



AS PROJECT
ANDRZEJ
SKRZYPCZAK

Brak ocen dla tego dostawcy

Bezpieczeństwo, etyka i regulacje prawne przy wdrażaniu automatyzacji i AI - szkolenie

Numer usługi 2026/09/01/205195/3782129

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👤 Zajęcia indywidualne
- 🕒 40:00 h
- 📅 11.01.2027 do 15.01.2027

7 800,00 PLN brutto
7 800,00 PLN netto
195,00 PLN brutto/h
195,00 PLN netto/h
284,58 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Grupa docelowa usługi	Właściciele samozatrudnieni w firmie będącą Jednoosobową Działalnością Gospodarczą - wdrażający rozwiązania technologiczne i systemy sztucznej inteligencji w sektorze MŚP, posiadający minimalną wiedzę z zakresu zarządzania procesami i infrastrukturą IT w organizacji (firmie).
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1
Data zakończenia rekrutacji	04-12-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

"Bezpieczeństwo, etyka i i regulacje prawne przy wdrożeniu automatyzacji i AI - szkolenie" przygotowuje do samodzielnego przeprowadzenia analizy ryzyka cyberbezpieczeństwa, wdrażania norm i standardów IT oraz projektowania etycznych i zgodnych z prawem rozwiązań automatyzacyjnych opartych na sztucznej inteligencji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Posiada wiedzę z zakresu bezpieczeństwa informacji oraz ochrony danych , które są przydatne na cyberzagrożenia.	Rozpoznaje podstawowe cyberzagrożenia i ich konsekwencje. Poprawnie identyfikuje typowe zagrożenia (phishing, malware, ransomware, ataki socjotechniczne) oraz potrafi wskazać ich potencjalny wpływ na organizację.	Test teoretyczny
	Wyjaśnia zasady bezpiecznego przetwarzania danych. Opisuje kluczowe praktyki ochrony danych (silne hasła, szyfrowanie, kontrola dostępu, polityka czystego biurka, bezpieczne przechowywanie dokumentów) oraz potrafi wskazać, jak minimalizują ryzyko incydentów.	Test teoretyczny
	Stosuje podstawowe procedury reagowania na incydenty. Potrafi wskazać właściwe działania w przypadku podejrzenia naruszenia bezpieczeństwa (zgłoszenie incydentu, odłączenie urządzenia, nieotwieranie podejrzanych plików, zachowanie dowodów).	Test teoretyczny
Zna i rozumie powagę zagrożeń wynikających ze stosowania botów, farmy trolli. malware, ransomware.	Opisuje mechanizmy działania botów, farm trolli, malware i ransomware oraz potrafi wskazać, jakie zagrożenia niosą dla organizacji (np. dezinformacja, utrata danych, paraliż systemów).	Test teoretyczny
	Rozpoznaje symptomy i przykłady ataków związanych z botami, farmami trolli, malware i ransomware oraz potrafi wskazać ich potencjalne skutki (np. utrata reputacji, koszty odzyskiwania danych, wyciek informacji).	Test teoretyczny
	Wskazuje zasady bezpiecznego postępowania i minimalizacji ryzyka (np. aktualizacje, polityki haseł, weryfikacja źródeł informacji, procedury reagowania na incydenty).	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozumie celowość stosowania norm i wytycznych jako elementu zapewniającego jakość i bezpieczeństwo.	Rozumie znaczenie norm i wytycznych w zapewnianiu jakości i bezpieczeństwa. Potrafi wskazać, dlaczego normy i wytyczne są stosowane w procesach organizacyjnych. Opisuje konsekwencje ich braku lub nieprzestrzegania.	Test teoretyczny
