



Cyfrowe Kompetencje w cyberbezpieczeństwie: ochrona danych, tożsamość cyfrowa i bezpieczna praca online: 24-09-2026

Numer usługi 2026/08/12/204299/3743081

299,00 PLN brutto

299,00 PLN netto

99,67 PLN brutto/h

99,67 PLN netto/h

261,33 PLN cena rynkowa ⓘ

LT MASTERY

SZKOLENIA DLA

BIZNESU PIOTR

SZYMCZYK

★★★★★ 4,8 / 5

37 ocen

🏠 Usługa szkoleniowa

📄 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 03:00 h

📅 24.09.2026 do 24.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, FELB.06.03-IZ.00-0003/24 ZIPH, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie skierowane jest do szerokiego grona odbiorców: osób dorosłych aktywnych zawodowo i uczących się, pracowników i właścicieli mikro, małych i średnich przedsiębiorstw, kadry administracyjnej i biurowej, pracowników działów sprzedaży i obsługi klienta, pracowników sektora publicznego oraz osób prywatnych chcących świadomie funkcjonować w środowisku cyfrowym. Szkolenie nie wymaga specjalistycznej wiedzy technicznej – wystarczy podstawowa obsługa komputera i dostęp do Internetu. Program jest zgodny z Europejską Ramą Kompetencji Cyfrowych DigComp 2.2 i obejmuje Obszar 4: Bezpieczeństwo, który ma charakter przekrojowy i dotyczy każdej osoby korzystającej z technologii cyfrowych w pracy lub życiu codziennym. Uczestników projektów dofinansowanych: kierunek rozwój, Bony Rozwojowe, MP Pociąg do Kariery, NSE i innych projektów EFS/FERS.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	23-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie oraz rozwinięcie kompetencji cyfrowych uczestników w obszarze bezpieczeństwa zgodnie z DigComp 2.2 (4.1–4.4). Uczestnik nauczy się chronić urządzenia i dane, świadomie zarządzać prywatnością, stosować zasady zdrowego i bezpiecznego korzystania z technologii oraz rozumieć wpływ cyfryzacji na środowisko i społeczeństwo. Szkolenie wzmacnia odpowiedzialne, krytyczne i bezpieczne postawy cyfrowe, dostosowane do aktualnych zagrożeń 2026 roku.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wiedza: Opisuje strukturę Obszaru 4 DigComp 2.2 (Bezpieczeństwo) oraz wyjaśnia różnicę między ochroną urządzeń, ochroną danych osobowych, dobrostanem cyfrowym a wpływem technologii na środowisko.	Uczestnik poprawnie przypisuje co najmniej 3 przykładowe działania do właściwych kompetencji (4.1–4.4) DigComp 2.2 w teście wielokrotnego wyboru.	Test teoretyczny z wynikiem generowanym automatycznie
Umiejętności: Dobiera i stosuje odpowiednie narzędzia i praktyki ochrony tożsamości cyfrowej, danych i urządzeń (hasła, 2FA, aktualizacje, kopie zapasowe, ustawienia prywatności).	Uczestnik na podstawie opisanych scenariuszy roboczych poprawnie wskazuje właściwe działanie ochronne (np. prawidłowe parametry hasła, włączenie 2FA, wykrycie phishingu)	Test teoretyczny z wynikiem generowanym automatycznie
Kompetencje społeczne: Prezentuje postawę świadomego i odpowiedzialnego użytkownika cyfrowego — rozumie konsekwencje własnych działań online dla bezpieczeństwa organizacji i osób trzecich.	Uczestnik poprawnie wybiera właściwą ścieżkę postępowania w opisanym scenariuszu incydentu cyfrowego (zgłoszenie, reakcja, minimalizacja skutków) zgodnie z zasadami cyberhigieny i ochrony danych.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażenie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

PROGRAM SZKOLENIA:

BLOK 1: Wprowadzenie do DigComp 2.2 i kompetencji cyfrowych (0:20 h)

- Czym są kompetencje cyfrowe wg Komisji Europejskiej – DigComp 2.2
- Pięć obszarów ramy: przegląd i wzajemne powiązania
- Dlaczego Obszar 4 (Bezpieczeństwo) ma charakter przekrojowy i dotyczy każdego
- Kontekst zawodowy: kompetencje cyfrowe jako wymóg rynku pracy 2026

BLOK 2: Kompetencja 4.1: Ochrona urządzeń i danych (DigComp 2.2) (0:30 h)

