Możliwość dofinansowania

Cyberbezpieczeństwo z RODO – praktyczne podejście

Numer usługi 2026/02/19/124519/3347272

1 700,00 PLN brutto
1 700,00 PLN netto
141,67 PLN brutto/h
141,67 PLN netto/h
261,33 PLN cena rynkowa

OŚRODEK SZKOLENIOWO USŁUGOWY OPERATOR TOMASZ PIETRAS

4,9 / 5

546 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
12:00 h
25.06.2026 do 26.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe, Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	Grupą docelową są osoby pełnoletnie, które posiadają wykształcenie minimum średnie lub zawodowe, chcące zdobyć wiedzę i praktyczne umiejętności z zakresu cyberbezpieczeństwa i RODO w pracy biurowej. Usługa skierowana w sposób szczególny dla uczestników projektu „Regionalny Fundusz Szkoleniowy II".
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	24-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Celem szkolenia jest omówienie najlepszych praktyk dotyczących bezpiecznego korzystania z urządzeń mobilnych, przeglądarek internetowych, kont internetowych i płatności online; kontekstualizacja nabytej wiedzy na przykładzie realnych historii; analiza zabezpieczeń, które zawiodły oraz zapoznanie z zasadami RODO i ochrony danych osobowych podczas pracy biurowej w ujęciu praktycznym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje kluczowe pojęcia z zakresu cyberbezpieczeństwa	Charakteryzuje zagadnienia: cyberbezpieczeństwa, danych wrażliwych oraz incydentu bezpieczeństwa	Test teoretyczny
Definiuje typowe zagrożenia dla danych osobowych	Charakteryzuje zagadnienia typowych zagrożeń dla danych osobowych oraz Phishing, ransomware, malware	Test teoretyczny
Definiuje zagadnienie wycieku danych	Charakteryzuje konsekwencje prawne oraz finansowe dotyczące wycieku danych wraz z przykładami	Test teoretyczny
Stosuje dobre praktyki w zakresie ochrony danych w środowisku cyfrowym	Wykorzystuje najlepsze praktyki podczas bezpiecznego korzystania z urządzeń mobilnych, przeglądarek internetowych, kont internetowych i płatności online	Wywiad swobodny
Uczestnik definiuje i charakteryzuje ochranę danych osobowych	Uczestnik rozróżnia podstawowe terminy związane z ochroną danych osobowych	Test teoretyczny
	Uczestnik definiuje oraz przestrzega ochrony danych osobowych zgodnie z obowiązującymi zasadami	Test teoretyczny Wywiad swobodny
Uczestnik zarządza danymi osobowymi pracowników, klientów i kontrahentów, zgodnie z obowiązującymi przepisami, ze szczególnym uwzględnieniem przepisów RODO	Uczestnik rozróżnia, przestrzega i aktualizuje zasady regulujące ochronę danych osobowych, również w kontekście RODO	Test teoretyczny Wywiad swobodny
	Uczestnik pracuje na zbiorach danych – samodzielnie dokonuje ich klasyfikacji, sposobu ich zabezpieczenia i rejestracji zbiorów	Obserwacja w warunkach rzeczywistych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik nadzoruje ochronę danych osobowych w przedsiębiorstwie oraz reaguje w przypadku naruszeń	Uczestnik definiuje i rozróżnia naruszenia związane z ochroną danych osobowych oraz postępuje zgodnie z przyjętymi instrukcjami i zasadami, w tym zgłoszenia i powiadomienia odpowiednich osób i instytucji	Test teoretyczny
	Uczestnik definiuje i rozróżnia elementy audytu wewnętrznego względem przestrzegania danych osobowych	Test teoretyczny

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

Moduł	Temat szkolenia	Liczba godzin		
		Teoria	Praktyka	Razem

1.	**Wprowadzenie do cyberbezpieczeństwa** **1. Kluczowe pojęcia: cyberbezpieczeństwo, dane wrażliwe, incydent bezpieczeństwa.** **2. Typowe zagrożenia dla danych osobowych:** **o Phishing, ransomware, malware.** **o Wycieki danych i ich konsekwencje prawne oraz finansowe.** **3. Wprowadzenie do dobrych praktyk w zakresie ochrony danych w środowisku cyfrowym**	1	1	2
2.	**RODO w praktyce** **1. Podstawy prawne ochrony danych osobowych:** **o Obowiązki administratora danych i procesora.** **o Prawa osób, których dane są przetwarzane.** **2. Praktyczne aspekty wdrażania RODO:** **o Analiza ryzyka w organizacji.** **o Przetwarzanie danych zgodnie z zasadą minimalizacji i ograniczenia celu.** **3. Obowiązki w przypadku naruszenia ochrony danych:** **o Zgłaszanie incydentów do UODO.** **o Powiadamianie osób, których dane zostały naruszone.**	1	1	2
3.	**Zabezpieczenia techniczne i organizacyjne** **1. Tworzenie polityki bezpieczeństwa danych w organizacji.** **2. Narzędzia i technologie zabezpieczające dane:** **o Szyfrowanie danych.** **o Systemy zapobiegania wyciekom (DLP).** **o Dwuskładnikowe uwierzytelnianie (2FA).** **3. Zarządzanie dostępem do danych w firmie.** **4. Regularne aktualizacje i szkolenia personelu jako podstawa ochrony.**	2	1	3
4.	**Rozpoznawanie i reagowanie na incydenty** **1. Jak zidentyfikować zagrożenie?** **o Nietypowe wiadomości e-mail, anomalie w systemach IT.** **2. Procedura reagowania na incydent:** **o Izolowanie zagrożenia.** **o Dokumentowanie i raportowanie.** **3. Studia przypadków: przykłady incydentów w organizacjach i analiza błędów.**	1	1	2

