

Akademia WSB
WSB University

Akademia WSB

★★★★☆ 4,4 / 5

1 189 ocen

Ochrona danych osobowych w administracji i biznesie - Inspektor ochrony danych - studia podyplomowe - online

Numer usługi 2026/02/27/8729/3366870

📍 zdalna w czasie rzeczywistym

📅 Studia podyplomowe

🕒 155 h

📅 11.04.2026 do 28.02.2027

6 600,00 PLN brutto

6 600,00 PLN netto

42,58 PLN brutto/h

42,58 PLN netto/h

Informacje podstawowe

Kategoria

Prawo i administracja / Ochrona informacji niejawnych

Grupa docelowa usługi

Studia skierowane są głównie do osób zajmujących się szeroko rozumianą problematyką ochrony informacji, w tym biznesowych i danych osobowych we wszystkich sektorach gospodarki (pracownicy przedsiębiorstw i firm, administracji państwowej i samorządowej), **czyli do osób, które kierują lub przygotowują się do pracy w pionach ochrony danych osobowych lub odpowiadają za politykę bezpieczeństwa w swoich jednostkach organizacyjnych.** To studia odpowiednie dla pracodawców i pracowników, którzy na co dzień mają do czynienia z przetwarzaniem danych osobowych.

Minimalna liczba uczestników

10

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji

31-03-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

155

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 2024 r. poz. 1571, z późn. zm.)

Zakres uprawnień

studia podyplomowe

Cel

Cel edukacyjny

Celem studiów jest zwiększenie atrakcyjności zawodowej pracowników administracji publicznej i innych podmiotów organizacyjnych, mających w swej działalności do czynienia z danymi osobowymi oraz podniesienie kompetencji specjalistów zajmujących się tworzeniem systemu skutecznej ochrony strategicznych informacji przedsiębiorstw lub instytucji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje zasady ochrony danych osobowych wynikające z RODO oraz krajowych przepisów uzupełniających. Omawia obowiązki administratora i podmiotu przetwarzającego dane w sektorze publicznym i prywatnym. Charakteryzuje systemy zarządzania bezpieczeństwem informacji, w tym wymagania normy ISO/IEC 27001. Omawia metody identyfikacji zagrożeń i analizy ryzyka w ochronie danych osobowych. Wyjaśnia zasady zarządzania ciągłością działania oraz reagowania na incydenty bezpieczeństwa. Zna zasady kontroli prowadzonych przez Urząd Ochrony Danych Osobowych. Omawia obowiązki administratora i podmiotu przetwarzającego dane w sektorze publicznym i prywatnym. Wyjaśnia zasady realizacji praw podmiotów danych oraz tworzenia klauzul informacyjnych i zgód. Opisuje procedury postępowania w przypadku naruszenia ochrony danych osobowych.	egzamin po każdym semestrze	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opracowuje klauzule informacyjne oraz zgody zgodne z przepisami o ochronie danych osobowych. Przygotowuje i aktualizuje dokumentację z zakresu ochrony danych osobowych. Identyfikuje zagrożenia i przeprowadza analizę oraz ocenę ryzyka zgodnie z wymogami RODO. Opracowuje procedury reagowania na naruszenia ochrony danych i zarządza incydentami bezpieczeństwa. Przygotowuje organizację do kontroli organu nadzorczego. Wdraża elementy systemu zarządzania bezpieczeństwem informacji zgodnie z ISO/IEC 27001. Prowadzi audyty wewnętrzne w obszarze ochrony danych i bezpieczeństwa informacji. Analizuje zdarzenia w systemach teleinformatycznych pod kątem bezpieczeństwa informacji.	egzamin po każdym semestrze	Test teoretyczny
Dostrzega znaczenie ochrony danych osobowych dla funkcjonowania organizacji i budowania zaufania społecznego. Odpowiedzialnie pełni funkcję inspektora ochrony danych lub osoby odpowiedzialnej za bezpieczeństwo informacji. Podejmuje decyzje z uwzględnieniem analizy ryzyka i konsekwencji prawnych. Współpracuje z kadrą zarządzającą, działem IT oraz organem nadzorczym. Reaguje adekwatnie w sytuacjach kryzysowych związanych z naruszeniem bezpieczeństwa informacji. Dąży do stałego doskonalenia kompetencji w zakresie nowych technologii i zagrożeń cybernetycznych.	egzamin po każdym semestrze	Test teoretyczny

