



Nr sprawy O.253.58.2025

Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA dla strony projektu „1101 Kompetencji Cyfrowych”

1. Przedmiot zamówienia:

Przedmiotem zamówienia jest **usługa zaprojektowania, wykonania, wdrożenia oraz utrzymania strony internetowej na infrastrukturze Zamawiającego na potrzeby projektu pn. „Tysiąc sto jeden kompetencji cyfrowych” realizowanego w ramach Priorytetu 01 Gospodarka, Działanie 01.06 E-usługi publiczne (schemat B), programu regionalnego Fundusze Europejskie dla Warmii i Mazur 2021-2027 (FEWM.01.06-IZ.00-0001/24).**

2. Cel strony internetowej:

Celem strony jest dostarczenie szczegółowych informacji o projekcie, umożliwienie użytkownikom rejestracji na szkolenia oraz zapewnienie dostępu do niezbędnej dokumentacji, statystyk i harmonogramów dla administratora strony. Jako administratora rozumie się pracownika Zamawiającego, który po odbiorze strony będzie mógł edytować treści i zarządzać danymi osób zgłoszonych na szkolenia.

3. Zakres usług:

Wykonawca będzie odpowiedzialny za:

a) Projektowanie graficzne strony

- Opracowanie estetycznego i funkcjonalnego designu inspirowanego makietą (Załącznik nr 2 do Umowy) zachowując zasady dostępności cyfrowej.
- Uwzględnienie identyfikacji wizualnej projektu, w tym dostarczonej przez zamawiającego kolorystyki, typografii oraz rozmieszczenia elementów interaktywnych.

b) Wykonanie oraz wdrożenie strony internetowej w oparciu o system zarządzania treścią (CMS)

- Zastosowanie nowoczesnych technologii, takich jak HTML5, CSS3, JavaScript oraz frameworków zapewniających responsywność, interaktywność i optymalizację wydajności. Dotyczy wersji na komputer oraz urządzenia mobilne.
- Optymalizacja kodu, minimalizacja plików CSS/JS, mechanizmy cache'owania i poprawne kompresowanie grafik.
- Zapewnienie kompatybilności z aktualnymi wersjami przeglądarek, tj. Chrome, Firefox, Edge, Opera oraz mechanizmu informującego użytkowników starszych przeglądarek o wymaganych wersjach.
- Implementacja intuicyjnego CMS, umożliwiającego łatwe dodawanie, edycję i usuwanie treści przez administratorów bez potrzeby znajomości programowania.
- Funkcje edycji zdjęć, takie jak dodawanie, przycinanie, zmiana rozmiaru z zachowaniem oryginału.
- Możliwość tworzenia i zarządzania słownikami oraz kategoriami treści.
- Zarządzanie użytkownikami (dodawanie administratorów, redaktorów treści, obsługa zgłoszeń)

c) Dodanie treści na stronie

- Implementacja treści dostarczonych przez Zamawiającego drogą elektroniczną. Treści zostaną dostarczone drogą elektroniczną i liczą około 40 stron A4.
- W przypadku braku pełnych materiałów, zastosowanie tymczasowych treści lub słowników (np. lista szkoleń, terminy), które Zamawiający będzie mógł łatwo edytować z poziomu panelu administratora.
- Wdrożenie mechanizmu, że dodawane treści nie zmieniają układu strony i są zgodne z jej designem.

d) Integracja z formularzem zgłoszeniowym (ZAPISZ SIĘ)

- Stworzenie formularza rejestracyjnego dla uczestników szkoleń z możliwością:
- Wprowadzania i edycji danych przed finalnym przesłaniem.
- Podglądu zgłoszenia przed zatwierdzeniem.
- Wycofania zgłoszenia przed jego przesłaniem.
- Obsługi zgód na przetwarzanie danych osobowych zgodnie z RODO.
- Druku oraz wysyłki potwierdzenia na e-mail dla uczestnika oraz administratora. (Konto pocztowe z którego wysyłane jest potwierdzenie dostarcza Zamawiający)
- Walidacji danych (PESEL, NIP, e-mail, numer telefonu).
- Automatyczne generowanie dokumentów na podstawie danych z formularza, takich jak:
 - Umowa o uczestnictwo w projekcie.
 - Zaświadczenie pracodawcy.
 - Oświadczenia zgodnie z regulaminem projektu.

Powyższe dokumenty zostaną dostarczone przez zamawiającego a Wykonawca zaimplementuje mechanizm automatycznego wstawiania danych z formularza do tych dokumentów (Załącznik nr 1 – formularz zgłoszeniowy).

