Możliwość dofinansowania

ODO 24 sp. z o.o.

4,6 / 5

4 oceny

Praktyczny kurs dla IOD. Kompleksowo przygotujemy Cię do pełnienia funkcji inspektora ochrony danych osobowych (IOD)

Numer usługi 2026/08/18/7492/3752456

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 31:45 h
- 19.10.2026 do 22.10.2026

3 198,00 PLN brutto
2 600,00 PLN netto
100,72 PLN brutto/h
81,89 PLN netto/h
154,81 PLN cena rynkowa

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo Unii Europejskiej
Grupa docelowa usługi	Usługa jest skierowana do osób, które pełnią lub planują pełnić funkcję Inspektora Ochrony Danych (IOD), a także do osób odpowiedzialnych za ochronę danych osobowych i zapewnienie zgodności procesów przetwarzania danych z przepisami. W szczególności do osób rozpoczynających pracę jako IOD, obecnych IOD chcących poszerzyć wiedzę i umiejętności praktyczne, pracowników odpowiedzialnych za audyty zgodności, analizę ryzyka, DPIA i obsługę naruszeń oraz osób współpracujących z IOD w obszarze prawnym, organizacyjnym, bezpieczeństwa informacji lub IT. Kurs przeznaczony zarówno dla osób z doświadczeniem w ochronie danych, jak i osób rozpoczynających pracę w tym obszarze. Program obejmuje zagadnienia od podstaw RODO po praktyczne wykonywanie zadań IOD, audyt, analizę ryzyka, DPIA i bezpieczeństwo IT.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	14
Data zakończenia rekrutacji	16-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do samodzielnego wykonywania zadań Inspektora Ochrony Danych (IOD), w szczególności do oceny zgodności procesów przetwarzania danych, przeprowadzania audytów, analizy ryzyka i DPIA, obsługi naruszeń oraz oceny stosowanych zabezpieczeń organizacyjnych i technicznych, zgodnie z wymaganiami RODO.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje podstawowe zasady i wymagania RODO w odniesieniu do procesów przetwarzania danych osobowych.	Kryteria weryfikacji: rozróżnia podstawowe pojęcia związane z ochroną danych osobowych; wskazuje właściwe zasady przetwarzania danych osobowych w przedstawionym przypadku; wskazuje właściwą podstawę prawną przetwarzania danych w przedstawionym przypadku; rozpoznaje obowiązki administratora, podmiotu przetwarzającego, współadministratora oraz IOD; wskazuje prawa osób, których dane dotyczą, właściwe dla przedstawionej sytuacji; identyfikuje obowiązki organizacji związane z bezpieczeństwem i zgodnością przetwarzania danych.	Test teoretyczny
Uczestnik ocenia zgodność procesu przetwarzania danych osobowych oraz przygotowuje założenia audytu ochrony danych.	Kryteria weryfikacji: określa zakres i cel audytu na podstawie przedstawionego przypadku; wskazuje czynności przygotowawcze niezbędne do przeprowadzenia audytu; dobiera właściwe kryteria oceny zgodności; identyfikuje niezgodności i obszary wymagające działań naprawczych; dobiera właściwe elementy dokumentacji audytowej; formułuje wnioski wynikające z przeprowadzonej oceny.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik przeprowadza analizę ryzyka związanego z przetwarzaniem danych osobowych.	Kryteria weryfikacji: identyfikuje zasoby związane z analizowanym procesem przetwarzania; identyfikuje zagrożenia i podatności; wskazuje istniejące zabezpieczenia; ocenia prawdopodobieństwo wystąpienia zagrożenia; określa następstwa wystąpienia zagrożenia; określa poziom zidentyfikowanego ryzyka; określa próg akceptowalności ryzyka.	Obserwacja w warunkach symulowanych
Uczestnik określa sposób przeprowadzenia oceny skutków dla ochrony danych (DPIA) dla wskazanego procesu przetwarzania.	Kryteria weryfikacji: rozpoznaje sytuacje, w których przeprowadzenie DPIA jest wymagane; określa kontekst analizowanego procesu przetwarzania; identyfikuje zasoby i ryzyka związane z procesem; wskazuje podstawowe elementy DPIA; identyfikuje potencjalne zagrożenia dla praw i wolności osób fizycznych; dobiera działania ograniczające zidentyfikowane ryzyko.	Obserwacja w warunkach symulowanych
Uczestnik określa właściwy sposób postępowania w przypadku naruszenia ochrony danych osobowych.	Kryteria weryfikacji: rozpoznaje naruszenie ochrony danych na podstawie przedstawionego przypadku; klasyfikuje naruszenie z uwzględnieniem jego charakteru i potencjalnych skutków; wskazuje działania, które należy podjąć po stwierdzeniu naruszenia; określa informacje wymagające udokumentowania; wskazuje przesłanki i sposób zgłoszenia naruszenia organowi nadzorczemu; dobiera działania ograniczające skutki naruszenia.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje zagrożenia i podatności związane z bezpieczeństwem danych osobowych w środowisku IT oraz dobiera adekwatne środki ochrony.	Kryteria weryfikacji: identyfikuje zagrożenia związane z cyberatakami, socjotechniką, spoofingiem i DDoS; identyfikuje podatności w przedstawionym środowisku IT; ocenia podstawowe mechanizmy kontroli dostępu i uwierzytelniania; wskazuje zagrożenia związane z siecią, pracą zdalną i usługami chmurowymi; dobiera odpowiednie techniczne i organizacyjne środki ochrony danych; wskazuje działania związane z wykrywaniem i ograniczaniem podatności technicznych.	Obserwacja w warunkach symulowanych
Uczestnik dobiera i wykorzystuje właściwe wzory dokumentacji RODO do realizacji zadań związanych z ochroną danych osobowych.	Kryteria weryfikacji: dobiera właściwy wzór dokumentu do przedstawionej sytuacji; określa cel i zastosowanie wybranego dokumentu; prawidłowo wykorzystuje wybrany wzór w przedstawionym przypadku; wskazuje informacje wymagające uzupełnienia lub dostosowania do specyfiki organizacji; rozróżnia dokumentację dotyczącą audytu, DPIA, analizy ryzyka, naruszeń, realizacji praw osób, procesorów oraz bezpieczeństwa IT.	Analiza dowodów i deklaracji

