



Uniwersytet WSB
Merito w Poznaniu



Inspektor Ochrony Danych

Numer usługi 2024/06/11/7405/2179362

📍 Poznań / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

📖 Studia podyplomowe

🕒 160 h

📅 01.10.2024 do 30.06.2025

5 600,00 PLN brutto

5 600,00 PLN netto

35,00 PLN brutto/h

35,00 PLN netto/h

Informacje podstawowe

Kategoria	Prawo i administracja / Prawo ogólne
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	<ul style="list-style-type: none">osoby pełniące lub zamierzające zawodowo pełnić rolę Inspektora Ochrony Danych,konsultanci wspierający swoich klientów w przestrzeganiu przepisów RODO i przepisów krajowych,audytorzy i osoby kontrolujące przestrzeganie przepisów o ochronie danych osobowych,prawnicy, radcy prawni, adwokaci świadczący pomoc prawną dla swoich klientów w zakresie przepisów krajowych o ochronie danych i RODOpracownicy działów personalnych, IT, kadra kierownicza organów administracji publicznej (sekretarze, naczelnicy / dyrektorzy / kierownicy komórek organizacyjnych),
Minimalna liczba uczestników	18
Maksymalna liczba uczestników	33
Data zakończenia rekrutacji	30-09-2024
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną 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.)

Cel

Cel edukacyjny

Podstawowym celem studiów jest nabycie przez słuchaczy kompetencji niezbędnych do wykonywania funkcji Inspektora Ochrony Danych zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>Wiedza:</p> <ul style="list-style-type: none"> • Systematyzuje zagadnienia związane z międzynarodowymi oraz krajowymi regulacjami dotyczącymi ochrony danych osobowych. • Przyswaja koncepcje, narzędzia i metody wykorzystywane w zabezpieczeniu danych osobowych. • Poznaje zasady interpretacji przepisów o ochronie danych osobowych. 	<ul style="list-style-type: none"> • Przedstawia zagadnienia związane z międzynarodowymi oraz krajowymi regulacjami dotyczącymi ochrony danych osobowych • Interpretuje przepisy o ochronie danych osobowych • Wymienia koncepcje, narzędzia i metody wykorzystywane w zabezpieczeniu danych osobowych 	<p>Test teoretyczny</p> <p>Obserwacja w warunkach symulowanych</p>
<p>Umiejętności:</p> <ul style="list-style-type: none"> • Przygotowuje samodzielnie wzory formularzy, klauzule, dokumenty wymagane przez przepisy o ochronie prywatności. • Sporządza opinie na temat stosowania przepisów o ochronie danych osobowych. • Wskazuje odpowiednie argumenty prawne do stanu faktycznego. <p>Kompetencje społeczne:</p> <ul style="list-style-type: none"> • Samodzielnie poszukuje odpowiedzi na zagadnienia prawne. • Przygotowuje do prowadzenia prezentacji / szkoleń z zakresu przepisów prawa. • Przygotowuje do prowadzenia kontroli wewnętrznych z zachowaniem neutralności, asertywności i profesjonalizmu. 	<ul style="list-style-type: none"> • Tworzy wzory formularzy, klauzule, dokumenty wymagane przez przepisy o ochronie prywatności • Przedstawia odpowiednie argumenty prawne do stanu faktycznego • Prowadzi prezentacje / szkolenia z zakresu przepisów prawa • Prowadzi kontrole wewnętrzne z zachowaniem neutralności, asertywności i profesjonalizmu 	<p>Obserwacja w warunkach symulowanych</p> <p>Test teoretyczny</p> <p>Obserwacja w warunkach rzeczywistych</p> <p>Test teoretyczny</p>

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Świadectwo studiów podyplomowych zawiera program kierunku wraz ze zrealizowanymi godzinami i punktami ECTS. Absolwent uzyskuje zaświadczenie potwierdzające zdobyte efekty kształcenia.

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

Świadectwo ukończenia studiów podyplomowych jest wydawane na podstawie uzyskania pozytywnej oceny z każdego semestru zgodnie z Regulaminem Studiów Podyplomowych.

Studia kończą się zaliczeniem na ocenę określonym w karcie kierunku.

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

Świadectwo ukończenia studiów podyplomowych jest potwierdzeniem uzyskania pozytywnego wyniku z testu semestralnego i egzaminu końcowego.

Program

WSTĘP DO PRAWA DO OCHRONY DANYCH OSOBOWYCH (8 godz.)