e) Zapewnienie bezpieczeństwa strony

- Wykonawca przekazując Stronę potwierdzi pisemnie, że Strona stworzona jest zgodnie z najnowszym standardem ASVS (Application Security Verification Project) poziom L2 autorstwa Fundacji OWASP (Open Web Application Security Project) oraz, że strona odporna jest na popularne ataki z listy OWASP top 10.
- Wykonawca przeprowadzi testy sprawdzające bezpieczeństwo Strony pod kątem zgodności z najnowszym standardem ASVS poziom L2 Strony i przedstawi raport z testów oraz wprowadzi naprawy błędów, jeżeli zostaną one zidentyfikowane.
- Raport z testów Strony musi składać się, co najmniej z następujących elementów:
 - harmonogram przeprowadzonych testów,
 - informacje o przebiegu poszczególnych testów,
 - podsumowanie ilościowe i jakościowe wykrytych błędów
- Strona musi zapewniać silne uwierzytelnienie i autoryzację do zasobów. Kontrola dostępu musi być oparta na rolach
- Strona musi zapewniać szyfrowaną transmisję z wykorzystaniem silnych algorytmów kryptograficznych, tj. TLS 1.2+,
- Ochrona danych na poziomie sesji (np. sesyjne pliki cookie powinny być przesyłane wyłącznie za pomocą HTTPS),
 - Strona powinna wykazywać ochronę przed atakami typu XSS (Cross Site Scripting), SQL Injection, CSRF (Cross-Site Request Forgery), zafiksowanie sesji (Session Fixation),
 - Powinny być skonfigurowane nagłówki bezpieczeństwa HTTP, w szczególności (X Frame Options, X XXS Protection, X Content Type Options, X Permitted Cross Domain Policies, Strict Transport Security, Content Security Policy, Rererrer Policy) w zakresie oczekiwanej funkcjonalności,
- Wrażliwe dane strony (np. token) nie powinny być przekazywane w adresie URL strony,
- Jeśli strona będzie umożliwiała zdalne przesyłanie plików przez użytkowników, pliki takie powinny być sprawdzane przez system antywirusowy zanim zostaną umieszczone na zdalnym serwerze. Wrzucane pliki powinny być również sprawdzane pod kątem typu pliku oraz wyizolowane poza główny katalog aplikacji,
- Strona musi walidować dane znajdujące się bezpośrednio w przesyłanych przez użytkowników plikach, np. komórki arkusza Excel
- Strona musi rejestrować całą aktywność użytkownika na poziomie serwera www jak i strony www (systemu CMS),

- Strona musi poprawnie obsługiwać błędy,
- Wszystkie zależne komponenty niezbędne do działania strony (np. system operacyjny, serwer www, biblioteki itp.) powinny być skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa oraz uszczelnione w zakresie konfiguracji,
- Wszystkie dodatkowe komponenty użyte na stronie nie będące utworem dostawcy (np. biblioteki open source, wtyczki, pluginy) powinny być sprawdzone pod kątem bezpieczeństwa, w zakresie potencjalnej eksfiltracji danych,
- Strona musi zapewniać dokładną walidację danych pobieranych z formularzy, danych URL oraz być odporna między innymi na ataki semantyczne na adres URL, ataki związane z ładowaniem plików, ataki spamowe, podrabianie zatwierdzenia formularza, sfałszowanie żądania HTTP, ujawnienie uwierzytelnień dostępu, kradzież cookies, przechwytywanie sesji, trawersowanie katalogów, wstrzykiwanie poleceń systemowych, ujawnianie kodu źródłowego, np. plików .inc, „template” itp.
- Formularze, dla osób nieautoryzowanych, powodujące zapis do bazy danych po stronie publicznej Strony muszą posiadać zabezpieczenie typu tzw. „captcha”, odporne na ataki automatyczne a ukierunkowane na interakcję użytkownika,
- Strona musi być uszczelniona w zakresie robotów indeksujących (web crawlers) i ograniczać zbierane informacje o strukturach strony, które nie zawierają informacji biznesowych adresowanych publicznie.

f) Utrzymanie i wsparcie techniczne

- Utrzymanie strony na infrastrukturze Zamawiającego do 31.12.2027.
- Zapewnienie minimum 150 godzin serwisowych w wyżej wymienionym terminie na modyfikacje i aktualizacje, w tym:
 - Naprawy zgłoszonych błędów funkcjonalnych w terminie nie dłuższym niż 2 dni po zgłoszeniu drogą mailową lub telefoniczną.
 - Dostosowanie systemu CMS do nowych potrzeb Zamawiającego.
 - Wdrożenie niezbędnych poprawek w zakresie wydajności i dostępności.
- Szkolenie administratorów w zakresie obsługi CMS i zarządzania treścią (minimum 4 godziny, online lub w siedzibie Zamawiającego).
- Wykonawca w okresie gwarancji dba o poziom bezpieczeństwa strony (aktualizacje/ dostarczanie komponentów). Strona musi być zgodna z najnowszym standardem ASVS poziom L2 autorstwa Fundacji OWASP oraz musi być oporna na popularne ataki z listy OWASP top 10. Raz na pół roku Wykonawca dostarczy raport potwierdzający odporność strony na w.w ataki.

g) Wydajność i skalowalność

Strona powinna obsługiwać co najmniej 300 użytkowników jednocześnie bez zauważalnych spadków wydajności.