- Narzędzia ochrony: antywirusy, firewalle, menedżery haseł
- Zasady tworzenia silnych haseł i konfiguracji 2FA/MFA
- Kopie zapasowe (backup) – kiedy, gdzie i jak
- Aktualizacje systemu i oprogramowania jako fundament bezpieczeństwa
- Ćwiczenie: Ocena poziomu zabezpieczenia przykładowego stanowiska pracy

BLOK 3: Kompetencja 4.2: Ochrona danych osobowych i prywatności (DigComp 2.2) (0:30 h)

- Czym są dane osobowe w środowisku cyfrowym – RODO w praktyce użytkownika
- Ślad cyfrowy: co zostawiamy i jak to ograniczyć
- Ustawienia prywatności w systemach operacyjnych, przeglądarkach i aplikacjach
- Bezpieczna komunikacja e-mail i rozpoznawanie phishingu
- Ćwiczenie: „Prawdziwy czy fałszywy?” – analiza wiadomości e-mail i linków

BLOK 4: Kompetencja 4.3: Ochrona zdrowia i dobrostanu cyfrowego (DigComp 2.2) (0:25 h)

- Higiena cyfrowa: ergonomia pracy, przeciążenie informacyjne, uzależnienie od technologii
- Dezinformacja i fake news – jak weryfikować informacje online (fact-checking)
- Bezpieczeństwo psychiczne w środowisku cyfrowym: mowa nienawiści, cybermobbing
- Zasada minimalnego zaufania (zero trust) w codziennej pracy

BLOK 5: Kompetencja 4.4: Ochrona środowiska i świadomość wpływu technologii (DigComp 2.2) (0:25 h)

- Ślad węglowy technologii cyfrowych – co to oznacza w praktyce
- Racjonalne korzystanie z urządzeń i chmury jako działanie proekologiczne
- E-waste (odpady elektroniczne): odpowiedzialne zarządzanie sprzętem
- Zasady zrównoważonego korzystania z zasobów cyfrowych w organizacji

BLOK 6: Bezpieczeństwo cyfrowe w środowisku zawodowym: synteza (0:20 h)

- Cyberbezpieczeństwo jako element kompetencji cyfrowych pracownika

- 10 zasad bezpiecznego pracownika cyfrowego (synteza DigComp 4.1–4.4)

- Reagowanie na incydenty: krok po kroku, zgłaszanie zagrożeń

- Podsumowanie i odpowiedzi na pytania uczestników

BLOK 7: Walidacja (egzamin wewnętrzny) (0:30 h)

- Test teoretyczny online (Google Forms) – pytania zamknięte wielokrotnego wyboru

- Zakres: kompetencje 4.1–4.4 DigComp 2.2, scenariusze praktyczne, identyfikacja zagrożeń

- Wynik generowany automatycznie po zakończeniu testu

- Warunek zaliczenia: min. 70% poprawnych odpowiedzi

- Po zaliczeniu: certyfikat uczestnictwa z wyszczególnionymi efektami uczenia się (PDF, e-mail)

Łączny czas szkolenia: 3:15 h zegarowe (2:45 h zajęć + 0:15 h walidacji + 0:15 h przerw)

· Egzamin wewnętrzny / walidacja jest wliczona w czas trwania szkolenia.

KLUCZOWE ELEMENTY ZAPEWNIAJĄCE KWALIFIKOWALNOŚĆ JAKO „CYFROWE KOMPETENCJE”

Trzy rzeczy, które odróżniają tę kartę od zwykłego szkolenia z bezpieczeństwa:

1. Jawne osadzenie w DigComp 2.2 – tytuł, cel, efekty uczenia się i certyfikat wprost odwołują się do numerów kompetencji (4.1–4.4).

Operator widzi od razu, że to rama cyfrowa, nie szkolenie branżowe.

2. Kompetencja 4.4 (środowisko) – blok o śladzie węglowym technologii i e-waste łączy kompetencje cyfrowe z zieloną świadomością.

To dodatkowy atut przy weryfikacji przez operatorów promujących "cyfrowe i zielone".

3. Rozdzielność walidacji – walidacja w osobnym bloku czasowym, narzędziem niedostępnym w trakcie zajęć (Google Forms aktywowany po zakończeniu dydaktyki) – spełnia wymóg pytania 3 BUR wprost.

