



RODO i cyberbezpieczeństwo w kontekście realizacji i rozliczenia projektów unijnych.

Numer usługi 2024/11/14/169989/2411245

6 100,00 PLN brutto

6 100,00 PLN netto

290,48 PLN brutto/h

290,48 PLN netto/h

WELLNESS
PROGRESSIVE
GROUP POLSKA
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ

Brak ocen dla tego dostawcy

- 📍 Piła / stacjonarna
- 👤 Usługa szkoleniowa
- 🕒 21 h
- 📅 21.12.2024 do 22.12.2024

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Kurs skierowany jest do: Pracowników administracji publicznej Przedsiębiorców i firm realizujących projekty Zespołów projektowych i menedżerów projektów Uczestnicy powinni mieć ogólne zrozumienie przepisów RODO, w szczególności podstawowych zasad ochrony danych osobowych, takich jak poufność, integralność, dostępność oraz zasady przetwarzania danych. Uczestnicy powinni umieć czytać i rozumieć dokumentację oraz procedury związane z bezpieczeństwem danych i zarządzaniem projektami, ponieważ kurs obejmuje analizę dokumentów i procedur związanych z zgodnością z RODO. Mile widziana jest podstawowa wiedza na temat cyberzagrożeń, takich jak phishing, malware, ransomware, aby uczestnicy mogli łatwiej przyswajać wiedzę i techniki ochrony przed zagrożeniami.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	20-12-2024
Forma prowadzenia usługi	stacjonarna

Cel

Cel edukacyjny

Celem kursu jest przygotowanie uczestników do samodzielnego zarządzania ochroną danych osobowych i cyberbezpieczeństwem w projektach. Uczestnicy nauczą się stosować przepisy RODO, identyfikować zagrożenia, zarządzać ryzykiem, przygotowywać dokumentację zgodną z RODO, monitorować środki bezpieczeństwa i reagować na incydenty. Kurs pomoże podnieść poziom bezpieczeństwa informacyjnego w organizacji, zapewniając zgodność z przepisami i najlepszymi praktykami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W zakresie wiedzy	Uczestnicy kursu poznają kluczowe przepisy RODO i ich zastosowanie w projektach, w tym zasady przetwarzania i przechowywania danych oraz obowiązki administratora i podmiotu przetwarzającego. Nauczą się identyfikować zagrożenia, zarządzać ryzykiem cyberbezpieczeństwa, oceniać ryzyko dla danych osobowych oraz dobierać odpowiednie środki ochrony. Zdobędą wiedzę o procedurach reagowania na incydenty i zasadach zgłaszania naruszeń.	Test teoretyczny
W zakresie umiejętności	Uczestnicy kursu nauczą się identyfikować zagrożenia dla danych osobowych, oceniać ryzyko w projektach oraz wdrażać odpowiednie środki zabezpieczające, dostosowane do wymagań projektu. Będą potrafili opracować i wdrażać polityki oraz procedury zgodne z RODO, monitorować ich realizację i aktualizować je w razie potrzeby. Zdobędą umiejętność skutecznego reagowania na incydenty bezpieczeństwa, w tym wykrywania, dokumentowania i raportowania naruszeń.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W zakresie kompetencji społecznych	Uczestnicy kursu będą świadomi roli ochrony danych osobowych w projektach i jej wpływu na bezpieczeństwo organizacji, co zwiększy ich odpowiedzialność zawodową. Rozwiną umiejętności współpracy z innymi działami, promując etyczne postawy i odpowiedzialność w zakresie ochrony danych. Będą przygotowani do komunikowania zasad RODO oraz budowania świadomości bezpieczeństwa w zespołach projektowych.	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.

Zaświadczenie zawiera opis efektów uczenia się.

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

Tak.

Dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak.

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Czas: 1 dzień, 21 godzin dydaktycznych

1 godzina szkolenia = 45 minut. Przerwy nie są wliczone w czas trwania usługi.