- prawny system ochrony danych osobowych w UE i w Polsce
- rola TSUE, ETPC, NSA, WSA, Prezesa UODO w systemie
- funkcje i cele rozporządzenie UE nr 2016/679 i zakres przedmiotowy i podmiotowy rozporządzenia
- wybrane orzecznictwo w zakresie ochrony danych osobowych

WYKONYWANIE ZADAŃ INSPEKTORA OCHRONY DANYCH (8 godz.)

- kompetencje Inspektora Ochrony Danych
- niezależność funkcji Inspektora i konflikt interesu
- zakres zadań Inspektora
- określanie podmiotów zobligowanych do wyznaczenia Inspektora i omówienie art. 37-39 RODO

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH (8 godz.)

- zakres informacji obowiązkowych i dodatkowych w RCP
- sposób twierdzenia i korzystania z rejestru
- zasady tworzenia i aktualizowania RCP i RKCP i omówienie art. 30-31 RODO

SZTUCZNA INTELIGENCJA W OCHRONIE DANYCH OSOBOWYCH (8 godz.)

- zasady działania sztucznej inteligencji na przykładzie ChatGTP / Gemini
- wykorzystanie AI w pracy Inspektora Ochrony Danych
- ryzyka związane z korzystaniem z narzędzi opartych o sztuczną inteligencję

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH ORAZ POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH (8 godz.)

- omówienie zasad określonych w art. 5 (zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość danych, ograniczenie przechowywania, integralność i poufność) oraz art. 12 (przejrzysta komunikacja)
- zasady wyboru podmiotów przetwarzających
- zapisy niezbędne do umowy powierzenia przetwarzania

- różnice pomiędzy powierzaniem a udostępnianiem danych
- omówienie art. 5 RODO

PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH (8 godz.)

- szczegółowe omówienie podstaw prawnych
- wybrane podstawy prawne uzupełniające (będące obowiązkiem prawnym ciążącym na administratorze)
- przykłady podstaw prawnych danych osobowych w sektorze publicznymi i prywatnym
- omówienie art. 6, 9, 10 RODO

PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W REKRUTACJI I ZATRUDNIENIU (4 h)

- rekrutacje planowane i spontaniczne,
- postępowania z dokumentami rekrutacyjnymi
- podstawy prawne wybranych zagadnień z obszaru zatrudnienia: akta osobowe, szkolenia, BHP, ZFŚS, ewidencja czasu pracy, APT itd.
- monitoring wizyjny, poczty elektronicznej i innych form monitoringu pracowników
- omówienie przepisów Kodeksu pracy dotyczących przetwarzania danych osobowych oraz art. 88 RODO

PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH W MARKETINGU I SPRZEDAŻY (4 godz.)

- pozyskiwanie danych w trakcie nawiązywania relacji handlowych,
- przesyłanie informacji handlowych za pomocą SMS, MMS, e-mail,
- marketing na stronach WWW, konkursy, loterie promocyjne
- zgody na przetwarzanie danych osobowych – zasady

KOMPETENCJE I KONTROLA PREZESA UODO (4 godz.)

- zakres kompetencji organu ochrony danych osobowych
- ochrona tajemnicy przedsiębiorstwa w trakcie kontroli
- praktyczne wskazówki przygotowania do kontroli
- omówienie art. 57-58 RODO oraz przepisów Ustawy o ochronie danych osobowych z 2018 r.

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ (8 godz.)

- art. 13. Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą
- art. 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą
- art. 15 Prawo dostępu przysługujące osobie, której dane dotyczą

PRAWO DO OCHRONY DANYCH OSOBOWYCH A PRAWO DO INFORMACJI PUBLICZNEJ I PRAWO DO PONOWNEGO WYKORZYSTYWANIA INFORMACJI (8 godz.)

- analiza przykładów wniosków o udostępnienie informacji publicznej i zakresu ujawnianych danych osobowych
- omówienie art. 86 RODO

WSPÓŁPRACA INSPEKTORA OCHRONY DANYCH Z DZIAŁEM IT (8 godz.)

- Wybrane przykłady współpracy Inspektora ze służbą IT w kontekście przetwarzania danych osobowych i wsparcia w realizacji praw podmiotów danych oraz wdrażania środków technicznych i organizacyjnych ochrony danych osobowych
- omówienie art. 37-39 RODO

USŁUGI CYFROWE A OCHRONA DANYCH OSOBOWYCH (4 godz.)

