Szczegółowy Opis Przedmiotu Zamówienia [SOPZ]

„Opracowanie i wdrożenie platformy informatycznej na rzecz jednolitych ram cyfrowych dotyczących procedur wydawania pozwoleń na instalacje odnawialnych źródeł energii - Portal Informacyjny Odnawialnych Źródeł Energii (PIOZE)”

Zamawiający:
Ministerstwo Klimatu i Środowiska
ul. Wawelska 52/54, 00-922 Warszawa

Projekt finansowany w ramach Inwestycji G1.1.4 Krajowego Planu Odbudowy i Zwiększania Odporności: Wsparcie instytucji realizujących reformy i inwestycje w ramach REPowerEU

Spis treści

1. Słownik pojęć

Aktualna wersja oprogramowania	Należy przez to rozumieć wersję spełniającą **łącznie następujące kryteria**:
	• **Oficjalnie dostępna** w dniu rozpoczęcia realizacji projektu (lub dniu podpisania umowy), zgodnie z oficjalną publikacją producenta.
	• **Status wspierany:** Wersja objęta aktywnym wsparciem technicznym (maintenance/support), tj. oficjalnie zapewnia:
	  ○ aktualizacje bezpieczeństwa,
	  ○ poprawki błędów,
	  ○ aktualizacje zgodności (np. wsparcie nowych wersji systemów operacyjnych),
	  ○ wsparcie użytkowników.
	• **Zgodność z harmonogramem wsparcia producenta:** Wybrana wersja musi mieć zagwarantowany cykl życia (support lifecycle) obejmujący co najmniej cały okres realizacji projektu + 3 lata od jego zakończenia lub powinna należeć do linii wydań LTS (Long Term Support), jeżeli taki model jest dostępny.
	• **Brak przedpremierowego statusu:** Wersja nie może być oznaczona jako wydanie testowe, rozwojowe lub eksperymentalne (np. „alpha", „beta", „RC", „snapshot").

Definicja Projektu [DEF]	Dokument opisany szczegółowo w sekcji 4.1.
Dokumentacja	Zbiór uporządkowanych informacji i materiałów tworzonych na różnych etapach realizacji projektu, które opisują wymagania, procesy, rozwiązania techniczne, wyniki testów oraz inne elementy kluczowe dla zrozumienia, użytkowania, utrzymania i rozwijania systemu. Ogólne wymagania dla dokumentacji zostały w sekcji 2.3. Patrz również definicje poszczególnych typów dokumentów: DEF, PRT, PLT, PWI, które zostaną wytworzone w toku realizacji **Projektu**.
Etap	Wyodrębniona część realizacji projektu, która obejmuje zdefiniowany zakres prac i produktów. Każdy etap charakteryzuje się: • **Określonymi celami:** Precyzyjne zadania, które muszą zostać zrealizowane w ramach etapu. • **Produktami etapu:** Wynikiem każdego etapu są produkty (np. dokumenty, systemy, moduły) dostarczane zgodnie z wymaganiami określonymi w **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ)**. • **Harmonogramem:** Czas realizacji każdego etapu jest określony w harmonogramie projektu. • **Formalnym odbiorem:** Każdy etap kończy się odbiorem przez **Zamawiającego**, co potwierdza zgodność dostarczonych produktów z wymaganiami.

Gwarancja	Zobowiązania gwarancyjne Wykonawcy wobec **Zamawiającego** w sensie Kodeksu Cywilnego opisane w Rozdziale 9.
Harmonogram	Ramowe wymagania dotyczące terminów realizacji Umowy opisane w Rozdziale 3 niniejszej **SOPZ**.
Kod źródłowy	Czytelny dla człowieka zestaw instrukcji, napisany w wybranym języku programowania, który określa działanie oprogramowania. W kontekście projektu, kod źródłowy jest kluczowym elementem systemu, stanowiącym podstawę jego budowy, modyfikacji i rozwoju.
Krajowe Ramy Interoperacyjności, KRI	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. z 2024 r. poz. 773).
Lokalizacja Zamawiającego	Należy przez to rozumieć wszystkie jednostki organizacyjne, oddziały, wydziały i inne miejsca wykonywania działalności przez Zamawiającego, określone w aktualnym Regulaminie Organizacyjnym Zamawiającego, a także wszystkie miejsca wskazane przez Zamawiającego jako związane z realizacją projektu. W szczególności do Lokalizacji Zamawiającego zalicza się serwerownie oraz inne obiekty infrastrukturalne, w których prowadzone są lub będą prowadzone prace związane z instalacją, konfiguracją, testowaniem, eksploatacją lub rozwojem oprogramowania realizowanego w ramach zamówienia, a także miejsca przechowywania danych Zamawiającego objętych projektem.
Oprogramowanie standardowe	Gotowe, ogólnodostępne oprogramowanie komputerowe przeznaczone do powszechnego użytku, które jest oferowane na rynku w stałej wersji i konfiguracji, a jego funkcjonalności spełniają typowe, uniwersalne potrzeby użytkowników bez konieczności dokonywania istotnych modyfikacji lub dostosowań. Oprogramowanie to jest dostarczane w formie umożliwiającej jego natychmiastową instalację i użytkowanie zgodnie z dokumentacją dostarczoną przez producenta. <u>Komentarz:</u> W ramach niniejszego zamówienia w skład Oprogramowania Standardowego wchodzą: 1. system operacyjny opisany w sekcji OPS. 2. baza danych, o której mowa w sekcji BD. 3. inne **Oprogramowanie Standardowe** dostarczane przez Wykonawcę w celu realizacji przedmiotu zamówienia (np. system zarządzania portalem, o którym mowa w sekcji CMS).
OZE	**Odnawialne Źródła Energii** to odnawialne, niekopalne źródła energii obejmujące energię wiatru, energię promieniowania słonecznego, energię aerotermalną, energię geotermalną, energię hydrotermalną, hydroenergię, energię fal, prądów i pływów morskich, energię otoczenia, energię otrzymywaną z biomasy, biogazu, biogazu rolniczego, biometanu, biopłynów

	oraz z wodoru odnawialnego. OZE charakteryzują się zdolnością do odnawiania w krótkim czasie, w przeciwieństwie do paliw kopalnych, które powstają przez miliony lat. Są one kluczowym elementem w globalnej transformacji energetycznej, mającej na celu redukcję emisji gazów cieplarnianych i ochronę środowiska.
Personel	Zespół osób posiadających odpowiednie kwalifikacje, doświadczenie i kompetencje. , odpowiedzialnych za realizację poszczególnych zadań w projekcie, zgodnie z wymaganiami **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ)**.
PIOZE (Platforma)	Kompleksowy system informatyczny opracowywany w ramach realizacji umowy, mający na celu wspieranie procedur administracyjnych związanych z instalacjami odnawialnych źródeł energii (**OZE**). Portal zapewnia jednolite ramy cyfrowe, ułatwiając obsługę wniosków, dostęp do informacji oraz realizację procesów związanych z projektami budowy instalacji OZE.
Plan Testów [PLT]	Dokument opisany szczegółowo w sekcji 4.3.
Plan Prac	Należy przez to rozumieć dokument roboczy opracowany przez Wykonawcę, zawierający szczegółowy opis działań, zadań, kamieni milowych oraz terminów realizacji, mający na celu zapewnienie prawidłowej i terminowej realizacji Harmonogramu Projektu określonego w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ). Plan Prac jest wewnętrznym narzędziem organizacyjnym Wykonawcy i nie zastępuje, nie zmienia ani nie modyfikuje Harmonogramu Projektu. Plan Prac musi pozostawać zgodny z Harmonogramem Projektu i być na jego potrzeby aktualizowany.
Produkt	Należy przez to rozumieć każdy rezultat pracy wykonanej w ramach realizacji Projektu, który stanowi spełnienie wymagań określonych w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ), dokumentacji projektowej lub technicznej. Produkt może mieć charakter: 1. **Funkcjonalny lub programistyczny** – np. moduł systemu informatycznego, funkcja użytkowa, interfejs API, mikroserwis lub komponent oprogramowania umożliwiający realizację procesów określonych w SOPZ (np. rejestracja wniosku, integracja z ePUAP). 2. **Dokumentacyjny** – np. dokumentacja analityczna, projektowa, testowa, eksploatacyjna, bezpieczeństwa lub szkoleniowa przygotowana zgodnie z wymaganiami zawartymi w SOPZ lub opracowana w wyniku wcześniejszych etapów projektu (np. Plan Testów, Raport Zgodności, Opis architektury systemu). 3. **Organizacyjny lub infrastrukturalny** – np. skonfigurowane środowisko systemowe, uruchomiona instancja bazy danych, dostarczony kontener

	aplikacyjny, skonfigurowane kanały komunikacji z systemami zewnętrznymi, narzędzia do monitorowania i logowania, aktywne konta w systemie testowym. Każdy Produkt: • **jest przypisany do konkretnego etapu realizacji projektu** (zgodnie z harmonogramem w SOPZ), • **stanowi podstawę formalnego odbioru danego etapu** – jego weryfikacja jest warunkiem zaliczenia zakończenia danego etapu, • może być samodzielnym elementem końcowym lub częścią większego Produktu złożonego (np. pakietu funkcjonalności lub pełnego wdrożenia modułu). .
Projekt	Zbiór powiązanych ze sobą działań realizowanych w określonym czasie, które mają na celu osiągnięcie unikalnych rezultatów, zgodnych z wymaganiami i założeniami określonymi w **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ**).
Projekt Techniczny [PRT]	Dokument opisany szczegółowo w sekcji 4.2.
Projekt Wizualizacji [PWI]	Dokument opisany szczegółowo w sekcji 4.4.
Protokół Odbioru Cząstkowego	Formalny dokument potwierdzający zakończenie realizacji określonego produktu lub etapu projektu, zgodnie z wymaganiami określonymi w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ). Dokument ten jest efektem wspólnej weryfikacji przeprowadzonej przez Zamawiającego i Wykonawcę, potwierdzającej, że dostarczony Produkt lub wykonany Etap spełnia wymagania funkcjonalne, techniczne i jakościowe opisane w SOPZ oraz **Harmonogramie**. Podpisanie Protokołu Odbioru Cząstkowego jest warunkiem przejścia do kolejnych etapów lub rozpoczęcia następnych działań projektowych.
Protokołu Odbioru Końcowego	Formalny dokument potwierdzający zakończenie realizacji projektu lub jego etapu oraz zgodność dostarczonych produktów z wymaganiami określonymi w **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ)**. Dokument ten jest efektem wspólnej weryfikacji przeprowadzonej przez **Zamawiającego** i **Wykonawcę**.
RODO	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2023 r. poz. 100, z późn. zm.)
Środowisko produkcyjne	Należy przez to rozumieć środowisko informatyczne, na którym wdrożona i uruchomiona zostaje finalna, pełna wersja systemu PIOZE, przeznaczona do rzeczywistego świadczenia usług użytkownikom końcowym oraz realizacji procesów biznesowych określonych w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ).

	Środowisko produkcyjne stanowi oficjalne, operacyjne środowisko eksploatacyjne systemu i obejmuje wszystkie komponenty systemowe, infrastrukturalne i komunikacyjne niezbędne do prawidłowego funkcjonowania usług świadczonych przez system.
Środowisko rozwojowe (deweloperskie)	Należy przez to rozumieć środowisko informatyczne zarządzane i utrzymywane przez Wykonawcę, służące do tworzenia, rozwoju, wstępnego testowania i walidacji komponentów systemu przed ich przekazaniem do dalszych faz wdrożeniowych. Środowisko rozwojowe pozostaje pod wyłączną kontrolą Wykonawcy. Zamawiający nie posiada dostępu do tego środowiska i nie ingeruje w sposób jego organizacji. Wykonawca zobowiązany jest zapewnić ochronę informacji udostępnionych przez Zamawiającego (takich jak dane testowe, klucze integracyjne, dokumentacja techniczna) zgodnie z wymaganiami SOPZ, umowy oraz obowiązującymi standardami bezpieczeństwa informacji, w szczególności zgodnie z normą ISO/IEC 27001 lub równoważną.
Środowisko testowe	Należy przez to rozumieć środowisko informatyczne przeznaczone do przeprowadzania testów akceptacyjnych, testów funkcjonalnych oraz testów niefunkcjonalnych systemu przed jego wdrożeniem na środowisko produkcyjne. Środowisko testowe jest dostępne dla Zamawiającego oraz, w uzgodnionym zakresie, dla Wykonawcy. Testy przeprowadzane w tym środowisku mają na celu potwierdzenie zgodności systemu z wymaganiami określonymi w SOPZ, w tym w szczególności spełnienie wymagań funkcjonalnych, wydajnościowych, bezpieczeństwa oraz interoperacyjności. Środowisko testowe musi odwzorowywać konfigurację środowiska produkcyjnego w zakresie niezbędnym do przeprowadzenia rzetelnych testów.
Stabilna Wersja Oprogramowania	Należy przez to rozumieć wersję (wydanie) oprogramowania spełniającą **łącznie następujące kryteria**: • **Status wydania produkcyjnego:** Posiada status oficjalnego wydania stabilnego (tzw. GA – *General Availability*) lub długoterminowego wsparcia **LTS** (*Long Term Support*) nadany przez. Oznacza to, że jest to wersja przeznaczona do zastosowań produkcyjnych, objęta pełnym, długoterminowym wsparciem i poprawkami od dostawcy (w odróżnieniu od wydań rozwojowych). • **Brak oznaczeń testowych w wersji:** Jej oznaczenie (numer i nazwa) **nie zawiera określeń fazy testowej lub rozwojowej** (np. „alpha", „beta", „RC" – *Release Candidate*, „snapshot"). Innymi słowy, **nie jest to wydanie przedpremierowe** ani eksperymentalne –

	zgodnie z zasadami semantycznego wersjonowania wszelkie oznaczenia przedpremierowe wskazują na **niestabilność** danej wersji (Wersjonowanie semantyczne 2.0.0 | Semantic Versioning). • **Rekomendowana do użytku produkcyjnego:** Została **oficjalnie uznana za gotową do eksploatacji w środowisku produkcyjnym** przez podmiot odpowiedzialny za oprogramowanie. Taka wersja jest zazwyczaj oznaczona przez producenta jako **zalecana** do wdrożeń (np. na stronie producenta figuruje jako bieżące stabilne wydanie), podczas gdy wersje rozwojowe opatrzone są ostrzeżeniem o braku rekomendacji do produkcji. Innymi słowy, istnieje potwierdzenie ze strony producenta lub społeczności, że dana wersja jest sprawdzona i **polecana do zastosowań komercyjnych**.
System	Zintegrowany zestaw elementów technicznych, programistycznych oraz organizacyjnych obejmujący: • **Oprogramowanie:** Moduły i aplikacje realizujące funkcje zgodne z wymaganiami funkcjonalnymi i niefunkcjonalnymi. • **Interfejsy:** Narzędzia do komunikacji z innymi systemami i komponentami, w tym API i mechanizmy integracji. • **Procesy:** Zasady i procedury zarządzania, monitorowania oraz utrzymania funkcjonalności systemu. **Uwaga!** Projekt będzie realizowany na infrastrukturze udostępnionej przez Wykonawcę, a następnie przeniesiony na infrastrukturę **Zamawiającego**.
Szczegółowy Opis Przedmiotu Zamówienia (SOPZ)	Niniejszy dokument.
Umowa	Umowa zawarta w wyniku rozstrzygnięcia postępowania …..
Wykonawca	Podmiot określony jako „Wykonawca” w sensie Umowy.
Zamawiający	Podmiot określony jako „Zamawiający” w sensie umowy.

2. Wymagania ogólne

2.1 Wymagania dotyczące projektu [WPR]

WPR.1. System oparty na najnowszej, stabilnej wersji Oprogramowania Standardowego

WPR.1.1 Wybór oprogramowania

- **System** musi być oparty na wersji **Oprogramowania Standardowego**, która jest:
    - Stabilną Wersją Oprogramowania.
    - Aktualną Wersją Oprogramowania.
    - Zgodna z wymaganiami **SOPZ**, w tym z wymaganiami bezpieczeństwa, wydajności i skalowalności.

WPR.1.2 Wsparcie techniczne i aktualizacje

- **Wykonawca** musi zapewnić, że wybrane **Oprogramowanie Standardowe** będzie posiadało zapewnione wsparcie techniczne, w tym możliwość korzystania z dostępnych aktualizacji, poprawek bezpieczeństwa oraz dokumentacji, przez co najmniej 3 lata od zakończenia projektu,.

WPR.2. Warunkiem rozpoczęcia budowy Systemu jest uzgodnienie z Zamawiającym i dostarczenie kluczowych dokumentów zarządczych z Etapu I

WPR.2.1 Definicja kluczowych dokumentów zarządczych

- **Definicja Projektu [DEF]**: Określenie zakresu, celów, interesariuszy, ryzyk oraz zasad komunikacji w projekcie.
- **Projekt Techniczny [PRT]**: Szczegółowy opis technicznej architektury systemu, w tym struktury baz danych, integracji oraz zabezpieczeń.
- **Plan Testów [PLT]**: Szczegółowy harmonogram i metodologia testów funkcjonalnych, integracyjnych, wydajnościowych oraz akceptacyjnych.
- **Projekt Wizualizacji [PWI]**: Wstępna wizualizacja interfejsu użytkownika, prototypy ekranów i ścieżki użytkownika.

WPR.2.2 Proces uzgadniania dokumentów

- Dokumenty muszą być opracowane przez **Wykonawcę** zgodnie z wymaganiami **SOPZ**.

- Po przygotowaniu dokumenty są przekazywane **Zamawiającemu** do weryfikacji i akceptacji.
- Uzgodnienie dokumentów musi zakończyć się podpisaniem Protokołu Odbioru Cząstkowego, co jest formalnym potwierdzeniem gotowości do rozpoczęcia kolejnych etapów.

WPR.2.3 Czas realizacji

- Przygotowanie i uzgodnienie dokumentów zarządczych musi być zakończone w **Etapie I**.

WPR.3. Każdy etap będzie kończył się odbiorem produktów zgodnie z wymaganiami określonymi w SOPZ poprzez podpisanie odpowiedniego Protokołu odbioru Cząstkowego.

WPR.3.1 Odbiór Produktów

- **Wykonawca** jest zobowiązany do dostarczenia wszystkich **Produktów** określonych dla każdego etapu w **Harmonogramie** projektu.
- Produkty muszą być zgodne z wymaganiami technicznymi, funkcjonalnymi i jakościowymi zdefiniowanymi w **SOPZ**.

WPR.3.2 Proces odbioru

- Odbiór odbywa się w obecności przedstawicieli **Zamawiającego** i **Wykonawcy**.
- Odbiór jest dokumentowany Protokołem Odbioru Cząstkowego, który potwierdza spełnienie wymagań i akceptację produktu.
- W przypadku niezgodności produktu z wymaganiami **SOPZ**, **Wykonawca** zobowiązany jest do wprowadzenia poprawek w terminie 14 dni.

WPR.3.3 Odbiór produktu

- Wykonanie każdego produktu kończy się formalnym odbiorem przez **Zamawiającego** poprzez podpisanie odpowiedniego Protokołu Odbioru Cząstkowego.

WPR.3.4 Odbiór etapu

- Wykonanie każdego etapu kończy się formalnym odbiorem przez **Zamawiającego** poprzez podpisanie **Protokołu Odbioru Cząstkowego**.
- Zakończenie etapu wymaga zatwierdzenia wszystkich produktów przewidzianych dla tego etapu oraz potwierdzenia przez Zamawiającego ich zgodności z **SOPZ**.

- Odbiór etapu jest warunkiem rozpoczęcia kolejnego etapu realizacji **Projektu**.

WPR.3.4. Testy i odbiory końcowe

- **Testy systemu**:
    - Wykonanie testów funkcjonalnych, wydajnościowych, integracyjnych i akceptacyjnych w środowisku testowym.
- **Odbiory końcowe**:
    - Zakończenie **Projektu** wymaga podpisania **Protokołu Odbioru Końcowego** przez **Zamawiającego**.

2.2 Wymagania ogólne dotyczące prac [WTA]

WTA.1. Projekt jako zaplanowany proces

Projekt należy traktować jako kompleksowy, zorganizowany proces prowadzący do wytworzenia **Systemu**, w ramach którego realizowane będą następujące działania:

- Planowanie działań projektowych: Szczegółowe określenie **Planu Prac** oraz zasobów wymaganych po obu stronach (**Zamawiającego** i **Wykonawcy**).
- Współpraca zespołów projektowych: Utworzenie dedykowanych struktur organizacyjnych (kierownictwo projektu, zespoły techniczne) dla realizacji projektu.
- Koordynacja działań: Bieżące monitorowanie postępów, identyfikacja ryzyk oraz wdrażanie działań korygujących.
- Komunikacja: Utrzymanie stałego przepływu informacji między **Zamawiającym** a Wykonawcą w trakcie realizacji projektu.

WTA.2. Odpowiedzialność Wykonawcy

- Za pracowników i ich działania: **Wykonawca** ponosi pełną odpowiedzialność za wszelkie działania swoich pracowników (**Personelu**), w tym ewentualne szkody wyrządzone w **Lokalizacjach Zamawiającego**.
- Za zgodność z dokumentacją projektową: Wszelkie działania wdrożeniowe muszą być zgodne z zatwierdzoną **Dokumentacją**, która będzie aktualizowana w miarę postępów projektu.

WTA.3. Organizacja prac wdrożeniowych

- **Godziny pracy**: Prace wdrożeniowe będą realizowane w godzinach pracy **Zamawiającego (w dni robocze 8.15-16.15)**, z uwzględnieniem ewentualnych dodatkowych dni wolnych od pracy określonych zarządzeniami ogłoszonymi w

Biuletynie Informacji Publicznej (BIP). Prace poza godzinami pracy muszą być wcześniej uzgodnione i zatwierdzone.

- **Etapy** realizacji prac oraz **Produkty**: określono w Rozdziale 3 **SOPZ**.

WTA.4. Wymagania techniczne

WTA.4.A. Standardy funkcjonalne systemu

- *SOA*:
    - System musi wspierać architekturę zorientowaną na usługi (*SOA*) z integracją poprzez:
        - *WSDL*: Specyfikacja interfejsów.
        - *XML*: Struktura danych.
        - *PSOAP*: Standard przesyłania komunikatów.
- Bezpieczeństwo *(WS-Security):*
    - *SAML*: Uwierzytelnianie i autoryzacja użytkowników.
- Zarządzanie projektem:
    - Wymóg stosowania metodyki *PRINCE2* lub równoważnej w zarządzaniu projektem.

WTA.4.B. Zgodność z aktami prawnymi

- **System** oraz **Projekt**, w zakresie nieuregulowanym niniejszą **SOPZ** *(*tj. **Wykonawca** realizując projekt oraz System może przyjąć dowolne rozwiązania w zakresie nieuregulowanym przez **SOPZ** pod warunkiem spełnienia wymogów niniejszych aktów prawnych, a także po wyrażeniu zgody **Zamawiającego**) musi spełniać wszystkie wymogi określone w przepisach prawa, w szczególności:
    - **Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2024 r. poz. 1530, z późn. zm.)**

      Reguluje zarządzanie finansami publicznymi, w tym kwestie dotyczące przyznawania i rozliczania środków publicznych na projekty OZE.
    - **Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024 r. poz. 1557, z późn. zm.)**

      Określa zasady informatyzacji w administracji publicznej, co jest kluczowe dla projektowania platformy cyfrowej portalu.
    - **Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. z 2024 r. poz. 773)**

Ustala minimalne wymagania dotyczące systemów teleinformatycznych, zapewniając zgodność z krajowymi standardami informatycznymi.

