Możliwość dofinansowania

Bezpieczeństwo informacji i ochrona danych osobowych - studia podyplomowe

Numer usługi 2025/07/02/9407/2852778

6 500,00 PLN brutto
6 500,00 PLN netto
40,63 PLN brutto/h
40,63 PLN netto/h

Akademia Górnośląska im. Wojciecha Korfantego w Katowicach

4,5 / 5

851 ocen

zdalna w czasie rzeczywistym
Studia podyplomowe
160 h
01.10.2025 do 30.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Adresatami studiów są osoby, zatrudnione oraz poszukujące zatrudnienia w obszarze ochrony danych osobowych, bezpieczeństwa informacji i zarządzania cyberbezpieczeństwem w organizacjach publicznych i prywatnych. Studia dedykowane są także specjalistom IT, pracownikom administracji, działów prawnych, audytu i compliance. Oferta kierowana jest również do Inspektorów Ochrony Danych (IOD), Inspektorów Bezpieczeństwa Informacji (IBI) oraz osób planujących objęcie tych funkcji, a także menedżerów odpowiedzialnych za politykę bezpieczeństwa informacji w swoich organizacjach. Studia będą także wartościowe dla osób planujących rozpoczęcie kariery w branży ochrony danych i cyberbezpieczeństwa, które chcą zdobyć praktyczne i poszukiwane na rynku pracy kompetencje w tym dynamicznie rozwijającym się sektorze.
Minimalna liczba uczestników	7
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	29-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	160
Podstawa uzyskania wpisu do BUR	art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742, z późn. zm.)

Zakres uprawnień	studia podyplomowe

Cel

Cel edukacyjny

Usługa "Bezpieczeństwo informacji i ochrona danych osobowych - studia podyplomowe" potwierdza przygotowanie do zarządzania bezpieczeństwem informacji, zapewnienia zgodności z przepisami o ochronie danych osobowych (RODO/GDPR) oraz pełnienia funkcji Inspektora Ochrony Danych (IOD) i Inspektora Bezpieczeństwa Informacji (IBI).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje regulacje prawne dotyczące ochrony danych osobowych i bezpieczeństwa informacji.	Rozróżnia przepisy RODO, NIS2 oraz AI Act. Wyjaśnia różnice między obowiązkami IOD a IBI.	Test teoretyczny
Wyjaśnia zasady funkcjonowania systemów bezpieczeństwa informacji i ryzyk z nimi związanych.	Identyfikuje elementy polityki bezpieczeństwa informacji. Opisuje metody analizy ryzyka.	Test teoretyczny
Analizuje zagrożenia wynikające z przetwarzania danych osobowych i cyfrowych incydentów.	Klasyfikuje typy incydentów i ich skutki. Wyjaśnia znaczenie prewencji (socjotechnika, OSiNT, DPIA).	Test teoretyczny
Ocenia zgodność przetwarzania danych z obowiązującymi przepisami.	Analizuje procedury wewnętrzne pod kątem zgodności z RODO. Projektuje plan działań naprawczych po wykryciu niezgodności.	Test teoretyczny
Projektuje polityki ochrony danych i bezpieczeństwa informacji w organizacji.	Opracowuje politykę bezpieczeństwa zgodną z ISO 27001. Wdraża dokumentację zgodną z wymaganiami PUODO.	Test teoretyczny
Monitoruje i reaguje na incydenty dotyczące bezpieczeństwa informacji.	Stosuje procedury obsługi incydentów bezpieczeństwa informacji. Sporządza dokumentację działań naprawczych i zgłoszeń do PUODO.	Test teoretyczny
Przestrzega zasad etycznych i prawnych w zakresie ochrony danych i informacji.	Identyfikuje sytuacje wymagające zachowania poufności. Uzasadnia konieczność ochrony sygnalistów i tajemnic zawodowych.	Test teoretyczny
Komunikuje się z interesariuszami w zakresie bezpieczeństwa informacji.	Inicjuje współpracę z wewnętrznymi działami w zakresie bezpieczeństwa. Przekazuje wyniki audytu w sposób adekwatny do poziomu wiedzy odbiorców.	Test teoretyczny Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1: Bezpieczeństwo informacji

1. Wprowadzenie do bezpieczeństwa informacji

Podstawowe pojęcia i definicje. Regulacje prawne dotyczące przetwarzania danych osobowych w przedsiębiorstwie.

