



Kryptoaktywa – prawne aspekty w administracji publicznej

Numer usługi 2025/05/08/161638/2731884

2 400,00 PLN brutto
2 400,00 PLN netto
120,00 PLN brutto/h
120,00 PLN netto/h

KORYCKI &
GRACZYK
CONSULTING
GROUP SPÓŁKA Z
OGRAŃCZONĄ
ODPOWIEDZIALNOŚ
CIĄ



📍 zdalna w czasie rzeczywistym
🏠 Usługa szkoleniowa
🕒 20 h
📅 26.07.2025 do 27.07.2025

Informacje podstawowe

Kategoria	Prawo i administracja / Administracja publiczna
Identyfikator projektu	Małopolski Pociąg do kariery
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Specjaliści ds. bezpieczeństwa i cyberbezpieczeństwa, • Pracownicy działów AML/KYC, Compliance i audytu wewnętrznego, • Prawnicy i doradcy podatkowi zajmujący się tematyką kryptoaktywów, • Pracownicy instytucji finansowych, banków oraz fintechów, • Osoby odpowiedzialne za wdrażanie procedur zarządzania ryzykiem i regulacji, • Osoby zainteresowane tematyką cyberbezpieczeństwa w zakresie transakcji kryptowalutami. • Uczestnicy projektu Małopolski Pociąg do Kariery
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	1
Data zakończenia rekrutacji	14-07-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	20
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem edukacyjnym jest wyposażenie uczestników w zaawansowaną, praktyczną wiedzę dotyczącą zarówno technicznych mechanizmów funkcjonowania kryptowalut i rozwiązań blockchain, jak i prawno-regulacyjnych wymagań związanych z tym rynkiem. Uczestnicy nauczą się ponadto identyfikować, analizować i raportować podejrzone transakcje w kontekście AML i cyberbezpieczeństwa, co ułatwi im skuteczne zabezpieczanie organizacji przed zagrożeniami i zapewnienie zgodności z obowiązującymi przepisami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
rozdziela kluczowe typy kryptoaktywów (kryptowaluty, tokeny użytkowe, security tokens, NFT) oraz odróżnia je od walut wirtualnych używanych np. w grach	Uczestnik rozróżnia poszczególne rodzaje kryptoaktywów	Test teoretyczny
	Uczestnik definiuje pojęcia związane z kryptoaktywami	Test teoretyczny
definiuje podstawowe pojęcia z obszaru kryptowalut i blockchain (m.in. decentralizacja, konsensus, smart kontrakty),	Uczestnik rozróżnia podstawowe pojęcia z obszaru kryptowalut i blockchain	Test teoretyczny
	Uczestnik opisuje cechy blockchain	Test teoretyczny
charakteryzuje mechanizmy działania sieci blockchain (m.in. funkcje hashujące, rolę górników/walidatorów, model P2P) oraz specyfikę transakcji,	Uczestnik charakteryzuje specyfikę transakcji w systemie blockchain	Test teoretyczny
	Uczestnik definiuje pojęcia związane z działaniem mechanizmu blockchain	Test teoretyczny
uzasadnia konieczność wypełniania wymogów KYC/AML oraz znaczenie raportowania podejrzanym transakcji w kontekście przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu	Uczestnik charakteryzuje wymogi KYC oraz AML w kontekście przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu	Deбата swobodna
	Uczestnik uzasadnia istotę raportowania podejrzanym transakcji	Deбата swobodna
	Uczestnik rozróżnia najważniejsze schematy działań hakerów z wykorzystaniem kryptoaktywów	Test teoretyczny
	Uczestnik identyfikuje potencjalnie podejrzanym schematy działań w systemie blockchain	Obserwacja w warunkach symulowanych
	Uczestnik monitoruje rynek kryptowalut i transakcji w systemie blockchain	Obserwacja w warunkach symulowanych
monitoruje rynek kryptowalut i transakcje w celu identyfikacji potencjalnie podejrzanym schematów (darknet markets, ataki phishingowe, rug pull)		