- **Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2023 r., poz. 1440, z późn. zm.)**

  Wymaga, aby portal był dostępny cyfrowo, uwzględniając potrzeby osób z niepełnosprawnościami.

- **Rozporządzenie Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego (Dz.U. 2020 poz. 1194)**

  Reguluje użycie profilu zaufanego do uwierzytelniania użytkowników, co jest przydatne przy składaniu wniosków online.

- **Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie elektronicznej platformy usług administracji publicznej (Dz.U. z 2016 r. poz. 1626)**

  Określa standardy i zakres korzystania z *ePUAP*, co może być przydatne do integracji z portalem.

- **Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2024 r. poz. 1513, z późn. zm.)**

  Definiuje zasady świadczenia usług online, w tym kwestie prawne związane z zawieraniem umów elektronicznych.

- **Ustawa z dnia 29 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2024 r. poz. 1725, z późn. zm.)**

  Reguluje kwestie związane z elektroniczną identyfikacją i podpisem, które mogą być wykorzystywane na portalu.

- **Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781, z późn. zm.)**

  Zapewnia ochronę danych osobowych użytkowników portalu, w tym bezpieczeństwo przetwarzania danych.

- **Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2023 r. poz. 1206, z późn. zm.)**

  Ochrona danych osobowych w sytuacjach związanych z zapobieganiem przestępczości, istotne, jeśli w systemie zbierane są dane wrażliwe.

- **Ustawa z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (Dz.U. z 2024 r. poz. 1361, z późn. zm.)**

Kluczowa dla wszystkich przepisów i wymogów związanych z wdrażaniem oraz wspieraniem projektów **OZE**.

- **Ustawa z dnia 6 marca 2018 r. Prawo przedsiębiorców (Dz.U. z 2024 r. poz. 236, z późn. zm.)**

  Reguluje zasady działalności gospodarczej, co może dotyczyć inwestorów i wykonawców realizujących projekty **OZE**.

- **Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne (Dz.U. z 2024 r. poz. 266, z późn. zm.)**

  Określa zasady funkcjonowania rynku energetycznego, w tym przyłączenia do sieci, co jest istotne dla instalacji OZE.

- **Ustawa z dnia 27 kwietnia 2001 r. Prawo ochrony środowiska (Dz.U. z 2024 r. poz. 54, z późn. zm.)**

  Zasady ochrony środowiska, szczególnie istotne dla instalacji OZE wpływających na środowisko.

- **Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2024 r. poz. 1061, z późn. zm.)**

  Reguluje zasady zawierania umów cywilnoprawnych, co może być użyteczne dla usług świadczonych przez portal.

- **Zalecenie Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym (Dz. Urz. UE, seria L, nr 96, str. 50–54, z dnia 5 kwietnia 2019 r.)**

  Podkreśla znaczenie ochrony infrastruktury energetycznej przed zagrożeniami cybernetycznymi.

- **Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077, z późn. zm.)**

  Ogólne wymogi dotyczące ochrony cyberprzestrzeni, niezbędne dla zapewnienia bezpieczeństwa portalu.

- **Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz.U. z 2023 r. poz. 2383, z późn. zm.)**

  Może być potrzebna przy obliczaniu ulg lub odliczeń podatkowych dla inwestycji w **OZE**.

- **Rozporządzenie Ministra Klimatu i Środowiska z dnia 7 grudnia 2020 r. w sprawie wymagań dotyczących minimalnych standardów efektywności energetycznej (Dz.U. z 2020 r., poz. 2148)**

Minimalne standardy efektywności energetycznej dla urządzeń stosowanych w projektach **OZE**.

- **Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Dz.U. z 2024 r. poz. 1130, z późn. zm.)**

  Reguluje zasady kształtowania polityki przestrzennej, co jest kluczowe przy lokalizacji instalacji OZE. Nowelizacja z 7 lipca 2023 r. wprowadza zmiany ułatwiające inwestycje w OZE, co powinno być odzwierciedlone w funkcjonalnościach PIOZE.

- **Ustawa z dnia 3 lutego 1995 r. o ochronie gruntów rolnych i leśnych (Dz.U. z 2024 r. poz. 82, z późn. zm.)**

  Określa zasady ochrony gruntów przed degradacją i niewłaściwym wykorzystaniem. Procedury wyłączania gruntów z produkcji rolnej lub leśnej pod inwestycje OZE muszą być uwzględnione w platformie.

- **Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/2413 z dnia 18 października 2023 r. zmieniająca dyrektywę (UE) 2018/2001, rozporządzenie (UE) 2018/1999 i dyrektywę 98/70/WE w odniesieniu do promowania energii ze źródeł odnawialnych oraz uchylająca dyrektywę Rady (UE) 2015/652**

  Zmienia wcześniejsze i wprowadza nowe przepisy w zakresie promowania energii ze źródeł odnawialnych. PIOZE powinna być zgodna z unijnymi standardami i ułatwiać implementację dyrektywy na poziomie krajowym.

- **Ustawa z dnia 20 maja 2016 r. o inwestycjach w zakresie elektrowni wiatrowych (Dz.U. z 2024 r. poz. 317, z późn. zm.)**

  Reguluje zasady lokalizacji i budowy elektrowni wiatrowych. Platforma powinna uwzględniać specyficzne wymogi proceduralne dla tego typu inwestycji.

- **Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz.U. z 2024 r. poz. 1112, z późn. zm.)**

  Zapewnia dostęp do informacji o środowisku oraz udział społeczeństwa w procedurach. PIOZE musi umożliwiać transparentność i dostęp do niezbędnych danych środowiskowych.

- **Ustawa z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych (Dz.U. 2024 poz. 182, z późn. zm.)**

  Reguluje procedury związane z morskimi farmami wiatrowymi. Platforma powinna wspierać procesy związane z tego typu inwestycjami.

- **Ustawa z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz.U. 2024 poz. 1125, z późn. zm.)**

  Określa zasady gospodarowania obszarami morskimi, istotne dla morskich instalacji OZE. PIOZE musi uwzględniać te regulacje.

- **Rozporządzenie Rady Ministrów z dnia 14 kwietnia 2021 r. w sprawie przyjęcia planu zagospodarowania przestrzennego morskich wód wewnętrznych, morza terytorialnego i wyłącznej strefy ekonomicznej w skali 1:200 000 (Dz.U. 2022 poz. 2518)**

  Dotyczy planowania przestrzennego na obszarach morskich, co jest kluczowe dla lokalizacji morskich OZE.

- **Ustawa z dnia 13 lipca 2023 r. o ułatwieniach w przygotowaniu i realizacji inwestycji w zakresie biogazowni rolniczych, a także ich funkcjonowaniu (Dz.U. 2023 poz. 1597, z późn. zm.)**

  Wprowadza uproszczenia proceduralne dla biogazowni rolniczych. Platforma powinna odzwierciedlać te ułatwienia.

- **Rozporządzenie Ministra Rolnictwa i Rozwoju Wsi z dnia 12 października 2023 r. w sprawie szczegółowej listy substratów możliwych do wykorzystania w biogazowni rolniczej (Dz.U. 2023 poz. 2230)**

  Określa dopuszczalne substraty, co wpływa na procedury związane z biogazowniami.

- **Rozporządzenie Ministra Środowiska z dnia 30 kwietnia 2013 r. w sprawie składowisk odpadów (Dz.U. 2022 poz. 1902)**

  Reguluje kwestie związane z gospodarką odpadami, istotne przy inwestycjach OZE.

- **Ustawa z dnia 9 czerwca 2011 r. - Prawo geologiczne i górnicze (Dz.U. 2024 poz. 1290, z późn. zm.)**

  Dotyczy m.in. pozyskiwania surowców, co może mieć znaczenie przy budowie instalacji OZE.

- **Ustawa z dnia 20 lipca 2017 r. - Prawo wodne (Dz.U. 2024 poz. 1087, z późn. zm.)**

  Reguluje gospodarowanie wodami, co jest istotne dla niektórych instalacji OZE, np. elektrowni wodnych.

- **Rozporządzenie Rady Ministrów z dnia 10 września 2019 r. w sprawie przedsięwzięć mogących znacząco oddziaływać na środowisko (Dz.U. 2023 poz. 1724)**

Określa procedury oceny oddziaływania na środowisko, kluczowe dla inwestycji OZE.

- **Ustawa z dnia 14 kwietnia 2023 r. o przygotowaniu i realizacji inwestycji w zakresie elektrowni szczytowo-pompowych oraz inwestycji towarzyszących (Dz.U. 2023 poz. 1113, z późn. zm.)**

  Wprowadza szczególne zasady dla tego typu elektrowni, które powinny być uwzględnione w PIOZE.

- **Rozporządzenie Ministra Klimatu i Środowiska z dnia 21 października 2021 r. w sprawie rejestru magazynów energii elektrycznej (Dz.U. 2021 poz. 2010)**

  Określa zasady prowadzenia rejestru magazynów energii, co jest istotne dla integracji OZE z systemem energetycznym.

- **Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320, z późn. zm.).**

  PIOZE musi obsługiwać eDoręczenia, integrację z KWIE, skrzynki doręczeń i potwierdzenia odbioru, zgodnie z ustawą.

WTA.4.C. Integracja z istniejącymi platformami

- **System musi być kompatybilny oraz zapewniać integrację z następującymi platformami publicznymi:**

  - **ePUAP** (elektroniczna Platforma Usług Administracji Publicznej) – w zakresie przesyłania i odbioru korespondencji urzędowej,
  - **eDoręczenia** – w zakresie obsługi doręczeń elektronicznych, zgodnie z ustawą o doręczeniach elektronicznych,
  - **Profil Zaufany** – w zakresie uwierzytelniania użytkowników oraz składania podpisów elektronicznych,
  - **Węzeł Krajowy (Login.gov.pl)** – w zakresie obsługi federacji tożsamości w usługach publicznych,
  - **KWIE (Krajowy Węzeł Identyfikacji Elektronicznej)** – w zakresie zapewnienia obsługi różnych metod identyfikacji elektronicznej (np. eID),
  - **Centralna Lista Rewokacji Certyfikatów** – w zakresie weryfikacji aktualności i unieważnienia certyfikatów.

2.3 Wymagania ogólne dotyczące dokumentacji [WDO]

Przygotowana **Dokumentacja** musi spełniać najwyższe standardy jakości, być spójna, kompletna i zgodna z wymaganiami **Zamawiającego**. Każdy etap jej tworzenia oraz dostarczania będzie realizowany zgodnie z przyjętym **Harmonogramem**, z uwzględnieniem odpowiednich procedur akceptacji i aktualizacji. **Dokumentacja** ma być dostarczona w

formie pozwalającej na edycję, przeglądanie oraz wyszukiwanie. **Wykonawca** zapewnia także przekazanie praw autorskich do dokumentacji na rzecz **Zamawiającego**.

WDO.1. Jakość dokumentacji

Wszystkie dokumenty tworzone w ramach realizacji zamówienia muszą charakteryzować się wysoką jakością, na którą wpływają następujące czynniki:

- Struktura dokumentu: Wyraźny podział na rozdziały, podrozdziały i sekcje w sposób czytelny i zrozumiały.
- Zachowanie standardów: Użycie znanych i przyjętych standardów dokumentowania, np. notacji *UML*.
- Spójność stylu: Zachowanie jednolitej struktury, formy i sposobu pisania zarówno w poszczególnych dokumentach, jak i w ich fragmentach.
- Kompletność: Wyczerpujące przedstawienie omawianych problemów, obejmujące pełny zakres zagadnienia bez wyraźnych braków.
- Spójność i niesprzeczność: Zapewnienie zgodności pomiędzy informacjami w dokumencie oraz brak logicznych sprzeczności pomiędzy różnymi dokumentami lub ich fragmentami.

WDO.2. Odniesienie do SOPZ

- Każde wymaganie w części **SOPZ** dotyczącej specyfikacji wymagań, jest oznaczone niepowtarzalną etykietą, umożliwiającą jednoznaczną identyfikację oraz odniesienie w dokumentacji. Na te etykiety należy się powoływać w celu zapewnienia odniesienia do danego wymagania niniejszego dokumentu.

WDO.3. Rodzaje dokumentacji

Wykonawca przygotuje następujące rodzaje dokumentacji zgodnie z wymaganiami opisanymi w sekcji WDO .

- Dokumentacja projektowa – dokumenty DEF, PRT, PLT, PWI,, RTO, RTS oraz Raport ze Szkoleń.
- Dokumentacja systemowa – dokument DOS.
- Dokumentacja eksploatacyjna – dokument DOE.
- Instrukcja użytkownika – dokument INS.

WDO.5. Forma przekazania Dokumentacji

- Dokumentacja przekazywana Zamawiającemu do odbioru:
    - Musi być sporządzona *w języku polskim*.
    - Wyjątek: Dokumentacja producentów **Oprogramowania Standardowego** może być dostarczona w języku angielskim.
    - Dostarczona w postaci elektronicznej w dwóch kopiach na nośniku optycznym z zablokowaną możliwością zapisu.
    - Musi spełniać wymagania dotyczące oznaczania dokumentów współfinasowanych z Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) oraz NextGenerationEU, co oznacza w szczególności:
        - Umieszczanie odpowiednich logotypów: Na wszystkich dokumentach związanych z realizacją projektów finansowanych z KPO należy zamieszczać logotypy KPO, flagi Polski oraz Unii Europejskiej oraz NextGenerationEU. Logotypy powinny być wyraźne, odpowiednio widoczne i zgodne z oficjalnymi wytycznymi dotyczącymi ich stosowania.
        - Stosowanie jednolitej identyfikacji wizualnej: Dokumenty powinny być zgodne z wytycznymi zawartymi w Księdze Identyfikacji Wizualnej KPO, która określa standardy dotyczące kolorystyki, typografii oraz rozmieszczenia elementów graficznych.
        - Informowanie o współfinansowaniu: W treści dokumentów należy jasno wskazać, że projekt jest współfinansowany ze środków KPO, co zwiększa świadomość o roli tych funduszy w realizacji przedsięwzięcia.
    - Format:
        - Wersja pierwsza: edytowalna, umożliwiająca wyszukiwanie po słowach kluczowych oraz
        - *Wersja druga: PDF*.
        - *Wytyczne w zakresie materiałów szkoleniowych znajdują się w sekcji 7*.5.

WDO.6. Aktualizacja dokumentacji

- W okresie **Gwarancji** systemu, **Wykonawca** będzie aktualizował dokumentację w przypadku dokonywania przez **Wykonawcę** zmian w **Systemie**.
- Zaktualizowaną **Dokumentację Wykonawca** przekazuje **Zamawiającemu** w terminie do 30 dni od wprowadzenia zmian.

2.4 Wymagania w zakresie standardu kodu źródłowego i jego dokumentacji

Zgodnie z *ISO/IEC 12207*, faza eksploatacji oprogramowania obejmuje wszystkie działania niezbędne do jego utrzymania, w tym możliwość adaptacji do nowych wymagań. Dlatego **Wykonawca** powinien dostarczyć kod źródłowy wraz z dokumentacją umożliwiającą jego rozwój, tak aby **Zamawiający** mógł swobodnie tłumaczyć, przystosowywać, zmieniać układ lub dodawać nowe moduły.

Dokumentacja powinna obejmować:

- Opis architektury (*ISO/IEC 25010*: cecha „*zrozumiałość*"),
- Organizację kodu źródłowego (*ISO/IEC 12207*: wymagania dot. fazy utrzymania),
- Opis klas, zmiennych i protokołów transmisji danych, co pozwoli na integrację z innymi systemami, zgodnie z zasadą „*interoperacyjności*" z *ISO/IEC 25010*.

Dzięki temu **Zamawiający**, mając kompletną dokumentację i komentarze, będzie w stanie efektywnie przeprowadzać diagnostykę i modyfikacje kodu.

1. Dostarczanie kodu na nośniku w formie odczytywalnej i kompilowalnej

Kodeks *ISO/IEC 27001* wymaga, aby informacje były dostarczane w formie odczytywalnej i bezpiecznej. **Wykonawca** powinien dostarczyć kod na informatycznym nośniku, z możliwością jego zapisania i kompilacji. Zgodnie z *ISO/IEC 12207*, w **Dokumentacji** powinien znaleźć się:

- Wykaz narzędzi programistycznych i bibliotek niezbędnych do kompilacji,
- Instrukcja konfiguracyjna dla komputerów i środowisk, aby **Zamawiający** mógł doprowadzić oprogramowanie do formy wykonywalnej.

Dodatkowo, wymagane jest unikanie technik szyfrowania czy *obfuskacji*, które mogą ograniczać dostępność kodu, zgodnie z zasadą „*przejrzystości*" w *ISO/IEC 25010*.

2. Aktualizacje kodu źródłowego i wsparcie gwarancyjne

Przy świadczeniu wsparcia i usług gwarancyjnych **Wykonawca** ma obowiązek dostarczyć zaktualizowany **Kod Źródłowy** wraz z pełną **Dokumentacją**. Zgodnie z *ISO/IEC 12207*, każda aktualizacja kodu powinna być traktowana jako osobna wersja i dokumentowana w sposób umożliwiający **Zamawiającemu** samodzielną kompilację po zakończeniu świadczenia usług. To zapewni „*łatwość konserwacji*" i „*łatwość zarządzania*" oprogramowaniem zgodnie z *ISO/IEC 25010*.

3. Korzystanie z kodu źródłowego po zakończeniu realizacji umowy

Po zakończeniu umowy **Zamawiający** zachowuje pełne prawa do kodu źródłowego, co jest zgodne z normami *ISO/IEC 12207* w fazie operacyjnej. **Kod źródłowy** oraz prawa do korzystania z niego pozostają aktywne, a **Zamawiający** może dalej rozwijać i modyfikować oprogramowanie bez dodatkowych barier.

3. Harmonogram realizacji projektu

Poniższa sekcja szczegółowo przedstawia **Harmonogram** projektu, w tym opis etapów, ich produkty oraz ramy czasowe realizacji, które stanowią podstawę do egzekwowania realizacji umowy.

Zamawiający wymaga od **Wykonawcy** pełnej zgodności z **Harmonogramem**, zarówno pod względem terminowości, jak i jakości dostarczanych produktów. Wszelkie odchylenia od **Harmonogramu** będą analizowane i mogą skutkować sankcjami przewidzianymi w =Umowie. Realizacja **Projektu** zgodnie z harmonogramem zapewni jego terminowe zakończenie oraz pełną funkcjonalność systemu zgodnie z oczekiwaniami **Zamawiającego**.

Etap	Produkty etapu	Czas realizacji
Etap I – Przygotowanie projektu	- Definicja Projektu [**DEF**] - Projekt Techniczny [**PRT**] - Plan Testów [**PLT**] - Projekt Wizualizacji PIOZE (**PWI**) - Środowisko Rozwojowe i Środowisko Testowe [**IDT**] - Licencje Oprogramowania Standardowego [**LOS**]	**4 tygodnie** od daty podpisania Umowy
Etap II – Stworzenie PIOZE	- Oprogramowanie Portalu [**OPR**] - Dokumentacja systemowa PIOZE [**DOS**] - Raport z testów oprogramowania [**RTO**]	**12 tygodni** od daty odbioru **Etapu I**
Etap III – Konfiguracja systemu	- Konfiguracja Portalu [**KNF**] - Dokumentacja eksploatacyjna PIOZE [**DOE**] - Instrukcja użytkownika wewnętrznego PIOZE [**INS**] - Raport z testów systemu [**RTS**]	**8 tygodni** od daty odbioru **Etapu II**
Etap IV – Szkolenia użytkowników	- Szkolenia użytkowników [**SZK**]	**8 tygodni** od daty odbioru **Etapu III**

Uwaga! W przypadku równoległej realizacji Etapu III i IV Wykonawca musi tak skoordynować prace, by użytkownicy posiadali umiejętności niezbędne do testowania systemu w ramach realizacji produktu Raport z testów systemu [RTS[.

Etap	Produkty etapu	Czas realizacji
Etap V – Migracja na środowisko Zamawiającego	- Migracja [**MIGR**]	**4 tygodnie** od daty wezwania przez **Zamawiającego**, lecz nie wcześniej niż 4 tygodnie od zakończenia Etapu III

4. Etap I – Przygotowanie projektu

4.1 Wymagania dotyczące sformułowania Definicji Projektu [DEF]

Definicja Projektu [DEF] jest obowiązkowym dokumentem, który musi zostać opracowany przez Wykonawcę w ramach **Etapu I** realizacji projektu. Stanowi ona podstawę do efektywnego planowania, realizacji oraz monitorowania postępów prac, a także zapewnienia wspólnego zrozumienia zakresu, celów i założeń projektu przez wszystkie zaangażowane strony.

Wykonawca jest odpowiedzialny za przygotowanie **Definicji Projektu** w sposób zgodny z poniższymi wytycznymi oraz za jej terminowe dostarczenie w ramach określonego **Harmonogramu**. Dokument musi być szczegółowy, kompletny i zgodny z wymaganiami **Zamawiającego**, ponieważ jego akceptacja stanowi warunek konieczny do przejścia do kolejnych etapów projektu.

Zakres opracowania:

a. Wprowadzenie

- Tytuł projektu: Jednoznaczne określenie nazwy projektu.
- Wersja dokumentu: Numeracja wersji wraz z datą utworzenia i autorami.
- Cel dokumentu: Wyjaśnienie, dlaczego dokument został przygotowany.

b. Cel projektu

- Opis celów biznesowych: Powody realizacji projektu, mierzalne cele biznesowe.
- Korzyści: Przewidywane rezultaty i korzyści dla organizacji oraz interesariuszy.

c. Zakres projektu

- Opis zakresu: Zakres funkcjonalny i niefunkcjonalny, obszary realizacji projektu.
- Wykluczenia z zakresu: Elementy, które nie są częścią projektu.

d. Kluczowe założenia

- Warunki początkowe, od których zależy realizacja projektu (np. dostępność zasobów, technologie, zależności organizacyjne).

e. Ograniczenia

- Ograniczenia czasowe, budżetowe, technologiczne, organizacyjne i prawne.

f. Interesariusze

- Lista kluczowych interesariuszy wraz z opisem ich ról i oczekiwań (np. sponsorzy, użytkownicy końcowi, zespoły techniczne).

g. Harmonogram Projektu

- Harmonogram Projektu.
- Plan Prac.

h. Zasoby

- Zasoby ludzkie: Opis zespołów projektowych, wymaganych kompetencji.
- Zasoby materialne: Sprzęt, oprogramowanie, narzędzia.

i. Budżet

- Wysokość dostępnych środków.
- Podział budżetu na kategorie kosztów.

j. Ryzyka projektu

- Potencjalne ryzyka wraz z ich oceną (prawdopodobieństwo, wpływ).
- Sposoby zarządzania ryzykiem.

k. Opis procesu zarządzania ryzykiem obejmujący takie elementy jak:

- Identyfikacja ryzyk.
- Analiza ryzyk.
- Planowanie reakcji na ryzyka.
- Monitorowanie ryzyk.
- Standard produktów:
    - Rejestr ryzyk,
    - Plan reakcji na ryzyka.
    - Raporty z przeglądów ryzyk.

l. Struktura organizacyjna projektu

- Opis ról w projekcie (np. kierownik projektu, sponsor, członkowie zespołu).
- Relacje między interesariuszami.

m. Kryteria sukcesu projektu

- Mierniki sukcesu, np. ukończenie w terminie, w ramach budżetu, zgodność z wymaganiami.

n. Plan komunikacji

- Kanały komunikacji wewnętrznej i zewnętrznej.
- Częstotliwość i formy raportowania.

o. Plan zarządzania zmianą

- Procedura wprowadzania i akceptacji zmian w zakresie, **Harmonogramie** czy budżecie projektu.

p. Kluczowe produkty projektu

- Opis wyników projektu (np. oprogramowanie, raporty, szkolenia).