Cel biznesowy

Do zakończenia 32-godzinnej usługi uczestnik przygotuje i przećwiczy zastosowanie praktycznych rozwiązań wspierających organizację w zarządzaniu ochroną danych osobowych, obejmujących ocenę zgodności procesu przetwarzania danych, przygotowanie założeń audytu, przeprowadzenie analizy ryzyka, określenie sposobu postępowania w ramach DPIA, klasyfikację naruszenia ochrony danych oraz dobór organizacyjnych i technicznych środków ochrony danych. Osiągnięcie celu zostanie potwierdzone prawidłowym wykonaniem zadań praktycznych i analiz przypadków przewidzianych w programie usługi.

Efekt usługi

Efekt 1. Ocena zgodności przetwarzania danych osobowych

Efekt usługi:

Uczestnik ocenia zgodność procesu przetwarzania danych osobowych z wymaganiami RODO.

Kryteria weryfikacji:

- identyfikuje podstawę prawną przetwarzania danych w przedstawionym przypadku,
- wskazuje właściwe zasady przetwarzania danych,
- rozpoznaje obowiązki administratora, procesora lub współadministratora,

- identyfikuje niezgodności oraz obszary wymagające działań naprawczych.

Efekt 2. Planowanie i przeprowadzanie audytu zgodności

Efekt usługi:

Uczestnik przygotowuje i przeprowadza podstawowe czynności związane z audytem zgodności ochrony danych osobowych.

Kryteria weryfikacji:

- określa zakres i cel audytu na podstawie przedstawionego przypadku,
- wskazuje czynności przygotowawcze niezbędne przed rozpoczęciem audytu,
- dobiera elementy dokumentacji roboczej i kryteria oceny zgodności,
- formułuje wnioski dotyczące stwierdzonych niezgodności.

Efekt 3. Analiza ryzyka ochrony danych

Efekt usługi:

Uczestnik przeprowadza analizę ryzyka związanego z przetwarzaniem danych osobowych.

Kryteria weryfikacji:

- identyfikuje zasoby, zagrożenia i podatności,
- wskazuje istniejące zabezpieczenia,
- ocenia prawdopodobieństwo wystąpienia zagrożenia i jego następstwa,
- określa poziom ryzyka oraz próg jego akceptowalności.

Efekt 4. Ocena skutków dla ochrony danych (DPIA)

Efekt usługi:

Uczestnik określa sposób przeprowadzenia oceny skutków dla ochrony danych (DPIA) dla wskazanego procesu przetwarzania.

Kryteria weryfikacji:

- rozpoznaje sytuacje wymagające przeprowadzenia DPIA,
- identyfikuje procesy, zasoby i ryzyka wymagające uwzględnienia w DPIA,
- wskazuje podstawowe elementy oceny skutków dla ochrony danych,
- dobiera działania ograniczające zidentyfikowane ryzyko.