Kurs trwa 21 godz. dydaktycznych tj. 16 godz. zegarowych. W harmonogramie kursu zostały ujęte przerwy, łącznie 1 h. Krótkie przerwy są dostosowane do tempa pracy uczestników podczas kursu.

Warunki niezbędne do spełnienia, aby realizacja usługi pozwoliła na osiągnięcie celu: Celem kursu jest przygotowanie uczestników do samodzielnego zarządzania ochroną danych osobowych i cyberbezpieczeństwem w projektach. Uczestnicy nauczą się stosować przepisy RODO, identyfikować zagrożenia, zarządzać ryzykiem, przygotowywać dokumentację zgodną z RODO, monitorować środki bezpieczeństwa i reagować na incydenty. Kurs pomoże podnieść poziom bezpieczeństwa informacyjnego w organizacji, zapewniając zgodność z przepisami i najlepszymi praktykami.

Forma szkolenia: Trening stacjonarny połączony z wykładem, dyskusją i ćwiczeniami.

PROGRAM KURSU:

DZIEŃ I:

-Wprowadzenie do cyberbezpieczeństwa- Podstawowe pojęcia i definicje (zagrożenia, podatności, ryzyko, incydenty)

Rodzaje zagrożeń cybernetycznych (malware, phishing, ataki DDoS, socjotechnika)

Aktualne trendy w cyberprzestępczości Krajowe Ramy Interoperacyjności (KRI) - podstawy prawne i zakres (45 min)

Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne

Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności

Minimalne wymagania dla rejestrów publicznych i wymiany informacji

Minimalne wymagania dla systemów teleinformatycznych

Cyberbezpieczeństwo w KRI (45 min)

Zarządzanie bezpieczeństwem informacji w kontekście KRI

Wymagania KRI dotyczące bezpieczeństwa systemów teleinformatycznych

Polityka bezpieczeństwa informacji a KRI

Audyt bezpieczeństwa a KRI

-Zarządzanie ryzykiem w cyberbezpieczeństwie- Identyfikacja i analiza ryzyka

Metody oceny ryzyka

Wybór i wdrożenie zabezpieczeń

Monitorowanie i przegląd ryzyka

Praktyczne aspekty cyberbezpieczeństwa Bezpieczne hasła i uwierzytelnianie

Ochrona przed phishingiem i socjotechniką

Bezpieczne korzystanie z poczty elektronicznej i internetu

Ochrona danych osobowych (RODO) w kontekście cyberbezpieczeństwa

-Bezpieczeństwo systemów i aplikacji- Zabezpieczanie systemów operacyjnych

Bezpieczeństwo aplikacji i baz danych

Aktualizacje oprogramowania

Kopie zapasowe i plany odzyskiwania danych

Reagowanie na incydenty bezpieczeństwa (30 min)

Procedury postępowania w przypadku incydentu

Zgłaszanie incydentów

Analiza i likwidacja skutków incydentów

Działania prewencyjne

-Warsztaty praktyczne- Warsztaty praktyczne

DZIEŃ II

-- **Dane Osobowe** – podstawowe pojęcia: Ochrona danych osobowych w polskim prawodawstwie: Zasady przetwarzania danych osobowych: Formy przetwarzania danych osobowych- Wprowadzenie do podstawowych pojęć związanych z danymi osobowymi, takich jak dane osobowe, przetwarzanie, administrator danych, podmiot przetwarzający, dane wrażliwe. Wyjaśnienie terminologii stosowanej w przepisach RODO. Omówienie najważniejszych przepisów dotyczących ochrony danych osobowych w polskim systemie prawnym, w tym związków z przepisami unijnymi, głównie RODO, oraz implementacji przepisów na poziomie krajowym. Przedstawienie fundamentalnych zasad przetwarzania danych osobowych zgodnych z RODO, takich jak legalność, rzetelność, przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość oraz integralność i poufność. Omówienie różnych form przetwarzania danych, takich jak zbieranie, przechowywanie, przekazywanie, anonimizacja, archiwizacja, usuwanie i niszczenie danych. Analiza typowych działań przetwarzania w kontekście projektów.