	Identyfikuje normy i wytyczne właściwe dla danego obszaru działania. Rozpoznaje, które normy, procedury lub standardy mają zastosowanie w konkretnym procesie. Potrafi uzasadnić wybór odpowiednich norm.	Test teoretyczny
	Analizuje wpływ stosowania norm na jakość i bezpieczeństwo pracy. Wskazuje, jakie elementy procesu są zabezpieczane przez normy; Opisuje, w jaki sposób normy minimalizują ryzyka i podnoszą jakość działań.	Test teoretyczny
Zna i wykorzystuje strukturę normatywów wykorzystywanych w usługach IT.	Identyfikuje i opisuje strukturę normatywów stosowanych w usługach IT . Potrafi wskazać elementy norm (np. zakres, definicje, wymagania, załączniki). Rozróżnia typy norm (np. ISO, branżowe, wewnętrzne procedury).	Test teoretyczny
	Dobiera właściwe normatywy do konkretnej usługi IT. Uzasadnia wybór normy w odniesieniu do charakteru usługi. Wskazuje, które wymagania normy mają zastosowanie w danym procesie.	Test teoretyczny
	Stosuje wymagania normatywów w praktycznym zadaniu. Poprawnie wykorzystuje strukturę normy przy projektowaniu lub ocenie usługi IT. Przedstawia zgodność rozwiązania z wymaganiami normatywnymi.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zna podstawowe zasady etyki w zakresie sztucznej inteligencji.	Identyfikuje i opisuje podstawowe zasady etyki AI – np. przejrzystość, nadzór człowieka, bezpieczeństwo, prywatność, niedyskryminacja, odpowiedzialność.	Test teoretyczny
	Analizuje krótkie studium przypadku i wskazuje, które zasady etyczne zostały zachowane lub naruszone – np. potrafi ocenić, czy system działa transparentnie, czy minimalizuje ryzyko szkód, czy unika stronniczości.	Test teoretyczny
	Wyjaśnia konsekwencje nieprzestrzegania zasad etyki AI – np. ryzyko dyskryminacji, utraty zaufania, szkód społecznych, naruszeń prywatności.	Test teoretyczny
Zna zasady odpowiedzialnego zbierania i wykorzystywania danych na potrzeby wprowadzenia automatyzacji.	Identyfikuje źródła danych oraz określa ich legalność i zgodność z zasadami ochrony danych (RODO / AI Act). Potrafi wskazać, które dane mogą być zbierane, na jakiej podstawie prawnej oraz jakie ograniczenia dotyczą danych wrażliwych.	Test teoretyczny
	Wyjaśnia zasady jakości, kompletności i reprezentatywności danych wykorzystywanych w automatyzacji. Rozumie, że dane muszą być adekwatne do celu, wolne od błędów lub z udokumentowanymi błędami resztkowymi, oraz że ich jakość wpływa na skuteczność automatyzacji.	Test teoretyczny
	Opisuje zasady minimalizacji, bezpieczeństwa i odpowiedzialnego dostępu do danych wykorzystywanych w procesach automatyzacji. Potrafi wskazać, jak ograniczać dostęp (IAM/ABAC), stosować anonimizację/pseudonimizację oraz zapewniać zgodne z prawem wykorzystanie danych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Potrafi dokonać analizy ryzyka dla zautomatyzowanych procesów.	Potrafi wskazać, czym różnią się m.in. boty, farmy trolli, malware, ransomware, oraz wyjaśnić, jakie konsekwencje mogą mieć dla organizacji (np. utrata danych, paraliż systemów, szkody reputacyjne).	Obserwacja w warunkach symulowanych
	Potrafi opisać, jakie dane są szczególnie podatne na cyberzagrożenia (np. dane osobowe, dane finansowe, loginy), oraz przedstawia podstawowe środki ochrony (szyfrowanie, segmentacja sieci, polityki dostępu, aktualizacje). Potrafi dobrać adekwatne środki zapobiegawcze do konkretnego zagrożenia (np. jak chronić się przed ransomware, jak ograniczyć wpływ botów i farm trolli, jak reagować na podejrzane aktywności).	Obserwacja w warunkach symulowanych Obserwacja w warunkach symulowanych