Efekt 5. Zarządzanie naruszeniami ochrony danych

Efekt usługi:

Uczestnik prawidłowo reaguje na naruszenie ochrony danych osobowych.

Kryteria weryfikacji:

- rozpoznaje i klasyfikuje naruszenie na podstawie przedstawionego przypadku,
- wskazuje właściwą procedurę postępowania,
- określa działania wymagane w związku z naruszeniem,
- wskazuje, kiedy i w jaki sposób należy zgłosić naruszenie organowi nadzorczemu.

Efekt 6. Ocena bezpieczeństwa technicznego danych osobowych

Efekt usługi:

Uczestnik identyfikuje podstawowe zagrożenia i podatności związane z bezpieczeństwem danych osobowych w środowisku IT oraz dobiera odpowiednie środki ochrony.

Kryteria weryfikacji:

- identyfikuje zagrożenia związane z cyberatakami i nieuprawnionym dostępem,
- rozpoznaje podatności w przedstawionym środowisku IT,
- ocenia stosowane środki kontroli dostępu, zabezpieczenia sieci, chmury i pracy zdalnej,

- dobiera adekwatne techniczne i organizacyjne środki ochrony danych.

Efekt 7. Wykorzystanie dokumentacji wspierającej realizację obowiązków IOD

Efekt usługi:

Uczestnik dobiera i wykorzystuje właściwe wzory dokumentacji RODO do realizacji zadań związanych z ochroną danych osobowych w organizacji.

Kryteria weryfikacji:

- dobiera właściwy dokument do przedstawionego procesu lub sytuacji związanej z ochroną danych osobowych,
- wskazuje cel i zastosowanie wybranego dokumentu,
- prawidłowo wykorzystuje wybrany wzór dokumentu w przedstawionym przypadku,
- wskazuje informacje wymagające uzupełnienia lub dostosowania dokumentu do specyfiki organizacji,
- rozróżnia dokumentację dotyczącą audytu, analizy ryzyka, DPIA, naruszeń, realizacji praw osób, procesorów oraz bezpieczeństwa systemów IT.

Metoda potwierdzenia osiągnięcia efektu usługi

Osiągnięcie efektów usługi zostanie potwierdzone na podstawie wykonania przez uczestnika zadań praktycznych i analiz przypadków związanych z ochroną danych osobowych, zgodnie z kryteriami weryfikacji określonymi dla poszczególnych efektów usługi.

W ramach weryfikacji uczestnik wykona zadania dotyczące m.in. oceny zgodności procesu przetwarzania danych, przygotowania założeń audytu, analizy ryzyka, oceny skutków dla ochrony danych (DPIA), postępowania w przypadku naruszenia ochrony danych oraz identyfikacji zagrożeń i doboru środków ochrony w środowisku IT.

Potwierdzeniem osiągnięcia efektów będą wypełnione przez uczestnika arkusze i formularze wykorzystywane podczas ćwiczeń, w tym dokumentacja dotycząca audytu, analizy ryzyka i DPIA, oraz wyniki końcowej weryfikacji wiedzy. Ocena będzie prowadzona na podstawie poprawności wykonania zadań i zgodności zastosowanych rozwiązań z kryteriami weryfikacji.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Dzień I – RODO od podstaw

Rejestracja i rozpoczęcie usługi

- rejestracja uczestników,
- przedstawienie organizacji szkolenia,
- określenie oczekiwań uczestników oraz zagadnień wymagających szczególnego omówienia,
- test sprawdzający poziom wiedzy uczestników.

Moduł I. Zgodność z RODO i podstawowe zagadnienia ochrony danych

1. Zgodność z RODO – znaczenie i praktyczne konsekwencje dla organizacji.
2. Najważniejsze pojęcia związane z ochroną danych osobowych, w tym:
   - dane osobowe,
   - dane osobowe szczególnych kategorii,
   - przetwarzanie,
   - profilowanie,
   - pseudonimizacja,
   - administrator,
   - współadministratorzy,
   - podmiot przetwarzający,
   - odbiorca danych.
3. Wyznaczenie Inspektora Ochrony Danych:
   - kiedy wyznaczenie IOD jest obligatoryjne,
   - regularne i systematyczne monitorowanie,
   - pojęcie dużej skali,
   - konflikt interesów i zadania, których IOD nie powinien wykonywać,
   - zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych.
4. Zasady przetwarzania danych osobowych:
   - zgodność z prawem i przejrzystość,
   - podstawy przetwarzania danych,
   - warunki udzielenia zgody,
   - ograniczenie celu,
   - minimalizacja danych,
   - prawidłowość,
   - ograniczenie przechowywania,
   - integralność i poufność,
   - rozliczalność.