Wykonawca zobowiązany jest do przeprowadzenia testów obciążeniowych i dostarczenia raportów potwierdzających osiągnięcie wymaganej wydajności określonej w punkcie 6.2. Wykonawca zoptymalizuje stronę i wszelkie parametry pod infrastrukturę zamawiającego podaną w punkcie 5.1.

h) Backup i ochrona danych

Automatyczne backupy bazy danych i zgłoszeń użytkowników co najmniej raz dziennie. Administrator strony ma mieć możliwość przywrócenia zgłoszeń z poprzedniego dnia z poziomu panelu administratora. Możliwość przywracania danych w przypadku awarii lub błędu użytkownika.

i) Dokumentacja i instrukcje

Dostarczenie instrukcji dotyczącej:

- Dodawania treści.
- Zarządzania słownikami i kategoriami.
- Obsługi panelu administratora.

j) Zgodność z WCAG 2.1 na poziomie AA i ustawą o dostępności cyfrowej

Strona musi spełniać standardy dostępności cyfrowej WCAG 2.1 na poziomie AA, zgodnie z Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Wykonawca zobowiązany jest do przeprowadzenia audytu dostępności przez dedykowany zewnętrzny podmiot oraz dostarczenia raportu potwierdzającego zgodność.

k) Zgodność z Krajowymi Ramami Interoperacyjności i przepisami prawa

Strona musi być zgodna z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

l) Spełnienie Pryncypiów Architektury Informacyjnej Państwa

Strona musi spełniać zasady neutralności technologicznej, przejrzystości, bezpieczeństwa, ochrony informacji i dostępności, określone w Pryncypiach Architektury Informacyjnej Państwa.

4. Wymagania dotyczące strony internetowej – Opis i Struktura

Cała strona główna ma mieć dynamiczną i edytowalną strukturę, co pozwala administratorowi na łatwą aktualizację treści bez konieczności ingerencji w kod strony. W przypadku braku dostarczonych treści, Wykonawca ma obowiązek stworzenia tymczasowych bloków treści i słowników, które mogą być edytowane przez Zamawiającego.

a) Strona Główna –Struktura nawigacji i menu

Menu poziome/rozwijane (sticky menu) – stałe menu nawigacyjne, widoczne podczas przewijania strony, zapewniające szybki dostęp do kluczowych sekcji.

Jednolita struktura na każdej podstronie – menu pozostaje spójne we wszystkich sekcjach serwisu, co zapewnia intuicyjność korzystania.

Interaktywne rozwijane podmenu – po najechaniu myszką na wybraną pozycję rozwija się lista podstron, które prowadzą do określonych sekcji strony głównej lub dedykowanych podstron.

Hierarchia menu:

O Projekcie

Szkolenia

Wsparcie w rekrutacji

Kontakt

ZAPISZ SIĘ (3.d)

b) Sekcja „O Projekcie”

Zawiera kompleksowe informacje na temat projektu, w tym:

Cel projektu – krótki opis misji i założeń programu.

Dla kogo? – określenie grupy docelowej uczestników.

Korzyści z udziału – lista najważniejszych profitów wynikających z uczestnictwa.

Opis projektu – szczegółowy podział na moduły i szkolenia.

Rezultaty projektu – przewidywane wyniki, wskaźniki i efekty programu.

Informacja o finansowaniu – koszty ogółem projektu, koszty kwalifikowalne oraz wartość dofinansowania.

Regulamin uczestnictwa w projekcie – zasady, wymagania formalne, wzory umów.

Aktualności – dynamicznie aktualizowany blok informacyjny o bieżących wydarzeniach.

Archiwum lat poprzednich – „I rok projektu”, „II rok projektu”, „III rok projektu” – podsumowania działań z każdego roku realizacji.

c) Sekcja „Szkolenia”

Podział na ścieżki szkoleniowe – każda z nich zawiera listę dostępnych kursów.
Każde szkolenie prowadzi do dedykowanej podstrony, gdzie znajdują się szczegóły kursu.

d) Sekcja „Wsparcie w rekrutacji”

Jak wziąć udział w projekcie? – instrukcja w formie tekstowej lub infografiki.
Terminy zgłoszeń – harmonogram rekrutacji.
Rekrutacja – zasady procesu kwalifikacji i dostępne miejsca./Szybki przewodnik po projekcie
Mentorzy projektu – przedstawienie zespołu wspierającego uczestników.
Q&A – sekcja pytań i odpowiedzi dla uczestników.

e) Sekcja „Kontakt”

Biuro projektu – dane kontaktowe, adres biura i godziny funkcjonowania, zdjęcia pracowników

f) ZAPISZ SIĘ (3.d)

Wszystkie treści do w/w sekcji dostarczy zamawiający zgodnie z punktem 3.c OPZ.

g) Inne elementy strony głównej

Logotypy UE i instytucji partnerskich – wymagane oznaczenia zgodnie z wytycznymi projektu makiety.
Wstępne informacje o projekcie – kluczowe informacje w formie dynamicznego banneru lub grafiki w sekcji głównej.
Przesuwana lista aktualnych szkoleń (slider/karuzela) – dynamiczne kafle szkoleń, prowadzące do dedykowanych podstron.
Przyciski CTA (Call To Action) – np. „Zapisz się”, „Dowiedz się więcej”, „Kontakt” – umieszczone w strategicznych miejscach dla łatwego dostępu do kluczowych funkcji strony.

