PRAKTYCZNE
ROZWIĄZANIA

AKREDYTOWANY KURS IOD (4-dniowy)
kompleksowe przygotowanie do pełnienia funkcji inspektora ochrony danych

2018 r.

Warszawa

03-06 IX, 17-20 IX, 01-04 X, 15-18 X, 05 - 08 XI, 19 - 22 XI, 03 - 06 XII, 17 - 20 XII

Katowice

10-13 IX, 24-27 IX, 08-11 X, 22-25 X, 26 - 29 XI, 10 - 13 XII

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:

- przedmiot i cele reformy przepisów o ochronie danych osobowych,
- środowisko bezpieczeństwa danych osobowych,
- wyjaśnienie najważniejszych pojęć RODO/GDPR,
- zasady przetwarzania danych osobowych,
- prawa osób, których dane dotyczą,
- obowiązki administratora danych,
- obowiązki podmiotu przetwarzającego (procesora danych),
- status inspektora ochrony danych,
- przekazywanie danych do państw trzecich i organizacji międzynarodowych,
- Urząd Ochrony Danych Osobowych (UODO).

PRZYGOTOWANIE PLANU WDROŻENIA I AUDYT ZGODNOŚCI:

- planowanie procesu wdrożenia RODO/GDPR,
- rola audytu w procesie wdrożenia RODO/GDPR,
- rodzaje audytów na gruncie RODO/GDPR,
- wyjaśnienie najważniejszych pojęć związanych z audytowaniem,
- zasady audytowania,
- zarządzanie programem audytów,
- przeprowadzanie audytu.

SZACOWANIE RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH:

- organizacja procesu oceny skutków dla ochrony danych (ang. Data Protection Impact Assessment, DPIA),
- zapoznanie z podstawowymi pojęciami i kryteriami procesu szacowania ryzyka,
- zabezpieczenia minimalizujące ryzyko według RODO/GDPR,
- przygotowanie organizacji do procesu szacowania ryzyka,
- wykonanie procesu szacowania ryzyka dla zasobu,
- ćwiczenia z identyfikacji zasobów i zabezpieczeń,
- przygotowanie planu postępowania z ryzykiem,
- konsultacje z organem nadzorczym,
- konsolidacja oceny skutków przetwarzania oraz procesu szacowania ryzyka dla zasobu,
- potencjalne zagrożenia oraz trudności wykonania DPIA oraz szacowania ryzyka dla zasobu.

DOSTOSOWANIE PROCESÓW, DOKUMENTACJI I ŚRODOWISKA TELEINFORMATYCZNEGO:

- dostosowanie procesów biznesowych,
- dostosowanie polityk ochrony danych,
- dostosowanie środowiska teleinformatycznego,
- podsumowanie zagadnień omawianych w ramach kurs.

KAŻDY UCZESTNIK OTRZYMUJE

Materiały szkoleniowe oraz **Certyfikat IOD** potwierdzający udział w kursie.

Wymaganą ustawowo pełną Dokumentację ODO, czyli wydrukowane szablony polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym – dokumenty przygotowane do wypełnienia podczas warsztatów (również w wersji elektronicznej). Szablony tych dokumentów oraz materiały dodatkowe takie jak: poradnik „Jak zawrzeć umowę powierzenia przetwarzania danych osobowych", katalog przykładowych incydentów ODO wraz z rekomendowanymi działaniami naprawczymi, dekalog ODO, oraz listę zagadnień o których należy informować IOD. Dokumentacja jest zgodna z obowiązującym stanem prawnym.

Wzory dokumentów służących do realizacji sprawdzeń (m.in. plan sprawdzeń, zawiadomienie o rozpoczęciu sprawdzenia, notatka z odebrania ustnych wyjaśnień, przykładowe sprawozdanie ze sprawdzenia). Otrzymacie Państwo również edytowalną prezentację szkolenia pracowniczego pobierz fragment (docelowo będzie to plik programu Microsoft PowerPoint), które służy do sprawnego zarządzania systemem ochrony danych osobowych. Ponad to praktyczny poradnik "Reforma ochrony danych osobowych w UE - 24 kluczowe zmiany" oraz "Jak w praktyce i zgodnie z prawem przetwarzać dane osobowe", etui ochronne na kartę płatniczą - RFID blocker.

Gwarantujemy uczestnikom bezpłatne wsparcie w przygotowaniu dokumentacji ODO jak również rozwiązywaniu innych problemów związanych z ochroną danych osobowych poprzez usługę POMOC ODO 24 [link].