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

Lp.	Nazwa przedmiotu	Liczba godzin zajęć teoretycznych	Liczba godzin zajęć praktycznych	Liczba punktów ECTS
1.	Wprowadzenie do RODO	-	4	1
2.	Zasady ochrony danych osobowych w działalności instytucji publicznych i sektora prywatnego	-	-7	1
3.	Praktyczne aspekty tworzenia klauzul zgód i klauzul informacyjnych w kontekście realizacji uprawnień podmiotów danych	-	4	1
4.	Postępowanie w przypadku naruszenia ochrony danych	1	2	1
5.	Zarządzanie incydentami bezpieczeństwa	1	1	1
6.	Praktyczne aspekty tworzenia dokumentacji z zakresu ochrony danych osobowych oraz realizacji zadań inspektora ochrony danych	6	6	2

7.	Systemy zarządzania jakością i bezpieczeństwem informacji	10	10	2	
8.	Bezpieczeństwo informacji biznesowych. Teoretyczne i praktyczne aspekty ustanawiania i wdrażania tajemnicy przedsiębiorstwa	4	4	2	
9.	Praktyka prowadzenie audytów	3	7	1	
10.	Akt w sprawie zarządzania danymi	2	-	1	
11.	Bezpieczeństwo informacji biznesowych. Teoretyczne i praktyczne aspekty ustanawiania i wdrażania tajemnicy przedsiębiorstwa	4	4	2	
12.	Nowoczesne techniki i technologie ochrony informacji	4	2	1	
13.	Kontrole UODO – zakres, treść, obowiązki kontrolowanych	7	-	1	
14.	Ochrona danych osobowych a informacja publiczna	4	2	1	
15.	Analiza ryzyka w bezpieczeństwie informacji	2	5	2	
16.	Budowanie nowych rozwiązań technologicznych w działaniach biznesowych a ochrona danych osobowych	2	-	1	
17.	Zarządzanie ciągłością działania w tym administracji publicznej	3	2	1	
18.	Praktyczne problemy i możliwości zabezpieczania, audytowania oraz analizy zdarzeń w systemach teleinformatycznych	5	5	2	
19.	Sytuacje kryzysowe w aspekcie systemu ochrony danych osobowych	4	4	2	
20.	Zagrożenia cybernetyczne	8	-	2	
21.	Kodeksy postępowania jako narzędzie realizacji obowiązków wynikających z RODO	4	-	1	

22.	Identyfikacja zagrożeń i ocena ryzyka w ochronie danych osobowych zgodnie z RODO	4	4	2	
23.	Prawnocywilne aspekty ochrony danych osobowych w teorii i praktyce	4	-	1	
	Razem	83	72	32	

Studia trwają dwa semestry.

Proces uczenia się jest rozdzielny od procesu walidacji usługi.

Walidacja zostaje przeprowadzona za pośrednictwem testu z wiedzy na platformie internetowej.

Linki do poszczególnych zajęć zostaną zamieszczane w zakładce "Kody dostępowe do usługi" z kilkudniowym wyprzedzeniem przed każdymi realizowanymi zajęciami.

Zajęcia realizowane weekendowo w wybrane soboty i niedziele. Przerwy nie wliczają się w czas usługi.