5. Zamawiający zapewnia w ramach swojej infrastruktury

Zamawiający zapewnia następujące środowisko i zasoby teleinformatyczne, niezbędne do wdrożenia i utrzymania strony internetowej:

5.1. Środowisko hostingowe i serwerowe

Środowisko serwerowe oparte na:

Apache 2.4 lub nowszym,

PHP 8 lub nowszym,

Silniku bazodanowym MySQL 8 (MariaDB 10) lub PostgreSQL 12.

Przestrzeń dyskowa o pojemności min. 20 GB.

4 vCPU, 8GB RAM (Wirtualna maszyna)

5.2. Dostęp i zabezpieczenia

Dostęp do serwera zostanie zapewniony Wykonawcy po jego oficjalnym wniosku i zaakceptowaniu przez Zamawiającego.

Dostęp do infrastruktury teleinformatycznej Województwa Warmińsko-Mazurskiego możliwy będzie jedynie poprzez **usługę szyfrującą VPN.**

Dane dostępne (login, hasło, certyfikaty VPN) zostaną dostarczone Wykonawcy **po podpisaniu umowy** oraz po dostarczeniu przez niego wypełnionego dokumentu **Polityki Bezpieczeństwa Teleinformatycznego** obowiązującej u Zamawiającego.

Dostęp do serwera oraz usługi VPN będzie **każdorazowo otwierany w ramach tzw. „okienka serwisowego”** na wniosek Wykonawcy.

Wniosek powinien zawierać:

przewidywalny **zakres realizowanych prac, czas trwania** dostępu, powinien być wysłany co najmniej **1 dzień**

roboczy przed wskazanym terminem.

Wniosek należy kierować na adres e-mail: projekty@wmcnt.pl

5.3. Środowisko testowe i warunki odbioru

Strona testowa i odbiór:

Wykonawca zobowiązany jest do **przygotowania środowiska testowego** poza serwerami Zamawiającego, na którym będzie **weryfikowana funkcjonalność i kompletność rozwiązania**.

Po **zatwierdzeniu przez Zamawiającego**, strona zostanie zaimplementowana na serwer produkcyjny Zamawiającego i tam Zamawiający **dokona procedury odbioru**. Na czas odbioru stronie nie może być dostępna publicznie. Wykonawca zabezpieczy dostęp do niej hasłem.

Wszelkie częściowe wdrożenia na serwer produkcyjny bez pełnej akceptacji Zamawiającego są zabronione.

6. Wymagania dotyczące zgodności i wydajności

W celu zapewnienia wysokiej jakości oraz zgodności strony internetowej z przyjętymi standardami, Wykonawca zobowiązuje się do dostarczenia **kompletnych raportów i audytów**, które potwierdzą spełnienie wymagań z OPZ.

6.1. Raporty i audyty techniczne

Wszystkie raporty muszą zawierać:

Interpretację wyników oraz rekomendacje, użyte parametry i metodykę testów, nazwę narzędzia testowego oraz wyniki przeprowadzonych testów.

Raporty muszą być dostarczone w wersji elektronicznej (pdf/word) wraz z plikami źródłowymi na podstawie, których raporty zostały wygenerowane.

Rekomendowane narzędzia do przeprowadzania testów, na których zamawiający będzie dokonywał weryfikacji raportów:

Dostępność i zgodność z WCAG 2.1 AA → Wave (<https://wave.webaim.org>), axe DevTools, Pa11y, Lighthouse

Optymalizacja kodu i szybkości działania → Google PageSpeed Insights, GTmetrix, Lighthouse

Bezpieczeństwo:

- Przykładowe narzędzia do przeprowadzania testów: Burp Suite, ZAP, Wapiti, Nikto, w3af, snyk, OpenVAS, Nessus i inne znane narzędzia wykorzystywane w testach bezpieczeństwa na każdym etapie powstawania Strony.

- Wykonawca przekazując Stronę potwierdzi pisemnie, że Strona stworzona jest zgodnie z najnowszym standardem ASVS poziom L2 autorstwa Fundacji OWASP oraz, że strona odporna jest na popularne ataki z listy OWASP top 10.

- Wykonawca przeprowadzi testy sprawdzające bezpieczeństwo Strony pod kątem zgodności z najnowszym standardem ASVS poziom L2 Strony i przedstawi raport z testów oraz wprowadzi naprawy błędów, jeżeli zostaną one zidentyfikowane.

a. Raport z testów Strony musi składać się, co najmniej z następujących elementów:

- harmonogram przeprowadzonych testów,
- informacje o przebiegu poszczególnych testów,
- podsumowanie ilościowe i jakościowe wykrytych błędów

Zgodność z W3C → W3C Validator (<https://validator.w3.org>)

6.2. Minimalne wymagania wydajnościowe

Strona internetowa musi spełniać **następujące minimalne wartości optymalizacyjne**, mierzone w Google PageSpeed Insights (lub innym uznanym narzędziu audytowym):

Metryka	Wartość minimalna
Wydajność (Performance Score)	min. 90/100

Metryka	Wartość minimalna
Dostępność (Accessibility)	min. 95/100
SEO	min. 90/100
Zgodność z WCAG 2.1 AA	min. AA
Czas ładowania strony (FCP - First Contentful Paint)	max. 1,8 sekundy
Opóźnienie wejściowe (TBT - Total Blocking Time)	max. 200 ms
Zmiana układu (CLS - Cumulative Layout Shift)	max. 0.1

6.3. Wymagania dotyczące optymalizacji kodu

Kod strony musi spełniać standardy W3C (brak krytycznych błędów w walidatorze W3C).