Potrafi ocenić zgodność procesów w zakresie automatyzacji z obowiązującymi regulacjami prawnymi dotyczącymi cyberbezpieczeństwa i ochrony danych.	Potrafi wskazać konkretne przepisy (np. RODO, KSC, wytyczne EROD, normy ISO 27001/27701), które regulują bezpieczeństwo informacji i ochronę danych w danym procesie.	Obserwacja w warunkach symulowanych
	Ocenia, czy sposób działania automatyzacji może prowadzić do niezgodności (np. nadmierne przetwarzanie danych, brak kontroli dostępu, brak rejestrowania operacji, nieadekwatne szyfrowanie).	Obserwacja w warunkach symulowanych
	Przedstawia konkretne środki techniczne i organizacyjne (np. pseudonimizacja, minimalizacja danych, DPIA, aktualizacja polityk bezpieczeństwa), które zapewniają zgodność procesu z wymaganiami prawnymi.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Analizuje wymagania projektowe i dopasowuje odpowiednie standardy IT	Potrafi wskazać, które elementy projektu wymagają odniesienia do norm (np. bezpieczeństwo, interoperacyjność, jakość danych) oraz dobiera odpowiednie standardy (np. ISO/IEC 27001, ITIL, COBIT, ISO/IEC 25010).	Obserwacja w warunkach symulowanych
	Przedstawia logiczne, merytoryczne uzasadnienie wyboru norm, pokazując zależność między wymaganiami projektowymi a wybranym standardem (np. „wybieram ISO/IEC 27002, ponieważ projekt obejmuje przetwarzanie danych osobowych i wymaga wdrożenia środków bezpieczeństwa”).	Obserwacja w warunkach symulowanych
	Potrafi ocenić różnice między standardami (np. ITIL vs. COBIT, ISO 9001 vs. ISO/IEC 20000) i wybrać ten, który najlepiej odpowiada specyfice projektu, ryzykom i wymaganiom interesariuszy.	Obserwacja w warunkach symulowanych
Wdraża procedury zgodnie z normami, przegląda i cyklicznie aktualizuje Politykę Bezpieczeństwa Informacji	Potrafi poprawnie zastosować procedury bezpieczeństwa informacji w oparciu o normy (np. ISO/IEC 27001, ISO/IEC 27002) oraz wykazuje zgodność działań z wymaganiami organizacyjnymi.	Obserwacja w warunkach symulowanych
	Potrafi ocenić, które elementy PBI wymagają aktualizacji, wskazuje niezgodności, ryzyka lub obszary wymagające doprecyzowania w kontekście zmian technologicznych, organizacyjnych lub prawnych.	Obserwacja w warunkach symulowanych
	Przygotowuje lub modyfikuje zapisy PBI zgodnie z ustalonym harmonogramem przeglądów, dokumentuje zmiany oraz uzasadnia ich konieczność w odniesieniu do norm i ryzyk bezpieczeństwa.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Potrafi wskazać ryzyko etyczne i prawne przy wdrożeniu automatyzacji opartej na AI, takie jak np. dyskryminacja czy profilowanie	Identyfikuje i opisuje kluczowe ryzyka etyczne i prawne związane z automatyzacją AI – np. dyskryminację wynikającą z danych treningowych, nieuprawnione profilowanie, brak przejrzystości decyzji, ryzyko naruszenia praw podstawowych. Przypisuje zidentyfikowane ryzyka do odpowiednich wymogów regulacyjnych – np. wskazuje, że dyskryminacja i profilowanie mogą naruszać RODO, a brak nadzoru człowieka lub nieprzejrzystość decyzji narusza wymogi dla systemów wysokiego ryzyka (Art. 9, Art. 13–14 AI Act).	Obserwacja w warunkach symulowanych Obserwacja w warunkach symulowanych
