PRAKTYCZNE
ROZWIĄZANIA

Praktyczny kurs IOD (4-dniowy)

kompleksowe przygotowanie do pełnienia funkcji inspektora ochrony danych

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. 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 – 11.10

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, • prawo do niepodlegania profilowaniu, • zasada przejrzystości.	11.10 –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 – 15.45

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, w tym kryteria ustalenia wysokości kar.	15.45 – 17.15
INDYWIDUALNE KONSULTACJE	17.15 – 17.30

DZIEŃ II

PRZYGOTOWANIE PLANU WDROŻENIA I AUDYT ZGODNOŚCI	GODZINY
MODUŁ I	
I. Wyjaśnienie najważniejszych pojęć związanych z audytem (m.in.): • 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: • rzetelność, • uczciwe przedstawienie wyników, • należyta staranność zawodowa, • poufność, • niezależność, • podejście oparte na dowodach.	9.00 – 11.15

MODUŁ II	
I. Ustalanie struktury odpowiedzialnej za przeprowadzanie audytu • ustalenia proceduralne, • wybór członków zespołu audytującego, • harmonogram prac. II. Przygotowanie działań audytowych • określenie wykonalności audytu, • przygotowanie planu audytowego (omówienie wzoru), • przydzielenie pracy zespołowi audytującemu, • przygotowanie dokumentów roboczych, • inicjowanie audytu, • przebieg procesu audytowania.	11.15 –13.30
MODUŁ III	
I. Działania audytowe • spotkanie otwierające • przegląd dokumentacji podczas przeprowadzania audytu, • komunikowanie się podczas audytu, • wyznaczenie roli 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
II. Działania po audytowe • 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	
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. • cel szacowania ryzyka, • korzyści z wykonania szacowania ryzyka, • kryteria oceny ryzyka, • szacowanie ryzyka, • poziom ryzyka.	11.15 – 13.00
LUNCH	13.00 – 13.30

MODUŁ III	
I. Ćwiczenia z zakresu wykonania analizy ryzyka. • szacowanie prawdopodobieństwa wystąpienia zagrożenia, • identyfikacja podatności, • identyfikacja 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

DZIEŃ IV

DOSTOSOWANIE PROCESÓW, DOKUMENTACJI I ŚRODOWISKA TELEINFORMATYCZNEGO	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 - możliwe sposoby realizacji.	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.15
MODUŁ II	
I. Techniczne środki ochrony danych osobowych • 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. 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 W DNIU ZAKOŃCZENIA KURSU	16:00 – 16:15
ZAKOŃCZENIE SZKOLENIA - WYDANIE CERTYFIKATÓW	16.15 - 16.30