-**Obszar przetwarzania danych:** Dostęp do danych osobowych: Zasady zabezpieczania danych osobowych: Obowiązki osób przetwarzających dane osobowe:-Wyjaśnienie, co oznacza obszar przetwarzania danych, omówienie zakresu geograficznego, a także granic przetwarzania danych w ramach UE i poza nią, w tym przepływu danych transgranicznego oraz zasad ochrony danych w przypadku outsourcingu. Przedstawienie zasad dostępu do danych osobowych przez osoby upoważnione. Procedury przyznawania uprawnień i obowiązki dotyczące ich monitorowania oraz wycofywania, jeśli dostęp nie jest już konieczny. Omówienie technicznych i organizacyjnych środków bezpieczeństwa wymaganych do skutecznego zabezpieczenia danych osobowych, takich jak szyfrowanie, kontrola dostępu, zabezpieczenia fizyczne i elektroniczne, a także audyty i analiza ryzyka. Przedstawienie odpowiedzialności i obowiązków osób, które mają dostęp do danych osobowych, w tym przestrzegania polityk bezpieczeństwa, procedur, szkoleń oraz obowiązku zgłaszania incydentów.

-**Prawa osoby, której dane dotyczą:** Odpowiedzialność prawna osoby przetwarzającej dane osobowe: Przepisy wewnętrzne PW o ochronie danych osobowych:-Omówienie praw przysługujących osobom, których dane są przetwarzane, w tym prawa dostępu do danych, ich sprostowania, usunięcia („prawo do bycia zapomnianym”), ograniczenia przetwarzania, przenoszenia oraz prawa do sprzeciwu wobec przetwarzania danych. Analiza konsekwencji prawnych i finansowych wynikających z naruszenia przepisów RODO, w tym kar administracyjnych, odpowiedzialności cywilnej i karnej, a także sankcji związanych z nieprzestrzeganiem zasad ochrony danych. Omówienie wewnętrznych regulacji uczelni (PW) dotyczących ochrony danych, polityk i procedur obowiązujących pracowników oraz studentów, w tym wymagań dotyczących bezpieczeństwa i zarządzania danymi.

-**Pytania/dyskusja:**-Sesja pytań i odpowiedzi oraz dyskusja podsumowująca, umożliwiająca wyjaśnienie ewentualnych wątpliwości i omówienie przypadków praktycznych, z którymi uczestnicy mogą mieć do czynienia w kontekście ochrony danych osobowych.

Harmonogram

Liczba przedmiotów/zajęć: 13

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Realizacja szkolenia zgodnie z programem – część I,	Mariusz Kończak	21-12-2024	09:00	10:30	01:30
2 z 13 Przerwa	Mariusz Kończak	21-12-2024	10:30	10:45	00:15
3 z 13 Realizacja szkolenia zgodnie z programem – część I	Mariusz Kończak	21-12-2024	10:45	12:30	01:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 13 Przerwa	Mariusz Kończak	21-12-2024	12:30	13:30	01:00
5 z 13 Realizacja szkolenia zgodnie z programem – część I,	Mariusz Kończak	21-12-2024	13:30	15:30	02:00
6 z 13 Realizacja szkolenia zgodnie z programem – część I,	Mariusz Kończak	21-12-2024	15:30	17:00	01:30
7 z 13 Realizacja szkolenia zgodnie z programem – część II	Arnold Paszta	22-12-2024	09:00	10:30	01:30
8 z 13 Realizacja szkolenia zgodnie z programem – część II	Arnold Paszta	22-12-2024	10:00	11:00	01:00
9 z 13 Przerwa	Arnold Paszta	22-12-2024	11:00	11:15	00:15
10 z 13 Realizacja szkolenia zgodnie z programem – część II	Arnold Paszta	22-12-2024	11:15	13:15	02:00
11 z 13 Przerwa	Arnold Paszta	22-12-2024	13:15	14:15	01:00
12 z 13 Realizacja szkolenia zgodnie z programem – część II	Arnold Paszta	22-12-2024	14:15	15:30	01:15
13 z 13 Realizacja szkolenia zgodnie z programem – część II	Arnold Paszta	22-12-2024	15:30	16:30	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 100,00 PLN
Koszt przypadający na 1 uczestnika netto	6 100,00 PLN
Koszt osobogodziny brutto	290,48 PLN
Koszt osobogodziny netto	290,48 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2