	Wyjaśnia konsekwencje prawne i organizacyjne niezarządzania ryzykiem – np. ryzyko kar finansowych, zakazu używania systemu, szkód reputacyjnych, utraty zaufania użytkowników, naruszenia praw podstawowych.	Obserwacja w warunkach symulowanych
Tworzy polityki i procedury dotyczące odpowiedniego wykorzystania AI w przedsiębiorstwie.	Potrafi wskazać, które dane nie mogą trafić do narzędzi AI (np. dane osobowe, tajemnice przedsiębiorstwa, dane klientów, dane finansowe).	Obserwacja w warunkach symulowanych
	Opracowuje ścieżkę zgłaszania incydentów (np. przypadkowe wprowadzenie danych osobowych do narzędzia AI) oraz określa czas reakcji i odpowiedzialne role.	Obserwacja w warunkach symulowanych
	Opracowuje kompletną strukturę polityki AI zgodną z obowiązkami wynikającymi z AI Act i RODO	Obserwacja w warunkach symulowanych
Swoje działania opiera na podejściu pełnym odpowiedzialności i rzetelności.	Podejmuje decyzje z uwzględnieniem konsekwencji dla innych	Obserwacja w warunkach symulowanych
	Przestrzega ustalonych zasad, procedur i standardów jakości	Obserwacja w warunkach symulowanych
	Rzetelnie realizuje powierzone zadania i bierze odpowiedzialność za ich wynik	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Posiada świadomość konsekwencji prawnych i biznesowych i umiejętność pracy w sytuacjach kryzysowych.	Potrafi wskazać prawne i biznesowe skutki decyzji podejmowanych w sytuacji kryzysowej	Obserwacja w warunkach symulowanych
	Reaguje w sposób odpowiedzialny i zgodny z zasadami etycznymi oraz obowiązującymi regulacjami	Obserwacja w warunkach symulowanych
	Wykazuje umiejętność współpracy i komunikacji w warunkach presji	Obserwacja w warunkach symulowanych
Stosuje wewnętrzny ład korporacyjny na styku wymagań klienta a standardami i normami IT	Potrafi negocjować wymagania klienta w sposób zgodny z zasadami ładu korporacyjnego	Test teoretyczny
	Komunikuje ograniczenia wynikające ze standardów IT w sposób profesjonalny i transparentny Wykazuje odpowiedzialność w podejmowaniu decyzji na styku interesów klienta i organizacji	Obserwacja w warunkach rzeczywistych Test teoretyczny
Wspiera tłumaczy regulacje, normy i standardy w celu wytworzenia produktu końcowego jakim mogą być systemy IT	Potrafi wyjaśnić regulacje i normy w sposób zrozumiały	Obserwacja w warunkach symulowanych
	Współpracuje z różnymi rolami w projekcie, aby zapewnić zgodność produktu z wymaganiami regulacyjnymi	Obserwacja w warunkach symulowanych
	Reaguje na problemy związane z niezgodnością regulacyjną i wspiera zespół w ich rozwiązywaniu	Obserwacja w warunkach symulowanych
Rozumie i stosuje się do regulacji i norm.	Przestrzega ustalonych zasad i procedur w pracy zespołowej	Obserwacja w warunkach symulowanych
	Wykazuje odpowiedzialność za skutki działań związanych z przestrzeganiem norm	Obserwacja w warunkach symulowanych
	Wspiera innych w stosowaniu regulacji i norm	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje ryzyka regulacyjne na wczesnym etapie analizy.	Identyfikuje potencjalne naruszenia regulacji w początkowej fazie pracy	Obserwacja w warunkach symulowanych
	Wykazuje czujność na zmiany w otoczeniu prawnym	Obserwacja w warunkach symulowanych
	Proponuje działania ograniczające ryzyko regulacyjne	Obserwacja w warunkach symulowanych

