Możliwość dofinansowania

Szkolenie: IOD + Cyberhigiena: ochrona danych i bezpieczna organizacja od zera

Numer usługi 2026/04/22/203083/3505669

2 300,00 PLN brutto
1 869,92 PLN netto
127,78 PLN brutto/h
103,88 PLN netto/h
196,00 PLN cena rynkowa

C4Y KATARZYNA ZASIECZNA

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
18 h
28.05.2026 do 29.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Osoby fizyczne rozpoczynające ścieżkę zawodową w obszarze ochrony danych i cyberbezpieczeństwa, w szczególności: • asystenci IOD, • junior specjaliści ds. ochrony danych, • koordynatorzy RODO, • młodsi specjaliści ds. compliance i cyberhigieny. Efektem szkolenia jest nabycie umiejętności umożliwiających rozpoczęcie pracy w roli: asystenta IOD, młodszego specjalisty ds. ochrony danych, koordynatora RODO lub junior compliance/cyberhigiena.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	27-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	18
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do samodzielnego wykonywania podstawowych zadań z zakresu ochrony danych osobowych i cyberhigieny w organizacji, w szczególności do: identyfikowania ról i obowiązków podmiotów przetwarzających dane, organizowania podstawowej dokumentacji RODO (RCP, procedura DSAR, rejestr incydentów), dobierania adekwatnych środków technicznych i organizacyjnych zgodnie z art. 32 RODO, reagowania na incydenty naruszenia ochrony danych i dokonywania wstępnej oceny ryzyka.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje role i obowiązki ADO, procesora i IOD oraz wyjaśnia zasady przetwarzania danych zgodnie z art. 5 RODO	rozróżnia role administratora, podmiotu przetwarzającego i IOD	Test teoretyczny
	wskazuje obowiązki IOD wynikające z art. 39 RODO	Test teoretyczny
	opisuje zasady przetwarzania danych (art. 5) na przykładach praktycznych	Test teoretyczny
Wyjaśnia wymagania art. 32 RODO oraz rozróżnia przykłady środków technicznych i organizacyjnych	identyfikuje przykłady środków technicznych (MFA, szyfrowanie, kopie zapasowe, logowanie zdarzeń)	Test teoretyczny
	wskazuje środki organizacyjne (polityki, szkolenia, onboarding/offboarding)	Test teoretyczny
	dopasowuje środek zabezpieczający do rodzaju zagrożenia	Test teoretyczny
	rozróżnia sytuacje wymagające zwiększonego poziomu zabezpieczeń	Test teoretyczny
Opisuje proces obsługi praw osób (DSAR) oraz procedurę reagowania na naruszenie ochrony danych (72h)	wskazuje etapy realizacji wniosku DSAR	Test teoretyczny
	określa terminy ustawowe i możliwe wyjątki	Test teoretyczny
	identyfikuje przesłanki zgłoszenia naruszenia do UODO	Test teoretyczny
	opisuje zasady komunikacji z osobą, której dane dotyczą	Test teoretyczny
Dobiera adekwatne środki zabezpieczenia do przykładowego procesu przetwarzania danych	analizuje opis procesu przetwarzania	Analiza dowodów i deklaracji
	identyfikuje potencjalne zagrożenia	Analiza dowodów i deklaracji
	wskazuje właściwe środki techniczne i organizacyjne	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opracowuje podstawowy wpis do Rejestru Czynności Przetwarzania (RCP) oraz formułuje klauzulę informacyjną	wskazuje elementy wymagane art. 30 RODO	Analiza dowodów i deklaracji
	prawidłowo określa cele, podstawy prawne i okres retencji	Analiza dowodów i deklaracji
	konstruuje klauzulę informacyjną zgodną z art. 13/14 RODO	Analiza dowodów i deklaracji
Projektuje schemat obsługi DSAR oraz dokonuje wstępnego triage incydentu	opracowuje schemat obsługi wniosku o dostęp/usunięcie danych	Analiza dowodów i deklaracji
	kwalifikuje incydent jako podlegający lub niepodlegający zgłoszeniu do UODO	Analiza dowodów i deklaracji
	wskazuje działania naprawcze	Analiza dowodów i deklaracji
	dokumentuje decyzję w karcie incydentu	Analiza dowodów i deklaracji
Analizuje scenariusz zagrożenia i dokonuje uproszczonej oceny ryzyka	identyfikuje podatność i potencjalny skutek naruszenia	Analiza dowodów i deklaracji
	określa prawdopodobieństwo i wagę skutku	Analiza dowodów i deklaracji
	proponuje działania ograniczające ryzyko	Analiza dowodów i deklaracji
Komunikuje wymagania RODO i cyberhigieny w sposób zrozumiały dla pracowników organizacji.	formułuje komunikaty bez użycia nadmiernej terminologii prawniczej	Analiza dowodów i deklaracji
	przedstawia konsekwencje naruszeń w sposób adekwatny do odbiorcy	Analiza dowodów i deklaracji