Moduł II. Prawa osób i obowiązki administratora

1. Prawa osób, których dane dotyczą:
   - prawo do uzyskania informacji i obowiązek informacyjny,
   - prawo dostępu do danych,
   - prawo do sprostowania danych,
   - prawo do usunięcia danych,
   - prawo do ograniczenia przetwarzania,
   - prawo do przenoszenia danych,
   - prawo do sprzeciwu,
   - prawo do niepodlegania profilowaniu,
   - zasada przejrzystości.
2. Obowiązki administratora danych:
   - privacy by design i privacy by default,
   - rejestrowanie czynności przetwarzania,
   - bezpieczeństwo przetwarzania,
   - zgłaszanie naruszeń ochrony danych do PUODO,

- zawiadamianie osób, których dane dotyczą, o naruszeniach,
- ocena skutków dla ochrony danych (DPIA).

Moduł III. Procesorzy, transfery danych i organ nadzorczy

1. Podmiot przetwarzający:
   - obowiązki procesora,
   - elementy umowy powierzenia przetwarzania danych.
2. Przekazywanie danych do państw trzecich i organizacji międzynarodowych.
3. Prezes Urzędu Ochrony Danych Osobowych:
   - postępowania kontrolne,
   - administracyjne kary pieniężne,
   - certyfikacja i akredytacja.

Zakończenie dnia

- indywidualne konsultacje z uczestnikami.

Dzień II – IOD w praktyce

Moduł I. Organizacja systemu ochrony danych i praca IOD

1. Wybór modelu zarządzania ochroną danych osobowych:
   - warunki skutecznego systemu ochrony danych,
   - modele zarządzania ochroną danych,
   - podział ról i obowiązków w procesach ochrony danych.
2. Pozycja, praca i kwalifikacje Inspektora Ochrony Danych:
   - wiedza i umiejętności niezbędne IOD,
   - źródła wiedzy,
   - gwarancje wykonywania zadań IOD,
   - zadania IOD,
   - case study dotyczące rozpoczęcia pracy na stanowisku IOD.
3. Rozpoznawanie przepływów danych w organizacji:
   - identyfikowanie procesów i przepływów danych,
   - znaczenie przepływów danych dla realizacji zadań IOD,
   - praktyczne zastosowanie wiedzy o przepływach danych,
   - case study.

Moduł II. Audyt zgodności

1. Przygotowanie i przeprowadzenie audytu:
   - czynności przygotowawcze,
   - przygotowanie planu audytowego,
   - przydzielenie zadań zespołowi audytującemu,
   - przygotowanie dokumentów roboczych,
   - wykorzystanie arkusza audytowego i checklisty,
   - przebieg procesu audytowania.
2. Ocenianie stopnia zgodności:
   - bezpieczeństwo przetwarzania,
   - podstawy przetwarzania,
   - zasady wyrażenia zgody,
   - minimalizacja danych,
   - przejrzystość,
   - powierzenie przetwarzania,
   - międzynarodowy transfer danych osobowych.

Moduł III. Raportowanie i utrzymywanie zgodności

1. Przygotowanie raportu z audytu.

2. Budowanie świadomości pracowników w zakresie ochrony danych.
3. Polityki ochrony danych osobowych.
4. Privacy by design i privacy by default w praktyce – case study.
5. Obsługa żądań osób, których dane dotyczą.
6. Realizacja prawa dostępu – case study.
7. Weryfikacja gwarancji zapewnianych przez procesora.
8. Ocena ról podmiotów uczestniczących w przetwarzaniu, w tym współadministrowanie.
9. Utrzymywanie zgodności w bieżącej działalności organizacji.

Moduł IV. Zarządzanie naruszeniami i przygotowanie do kontroli

1. Zarządzanie naruszeniami ochrony danych osobowych:
   - procedura postępowania w przypadku stwierdzenia naruszenia,
   - ocena i klasyfikacja naruszeń – case study,
   - zgłaszanie naruszeń – case study.

2. Przygotowanie organizacji do kontroli PUODO:
   - organizacja postępowania w przypadku kontroli,
   - identyfikowanie obszarów wymagających przygotowania,
   - praktyczne zastosowanie procedur związanych z ochroną danych.

Zakończenie dnia

- indywidualne konsultacje z uczestnikami.

Dzień III – DPIA i analiza ryzyka

Moduł I. Zarządzanie ryzykiem ochrony danych osobowych

1. Wprowadzenie do zarządzania ryzykiem:
   - podstawowe pojęcia,
   - organizacja procesu szacowania ryzyka,
   - wybrane metodyki szacowania ryzyka,
   - elementy procesu DPIA.