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

Warunki organizacyjne:

Szkolenie realizowane w kameralnej grupie (2–5 osób), co gwarantuje pełną interakcję i warsztatowy charakter pracy. Każdy uczestnik ma zapewnione indywidualne, w pełni wyposażone stanowisko komputerowe z dostępem do Internetu, oprogramowania chmurowego i platform no-code oraz narzędzi AI

Walidacja:

Walidacja przeprowadzana jest w 5. dniu usługi w dedykowanym bloku 15:00–16:00 przez niezależnego walidatora z zachowaniem bezwzględnej rozdzielnosci funkcji szkoleniowej i egzaminacyjnej.

Walidacja Formatywna (w trakcie szkolenia):

- bieżąca ocena ćwiczeń przez trenera,
- Feelback i korekta promptów oraz automatyzacji na bieżąco.

Walidacja Sumatywna (na zakończenie szkolenia):

- **Test wiedzy:** Test jednokrotnego wyboru sprawdzający zagadnienia pojęciowe i ekologiczne
- **Projekt Praktyczny (Case Study):** Samodzielna automatyzacja wskazanego procesu handlowo-biurowego przy użyciu AI i narzędzi no-code,
- **Ocena końcowa:** Pozytywne wykonanie zadania praktycznego (minimum 70 % poprawności) oraz zaliczenie testu wiedzy.

Plan szkolenia:

- Dzień 1 - Cyberbezpieczeństwo i ochrona danych w MŚP (8 godzin)
- Dzień 2 - Normy, wytyczne i standardy IT w automatyzacji (8 godzin)
- Dzień 3 - Etyka AI, dane i odpowiedzialne projektowanie automatyzacji (8 godzin)
- Dzień 4 - Analiza ryzyka i zgodność prawna automatyzacji (8 godzin)
- Dzień 5 - Polityki AI, PBI i walidacja (8 godzin)