Optymalizacja plików CSS i JavaScript:

Usunięcie zbędnych zależności,
 Minifikacja i łączenie plików,
 Lazy-loading dla obrazów i zasobów.

Mechanizmy cache'owania:

Statyczne zasoby (np. CSS, JS) muszą mieć ustawiony cache-control na min. **7 dni**.

Obrazy:

Format **WebP** dla grafik rastrowych,
 SVG dla ikon i wektorowych elementów,

Maksymalny rozmiar jednego obrazu: 250 KB (bez utraty jakości).

6.4. Testy bezpieczeństwa

Strona musi przejść testy pod kątem:

OWASP TOP 10.

Minimalne zabezpieczenia strony:

- Strona musi zapewniać szyfrowaną transmisję z wykorzystaniem silnych algorytmów kryptograficznych, tj. TLS 1.2+,
- Ochrona danych na poziomie sesji (np. sesyjne pliki cookie powinny być przesyłane wyłącznie za pomocą HTTPS),
- Strona powinna wykazywać ochronę przed atakami typu XSS (Cross Site Scripting), SQL Injection, CSRF (Cross-Site Request Forgery), zafiksowanie sesji (Session Fixation),
- Muszą być skonfigurowane nagłówki bezpieczeństwa HTTP, w szczególności (X Frame Options, X XXS Protection, X Content Type Options, X Permitted Cross Domain Policies, Strict Transport Security, Content Security Policy, Rererrer Policy) w zakresie oczekiwanej funkcjonalności,
- Wrażliwe dane strony (np. token) nie powinny być przekazywane w adresie URL strony,
- Jeśli strona będzie umożliwiała zdalne przesyłanie plików przez użytkowników, pliki takie powinny być sprawdzane przez system antywirusowy zanim zostaną umieszczone na zdalnym serwerze. Wrzucane pliki powinny być również sprawdzane pod kątem typu pliku oraz wyizolowane poza główny katalog aplikacji,
- Strona musi walidować dane znajdujące się bezpośrednio w przesyłanych przez użytkowników plikach, np. komórki arkusza Excel
- Strona musi rejestrować całą aktywność użytkownika na poziomie serwera www jak i strony www (systemu CMS),
- Strona musi poprawnie obsługiwać błędy,
- Wszystkie zależne komponenty niezbędne do działania strony (np. system operacyjny, serwer www, biblioteki itp.) powinny być skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa oraz uszczelnione w zakresie konfiguracji,
- Wszystkie dodatkowe komponenty użyte na stronie nie będące utworem dostawcy (np. biblioteki open source, wtyczki, pluginy) muszą być sprawdzone pod kątem bezpieczeństwa, w zakresie

- potencjalnej eksfiltracji danych,
- Strona musi zapewniać dokładną walidację danych pobieranych z formularzy, danych URL oraz być odporna między innymi na ataki semantyczne na adres URL, ataki związane z ładowaniem plików, ataki spamowe, podrabianie zatwierdzenia formularza, sfałszowanie żądania HTTP, ujawnienie uwierzytelnień dostępu, kradzież cookies, przechwytywanie sesji, trawersowanie katalogów, wstrzykiwanie poleceń systemowych, ujawnianie kodu źródłowego, np. plików .inc, „template” itp.
- Formularze, dla osób nieautoryzowanych, powodujące zapis do bazy danych po stronie publicznej Strony muszą posiadać zabezpieczenie typu tzw. „captcha”, odporne na ataki automatyczne a ukierunkowane na interakcję użytkownika,
- Strona musi być uszczelniona w zakresie robotów indeksujących (web crawlers) i ograniczać zbierane informacje o strukturach strony, które nie zawierają informacji biznesowych adresowanych publicznie

Dodatkowe postanowienia

1. Zamawiający przeprowadzi kontrolę zgodności z wymaganiami OPZ przed ostatecznym odbiorem zgodnie z plikiem weryfikacyjnym, który stanowi podstawę do rozliczenia się i odbioru przedmiotu zamówienia od wykonawcy. Kontrola zgodności odbędzie się na Arkuszu odbioru stanowiącym Załącznik nr 3 do Umowy.
2. **Proponowane etapy projektowania, wdrożenia, wsparcia i utrzymania strony:**
 - 1) Etap 0: Ustalenie harmonogramu na wszystkie etapy jednak Etapy I – IV nie powinny trwać łącznie dłużej niż 35 dni.
 - 2) Etap I: Ustalenie i zatwierdzenie finalnej makiety graficznej.
 - 3) Etap II: Implementacja struktury, szablonów i funkcjonalności strony bez finalnych treści
 - 4) Etap III: Dodanie finalnych treści dostarczonych przez Zamawiającego i testy (wersja beta).
 - 5) Etap IV: Uruchomienie strony na serwerze produkcyjnym, finalne testy i odbiór (wersja 1.0).
 - 6) Etap V: Wsparcie techniczne, gwarancja, rozwój w okresie utrzymania.
3. **Wzór formularza zgłoszeniowego:**