2. Badanie kontekstu przetwarzania danych osobowych:
   - określanie kontekstu zewnętrznego,
   - określanie kontekstu wewnętrznego,
   - ćwiczenia z określania kontekstu procesu szacowania ryzyka.

3. Zabezpieczenia minimalizujące ryzyko według RODO/GDPR.

Moduł II. Ocena skutków dla ochrony danych (DPIA)

1. Czym jest DPIA i jaki jest cel jej wykonania.
2. Sytuacje, w których przeprowadzenie DPIA jest obligatoryjne.
3. Niezbędne elementy procesu DPIA.
4. Inwentaryzacja procesów przetwarzania.
5. Identyfikowanie zasobów związanych z przetwarzaniem mogącym powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
6. Wykonanie oceny skutków dla ochrony danych oraz szacowanie ryzyka dla zasobu przetwarzającego dane osobowe.

Moduł III. Praktyczna analiza ryzyka

1. Ćwiczenia z wykonania analizy ryzyka:
   - szacowanie prawdopodobieństwa wystąpienia zagrożenia,
   - identyfikacja podatności,
   - identyfikacja istniejących zabezpieczeń,
   - ocena efektywności istniejących zabezpieczeń,
   - szacowanie następstw,
   - identyfikacja ryzyka,
   - określanie poziomu ryzyka,

- określanie progu akceptowalności ryzyka.

2. Ćwiczenia z identyfikacji zasobów i zabezpieczeń.
3. Ustalanie wartości ryzyka procesu dla zasobu.
4. Praktyczne zastosowanie metodyki szacowania ryzyka.

Moduł IV. Postępowanie z ryzykiem i współpraca z organem nadzorczym

1. Przygotowanie planu postępowania z ryzykiem:
   - obniżanie i redukcja ryzyka,
   - unikanie ryzyka,
   - transfer ryzyka.

2. Konsultacje z organem nadzorczym:
   - zakres informacji przekazywanych organowi nadzorczemu,
   - uprawnienia organu nadzorczego.

Zakończenie dnia

- indywidualne konsultacje z uczestnikami.

Dzień IV – Dostosowanie IT

Moduł I. Cyberzagrożenia i bezpieczeństwo systemów informatycznych

1. Rodzaje cyberzagrożeń:
   - metody socjotechniczne,
   - identyfikowanie zagrożeń wynikających z socjotechniki,
   - ataki spoofingowe,
   - zagrożenia wynikające z ataków DDoS.

2. Systemy informatyczne i ich funkcjonalności bezpieczeństwa:
   - identyfikacja systemów informatycznych,
   - zarządzanie dostępem użytkowników,
   - polityka haseł,
   - symulacja ataku na stronę logowania,
   - kontrola dostępu do systemów i aplikacji,
   - zarządzanie informacjami uwierzytelniającymi użytkowników,
   - privacy by design i privacy by default.

Moduł II. Bezpieczeństwo sieci, komunikacji i usług chmurowych

1. Bezpieczeństwo sieci i komunikacji:
   - bezpieczeństwo sieci LAN,
   - monitoring sieci,
   - bezpieczeństwo pracy zdalnej,
   - kryptografia.

2. Bezpieczeństwo usług chmurowych:
   - kontrola dostępu,
   - zarządzanie tożsamością użytkowników,
   - szyfrowanie danych w chmurze,
   - niezbędne elementy umowy SLA.

Moduł III. Techniczne środki ochrony danych i zarządzanie podatnościami

1. Techniczne środki ochrony danych osobowych:
   - ochrona antywirusowa,
   - kontrola dostępu fizycznego,
   - infrastruktura serwerowa,
   - zabezpieczenia przed nieuprawnionym dostępem fizycznym,
   - bezpieczeństwo urządzeń mobilnych,
   - bezpieczeństwo systemów wydruku.

2. Zarządzanie podatnościami technicznymi:
    - wykrywanie podatności,
    - zarządzanie ryzykiem,
    - reagowanie na podatności i ich eliminowanie,
    - narzędzia do wykrywania podatności.

3. Dokumentacja przetwarzania danych osobowych w kontekście bezpieczeństwa IT.

Zakończenie usługi

1. Indywidualne konsultacje.
2. Test sprawdzający poziom wiedzy uczestników.
3. Podsumowanie szkolenia.
4. Zakończenie usługi i wydanie certyfikatów.
5. Omówienie możliwości dalszego wykorzystania wiedzy, dokumentacji i narzędzi otrzymanych w ramach usługi.