Harmonogram

Liczba przedmiotów/zajęć: 0

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

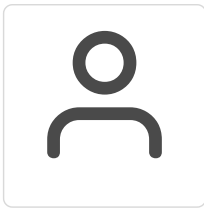
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 600,00 PLN
Koszt przypadający na 1 uczestnika netto	6 600,00 PLN
Koszt osobogodziny brutto	42,58 PLN
Koszt osobogodziny netto	42,58 PLN

Prowadzący

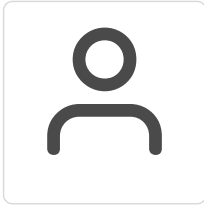
Liczba prowadzących: 9



1 z 9

mgr Monika Krasieńska

Dyrektor Departamentu Orzecznictwa i Legislacji w Urzędzie Ochrony Danych Osobowych. Wieloletni wykładowca z zakresu ochrony danych osobowych, dostępu do informacji publicznej i informacji prawnie chronionych. Autorka licznych publikacji i komentarzy w zakresie kształtowania ochrony prywatności i danych osobowych w sektorze publicznym i prywatnym. Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, związane z praktycznym stosowaniem przepisów o ochronie danych osobowych, udziałem w postępowaniach administracyjnych oraz procesie legislacyjnym w obszarze ochrony danych i prawa do informacji.



2 z 9

dr inż. Krystian Mączka

dr inż. Krystian Mączka – wykładowca Akademia WSB (Katedra Bezpieczeństwa), specjalista w zakresie cyberprzestępczości komputerowej, bezpieczeństwa sieci, odzyskiwania danych, analizy nośników cyfrowych, szyfrowania oraz monitoringu systemów teleinformatycznych.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, obejmujące praktyczne działania w obszarze cyberbezpieczeństwa, analizę incydentów bezpieczeństwa, zabezpieczanie i badanie materiału cyfrowego oraz wdrażanie rozwiązań z zakresu ochrony informacji w organizacjach.



3 z 9

mgr Przemysław Szczurek

Absolwent Uniwersytet Ekonomiczny w Krakowie. Z branżą IT związany od ponad 15 lat. Obecnie pełni funkcję Senior Managera ds. Bezpieczeństwa Informacji w TÜV NORD Polska, gdzie odpowiada za rozwój usług związanych z normami ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301 oraz tematyką ochrony danych osobowych, cyberbezpieczeństwa i TISAX.

Posiada certyfikaty: Audytora Wiodącego ISO 27001, ISO 20000, Audytora Wewnętrznego ISO 22301, Incident Response Managera oraz Inspektora Ochrony Danych. Jest egzaminatorem dla Audytorów Wiodących SZBI akredytowanym przez Polskie Centrum Akredytacji. Jako trener TÜV NORD oraz wykładowca akademicki kładzie duży nacisk na budowanie świadomości bezpieczeństwa wśród kadry zarządzającej i pracowników.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, obejmujące realizację projektów wdrożeniowych i audytowych w obszarze systemów zarządzania bezpieczeństwem informacji, ciągłości działania, ochrony danych osobowych oraz reagowania na incydenty bezpieczeństwa w organizacjach różnych sektorów.



4 z 9

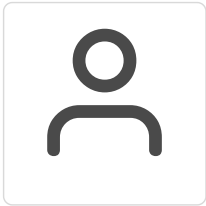
mec. Paula Majcher-Guzik

mec. Paula Majcher-Guzik – radca prawny specjalizująca się w prawie ochrony danych osobowych, prawie nowych technologii oraz zagadnieniach związanych z dostępem do informacji publicznej i informacją prawnie chronioną. Wspiera podmioty sektora publicznego i prywatnego w zakresie wdrażania i stosowania przepisów o ochronie danych osobowych, prowadzi szkolenia oraz doradza w procesach dostosowawczych i audytowych.

Autorka i współautorka opracowań z zakresu ochrony prywatności i odpowiedzialności prawnej związanej z przetwarzaniem danych.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat,

obejmujące bieżące doradztwo prawne, udział w postępowaniach administracyjnych oraz wsparcie organizacji w zakresie minimalizowania ryzyk prawnych związanych z przetwarzaniem danych osobowych.