FIRST MINUTE

Każda osoba, która dokona wpłaty za kurs na 14 dni przed planowanym terminem, w ramach prezentu otrzyma na szkoleniu komplet książek.

ZGŁOSZEŃ NALEŻY DOKONYWAĆ

Za pomocą formularza rejestracji dostępnego na naszej stronie internetowej lub telefonicznie: 22 740 99 96, 690 957 662

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

Koszt uczestnictwa 1 osoby w warsztatach wynosi:

- 2950 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	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	
I. Przedmiot i cele reformy przepisów o ochronie danych osobowych. II. Środowisko bezpieczeństwa danych osobowych. • cyberprzestrzeń, • przepisy prawa w zakresie ochrony danych osobowych, o RODO/GDPR, o ustawa o ochronie danych osobowych (projekt), o dyrektywa policyjna, o rozporządzenie e-Privacy (projekt), o wytyczne Grupy Roboczej Artykułu 29. III. Wyjaśnienie najważniejszych pojęć RODO/GDPR (m.in.) • dane osobowe, • przetwarzanie, • profilowanie, • pseudominizacja, • administrator, • podmiot przetwarzający, • naruszenie ochrony danych osobowych. IV. Zasady przetwarzania danych osobowych. • zgodność z prawem, rzetelność i przejrzystość, • ograniczenie celu, • prawidłowość, • ograniczenie przechowywania, • integralność i poufność,	09.30 – 11.00

• rozliczalność.	
PRZERWA KAWOWA	11.00 – 11.10
MODUŁ II	
I. Prawa osób, których dane dotyczą. • 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. II. Obowiązki administratora danych. • pozyskiwanie i dalsze przetwarzanie danych osobowych – podsumowanie obowiązków 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, o pseudonimizacja i szyfrowanie danych osobowych, o zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, o zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, o regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, • zgłaszanie naruszeń ochrony danych do organu nadzorczego, • zawiadamianie osób, których dane dotyczą o naruszeniach, • ocena skutków dla ochrony danych (ang. Data Protection Impact Assessment, DPIA).	11.10 –13.00
LUNCH	13.00 – 13.30
MODUŁ III	
I. Obowiązki podmiotu przetwarzającego (procesora danych). II. Status inspektora ochrony danych. • wymagania względem inspektora ochrony danych (ang. Data Protection Officer, DPO), • pozycja IOD/DPO, • zadania IOD/DPO,	13.30 – 15.30

• IOD/DPO w ramach grupy kapitałowej, • odpowiedzialność IOD/DPO. III. Przekazywanie danych do państw trzecich i organizacji międzynarodowych.	
PRZERWA KAWOWA	15.30 – 15.40
IV. Urząd Ochrony Danych Osobowych (UODO). • status Prezesa UODO, • uprawnienia Prezesa UODO, • obowiązki Prezesa UODO, • certyfikacja i akredytacja, • postępowania kontrolne, • administracyjne kary pieniężne.	15.40 – 17.10
Indywidualne konsultacje	17.10 – 17.30

DZIEŃ II PRZYGOTOWANIE PLANU WDROŻENIA I AUDYT ZGODNOŚCI	GODZINY
MODUŁ I	
I. Planowanie procesu wdrożenia RODO/GDPR. • definiowanie celów w zakresie ochrony danych osobowych, • wybór członków zespołu wdrożeniowego, • ustalanie etapów wdrożenia RODO, • określanie niezbędnych zasobów, • harmonogram prac. II. Rola audytu w procesie wdrożenia RODO/GDPR. III. Rodzaje audytów na gruncie RODO/GDPR. IV. Wyjaśnienie najważniejszych pojęć związanych z audytowaniem. • audyt, • audytor, • dowód z audytu, • ekspert techniczny, • kompetencje, • kryteria audytu, • plan audytu, • system ochrony danych osobowych, • ustalenia z audytu, • wnioski z audytu, • zakres audytu, • zespół audytujący, • zgodność/niezgodność.	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.10
MODUŁ II	
I. Zasady audytowania. II. Zarządzanie programem audytów. • ustalanie celów audytu, • ustalanie programu audytu, • wdrażanie programu audytu, • monitorowanie programu audytu, • przegląd i doskonalenie programu audytu.	11.10 –13.00
LUNCH	13.00 – 13.30

MODUŁ III	
I. Przeprowadzanie audytu. • inicjowanie audytu, • przygotowanie działań audytowych,	13.30 – 15.30
PRZERWA KAWOWA	15.30 – 15.40
II. Przeprowadzanie audytu c.d. • przygotowanie i rozpowszechnianie raportu z audytu, • zakończenie audytu, • przeprowadzenie działań poaudytowych.	15.40 – 17.10
Indywidualne konsultacje	17.10 – 17.30