Mariusz Kończak

Biegły sądowy w dziedzinie ochrony danych osobowych i informacji niejawnych w systemach informatycznych przy Sądzie Okręgowym w Poznaniu

Pełnomocnik ds. ochrony informacji niejawnych

Inspektor Ochrony Danych Osobowych

Auditor wewnętrzny ISO 27001

Doświadczony trener szkoleń biznesowych. Szkolenia prowadzi od kilkunastu lat.



2 z 2

Arnold Paszta

Biegły sądowy w dziedzinie ochrony informacji niejawnych i danych osobowych przy Sądzie Okręgowym w Bydgoszczy

Inspektor Ochrony danych

Pełnomocnik ochrony informacji niejawnych

Auditor wewnętrzny ISO 27001, ISO 9001

Szkoleniowiec z wieloletnim doświadczeniem.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na początku kursu uczestnicy otrzymują skrypt obejmujący materiał dydaktyczny przygotowany dla danego szkolenia.

Warunki uczestnictwa

Warunkiem uczestnictwa w kursie jest :

1. Posiadanie ważnego numeru ID wsparcia
2. Zapisanie się na wybraną usługę przez stronę www.well.edu.pl (z zaznaczeniem opcji: **Dofinansowanie BUR**)

Uprzejmie przypominamy, iż zgłoszenie na kurs przez BUR nie stanowi potwierdzenia udziału w kursie. **Obligatoryjny jest kontakt z Organizatorem w celu potwierdzenia wolnych miejsc oraz wykonanie czynności opisanych w pkt.2.**

3. W szkoleniu mogą wziąć udział osoby wskazane w sekcji "Grupa docelowa usługi"- w przypadku wątpliwości związanych z uprawnieniami dotyczącymi udziału w szkoleniach, prosimy o kontakt e-mailowy lub telefoniczny.

Informacje dodatkowe

Cena kursu nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności Organizator nie pokrywa oraz nie dokonuje zwrotu kosztów związanych z dojazdem uczestnika na usługę, jego zakwaterowaniem oraz wyżywieniem.

W liczbę godzin dydaktycznych kursu **nie są** wliczone przerwy.

Szkolenie jest zwolnione z podatku VAT na podstawie art. 43 ust. 1 punkt 26 podpunkt a ustawa o VAT lub w przypadku kursów dofinansowanych ze środków publicznych w min. 70% zwolnione z podatku VAT na podstawie art. 43 ust. 1 punkt 29 c.

W zależności od wymogów Operatorów i kwot dofinansowań, mogą pojawić się dodatkowe dopłaty do kursu.

Krótkie przerwy realizowane w czasie trwania kursu dostosowane są do tempa pracy uczestników podczas szkolenia. **Godziny przerw są podane orientacyjnie- w zależności od dynamiki i tempa grupy- mogą ulec zmianie.**

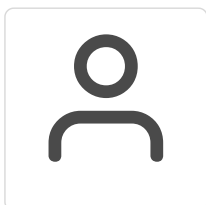
Adres

ul. Okrzei 18
64-920 Piła
woj. wielkopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt



Jakub Ślaga

E-mail dofinansowania@well.edu.pl

Telefon (+48) 718 808 250