



Ochrona danych osobowych i zabezpieczenie systemów informatycznych w placówkach służby zdrowia

Numer usługi 2025/05/05/52682/2724867

1 200,00 PLN brutto
1 200,00 PLN netto
150,00 PLN brutto/h
150,00 PLN netto/h

Warszawska
Akademia
Medyczna Nauk
Stosowanych

★★★★★ 4,8 / 5

52 oceny

📍 zdalna w czasie rzeczywistym

👤 Usługa szkoleniowa

🕒 8 h

📅 11.10.2025 do 11.10.2025

Informacje podstawowe

Kategoria

Prawo i administracja / Administracja publiczna

Grupa docelowa usługi

Szkolenie skierowane jest do:

- pracowników służby zdrowia (w tym kadry zarządzającej),
- prawników i osób zainteresowanych problematyką ochrony danych osobowych,
- pracowników urzędów i instytucji publicznych współpracujących ze służbą zdrowia.

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji

10-10-2025

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

8

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

kursy i szkolenia

Cel

Cel edukacyjny

- minimalizacja ryzyka incydentów związanych z nieuprawnionym ujawnieniem danych osobowych
- zapoznanie uczestników z metodami zarządzania bazami danych
- omówienie sposobów zabezpieczania systemów informatycznych przed atakami hakerskimi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1.Zna podstawowe pojęcia i przepisy wynikające z RODO oraz krajowych regulacji dotyczących ochrony danych osobowych. 2.Rozumie specyfikę przetwarzania danych osobowych w placówkach medycznych, w tym danych szczególnych kategorii. 3.Zna metody zabezpieczania danych osobowych w formie papierowej i elektronicznej. 4.Posiada wiedzę na temat zagrożeń związanych z cyberatakami (np. ransomware, phishing) oraz sposobów zabezpieczania systemów informatycznych	1. Wymienia podstawowe zasady przetwarzania danych osobowych oraz zna prawa osób, których dane dotyczą. 2.Potrafi wskazać różnice w przetwarzaniu danych osobowych w placówce medycznej w porównaniu z innymi sektorami. 3. Rozpoznaje typowe zagrożenia dla danych w systemach informatycznych (np. rodzaje ataków). 4.Wymienia kroki postępowania w razie ujawnienia danych osobowych.	Test teoretyczny
5.Stosuje w praktyce przepisy RODO w codziennej pracy w placówce medycznej. 6.Identyfikuje sytuacje zagrożenia dla danych osobowych i podejmuje odpowiednie środki zapobiegawcze. 7.Dobiera właściwe metody ochrony danych osobowych w zależności od ich rodzaju i sposobu przetwarzania. 8. Rozpoznaje symptomy potencjalnych cyberataków i reaguje zgodnie z obowiązującymi procedurami. 9. Postępuje właściwie w przypadku incydentu naruszenia danych osobowych i dokumentuje działania.	5. Potrafi zastosować zasady minimalizacji danych i prawidłowego nadawania uprawnień. 6.Prawidłowo identyfikuje błędy lub luki w fikcyjnym scenariuszu przetwarzania danych w placówce medycznej. 7.Ocena sytuację zagrożenia (np. próbę phishingu) i wskazuje odpowiednie działania zapobiegawcze. 8.Potrafi wskazać sposób zabezpieczenia danych w wersji papierowej i elektronicznej. 9.Zna poprawną procedurę zgłoszenia incydentu do UODO oraz umie przeprowadzić wewnętrzne postępowanie.	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

Program szkolenia obejmuje m.in.:

- przepisy RODO i regulacje krajowe dotyczące ochrony danych osobowych,
- specyfikę gromadzenia, przetwarzania i przechowywania danych osobowych w placówkach medycznych,
- metody zabezpieczania danych osobowych,
- zabezpieczenie systemów informatycznych – przeciwdziałanie atakom hakerskim (w tym przykłady ataków ransomware, phishing, oszustwa internetowe),
- procedury postępowania w przypadku incydentu ujawnienia danych lub przestępstwa na szkodę placówki służby zdrowia.

Harmonogram

Liczba przedmiotów/zajęć: 8

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Otwarcie szkolenia i wprowadzenie	Piotr Kusznierek	11-10-2025	09:00	09:15	00:15
2 z 8 Przepisy RODO i regulacje krajowe	-	11-10-2025	09:20	10:20	01:00
3 z 8 Specyfika przetwarzania danych w placówkach medycznych	-	11-10-2025	10:30	12:30	02:00
4 z 8 Metody zabezpieczania danych osobowych	-	11-10-2025	12:30	14:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 8 Zabezpieczenie systemów informatycznych	-	11-10-2025	14:00	14:30	00:30
6 z 8 Procedury reagowania na incydenty i naruszenia	-	11-10-2025	14:30	15:30	01:00
7 z 8 Współpraca z organami ścigania	-	11-10-2025	15:30	16:00	00:30
8 z 8 Podsumowanie - rozwiązywanie problemów praktycznych – mini-cases- test wiedzy (walidacja)	-	11-10-2025	16:00	17:15	01:15

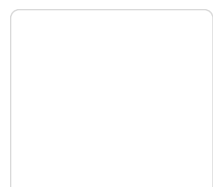
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 200,00 PLN
Koszt przypadający na 1 uczestnika netto	1 200,00 PLN
Koszt osobogodziny brutto	150,00 PLN
Koszt osobogodziny netto	150,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Piotr Kuszczneruk

Rektor WAM, doktor nauk prawnych

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- dostęp do materiałów szkoleniowych w formie elektronicznej

Warunki techniczne

Uczestnicy kursu będą łączyć się z prowadzącym na platformie MS Teams.

Kontakt



Katarzyna Brzychcy

E-mail kbrzychcy@wam.edu.pl

Telefon (+48) 602 422 922