Metody pracy podczas usługi

Usługa ma charakter praktyczny i łączy przekazywanie wiedzy z analizą przypadków, ćwiczeniami oraz pracą z dokumentacją wykorzystywaną w ochronie danych osobowych. W szczególności wykorzystywane są:

- analiza przypadków (case study),
- ćwiczenia z analizy ryzyka i DPIA,
- ćwiczenia dotyczące audytu zgodności,
- praca z arkuszami, formularzami i wzorami dokumentacji RODO,
- analiza sytuacji związanych z naruszeniami ochrony danych,
- ćwiczenia dotyczące bezpieczeństwa systemów IT,
- konsultacje indywidualne z uczestnikami,
- testy sprawdzające poziom wiedzy.

Program prowadzi uczestnika od podstawowych zagadnień RODO, przez praktyczne wykonywanie zadań IOD, audyt i ocenę zgodności, zarządzanie ryzykiem i DPIA, aż po zagadnienia bezpieczeństwa technicznego i współpracę obszaru ochrony danych z IT.

Harmonogram

Liczba pozycji harmonogramu: 29

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Rejestracja uczestników	Zajęcia	Marta Bogusz	19-10-2026	09:00	09:05	00:05
2 z 29 Określenie oczekiwań uczestników i obszarów wymagających szczególnego omówienia	Zajęcia	Marta Bogusz	19-10-2026	09:05	09:15	00:10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 29 Moduł I: Zgodność z RODO, podstawowe pojęcia, wyznaczenie IOD i zasady przetwarzania danych	Zajęcia	Marta Bogusz	19-10-2026	09:30	11:00	01:30
4 z 29 -	Przerwa	-	19-10-2026	11:00	11:10	00:10
5 z 29 Moduł II: Prawa osób, których dane dotyczą oraz obowiązki administratora	Zajęcia	Marta Bogusz	19-10-2026	11:10	13:00	01:50
6 z 29 -	Przerwa	-	19-10-2026	13:00	13:30	00:30
7 z 29 Moduł III: Podmiot przetwarzający, umowy powierzenia i przekazywanie danych do państw trzecich	Zajęcia	Marta Bogusz	19-10-2026	13:30	15:30	02:00
8 z 29 -	Przerwa	-	19-10-2026	15:30	16:00	00:30
9 z 29 Moduł IV: Prezes UODO, postępowania kontrolne, kary, certyfikacja i akredytacja	Zajęcia	Marta Bogusz	19-10-2026	16:00	17:00	01:00
10 z 29 Moduł I: Model zarządzania ochroną danych, rola IOD i przepływy danych	Zajęcia	Justyna Pergałowska	20-10-2026	09:00	11:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 29 -	Przerwa	-	20-10-2026	11:00	11:10	00:10
12 z 29 Moduł II: Przygotowanie i przeprowadzenie audytu oraz ocena stopnia zgodności	Zajęcia	Justyna Pergałowska	20-10-2026	11:10	13:00	01:50
13 z 29 -	Przerwa	-	20-10-2026	13:00	13:30	00:30
14 z 29 Moduł III: Przygotowanie raportu z audytu i utrzymywanie zgodności w organizacji	Zajęcia	Justyna Pergałowska	20-10-2026	13:30	15:30	02:00
15 z 29 -	Przerwa	-	20-10-2026	15:30	16:00	00:30
16 z 29 Moduł IV: Zarządzanie naruszeniami ochrony danych i gotowość do kontroli PUODO	Zajęcia	Justyna Pergałowska	20-10-2026	16:00	17:00	01:00
17 z 29 Moduł I: Zarządzanie ryzykiem ochrony danych, kontekst przetwarzania i zabezpieczenia minimalizujące ryzyko	Zajęcia	Tomasz Ochocki	21-10-2026	09:00	11:00	02:00
18 z 29 -	Przerwa	-	21-10-2026	11:00	11:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 29 Moduł II: DPIA, inwentaryzacja procesów i szacowanie ryzyka dla zasobów przetwarzających dane	Zajęcia	Tomasz Ochocki	21-10-2026	11:15	13:00	01:45
20 z 29 -	Przerwa	-	21-10-2026	13:00	13:30	00:30
21 z 29 Moduł III: Analiza ryzyka, identyfikacja zagrożeń, podatności, zabezpieczeń i określanie poziomu ryzyka	Zajęcia	Tomasz Ochocki	21-10-2026	13:30	15:30	02:00
22 z 29 -	Przerwa	-	21-10-2026	15:30	16:00	00:30
23 z 29 Moduł IV: Przygotowanie planu postępowania z ryzykiem i konsultacje z organem nadzorczym	Zajęcia	Tomasz Ochocki	21-10-2026	16:00	17:00	01:00
24 z 29 Moduł I: Cyberzagrożenia i funkcjonalności bezpieczeństwa systemów informatycznych	Zajęcia	Przemysław Stasiak	22-10-2026	09:00	11:00	02:00
25 z 29 -	Przerwa	-	22-10-2026	11:00	11:25	00:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 29 Moduł II: Bezpieczeństwo sieci, komunikacji, pracy zdalnej i usług chmurowych	Zajęcia	Przemysław Stasiak	22-10-2026	11:25	13:30	02:05
27 z 29 -	Przerwa	-	22-10-2026	13:30	14:15	00:45
28 z 29 Moduł III: Techniczne środki ochrony danych, zarządzanie podatnościami i dokumentacja przetwarzania danych	Zajęcia	Przemysław Stasiak	22-10-2026	14:15	16:30	02:15
29 z 29 -	Walidacja	-	22-10-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	31:45
w tym suma godzin zajęć	26:30
w tym suma godzin walidacji	00:30
w tym suma przerw	04:45
Suma godzin dydaktycznych bez przerw	36:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia

20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 198,00 PLN
Koszt przypadający na 1 uczestnika netto	2 600,00 PLN
Koszt osobogodziny brutto	100,72 PLN
Koszt osobogodziny netto	81,89 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	31:45

Prowadzący

Liczba prowadzących: 4

1 z 4

Marta Bogusz

Adwokat z wieloletnim doświadczeniem procesowym, ukończyła prawo na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, a następnie aplikację adwokacką przy Izbie Adwokackiej w Warszawie.

W tematach prawnych działa twórczo. Specjalizuje się w:
- ustalaniu podstaw przetwarzania (art. 6 RODO),
- zadaniach IOD (art. 39 RODO),
- obsłudze zawiadomień, zgłoszeń i rejestracji naruszeń ochrony danych osobowych (art. 33-34 RODO),
- tworzeniu i opiniowaniu umów powierzenia przetwarzania danych osobowych (art. 28 RODO).

Przykłady zrealizowanych projektów:
1.Pomoc przy wdrożeniu nowej aplikacji (data protection by design) do zarządzania personelem.
2.Dostosowanie procesu kredytu konsumenckiego do wymagań RODO.
3.Przygotowanie regulaminu zakładowego funduszu świadczeń socjalnych w części dotyczącej ochrony danych osobowych.
4.Regulacja współpracy z agencją pracy tymczasowej.
5.Przygotowanie polityki prywatności i plików cookie dla firmy motoryzacyjnej.

2 z 4

Justyna Pergałowska

Od 2020 roku wpisana na listę radców prawnych przy Okręgowej Izbie Radców Prawnych w Warszawie. Ukończyła studia podyplomowe z zakresu ochrony danych osobowych i informacji niejawnych na Akademii Leona Koźmińskiego. Jest członkiem Sekcji Prawa Ochrony Danych Osobowych przy ORA Warszawa.Autorka publikacji o tematyce ochrony danych osobowych w magazynach branżowych.

Jestem zadaniowcem, dla którego nie ma problemów, są tylko wyzwania. Specjalizuje się w:
- opiniowaniu umów powierzenia (art. 28 RODO),
- obsłudze naruszeń i zawiadamianiu osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (art. 33 i 34 RODO)
- projektowaniu klauzul informacyjnych (art. 13 i 14 RODO),
- przeprowadzaniu audytów w zakresie zgodności z przepisami o ochronie danych osobowych (art. 24 RODO).

Przykłady zrealizowanych projektów:
1.Realizacja KPI w zakresie ochrony danych osobowych w spółkach energetycznych.
2.Wdrożenie RODO w spółce z branży stomatologicznej.
3.Przygotowanie polityki prywatności i plików cookie dla największego w Polsce dystrybutora środków ochrony roślin.
4.Obsługa naruszeń w firmie księgowo-konsultingowej.
5.Przeprowadzenie audytów w stowarzyszeniu oraz spółkach i firmach z branży energetycznej, HR, medycznej i dystrybucyjnej.

3 z 4

Tomasz Ochocki

Absolwent Akademii Obrony Narodowej na kierunku „Bezpieczeństwo narodowe” (specjalizacja zarządzanie kryzysowe). Ukończył studia podyplomowe z zakresu analizy bezpieczeństwa i zagrożeń terrorystycznych (Collegium Civitas) oraz ochrony danych osobowych i informacji niejawnych (Uniwersytet Kardynała Stefana Wyszyńskiego). Doktorant Szkoły Głównej Handlowej (Kolegium Ekonomiczno-Społeczne). Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001), systemu zarządzania ciągłością działania (ISO 22301) oraz audytor wewnętrzny systemu zarządzania informacjami o prywatności (ISO/IEC 27701). Współautor komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Odpowiada za pracę i rozwój zespołu merytorycznego. Specjalizuje się w:
- ochronie danych w fazie projektowania (art. 25 RODO),
- analizie ryzyka (art. 32 RODO),
- ocenie skutków dla ochrony danych (art. 35 RODO),
- zarządzaniu naruszeniami (art. 33 i 34 RODO).