4.2. Wymagania dotyczące opracowania Projektu Technicznego [PRT]

Projekt Techniczny [PRT] jest obowiązkowym dokumentem, który musi zostać opracowany przez Wykonawcę w ramach realizacji projektu. Jego celem jest precyzyjne określenie założeń, wymagań technicznych oraz szczegółowych rozwiązań, które będą stanowiły podstawę dla projektowania, budowy oraz wdrożenia Systemu. Dokument ten musi w pełni odzwierciedlać wymagania **Zamawiającego** zawarte w **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ),** gwarantując ich realizację na każdym etapie projektu.

Zakres opracowania:PRT.1 Opis architektury Systemu

- Architektura sprzętowa:
  - Szczegółowy opis środowiska sprzętowego, w tym serwerów, urządzeń sieciowych, pamięci masowej.
- Architektura logiczna:
  - Podział na moduły logiczne wraz z opisem ich funkcjonalności i zależności.
- Architektura techniczna:

- Technologie, frameworki, biblioteki, oraz standardy wykorzystywane w budowie systemu.
- Rozwiązania zapewniające skalowalność i wysoką dostępność.

PRT.2 Narzędzia i oprogramowanie

- Wykaz narzędzi do programowania, testowania, integracji oraz wdrażania.
- Oprogramowanie standardowe oraz autorskie, które będzie częścią Systemu.
- Opis narzędzi monitorowania oraz diagnostyki.

PRT.3 Zasady integracji i interfejsy

- Opis metod integracji pomiędzy modułami systemu (np. *REST API, SOAP*, WebSocket).
- Standardy komunikacji (np. *JSON, XML*).
- Szczegółowy opis interfejsów integracyjnych, w tym schematy wymiany danych, obsługiwane protokoły oraz mechanizmy uwierzytelniania.

PRT.4 Model danych

- Logiczny model danych:
  - Klasyfikacja i opis danych systemowych, struktury danych, schematy baz danych.
- Fizyczny model danych:
  - Konfiguracja fizyczna baz danych, schematy przechowywania, indeksowania oraz relacji.

PRT.5 Zakres i metody integracji

- Wykaz komponentów oraz systemów zewnętrznych objętych integracją.
- Szczegółowe metody oraz harmonogram integracji.
- Mechanizmy synchronizacji danych oraz rozwiązywania konfliktów.

PRT.6 Interfejs użytkownika

- Opis układu graficznego oraz sposobu interakcji użytkownika z systemem.
- Przykłady ekranów i prototypy kluczowych elementów interfejsu.

PRT.7 System zabezpieczeń

- Mechanizmy uwierzytelniania i autoryzacji.
- Szyfrowanie danych w tranzycie oraz w spoczynku.

- Plan ciągłości działania

4.3. Wymagania dotyczące stworzenia Planu Testów [PLT]

Plan Testów (PLT) jest obowiązkowym dokumentem, który musi zostać opracowany przez Wykonawcę w ramach realizacji projektu. Stanowi kompleksowy dokument zarządczy, precyzyjnie opisujący sposób przeprowadzenia testów **Systemu**, weryfikację zgodności z wymaganiami oraz **Projektem Technicznym**. **PLT** powinien uwzględniać wszystkie aspekty testowania niezbędne do zapewnienia wysokiej jakości oraz zgodności **Systemu** z oczekiwaniami **Zamawiającego**.

Zakres opracowania:

I. Cele Planu Testów

1. Zdefiniowanie procesu weryfikacji i walidacji **Systemu**.
2. Ustalenie harmonogramu testów oraz iteracji.
3. Zidentyfikowanie ról i odpowiedzialności w procesie testowania.
4. Zapewnienie zgodności **Systemu** z:
    - wymaganiami funkcjonalnymi,
    - standardami technicznymi,
    - ergonomii i dostępności (*WCAG 2.1*).

II. Struktura Planu Testów

1. **Informacje ogólne**:
    - Cel dokumentu.
    - Zakres testowania (opis funkcji i komponentów systemu objętych testami).
    - Kryteria sukcesu testów (akceptacyjne).
2. **Opis środowiska testowego**:
    - Wymagania sprzętowe i programowe środowiska testowego.
    - Szczegóły dotyczące infrastruktury testowej (wyodrębnionej na potrzeby zamówienia).
    - Mechanizm dostępu zdalnego umożliwiający **Zamawiającemu** weryfikację testów.

3. **Plan i harmonogram testów**:
    - Proponowany czas trwania testów, iteracje, kamienie milowe.
    - Powiązanie harmonogramu testów z etapami projektu (**Harmonogramem**a).
4. **Kategorie testów**:
    - Testy jakościowe: ocena zgodności z normami jakości.
    - Testy funkcjonalne: weryfikacja działania systemu w zgodności z opisanymi wymaganiami.
    - Testy integracyjne: analiza współpracy między modułami systemu.
    - Testy bezpieczeństwa: ocena ochrony danych i odporności na zagrożenia.
    - Testy wydajnościowe: sprawdzenie czasu odpowiedzi, przepustowości i stabilności systemu.
    - Testy ergonomii: badanie intuicyjności i wygody użytkowania.
    - Testy UX oraz zgodności z WCAG 2.1: zapewnienie dostępności dla użytkowników z różnymi niepełnosprawnościami.
5. **Szczegółowe scenariusze testowe**:
    - Nazwa modułu, komponentu lub funkcji.
    - Szczegóły konfiguracji (jeśli wymagane).
    - Kroki testowe i oczekiwane wyniki.
    - Kryteria akceptacyjne.
6. **Zasady reagowania na niepowodzenia testów**:
    - Opis procedur eskalacji błędów.
    - Proces dokumentowania i śledzenia błędów w narzędziach takich jak system zarządzania zgłoszeniami (np. *JIRA – patrz również sekcja RTS – system według wyboru* ***Wykonawcy*** *o minimalnych wymaganiach wskazanych przez* ***Zamawiającego***).

III. Wymagania proceduralne

1. **Akceptacja Planu Testów**:
    - **Plan Testów** jest dokumentem zarządczym przyjmowanym zgodnie z procedurą odbiorczą przewidzianą w umowie.
    - Brak akceptacji uniemożliwia rozpoczęcie testów funkcjonalnych.

2. **Testowanie zgodności z wymaganiami**:
    - Plan Testów musi obejmować każdy element opisany w wymaganiach.
    - **Zamawiający** może zrezygnować z testowania wybranych elementów.
3. **Dokumentacja użytkowa przed testami**:
    - Dokumentacja powinna być zgodna z testowaną iteracją **Systemu**.

4.4 Wymagania dotyczące stworzenia Projektu Wizualizacji PIOZE [PWI]

Proces Weryfikacji Wizualizacji

W ramach realizacji zadania **Wykonawca** jest zobowiązany do przedstawienia trzech różnych wersji wizualizacji portalu, każda dostosowana do trzech głównych wariantów rozdzielczości. Spośród zaproponowanych wariantów **Zamawiający** wybierze wersję docelową, która będzie rozwijana i wdrażana w dalszych **Etapach Projektu**.

Dokumentacja Projektowa

Ten etap projektu powinien być udokumentowany poprzez:

- Makiety UX/UI dla różnych rozdzielczości.
- Przykłady responsywności oraz animacji przejść.
- Warianty kolorystyczne i wersje tematyczne.
- Dokumentację konfiguracyjną dla wybranych elementów wizualnych.

Wymagania dla tego zadania obejmują:

1. **Ogólne Wymagania Funkcjonalne**
    - Zgodność z **Krajowymi Ramami Interoperacyjności** oraz standardami *WCAG 2.1*, co zapewni dostępność dla osób z niepełnosprawnościami.
2. **Elementy Składowe Wizualizacji**
    - **Rozmieszczenie Komponentów:**
        - Makiety prezentujące układ komponentów na stronie internetowej, uwzględniające intuicyjną nawigację.

- **Wygląd Komponentów:**
  - Propozycje wizualne dla każdego elementu interfejsu, takich jak przyciski, formularze, pola tekstowe i ikony.
- **Kolorystyka i Szata Graficzna:**
  - Opracowanie harmonijnej kolorystyki i spójnego stylu graficznego odpowiadającego tematyce *OZE*.
- **Przejścia i Animacje:**
  - Określenie animacji przejść pomiędzy stronami, elementami interfejsu i interakcji z użytkownikiem.
- **Czcionki i Styl Typograficzny:**
  - Wybór odpowiednich czcionek i stylów typograficznych dla poszczególnych sekcji, gwarantujący czytelność i estetyczny wygląd.

3. **Responsywność i Warianty Rozdzielczości**
   - Trzy różne projekty wizualizacji dostosowane do trzech głównych rozdzielczości ekranowych (np. dla laptopów, monitorów desktopowych, ekranów o wysokiej rozdzielczości).
   - Responsywność, zapewniająca odpowiednie wyświetlanie portalu na różnych wielkościach ekranu.
4. **Personalizacja i Konfigurowalność**
   - Możliwość zmiany wybranych elementów graficznych i tekstowych:
     - Kolorystyka, logo **Zamawiającego**.
     - Stopka z logotypami (z możliwością określenia liczby logotypów).
     - Nazwa i tło nagłówka strony.
   - Konfigurowalne elementy mają być dostępne z poziomu ustawień portalu.
   - System PIOZE powinien umożliwiać konfigurację elementów wizualnych, w tym logotypów oraz komunikatu informującego o finansowaniu projektu z Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) oraz REPowerEU.
5. **Wersje Tematyczne**
   - Wizualizacja wersji stylu żałobnego oraz 4 skórek sezonowych dla każdego z projektów, które będą dostępne przy specjalnych okazjach.
6. **Zgodność z obecnymi portalami Zamawiającego**

- Możliwość wykorzystania najlepszych elementów z aktualnych portali **Zamawiającego**, po konsultacji.
- Zamawiający wymaga, aby platforma PIOZE była zgodna z zasadami oznakowania projektów finansowanych z KPO i REPowerEU, w tym z wytycznymi dotyczącymi umieszczania logotypów oraz komunikatów informacyjnych na stronach internetowych

7. **Logo Systemu**

   W ramach realizacji zadania Wykonawca zobowiązany jest do:

   - **Przygotowania trzech unikalnych propozycji logo dla systemu PIOZE**, z uwzględnieniem ich zastosowania na stronie internetowej oraz w dokumentach związanych z projektem.
   - **Dostosowania każdej propozycji logo do trzech głównych wariantów rozdzielczości**, zapewniając ich optymalne wyświetlanie na różnych urządzeniach i nośnikach.
   - **Przedstawienia Zamawiającemu wszystkich trzech propozycji logo** w formie wizualizacji, umożliwiając wybór najbardziej odpowiedniej wersji.
   - **Rozwijania i wdrożenia wybranego przez Zamawiającego projektu logo** w dalszych etapach realizacji projektu, zgodnie z ustaleniami i harmonogramem.

8. **Dostosowanie do UX i WCAG 2.1**

   - Projektowanie zgodnie z zasadami UX dla zapewnienia intuicyjnego i przyjaznego doświadczenia użytkownika.
   - Pełna zgodność z *WCAG 2.1*, co zapewni dostępność strony dla użytkowników z różnymi rodzajami niepełnosprawności.

4.5. Stworzenie i udostępnienie instalacji rozwojowej i testowej [IDT]

Obowiązkiem **Wykonawcy** jest zapewnienie środowiska rozwojowego i testowego w ramach realizacji projektu.

Środowiska muszą być odseparowane i niezależne, zapewniając:

- Bezpieczne środowisko rozwojowe z ograniczonym dostępem wyłącznie dla zespołu deweloperskiego oraz osób wskazanych przez **Zamawiającego**.
- Środowisko testowe umożliwiające przeprowadzanie testów funkcjonalnych, wydajnościowych i bezpieczeństwa.

Obie instalacje muszą obsługiwać jednocześnie do **200 użytkowników**.

Minimalna przestrzeń dyskowa dla danych aplikacji: **100 GB**.

Szczegółowe wymagania zawarto w kolejnych sekcjach.

4.5.1 Udostępnienie platformy sprzętowo-programowej

4.5.1.I. Ogólne wymagania infrastrukturalne

- Środowisko rozwojowe i testowe musi być zapewnione przez Wykonawcę w ramach realizacji projektu.
- Środowiska muszą być odseparowane i niezależne, zapewniając:
  - Bezpieczne środowisko rozwojowe z ograniczonym dostępem dla zespołu deweloperskiego.
  - Środowisko testowe umożliwiające przeprowadzanie testów funkcjonalnych, wydajnościowych oraz bezpieczeństwa.
- Obie instalacje powinny obsługiwać jednocześnie do **200 użytkowników**.
- Minimalna przestrzeń dyskowa dostępna dla danych aplikacji: **100 GB**.

4.5.1.II. Wymagania dla środowiska rozwojowego

- Zasoby infrastrukturalne:
- - Procesor: Wirtualne *CPU* o wydajności umożliwiającej obsługę prac programistycznych.- Pamięć RAM: Minimum **16 GB**.- Dysk o pojemności min. **50 GB**.
- Funkcjonalność:
  - Możliwość pracy równoległej zespołów programistycznych.
  - Dostępność mechanizmu wersjonowania kodu i bazy danych.
  - Obsługa konteneryzacji i orkiestracji kontenerów (jeśli wymagane).
- Bezpieczeństwo:
  - Dostęp do środowiska wyłącznie przez szyfrowane połączenie (np. *VPN*).
  - Regularne kopie zapasowe danych i konfiguracji, z możliwością ich przywrócenia w ciągu *24 godzin*.

4.5.1.III. Wymagania dla środowiska testowego

- Zasoby infrastrukturalne:
  - Procesor: Wirtualne CPU o wydajności umożliwiającej symulację maksymalnego obciążenia (**200 użytkowników jednocześnie**).
  - Pamięć RAM: Minimum **32 GB**.
  - Dysk o pojemności min. **100 GB**.
- Funkcjonalność:
  - Środowisko umożliwiające testowanie funkcjonalności, wydajności, bezpieczeństwa oraz skalowalności systemu.
  - Możliwość generowania ruchu symulującego obciążenie systemu przez użytkowników.
  - Możliwość testowania scenariuszy awaryjnych (np. symulacja utraty połączenia z bazą danych).

- Bezpieczeństwo:
  - Dostęp do środowiska testowego wyłącznie dla autoryzowanych osób.
  - Zastosowanie certyfikatów szyfrujących transmisję danych.
  - Automatyczne resetowanie środowiska po zakończeniu testów.

4.5.1.IV. Wymagania dotyczące zarządzania i monitorowania

- Automatyzacja:
  - Środowisko powinno umożliwiać automatyczne wdrażanie aplikacji i zarządzanie konfiguracją.
  - Wykorzystanie narzędzi do automatyzacji infrastruktury i procesów testowych.
- Monitorowanie:
  - Środowiska muszą posiadać system monitorowania wydajności, wykorzystania zasobów oraz analizy logów.
  - Funkcjonalność raportowania błędów i alertów w czasie rzeczywistym.
- Zarządzanie środowiskami:
  - Możliwość szybkiego skalowania zasobów w miarę potrzeb.
  - Regularne raportowanie stanu środowisk do **Zamawiającego**.

4.5.1.V. Wymagania dotyczące wydajności

- **Wykonawca** musi zapewnić możliwość przeprowadzania testów obciążeniowych dla **200 jednoczesnych użytkowników**.
- Środowisko powinno umożliwiać testy skalowalności dla obciążenia większego niż założone (**400 użytkowników**).
- Maksymalny czas odpowiedzi systemu pod pełnym obciążeniem nie powinien przekraczać 2 sekund dla kluczowych funkcji.

4.5.1.VI. Wymagania dotyczące kopii zapasowych i odtwarzania

- Regularne wykonywanie kopii zapasowych:
  - Środowisko rozwojowe: co najmniej raz dziennie.
  - Środowisko testowe: przed każdą serią testów.
- Możliwość przywrócenia środowiska z kopii zapasowej w czasie nie dłuższym niż 24 godziny.

4.5.1.VII. Wymagania dotyczące zgodności z przepisami

- **Wykonawca** musi zapewnić zgodność środowisk z obowiązującymi przepisami prawa oraz wymogami regulacyjnymi dotyczącymi ochrony danych osobowych (np. RODO) i cyberbezpieczeństwa.

4.5.1.VIII. Dodatkowe wymagania

- **Wykonawca** musi zapewnić instrukcje użytkowania środowisk oraz wsparcie techniczne dla zespołów **Zamawiającego**.

4.5.2 Instalacja i udostępnienie Oprogramowania Standardowego

W ramach tego zadania należy:

1. Przygotować środowiska pod kątem instalacji oprogramowania standardowego – w tym:
    1. systemu operacyjnego opisanego w sekcji OPS,
    2. bazy danych, o której mowa w sekcji BD,
    3. innego **Oprogramowania Standardowego** dostarczonego przez Wykonawcę w celu realizacji przedmiotu zamówienia.
2. Zainstalować i skonfigurować oprogramowanie zgodnie z wymaganiami funkcjonalnymi oraz regulacjami prawnymi.

4.5.3 Stworzenie kont użytkowników

W ramach tego zadania należy zrealizować:

1. Przygotowanie kont użytkowników dla zespołów deweloperskich i testowych.
2. Zapewnienie odpowiednich uprawnień oraz ich zgodności z polityką bezpieczeństwa.

4.5.4 Utworzenie środowiska rozwojowego i testowego

W ramach tego zadania należy zrealizować następujące zadania:

1. **Konfiguracja środowiska testowego**:
    - Przygotowanie infrastruktury testowej zgodnie z wymaganiami środowiskowymi.
    - Weryfikacja poprawności działania środowiska i jego zgodności z warunkami rzeczywistymi.
    - Zapewnienie dostępu dla zespołu testowego i **Zamawiającego**.
2. **Przygotowanie danych testowych**:
    - Stworzenie, w uzgodnieniu z Zamawiającym, fikcyjnych zbiorów danych reprezentatywnych dla rzeczywistych warunków użytkowania.
    - Uwzględnienie przypadków brzegowych, danych niepełnych i nieprawidłowych.

4.6. Przekazanie licencji Oprogramowania Standardowego [LOS]

Przekazanie licencji do oprogramowania standardowego jest **obowiązkiem Wykonawcy** i musi być zrealizowane zgodnie z następującymi zasadami:

LOS.1. Obowiązek zapewnienia licencji zgodnych z SOPZ

- **Wykonawca** ma obowiązek dostarczenia licencji na **Oprogramowanie Standardowe**, które spełniają wszystkie warunki określone w **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ),** w szczególności opisane w sekcji **AUT**.
- Licencje muszą umożliwiać realizację wymaganych funkcjonalności, takich jak:
    - **OPS** (system operacyjny) – realizujący funkcje opisane w sekcji OPS.
    - **BD** (baza danych) – licencje muszą wspierać pełną funkcjonalność zarządzania i przechowywania danych zgodnie z wymaganiami.
    - **CMS** (moduł zarządzania treścią) – licencje muszą umożliwiać wykorzystanie systemu CMS zgodnie z opisanymi wymaganiami funkcjonalnymi.

LOS.2. Możliwość zawarcia umowy sublicencyjnej

- **Wykonawca** musi zapewnić, że przekazane licencje pozwalają na zawarcie umowy sublicencyjnej, która umożliwi **Wykonawcy** dalsze wykorzystywanie oprogramowania w ramach realizacji projektu.
- Umowa sublicencyjna musi uwzględniać prawa i obowiązki wynikające z wymagań **SOPZ**, w tym w szczególności:
    - Możliwość integracji i modyfikacji oprogramowania.
    - Zachowanie zgodności z wymaganiami opisanymi w sekcji **AUT**.

LOS.4. Wymagania funkcjonalne i techniczne

- Licencje muszą zapewniać realizację wszystkich wymaganych funkcjonalności niezbędnych do stworzenia systemu..

LOS.5. Zgodność z wymaganiami prawnymi i regulacyjnymi

- Wszystkie licencje muszą być zgodne z obowiązującymi przepisami prawa oraz wymogami regulacyjnymi dotyczącymi ochrony danych osobowych (RODO) i cyberbezpieczeństwa.
- Licencje na oprogramowanie muszą uwzględniać wymagania wydajnościowe, skalowalności oraz bezpieczeństwa opisane w **SOPZ**.

LOS.6. Dokumentacja licencyjna

- **Wykonawca** ma obowiązek dostarczyć pełną dokumentację licencyjną, w tym:
    - Rodzaj i zakres licencji.

- Warunki korzystania z oprogramowania.
- Informacje o zgodności licencji z wymaganiami opisanymi w sekcji **AUT**.

LOS.7. Odpowiedzialność Wykonawcy

- **Wykonawca** jest w pełni odpowiedzialny za zapewnienie, że dostarczone licencje spełniają wszystkie wymogi **SOPZ** oraz umożliwiają Zamawiającemu pełne wykorzystanie oprogramowania w dalszym użytkowaniu i rozwoju systemu.

5. Etap II – Stworzenie PIOZE

5.1 Stworzenie oprogramowania Portalu (OPR)

Cel Zadania

Celem zadania jest opracowanie oraz wdrożenie oprogramowania **Portalu Informacyjnego Odnawialnych Źródeł Energii (PIOZE)**, które spełni wymagania funkcjonalne i niefunkcjonalne określone w dokumentacji zamówienia (**SOPZ**). Realizacja obejmuje:

1. **Implementację funkcjonalności opisanych w sekcji 10:**
    - F2A. Część ogólnodostępna PIOZE
    - GEO. Integracja z GeoportalemInfrastruktury Informacji Przestrzennej
    - REJ. Rejestracja w Portalu
    - WRJ. Wyrejestrowanie z Portalu
    - LOG. Logowanie w Portalu
    - PHI. Zabezpieczenia formularza rejestracyjnego oraz logowania
    - UDA. Dane użytkownika
    - L2A. Część PIOZE dostępna po zalogowaniu
    - ENG. Silnik obsługi wniosków
    - SEL. Moduł wyboru formularzy („Formularze”)
    - ORG. Moduł wyboru organów właściwych w danej sprawie
    - FOR. Formularze dostępne w systemie
    - WNI. Wsparcie składania wniosków
    - VAL. Walidacje wprowadzanych danych
    - BA Baza adresowa
    - MON. Monitorowanie odpowiedzi organów oraz uzupełnień
    - MWN. Zarządzanie złożonymi wnioskami („Moje Wnioski”)
    - CER. Zarządzanie certyfikatami („Certyfikaty”)
    - REP. Raportowanie („Raporty”)

- SUP. Pomoc techniczna
- ADM. Funkcje administracyjne.