**Formularz zgłoszeniowy
do Projektu „Tysiąc sto jeden kompetencji cyfrowych”
WYMAGANIA DLA STRONY**

Warunkiem ubiegania się o miejsce w Projekcie „Tysiąc sto jeden kompetencji cyfrowych” jest uzupełnienie wszystkich pól arkusza formularza zgłoszeniowego, zaznaczenie wszystkich oświadczeń, a także złożenie czytelnych podpisów pod klauzulą informacyjną RODO i oświadczeniami.

A. DANE OSOBOWE

IMIĘ (IMIONA) I NAZWISKO	<i>Osoba Kandydująca wpisuje dane</i>
PESEL LUB INNY IDENTYFIKATOR	<i>Lista wyboru:</i> <ul style="list-style-type: none"> • TAK – Osoba Kandydująca wpisuje dane • NIE – inny identyfikator – Osoba Kandydująca wpisuje dane – typ identyfikatora i numer
SERIA I NUMER DOKUMENTU TOŻSAMOŚCI	<i>Lista wyboru:</i> <ul style="list-style-type: none"> • Dowód osobisty – Osoba Kandydująca wpisuje serię i numer Paszport – Osoba Kandydująca wpisuje numer
ZATRUDNIENIE	<i>Lista wyboru:</i>

	<ul style="list-style-type: none"> • Osoba zatrudniona na umowę o pracę w jednostce samorządu terytorialnego <i>Wyjaśnienie: osoba zatrudniona na umowę o pracę na okres co najmniej pół roku od dnia zakończenia szkolenia w urzędzie gminy lub powiatu, lub urzędzie marszałkowskim</i> • Osoba zatrudniona na umowę o pracę w jednostce organizacyjnej jednostki samorządu terytorialnego • <i>Wyjaśnienie: osoba zatrudniona na umowę o pracę na okres co najmniej pół roku od dnia zakończenia szkolenia w jednostce administracji publicznej utworzonej przez samorząd gminny lub powiatowy, lub wojewódzki</i>
DANE TELEADRESOWE	
KRAJ	<i>Osoba Kandydująca wpisuje dane</i>
WOJEWÓDZTWO	<i>Osoba Kandydująca wpisuje dane</i>
POWIAT	<i>Osoba Kandydująca wpisuje dane</i>
GMINA	<i>Osoba Kandydująca wpisuje dane</i>
MIJSCOWOŚĆ	<i>Osoba Kandydująca wpisuje dane</i>
KOD POCZTOWY	<i>Osoba Kandydująca wpisuje dane</i>
ULICA	<i>Osoba Kandydująca wpisuje dane</i>
NUMER BUDYNKU	<i>Osoba Kandydująca wpisuje dane</i>
NUMER LOKALU	<i>Osoba Kandydująca wpisuje dane</i>
NUMER TELEFONU	<i>Osoba Kandydująca wpisuje dane</i>
ADRES E-MAIL	<i>Osoba Kandydująca wpisuje dane – na ten mail zostaną wysłane wygenerowane dokumenty: formularz zgłoszeniowy, umowa uczestnictwa w projekcie, zaświadczenie pracodawcy</i>

B. WYBÓR SZKOLENIA

MODUŁ	<i>Lista wyboru – na podstawie danych wskazanych w aktualnym harmonogramie szkoleń opublikowanym na Stronie Projektu</i>
TEMAT SZKOLENIA	<i>Lista wyboru – na podstawie danych wskazanych w aktualnym harmonogramie szkoleń opublikowanym na Stronie Projektu</i>
TERMIN SZKOLENIA	<i>Lista wyboru – na podstawie danych wskazanych w aktualnym harmonogramie szkoleń opublikowanym na Stronie Projektu</i>
KORZYSTANIE Z NOCLEGU (pokój dwuosobowy – możliwość noclegu dotyczy wyłącznie szkoleń stacjonarnych z wyłączeniem osób, które mieszkają w miejscu realizacji szkolenia)	<p><i>Lista wyboru:</i></p> <ul style="list-style-type: none"> • Tak – przy wyborze odpowiedzi pojawia się lista dwóch możliwości: - Mam współlokatora – Osoba Kandydująca wpisuje dane - Nie mam współlokatora – losowy przydział • Nie
SPECJALNE POTRZEBY	
ŻYWIENIOWE (jeżeli Tak, to należy wymienić szczególne potrzeby – dotyczy	<p><i>Lista wyboru:</i></p> <ul style="list-style-type: none"> • Tak – przy uzupełnieniu odpowiedzi tak, powinno pojawić się pole do wskazania potrzeb, w tym

wyłącznie szkoleń stacjonarnych)	<p><i>przypadku Osoba Kandydująca wpisuje dane</i></p> <ul style="list-style-type: none"> • Nie
INNE (jeżeli Tak, to należy wymienić szczególne potrzeby)	<p><i>Lista wyboru:</i></p> <ul style="list-style-type: none"> • Tak – przy uzupełnieniu odpowiedzi tak, powinno pojawić się pole do wskazania potrzeb, w tym przypadku Osoba Kandydująca wpisuje dane • Nie