Przykłady zrealizowanych projektów:
1.Stworzenie narzędzia do analizy ryzyka i DPIA.
2.Stworzenie narzędzia do ochrony danych osobowych w fazie projektowania.
3.Współtwórca narzędzia do oceny ryzyka związanej z transferem danych do państw trzecich (TIA).
4.Rozwój dokumentacji ochrony danych i bezpieczeństwa informacji.

4 z 4

Przemysław Stasiak

Absolwent Informatyki na Politechnice Łódzkiej. Dodatkowo ukończył studia podyplomowe o kierunku „Zarządzanie systemami Linux”. Posiada certyfikaty dotyczące bezpieczeństwa sieci i aplikacji, ochrony danych osobowych i znajomości rozwiązań chmurowych. Ukończył kurs pedagogiczny. Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001).

Zawsze z głową w chmurach, przede wszystkim w AZURE, AWS, Google. Specjalizuje się w:
- procedurach bezpieczeństwa (art. 24 ust. 2 RODO),
- ochronie danych w fazie projektowania (art. 25 RODO),
- analizie ryzyka (art. 32 ust. 1 RODO)
- bezpieczeństwie usług chmurowych (art. 32 ust. 1 lit. b RODO).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik przed rozpoczęciem usługi otrzymuje prezentacje szkoleniowe oraz kompletny zestaw wzorów dokumentacji RODO, obejmujący ponad 30 dokumentów wspierających realizację zadań IOD, w tym m.in. arkusz audytowy RODO, plan i raport z audytu, arkusz DPIA, procedurę DPIA, dokumentację naruszeń, rejestry, polityki ochrony danych oraz dokumentację dotyczącą bezpieczeństwa IT. Dokumentacja obejmuje obszar formalny oraz procedury zarządzania infrastrukturą informatyczną.

Po zakończeniu usługi uczestnik otrzymuje certyfikat potwierdzający udział, dostęp do poradników i materiałów edukacyjnych oraz dostęp do dodatkowych zasobów wspierających dalsze stosowanie wiedzy w praktyce. W ramach kursu uczestnik otrzymuje również 90-dniowy dostęp do aplikacji Dr RODO oraz możliwość korzystania ze wsparcia merytorycznego po szkoleniu.

Warunki uczestnictwa

Uczestnik nie musi posiadać wcześniejszego doświadczenia zawodowego ani specjalistycznej wiedzy z zakresu ochrony danych osobowych. Usługa jest przeznaczona zarówno dla osób rozpoczynających pracę w obszarze ochrony danych osobowych, jak i dla osób posiadających doświadczenie w realizacji zadań IOD.

Uczestnik powinien posiadać podstawową umiejętność obsługi komputera oraz możliwość korzystania z materiałów szkoleniowych w formie elektronicznej. W przypadku realizacji usługi w formie zdalnej wymagany jest komputer z dostępem do Internetu, wyposażony w mikrofon i kamerę.

Przed rozpoczęciem usługi uczestnik może określić swoje oczekiwania oraz zagadnienia, które wymagają szczególnego omówienia.

Warunki techniczne

Usługa jest realizowana online za pośrednictwem platformy Microsoft Teams.

Do udziału w usłudze uczestnik potrzebuje:

- komputera lub laptopa z dostępem do Internetu,
- stabilnego łącza internetowego umożliwiającego udział w transmisji audio i wideo,
- aktualnej przeglądarki internetowej lub aplikacji Microsoft Teams,
- sprawnego mikrofonu i głośników lub słuchawek,
- kamery internetowej umożliwiającej udział w zajęciach w formie wideo,
- adresu e-mail umożliwiającego otrzymanie linku do spotkania i materiałów szkoleniowych.

Materiały szkoleniowe są udostępniane uczestnikom w formie elektronicznej. Uczestnik powinien mieć możliwość otwierania i zapisywania dokumentów w formatach wykorzystywanych podczas szkolenia, w szczególności PDF i DOCX.

Przed rozpoczęciem usługi uczestnik otrzymuje informacje umożliwiające dołączenie do spotkania na platformie Microsoft Teams.

Kontakt

Dominik Kantorowicz

E-mail d.kantorowicz@odo24.pl

Telefon (+00) 690 004 852