2. **Spełnienie wymagań niefunkcjonalnych:**
   - Skalowalność, wydajność i wysoką dostępność,
   - Zgodność z *WCAG 2.1* w zakresie dostępności cyfrowej,
   - Zabezpieczenia zgodne z normami bezpieczeństwa (np. *ISO/IEC 27001*).
3. **Zgodność z dokumentacją projektową i standardami kodowania:**
   - Stosowanie wytycznych dokumentacyjnych (*ISO/IEC 25010, ISO/IEC 12207*),
   - Dostarczenie pełnego kodu źródłowego wraz z opisem.

Zadanie będzie odbierane wraz z **Raportem z Testów Oprogramowania [RTO].**

5.2 Integracja systemu [INT]

Cel Zadania

Integracja systemu PIOZE polega na zapewnieniu spójnego i efektywnego przepływu danych między różnymi jego komponentami oraz systemami zewnętrznymi. Głównym celem jest osiągnięcie interoperacyjności i zgodności z wymaganiami funkcjonalnymi oraz prawnymi, przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa i wydajności.

Rodzaje Integracji

INT.1. Z bazami danych publicznych

- **Bazy:** CEIDG, KRS, REGON.
- **Zakres:**
  - Pobieranie danych identyfikacyjnych i rejestracyjnych dla wnioskodawców.
  - Automatyczne weryfikowanie zgodności danych z rejestrami publicznymi.
- **Technologie:**
  - *REST API, SOAP*;
  - Format danych: *JSON, XML*.

- **Bezpieczeństwo:** Uwierzytelnianie i autoryzacja dostępu do API za pomocą certyfikatów cyfrowych lub tokenów (np. OAuth).

INT.2. Z usługami zewnętrznymi

- **Przykłady:** API GIS, platformy do geolokalizacji, mapy terenu.
- **Zakres:**
    - Pobieranie i prezentowanie danych geolokalizacyjnych dotyczących lokalizacji inwestycji w OZE.
    - Wizualizacja map oraz analiza przestrzenna dla potrzeb decyzji środowiskowych.
- **Technologie:**
    - Protokół HTTP/HTTPS, standardy WMS (Web Map Service) i WFS (Web Feature Service).
- **Bezpieczeństwo:** Szyfrowanie transmisji danych (TLS 1.2 i 1.3), ograniczenie dostępu do API na podstawie adresów IP.

..

INT.3. Integracja wewnętrzna między modułami systemu

Zakres:

- Wymiana danych między wydzielonymi modułami systemu, w szczególności modułem CMS, modułem obsługi wniosków oraz modułem raportowania, realizowana w architekturze mikroserwisowej.
- Synchronizacja informacji o użytkownikach, uprawnieniach oraz logach aktywności pomiędzy modułami.
- Automatyczne przekazywanie wyników realizowanych procesów biznesowych między modułami w sposób zapewniający integralność danych i spójność transakcyjną.

Architektura i technologie:

- Integracja realizowana w oparciu o **wewnętrzne API** zgodne z zasadami architektury mikroserwisowej (REST, gRPC lub równoważne).
- Wymiana danych poprzez **asynchroniczne mechanizmy kolejkowania** (np. RabbitMQ, Apache Kafka lub inne równoważne rozwiązanie wskazane przez

Wykonawcę) w celu zapewnienia odporności na przeciążenia oraz wysokiej dostępności komunikacji.

- Obsługiwane formaty danych: **JSON** i **XML**, z preferencją dla struktur opartych na JSON w komunikacji wewnętrznej.

Bezpieczeństwo:

- Weryfikacja integralności i autentyczności przesyłanych danych w komunikacji między modułami.
- Autoryzacja połączeń wewnętrznych na poziomie aplikacji, z wykorzystaniem tokenów bezpieczeństwa lub certyfikatów usługowych.
- Zapewnienie izolacji komunikacyjnej pomiędzy mikroserwisami w celu ograniczenia powierzchni potencjalnych ataków.

Zadanie będzie odbierane wraz z **Raportem z Testów Oprogramowania [RTO].**

5.3. Dokumentacja Systemowa PIOZE [DOS]

Przygotowanie **Dokumentacji Systemowej PIOZE [DOS**] jest jednym z kluczowych elementów realizacji projektu, zapewniającym trwałość, efektywność i zgodność rozwiązania z wymaganiami **Zamawiającego**. Dokumentacja będzie stanowić niezbędny fundament dla utrzymania, rozwoju oraz codziennej eksploatacji systemu, a jej opracowanie jest obowiązkiem **Wykonawcy** wynikającym z postanowień **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ).**

Wykonawca, przygotowując dokumentację systemową, zobowiązany jest do szczegółowego opisania wszystkich aspektów działania systemu, w tym jego architektury, funkcjonalności, wymagań sprzętowych i programowych, a także procesów operacyjnych. Kompleksowa i precyzyjna dokumentacja umożliwi **Zamawiającemu** skuteczne zarządzanie systemem oraz wprowadzanie niezbędnych zmian w przyszłości.

Realizacja tego zadania jest kluczowa dla:

- Zgodności z wymaganiami projektowymi i prawnymi, w tym normami ISO i regulacjami dotyczącymi bezpieczeństwa oraz ochrony danych.
- Zapewnienia interoperacyjności systemu z innymi platformami i systemami, zarówno w ramach PIOZE, jak i w środowisku zewnętrznym.

- Utrzymania wysokiego poziomu bezpieczeństwa i niezawodności, poprzez dokumentację procesów zabezpieczeń, kopii zapasowych i procedur awaryjnych.
- Efektywnego wdrażania i eksploatacji systemu, dzięki szczegółowym instrukcjom użytkownika i administratora.

Tym samym opracowanie dokumentacji systemowej jest nie tylko formalnym wymogiem realizacyjnym, ale także kluczowym narzędziem wspierającym długoterminowe funkcjonowanie systemu **PIOZE**. **Wykonawca** powinien podejść do tego zadania z najwyższą starannością, dbając o jej kompletność, spójność i dostosowanie do potrzeb **Zamawiającego**.

Wymagany zakres dokumentacji systemowej:

a) **Wprowadzenie**:

- Cel dokumentu.
- Zakres działania systemu.
- Krótkie streszczenie rozwiązania.

b) **Diagram kontekstowy i model zachowania**:

- Diagram obrazujący interakcje systemu z otoczeniem.
- Model zachowania opisujący przepływy informacji oraz główne procesy.

c) **Ograniczenia rozwiązania**:

- Techniczne, organizacyjne i regulacyjne.
- Zależności od dostępnych technologii i infrastruktury.

d) **Założenia i zależności**:

- Przyjęte założenia projektowe.
- Kluczowe zależności technologiczne i organizacyjne.

e) **Ogólna charakterystyka użytkowników**:

- Profile użytkowników końcowych i administratorów.
- Wymagania kompetencyjne.

f) **Opis wymagań funkcjonalnych i niefunkcjonalnych**:

- Funkcjonalne: Lista funkcji, które system ma realizować.
- Niefunkcjonalne: Wymagania dotyczące wydajności, dostępności, bezpieczeństwa.

g) **Specyfikacja wymagań funkcjonalnych**:

- Szczegółowe opisy funkcji z podziałem na moduły wraz z odniesieniem do wymagań **SOPZ**.

h) **Specyfikacja wymagań niefunkcjonalnych**:

- Szczegóły dotyczące zgodności ze standardami, wsparcia technicznego, redundancji.

i) **Opis wymagań sprzętowych i programowych**:

- Minimalne i zalecane wymagania sprzętowe oraz środowiskowe.

j) **Specyfikacja wymagań sprzętowych i programowych**:

- Szczegółowy opis konfiguracji sprzętu i oprogramowania.

k) **Opis i specyfikacja interfejsów**:

- Komunikacja między systemami i urządzeniami.

l) **Kody źródłowe**:

- Udostępnienie kodów zgodnie z uzgodnionymi zasadami).

5.4. Raport z testów oprogramowania [RTO]

Cel Raportu

Raport z **Testów Oprogramowania (RTO)** ma na celu dostarczenie **Zamawiającemu** szczegółowej analizy technicznej strony **Systemu PIOZE**, weryfikując możliwość uruchomienia **Systemu** oraz jego podstawowej obsługi, a także potwierdzając poprawność procesu kompilacji kodu. Raport nie koncentruje się na szczegółowej ocenie funkcjonalności, chyba że w trakcie testów zostaną ujawnione istotne niezgodności lub braki w implementacji, które uniemożliwiają prawidłowe działanie **Systemu**.

Zakres Raportu

❖ **Weryfikacja techniczna systemu**

➢ **Możliwość uruchomienia systemu:**

- Sprawdzenie poprawności instalacji i konfiguracji oprogramowania na wskazanej platformie.
- Testy inicjalizacji systemu, w tym uruchamianie głównych modułów.

➢ **Dostęp do systemu:**

- Weryfikacja możliwości zalogowania do systemu z kont użytkownika i administratora.
- Sprawdzenie, czy dostęp do głównych opcji systemu jest możliwy i zgodny z oczekiwanym stanem.

❖ **Proces kompilacji kodu**

➢ **Weryfikacja kompilacji:**

- Analiza możliwości skompilowania kodu źródłowego przy użyciu dostarczonych narzędzi i bibliotek.
- Weryfikacja zgodności kodu z dokumentacją konfiguracyjną (np. środowisko kompilacji, zależności).

➢ **Poprawność kompilacji:**

- Sprawdzenie, czy proces kompilacji kończy się sukcesem bez błędów krytycznych.
- Dokumentacja ewentualnych ostrzeżeń pojawiających się podczas kompilacji.

➢ **Wynik procesu:**

- **Potwierdzenie, że kod źródłowy systemu, dla każdego wydzielonego modułu (mikroserwisu), generuje działające pliki wykonywalne lub kontenery aplikacyjne gotowe do wdrożenia i uruchomienia** w środowisku testowym, produkcyjnym lub chmurowym.
- **Dla architektury mikroserwisowej** standardowym wynikiem procesu budowania powinien być **kontener aplikacyjny** (np. obraz Docker lub równoważny), zawierający:
  - w pełni funkcjonalną instancję mikroserwisu,
  - wszystkie zależności niezbędne do jego samodzielnego uruchomienia,
  - mechanizmy monitorowania stanu (health checks) oraz logowania błędów na poziomie kontenera.
- Kontenery aplikacyjne muszą być budowane w sposób umożliwiający ich łatwe wdrożenie na platformach konteneryzacyjnych (np. Docker, Kubernetes, OpenShift lub równoważnych).
- W przypadku modułów, które nie są mikroserwisami (np. aplikacje pomocnicze lub skrypty migracyjne), dopuszcza się generowanie samodzielnych plików

wykonywalnych (np. .jar, .exe), jednak preferowanym standardem dostarczania oprogramowania pozostają **kontenery aplikacyjne**.

- Wykonawca zobowiązany jest do udostępnienia instrukcji budowania kontenerów oraz zasad ich wersjonowania, zgodnie z dobrą praktyką CI/CD (Continuous Integration / Continuous Deployment).

❖ **Podstawowe testy techniczne**

➢ **Struktura systemu:**

- Sprawdzenie, czy poszczególne moduły systemu są dostępne i możliwe do uruchomienia.

➢ **Interfejs użytkownika:**

- Weryfikacja możliwości wejścia do poszczególnych opcji w systemie.
- Test poprawności wyświetlania głównych ekranów systemu.

➢ **Obsługa podstawowych zdarzeń systemowych:**

- Sprawdzenie, czy system reaguje na standardowe zdarzenia (np. błędne logowanie, brak dostępu do zasobów).

Wymagania dla formy i treści raportu

1. **Struktura raportu:**
   - Sekcja wprowadzająca z opisem zakresu przeprowadzonych testów.
   - Szczegółowy opis procedury testowej:
     - Kroki wykonane podczas testów.
     - Wykorzystane narzędzia i środowiska testowe.
   - Wyniki testów:
     - Status uruchomienia systemu i dostępności modułów.
     - Wyniki kompilacji (sukces, błędy, ostrzeżenia).
   - Lista problemów technicznych:
     - Dokumentacja błędów, które uniemożliwiają poprawne działanie systemu.

- Sugestie poprawek dla wykrytych problemów.

2. **Forma raportu:**
    - Raport musi być przejrzysty, zawierać tabele i diagramy, jeśli to konieczne.
    - Wyniki muszą być jasno oznaczone jako „*Pozytywne*" lub „*Negatywne*" z odniesieniem do poszczególnych testów.

Wymagane narzędzia wspierające proces testowy

Zastosowanie odpowiednich narzędzi wspierających proces testowy, takich jak narzędzia do automatyzacji testów, zarządzania testami, raportowania błędów, testów obciążeniowych oraz analizy kodu, jest wymagane i stanowi integralny element realizacji projektu zgodnie z zapisami **Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ)**.

Wykonawca ma prawo do swobodnego wyboru narzędzi, pod warunkiem, że:

- Wybrane narzędzia spełniają minimalne wymagania funkcjonalne określone w **SOPZ**.
- **Narzędzia muszą zapewniać możliwość realizacji wszystkich wymaganych testów i analiz w sposób zgodny ze standardami jakości określonymi w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ), w szczególności w sekcjach dotyczących wymagań dotyczących testowania (TEST), wymagań bezpieczeństwa (SEC) oraz standardów rozwoju oprogramowania (DEV).**
- Wymagane testy i analizy obejmują w szczególności:
    - testy funkcjonalne,
    - testy niefunkcjonalne (wydajnościowe, bezpieczeństwa, dostępności, skalowalności),
    - testy integracyjne między modułami systemu,
    - testy akceptacyjne (UAT),
    - analizy jakości kodu źródłowego (np. pokrycie kodu testami, zgodność ze standardami kodowania),
    - analizy bezpieczeństwa aplikacji i komunikacji (np. SAST – Static Application Security Testing, DAST – Dynamic Application Security Testing).
- Standardy jakości odnoszą się do:
    - **dokumentu SOPZ** i zawartych w nim wymagań,

- **powszechnie przyjętych dobrych praktyk branżowych** takich jak OWASP, ISO/IEC 25010 (model jakości systemów i oprogramowania) oraz ISO/IEC 27001 (bezpieczeństwo informacji),
- **zasad definiowanych przez instytucje certyfikujące lub nadzorujące jakość oprogramowania** (np. ISTQB dla testów oprogramowania).

- **Zamawiający** ma zapewniony pełny dostęp do zapisów, wyników testów, zgłoszeń błędów oraz raportów generowanych w wybranych narzędziach.

Ponadto, **Wykonawca** jest zobowiązany:

1. **Udostępnić Zamawiającemu pełny dostęp administracyjny lub równoważny** do wybranego narzędzia, umożliwiający przeglądanie, eksportowanie oraz archiwizację danych.
2. **Przekazać szczegółową instrukcję obsługi narzędzi**, dostosowaną do poziomu wiedzy technicznej **Zamawiającego**, umożliwiającą samodzielne korzystanie z dostarczonych danych.
3. **Zapewnić zgodność danych zgromadzonych w narzędziach z wymaganiami dotyczącymi ochrony informacji**, w tym w zakresie bezpieczeństwa i przechowywania danych.

Zastosowanie tych narzędzi jest nie tylko formalnym wymogiem realizacji projektu, ale również niezbędnym elementem zapewnienia jakości i przejrzystości procesu testowego. Brak wykorzystania odpowiednich narzędzi lub niewypełnienie obowiązku dostępu **Zamawiającego** do wyników testów może skutkować brakiem odbioru realizacji zadania.

1. Narzędzia do kompilacji

Przykłady: GCC, MSBuild, Maven (wybór Wykonawcy)
Narzędzia będą służyć do przekształcenia kodu źródłowego w działające aplikacje, zapewniając zgodność ze środowiskiem produkcyjnym i testowym.

- **Minimalny zakres funkcjonalności wybranego narzędzia:**
  - Obsługa różnych języków programowania zgodnych z technologią używaną w projekcie (np. Java, C#, C++).
  - Możliwość definiowania zależności projektowych (np. poprzez pliki konfiguracyjne).
  - Weryfikacja kompletności i poprawności kodu podczas procesu kompilacji.

- Automatyczne generowanie plików binarnych, bibliotek lub kontenerów aplikacyjnych gotowych do wdrożenia.
- Obsługa wielu środowisk docelowych (np. testowe, developerskie, produkcyjne).
- Generowanie szczegółowych logów z procesu kompilacji, w tym błędów i ostrzeżeń.

2. Narzędzia do analizy kodu

Przykłady: SonarQube (wybór Wykonawcy)
Narzędzia będą umożliwiać statyczną analizę kodu w celu identyfikacji potencjalnych błędów, problemów jakościowych i zagrożeń bezpieczeństwa.

- **Minimalny zakres funkcjonalności wybranego narzędzia:**
  - Analiza kodu pod kątem zgodności ze standardami programowania i najlepszymi praktykami.
  - Identyfikacja błędów i podatności bezpieczeństwa, takich jak:
    - Problemy z obsługą pamięci.
    - Niebezpieczne funkcje lub fragmenty kodu.
    - Nieefektywne konstrukcje kodu.
  - Ocena jakości kodu poprzez wskaźniki, takie jak:
    - Pokrycie testami jednostkowymi.
    - Złożoność cyklomatyczna (złożoność logiki kodu).
    - Dług techniczny (oszacowanie czasu potrzebnego na usunięcie problemów w kodzie).
  - Tworzenie raportów jakości kodu z priorytetyzacją problemów.
  - Możliwość integracji z narzędziami CI/CD w celu automatyzacji procesu analizy.
  - Sugerowanie poprawek i udostępnienie szczegółowych wyjaśnień dotyczących wykrytych problemów.

Ponadto wymagane jest zastosowanie

- Narzędzia do zarządzania testami
- Narzędzia do raportowania błędów

Minimalne wymagania w tym zakresie są zawarte przy okazji produktu RTS.

Wymagania proceduralne

1. **Dla narzędzi do kompilacji:**
    - **Wykonawca** musi zapewnić dostarczenie dokumentacji opisującej proces kompilacji, w tym wymagania dotyczące środowiska i zależności projektowych.
    - Narzędzia muszą umożliwiać łatwe odtworzenie procesu kompilacji przez **Zamawiającego**.
2. **Dla narzędzi do analizy kodu:**
    - **Wykonawca** jest odpowiedzialny za regularną analizę kodu w trakcie realizacji projektu oraz dostarczenie raportów z każdej iteracji analizy.
    - Analiza kodu musi być przeprowadzana w sposób zgodny z wymaganiami bezpieczeństwa i jakości zawartymi w **SOPZ**.

Wyniki Oczekiwane

- Potwierdzenie, że system można uruchomić i jest dostępny dla użytkowników.
- Weryfikacja, że proces kompilacji kończy się sukcesem i generuje działający system.
- Dokumentacja wszelkich problemów technicznych, które wymagają poprawy przed przejściem do szczegółowej weryfikacji funkcjonalnej.

6. Etap III – Konfiguracja systemu

6.1 Konfiguracja Portalu (KNF)

Cel Zadania

Konfiguracja Portalu (KNF) obejmuje przygotowanie systemu **PIOZE** do pełnej operacyjności, w tym wdrożenie procedur uruchomienia, integracji z systemami zewnętrznymi, oraz skonfigurowanie kluczowych elementów, takich jak formularze OZE i procesy zgodne z dokumentacją zawartą w załącznikach do **SOPZ**. **Wykonawca** jest

zobowiązany do zapewnienia wsparcia merytorycznego i proceduralnego w przypadku konieczności realizacji integracji z innymi podmiotami, np. z Węzłem Krajowym.

W ramach konfiguracji należy wykonać działania opisane w sekcjach INIT oraz INIT-ADDR.

Zakres Zadania

1. Procedury uruchomienia

- Skonfigurowanie środowiska testowego zgodnie z wymaganiami infrastrukturalnymi.
- Instalacja i konfiguracja finalnych komponentów systemu (moduły, bazy danych, środowisko aplikacyjne).
- Przeprowadzenie testów startowych, które potwierdzą poprawność konfiguracji i gotowość systemu do pracy.
- Opracowanie dokumentacji uruchomieniowej, zawierającej szczegółowy opis kroków konfiguracji oraz weryfikacji poprawności działania.

2. Konfiguracja integracji

- **Zakres:**
  - Ustanowienie i konfiguracja testowych połączeń z systemami zewnętrznymi, takimi jak Węzeł Krajowy, CEIDG, KRS czy API GIS.
  - Implementacja procedur wymiany danych w oparciu o standardy wymienione w **SOPZ** (np. *REST API, SOAP, JSON, XML*).
- **Wsparcie proceduralne i merytoryczne:**
  - Współpraca z podmiotami zewnętrznymi w celu zapewnienia skutecznej integracji.
  - Opracowanie szczegółowych instrukcji dotyczących procedur integracyjnych.
  - Konsultacje i bieżąca pomoc techniczna w zakresie wymaganej konfiguracji i diagnostyki.
- **Testy integracyjne:**
  - Przeprowadzenie testów połączeń i wymiany danych z systemami zewnętrznymi.

- Weryfikacja poprawności i kompletności przesyłanych danych.

3. Konfiguracja formularzy OZE

- **Zakres:**
  - Przygotowanie i dostosowanie formularzy do obsługi wniosków związanych z odnawialnymi źródłami energii (**OZE**).
  - Implementacja formularzy zgodnie z wymaganiami funkcjonalnymi i prawnymi zawartymi w załącznikach do **SOPZ**.
- **Funkcjonalność formularzy:**
  - Walidacja danych wejściowych.
  - Automatyczne uzupełnianie danych na podstawie informacji pobieranych z systemów zewnętrznych.
  - Obsługa załączników w formatach określonych w **SOPZ** (np. *PDF*, *JPEG*).
- **Testy poprawności:**
  - Weryfikacja, czy formularze działają zgodnie z opisanymi procesami i spełniają wszystkie wymagania.

4. Konfiguracja procedur zgodnie z SOPZ

- Implementacja procesów obsługi wniosków, ścieżek akceptacyjnych oraz przepływu pracy (*workflow*) związanego z obsługą danych **OZE**.
- Ustanowienie harmonogramu automatycznych zadań, takich jak:
  - Archiwizacja danych.
  - Generowanie raportów i powiadomień.
- Zapewnienie zgodności procedur z wymaganiami prawnymi i funkcjonalnymi.

Produkty Zadania

1. **Konfigurowalny Portal PIOZE**
   - Gotowy do obsługi wniosków **OZE** oraz współpracy z systemami zewnętrznymi.
   - Wszystkie kluczowe funkcjonalności zgodne z **SOPZ**.

2. **Dokumentacja konfiguracji**
    - Szczegółowe instrukcje dotyczące przeprowadzonych konfiguracji - patrz również **Dokumentacja Eksploatacyjna [DOE].**
    - Procedury zarządzania i aktualizacji ustawień portalu.
3. **Testy akceptacyjne**
    - Wyniki testów uruchomieniowych i integracyjnych potwierdzające poprawność działania systemu – patrz **Raport z Testów Systemu [RTS].**
4. **Wsparcie techniczne i merytoryczne**
    - Dostosowane do specyficznych potrzeb związanych z integracją i konfiguracją systemu.

Wymagania Proceduralne

- Realizacja konfiguracji zgodnie z harmonogramem projektu.
- Bieżące konsultacje z **Zamawiającym** w zakresie wprowadzanych ustawień.
- Dostarczenie wszystkich wyników testów i dokumentacji w formie zatwierdzonej przez **Zamawiającego**.