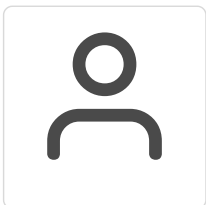
5 z 9

mgr Jarosław Żabówka

Ekspert w zakresie ochrony danych osobowych, bezpieczeństwa informacji oraz systemów zarządzania zgodnością. Specjalizuje się w praktycznych aspektach wdrażania przepisów o ochronie danych osobowych w sektorze publicznym i prywatnym, prowadzeniu audytów oraz budowaniu i doskonaleniu systemów zarządzania bezpieczeństwem informacji.

Posiada doświadczenie w opracowywaniu dokumentacji z zakresu ochrony danych, analizie ryzyka, zarządzaniu incydentami bezpieczeństwa oraz przygotowywaniu organizacji do kontroli organu nadzorczego.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, obejmujące realizację projektów wdrożeniowych, audytowych i doradczych w obszarze ochrony danych osobowych oraz cyberbezpieczeństwa.



6 z 9

dr Marcin Szymczak

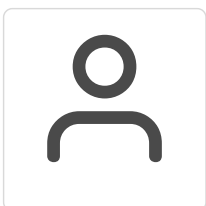
Doktor nauk prawnych, specjalista w dziedzinie kryminalistyki i informatyki śledczej. Sędzia Wydziału Karnego Sądu Rejonowego Katowice-Wschód. Współzałożyciel Instytutu Informatyki Śledczej, gdzie aktywnie uczestniczy w projektach i analizach z zakresu ochrony danych cyfrowych oraz cyberbezpieczeństwa.

Od wielu lat prowadzi działalność dydaktyczną, obecnie jako wykładowca Akademii WSB w Dąbrowie Górniczej, gdzie realizuje zajęcia na kierunkach związanych z bezpieczeństwem, prawem i informatyką śledczą. W ostatnich latach koncentruje się na zagadnieniach ochrony danych cyfrowych, przestępczości komputerowej i praktycznym zastosowaniu informatyki śledczej w postępowaniu karnym.

Spełnienie wymogów potencjału kadrowego:

- Doświadczenie zawodowe (ostatnie 5 lat): praca orzecznicza w wydziale karnym sądu, udział w sprawach dotyczących cyberprzestępczości i ochrony danych cyfrowych, aktywna działalność ekspercka w Instytucie Informatyki Śledczej.
- Kwalifikacje: doktor nauk prawnych w specjalności kryminalistyka – informatyka śledcza, stale rozwijane poprzez działalność dydaktyczną i praktykę zawodową w obszarze prawa karnego i cyberbezpieczeństwa.

Dzięki łączeniu praktyki orzeczniczej, wiedzy akademickiej i pracy eksperckiej w obszarze informatyki śledczej, dr Marcin Szymczak posiada odpowiednie kwalifikacje i aktualne doświadczenie niezbędne do prowadzenia usług w zakresie prawa, ochrony danych cyfrowych oraz cyberbezpieczeństwa.



7 z 9

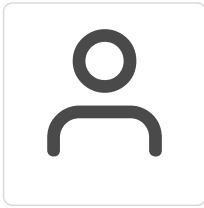
dr Jarosław Wojcieszek

dr Jarosław Wojcieszek – doktor nauk prawnych, specjalista w zakresie ochrony danych osobowych, prawa nowych technologii oraz bezpieczeństwa informacji. Wykładowca akademicki i praktyk, zajmujący się problematyką zgodności procesów przetwarzania danych z obowiązującymi przepisami prawa, analizą ryzyka oraz odpowiedzialnością prawną administratorów danych.

Autor i współautor publikacji dotyczących ochrony prywatności, jawności życia publicznego oraz prawnych aspektów funkcjonowania systemów informatycznych. Prowadzi szkolenia i warsztaty dla sektora publicznego i prywatnego w zakresie stosowania przepisów o ochronie danych osobowych

oraz zarządzania bezpieczeństwem informacji.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, obejmujące doradztwo prawne, udział w audytach oraz wsparcie organizacji w dostosowywaniu procesów przetwarzania danych do wymogów prawa i standardów bezpieczeństwa.