C. KLAUZULA INFORMACYJNA DLA OSOBY, KTÓREJ DANE SĄ PRZETWARZANE W RAMACH REALIZACJI PROJEKTU

W związku z Państwa udziałem w realizacji Projektu pt. „Tysiąc sto jeden kompetencji cyfrowych”(nr FEWM.01.06-IZ.00-0001/24) w ramach programu regionalnego Fundusze Europejskie dla Warmii

i Mazur 2021-2027 na podstawie art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej: RODO), informuję iż:

1. Administratorem danych osobowych przetwarzanych w związku z realizacją projektu pt. „Tysiąc sto jeden kompetencji cyfrowych” jest Województwo Warmińsko-Mazurskie – Warmińsko Mazurskie Centrum Nowych Technologii z siedzibą w Olsztynie przy ul. Bartosza Głowackiego 14, 10-448 Olsztyn, reprezentowane przez Pana Pawła Kaszubskiego Dyrektora Warmińsko-Mazurskiego Centrum Nowych Technologii będące Beneficjentem tego Projektu (dalej: Beneficjent).
2. Beneficjent powołała Inspektora Ochrony Danych, z którym kontakt jest możliwy pod adresem email: iod@wmcnt.pl.
3. Państwa dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. c RODO i art. 9 RODO. Oznacza to, że Państwa dane osobowe są niezbędne do wypełnienia przez Beneficjenta obowiązków prawnych ciążących na nim w związku z realizacją ww. Projektu. Wspomniane obowiązki prawne ciążące na Beneficjencie w związku z realizacją ww. Projektu określone zostały w Zasadach realizacji Projektu nr FEWM.01.06-IZ.00-0001/24 pt. „Tysiąc sto jeden kompetencji cyfrowych” oraz przepisami m.in. w niżej wymienionych aktach prawnych:
 - 1) *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowe,*
 - 2) *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+) oraz uchylające rozporządzenie (UE) nr 1296/2013,*
 - 3) *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1058 z dnia 24 czerwca 2021 r. w sprawie Europejskiego Funduszu Rozwoju Regionalnego i Funduszu Spójności,*
 - 4) *Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (dalej: ustawa wdrożeniowa).*
4. Państwa dane osobowe będą przetwarzane wyłącznie w celu wykonania przez Beneficjenta określonych prawem i Uchwałą w sprawie dofinansowania Projektu nr FEWM.01.06-IZ.00-0001/24 obowiązków w związku z realizacją projektu nr FEWM.01.06-IZ.00-0001/24 pt. „Tysiąc sto jeden kompetencji cyfrowych”.

5. Państwa dane osobowe zgodnie z obowiązującymi przepisami prawa są udostępniane uprawnionym podmiotom i instytucjom, w tym wskazanym w art. 89 *ustawy wdrożeniowej*, w szczególności:
 - 1) Ministrowi właściwemu ds. rozwoju regionalnego – Ministrowi Funduszy i Polityki Regionalnej, ul. Wspólna 2/4, 00-926 Warszawa,
 - 2) Ministrowi właściwemu ds. finansów publicznych – Ministrowi Finansów, ul. Świętokrzyska 12, 00-916 Warszawa,
 - 3) Instytucji Zarządzającej programem regionalnym Fundusze Europejskie dla Warmii i Mazur 2021-2027 – Zarządowi Województwa Warmińsko-Mazurskiego, ul. Emilii Plater 1, 10-562 Olsztyn,
 - 4) Instytucji Audytorowej – Szefowi Krajowej administracji Skarbowej, ul. Świętokrzyska 12, 00-916 Warszawa
 w zakresie niezbędnym do realizacji ich zadań wynikających z przepisów *ustawy wdrożeniowej*.
6. Państwa dane osobowe mogą zostać powierzone lub udostępnione także specjalistycznym podmiotom realizującym badania ewaluacyjne, kontrole i audyty w ramach FEWiM na zlecenie Instytucji Zarządzającej FEWiM 2021-2027.
7. Państwa dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
8. Państwa dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji.
9. Państwa dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych w art. 87 ust. 1 *ustawy wdrożeniowej*.
10. W każdym czasie przysługuje Państwu prawo dostępu do swoich danych osobowych, jak również prawo żądania ich sprostowania. Natomiast prawo do usunięcia danych, prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych oraz prawo do sprzeciwu, przysługuje Państwu w przypadkach i na zasadach określonych odpowiednio w art. 17-22 *RODO*.
11. Jeżeli uznają Państwo, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, mają oni prawo wnieść skargę do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
12. Podanie przez Państwa danych jest dobrowolne, aczkolwiek odmowa ich podania będzie równoznaczna brakiem możliwości udziału w realizacji Projektu.