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
planuje strategię przeciwdziałania zagrożeniom cyberbezpieczeństwa związanym z obrotem kryptowalutami (m.in. wdrażanie procedur wieloskładnikowego uwierzytelniania, audyty bezpieczeństwa)	Uczestnik projektuje strategię przeciwdziałania zagrożeniom naruszającym istotę cyberbezpieczeństwa związaną z obrotem kryptowalutami	Obserwacja w warunkach symulowanych
	Uczestnik przygotowuje procedury w zakresie zwiększenia cyberbezpieczeństwa związanego z obrotem kryptowalutami	Obserwacja w warunkach symulowanych
	Uczestnik organizuje audyty bezpieczeństwa cyfrowego	Obserwacja w warunkach symulowanych
projektuje wewnętrzne procedury i polityki AML, uwzględniające specyfikę transakcji w kryptowalutach oraz wymogi obowiązujących przepisów	Uczestnik projektuje polityki AML w celu zwiększenia bezpieczeństwa transakcji oraz zapewnienia zgodności z obowiązującymi przepisami	Obserwacja w warunkach symulowanych
organizuje proces identyfikacji ryzyka oraz wdrażania metod ograniczania nieprawidłowości i przestępstw (m.in. layering, smurfing, pranie pieniędzy przez DeFi)	Uczestnik uzasadnia istotę identyfikacji i analizy ryzyka	Debata swobodna
	Uczestnik analizuje ryzyko w celu ograniczania nieprawidłowości i przestępstw	Obserwacja w warunkach symulowanych
	Uczestnik rozróżnia rodzaje przestępstw związanych z kryptowalutami	Test teoretyczny
	Uczestnik analizuje zgodność przepływów kryptowalutowych z regulacjami w prawie krajowym, unijnym i międzynarodowym	Obserwacja w warunkach symulowanych
	Uczestnik charakteryzuje najważniejsze przepisy związane z zasadami bezpieczeństwa cyfrowego w zakresie transakcji kryptowalutami	Debata swobodna
kontroluje zgodność przepływów kryptowalutowych z regulacjami (polskimi i międzynarodowymi) oraz wewnętrznymi standardami bezpieczeństwa	Uczestnik rozróżnia podstawy prawne związane z bezpieczeństwem przepływów kryptowalutowych w zakresie prawa wewnętrznego, krajowego, unijnego i międzynarodowego	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
ocenia poziom ryzyka związanego z wykorzystaniem różnych rodzajów portfeli (hot, cold, sprzętowych) i giełd (CEX, DEX) w kontekście technicznym i prawnym nadzoruje wdrażanie procedur wewnętrznych (SOP) w firmie lub instytucji, mających na celu wykrywanie i raportowanie podejrzanych transakcji oraz utrzymanie zgodności z przepisami KYC/AML	Uczestnik rozróżnia rodzaje portfeli służących do przechowywania walut cyfrowych	Test teoretyczny
	Uczestnik charakteryzuje rodzaje giełd w zakresie handlu kryptowalutami	Debata swobodna
	Uczestnik analizuje poziom ryzyka związany z handlem kryptowalutami na giełdach kryptowalut w zakresie technicznym oraz prawnym	Obserwacja w warunkach symulowanych
	Uczestnik uzasadnia istotę wdrożenia procedur wewnętrznych (SOP) w firmie	Debata swobodna
	Uczestnik organizuje proces raportowania podejrzanych transakcji Uczestnik nadzoruje utrzymanie zgodności z przepisami KYC/AML	Obserwacja w warunkach symulowanych Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, dokument potwierdzający uzyskanie kompetencji 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

Dzień 1 – podstawy prawne i organizacyjne

8:00 – 8:45 – **Moduł 1: Otwarcie i kontekst sektorowy**

- Cele szkolenia i obowiązki służb publicznych
- Rola kryptoaktywów dla JST, ministerstw, służb skarbowych i organów ścigania

8:45 – 9:30 – **Moduł 2: Podstawowe pojęcia i technologie w ujęciu prawnym**

- Definicje: kryptoaktywo, waluta wirtualna, token (utility, asset-referenced, e-money, NFT)
- Blockchain i smart-kontrakty – tylko tyle techniki, ile potrzebne przy stosowaniu prawa

9:30 – 9:45 – *Przerwa*

9:45 – 11:15 – **Moduł 3: Status prawny kryptoaktywów w Polsce**

- Podatki PIT/CIT/VAT - kwalifikacja przychodów
- Ustawa AML, implementacja 5 AMLD / 6 AMLD
- Stanowiska KNF, NBP, GIIF
- Zadania Krajowej Administracji Skarbowej (egzekucja, zajęcia)

11:15 – 11:30 – *Przerwa*

11:30 – 13:15 – **Moduł 4: Prawo UE – MiCA i inne akty**

- Rozporządzenie MiCA – obowiązki emitentów i CASP-ów
- DORA (cyber-resilience) – znaczenie dla organów regulacyjnych
- Travel Rule (TFR) – wymiana danych między instytucjami
- Kiedy administracja publiczna staje się odpowiedzialna za nadzór lub raportowanie