- usługi świadczone drogą elektroniczną
- regulamin świadczenia usług
- podstawy prawne przetwarzania
- przesyłanie informacji handlowych drogą elektroniczną
- omówienie wybranych przepisów Ustawy o świadczeniu usług drogą elektroniczną oraz Aktu o usługach cyfrowych (DSA)

ZAGROŻENIA CYBERNETYCZNE ORAZ TECHNOLOGIE CHRONIĄCE PRYWATNOŚĆ SYSTEMÓW PRZETWARZAJĄCYCH DANE (8 godz.)

- wybrane zagrożenia i technologie chroniące prywatność polskojęzyczna
- przestępczość zorganizowana w darknecie
- karny aspekt przestępczości w internecie

NARUSZENIA DANYCH OSOBOWYCH (8 godz.)

- definicja, identyfikacja i dokumentowanie naruszeń

- różnice pomiędzy incydentami i naruszeniami ochrony danych osobowych
- ocena ryzyka z wiązka z naruszeniem ochrony danych osobowych
- omówienie art. 33-34

ŚRODKI TECHNICZNE I ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH – ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH (24 godz.)

- przekłady praktyków stosowania zasad, procedur ochrony danych osobowych
- przekłady środków technicznych ochrony danych osobowych
- zasady doboru środków technicznych i organizacyjnych do ryzyka naruszenia praw lub wolności podmiotów danych
- omówienie art. 25, 32, 35

KRYPTOGRAFIA W OCHRONIE DANYCH OSOBOWYCH (8 godz.)

- zasady działania i rodzaje funkcji haszujących oraz szyfrujących
- przykłady funkcji niebezpiecznych i bezpiecznych
- przykład zastosowania kryptografii w ochronie danych osobowych

RISK-BASED APPROACH (PODEJŚCIE OPARTE NA RYZYKU) OCENA RYZYKA I OCENA SKUTKÓW DLA OCHRONY – WARSZTAT (16 godz.)

- omówienie art. 25, 32, 35
- geneza podejścia opartego na ryzyku
- warsztat z identyfikowania operacji przetwarzania
- warsztat z opisu procesu przetwarzania (cel, kontekst, zakres itd.)
- warsztat z oceny ryzyka
- warsztat z oceny skutków dla ochrony

PSYCHOLOGICZNE ASPEKTY WYKONYWANIA ZADAŃ INSPEKTORA OCHRONY DANYCH – WARSZTATY (8 godz.)

- skuteczne przykazywanie wiedzy
- prowadzenie szkoleń/prezentacji
- umiejętność prowadzenia sprawdzeń – kontroli (unikanie konfliktów)
- asertywność w kontekście niezależności Inspektora

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 600,00 PLN
Koszt przypadający na 1 uczestnika netto	5 600,00 PLN

Koszt osobogodziny brutto

35,00 PLN

Koszt osobogodziny netto

35,00 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2

Maciej Kołodziej

Wykładowca, doradca, specjalista informatyki śledczej w e-Detektywi sp. z o.o.; Wiceprezes „SABI - Stowarzyszenie Inspektorów Ochrony Danych”; Informatyk; Audytor wiodący normy ISO/EIC 27001. Zajmuje się doradztwem przy wdrażaniu i ocenie funkcjonowania procesów dotyczących ochrony prywatności w usługach społeczeństwa informacyjnego oraz analizą jakości zabezpieczeń w systemach teleinformatycznych. Specjalizuje się w zarządzaniu incydem, zachowaniu ciągłości działania, przywracaniu procesów po awariach, odzyskiwaniu danych oraz post incydentalnych ekspertyzach i analizie śledczej. Wykładowca kilku polskich uczelni wyższych oraz projektów szkoleniowych dla instytucji rządowych, sektora publicznego, bankowości, telekomunikacji i branży e-commerce. Praktycznie szkoli i motywuje w zakresie ochrony informacji i zarządzania systemami IT.

Autor publikacji i opinii dotyczących systemów teleinformatycznych, cyberbezpieczeństwa oraz rozwiązań służących do przetwarzania i ochrony informacji, w tym danych osobowych.