6.2. Dokumentacja eksploatacyjna PIOZE [DOE]

Dokumentacja Eksploatacyjna PIOZE [DOE] stanowi kluczowy element **Projektu**, który zapewnia **Zamawiającemu** możliwość skutecznego zarządzania, utrzymania oraz codziennej eksploatacji systemu. Opracowanie tej dokumentacji jest bezwzględnym obowiązkiem **Wykonawcy**, który ponosi pełną odpowiedzialność za jej zgodność z wymaganiami zawartymi w **SOPZ**, kompletność oraz jakość.

Przygotowanie **Dokumentacji Eksploatacyjnej** należy do odpowiedzialności **Wykonawcy**, który zobowiązany jest:

1. Dostarczyć dokumentację w formie zgodnej z standardami jakości wynikającymi z zapisów niniejszej SOPZ, zapewniając jej spójność, przejrzystość i zrozumiałość dla użytkowników.

2. Uwzględnić w dokumentacji wszystkie procedury niezbędne do utrzymania **Systemu**, takie jak zarządzanie użytkownikami, wykonywanie kopii zapasowych, przywracanie funkcjonalności po awarii oraz zabezpieczanie danych.

3. Zagwarantować zgodność dokumentacji z obowiązującymi przepisami prawa i normami technicznymi, w szczególności w zakresie ochrony danych osobowych oraz bezpieczeństwa informacji.

4. Zapewnić aktualność dokumentacji w okresie gwarancji, aby odzwierciedlała wszelkie zmiany wprowadzone w **Systemie** przez **Wykonawcę**.

Wykonawca, wytwarzając **Dokumentację Eksploatacyjną**, musi zadbać, aby była ona kompletna i zgodna z rzeczywistością **Systemu PIOZE**. Niedostarczenie lub nieodpowiednie wykonanie tego zadania obciąża w całości Wykonawcę, zarówno w zakresie konsekwencji finansowych, jak i merytorycznych, wynikających z braku możliwości prawidłowego korzystania z systemu przez **Zamawiającego**.

Dokumentacja Eksploatacyjna jest nie tylko formalnym wymogiem realizacji Projektu, ale również podstawowym narzędziem wspierającym efektywne działanie systemu i minimalizującym ryzyko operacyjne, za co pełną odpowiedzialność ponosi **Wykonawca**.

Zakres dokumentu:

1. **Instrukcja instalacji:**
    - Szczegółowy opis procesu instalacji systemu **PIOZE** oraz jego komponentów, obejmujący:
        - Wymagania sprzętowe i programowe.
        - Przygotowanie środowiska (serwery, bazy danych, integracje).
        - Kroki instalacyjne z podziałem na etapy (np. przygotowanie środowiska, instalacja aplikacji, konfiguracja modułów).
        - Testy poprawności instalacji i weryfikacja uruchomienia.
2. **Procedury administracyjne**:
    - Zarządzanie użytkownikami, logami, aktualizacjami.
3. **Procedury zabezpieczeń (backup)**:
    - Harmonogram kopii zapasowych, przywracanie danych.

4. **Procedury awaryjne**:
    - Postępowanie w przypadku awarii.

Wymagane elementy każdej procedury:

1. Identyfikator i nazwa procedury.
2. Rodzaj procedury.
3. Data utworzenia i wersja.
4. Cel i zakres procedury.
5. Warunki uruchomienia i oczekiwany rezultat.
6. Dane osób odpowiedzialnych za opracowanie i zatwierdzenie.
7. Opis działań krok po kroku, z podziałem na role.

6.3. Instrukcja użytkownika wewnętrznego PIOZE [INS]

Przygotowanie szczegółowej i kompletniej **Instrukcji Użytkownika Wewnętrznego PIOZE** jest kluczowym obowiązkiem Wykonawcy. **Wykonawca** ponosi pełną odpowiedzialność za stworzenie instrukcji, która umożliwi Zamawiającemu samodzielne i efektywne korzystanie z systemu, w tym jego konfigurację, zarządzanie oraz rozwiązywanie problemów.

Instrukcja musi być dostosowana do potrzeb użytkowników systemu, intuicyjna i zawierająca szczegółowe kroki umożliwiające:

- Samodzielne przeprowadzanie instalacji oraz konfiguracji procedur i formularzy OZE.
- Zarządzanie codziennymi operacjami w systemie.
- Diagnozowanie i rozwiązywanie problemów technicznych bez potrzeby angażowania wsparcia zewnętrznego.

Wykonawca jest zobowiązany do dostarczenia instrukcji w formie zgodnej z najwyższymi standardami jakości, a jej brak lub niedostateczna jakość będzie obciążać go odpowiedzialnością, zarówno pod względem merytorycznym, jak i finansowym. Dodatkowo, przygotowana instrukcja musi uwzględniać materiały wizualne, przykłady i wskazówki, które zapewnią Zamawiającemu pełną kontrolę nad systemem PIOZE i jego eksploatacją.

Wykonawca odpowiada za to, by instrukcja była nie tylko dokumentem technicznym, ale także praktycznym narzędziem wspierającym codzienną pracę Zamawiającego.

Zakres dokumentu:

1. **Instrukcja obsługi:**
    - Kroki wykonywania codziennych zadań, takich jak:
        - Zarządzanie użytkownikami: tworzenie, edycja, przypisywanie ról.
        - Konfiguracja formularzy **OZE**:
            - Tworzenie i edycja formularzy.
            - Dodawanie walidacji danych oraz mapowanie pól.
            - Testowanie i publikacja formularzy.
        - Konfiguracja procedur:
            - Tworzenie nowych procesów workflow.
            - Edycja i zarządzanie istniejącymi procedurami.
            - Ustalanie harmonogramów automatycznych zadań (np. generowanie raportów, archiwizacja).
    - Obsługa podstawowych funkcji systemu:
        - Zarządzanie treściami w CMS.
        - Generowanie i pobieranie raportów.
        - Monitorowanie i logowanie działań systemu.
2. **FAQ i rozwiązywanie problemów:**
    - Lista najczęściej występujących problemów, takich jak:
        - Problemy z logowaniem (np. brak uprawnień, błędne hasło).
        - Problemy z integracją (np. błędy połączenia z Węzłem Krajowym lub innymi systemami).
        - Problemy techniczne podczas konfiguracji formularzy lub procedur.

- Propozycje rozwiązań krok po kroku, w tym:
  - Diagnostyka błędów.
  - Procedury eskalacji problemów do wsparcia technicznego.
  - Wskazówki dotyczące korzystania z funkcji systemu.

3. **Materiały wizualne:**
   - Zrzuty ekranu i diagramy ilustrujące:
     - Kroki instalacji i konfiguracji.
     - Tworzenie formularzy i procedur.
     - Przykładowe wyniki działań (np. raporty, zapisane konfiguracje).
   - Diagramy przepływów pracy (workflow) dla wyjaśnienia, jak system obsługuje procedury OZE.
   - Przykładowe błędy i ich rozwiązania wizualnie przedstawione.

6.4. Raport z testów systemu [RTS]

Raport z Testów Systemu (RTS) jest jednym z kluczowych elementów dokumentacji potwierdzających jakość, stabilność i gotowość **Systemu PIOZE** do eksploatacji. Opracowanie tego raportu jest obowiązkiem **Wykonawcy**, który ponosi pełną odpowiedzialność za przeprowadzenie testów oraz precyzyjne udokumentowanie ich wyników.

Celem raportu jest dostarczenie **Zamawiającemu** szczegółowych informacji o przeprowadzonych testach, które weryfikują działanie systemu w różnych scenariuszach, w tym testy jednostkowe, integracyjne, wydajnościowe oraz bezpieczeństwa.

Raport ma potwierdzić, że system:

- Spełnia wymagania funkcjonalne i niefunkcjonalne określone w **SOPZ**.
- Jest zgodny z przyjętymi standardami technicznymi i prawnymi.
- Działa stabilnie, wydajnie oraz bez krytycznych błędów uniemożliwiających jego użytkowanie.

Wyniki raportu są nie tylko dowodem poprawności działania systemu, ale także podstawą do jego akceptacji przez **Zamawiającego**. **Wykonawca ponosi odpowiedzialność za**

kompleksowe przygotowanie raportu oraz rzetelne przedstawienie wyników testów, uwzględniając wszystkie zauważone problemy, ich klasyfikację oraz propozycje rozwiązań.

Raport **RTS** stanowi gwarancję, że system **PIOZE** został szczegółowo przetestowany i jest gotowy do uruchomienia w środowisku produkcyjnym, zgodnie z wymaganiami **Zamawiającego**.

1. Przeprowadzenie testów

1. **Testy jednostkowe** (modułów i funkcji):
    - Weryfikacja poprawności działania każdego komponentu zgodnie z jego specyfikacją.
    - Testy przeprowadzane w izolacji od innych modułów.
2. **Testy integracyjne**:
    - Sprawdzenie współdziałania pomiędzy modułami systemu.
    - Weryfikacja poprawności przepływu danych między komponentami.
3. **Testy funkcjonalne**:
    - Przeprowadzanie scenariuszy testowych opartych na wymaganiach funkcjonalnych.
    - Sprawdzanie zgodności wyników z kryteriami akceptacyjnymi.
4. **Testy niefunkcjonalne**:
    - **Bezpieczeństwa**: ocena podatności systemu na zagrożenia, testy penetracyjne.
    - **Wydajnościowe**: testy obciążeniowe, sprawdzanie czasu odpowiedzi i stabilności.
    - **Ergonomii i UX**: ocena intuicyjności, łatwości obsługi i zgodności z *WCAG 2.1*.
5. **Rejestracja wyników**:
    - Dokumentowanie wyników każdej iteracji testów, w tym sukcesów i niezgodności.
    - Użycie narzędzi do śledzenia zgłoszeń błędów (np. JIRA, TestLink).
6. **Weryfikacja błędów**:

- Analiza zgłoszonych błędów i ich klasyfikacja (krytyczne, poważne, kosmetyczne).

2. Iteracyjne testowanie i weryfikacja poprawek

1. **Testy regresyjne**:
   - Powtórne testowanie naprawionych funkcjonalności.
   - Weryfikacja, czy wprowadzone poprawki nie wpłynęły negatywnie na inne obszary systemu.
2. **Testy akceptacyjne**:
   - Końcowe testy przeprowadzane wspólnie z **Zamawiającym**.
   - Ocena, czy system spełnia wszystkie wymagania i jest gotowy do wdrożenia.

3. Dokumentowanie wyników testów

1. **Raporty z testów**:
   - Opis przeprowadzonych testów, w tym:
     - Lista przetestowanych modułów.
     - Wyniki testów (sukces/niespełnienie kryteriów).
     - Identyfikacja błędów i niezgodności.
     - Wnioski i rekomendacje.
   - Raporty są przekazywane do **Zamawiającego** do akceptacji.
2. **Podsumowanie procesu testowego**:
   - Opracowanie zbiorczego raportu zawierającego wszystkie przeprowadzone testy.
   - Wskazanie gotowości systemu do wdrożenia na **Środowisku Produkcyjnym.**

4. Uzgodnienia i akceptacja wyników

1. **Przekazanie raportów Zamawiającemu**:
   - Przesłanie końcowego raportu z testów w celu akceptacji.
2. **Uwzględnienie uwag Zamawiającego**:
   - Wprowadzenie ewentualnych poprawek lub dodatkowych testów.
3. **Zatwierdzenie końcowe**:

- **Uzyskanie akceptacji raportu testowego jako formalnego zamknięcia procesu testowego, przy założeniu, że raport nie wskazuje na nieprawidłowości uniemożliwiające spełnienie wymagań określonych w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ).**
- **W przypadku wykrycia nieprawidłowości** opisanych w raporcie testowym, które wpływają na zgodność systemu z wymaganiami funkcjonalnymi lub niefunkcjonalnymi, Wykonawca jest zobowiązany do:
    1. usunięcia wykrytych błędów,
    2. ponownego wykonania testów w zakresie objętym poprawkami,
    3. aktualizacji raportu testowego uwzględniającej wyniki ponownego testowania.
- Proces zatwierdzania raportu testowego **może być powtarzany wielokrotnie**, do momentu uzyskania przez Zamawiającego pełnej akceptacji wyników testów i potwierdzenia zgodności systemu z wymaganiami określonymi w SOPZ.
- Ostateczne zatwierdzenie raportu zamyka formalnie proces testowy i umożliwia przejście do kolejnych etapów realizacji projektu.
- Uzyskanie akceptacji raportu jako formalnego zamknięcia procesu testowego.

5. Wymagane narzędzia wspierające proces testowy

Patrz również uwaga ogólna co do wymogu zastosowania narzędzi wspomagających proces testowania w opisie produktu **RTO**.

1. Narzędzia do automatyzacji testów

Przykłady: Selenium, JUnit (wybór Wykonawcy)
Narzędzia będą umożliwiać automatyczne wykonywanie testów w celu weryfikacji poprawności działania systemu na różnych poziomach:

- **Testy jednostkowe:** Sprawdzanie poprawności działania poszczególnych modułów lub funkcji systemu.
- **Testy integracyjne:** Weryfikacja współdziałania między różnymi modułami lub komponentami systemu.
- **Minimalny zakres funkcjonalności wybranego narzędzia:**
    - Tworzenie i uruchamianie automatycznych scenariuszy testowych.
    - Rejestrowanie wyników testów oraz porównywanie z oczekiwanymi rezultatami.

- Obsługa różnych środowisk i przeglądarek.
- Możliwość integracji z narzędziami do raportowania i zarządzania testami.

2. Narzędzia do zarządzania testami

Przykłady: TestLink, Zephyr (wybór Wykonawcy)
Narzędzia te służą do centralnego zarządzania procesem testowania i dokumentowania postępów testów:

- **Minimalny zakres funkcjonalności wybranego narzędzia:**
  - Tworzenie, organizowanie i zarządzanie przypadkami testowymi.
  - Przypisywanie przypadków testowych do testerów.
  - Monitorowanie postępów testów i raportowanie stanu realizacji.
  - Generowanie raportów dotyczących pokrycia testowego oraz statusu testów.
  - Integracja z narzędziami do automatyzacji testów oraz raportowania błędów.

3. Narzędzia do raportowania błędów

Przykłady: JIRA, Bugzilla (wybór Wykonawcy)
Narzędzia te umożliwiają zgłaszanie, śledzenie i zarządzanie błędami oraz problemami wykrytymi podczas testów:

- **Minimalny zakres funkcjonalności wybranego narzędzia:**
  - Rejestrowanie zgłoszeń błędów z opisem, priorytetem i kategorią.
  - Śledzenie statusu błędów od zgłoszenia do rozwiązania.
  - Współpraca między członkami zespołu (przypisywanie błędów, komentarze, historia zmian).
  - Generowanie raportów na temat zgłoszonych, otwartych i zamkniętych błędów.
  - Integracja z narzędziami do zarządzania testami oraz automatyzacji testów.

4. Narzędzia do testów obciążeniowych i wydajnościowych

Przykłady: JMeter, LoadRunner (wybór Wykonawcy)
Narzędzia te służą do symulowania obciążeń systemu i oceny jego wydajności:

- **Minimalny zakres funkcjonalności wybranego narzędzia:**

- Tworzenie scenariuszy testowych do symulacji obciążeń użytkowników (np. jednoczesne logowanie, wyszukiwanie danych).
- Monitorowanie wydajności systemu (czas odpowiedzi, przepustowość, stabilność).
- Analiza zachowania systemu pod dużym obciążeniem (np. maksymalna liczba jednoczesnych użytkowników).
- Generowanie raportów i wykresów przedstawiających wyniki testów obciążeniowych.
- Możliwość integracji z narzędziami do monitorowania i analizy systemu.

5. Narzędzia do testowania bezpieczeństwa

Przykłady: OWASP ZAP, Burp Suite (wybór Wykonawcy)
Narzędzia te są używane do identyfikacji potencjalnych luk w zabezpieczeniach systemu:

- **Minimalny zakres funkcjonalności wybranego narzędzia:**
  - Skanowanie aplikacji pod kątem znanych podatności (np. SQL Injection, Cross-Site Scripting).
  - Analiza ruchu sieciowego między klientem a serwerem.
  - Testowanie mechanizmów uwierzytelniania i autoryzacji.
  - Generowanie raportów z wykrytymi podatnościami, wraz z ich klasyfikacją i sugestiami rozwiązań.
  - Możliwość symulacji ataków w celu weryfikacji odporności systemu na zagrożenia.

6. Oczekiwane rezultaty

- System spełnia wszystkie wymagania funkcjonalne i pozafunkcjonalne.
- Testy zakończone bez krytycznych błędów uniemożliwiających użytkowanie.
- Raport z testów zaakceptowany przez **Zamawiającego** bez uwag.

7. Etap IV – Szkolenia użytkowników [SZK]

Szkolenia Użytkowników [SZK] stanowią kluczowy element wdrożenia systemu PIOZE, mający na celu zapewnienie, że wszyscy użytkownicy, zarówno końcowi, jak i administratorzy, będą w pełni przygotowani do efektywnego korzystania z jego

funkcjonalności. Realizacja tego etapu jest obowiązkiem Wykonawcy, który ponosi pełną odpowiedzialność za jakość, zakres i skuteczność szkoleń.

Głównym celem szkoleń jest przekazanie użytkownikom wiedzy teoretycznej i praktycznej, umożliwiającej im:

- Samodzielną obsługę systemu, w tym wykonywanie codziennych operacji i procedur.
- Konfigurację formularzy i procedur związanych z obsługą OZE, zgodnie z wymaganiami **SOPZ**.
- Rozwiązywanie podstawowych problemów technicznych i operacyjnych.
- Skuteczne administrowanie systemem, w tym zarządzanie użytkownikami, raportami i integracjami z systemami zewnętrznymi.

Szkolenia powinny być dostosowane do poziomu wiedzy i potrzeb różnych grup użytkowników, z uwzględnieniem ich ról i obowiązków w systemie. **Wykonawca** zobowiązany jest do dostarczenia materiałów szkoleniowych, w tym podręczników, prezentacji, zrzutów ekranów oraz dostępu do wersji testowej systemu na czas trwania szkoleń.

Produkt SZK jest niezbędny, aby zapewnić płynne przejście systemu PIOZE z fazy wdrożeniowej do codziennej eksploatacji. Sukces tego etapu będzie miał bezpośredni wpływ na efektywność działania systemu oraz poziom satysfakcji użytkowników. **Wykonawca ponosi pełną odpowiedzialność za realizację szkoleń zgodnie z harmonogramem, ich jakość.**

7.1. Ogólne zasady

1. Forma szkoleń: Szkolenia prowadzone będą w formie zdalnej (on-line) za pomocą narzędzi do wideokonferencji oraz w systemie stacjonarnym w zależności od grupy docelowej. Podstawową formą jest forma zdalna, chyba, że **Wykonawca** złoży wniosek o formę stacjonarną.
2. Język szkoleń: Wszystkie szkolenia będą przeprowadzane w języku polskim.
3. Materiały szkoleniowe:
    - Dostarczane w wersji elektronicznej.
    - Obejmują FAQ, manual użytkownika oraz materiały uzupełniające.
    - Uczestnicy otrzymają materiały co najmniej na 3 dni robocze przed terminem rozpoczęcia szkoleń.

7.2. Cele szkoleń

1. Przygotowanie teoretyczne i praktyczne użytkowników oraz administratorów do obsługi systemu **PIOZE**.
2. Umożliwienie samodzielnej konfiguracji i zarządzania systemem przez przeszkolone osoby.
3. Opracowanie kompetencji umożliwiających merytoryczne wsparcie pozostałych pracowników.

7.3 Harmonogram

1. **Wykonawca zobowiązany jest do ustalenia szczegółowego harmonogramu szkoleń w porozumieniu z Zamawiającym**:
    - Termin i lokalizacja szkoleń (on-line/stacjonarne).
    - Lista uczestników.
    - Imię i nazwisko trenera.
    - Szczegółowy program szkolenia, podział na bloki tematyczne.
2. Harmonogram musi być przedstawiony do akceptacji **Zamawiającemu** na 10 dni roboczych przed planowaną realizacją szkoleń. **Zamawiający** zatwierdza lub wnosi uwagi w terminie 3 dni roboczych. W przypadku uwag, **Wykonawca** ma 2 dni na wprowadzenie poprawek.

7.4. Grupy szkoleniowe

1. **Szkolenia dla użytkowników wewnętrznych (do 15 osób)**:
    - Grupy do 15 uczestników.
    - Szkolenie co najmniej jednodniowe (co najmniej 8 godzin zajęć) z dwiema przerwami 20-minutowymi i jedną 40-minutową.

    Cel szkoleń:

    - Zapoznanie użytkowników z funkcjonalnościami portalu PIOZE.
    - Nauka korzystania z modułów obsługi wniosków, formularzy i zarządzania treścią.
    - Wyjaśnienie zasad pracy z danymi oraz korzystania z systemu zgodnie z procedurami.
    - Bloki tematyczne:

      Wprowadzenie do portalu PIOZE:

- Podstawowe informacje o systemie i jego roli.
- Struktura systemu i zasady działania.

Moduł zarządzania wnioskami:

- Składanie i przetwarzanie wniosków.
- Śledzenie statusu wniosków w module „Moje Wnioski".
- Zasady komunikacji z użytkownikami końcowymi.

Obsługa formularzy i walidacja danych:

- Tworzenie i edycja formularzy w portalu.
- Zasady walidacji i weryfikacji danych wprowadzanych przez użytkowników.

Raportowanie i analityka:

- Generowanie raportów z systemu.
- Wykorzystanie danych statystycznych dla celów operacyjnych.

Bezpieczeństwo i ochrona danych:

- Podstawy ochrony danych osobowych (zgodność z RODO).
- Bezpieczne korzystanie z systemu.

- Część praktyczna (warsztaty): minimum 5 godzin (w ramach 8 godzin szkolenia).

2. **Szkolenia dla administratorów**:
   - Grupy maksymalnie 5-osobowe.
   - Szkolenie co najmniej jednodniowe (co najmniej 8 godzin zajęć) z dwiema przerwami 20-minutowymi i jedną 40-minutową.

Cel szkoleń:

- Przygotowanie administratorów do zarządzania i utrzymania systemu.
- Nauka konfiguracji, monitorowania oraz integracji systemu PIOZE.
- Rozwiązywanie problemów i zapewnianie bezpieczeństwa systemu.

- Bloki tematyczne:

Podstawy zarządzania systemem PIOZE:

- Struktura i architektura systemu.
- Role i uprawnienia administratorów.

Konfiguracja i utrzymanie systemu:

- Tworzenie i zarządzanie użytkownikami.
- Zarządzanie modułami i funkcjonalnościami portalu.

Monitorowanie i diagnostyka systemu:

- Korzystanie z narzędzi monitorowania wydajności i bezpieczeństwa.
- Analiza logów systemowych.

Integracja systemu z zewnętrznymi platformami:

- **Zarządzanie i integracja** platformami publicznymi i systemami zewnętrznymi, w szczególności:
    - ePUAP (elektroniczna Platforma Usług Administracji Publicznej),
    - eDoręczeniami,
    - Geoportalem Infrastruktury Informacji Przestrzennej,
    - oraz innymi wskazanymi w Specyfikacji Opisu Przedmiotu Zamówienia (SOPZ).
- **Weryfikacja i monitorowanie stanu integracji** (logi połączeń, informacje o błędach komunikacji) oraz omówienie podstawowych narzędzi diagnostycznych dostępnych z poziomu GUI.

Backup i disaster recovery:

- Tworzenie kopii zapasowych.
- Procedury odzyskiwania systemu po awarii.