13:15 – 14:00 – *Przerwa obiadowa*

14:00 – 15:30 – **Moduł 5: KYC/AML w praktyce urzędów**

- Identyfikacja stron transakcji (zamówienia publiczne, darowizny)
- Wzorcowe procedury wewnętrzne (SOP)
- Współpraca z GIIF, raporty STR/SAR

15:30 – 15:45 – *Przerwa*

15:45 – 17:00 – **Moduł 6: Kryptoaktywa a prawo finansów publicznych i zamówienia**

- Czy samorząd może przyjmować płatności w kryptoaktywach?
- Ewidencja i wycena kryptowalut w księgach JST
- Ryzyka kursowe i zabezpieczenia prawne
- Zapłata tokenami w zamówieniach publicznych – dopuszczalność i procedura

Dzień 2 – egzekucja, dowody cyfrowe i współpraca międzyinstytucjonalna

8:00 – 9:30 – **Moduł 7: Analiza blockchain dla potrzeb organów administracji**

- Eksploracja blockchain (Etherscan, mempool-watch)
- Identyfikacja adresów powiązanych z przestępstwem (heurystyki, klastrowanie)
- Otwarte vs. komercyjne narzędzia (Chainalysis, GraphSense) – licencje dla sektora publicznego

9:30 – 9:45 – *Przerwa*

9:45 – 11:15 – **Moduł 8: Zabezpieczenie i zajęcie kryptoaktywów**

- Podstawa prawna zajęcia (KPK, KKS, egzekucja administracyjna)
- Kopia klucza prywatnego / transfer środków – procedura
- Przechowywanie skonfiskowanych walut – cold-storage pod nadzorem skarbowym

11:15 – 11:30 – *Przerwa*

11:30 – 13:15 – **Moduł 9: Schematy nadużyć przeciw instytucjom publicznym**

- Wyłudzenia dotacyjne, fałszywe tokenizacje majątku publicznego
- Ransomware w infrastrukturze JST – analiza strumieni płatności
- Pranie pieniędzy przez darowizny kryptowalutowe na cele charytatywne gmin

13:15 – 14:00 – *Przerwa obiadowa*

14:00 – 15:00 – **Moduł 10: Ochrona danych osobowych i cyberbezpieczeństwo**

- RODO vs. nieodwracalność blockchain (pseudonimizacja, prawo do bycia zapomnianym)
- Ustawa o KSC – wymogi wobec giełd i portfeli
- DORA – raportowanie incydentów cybernetycznych

15:00 – 16:00 – **Moduł 11: Studia przypadków i ćwiczenia warsztatowe**

- Analiza łańcucha transakcji NFT użytego do prania pieniędzy
- Symulacja postępowania egzekucyjnego – od zajęcia do sprzedaży kryptoaktywa