Prawne aspekty ochrony bezpieczeństwa informacji i danych przetwarzanych w organizacji

Cyberbezpieczeństwo w sektorach krytycznych – NIS 2.

Wymiana danych na terenie UE w Data Act.

Wartość informacji i danych dla organizacji.

Zagrożenia dla bezpieczeństwa informacji.

2. Zarządzanie bezpieczeństwem informacji

Polityki bezpieczeństwa informacji.

Standardy bezpieczeństwa informacji (ISO 27001, ISO 27002).

Rola i zadania Inspektora Bezpieczeństwa Informacji (IBI).

Reakcja na incydent naruszenia bezpieczeństwa informacji

3. Analiza ryzyka i zarządzanie ryzykiem

Identyfikacja zagrożeń i podatności.

Ocena ryzyka i planowanie działań zapobiegawczych.

Metody monitorowania i przeglądów ryzyka.

Informatyczne narzędzia analizy zagrożeń i oceny ryzyk – SIEM, SOC

4. Bezpieczeństwo systemów informatycznych i sieciowych

Mechanizmy ochrony systemów informatycznych.

Najnowsze metody ochrony danych w organizacji (firewalle)

Zasady wykorzystywania sztucznej inteligencji w UE – AI Act.

Prawne aspekty ochrony bezpieczeństwa informacji

Podstawy kryptografii (szyfrowanie, podpis cyfrowy, certyfikaty).

Bezpieczeństwo w chmurze obliczeniowej i rozwiązania mobilne.

5. Audyt i monitorowanie bezpieczeństwa informacji

Fazy przeprowadzania audytów bezpieczeństwa informacji.

Analiza obszarów i procesów mających wpływ na bezpieczeństwo informacji

Raportowanie i dokumentowanie działań audytowych.

6. Reakcja na incydent dotyczących zagrożeń bezpieczeństwa informacji

Rola dowodów cyfrowych w przypadku wystąpienia incydentu w działalności organizacji.

Reakcja na incydent – informatyka śledcza, Blue Team, outsourcing bezpieczeństwa.

Metody prewencji wystąpienia incydentów bezpieczeństwa – socjotechnika, OSiNT, testy penetracyjne.

Moduł 2: Ochrona danych osobowych

7. Podstawy prawne ochrony danych osobowych

Ogólne rozporządzenie o ochronie danych (RODO/GDPR) w UE.

Polskie regulacje prawne z zakresu ochrony danych osobowych.

Zasady poprawnego przetwarzania danych osobowych.

Międzynarodowe standardy ochrony danych osobowych.

8. Zarządzanie ochroną danych osobowych

Rola i zadania Inspektora Ochrony Danych (IOD) w organizacji.

Tworzenie i wdrażanie polityk ochrony danych osobowych.

Procedury i mechanizmy zapewniania zgodności z RODO.

Obowiązkowa dokumentacja na wypadek kontroli z UODO.

9. Prawa osób, których dane dotyczą, i ich realizacja

Prawo do dostępu, poprawiania, usunięcia i przenoszenia danych.

Ograniczenie przetwarzania danych i tzw. Prawo do sprzeciwu.

Obsługa skarg i żądań związanych z ochroną danych osobowych.

10. Ocena skutków dla ochrony danych (DPIA)

Kiedy i jak przeprowadzać DPIA.

Identyfikacja ryzyk związanych z przetwarzaniem danych.

Opracowywanie planów zaradczych (naprawczych)

11. Incydenty ochrony danych osobowych i ich obsługa

Identyfikacja naruszeń ochrony danych.

Incydenty podlegające zgłoszeniu przez IODO.

Zgłoszenie incydentu naruszenia ochrony danych osobowych do PUODO w praktyce.

Dokumentowanie naruszeń i wdrażanie działań korygujących.

12. Aspekty ochrony danych osobowych i tajemnic zawodowych.

Prawne aspekty tajemnicy zawodowej (służbowej), tajemnica adwokacka.

Techniczne sposoby ochrony danych osobowych w organizacji.

Ochrona sygnalistów.

Współpraca pionów bezpieczeństwa z pozostałymi pionami organizacji oraz instytucjami odpowiedzialnymi za ochronę bezpieczeństwa.