Zarządzanie bezpieczeństwem systemu:

- Zasady uwierzytelniania i autoryzacji użytkowników.
- Ochrona przed zagrożeniami cyberbezpieczeństwa.

- Część praktyczna (warsztaty): minimum 5 godzin (w ramach 8 godzin szkolenia).

7.5. Wymagania techniczne i organizacyjne

1. Platforma szkoleniowa: **Wykonawca** zapewnia instancję testową systemu PIOZE oraz platformę techniczną do przeprowadzania szkoleń na odległość.
2. Certyfikaty uczestnictwa: Po zakończeniu szkolenia uczestnicy otrzymują certyfikaty z wyszczególnieniem zakresu szkolenia oraz informacją o współfinansowaniu UE.
3. Ankiety ewaluacyjne:
    - Wypełniane przez uczestników po każdym szkoleniu.
    - Minimalna ocena dla uznania szkolenia za zakończone sukcesem: 3,5 pkt na 5 pkt.
4. Materiały szkoleniowe:

    Materiały Szkoleniowe muszą być dostarczone w formie elektronicznej w formacie możliwym do użycia na platformie *Moodle* tj:

    - Dokumenty tekstowe: *PDF, DOC/DOCX, ODT*
    - Prezentacje: *PPT/PPTX, ODP*
    - Materiały multimedialne: *MP4* (wideo), *MP3* (audio)
    - Obrazy: *JPEG, PNG, GIF*
    - E-learning SCORM/IMS: Pakiety *SCORM* lub *IMS Content Package*
    - Pliki interaktywne: *H5P*

7.6. Raporty i odbiór szkoleń

1. Po zakończeniu szkoleń **Wykonawca** sporządzi raport zawierający:
    - Listę przeprowadzonych szkoleń z nazwą, czasem i miejscem.
    - Liczbę uczestników.
    - Imię i nazwisko trenera.
    - Listy obecności oraz wyniki egzaminów weryfikujących wiedzę.
2. Raport musi być zgodny z rzeczywistością oraz zaakceptowany przez **Zamawiającego** w terminie 7 dni roboczych.
3. W przypadku uwag do raportu, **Wykonawca** dokonuje korekt w terminie 5 dni roboczych.

8. Etap V – Migracja na środowisko Zamawiającego [MIGR]

Cel Etapu

Migracja na środowisko **Zamawiającego** ma na celu przeniesienie w pełni funkcjonalnego systemu **PIOZE** z środowiska testowego na środowisko produkcyjne dostarczone przez **Zamawiającego (planowane jest środowisko w ramach Rządowej Chmury Obliczeniowej)**. W ramach tego etapu **Wykonawca** zapewni kompleksowe wsparcie techniczne i proceduralne, aby system został uruchomiony w warunkach rzeczywistych i był gotowy do eksploatacji.

Dodatkowo, w tym etapie Wykonawca uruchomi funkcjonalności określne w sekcji EF. Edytor formularzy.

Zakres Wymagań

1. **Przygotowanie do migracji**
    - Przeprowadzenie analizy infrastruktury produkcyjnej **Zamawiającego** w celu weryfikacji jej zgodności z wymaganiami systemu PIOZE.
    - Określenie wymagań środowiskowych (minimalne zasoby, sieć, typ usług chmurowych), w oparciu o dostępne zasoby RChO.
    - Weryfikacja zgodności komponentów systemu z infrastrukturą Chmury RP (np. zgodność kontenerów, systemów operacyjnych, silników baz danych, itd.).

Uwaga! **Wykonawca** nie jest odpowiedzialny za zapewnienie odpowiedniego środowiska sprzętowego po stronie **Zamawiającego**, a jedynie za dostarczenie w ramach dokumentacji kompletnego zestawu wymagań dla takiego środowiska oraz wsparcie w jego konfiguracji.

    - Opracowanie planu migracji, obejmującego:
        - Harmonogram migracji.
        - Wykaz działań niezbędnych do przygotowania środowiska produkcyjnego.
        - Zidentyfikowanie potencjalnych ryzyk oraz ich planów mitigacji.
    - Weryfikacja i konfiguracja środowiska produkcyjnego **Zamawiającego** w zakresie wymaganym do instalacji systemu.

2. **Migracja danych i konfiguracji**
    - Utworzenie i walidacja środowisk (testowego i produkcyjnego) w RChO zgodnie z polityką bezpieczeństwa i standardami operatora chmury.
    - Konfiguracja polityk dostępowych, sieciowych i szyfrowania danych przed przeniesieniem danych operacyjnych.
    - Zastosowanie mechanizmów szyfrowania danych (w tranzycie i w spoczynku) zgodnie z wytycznymi Chmury RP (np. TLS 1.3, AES-256).
    - Eksport wszystkich danych i konfiguracji systemu ze środowiska testowego.
    - Import danych i konfiguracji na **Środowisko Produkcyjne Zamawiającego**.
    - Weryfikacja kompletności i spójności danych po migracji.
    - Zapewnienie integralności danych i minimalizacja ryzyka ich utraty lub uszkodzenia.
    - Weryfikacja mechanizmów monitorowania, backupu, logowania oraz zgodności z wymogami bezpieczeństwa Chmury RP.
3. **Uruchomienie systemu w środowisku produkcyjnym**
    - Instalacja i konfiguracja wszystkich komponentów systemu w **Środowisku Produkcyjnym Zamawiającego**.
    - Proceduralne uruchomienie systemu, obejmujące:
        - Testy startowe potwierdzające poprawność działania systemu w warunkach rzeczywistych.
        - Weryfikację dostępności kluczowych funkcjonalności systemu.
        - Sprawdzenie integracji z systemami zewnętrznymi i ich poprawnego działania.
4. **Wsparcie techniczne i proceduralne**
    - Zapewnienie wsparcia w czasie rzeczywistej migracji, obejmującego:
        - Doradztwo techniczne.
        - Bieżące rozwiązywanie problemów.
        - Monitorowanie procesu migracji i jego zgodności z planem.

- Opracowanie i przekazanie **Zamawiającemu** szczegółowych instrukcji dotyczących obsługi systemu w środowisku produkcyjnym.

5. **Ostateczne testy akceptacyjne**
    - Przeprowadzenie pełnych testów akceptacyjnych w środowisku produkcyjnym, obejmujących:
        - Testy funkcjonalne i niefunkcjonalne.
        - Testy obciążeniowe w warunkach rzeczywistych.
        - Testy bezpieczeństwa systemu w warunkach rzeczywistych.
6. **Przekazanie dokumentacji**
    - Przekazanie **Zamawiającemu** kompletnej dokumentacji dotyczącej procesu migracji, w tym:
        - Raportu z realizacji migracji.
        - Instrukcji operacyjnych dla środowiska produkcyjnego.
        - Wyników testów przeprowadzonych w środowisku produkcyjnym.

Odpowiedzialność Wykonawcy

- **Wykonawca** ponosi pełną odpowiedzialność za prawidłowe przeprowadzenie migracji systemu na środowisko **Zamawiającego**.
- W przypadku problemów lub błędów wynikających z migracji, **Wykonawca** zobowiązuje się do ich niezwłocznego usunięcia na własny koszt.
- **Wykonawca** zobowiązuje się do zapewnienia wsparcia technicznego w okresie przejściowym, aż do zakończenia procesu migracji i potwierdzenia pełnej funkcjonalności systemu w warunkach produkcyjnych.

Produkty końcowe Etapu

1. W pełni funkcjonalny system **PIOZE** uruchomiony w środowisku produkcyjnym **Zamawiającego**.
2. Raport z realizacji migracji.
3. Wyniki testów akceptacyjnych w środowisku produkcyjnym.
4. Zaktualizowana dokumentacja techniczna i operacyjna uwzględniająca środowisko produkcyjne.

Proces migracji musi być przeprowadzony w ścisłej współpracy z **Zamawiającym** i zgodnie z harmonogramem projektu, aby zapewnić płynne i bezpieczne wdrożenie systemu **PIOZE** do warunków rzeczywistych.

9. Gwarancja

Gwarancja obejmuje działania mające na celu zapewnienie ciągłości działania, ulepszania, dostosowywania do nowych regulacji prawnych Portalu Informacyjnego Odnawialnych Źródeł Energii (PIOZE), zgodnie z wymaganiami technicznymi i organizacyjnymi Zamawiającego. W ramach gwarancji Wykonawca zobowiązuje się w szczególności do:

1. Monitorowania działania PIOZE i szybkiego reagowania na zgłoszenia dotyczące błędów oraz awarii,
2. Regularnej aktualizacji oprogramowania i infrastruktury w celu zapewnienia bezpieczeństwa oraz zgodności z najnowszymi standardami,
3. Dostosowywania konfiguracji systemu do bieżących potrzeb użytkowników i Zamawiającego,
4. Zapewnienia wsparcia technicznego dla administratorów i użytkowników wewnętrznych,
5. Prowadzenia dokumentacji zmian i modyfikacji systemu,
6. Utrzymania zgodności środowiska testowego z produkcyjnym,
7. Przestrzegania wymagań bezpieczeństwa obowiązujących w infrastrukturze Rządowej Chmury Obliczeniowej.

Celem wyżej opisanych działań jest zapewnienie stabilnej i niezawodnej pracy systemu PIOZE, tak aby spełniał swoje funkcje w zakresie obsługi procesów związanych z odnawialnymi źródłami energii oraz był zgodny z regulacjami prawnymi i technicznymi obowiązującymi w administracji publicznej.

Ad.1 Monitorowanie działania PIOZE i szybkie reagowanie na zgłoszenia dotyczące błędów oraz awarii

Monitorowanie systemu PIOZE obejmuje:

- **Automatyczną analizę logów i raportów systemowych** – identyfikacja potencjalnych problemów w działaniu systemu,

- **Monitorowanie wydajności systemu** – analiza obciążenia serwerów, czasu odpowiedzi aplikacji, stabilności baz danych,
- **Monitorowanie dostępności usług** – sprawdzanie poprawnego funkcjonowania komponentów systemu,
- **Identyfikację nieautoryzowanych prób dostępu lub naruszeń bezpieczeństwa**,
- **Wczesne wykrywanie błędów krytycznych i anomalii**, które mogą wpłynąć na funkcjonowanie systemu.

W zakresie zasad naprawy błędów obowiązują zasady w zakresie gwarancji.

Ad.2 Regularna aktualizacja oprogramowania i infrastruktury w celu zapewnienia bezpieczeństwa oraz zgodności z najnowszymi standardami

Wykonawca zobowiązuje się do regularnej aktualizacji oprogramowania PIOZE, co obejmuje zapewnienie bezpieczeństwa systemu. Proces aktualizacji obejmuje zarówno system operacyjny, oprogramowanie bazodanowe, jak i aplikację PIOZE.

2.1. Zakres aktualizacji

Regularne aktualizacje obejmują:

1. **System operacyjny i środowisko serwerowe**
    - Instalacje najnowszych poprawek bezpieczeństwa wydawanych przez dostawcę systemu operacyjnego.
    - Aktualizacje komponentów systemowych, takich jak serwery aplikacyjne i systemy cache.
    - Utrzymanie aktualnych wersji bibliotek wykorzystywanych w systemie.
2. **Oprogramowanie bazodanowe**
    - Instalacja aktualizacji i poprawek bezpieczeństwa dla bazy danych.
    - Optymalizacja bazy danych w celu poprawy wydajności i bezpieczeństwa.
    - Regularne przeglądy i archiwizacja zbędnych danych zgodnie z polityką retencji danych.
3. **Oprogramowanie aplikacyjne PIOZE**

- Aktualizacje frameworków i komponentów oprogramowania.
- Weryfikacja i testowanie kompatybilności nowej wersji oprogramowania z istniejącymi funkcjonalnościami.

4. **Bezpieczeństwo i zgodność z regulacjami**
   - Regularne aktualizacje systemów zabezpieczeń, w tym mechanizmów szyfrowania, ochrony przed atakami DDoS i wykrywania nieautoryzowanego dostępu.
   - Zgodność z przepisami dotyczącymi ochrony danych osobowych (RODO) oraz krajowymi regulacjami dotyczącymi cyberbezpieczeństwa.
   - Aktualizacja systemu autoryzacji i kontroli dostępu, w tym zarządzania rolami użytkowników.

2.2. Procedura aktualizacji

1. **Monitorowanie i identyfikacja dostępnych aktualizacji**
   - Wykonawca regularnie monitoruje publikowane przez producentów poprawki i aktualizacje dla wykorzystywanego oprogramowania.
   - Analiza nowych wersji pod kątem ich wpływu na działanie systemu PIOZE.
2. **Przygotowanie aktualizacji i testowanie**
   - Wykonanie testów aktualizacji w środowisku deweloperskim.
   - Analiza potencjalnych problemów wynikających z nowej wersji i określenie planu rollbacku w przypadku niepowodzenia wdrożenia.
3. **Wdrożenie w środowisku testowym**
   - Po pozytywnym przejściu testów, aktualizacje są wdrażane w środowisku testowym.
   - Przeprowadzenie testów regresyjnych w celu potwierdzenia stabilności systemu.
4. **Wdrożenie w środowisku produkcyjnym**
   - Aktualizacja komponentów w produkcji w uzgodnionym oknie gwarancyjnym.
   - Monitorowanie działania systemu po wdrożeniu i reagowanie na ewentualne nieprawidłowości.

2.3. Wymagania dotyczące bezpieczeństwa aktualizacji

- Aktualizacje są wdrażane zgodnie z polityką bezpieczeństwa infrastruktury Chmury RP.
- Wykonawca stosuje **zasadę minimalnego wpływu na dostępność systemu**, tzn. wdrożenia są planowane poza godzinami szczytu lub w weekendy.
- W przypadku krytycznych poprawek bezpieczeństwa, wdrożenie może nastąpić w trybie pilnym, po wcześniejszym uzgodnieniu z Zamawiającym.

2.4. Raportowanie i dokumentacja

Po każdej aktualizacji Wykonawca zobowiązuje się do:

- **Sporządzenia raportu** zawierającego:
  - Listę zainstalowanych aktualizacji i poprawek,
  - Wykonane testy,
  - Potencjalne ryzyka i ich mitygację,
  - Informacje o wszelkich zmianach w dokumentacji systemu.
- **Przekazania dokumentacji technicznej** zaktualizowanych komponentów na żądanie Zamawiającego.

Ad.3. Dostosowywanie konfiguracji systemu do bieżących potrzeb użytkowników i Zamawiającego

Wykonawca zobowiązuje się do elastycznego dostosowywania konfiguracji systemu PIOZE w odpowiedzi na zmieniające się potrzeby użytkowników oraz wymagania Zamawiającego. Działania te obejmują zarówno zmiany techniczne w infrastrukturze systemowej, jak i modyfikacje ustawień aplikacyjnych, które mogą usprawnić obsługę procesów związanych z odnawialnymi źródłami energii.

3.1. Zakres dostosowywania konfiguracji systemu

Dostosowanie konfiguracji systemu obejmuje:

1. Parametry systemowe i infrastrukturalne

- Zmiany w konfiguracji serwerów aplikacyjnych i baz danych w celu poprawy wydajności systemu,
- Modyfikacja zasobów infrastrukturalnych (np. skalowanie zasobów obliczeniowych w Chmurze RP w zależności od zapotrzebowania użytkowników),
- Konfiguracja systemu pod kątem optymalizacji szybkości działania i minimalizacji czasu odpowiedzi.

2. Parametry aplikacyjne i interfejs użytkownika

- Modyfikacja ustawień uprawnień i ról użytkowników zgodnie z polityką Zamawiającego,
- Personalizacja widoków i dostępnych opcji w interfejsie użytkownika,
- Dostosowanie obsługi procedur administracyjnych zgodnie z nowymi przepisami i wymaganiami użytkowników,
- Zmiana parametrów walidacji formularzy i procesów zatwierdzania wniosków.

3. Integracja z innymi systemami

- Dostosowywanie interfejsów API do wymagań nowych systemów administracyjnych,
- Konfiguracja mechanizmów autoryzacji i logowania (np. ePUAP, eDoręczenia, Profil Zaufany, integracja z systemami SSO),
- Optymalizacja mechanizmów komunikacji z Geoportalem i innymi źródłami danych przestrzennych.

4. Zarządzanie danymi i polityką retencji

- Konfiguracja zasad archiwizacji i przechowywania danych zgodnie z wymaganiami prawnymi i operacyjnymi,
- Dostosowywanie mechanizmów raportowania i eksportu danych,
- Zmiana konfiguracji powiadomień i alertów dla użytkowników systemu.

3.2. Procedura dostosowywania konfiguracji systemu

1. **Zgłoszenie potrzeby modyfikacji**
    - Użytkownicy systemu lub Zamawiający zgłaszają potrzebę zmian poprzez system zgłoszeń (bug tracker), e-mail lub inne ustalone kanały komunikacji.

- Każde zgłoszenie jest klasyfikowane według priorytetu i wpływu na działanie systemu.

2. **Analiza zgłoszenia**
   - Wykonawca dokonuje analizy technicznej zgłoszenia, oceniając wpływ zmian na funkcjonowanie systemu.
   - W razie potrzeby Wykonawca przygotowuje propozycję rozwiązania oraz plan wdrożenia zmian.
3. **Testowanie zmian w środowisku testowym**
   - Przed wdrożeniem na produkcji, wszystkie modyfikacje są testowane w środowisku testowym, aby uniknąć ryzyka awarii lub konfliktu z innymi funkcjonalnościami.
4. **Wdrożenie zmian w środowisku produkcyjnym**
   - Po akceptacji przez Zamawiającego, zmiany są wdrażane w systemie produkcyjnym.
   - Wykonawca monitoruje działanie zmodyfikowanych funkcji w celu wykrycia i naprawy ewentualnych problemów.
5. **Dokumentacja i raportowanie**
   - Po wdrożeniu zmian Wykonawca przygotowuje raport zawierający szczegóły dotyczące przeprowadzonych modyfikacji, ich wpływu na system oraz ewentualnych rekomendacji dotyczących dalszego rozwoju.

<u>Ad. 4 Zapewnienie wsparcia technicznego dla administratorów i użytkowników wewnętrznych</u>

Wykonawca zobowiązuje się do zapewnienia bieżącej pomocy technicznej dla **administratorów systemu oraz użytkowników wewnętrznych** PIOZE. Usługi te mają na celu **utrzymanie prawidłowego funkcjonowania systemu, szybkie rozwiązywanie problemów oraz podnoszenie kompetencji użytkowników w zakresie obsługi systemu**.

4.1. Zakres wsparcia technicznego

Wsparcie techniczne obejmuje:

1. Pomoc dla administratorów systemu

- Doradztwo w zakresie administracji systemem, zarządzania kontami użytkowników oraz konfiguracji uprawnień,
- Wsparcie w monitorowaniu działania systemu, analizie logów oraz wykrywaniu i eliminowaniu potencjalnych problemów,
- Pomoc w zarządzaniu bazą danych, optymalizacji zapytań oraz konfiguracji backupów,
- Instruktaż dotyczący stosowania najlepszych praktyk w zakresie utrzymania bezpieczeństwa systemu,
- Wsparcie w zakresie integracji systemu PIOZE z innymi platformami administracji publicznej, takimi jak ePUAP, Profil Zaufany czy Geoportal.

2. Pomoc dla użytkowników wewnętrznych

- Obsługa zgłoszeń dotyczących problemów z funkcjonalnościami systemu,
- Instrukcje dotyczące poprawnego wypełniania formularzy i procesów składania wniosków,
- Rozwiązywanie problemów z logowaniem, resetowaniem haseł i dostępem do zasobów,
- Wyjaśnianie zmian w systemie po wdrożeniu aktualizacji i nowych funkcji,
- Udzielanie odpowiedzi na pytania dotyczące procedur administracyjnych realizowanych w ramach PIOZE.

4.2. Kanały komunikacji i sposób zgłaszania problemów

Wykonawca zapewnia kilka kanałów wsparcia:

1. **Wsparcie telefoniczne** – dedykowany numer telefonu dostępny w dni robocze w godzinach **8:15 – 16:15**,
2. **Wsparcie e-mailowe** – kontakt za pośrednictwem adresu e-mail, z określonym czasem odpowiedzi na zgłoszenia,
3. **System zgłoszeń (bug tracker)** – możliwość zgłaszania błędów, awarii i problemów z użytkowaniem systemu wraz z możliwością dostępu do historii zgłoszeń oraz opisu napraw i testów,

4. **Konsultacje online** – wideokonferencje lub sesje Q&A organizowane w razie potrzeby dla administratorów i kluczowych użytkowników systemu,

5. **Dokumentacja techniczna i FAQ** – dostęp do bazy wiedzy zawierającej rozwiązania najczęściej występujących problemów oraz instrukcje obsługi systemu.

Ad. 5 Prowadzenie dokumentacji zmian i modyfikacji systemu

Wykonawca zobowiązuje się do **bieżącego prowadzenia, aktualizowania i przekazywania dokumentacji zmian i modyfikacji systemu PIOZE**. Dokumentacja ta stanowi kluczowy element zapewniający przejrzystość i kontrolę nad ewolucją systemu, ułatwiający utrzymanie, rozwój oraz przyszłe integracje.

5.1. Zakres dokumentacji zmian i modyfikacji systemu

Każda modyfikacja w systemie PIOZE musi być udokumentowana zgodnie z określonymi standardami i procedurami. Dokumentacja obejmuje:

1. Dokumentację techniczną

- Opis struktury systemu i jego komponentów,
- Szczegółowy opis architektury oprogramowania,
- Dokumentację baz danych – zmiany w schematach, indeksach, procedurach składowanych,
- Opis API i integracji z innymi systemami (np. ePUAP, eDoręczenia, Profil Zaufany, Geoportal),
- Historia zmian w kodzie źródłowym i wdrożonych funkcjonalnościach.

2. Dokumentację użytkową

- Instrukcje obsługi dla administratorów i użytkowników końcowych,
- Aktualizacja przewodników dotyczących korzystania z systemu,
- Opis nowych funkcji i ich wpływu na działanie systemu,
- Lista usuniętych błędów i sposobu ich naprawy.

3. Dokumentację audytową i bezpieczeństwa

- Zmiany w konfiguracji uprawnień użytkowników i dostępu do systemu,
- Historia wdrożeń i aktualizacji systemu,
- Opis wdrożonych mechanizmów bezpieczeństwa,
- Raporty zgodności z wymogami prawnymi i cyberbezpieczeństwa.

5.2. Procedura prowadzenia dokumentacji

1. Rejestrowanie zmian

Każda zmiana w systemie musi być zarejestrowana w **repozytorium dokumentacji** w sposób umożliwiający jej łatwą identyfikację i śledzenie.

2. Przekazywanie dokumentacji Zamawiającemu

- Dokumentacja zmian musi być aktualizowana **po każdym wdrożeniu aktualizacji lub modyfikacji systemu**.
- Na żądanie Zamawiającego, Wykonawca dostarcza pełną dokumentację zmian w terminie **do 7 dni roboczych** od zgłoszenia takiego żądania.
- Dokumenty spełniają ogólne wymagania dotyczące dokumentacji określone w ramach niniejszej SOPZ.

3. Historia zmian i repozytorium dokumentacji

- Każda zmiana wprowadzana w systemie jest zapisywana w repozytorium w postaci **wersjonowania dokumentacji**, co pozwala na śledzenie pełnej historii modyfikacji,
- Dokumentacja zawiera **datę wdrożenia zmiany, jej autora oraz opis wykonanych prac**.