2 z 2

Rafał Prabucki

Doktor nauk prawnych i inżynier. Auditor wiodący ISO/IEC 27001:2022 oraz posiadacz tytułu Certified in Cybersecurity (CC) wydanym przez (ISC)². Adiunkt na Uniwersytecie Śląskim. Członek CYBER SCIENCE. Założyciel LegalHackers Katowice. Asystent w zakończonych projektach dotyczących wykorzystania nowych technologii w przemyśle: MAS4AI na Uniwersytecie Śląskim i SHOP4CF na Uniwersytecie Opolskim. Alumn stypendiów w Polsce, Hiszpani i Niemczech.

Prowadzący wykłady na Uczelniach w Polsce, Litwie i we Włoszech. Kierownik studiów podyplomowych "Tokenizacja i automatyzacja procesów w gospodarce cyfrowej" na Uniwersytecie Śląskim.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podczas zjazdu każdy uczestnik programu otrzymuje komplet materiałów dydaktycznych w formie pdf bądź na platformie moodle. Materiały te przygotowują wykładowcy, dostosowując je do specyfiki prowadzonego tematu.

Uczestnicy studiów pracują na platformie Extranet, to wewnętrzna platforma komunikacyjna Uczelni WSB Merito, stworzona w celu ograniczenia formalności oraz ułatwienia przepływu informacji między uczestnikami a uczelnią. Za jej pomocą przez całą dobę i z każdego miejsca na świecie uczestnicy mają dostęp do:

- harmonogramu zajęć,
- informacji na temat płatności,
- materiałów dydaktycznych,
- katalogu bibliotecznego,

- informacji dotyczących zmian w planach zajęć, ogłoszeń i aktualności.

Warunki uczestnictwa

Zgodnie z regulaminem zapisów na studia podyplomowe na Uniwersytecie WSB Merito w Poznaniu należy zapisać się również poprzez formularz online znajdujący się na stronach Uniwersytetu WSB Merito w wybranych filiach w:

- Chorzowie,
- Poznaniu,
- Szczecinie,
- Warszawie

Kryteria uczestnictwa w Programie

- ukończone studia wyższe I lub II stopnia
- spełnienie warunków rekrutacyjnych

Warunki zaliczenia

- Test półroczny
- Egzamin końcowy pisemny, test z pytaniami do wyboru oraz pytaniami otwartymi

Interaktywna forma zajęć

Wykłady uzupełniane są ćwiczeniami, warsztatami oraz studiami przypadków.

Zjazdy odbywają się średnio raz lub dwa razy w miesiącu:

- w soboty od 9:00 do 16:00
- w niedziele od 9:00 do 16:00.

Informacje dodatkowe

- Uczestnicy naszych programów mogą brać udział w ciekawych szkoleniach, które prowadzą doświadczeni trenerzy. Udział w spotkaniach jest bezpłatny. Dzięki szkoleniom można uzupełnić wiedzę i potwierdzić ją certyfikatem.
- Szczegółowy harmonogram usługi może ulec zmianie w postaci realizowanych przedmiotów w danym dniu i osób prowadzących. Zmianie nie ulegają terminy zjazdów na studiach podyplomowych oraz ilość godzin usługi.
- Harmonogram zjazdów zostanie upubliczniony na stronach Uczelni lub w BUR na 2 tygodnie przed zajęciami
- Godziny zajęć podane w harmonogramie są godzinami zegarowymi, zaś ilość godzin programowych jest podana w godzinach dydaktycznych. 160 godzin dydaktycznych = 120 godzin zegarowych
- Cena usługi nie obejmuje opłaty wpisowej oraz końcowej.
- Cena usługi ulega zmianie, przy rozłożeniu płatności na 10,12 rat.

Warunki techniczne

Zajęcia odbywają się na platformie MS Teams, każdy z uczestników zobowiązany jest do posiadania własnego sprzętu z aktywnym mikrofonem oraz kamerą internetową oraz dostępu do Internetu.

Adres

ul. Powstańców Wielkopolskich 5
61-895 Poznań
woj. wielkopolskie

Zajęcia mogą być realizowane w różnych lokalizacjach:

1. Uniwersytet WSB Merito w Poznaniu ul. Powstańców Wielkopolskich 2A

2. Uniwersytet WSB Merito w Poznaniu ul. Powstańców Wielkopolskich 1A

3. VIII LO – ul. ul. Cegielskiego 1

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Udogodnienia dla osób ze szczególnymi potrzebami

Kontakt



Monika Plewa

E-mail rekrutacja-sp@poznan.merito.pl

Telefon (+48) 616 553 300