Harmonogram

Liczba pozycji harmonogramu: 50

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 50 Moduł 1 - Cyberbezpieczeństwo i ochrona danych w MŚP - Wprowadzenie, cele szkolenia, kontrakt, oczekiwania	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	08:00	08:30	00:30
2 z 50 Wprowadzenie do cyberbezpieczeństwa w MŚP	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	08:30	09:30	01:00
3 z 50 Podstawowe pojęcia i modele zagrożeń	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	09:30	10:30	01:00
4 z 50 -	Przerwa	-	11-01-2027	10:30	11:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 50 Ochrona danych osobowych (RODO) w praktyce MŚP	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	11:00	12:00	01:00
6 z 50 Bezpieczna praca użytkownika - praktyczne zasady	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	12:00	13:00	01:00
7 z 50 -	Przerwa	-	11-01-2027	13:00	13:30	00:30
8 z 50 Bezpieczeństwo systemów i urządzeń w MŚP	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	13:30	14:30	01:00
9 z 50 Incydenty bezpieczeństwa - jak reagować?	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	14:30	15:15	00:45
10 z 50 Ćwiczenia praktyczne i analiza przypadków	Zajęcia	ANDRZEJ SKRZYPCZAK	11-01-2027	15:15	16:00	00:45
11 z 50 Moduł 2 - Normy, wytyczne i standardy IT w automatyzacji - wprowadzenie	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	08:00	08:30	00:30
12 z 50 Wprowadzenie do norm i standardów IT	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	08:30	09:30	01:00
13 z 50 ISO w automatyzacji procesów IT	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	09:30	10:30	01:00
14 z 50 -	Przerwa	-	12-01-2027	10:30	11:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 50 ITIL 4 i automatyzacja usług IT	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	11:00	12:00	01:00
16 z 50 Standardy bezpieczeństwa i zgodności	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	12:00	13:00	01:00
17 z 50 -	Przerwa	-	12-01-2027	13:00	13:30	00:30
18 z 50 Standardy integracji i automatyzacji technicznej	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	13:30	14:30	01:00
19 z 50 Warsztaty - projektowanie automatyzacji zgodnej z normami - część 1	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	14:30	15:15	00:45
20 z 50 Warsztaty - projektowanie automatyzacji zgodnej z normami - część 2 i podsumowanie	Zajęcia	ANDRZEJ SKRZYPCZAK	12-01-2027	15:15	16:00	00:45
21 z 50 Moduł 3 - Etyka AI, dane i odpowiedzialne projektowanie automatyzacji - wprowadzenie	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	08:00	08:30	00:30
22 z 50 Fundamenty etyki AI i odpowiedzialnego wykorzystania danych	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	08:30	09:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 50 Ryzyka algorytmiczne i mechanizmy powstawania błędów	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	09:30	10:30	01:00
24 z 50 -	Przerwa	-	13-01-2027	10:30	11:00	00:30
25 z 50 RODO, prywatność i zgodność regulacyjna w projektowaniu automatyzacji	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	11:00	12:00	01:00
26 z 50 Odpowiedzialne projektowanie automatyzacji krok po kroku	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	12:00	13:00	01:00
27 z 50 -	Przerwa	-	13-01-2027	13:00	13:30	00:30
28 z 50 Etyczne wykorzystanie narzędzi AI w codziennej pracy	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	13:30	14:30	01:00
29 z 50 Audyt etyczny automatyzacji i AI	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	14:30	15:15	00:45
30 z 50 Podsumowanie, rekomendacje i plan wdrożenia	Zajęcia	ANDRZEJ SKRZYPCZAK	13-01-2027	15:15	16:00	00:45
31 z 50 Moduł 4 - Analiza ryzyka i zgodność prawna automatyzacji - wprowadzenie	Zajęcia	MARCIN PRACZYK	14-01-2027	08:00	08:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
32 z 50 Podstawy analizy ryzyka i zgodności prawnej	Zajęcia	MARCIN PRACZYK	14-01-2027	08:30	09:30	01:00
33 z 50 Analiza ryzyka - matryce, identyfikacja zagrożeń	Zajęcia	MARCIN PRACZYK	14-01-2027	09:30	10:30	01:00
34 z 50 -	Przerwa	-	14-01-2027	10:30	11:00	00:30
35 z 50 Dane podatkne na zagrożenia i środki ochrony	Zajęcia	MARCIN PRACZYK	14-01-2027	11:00	12:00	01:00
36 z 50 Przepisy RODO, ISO, AI Act, KSC	Zajęcia	MARCIN PRACZYK	14-01-2027	12:00	13:00	01:00
37 z 50 -	Przerwa	-	14-01-2027	13:00	13:30	00:30
38 z 50 Identyfikacja i ocena ryzyka	Zajęcia	MARCIN PRACZYK	14-01-2027	13:30	14:30	01:00
39 z 50 Ocena zgodności automatyzacji	Zajęcia	MARCIN PRACZYK	14-01-2027	14:30	15:15	00:45
40 z 50 Zarządzanie ryzykiem i zgodnością - wdrożenia	Zajęcia	MARCIN PRACZYK	14-01-2027	15:15	16:00	00:45
41 z 50 Moduł 5 - Polityki AI, PBI i walidacja - wprowadzenie	Zajęcia	MARCIN PRACZYK	15-01-2027	08:00	08:30	00:30
42 z 50 Polityka AI - struktura i obowiązki	Zajęcia	MARCIN PRACZYK	15-01-2027	08:30	09:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
43 z 50 Dane zakazane oraz procedury icydentowe	Zajęcia	MARCIN PRACZYK	15-01-2027	09:30	10:30	01:00
44 z 50 -	Przerwa	-	15-01-2027	10:30	11:00	00:30
45 z 50 Projektowanie polityki AI - praktyczne komponenty	Zajęcia	MARCIN PRACZYK	15-01-2027	11:00	12:00	01:00
46 z 50 Power BI w kontekście polityki AI - dane, jakość, odpowiedzialność	Zajęcia	MARCIN PRACZYK	15-01-2027	12:00	13:00	01:00
47 z 50 -	Przerwa	-	15-01-2027	13:00	13:30	00:30
48 z 50 AI i Power BI odpowiedzialne wykorzystanie automatyzacji	Zajęcia	MARCIN PRACZYK	15-01-2027	13:30	14:30	01:00
49 z 50 Wdrożenie polityki AI w organizacji (firmie)	Zajęcia	MARCIN PRACZYK	15-01-2027	14:30	15:00	00:30
50 z 50 -	Walidacja	-	15-01-2027	15:00	16:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	40:00
w tym suma godzin zajęć	34:00
w tym suma godzin walidacji	01:00
w tym suma przerw	05:00

Rodzaj godzin	Liczba godzin
Suma godzin dydaktycznych bez przerw	46:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	7 800,00 PLN
Koszt osobogodziny brutto	195,00 PLN
Koszt osobogodziny netto	195,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