4. Zatwierdzanie dokumentacji

- Każdy dokument podlega **akceptacji przez Zamawiającego**, który potwierdza jego zgodność z rzeczywistymi zmianami w systemie,
- W przypadku niezgodności, Wykonawca zobowiązany jest do poprawy dokumentacji **w ciągu 3 dni roboczych**.

5.3. Narzędzia wykorzystywane do prowadzenia dokumentacji

Wykonawca zobowiązuje się do wykorzystania odpowiednich narzędzi do prowadzenia dokumentacji, m.in.:

- **Systemu zarządzania dokumentacją** – do przechowywania dokumentów technicznych i użytkowych,
- **Repozytorium kodu** – do śledzenia zmian w kodzie źródłowym i opisu wersji,
- **Systemu zgłoszeń błędów i zmian** – do monitorowania modyfikacji i wdrożeń,
- **Systemów do generowania dokumentacji API** – do dokumentowania interfejsów integracyjnych.

5.4. Rodzaje raportów dokumentacyjnych

Rodzaj dokumentacji	Zakres	Częstotliwość aktualizacji
Raport zmian systemowych	Zmiany w funkcjonalnościach, wdrożone poprawki	Po każdym wdrożeniu
Dokumentacja techniczna	Architektura, API, baza danych, integracje	Co kwartał lub na żądanie
Dokumentacja użytkowa	Instrukcje, przewodniki, często zadawane pytania	Po każdej większej zmianie w systemie
Historia zgłoszeń i poprawek	Lista naprawionych błędów i zgłoszeń użytkowników	Co miesiąc
Dokumentacja bezpieczeństwa	Zmiany w polityce bezpieczeństwa i kontroli dostępu	Co pół roku lub na żądanie

Ad. 6. Utrzymanie zgodności środowiska testowego z produkcyjnym

Zapewnienie zgodności środowiska testowego z produkcyjnym jest kluczowym elementem wsparcia PIOZE, umożliwiającym skuteczne testowanie nowych funkcjonalności oraz minimalizowanie ryzyka błędów i awarii w środowisku operacyjnym.

Zakres działań w ramach utrzymania zgodności:

1. **Regularna synchronizacja środowisk**
    - Okresowe odświeżanie środowiska testowego poprzez odwzorowanie konfiguracji, struktury danych oraz wersji oprogramowania stosowanych w środowisku produkcyjnym.
    - Aktualizacja baz danych w środowisku testowym w celu zapewnienia zgodności z rzeczywistymi danymi produkcyjnymi, przy jednoczesnym zachowaniu zasad anonimizacji i bezpieczeństwa danych.
2. **Testowanie poprawek i aktualizacji przed wdrożeniem**

- Wdrożenie zmian najpierw w środowisku testowym celem ich walidacji przed implementacją w systemie produkcyjnym.
- Przeprowadzanie testów regresyjnych i wydajnościowych w celu wykrycia potencjalnych niezgodności oraz wpływu modyfikacji na działanie systemu.
- Identyfikacja i eliminacja błędów przed wprowadzeniem zmian do produkcji.

3. **Spójność konfiguracji i infrastruktury**
   - Utrzymanie jednolitej konfiguracji usług i komponentów systemowych między środowiskami.
   - Zapewnienie zgodności wersji oprogramowania, bibliotek, modułów oraz skryptów konfiguracyjnych.
   - Monitorowanie potencjalnych różnic wynikających z różnic sprzętowych lub ustawień infrastrukturalnych.
4. **Zapewnienie bezpieczeństwa i zgodności z politykami IT**
   - Stosowanie jednolitych polityk dostępu oraz mechanizmów zabezpieczeń dla obu środowisk.
   - Weryfikacja zgodności środowiska testowego z wymaganiami Chmury RP oraz regulacjami dotyczącymi ochrony danych (RODO, KSC).
5. **Automatyzacja procesów synchronizacji**
   - Wdrożenie narzędzi do automatycznej synchronizacji konfiguracji oraz kontrolowania różnic pomiędzy środowiskiem testowym a produkcyjnym.
   - Generowanie raportów zgodności oraz identyfikacja potencjalnych rozbieżności.
6. **Dokumentacja i raportowanie zmian**
   - Sporządzanie dokumentacji dotyczącej różnic pomiędzy środowiskami oraz ich wpływu na stabilność systemu.
   - Informowanie Zamawiającego o koniecznych działaniach naprawczych w przypadku wykrycia istotnych różnic.

Ad. 7. Przestrzeganie wymagań bezpieczeństwa obowiązujących w infrastrukturze Rządowej Chmury Obliczeniowej

Bezpieczeństwo systemu PIOZE w **Rządowej Chmurze Obliczeniowej (Chmura RP)** jest kluczowe dla ochrony danych, stabilności działania oraz zgodności z przepisami dotyczącymi infrastruktury teleinformatycznej w administracji publicznej. Wsparcie obejmuje dostosowanie i utrzymanie systemu zgodnie z wytycznymi w zakresie **cyberbezpieczeństwa, ochrony danych i zarządzania dostępem**.

Zakres działań w ramach przestrzegania wymagań bezpieczeństwa:

1. Stosowanie polityki bezpieczeństwa Chmury RP

- Przestrzeganie zasad określonych w dokumentacji Rządowej Chmury Obliczeniowej, w tym standardów **ISO/IEC 27001, Krajowych Ram Interoperacyjności (KRI)** oraz przepisów **ustawy o krajowym systemie cyberbezpieczeństwa (KSC)**.
- Stosowanie wytycznych Ministerstwa Cyfryzacji oraz Centrum Zasobów Chmurowych w zakresie zarządzania bezpieczeństwem danych i aplikacji.

2. Zarządzanie tożsamością i kontrola dostępu

- Stosowanie mechanizmów **uwierzytelniania wieloskładnikowego (MFA)** dla użytkowników administracyjnych i operatorów systemu.
- Ograniczenie dostępu do systemu zgodnie z zasadą **najmniejszych uprawnień (Least Privilege Access)**.
- Centralne zarządzanie dostępami użytkowników poprzez integrację z systemami tożsamości publicznej (np. ePUAP, eDoręczenia, Profil Zaufany, Węzeł Krajowy).

3. Ochrona danych i zgodność z RODO

- Zapewnienie szyfrowania danych **w spoczynku (at rest)** i **podczas przesyłania (in transit)** przy użyciu standardów **TLS 1.3 oraz AES-256**.
- Monitorowanie zgodności z regulacjami dotyczącymi przetwarzania danych osobowych (RODO), w tym polityki przechowywania i anonimizacji danych.
- Regularne (tj. zgodne z polityką bezpieczeństwa Zamawiajacego) przeprowadzanie audytów i przeglądów zgodności z przepisami **Krajowego Systemu Cyberbezpieczeństwa (KSC)**.

4. Ochrona przed cyberatakami i zagrożeniami

- Wdrożenie **systemów wykrywania i zapobiegania włamaniom (IDS/IPS)** do monitorowania aktywności w systemie PIOZE.
- Nawiązanie i utrzymanie współpracy z krajowymi zespołami ds. cyberbezpieczeństwa, takimi jak CSIRT GOV oraz CERT Polska, w celu skutecznego

reagowania na incydenty bezpieczeństwa, wymiany informacji o zagrożeniach oraz stosowania rekomendowanych procedur zarządzania incydentami..

- Stosowanie mechanizmów **automatycznego blokowania adresów IP** po wykryciu prób nieautoryzowanego dostępu.

5. Kopie zapasowe i odporność na awarie

- Wdrażanie mechanizmów **regularnych backupów danych**, zgodnie z polityką bezpieczeństwa Chmury RP.
- Utrzymanie **strategii Disaster Recovery**, zapewniającej możliwość szybkiego przywrócenia działania systemu w przypadku awarii.
- Testowanie mechanizmów przywracania systemu na środowisku testowym w celu zapewnienia skuteczności procedur awaryjnych.

6. Monitorowanie i rejestrowanie aktywności

- Stosowanie **centralnego systemu monitorowania (SIEM)** do analizy logów, wykrywania anomalii i reagowania na zagrożenia.
- Tworzenie dzienników zdarzeń zgodnych z polityką Rządowej Chmury Obliczeniowej, przechowywanych w bezpiecznej, zabezpieczonej lokalizacji.

7. Zgodność z krajowymi i unijnymi regulacjami

- Spełnianie wymagań **Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI)** w zakresie bezpieczeństwa danych i systemów IT.
- Uwzględnienie wymogów **Dyrektywy NIS2**, dotyczącej ochrony krytycznej infrastruktury cyfrowej, w tym administracji publicznej.
- Przestrzeganie zasad **ustawy o informatyzacji podmiotów realizujących zadania publiczne**, w zakresie bezpieczeństwa systemów teleinformatycznych.

8. Monitorowanie i doskonalenie systemu

- Regularne **analizowanie wydajności systemu**, identyfikacja wąskich gardeł i wdrażanie optymalizacji,

Współpraca z Zamawiającym w celu określania **priorytetowych kierunków rozwoju PIOZE**.

9.1. Zapewnienia gwarancyjne

Gwarancja na system PIOZE obowiązuje przez okres **36 miesięcy**, liczonych od daty odbioru końcowego przedmiotu zamówienia przez **Zamawiającego**.

W ramach okresu **Gwarancji Wykonawca** zapewnia:

- Obsługę zgłoszeń dotyczących błędów oprogramowania wytworzonego w ramach zamówienia oraz dostarczonych licencji.
- Regularne przeglądy oprogramowania i zapewnienie jego zgodności z aktualnymi przepisami prawnymi oraz środowiskami technologicznymi.
- Wsparcie techniczne, aktualizacje i modyfikacje systemu w celu utrzymania jego pełnej funkcjonalności.
- Gwarantowaną dostępność systemu oraz minimalizację przestojów wynikających z błędów krytycznych.

Okres gwarancyjny ma na celu zapewnienie **Zamawiającemu** bezpieczeństwa, stabilności i ciągłości działania systemu PIOZE, zgodnie z wymaganiami określonymi w umowie. Wszelkie zobowiązania Wykonawcy realizowane w tym czasie będą prowadzone w sposób terminowy i zgodny z obowiązującymi standardami.

1. Zakres odpowiedzialności Wykonawcy

Wykonawca ponosi odpowiedzialność wyłącznie za błędy w oprogramowaniu wytworzonym przez siebie w ramach realizacji zamówienia oraz za licencje dostarczone Zamawiającemu w ramach projektu.

- **Gwarancja** nie obejmuje błędów wynikających z niewłaściwego działania infrastruktury sprzętowej **Zamawiającego** oraz oprogramowania niedostarczonego przez Wykonawcę oraz zmian w systemie niewprowadzonych przez Wykonawcę.

2. Kategorie błędów i czasy reakcji

1. **Błąd Krytyczny**
    - **Definicja:** Błąd uniemożliwiający podstawowe działanie systemu, w tym dostęp do kluczowych funkcjonalności lub powodujący całkowite zatrzymanie pracy systemu.
    - **Czas reakcji:** Maksymalnie 2 godziny od zgłoszenia.
    - **Czas naprawy/rozwiązania obejściowego:** Do 8 godzin od zgłoszenia.

- **Czas pełnego usunięcia:** Do 48 godzin od zgłoszenia.

2. **Błąd Istotny**
    - **Definicja:** Błąd zakłócający działanie systemu, powodujący utrudnienia w korzystaniu z ważnych funkcjonalności, ale nie uniemożliwiający pracy systemu.
    - **Czas reakcji:** Maksymalnie 4 godziny od zgłoszenia.
    - **Czas naprawy/rozwiązania obejściowego:** Do 24 godzin od zgłoszenia.
    - **Czas pełnego usunięcia:** Do 5 dni roboczych od zgłoszenia.
3. **Błąd Standardowy**
    - **Definicja:** Błąd o niewielkim wpływie na działanie systemu lub powodujący niedogodności w jego użytkowaniu.
    - **Czas reakcji:** Maksymalnie 1 dzień roboczy od zgłoszenia.
    - **Czas naprawy/rozwiązania obejściowego:** Do 5 dni roboczych od zgłoszenia.
    - **Czas pełnego usunięcia:** Do 20 dni roboczych od zgłoszenia.

3. Procedura zgłaszania błędów

- Zgłoszenia błędów dokonywane są przez **Zamawiającego** za pomocą systemu zgłoszeniowego („*bug tracker*"), który jest dostępny 24/7.
- Zgłoszenie musi zawierać:
    - Datę i godzinę wystąpienia błędu.
    - Opis błędu, wraz z załącznikami (jeśli to możliwe).
    - Kategorię błędu (zgodnie z powyższą klasyfikacją).
- W przypadku błędów krytycznych **Zamawiający** może zgłosić problem również telefonicznie.

4. Gwarantowana dostępność systemu

Wykonawca zapewni gwarantowaną dostępność systemu na poziomie **99,5%** w skali miesiąca kalendarzowego, z wyłączeniem:

- Okresów uzgodnionych prac gwarancyjnych.

- Przestojów wynikających z awarii infrastruktury sprzętowej lub łącz telekomunikacyjnych po stronie **Zamawiającego**.

Metoda obliczania dostępności:

Dostępność Systemu (%) = (TD - Σ TN) / TD × 100

Gdzie:

- **TD:** Łączny czas dostępności systemu w miesiącu (z wyłączeniem prac gwarancyjnych).
- Σ **TN:** Łączny czas niedostępności systemu wynikający z błędów krytycznych lub istotnych.

5. Przerwy techniczne

- **Wykonawca** będzie informował **Zamawiającego** o planowanych przerwach na prace gwarancyjne z co najmniej 3-dniowym wyprzedzeniem.
- Prace gwarancyjne będą przeprowadzane w godzinach nocnych (22:00-6:00) lub innych terminach uzgodnionych z **Zamawiającym**, aby zminimalizować wpływ na działalność systemu.

6. Wyłączenia z odpowiedzialności

Wykonawca nie ponosi odpowiedzialności za:

- Problemy wynikające z nieprawidłowego działania infrastruktury sprzętowej **Zamawiającego**.
- Błędy w oprogramowaniu niedostarczonym w ramach realizacji zamówienia.
- Problemy spowodowane przez nieautoryzowaną ingerencję w system lub jego konfigurację przez osoby trzecie.

7. Ochrona danych i bezpieczeństwo

- Wszelkie prace gwarancyjne będą wykonywane w sposób minimalizujący ryzyko utraty danych.
- W przypadku ryzyka utraty danych **Wykonawca** zobowiązuje się poinformować **Zamawiającego** przed rozpoczęciem prac i umożliwić wykonanie kopii zapasowych.
- **Wykonawca** zapewni zgodność systemu z najlepszymi praktykami w zakresie bezpieczeństwa danych i ochrony przed nieautoryzowanym dostępem.

8. Raportowanie

Wykonawca sporządzi miesięczny raport zawierający:

- Listę zgłoszonych błędów z opisem działań naprawczych.
- Informacje o poziomie dostępności systemu.
- Szczegóły przeprowadzonych prac gwarancyjnych.

9.2. Minimalne wymagania funkcjonalne rozwiązania typu „bug tracker"

Rozwiązanie typu *bug tracker* udostępnione i utrzymywane przez Wykonawcę (nie ma konieczności przekazywania praw autorskich do tego oprogramowania) powinno wspierać kompleksowe zarządzanie zgłoszeniami dotyczącymi błędów i problemów systemowych. Minimalna funkcjonalność tego narzędzia obejmuje:

1. Rejestracja zgłoszeń

- Możliwość dodawania nowych zgłoszeń przez użytkowników z poziomu przeglądarki internetowej.
- Obowiązkowe pola zgłoszenia:
    - Opis błędu (co najmniej 500 znaków).
    - Kategoria błędu (np. krytyczny, istotny, standardowy).
    - Data i godzina zgłoszenia.
    - Użytkownik zgłaszający (z identyfikacją, np. login lub e-mail).
    - Załączniki (np. zrzuty ekranu, pliki logów).

2. Kategoryzacja i priorytetyzacja

- Możliwość przypisywania zgłoszeń do kategorii błędów zgodnie z ustaloną klasyfikacją (np. krytyczne, istotne, standardowe).
- Funkcja ustawiania priorytetu zgłoszenia (np. wysoki, średni, niski).
- Automatyczne przypisywanie czasów reakcji i naprawy zgodnie z kategorią błędu.

3. Śledzenie statusu zgłoszeń

- Wyraźnie określone statusy zgłoszeń, np.:

  - Nowe.
  - W trakcie realizacji.
  - Rozwiązane.
  - Oczekujące na weryfikację **Zamawiającego**.
- Rejestr historii działań na zgłoszeniu (log zmian), w tym:
  - Kto i kiedy podjął działania.
  - Jakie kroki zostały wykonane.

4. Powiadomienia

- Automatyczne powiadamianie użytkownika i zespołu gwarancyjnego o zmianach statusu zgłoszenia za pomocą e-maila.
- Przypomnienia o terminach realizacji zgłoszeń.

5. Raportowanie

- Możliwość generowania raportów z realizacji zgłoszeń, uwzględniających:
  - Liczbę zgłoszeń w danym okresie.
  - Podział zgłoszeń według kategorii i priorytetów.
  - Czasy realizacji zgłoszeń w porównaniu do zadeklarowanych **SLA**.
- Eksport raportów w formatach *PDF* i *xlsx*.

6. Wyszukiwanie i filtrowanie

- Funkcjonalność wyszukiwania zgłoszeń według:
  - Statusu.
  - Kategorii.
  - Daty zgłoszenia.
  - Użytkownika zgłaszającego.
- Możliwość zastosowania wielu filtrów jednocześnie.

7. Obsługa wielu użytkowników

- Podział na role użytkowników:

- Administratorzy systemu: zarządzanie wszystkimi zgłoszeniami, tworzenie raportów.
- Użytkownicy zgłaszający: dodawanie i przeglądanie swoich zgłoszeń.
- Zespół gwarancyjny: obsługa zgłoszeń przypisanych do danej grupy.

- Możliwość przypisywania zgłoszeń do konkretnych członków zespołu.

8. Bezpieczeństwo

- Autoryzacja użytkowników (np. logowanie za pomocą hasła lub systemu *SSO*).
- Ograniczenie dostępu do zgłoszeń w zależności od roli użytkownika.
- Szyfrowanie danych przesyłanych w systemie (*SSL/TLS*).

9. Integracje

- Możliwość integracji z innymi systemami, np.:
  - Systemami powiadomień (np. Microsoft Teams, Slack).
  - Narzędziami do zarządzania projektami (np. Jira, Trello).

10. Utrzymanie historii zgłoszeń

- Archiwizacja zamkniętych zgłoszeń.
- Możliwość wyszukiwania i odwołania się do zgłoszeń archiwalnych w celu analizy trendów i problemów.

9.3 Zadania Wykonawcy w ostatnim okresie trwania gwarancji związane z przekazaniem obowiązków podmiotowi wskazanemu przez Zamawiającego

W ciągu ostatnich trzech miesięcy trwania gwarancji **Wykonawca** zobowiązuje się do podjęcia szeregu działań mających na celu płynne i skuteczne przekazanie obowiązków utrzymania systemu PIOZE podmiotowi wskazanemu przez **Zamawiającego**.

Działania te obejmują:

1. Szkolenie wdrożeniowe

Wykonawca przeprowadzi szkolenie dla przedstawicieli podmiotu wskazanego przez **Zamawiającego**, które obejmie:

- **Administrowanie systemem:**

- Zarządzanie użytkownikami, rolami i dostępami.
- Konfiguracja systemu, w tym procedur i formularzy.
- Monitorowanie działania systemu oraz wykonywanie kopii zapasowych.

- **Diagnozowanie i rozwiązywanie problemów:**
  - Rozpoznawanie typowych błędów i sposobów ich naprawy.
  - Obsługa narzędzi diagnostycznych oraz bug trackera.
- **Zarządzanie integracjami:**
  - Konfiguracja i monitorowanie połączeń z systemami zewnętrznymi.
  - Testowanie integracji oraz obsługa błędów w komunikacji.

2. Przekazanie dokumentacji

Wykonawca przekaże kompletną i zaktualizowaną dokumentację systemu, obejmującą:

- Instrukcje użytkownika końcowego i administratora.
- Szczegółową dokumentację techniczną, w tym:
  - Architektura systemu.
  - Konfiguracja baz danych i serwerów.
  - Instrukcja instalacji i utrzymania systemu.
- Polityki bezpieczeństwa i ochrony danych.
- Regulaminy użytkownika oraz politykę prywatności.
- Ewidencję wszystkich aktualizacji i zmian dokonanych w systemie podczas trwania gwarancji.

3. Weryfikacja stanu systemu

Wykonawca dokona końcowego przeglądu systemu, który obejmuje:

- Weryfikację poprawności działania wszystkich modułów systemu.
- Kontrolę integralności danych i konfiguracji systemu.

- Potwierdzenie zgodności systemu z obowiązującymi przepisami prawa oraz aktualnymi wymaganiami technologicznymi (np. kompatybilność z przeglądarkami internetowymi i systemami operacyjnymi).

4. Wsparcie w przekazaniu obowiązków

- Zapewnienie wsparcia technicznego i merytorycznego podczas procesu przekazania.
- Odpowiadanie na pytania i wątpliwości podmiotu przejmującego w terminie do 2 dni roboczych od zgłoszenia.
- Współpraca z podmiotem wskazanym przez **Zamawiającego** w celu ułatwienia mu pełnego zrozumienia funkcjonowania systemu.

5. Dostarczenie kodów źródłowych i narzędzi

Wykonawca dostarczy:

- Pełny zestaw kodów źródłowych oprogramowania, wraz z:
  - Instrukcją kompilacji i konsolidacji.
  - Niezbędnymi bibliotekami i narzędziami wspomagającymi.
- Wszystkie narzędzia pomocnicze niezbędne do administrowania i utrzymania systemu, np.:
  - Narzędzia do backupu danych.
  - Narzędzia do monitorowania wydajności systemu.

6. Przygotowanie raportu końcowego

Wykonawca przygotuje szczegółowy raport obejmujący:

- Podsumowanie działań zrealizowanych w ramach gwarancji.
- Wykaz zgłoszeń i działań naprawczych wraz z ich statusami.
- Osiągnięte poziomy dostępności i wydajności systemu w okresie gwarancji.
- Rekomendacje dotyczące dalszego utrzymania i rozwoju systemu.

7. Przekazanie uprawnień

- Przekazanie haseł i kluczy dostępowych do wszystkich komponentów systemu (np. serwery, bazy danych, aplikacje).

- Umożliwienie podmiotowi wskazanemu przez **Zamawiającego** pełnego dostępu do systemu oraz narzędzi administracyjnych.

8. Testy akceptacyjne

- Wykonanie wspólnie z podmiotem przejmującym testów akceptacyjnych potwierdzających poprawne działanie systemu.
- Usunięcie wszelkich usterek lub problemów wykrytych podczas testów przed zakończeniem okresu gwarancji.