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Wprowadzenie do DigComp 2.2 – kompetencje cyfrowe i Obszar 4	Zajęcia	Piotr Szymczyk	24-09-2026	09:00	09:20	00:20
2 z 8 Kompetencja 4.1 – Ochrona urządzeń i danych + ćwiczenie	Zajęcia	Piotr Szymczyk	24-09-2026	09:20	09:50	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 8 Kompetencja 4.2 – Ochrona danych osobowych i prywatności + ćwiczenie phishing	Zajęcia	Piotr Szymczyk	24-09-2026	09:50	10:20	00:30
4 z 8 -	Przerwa	-	24-09-2026	10:20	10:35	00:15
5 z 8 Kompetencja 4.3 – Dobrostan cyfrowy i dezinformacja	Zajęcia	Piotr Szymczyk	24-09-2026	10:35	11:00	00:25
6 z 8 Kompetencja 4.4 – Wpływ technologii na środowisko i zrównoważone korzystanie	Zajęcia	Piotr Szymczyk	24-09-2026	11:00	11:20	00:20
7 z 8 Synteza – 10 zasad bezpiecznego pracownika cyfrowego + reagowanie na incydenty	Zajęcia	Piotr Szymczyk	24-09-2026	11:20	11:45	00:25
8 z 8 -	Walidacja	Piotr Szymczyk	24-09-2026	11:45	12:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	03:00
w tym suma godzin zajęć	02:30
w tym suma godzin walidacji	00:15
w tym suma przerw	00:15
Suma godzin dydaktycznych bez przerw	03:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	299,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
Koszt przypadający na 1 uczestnika netto	299,00 PLN
Koszt osobogodziny brutto	99,67 PLN
Koszt osobogodziny netto	99,67 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	03:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Piotr Szymczyk

Piotr Szymczyk to doświadczony menedżer techniczny oraz ekspert w obszarze cyberbezpieczeństwa i usług IT, z ponad 25-letnią praktyką zdobywaną w międzynarodowych korporacjach technologicznych. Specjalizuje się w nadzorze nad usługami bezpieczeństwa, procesami dostępowymi, cyklem wdrażania, prowadzeniem przeglądów operacyjnych i bezpieczeństwa integrując w/g UoKSC (NIS2), SZBI, ISO27k, CRA. Jako lider zespołów technicznych zarządzał wielokulturowymi grupami specjalistów IT, realizując projekty, inicjatywy podnoszące poziom bezpieczeństwa oraz działania zapewniające ciągłość operacyjną.

W globalnym centrum usług biznesowych odpowiadał za procesy IT, Cybersec, operacyjno-finansowe, kontrolę SLA/KPI oraz komunikację z klientami na poziomie międzynarodowym. Doświadczenie korporacyjne uzupełnia praktyka przedsiębiorcza zdobyta podczas prowadzenia własnej działalności w USA, gdzie zarządzał pełnym zakresem operacji, finansów i relacji biznesowych.

Piotr posiada doświadczenie oraz liczne szkolenia/certyfikaty międzynarodowe nie starsze niż 5 lat z zakresu IT: EITCA/IS Academy of Information Security, EITCA/KC Academy of Key IT Competencies. Z obszaru usług projektowych: Agile PM Practitioner, Change Management, AI w

Projektach oraz Security: Audytor ISO 27k, CompTIA Security+. Obecnie wykorzystuje swoje doświadczenie jako trener, prowadząc szkolenia z cyberbezpieczeństwa, higieny cyfrowej, odporności organizacyjnej oraz konsultant w zakresie NIS2 / UoKSC / SZBI / CRA / usług IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują drogą e-mailową: konspekt wiedzy z odniesieniami do kompetencji DigComp 2.2 (4.1–4.4) w formacie PDF, checklistę „10 zasad bezpiecznego pracownika cyfrowego”, szablony do ćwiczeń oraz certyfikat uczestnictwa z wyszczególnionymi efektami uczenia się i przypisaniem do kompetencji DigComp 2.2.

Warunki uczestnictwa

Udział w szkoleniu jest możliwy po spełnieniu następujących warunków:

- Konieczna jest rejestracja oraz utworzenie profilu użytkownika w Bazie Usług Rozwojowych (BUR).
- Zgłoszenie chęci udziału musi nastąpić poprzez system BUR.
- Uczestnik musi spełnić wszystkie kryteria formalne ustalone przez instytucję przyznającą dofinansowanie (Operatora).

Ważna informacja:

Zalecamy kontakt z nami w celu weryfikacji dostępności miejsc oraz potwierdzenia daty szkolenia, zanim podpiszą Państwo umowę o dofinansowanie z Operatorem. Informujemy również, że podmiot realizujący usługę musi być przygotowany na audyt lub wizytację (online lub stacjonarną) ze strony Polskiej Agencji Rozwoju Przedsiębiorczości (PARP), Operatora lub uprawnionej jednostki kontrolnej.