Prowadzący

Liczba prowadzących: 2

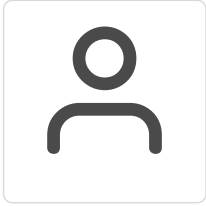


1 z 2

ANDRZEJ SKRZYPCZAK

Trener usług projektowych z zakresu ochrony środowiska. Prowadzi szkolenia dla firm i instytucji, aby pomóc im spełnić obowiązki prawne związane ze środowiskiem, wdrażać innowacyjne rozwiązania oraz minimalizować negatywny wpływ na otoczenie. Doskonale przekazuje wiedzę dotyczącą m.in. gospodarki odpadami, ochrony powietrza i wód, a także pomaga w tworzeniu i wdrażaniu projektów, które służą celom zrównoważonego rozwoju i zielonych kompetencji. Sporządza raporty ochrony środowiska dla przedsiębiorstw uciążliwych dla środowiska. Prowadzi także warsztaty z komunikacji i kompetencji miękkich. Posiada co najmniej 100-godzinne doświadczenie w prowadzeniu szkoleń, z zakresu tematycznego usługi dla osób dorosłych w ciągu ostatnich 3 lat wstecz od dnia rozpoczęcia szkolenia. Specjalizuje się także w szkoleniach z obszaru: komunikacji interpersonalnej, zarządzania, przywództwa i budowania zespołu, umiejętności wiedzy i postaw, które są niezbędne do wspierania zrównoważonego rozwoju i ochrony środowisk oraz kompetencji przyszłości.

Doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą opublikowania usługi



2 z 2

MARCIN PRACZYK

Z wykształcenia inżynier informatyk. Posiada również certyfikat PRINCE2 Foundation z zakresu zarządzania projektami oraz certyfikat znajomości języka angielskiego ACERT na poziomie C1. Prowadzi własną działalność gospodarczą, w tym szkolenia. Do głównych moich kompetencji należą:

- praktyczne wykorzystanie sztucznej inteligencji i narzędzi generatywnych w pracy zawodowej;
- zaawansowane korzystanie z ChatGPT i innych narzędzi AI;
- prompt engineering i projektowanie skutecznych instrukcji dla modeli AI;
- automatyzacja pracy biurowej i cyfryzacja procesów;
- kompetencje informatyczne i szeroko rozumiana praca z narzędziami cyfrowymi;
- podstawy cyberbezpieczeństwa użytkownika i bezpiecznej pracy z informacją;
- profesjonalny research internetowy, analiza źródeł i weryfikacja informacji;
- digitalizacja dokumentów OCR, praca z PDF i dokumentami archiwalnymi.

Dodatkowym atutem jest możliwość prowadzenia szkoleń nie tylko po polsku, ale również po portugalsku brazylijskim, oraz po angielsku.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik usługi otrzymuje komplet materiałów szkoleniowych w formie elektronicznej:

1. Autorski podręcznik szkoleniowy „Bezpieczeństwo, etyka i regulacje prawne przy wdrażaniu automatyzacji i AI”,
2. Materiały dydaktyczne w formie prezentacji powerpoint.

Warunki uczestnictwa

1. Wykształcenie minimum średnie.
2. Podstawowa umiejętność obsługi komputera, pakietów biurowych oraz środowiska przeglądarki internetowej.
3. Dostęp do komputera, laptopa lub telefonu
4. Dostęp darmowych lub testowych wersji narzędzi np. ChatGPT, Gemini, MsOffice
5. Wypełnienie wstępnej ankiety analizy potrzeb w celu zidentyfikowania procesów operacyjnych kwalifikujących się do optymalizacji zasobowej i automatyzacji w macierzystej firmie.

Informacje dodatkowe

1. Zapewniona sala szkoleniowa spełniająca wymogi BHP, stanowiska komputerowe z dostępem do Internetu szerokopasmowego, rzutnik multimedialny oraz dostęp do aktualnych regulacji i norm - w przypadku szkoleń stacjonarnych,
2. Dostęp do komputera z dostępem do Internetu szerokopasmowego - w przypadku szkolenia zdalnego w czasie rzeczywistym.

Warunki techniczne

W przypadku szkolenia zdalnego w czasie rzeczywistym Uczestnik szkolenia musi mieć dostęp do komputera z Internetem szerokopasmowym oraz dostęp do platformy Meet Google.

Kontakt



ANDRZEJ SKRZYPCZAK

E-mail asproject@wp.pl

Telefon (+48) 792 005 821