13. Rola edukacji w ochronie danych osobowych i ochronie informacji w organizacji

Szkolenia i systematyczna kontrola wiedzy i umiejętności pracowniczych w obszarze ochrony informacji w organizacji.

Analiza zasobów technicznych w aspekcie aktualizacji polityk bezpieczeństwa organizacji.

Rola współpracy działów bezpieczeństwa z pionami w strukturze organizacji.

Przygotowanie szkoleń dot. poszczególnych zakresów ochrony informacji.

Warunki zaliczenia: pisemny egzamin końcowy.

Program studiów jest realizowany według godzin dydaktycznych (1h dydaktyczna = 45 minut (zegarowych)). Przerwy nie są wliczane w czas trwania usługi rozwojowej.

Czas trwania: 2 semestry.

Dni zajęć: sobota, niedziela w godz. 8:00-16:00.

Łączna ilość godzin: 160 godzin kontaktowych.

Program umożliwia uzyskanie 30 punktów ECTS.

Zajęcia na studiach prowadzone są w formie ćwiczeń, rozmów na żywo, analizy kazusów, testów, współdzielenia ekranu oraz dyskusji moderowanych na czacie w czasie rzeczywistym.

Zajęcia prowadzone są przez praktyków z dziedziny ochrony danych, cyberbezpieczeństwa i audytu.

Aktywizująca Uczestników forma prowadzenia zajęć pozwoli na wyćwiczenie umiejętności rozwiazywania problemów zarówno przedstawianych przez wykładowcę jak i podnoszonych na bieżąco przez słuchaczy.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	6 500,00 PLN
Koszt przypadający na 1 uczestnika netto	6 500,00 PLN
Koszt osobogodziny brutto	40,63 PLN
Koszt osobogodziny netto	40,63 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Wojtczak

Doktor nauk prawnych, adiunkt w Katedrze Prawa i Administracji Akademii Górnośląskiej im. Wojciecha Korfantego w Katowicach. Specjalizuje się w problematyce praw i wolności jednostki, środków ich ochrony oraz sądownictwa konstytucyjnego. Absolwent Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Autor licznych publikacji z zakresu prawa, uczestnik krajowych i międzynarodowych konferencji naukowych. Współpracuje z kancelariami prawnymi, realizując praktyczne projekty związane z analizą i interpretacją przepisów prawnych. Jego doświadczenie zawodowe obejmuje także bieżącą działalność dydaktyczną, w tym prowadzenie wykładów z zakresu prawa konstytucyjnego i ochrony praw człowieka.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne przekazywane są uczestnicom drogą elektroniczną - za pośrednictwem poczty e-mail.

Warunki uczestnictwa

Na studia przyjmowane są osoby z wyższym wykształceniem.

Zapis w Bazie Usług Rozwojowych (BUR) nie jest równoznaczny z przyjęciem na studia w Uczelni. Warunkiem przyjęcia na studia jestrejestracja w systemie internetowej rekrutacji, złożenie kompletu wymaganych dokumentów oraz dopełnienie wszystkich formalności.

Informacje dodatkowe

Organizator zapewnia rozdzielność walidacji od procesu kształcenia.

Dokumentem potwierdzającym ukończenie studiów podyplomowych jest Świadectwo ukończenia studiów.

Usługi realizowane przez Akademię są zwolnione z VAT na podstawie Art. 43 ust. 1 pkt. 26 ustawy o Vat i §3 ust. 1 pkt 13 rozporządzeniaMinistra Finansów z dnia 20.12.2013 r. w sprawie wykonania niektórych przepisów ustawy o podatku od towarów i usług.

Warunki techniczne

Usługa realizowana zdalnie poprzez platformy Ms Teams, Zoom.

Minimalne wymagania sprzętowe: Urządzenie z dostępem do Internetu (telefon, tablet, komputer). Sprawny mikrofon i kamera internetowa.

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: download 8 mb/s, upload 8mb/s,ping15 ms.

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Zalecamy wykorzystanie przeglądarki internetowej najnowszej wersji.

Kontakt

SVITLANA BLINOVA

E-mail svitlana.blinova@akademiagornoslaska.pl

Telefon (+48) 32 3570 583