8 z 9

mgr Edyta Bartoszek

mgr Edyta Bartoszek – specjalistka w zakresie ochrony danych osobowych oraz bezpieczeństwa informacji, praktyk w obszarze wdrażania procedur zgodności i budowania systemów ochrony danych w organizacjach sektora publicznego i prywatnego.

Posiada doświadczenie w opracowywaniu i aktualizacji dokumentacji z zakresu ochrony danych osobowych, realizacji obowiązków informacyjnych, prowadzeniu analiz ryzyka oraz wspieraniu administratorów w realizacji praw osób, których dane dotyczą. Prowadzi szkolenia i warsztaty z zakresu stosowania przepisów o ochronie danych oraz zarządzania incydentami bezpieczeństwa.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, obejmujące praktyczne wdrażanie rozwiązań organizacyjnych i technicznych w obszarze ochrony danych osobowych oraz bieżące wsparcie podmiotów w zapewnianiu zgodności z przepisami.



9 z 9

dr Witold Pokora

dr witold pokora

dr Witold Pokora – doktor nauk prawnych, specjalista w zakresie ochrony danych osobowych, prawa administracyjnego oraz bezpieczeństwa informacji. Wykładowca akademicki i praktyk zajmujący się problematyką zgodności procesów przetwarzania danych z przepisami prawa, odpowiedzialnością administratorów oraz funkcjonowaniem systemów ochrony danych w organizacjach sektora publicznego i prywatnego.

Autor i współautor publikacji z zakresu ochrony prywatności, dostępu do informacji publicznej oraz prawnych aspektów przetwarzania danych osobowych. Prowadzi szkolenia i warsztaty dotyczące wdrażania procedur zgodności, analizy ryzyka oraz reagowania na naruszenia ochrony danych.

Wykładowca posiada również aktualne doświadczenie zawodowe zdobyte w ciągu ostatnich 5 lat, obejmujące doradztwo prawne, udział w audytach oraz wsparcie instytucji i przedsiębiorstw w dostosowywaniu działalności do wymogów przepisów o ochronie danych osobowych i standardów bezpieczeństwa informacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacje i materiały pdf udostępniane w trakcie lub po zajęciach

Warunki uczestnictwa

Warunkiem uczestnictwa w usłudze jest dokonanie wpłaty opłaty wpisowej w kwocie 300 zł, która jest dodatkową opłatą poza kosztem wskazanym w usłudze.

Ukończone studia I lub II stopnia.

Uczestnik zobowiązany jest do przystąpienia do egzaminów semestralnych i uzyskania oceny pozytywnej.

Informacje dodatkowe

1 godzina zajęć w Akademii WSB = 45 min. zajęć dydaktycznych

Zajęcia realizowane weekendowo w wybrane soboty i niedziele. Przerwy nie wliczają się w czas usługi.

155 godzin zajęć

Warunkiem uczestnictwa w usłudze jest dokonanie wpłaty opłaty wpisowej w kwocie 300 zł, która jest dodatkową opłatą poza kosztem wskazanym w usłudze.

UWAGA! Harmonogram może ulec zmianie.

Warunki techniczne

Warunki techniczne

Usługa realizowana zdalnie poprzez platformy ClickMeeting oraz Zoom

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: •Komputer stacjonarny/laptop z dostępem do Internetu

•Sprawny mikrofon i kamera internetowa (lub zintegrowane z laptopem)

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: download 8 mb/s, upload 8 mb/s, ping 15 ms

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Zalecamy wykorzystanie aktualnej wersji przeglądarki CHROME (zarówno na komputerach z systemem operacyjnym Windows jak i Apple

Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line: 7,5 h

Kontakt



Agnieszka Głąb

E-mail agnieszka.glab@wsb.edu.pl

Telefon (+48) 322 959 395