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

Szkolenie ma charakter praktyczno-warsztatowy i przygotowuje uczestników do samodzielnego realizowania podstawowych zadań z zakresu ochrony danych osobowych oraz organizacji cyberhigieny w podmiocie publicznym lub prywatnym.

Program obejmuje kompleksowe wprowadzenie do systemu ochrony danych zgodnie z przepisami RODO, organizację pracy Inspektora Ochrony Danych, projektowanie podstawowej dokumentacji (Rejestr Czynności Przetwarzania, procedura realizacji praw osób, rejestr incydentów), a także dobór adekwatnych środków technicznych i organizacyjnych zgodnie z art. 32 RODO.

W trakcie szkolenia uczestnicy pracują na szablonach dokumentów oraz analizują studia przypadków dotyczące m.in. phishingu, błędnego adresata, ransomware oraz obsługi wniosków DSAR.

Szkolenie realizowane jest w formule zdalnej w czasie rzeczywistym, z aktywnym udziałem uczestników w ćwiczeniach warsztatowych.

Szkolenie skierowane jest do osób rozpoczynających pracę lub planujących rozwój zawodowy w obszarze ochrony danych i cyberbezpieczeństwa, w szczególności:

- asystentów IOD,
- młodszych specjalistów ds. ochrony danych,
- koordynatorów RODO,
- pracowników działów compliance, HR, administracji i IT,
- osób przygotowujących się do pełnienia funkcji związanych z ochroną danych.

Szkolenie realizowane jest w formule zdalnej w czasie rzeczywistym (online na żywo).

W trakcie szkolenia wykorzystywane są:

- prezentacja multimedialna,
- współdzielenie ekranu,
- czat,
- praca na dokumentach w czasie rzeczywistym,
- ćwiczenia indywidualne i grupowe,
- studia przypadków.

Uczestnik powinien posiadać:

- komputer z dostępem do Internetu,
- sprawny mikrofon i kamerę,
- możliwość aktywnego udziału w ćwiczeniach warsztatowych.

Materiały szkoleniowe (szablony dokumentów, checklisty, prezentacja) przekazywane są w formie elektronicznej.

Program szkolenia

DZIEŃ 1 – RODO i organizacja systemu ochrony danych

09:00–09:15

Otwarcie szkolenia, przedstawienie celów i zasad pracy,

09:15–10:45

Moduł 1: RODO od podstaw

- zakres stosowania RODO
- role w organizacji (ADO, procesor, IOD)
- zasady przetwarzania danych (art. 5)
- zasada rozliczalności w praktyce

10:45–11:00 – Przerwa

11:00–12:30

Moduł 2: Zadania IOD i organizacja compliance (art. 39)

- niezależność IOD i konflikt interesów
- plan działań rocznych
- współpraca z IT i zarządem
- odpowiedzialność i dokumentowanie działań

12:30–13:15 – Przerwa obiadowa

13:15–14:45

Moduł 3: Legalność przetwarzania i projektowanie procesu

- podstawy prawne (art. 6)
- minimalizacja danych
- retencja i archiwizacja
- projektowanie procesu zgodnego z RODO

14:45–15:00 – Przerwa

15:00–16:15

Moduł 4: Obowiązek informacyjny i prawa osób (DSAR)

- zakres informacji (art. 13–14)
- terminy realizacji praw
- wyjątki i ograniczenia
- ryzyka organizacyjne

16:15–17:00

Warsztat 1 (praca praktyczna – miniportfolio)

- opracowanie schematu DSAR
- przygotowanie wzoru odpowiedzi (przypadek: dostęp/usunięcie danych)
- posumowanie dnia

Rezultat dnia 1:

Wersja robocza procedury DSAR.