Informacje dodatkowe

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

W przypadku korzystania z dofinansowania do szkolenia obowiązuje wymóg uczestnictwa w co najmniej 80% zajęć. Weryfikacja frekwencji na podstawie: raportu logowań lub listy obecności lub zrzutu ekranu wykonanego na początku i końcu szkolenia.

Całe szkolenie jest rejestrowane w celach kontroli oraz audytu.

Wykorzystanie nagrania w innym celu niż kontrola czy audyt wymaga zgody trenera oraz uczestników.

Uczestnicy otrzymają zaświadczenie / certyfikat, potwierdzające ukończenie szkolenia.

Usługa zdalna w czasie rzeczywistym - prowadzona na żywo.

Warunki techniczne

Poniżej opisane są minimalne wymagania techniczne dotyczące uczestnictwa w szkoleniu przy pomocy platformy TEAMS:

1. Parametry urządzenia: komputer / laptop / tablet

- Procesor dwurdzeniowy 1–2 GHz minimalnie; zalecany dual-core 2 GHz lub lepszy (Intel i3/i5 lub równoważny)
- 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 10/11, macOS 10.13+ (lub nowsze), Linux (nowsze dystrybucje wspierane), iOS 13+/Android 8+
 - • • • zainstalowany TEAMS (najświeższa wersja) oraz najnowsza wersja Chrome/Edge/Firefox;

1. Kamera i mikrofon

- TEAMS współpracuje z wbudowanymi kamerami w laptopach oraz większością kamer internetowych.
 - słuchawki z mikrofonem zalecane dla lepszej jakości dźwięku.
 - zaawansowane lub profesjonalne kamery/mikrofony, mogą wymagać zainstalowanie dodatkowego oprogramowania .

1. Urządzenia mobilne

- Jeżeli łączysz się z urządzenia mobilnego, pobierz i zainstaluj aplikację TEAMS z App Store (Apple) lub Google Play
- Aby korzystać z dźwięku i obrazu, użyj zestawu słuchawkowego z mikrofonem lub głośników podłączonych do urządzenia.
- Przed rozpoczęciem szkolenia sprawdź, czy urządzenie rozpoznaje wybrane urządzenie audio oraz czy nie jest ono jednocześnie zajęte przez inną aplikację
- Upewnij się, że aplikacja ma przyznane uprawnienia do korzystania z mikrofonu i kamery.

1. Wymagania dla łącza internetowego:

- *min. 1,5 Mbps download i upload* dla podstawowego udziału
- zalecane 3 Mbps+ dla stabilnego wideo HD i udostępniania ekranu
- najnowsza wersja używanej przeglądarki internetowej

1. Link do szkolenia oraz warunki / wymagania dodatkowe:

- • • • • Link do szkolenia zostanie dostany drogą elektroniczną przed rozpoczęciem usługi na adres email podany przez uczestnika szkolenia.
- Link do szkolenia będzie ważny w dniach i godzinach określonych w harmonogramie usługi.

1. Podczas szkolenia online zapewniamy:

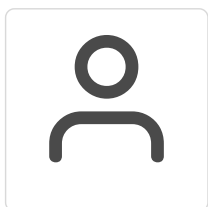
- • Wygodną formę szkolenia, gdzie wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki.
- Szkolenie zdalne w czasie rzeczywistym w wirtualnym pokoju konferencyjnym, w niewielkiej grupie uczestników.
- Możliwość pełnej interakcji z trenerem, który prowadzi zajęcia "na żywo" z włączoną kamerą w czasie trwania całego szkolenia.
- Możliwości zadawania pytań, omawiania indywidualnych zagadnień oraz aktywny udział w ćwiczeniach.

Przed szkoleniem:

- Upewnij się, że masz stabilne połączenie internetowe, które spełnia minimalne wymagane prędkości dla transmisji audio oraz wideo.
- Przetestuj dostęp i uruchomienie aplikacji TEAMS w wykorzystaniem kamery oraz mikrofonu.
- Rekomenduje się przygotowanie zapasowego zestawu awaryjnego sprzętu w celu zapewnienia ciągłości realizacji szkolenia. Powinien on obejmować kluczowe komponenty: komputer, kamerę, mikrofon/głośnik, klawiaturę, myszkę oraz alternatywne źródło dostępu do Internetu (np. modem Hot-Spot).

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Kontakt



Piotr Szymczyk

E-mail piotr.szymczyk@legacyturn.com

Telefon (+48) 600 390 516