17:30 – 18:15 – **Moduł 12: Walidacja**

Harmonogram

Liczba przedmiotów/zajęć: 19

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 19 Moduł 1: Otwarcie i kontekst sektorowy	Wojciech Graczyk	26-07-2025	08:00	08:45	00:45
2 z 19 Moduł 2: Podstawowe pojęcia i technologie w ujęciu prawnym	Wojciech Graczyk	26-07-2025	08:45	09:30	00:45
3 z 19 Przerwa	Wojciech Graczyk	26-07-2025	09:30	09:45	00:15
4 z 19 Moduł 3: Status prawny kryptoaktywów w Polsce	Wojciech Graczyk	26-07-2025	09:45	11:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 19 przerwa	Wojciech Graczyk	26-07-2025	11:15	11:30	00:15
6 z 19 Moduł 4: Moduł 4: Prawo UE – MiCA i inne akty	Wojciech Graczyk	26-07-2025	11:30	13:15	01:45
7 z 19 Przerwa obiadowa	Wojciech Graczyk	26-07-2025	13:15	14:00	00:45
8 z 19 Moduł 5: Moduł 5: KYC/AML w praktyce urzędów	Wojciech Graczyk	26-07-2025	14:00	15:30	01:30
9 z 19 przerwa	Wojciech Graczyk	26-07-2025	15:30	15:45	00:15
10 z 19 Moduł 6: Kryptoaktywa a prawo finansów publicznych i zamówienia	Wojciech Graczyk	26-07-2025	15:45	17:00	01:15
11 z 19 Moduł 7: Analiza blockchain dla potrzeb organów administracji	Wojciech Graczyk	27-07-2025	08:00	09:30	01:30
12 z 19 przerwa	Wojciech Graczyk	27-07-2025	09:30	09:45	00:15
13 z 19 Moduł 8: Zabezpieczenie i zajęcie kryptoaktywów	Wojciech Graczyk	27-07-2025	09:45	11:15	01:30
14 z 19 Przerwa	Wojciech Graczyk	27-07-2025	11:15	11:30	00:15
15 z 19 Moduł 9: Schematy nadużyć przeciw instytucjom publicznym	Wojciech Graczyk	27-07-2025	11:30	13:15	01:45
16 z 19 przerwa obiadowa	Wojciech Graczyk	27-07-2025	13:15	14:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 19 Moduł 10: Ochrona danych osobowych i cyberbezpieczeństwo	Wojciech Graczyk	27-07-2025	14:00	15:00	01:00
18 z 19 Moduł 11: Studia przypadków i ćwiczenia warsztatowe	Wojciech Graczyk	27-07-2025	15:00	16:00	01:00
19 z 19 Walidacja	-	27-07-2025	17:30	18:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 400,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN
Koszt osobogodziny brutto	120,00 PLN
Koszt osobogodziny netto	120,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Wojciech Graczyk

Wojciech Graczyk – trener kompetencji miękkich oraz cyfrowych, który podczas swoich szkoleń stawia na praktykę i efekty. W ciągu ostatnich pięciu lat przeprowadził ponad 2300 godzin szkoleń, w tym ponad 400 godzin zegarowych w zakresie cyberbezpieczeństwa. Obecnie jest administratorem danych osobowych w spółce pod firmą KORYCKI & GRACZYK CONSULTING GROUP sp. z o.o. oraz jest odpowiedzialny za zabezpieczanie systemów, danych oraz informacji w infrastrukturze firmowej. Ukończył specjalistyczne szkolenia w zakresie zaawansowanych technik cyberbezpieczeństwa ze szczególnym uwzględnieniem prawnych aspektów cyberbezpieczeństwa oraz ustalania haseł. Dodatkowo ukończył kurs w zakresie ochrony danych osobowych na wydziale psychologii i prawa Uniwersytetu SWPS w Poznaniu. Współpracował z Marcinem Smreczakem w

celu popularyzacji wiedzy technicznej i prawnej w zakresie kryptowalut. Jest również autorem e-booka w zakresie kryptowalut i licznych artykułów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany w wiadomości e-mail dla każdego z uczestników szkolenia.

Zestaw materiałów szkoleniowych składa się z **prezentacji** oraz **skryptu szkolenia**.

Informacje dodatkowe

1) Uczestnik szkolenia otrzyma zaświadczenie o ukończeniu szkolenia dopiero **po pozytywnym wyniku walidacji**, która składa się z **testu sprawdzającego wiedzę**, który odbędzie się w ostatnim bloku zajęciowym oraz **obserwacji w warunkach symulowanych** kompetencji zdobytych podczas szkolenia. Warunkiem otrzymania zaświadczenia o ukończeniu szkolenia jest pozytywny wynik walidacji (próg zdawalności **80%**) oraz frekwencja na minimalnym poziomie **80%**.

2) Informujemy, że szkolenie będzie nagrywane!

3) Jeśli szkolenie będzie dofinansowane ze środków publicznych w **co najmniej 70%**, to szkolenie będzie **zwolnione z podatku VAT** (podstawa prawna: par. 3 ust. 1 pkt 14 *Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień* (t.j. Dz. U. z 2023 r. poz. 955 z późn. zm.)).

Warunki techniczne

1. **Platforma komunikacyjna** — Google Meet

2. **Wymagania sprzętowe:** komputer stacjonarny/laptop, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/MacOS High Sierra, min. 2 GB pamięci RAM, pamięć dysku minimum 10GB,

3. **Sieć:** łącze internetowe minimum 50 kb/s,

4. **System operacyjny** minimum Windows XP/MacOS High Sierra, przeglądarka internetowa (marka nie ma znaczenia)

5. **Okres ważności linku:** od 1 h przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny po zakończeniu szkoleń w dniu ostatnim

Kontakt



Wojciech Graczyk

E-mail wojciech.graczyk@korycki-graczyk.pl

Telefon (+48) 698 291 420