DZIEŃ III OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA) ORAZ ANALIZA RYZYKA	GODZINY
MODUŁ I	
I. Organizacja procesu oceny skutków dla ochrony danych (ang. Data Protection Impact Assessment, DPIA). • cel wykonania DPIA, • sytuacje, w których przeprowadzenie DPIA jest obligatoryjne, • niezbędne elementy procesu DPIA, • inwentaryzacja procesów, • ustalenie zasobów związanych z przetwarzaniem wiążącym się z dużym prawdopodobieństwem spowodowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, • ćwiczenia z zakresu przeprowadzenia procesu DPIA. II. Zapoznanie z podstawowymi pojęciami i kryteriami procesu szacowania ryzyka. • szacowanie ryzyka, • poziom ryzyka, • ryzyko szczątkowe, • identyfikowanie zagrożenia, • identyfikowanie podatności, • kryteria oceny poziomu ryzyka. III. Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.10
MODUŁ II	

I. Przygotowanie organizacji do procesu szacowania ryzyka.
• ustalenie członków zespołu wdrożeniowego,
• ćwiczenia z zakresu określania kontekstu procesu szacowania ryzyka:
  ○ ustalanie kontekstu zewnętrznego,
  ○ ustalanie kontekstu wewnętrznego.
II. Ćwiczenia z zakresu inwentaryzacji zasobów.
• sprzęt,
• systemy operacyjne i aplikacje,
• strony internetowe przetwarzające dane osobowe,
• formaty plików w postaci elektronicznej (dane nieustrukturyzowane),
• osoby przetwarzające dane osobowe,
• główne lokalizacje i obszary krytyczne,
• krytyczne umowy.
	11.10 – 13.00

LUNCH	13.00 – 13.30

MODUŁ III	

I. Wykonanie procesu szacowania ryzyka dla zasobu.
• ryzyko przetwarzania danych osobowych:
  ○ cel analizy ryzyka,
  ○ korzyści z wykonania szacowania ryzyka,
• kryteria oceny 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 – 15.40
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. III. Konsolidacja oceny skutków przetwarzania oraz procesu szacowania ryzyka dla zasobu. IV. Potencjalne zagrożenia oraz trudności wykonania DPIA oraz szacowania ryzyka dla zasobu.	15.40 –17.10
Indywidualne konsultacje	17.10 – 17.30

DZIEŃ IV DOSTOSOWANIE PROCESÓW, DOKUMENTACJI I ŚRODOWISKA TELEINFORMATYCZNEGO	GODZINY
MODUŁ I	
TEST SPRAWDZAJĄCY POZIOM WIEDZY UCZESTNIKÓW W DNIU ZAKOŃCZENIA KURSU	09.00 – 09.15
I. Dostosowanie procesów biznesowych • warunki wyrażania zgody, • realizacja rozszerzonego obowiązku informacyjnego, • wybór podmiotu przetwarzającego (procesora danych osobowych), • retencja danych osobowych. II. Dostosowanie polityk ochrony danych • aktualizacja obowiązującej dokumentacji przetwarzania danych osobowych, • tworzenie procedur bezpieczeństwa.	9.15 – 11.00
PRZERWA KAWOWA	11.00 – 11.10
MODUŁ II	

I. Dostosowanie środowiska teleinformatycznego
• Wymagania względem systemów informatycznych.
  ○ zapewnienie poufności, integralności, dostępności i odporności systemów i usług,
  ○ zapewnienie ciągłości działania,
  ○ testowanie, mierzenie i ocena skuteczności ochrony danych.
• Obszary bezpieczeństwa infrastruktury teleinformatycznej.
  ○ kontrola dostępu,
  ○ klasyfikacja zasobów informacyjnych,
  ○ bezpieczeństwo fizyczne i środowiskowe,
  ○ obszary związane z użytkownikiem końcowym,
  ○ kopie zapasowe,
  ○ przekazywanie informacji,
  ○ ochrona przed szkodliwym oprogramowaniem,
  ○ zarządzanie podatnościami technicznymi,
  ○ zabezpieczenia kryptograficzne,
  ○ bezpieczeństwo komunikacji.
	11.10 – 13.00

LUNCH	13.00 – 13.30
I. Podsumowanie zagadnień omawianych w ramach kursu • pytania uczestników, • dyskusja.	13.30 – 16.00
ZAKOŃCZENIE SZKOLENIA - WYDANIE CERTYFIKATÓW	16.00 - 16.15
POŻEGNANIE UCZESTNIKÓW	