5.	**Warsztaty praktyczne** **1. Symulacja ataku phishingowego – nauka rozpoznawania.** **2. Tworzenie polityki bezpieczeństwa dla organizacji – ćwiczenie grupowe.** **3. Scenariusze reagowania na incydenty:** **o Co zrobić w przypadku wycieku danych?** **o Jak zminimalizować ryzyko ponownego wystąpienia?** Walidacja na zakończenie szkolenia	-	3	3
RAZEM:		**5**	**7**	**12**

Po ukończonym szkoleniu uczestnik otrzymuje zaświaczenie o ukończeeniu kursu wydawane przez ośrodek szkoleniowy zgodnie z rozporządzeniem MEN.

Szkolenie jest adresowane do osób pełnoletnich, które posiadają wykształcenie minimum średnie lub zawodowe, chcących zdobyć wiedzę i praktyczne umiejętności z zakresu cyberbezpieczeństwa i RODO w pracy biurowej.

Szkolenie jest adresowane do pracodawców i ich pracowników - uczestników projektu ,,Regionalny Fundusz Szkleniowy II"

Liczba osób w grupie szkoleniowej:

1. **zajęcia teoretyczne i praktyczne: do 30**

Szkolenie przy wykorzystaniu mikrofonu i/lub kamerki oraz materiałów w formie zdalnej.

Uwagi dotyczące godzin usługi i przerw: Każda godzina usługi to godzina dydaktyczna. Za godzinę dydaktyczną uznaje się 45 minut. Oznacza to, że usługa składa się z 12 godzin dydaktycznych obejmujacych kurs i walidację. Podczas przeprowadzania usługi pomiędzy godzinami dydaktycznymi występują 5-minutowe przerwy, a więc po każdej zrealizowanej 45-minutowej godzinie dydaktycznej zajęć jest 5 minut przerwy. W przypadku kiedy zajęcia w danym dniu trwają 5 godzin dydaktycznych i więcej, wówczas po czwartej godzinie dydaktycznej zajęć jest 15-minutowa długa przerwa, jednak w zależności od preferencji uczestników.

Przerwy nie są wliczane w czas usługi rozwojowej.

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	1 700,00 PLN
Koszt przypadający na 1 uczestnika netto	1 700,00 PLN
Koszt osobogodziny brutto	141,67 PLN
Koszt osobogodziny netto	141,67 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Adamski

Pan Paweł Adamski jest profesjonalistą w branży z ponad 20-letnim doświadczeniem w edukacji, zarządzaniu oraz mediach. Specjalizuje się w wielu branżach, w tym w dziedzinie cyberbezpieczeństwa, zarządzania zespołem sprzedaży oraz rozwoju pracowników. Posiada wieloletnie doświadczenie, jest trenerem biznesowym. Posiada doświadczenie w branży mediów radiowych. Jest właścicielem dwóch firm szkoleniowych. W ostatnich latach aktywnie prowadził szkolenia online z zarządzania projektami oraz cyberbezpieczeństwa. Posiada doświadczenie zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia usługi do BUR.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypt, notes, długopis, teczka

Warunki uczestnictwa

- ukończone 18 lat,

- wykształcenie min. średnie lub zawodowe.

Informacje dodatkowe

Usługa jest zwolniona z VAT.

Usługa z dofinansowaniem.

Podczas przeprowadzania usługi pomiędzy godzinami dydaktycznymi występują 5-minutowe przerwy, a więc po każdej zrealizowanej 45-minutowej godzinie dydaktycznej zajęć jest 5 minut przerwy. W przypadku kiedy zajęcia w danym dniu trwają 5 godzin dydaktycznych i więcej, wówczas po czwartej godzinie dydaktycznej zajęć jest 15-minutowa długa przerwa, jednak w zależności od preferencji uczestników.

Po ukończonym szkoleniu uczestnik otrzymuje zaświaczenie o ukończeeniu kursu wydawane przez ośrodek szkoleniowy zgodnie z rozporządzeniem MEN.

Usługa skierowana w sposób szczególny dla uczestników projektu RFS II.

Warunki techniczne

Zajęcia organizowane na platformie ZOOM, Google Meets,, MS Teams lub innej obsługiwanej przez Ośrodek.

Kontakt

Tomasz Pietras

E-mail szkolenia@osz-operator.pl

Telefon (+48) 660 768 969