych. • obligatoryjne wyznaczenie inspektora ochrony danych (IOD), • pozycja IOD, • zadania IOD, • konflikt interesów – jakich zadań nie powinien wykonywać IOD? • odpowiedzialność IOD. II. Prawa osób, których dane dotyczą i sposoby ich realizacji • 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	

I. Obowiązki administratora danych
• 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,
  ○ 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
I. Obowiązki podmiotu przetwarzającego. II. Przekazywanie danych do państw trzecich i organizacji międzynarodowych III. Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) • 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	
I. Jak zarządzać systemem ochrony danych? • 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. II. Pozycja, praca i kwalifikacje inspektora ochrony danych (IOD) • 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	
I. Inwentaryzacja i zrozumienie organizacji. • jak zrozumieć i zinwentaryzować przepływy danych, • jak prowadzić przydatny rejestr czynności przetwarzania, • ćwiczenie: jak dobrze zacząć pracę jako iod. II. Przygotowanie i przeprowadzenie audytu zgodności. • 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	
I. Utrzymanie i zarządzaniem systemu „na co dzień”. • 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? • 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 • podstawowe pojęcia, • organizacja procesu szacowania ryzyka, • omówienie wybranych metodyk szacowania ryzyka. niezbędne elementy procesu DPIA, II. Badanie kontekstu przetwarzania danych osobowych. • ćwiczenia z zakresu określania kontekstu procesu szacowania ryzyka: o ustalanie kontekstu zewnętrznego, o ustalanie kontekstu wewnętrznego.. III. Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.15

MODUŁ II	
I. Co to jest ocena skutków dla ochrony danych (DPIA)? • 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. II. Wykonanie oceny skutków dla ochrony danych oraz szacowanie ryzyka dla zasobu przetwarzającego dane osobowe.	11.15 – 13.00
LUNCH	13.00 – 13.30
MODUŁ III	
I. Ćwiczenia z zakresu wykonania analizy ryzyka. • szacowanie prawdopodobieństwa wystąpienia zagrożenia, • identyfikacja podatności, istniejących zabezpieczeń, • identyfikacja efektywności istniejących zabezpieczeń, • szacowanie następstw, • identyfikacja ryzyka, • określanie poziomu ryzyka, • określanie progu akceptowalności ryzyka. II. Ćwiczenia z identyfikacji zasobów i zabezpieczeń. • 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	
I. Przygotowanie planu postępowania z ryzykiem. • obniżanie ryzyka, redukcja ryzyka, • uniknięcie ryzyka, transfer ryzyka. II. Konsultacje z organem nadzorczym • zakres informacji dla organu nadzorczego, • uprawniania organu nadzorczego.	15.45 –17.15
INDYWIDUALNE KONSULTACJE	17.15 – 17.35

DOSTOSOWANIE IT (4 DZIEŃ)	GODZINY
MODUŁ I	
I. Systemy informatyczne – funkcjonalności bezpieczeństwa • identyfikacja systemów informatycznych, • zarządzanie dostępem użytkownikami, • kontrola dostępu do systemów i aplikacji, • dostęp do sieci i usług sieciowych, • zarządzanie informacjami uwierzytelniającymi użytkowników, • zabezpieczenia kryptograficzne. II. Systemy informatyczne – prawa osób, których dane dotyczą • 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	
I. Techniczne środki ochrony danych osobowych • kontrola dostępu, • infrastruktura serwerowa, • stacje robocze, urządzenia mobilne, • systemy wydruku, • pozyskiwanie, rozwój i utrzymanie systemów, • zarządzanie zasobami i usługami IT, • relacje z dostawcami. II. Zarządzanie naruszeniami ochrony danych osobowych	11.15 – 13.30
LUNCH	13.30 – 14.00
MODUŁ III	
I. Zarządzanie ciągłością działania • plan ciągłości działania, • procedury awaryjno-odtworzeniowe. II. Dokumentacja przetwarzania danych osobowych • 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, 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

Koszt uczestnictwa 1 osoby w szkoleniu wynosi:

- ~~2950~~ 2212 zł (do 30 IX 2020 r.) netto.
- ~~2950~~ 2212 zł (do 30 IX 2020 r.) 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
Akredytowany Kurs IOD
DPIA i analiza ryzyka
DODO od podstaw
Kontrola UODO
IOD w praktyce
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.