Oświadczam, że zapoznałem się/zapoznałam się z Klauzulą informacyjną dla osoby, której dane są przetwarzane w ramach realizacji Projektu. (System po zaznaczeniu płci powinien wskazać odpowiednią formę)	
MIJSCOWOŚĆ I DATA	<i>Do uzupełnienia po wydrukowaniu formularza</i>
CZYTELNY PODPIS OSOBY KANDYDUJĄCEJ	<i>Do uzupełnienia po wydrukowaniu formularza</i>

D. OŚWIADCZENIA

Oświadczam, że: **(przy Oświadczeniach w systemie musi być formuła do zaznaczenia – „aby móc wysłać Zgłoszenie wszystkie oświadczenia będą musiały być zaznaczone”)**

- Z własnej inicjatywy, deklaruję chęć podnoszenia umiejętności/kompetencji lub nabycia kwalifikacji poprzez udział w projekcie „Tysiąc sto jeden kompetencji cyfrowych”, realizowanym w ramach programu Fundusze Europejskie Warmii i Mazur 2021 – 2027, działanie 1.6 – Schemat B.
- Wszystkie informacje podane w formularzu zgłoszeniowym i dodatkowych dokumentach (o ile dotyczy) są prawdziwe, kompletne i w pełni odzwierciedlają moją sytuację prawną oraz są zgodne ze stanem faktycznym, a oświadczenie powyższe składam świadoma/świadomy **(System po zaznaczeniu płci powinien wskazać odpowiednią formę)** odpowiedzialności karnej za zeznanie nieprawdy lub zatajenie prawdy, wynikającej z art. 233 § 1 oraz art. 297 Kodeksu karnego.
- Poinformowano mnie o możliwości odmowy podania danych wrażliwych.

- Zobowiązuję się do niezwłocznego (do 7 dni kalendarzowych) powiadomienia Biura Projektu (ul. Bartosza Głowackiego 14 – IV piętro, pokój nr 3, 10-448 Olsztyn, e-mail: projekty@wmcnt.pl) o zmianie statusu, miejsca zamieszkania lub innych danych, które podałam/-em w procesie rekrutacji i uczestnictwa w Projekcie, w przypadku ich zmiany.
- Zapoznałem/Zapoznałam **(System po zaznaczeniu płci powinien wskazać odpowiednią formę)** się oraz akceptuję warunki Regulaminu Projektu.
- Zostałem poinformowany/Zostałam poinformowana **(System po zaznaczeniu płci powinien wskazać odpowiednią formę)**, że Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Fundusze Europejskie dla Warmii i Mazur (FEWiM) 2021-2027.
- Wyrażam zgodę na weryfikację danych zawartych we wszystkich złożonych dokumentach na każdym etapie realizacji projektu oraz na poddawanie się kontroli, ewaluacji i monitoringowi udzielonego wsparcia, na uczestnictwo w wszelkich kontrolach, badaniach, przeprowadzanych przez Operatora lub przez wskazany podmiot oraz inne uprawnione instytucje.
- Wyrażam zgodę na otrzymywanie wszelkich informacji o projekcie i uczestnictwa w nim, drogą elektroniczną na adres e-mail podany w części A formularza zgłoszeniowego w rozumieniu art. 10 ust. 2 Ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną.
- Wyrażam zgodę na wykorzystywanie/upowszechnianie mojego wizerunku na potrzeby wykonania przez Województwo Warmińsko-Mazurskie – Warmińsko Mazurskie Centrum Nowych Technologii określonych prawem obowiązków wynikających z realizacji projektu np. w materiałach zdjęciowych, audiowizualnych, zgodnie z art. 81 ust. 1 ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych.
- Zapoznałem/Zapoznałam **(System po zaznaczeniu płci powinien wskazać odpowiednią formę)** się z treścią Regulaminu rekrutacji i uczestnictwa w projekcie, rozumiem zawarte w nim zapisy i w pełni je akceptuję oraz zobowiązuję się przestrzegać jego postanowień w trakcie realizacji projektu.
- Oświadczam, że jestem świadomy/świadoma **(System po zaznaczeniu płci powinien wskazać odpowiednią formę)**, iż złożenie niniejszego formularza zgłoszeniowego wraz z załącznikami nie jest równoznaczne z zakwalifikowaniem się do objęcia wsparciem w ramach projektu pn. „Tysiąc sto jeden kompetencji cyfrowych”.
- Będę wykorzystywał/zdobycie umiejętności podczas realizacji pn. „Tysiąc sto jeden kompetencji cyfrowych” w ramach obowiązków zawodowych realizowanych u mojego pracodawcy.

Komentarz Zamawiającego do konstrukcji oświadczeń: System po zaznaczeniu płci powinien wskazać odpowiednią formę w zakresie jak wskazano powyżej.

MIJSCOWOŚĆ I DATA	<i>Do uzupełnienia po wydrukowaniu formularza</i>
CZYTELNY PODPIS OSOBY KANDYDUJĄCEJ	<i>Do uzupełnienia po wydrukowaniu formularza</i>