DZIEŃ 2 – Cyberhigiena, art. 32 RODO, incydenty i dokumentacja

09:00–09:15

Rozpoczęcie dnia, najważniejsze informacje z poprzedniego dnia

09:15–10:30

Moduł 5: Cyberhigiena w organizacji – praktyczne minimum

- polityka haseł i MFA
- phishing i socjotechnika
- kopie zapasowe i szyfrowanie
- praca zdalna i BYOD
- zasady bezpiecznej komunikacji e-mail

10:30–10:45 – Przerwa

10:45–12:15

Moduł 6: Art. 32 w praktyce

- środki techniczne i organizacyjne
- zarządzanie uprawnieniami (IAM)
- onboarding/offboarding
- logi i monitoring
- dostawcy chmurowi

12:15–13:00 – Przerwa obiadowa

13:00–14:15

Moduł 7: Dokumentacja i współpraca z dostawcami

- Rejestr Czynności Przetwarzania (art. 30)
- powierzenie przetwarzania (art. 28)
- minimalne elementy umowy powierzenia
- lista kontrolna dostawcy

14:15–14:30 – Przerwa

14:30–15:15

Moduł 8: Incydenty i naruszenia ochrony danych

- triage incydentu
- decyzja o zgłoszeniu do UODO (72h)
- rejestr naruszeń
- komunikacja z osobą, której dane dotyczą
- studium przypadku (phishing, ransomware, błędny adresat)

15:15–16:15

Warsztat 2 (miniportfolio)

- wpis do RCP (1 proces)
- karta incydentu
- miniocena ryzyka

16:15–17:00

Walidacja - test teoretyczny i analiza dowodów i deklaracji

Rezultat dnia 2:

Wpis do RCP + karta incydentu + miniocena ryzyka.

Walidacja

Walidacja odbywa się w formie testu (15–25 pytań, w tym pytania scenariuszowe) oraz analiza dowodów i deklaracji.

Rozdzielność szkolenia od walidacji (rozdzielność osobowa): osoba prowadząca szkolenie nie przeprowadza końcowej walidacji. Wyniki walidacji są dokumentowane protokołem oraz arkuszem oceny/testem.

Czas trwania i organizacja

Łączny czas trwania: 16 godzin dydaktycznych (2 dni po 9 godzin dydaktycznych). Szkolenie realizowane w godzinach dydaktycznych. Przerwy nie są wliczone w czas trwania usługi. Liczba godzin teoretycznych: 8, liczba godzin praktycznych 9 + 1 h walidacja

Harmonogram

Liczba przedmiotów/zajęć: 19

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 19 Dzień 1: Otwarcie szkolenia, przedstawienie celów i zasad pracy (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	28-05-2026	09:00	09:15	00:15
2 z 19 Moduł 1: RODO od podstaw (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	28-05-2026	09:15	10:45	01:30
3 z 19 Przerwa	Grzegorz Dżuga	28-05-2026	10:45	11:00	00:15
4 z 19 Moduł 2: Zadania IOD i organizacja compliance (art. 39) (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	28-05-2026	11:00	12:30	01:30
5 z 19 Przerwa obiadowa	Grzegorz Dżuga	28-05-2026	12:30	13:15	00:45
6 z 19 Moduł 3: Legalność przetwarzania i projektowanie procesu (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	28-05-2026	13:15	14:45	01:30
7 z 19 Przerwa	Grzegorz Dżuga	28-05-2026	14:45	15:00	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 19 Moduł 4: Obowiązek informacyjny i prawa osób (DSAR) (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	28-05-2026	15:00	16:15	01:15
9 z 19 Warsztat 1 (praca praktyczna – miniportfolio) (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	28-05-2026	16:15	17:00	00:45
10 z 19 Dzień 2: Rozpoczęcie dnia, najważniejsze informacje z poprzedniego dnia szkolenia (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	29-05-2026	09:00	09:15	00:15
11 z 19 Moduł 5: Cyberhigiena w organizacji – praktyczne minimum (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	29-05-2026	09:15	10:30	01:15
12 z 19 Przerwa	Grzegorz Dżuga	29-05-2026	10:30	10:45	00:15
13 z 19 Moduł 6: Art. 32 w praktyce (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	29-05-2026	10:45	12:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 19 Przerwa obiadowa	Grzegorz Dżuga	29-05-2026	12:15	13:00	00:45
15 z 19 Moduł 7: Dokumentacja i współpraca z dostawcami (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	29-05-2026	13:00	14:15	01:15
16 z 19 Przerwa	Grzegorz Dżuga	29-05-2026	14:15	14:30	00:15
17 z 19 Moduł 8: Incydenty i naruszenia ochrony danych (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	29-05-2026	14:30	15:15	00:45
18 z 19 Warsztat 2 (miniportfolio) (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	Grzegorz Dżuga	29-05-2026	15:15	16:15	01:00
19 z 19 Walidacja - test teoretyczny, analiza dowodów i deklaracji (ćwiczenia, rozmowy na żywo, chat, współdzielenie ekranu)	-	29-05-2026	16:15	17:00	00:45

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	2 300,00 PLN
Koszt przypadający na 1 uczestnika netto	1 869,92 PLN
Koszt osobogodziny brutto	127,78 PLN
Koszt osobogodziny netto	103,88 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Grzegorz Dżuga

Doświadczenie w zakresie szkoleń i weryfikacji umiejętności:
Doświadczony nauczyciel akademicki w zakresie systemów operacyjnych i sieci komputerowych. Wykładowca na Wydziale Ekonomii i Zarządzania Politechniki Koszalińskiej w Zakładzie Zastosowań Informatyki w Ekonomii.
Prowadzi szkolenia z zakresu ochrony danych osobowych, bezpieczeństwa informacji, systemów operacyjnych oraz infrastruktury sieciowej. Weryfikuje efekty uczenia się uczestników poprzez testy wiedzy, analizę przypadków, zadania praktyczne oraz ocenę zgodności rozwiązań z wymaganiami normatywnymi (RODO, ISO 27001).
Wykształcenie i kwalifikacje:
Absolwent studiów podyplomowych na Wyższej Szkole Administracji Państwowej w Szczecinie – kierunek „Administrator Bezpieczeństwa Informacji".

Od 2015 roku zawodowo zajmuje się ochroną danych osobowych oraz budową i doskonaleniem systemów zarządzania bezpieczeństwem informacji. Od 2017 roku pełnił funkcję Administratora Bezpieczeństwa Informacji, a od 2018 roku działa jako Inspektor Ochrony Danych w kilkunastu jednostkach samorządu terytorialnego oraz podmiotach prywatnych.

Od 2017 r. audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-EN ISO/IEC 27001:2013, a od 2023 r. audytor wiodący ISO/IEC 27001:2022.

Specjalizuje się w wdrażaniu procedur bezpieczeństwa, analizie ryzyka, tworzeniu dokumentacji SZBI oraz zapewnianiu zgodności organizacji z wymogami RODO i norm międzynarodowych

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe (szablony dokumentów, checklisty, prezentacja) przekazywane są w formie elektronicznej.

Informacje dodatkowe

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej
- 1 godzina rozliczeniowa = 45 minut
- przerwy nie wliczają się do czasu szkolenia

- Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych

Zapisując się na usługę wyrażasz zgodę na rejestrowanie/nagrywanie swojego wizerunku na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów uczenia się.

Usługa może być zwolniona z VAT dla Uczestników, których poziom dofinansowania wynosi co najmniej 70% na podstawie § 3 ust. 1 pkt. 14 Rozporządzenia Ministrów Finansów z 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

Warunki techniczne

Platforma: MS Teams

iOS: iOS 11

Windows: Windows 10 kompilacja 14393

Android: Android OS 5.0

Funkcje sieci Web. Najnowsza wersja przeglądarki Safari, Internet Explorer 11, Chrome, Edge lub Firefox

Komputer Mac: MacOS 10.13

Połączenie internetowe: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach:

- dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie).

- dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie).

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Link: będzie udostępniony i umieszczony w karcie na 5 dni roboczych przed szkoleniem.

Kontakt

KATARZYNA ZASIECZNA

E-mail katarzynazasieczna@gmail.com
Telefon (+48) 668 163 580