9. **Przeniesienie bazy danych bug trackera**

1. **Zakres przekazania:**
    - W przypadku zakończenia realizacji projektu lub zmiany wykonawcy odpowiedzialnego za utrzymanie i rozwój systemu PIOZE, Wykonawca zobowiązany jest do przekazania Zamawiającemu lub nowemu wykonawcy **pełnej bazy danych bug trackera**.
    - Przekazanie obejmuje wszystkie zgłoszenia błędów, incydentów, sugestii rozwojowych, historii zmian, przypisanych użytkowników, statusów zgłoszeń oraz metadanych.
2. **Forma przekazania:**
    - Baza danych bug trackera powinna zostać przekazana w formie umożliwiającej jej bezpośrednią migrację lub odtworzenie w nowym środowisku technicznym, tj.:
        - kopia bazy danych w standardowym formacie eksportu (np. SQL, JSON, XML – w zależności od używanego systemu),
        - dokumentacja techniczna formatu danych i struktury bazy,
        - informacja o wersji systemu bug trackera wykorzystywanego przez Wykonawcę (np. Redmine, Jira, Bugzilla itp.).
3. **Termin przekazania:**
    - Przekazanie bazy danych powinno nastąpić nie później niż w terminie 14 dni od dnia otrzymania przez Wykonawcę wezwania do przekazania danych przez Zamawiającego lub podpisania protokołu zakończenia współpracy.
4. **Wymagania dotyczące bezpieczeństwa i integralności danych:**

- Przekazywana baza danych musi być kompletna, aktualna na dzień przekazania i zabezpieczona w sposób zapewniający poufność i integralność informacji.

- Przekazanie danych musi odbywać się w sposób szyfrowany, z zastosowaniem hasła przesyłanego odrębnym kanałem komunikacji.

5. **Obowiązek współpracy:**

   - Wykonawca jest zobowiązany do współpracy z Zamawiającym lub nowym wykonawcą w zakresie umożliwienia poprawnej migracji lub odtworzenia bazy bug trackera, w tym do udzielenia niezbędnych wyjaśnień dotyczących struktury danych i sposobu ich interpretacji.

10. Wymagania ogólne Sytemu

WO. Wymagania dotyczące Portalu PIOZE

WO.1. Portal PIOZE musi być zbudowany z wykorzystaniem technologii zapewniających stabilność, wydajność, skalowalność oraz bezpieczeństwo. Wymaga się użycia technologii znanych, dojrzałych, sprawdzonych, udokumentowanych i powszechnie stosowanych w budowie portali internetowych.

WO.2. Portal musi działać poprawnie w przeglądarkach internetowych zgodnych z najnowszymi wersjami:

- **Microsoft Edge** (bieżąca wersja i dwie poprzednie),,
- **Mozilla Firefox** (bieżąca wersja i dwie poprzednie),
- **Google Chrome** (bieżąca wersja i dwie poprzednie),
- **Safari** (bieżąca wersja i dwie poprzednie),
- **Opera** (bieżąca wersja i jedna poprzednia).

W przypadku korzystania z nieobsługiwanej przeglądarki użytkownik musi być informowany o sposobie poprawnego wyświetlania strony oraz o wymaganych wersjach przeglądarek.

WO.3. Portal musi być w pełni skonfigurowany i przygotowany do realizacji wszystkich wymaganych funkcjonalności.

WO.4. System musi być kompleksowy i realizować wszystkie funkcje i procesy wymagane przez **Zamawiającego w SOPZ**.

WO.5. Portal musi spełniać wytyczne **WCAG 2.1** na poziomie AA, co zapewni dostępność dla osób niepełnosprawnych zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych (Dz.U. z 2023 r. poz. 1440 z późn. zm.).

WO.6. Strona **Portalu** musi być kompatybilna z wymaganiami normy **EN 301 549 V3.2.1**, a także zawierać deklarację dostępności zgodną z załącznikiem 2 ww. ustawy.

WO.7. Portal musi generować „przyjazne linki" zawierające słowa kluczowe zamiast losowych znaków, co ułatwia wyszukiwanie i indeksowanie stron przez wyszukiwarki internetowe.

WO.8. Portal musi być wykonany w technologii **Responsive Web Design (RWD)**, dostosowując wyświetlane treści do rozdzielczości i rozmiarów urządzenia (laptopy, monitory stacjonarne, urządzenia mobilne – tablety i telefony komórkowe).

WO.9. Generowany kod HTML i skrypty muszą być zgodne z aktualnymi standardami przeglądarek internetowych, takich jak **HTML5** i **CSS3**.

WO.10. Szata graficzna **Portalu** musi być łatwo modyfikowalna przez administratora poprzez **kaskadowe arkusze stylów (CSS)**. Projekt graficzny portalu zostanie opracowany przez Wykonawcę.

WO.11. Wszystkie elementy **Portalu** muszą być wolne od technologii Flash.

WO.12. Portal musi umożliwiać komunikację z systemami zewnętrznymi poprzez usługi sieciowe oparte na standardach **SOAP** i **XML**.

WO.13. Dostęp do elementów systemu musi być zarządzany na podstawie zdefiniowanych uprawnień i ról użytkowników.

WO.14. Moduł administracyjny **Portalu** musi umożliwiać zarządzanie użytkownikami, uprawnieniami oraz dostosowanie portalu do potrzeb organizacyjnych.

WO.15. Portal musi być zabezpieczony przed atakami zgodnie z wytycznymi *OWASP*, w tym poprzez dokładną walidację danych wprowadzanych przez użytkowników.

WO.16. Portal musi wspierać wielojęzyczność, w tym języki: polski i angielski. Dodatkowe języki mogą być dodawane w oparciu o dedykowane struktury *XML*. **Wykonawca** przygotuje wersję językową polską oraz angielską.

WO.17. Portal musi zawierać moduł do definiowania głównego języka wyświetlania treści, bazującego na ustawieniach przeglądarki użytkownika.

WO.18. Na stronie **Portalu** musi być dostępna automatyczna mapa serwisu, której szczegółowość będzie kontrolowana przez administratora.

WO.19. Portal musi umożliwiać integrację z *Google Analytics* lub innym równoważnym narzędziu oraz monitorowanie odwiedzin stron w określonych przedziałach czasowych.

WO.22. Portal musi wspierać osadzanie obiektów multimedialnych oraz kodów HTML5.

CMS. Moduł zarządzania treścią (CMS)

CMS.1. Moduł musi umożliwiać podgląd wyglądu strony przed zapisaniem jej nowej wersji.

CMS.2. Moduł musi dostarczać edytor stron oparty na HTML i WYSIWYG, oferujący wyłącznie predefiniowane style dla zapewnienia jednolitego wyglądu treści (czcionka, formatowanie).

CMS.3. Moduł musi umożliwiać publikację treści bez znajomości HTML, w tym:

- Wpisywanie treści w edytorze.

- Wklejanie treści z edytorów tekstowych.
- Wstawianie zdjęć i tworzenie galerii z opisami.
- Dodawanie plików do pobrania.
- Wstawianie odnośników do innych stron.

CMS.4. Moduł zarządzania treścią musi obsługiwać formatowanie czcionki (pogrubienie, kursywa, podkreślenie, przekreślenie, zmiana kolorów).

CMS.5. Moduł musi umożliwiać wyrównanie tekstu (lewo, prawo, centralnie).

CMS.6. Moduł zarządzania treścią musi obsługiwać:

- Wybór poziomu nagłówków.
- Wstawianie list punktowanych i numerowanych.
- Dodawanie wcięć, zmiany kolorów tekstu.
- Usuwanie formatowania (częściowe i pełne).
- Wstawianie tabel, obrazów, linków, filmów, plików audio.
- Opływanie tekstu wokół elementów multimedialnych.

CMS.7. Moduł musi pozwalać na definiowanie i wykorzystywanie szablonów stron oraz modułów.

CMS.8. Moduł zarządzania treścią musi umożliwiać zmianę wyglądu serwisu poprzez wybór „skórek" lub ich edycję, w tym:

- Przygotowanie co najmniej 4 „skórek" sezonowych i jednej na żałobę.
- Automatyczna zmiana skórek na podstawie harmonogramu lub ręczna edycja.
- Tworzenie własnych szablonów z wykorzystaniem kreatora.

CMS.09. Moduł musi umożliwiać osadzanie multimediów (grafika, filmy, audio), w tym:

- Obsługę formatów:
    - **Grafika** – JPG, PNG, BMP, GIF;
    - **Filmy** – OGG, AVI, MPG, MP4;
    - **Audio** – MP3, WAV, OGG.
- Dodawanie tagów/słów kluczowych.
- Organizację repozytorium multimediów według kategorii.

CMS.10. Moduł ma umożliwiać nanoszenie znaków wodnych na multimedia.

CMS.10. Moduł zarządzania treścią musi obsługiwać banery i slidery, w tym:

- Zarządzanie czasem wyświetlania i sposobem prezentacji.
- Grupowanie banerów w rotacji.

CMS.12. Moduł zarządzania treścią powinien umożliwiać szczegółową edycję tabel i ich atrybutów.

CMS.13. System musi zapewniać hierarchiczny proces publikacji treści z możliwością definiowania etapów, powiadomień i zatwierdzania.

CMS.14 Moduł powinien umożliwiać tworzenie mapy strony.

CMS.15. System musi obsługiwać wiele języków interfejsu i danych wyświetlanych.

CMS.16. Moduł zarządzania treścią musi posiadać repozytorium multimediów i treści.

CMS.17. Moduł musi udostępniać statystyki odwiedzin z możliwością przeglądania w podziale na godziny, dni, tygodnie, miesiące i lata, zawierające informacje takie jak:

- Liczba wejść na stronę.
- Liczba unikalnych gości.
- Czas trwania odwiedzin.
- Najczęściej odwiedzane strony.
- Lokalizacja użytkowników.

DB. Silnik bazy danych

DB.01: Baza danych musi wspierać skalowalność poziomą, umożliwiając obsługę nieograniczonej liczby użytkowników zewnętrznych.

DB.02: Licencja systemu musi umożliwiać równoczesną pracę co najmniej 10 użytkowników wewnętrznych.

DB.03: Baza danych musi umożliwiać przechowywanie zarówno strukturalnych (np. tabele), jak i niestrukturalnych danych (np. dokumenty JSON).

DB.04: Musi zapewniać możliwość dynamicznego dostosowywania struktury danych bez konieczności przerywania pracy systemu.

DB.05: Baza danychmusi obsługiwać wielojęzyczność w danych (np. obsługa znaków UTF-8).

DB.06: Maksymalny czas odpowiedzi na zapytanie w przypadku obciążenia 1000 równoczesnych zapytań nie może przekraczać 1 sekundy.

DB.07: Baza danych musi wspierać mechanizmy replikacji w celu zapewnienia wysokiej dostępności (HA).

DB.08: Powinna obsługiwać zapytania analityczne oraz możliwość generowania raportów w czasie rzeczywistym.

DB.09.1: Wszystkie dane przechowywane w bazie danych muszą być szyfrowane w stanie spoczynku (ang. at rest) z wykorzystaniem algorytmu AES-256 lub równoważnego.

DB.09.2: Dane przesyłane pomiędzy komponentami systemu muszą być szyfrowane przy użyciu protokołu TLS 1.3 lub nowszego.

DB.09.3: Klucze kryptograficzne muszą być zarządzane przez dedykowany system zarządzania kluczami (KMS).

DB.09.4: Mechanizm rotacji kluczy kryptograficznych musi być wspierany i wykonywany regularnie, np. co 6 miesięcy.

DB.09.6: Mechanizmy szyfrowania muszą być zgodne z normami i przepisami prawnymi, takimi jak RODO czy eIDAS.

DB.09.7: Szyfrowanie danych musi być uzupełnione mechanizmem podpisu kryptograficznego lub sum kontrolnych.

DB.09.8: Baza danych musi automatycznie blokować lub logować wszystkie nieautoryzowane próby dostępu do zaszyfrowanych danych.

DB.09.9: Wszystkie kopie zapasowe muszą być szyfrowane zgodnie z szyfrowaniem danych w bazie.

DB.09.10: Kopie zapasowe przechowywane w chmurze muszą być szyfrowane po stronie klienta przed przesłaniem danych na serwer.

DB.09.11: Baza danychmusi prowadzić logi operacji szyfrowania i odszyfrowywania danych.

DB.09.12: Raporty dotyczące zgodności mechanizmów szyfrowania z wymaganiami prawnymi i standardami muszą być generowane regularnie.

DB.12: Baza danych musi zapewniać pełną zgodność z RODO w zakresie przechowywania, przetwarzania i usuwania danych.

DB.14: Baza danych powinna wspierać integrację z popularnymi narzędziami ETL (np. Apache NiFi, Talend).

DB.15: Musi zapewniać wsparcie dla eksportu danych do formatu CSV, XML oraz JSON.

DB.16: Musi obsługiwać mechanizmy tworzenia kopii zapasowych i przywracania danych bez zatrzymywania pracy systemu.

DB.17: Baza danych musi umożliwiać przechowywanie dużych plików binarnych (np. załączników PDF, obrazów) w sposób wydajny i bezpieczny, z możliwością wyboru między przechowywaniem w samej bazie danych a integracją z zewnętrznym repozytorium plików dedykowanym do obsługi tego typu danych..

DB.18: Baza danych musi wspierać wersjonowanie danych w przypadku ich aktualizacji.

DB.19: Baza danych musi być zgodna z systemami operacyjnymi Linux oraz Windows.

DB.20: Powinna wspierać wdrożenie w środowisku chmurowym (np. AWS, Azure, Google Cloud) oraz lokalnym (on-premises).

DB.21: Baza danychmusi wspierać zarządzanie danymi zarówno o strukturze relacyjnej, jak i nierelacyjnej, umożliwiając elastyczne modelowanie danych w zależności od potrzeb.).

DB.22: Baza danych musi zapewniać możliwość generowania raportów o stanie wniosków, ich statusach oraz czasie przetwarzania.

DB.23: Baza danych musi zawierać moduł raportowy, który umożliwia generowanie raportów w formie wizualnej (wykresy) oraz tekstowej, bazując na danych przechowywanych w bazie danych..

DB.24: Baza danych musi zapewniać możliwość łatwej migracji danych na inną platformę bez istotnych przestojów w działaniu systemu.

DB.25: Baza danych powinien wspierać automatyczne skalowanie w odpowiedzi na wzrost liczby użytkowników.

OPS. System Operacyjny

OPS.01: Dostarczony system operacyjny musi być zgodny z wymaganiami umożliwiającymi uruchomienie mikroserwisów w architekturze systemu PIOZE.

OPS.02: System operacyjny musi wspierać technologie konteneryzacji, takie jak Docker, Podman lub równoważne.

OPS.03: System operacyjny musi zapewniać obsługę konteneryzacji oraz orkiestracji kontenerów (np. Kubernetes).

OPS.04: System operacyjny musi wspierać integrację z platformami chmurowymi (AWS, Azure, Google Cloud) oraz środowiskami lokalnymi.

OPS.05: System operacyjny musi zapewniać możliwość uruchamiania mikroserwisów..

OPS.06: Licencja musi obejmować prawo do użytkowania systemu operacyjnego w **Środowisku Produkcyjnym**, **Środowisku Testowym** oraz **Środowisku rozwojowym (developerskim).**

OPS.07: Licencja musi uwzględniać możliwość aktualizacji systemu w okresie obowiązywania licencji.

OPS.08: Licencja powinna być dostępna w formie subskrypcji lub licencji wieczystej w zależności od preferencji **Zamawiającego**.

OPS.09: System operacyjny musi umożliwiać automatyczne aktualizacje zabezpieczeń.

OPS.10: System operacyjny musi wspierać mechanizmy bezpieczeństwa, takie jak SELinux, AppArmor lub równoważne.

OPS.11: System musi umożliwiać zarządzanie dostępem użytkowników za pomocą mechanizmów RBAC (Role-Based Access Control) lub równoważnych.

OPS.12: System operacyjny musi być zgodny z bazami danych: PostgreSQL, MySQL, MongoDB oraz bazą danych dostarczoną w ramach realizacji zamówienia.

OPS.13: System operacyjny musi wspierać integrację z narzędziami CI/CD, takimi jak Jenkins, GitLab CI/CD, lub równoważne.

OPS.14: Dostarczony system operacyjny musi być objęty wsparciem technicznym przez cały okres obowiązywania licencji.

OPS.15: Wymagana jest dostępność dokumentacji technicznej i materiałów szkoleniowych dla administratorów.

11. Wymagania funkcjonalne i niefunkcjonalne PIOZE

ARCH. Ogólna koncepcja PIOZE

System będzie posiadał część ogólnodostępną będącą portalem informacyjnym oraz część dostępną po zalogowaniu, służącą składaniu i obsłudze wniosków.

Logowanie do części wnioskowej będzie odbywać się wyłącznie poprzez login.gov.pl - będzie wymagać posiadania konta ePUAP (docelowo również eDoręczeń), które i tak jest wymagane do składania wniosków.

PIOZE ma pełnić funkcję wspomagającą proces wnioskowania, bez ingerencji w formalne i merytoryczne rozpatrywanie wniosków oraz wydawanie decyzji administracyjnych. Wszystkie działania związane z obsługą formalną i merytoryczną decyzji administracyjnych będą należały wyłącznie do kompetencji podmiotów uprawnionych (np. urzędów).

Zakres działania PIOZE

1. Wsparcie wnioskodawcy w przygotowaniu wniosku:

- Umożliwienie użytkownikowi zebrania wymaganych informacji i dokumentów.
- Automatyczne generowanie poprawnie sformatowanych wniosków zgodnych z wymaganiami procedur.
- Dostarczanie informacji o sposobach składania wniosków (np. przez *ePUAP, eDoręczenia* lub dedykowane portale).

2. Integracja z systemami zewnętrznymi:

- Przekierowanie do platform takich jak *ePUAP*, *eDoręczenia* lub dedykowane portale, aby umożliwić złożenie wniosku.
- Automatyczne odbieranie potwierdzeń odbioru wniosków lub statusów ze zintegrowanych systemów (np. „wniosek przyjęty").

3. Wyświetlanie informacji o procedurach:

- Wyświetlanie wymaganych dokumentów, wzorów wniosków oraz informacji pomocniczych.
- Dostarczanie danych kontaktowych do właściwych organów administracyjnych.

Wyłączenie odpowiedzialności PIOZE

1. **Brak formalnej obsługi wniosków:**
    - PIOZE nie będzie odpowiadać za rejestrację ani ocenę wniosków po ich złożeniu w organach administracyjnych.
    - Wszystkie formalne aspekty przetwarzania wniosków będą realizowane poza PIOZE.
2. **Brak merytorycznej oceny dokumentacji:**
    - PIOZE nie przeprowadza merytorycznej analizy wniosków ani załączonych dokumentów.
    - Użytkownik ponosi pełną odpowiedzialność za poprawność i kompletność złożonych dokumentów.
3. **Brak wydawania decyzji administracyjnych:**
    - PIOZE nie obsługuje wydawania decyzji administracyjnych, takich jak pozwolenia, zgody czy odmowy.
    - Decyzje będą podejmowane przez uprawnione organy zgodnie z obowiązującymi przepisami.

Funkcje ograniczające interakcję z decyzjami administracyjnymi

1. Informowanie o statusie wniosków:

- PIOZE może informować użytkowników o statusie wniosków w oparciu o dane z systemów zewnętrznych (np. ePUAP, eDoręczenia), ale bez możliwości ingerencji w ten status (proces zautomatyzowany oraz zmiana statusu z poziomu warstwy administracyjnej).

2. Przekierowanie do właściwego organu:

- PIOZE wskazuje, który organ administracyjny jest właściwy do rozpatrzenia danego wniosku.
- Udostępnia dane kontaktowe oraz linki do dedykowanych stron informacyjnych.

3. Obsługa dokumentów:

- Umożliwienie przesyłania dokumentacji i jej formatowania na potrzeby wnioskodawcy, bez przechowywania wrażliwych danych dotyczących rozpatrywania wniosków.

Podsumowanie podziału odpowiedzialności

Zakres	Realizowany przez PIOZE	Realizowany przez organ administracyjny
Przygotowanie wniosku	Tak	Nie
Wypełnianie formularzy	Tak	Nie
Weryfikacja merytoryczna dokumentacji	Nie	Tak
Składanie wniosku	Przekierowanie do ePUAP, eDoręczeń /dedykowanego portalu	Tak (w systemie organu)
Rozpatrywanie wniosków	Nie	Tak
Wydawanie decyzji	Nie	Tak
Odbieranie decyzji	Przekierowanie do ePUAP lub eDoręczeń	Tak

F2A. Część ogólnodostępna PIOZE

F2A.01: Część ogólnodostępna zostanie zbudowana w oparciu o narzędzie CMS, o minimalnej funkcjonalności opisanej w sekcji CMS. Moduł zarządzania treścią (CMS) będzie składać się co najmniej z następujących elementów:

1. **Informacje ogólne:**
    - Aktualne informacje o możliwościach i warunkach składania wniosków.
    - Opis procesów związanych z wnioskowaniem, w tym wymagania dokumentacyjne i procedury oceny.
    - Sekcja FAQ z najczęściej zadawanymi pytaniami i odpowiedziami.
    - Kontakt do osób lub jednostek odpowiedzialnych za obsługę wniosków (np. formularz kontaktowy, telefon, e-mail) – wyszukiwarka w podziale terytorialnym (wybór z mapy).

- Na stronie głównej PIOZE zostanie umieszczona informacja o finansowaniu projektu wraz z logotypami KPO oraz Unii Europejskiej. Treść komunikatu: *Projekt finansowany w ramach Inwestycji G1.1.4 Krajowego Planu Odbudowy i Zwiększania Odporności: Wsparcie instytucji realizujących reformy i inwestycje w ramach REPowerEU*.

2. **Mapa wniosków OZE – wyświetlanie odpowiedniej warstwy na Geoportalu Infrastruktury Informacji Przestrzennej**:

   - **Automatyczne generowanie warstwy**

     1. Warstwa jest tworzona na podstawie danych złożonych wniosków OZE w portalu.
     2. Informacje o wnioskach obejmują m.in.:
        1. Lokalizację geograficzną (automatycznie pobieraną z danych wniosku).
        2. Status wniosku (np. złożony, w trakcie rozpatrywania, zaakceptowany, odrzucony).
        3. Dane o istniejących instalacjach OZE, w tym ich:

     - Lokalizację.
     - Typ technologii (np. fotowoltaika, wiatr, biomasa).
     - Moc instalacji.
     - Datę uruchomienia.

   - **Obsługa obszarów przyspieszonego rozwoju OZE**

     1. Funkcjonalność pozwala definiować obszary, gdzie promuje się inwestycje w OZE poprzez szczególne podejście systemowe do wymogów proceduralnych w ramach procesu inwestycyjnego.
     2. Obszary te mogą być wyróżnione na mapie (np. specjalne oznaczenia kolorystyczne).
     3. Użytkownik wewnętrzny może przypisać informacje o dodatkowych korzyściach dostępnych dla inwestorów na danym terenie.

- **Ręczne dodawanie danych**

    1. **Dodawanie instalacji OZE:**

        1. Możliwość wprowadzenia danych o instalacjach manualnie (przez użytkownika wewnętrznego).

        2. Dane mogą obejmować: lokalizację, typ technologii, moc, właściciela instalacji, datę uruchomienia.

    2. **Dodawanie wniosków OZE:**

        1. Możliwość wprowadzenia wniosków OZE z ręcznym wskazaniem etapu rozpatrywania.

        2. Dane obejmują lokalizację, status, szczegóły technologii, moc, oraz inne wymagane informacje.

- **Interfejs mapowy i funkcje użytkowe**

    1. Warstwa dostępna w Geoportalu Infrastruktury Informacji Przestrzennej jako część interaktywnej mapy.

    2. Użytkownik ma możliwość filtrowania danych według:

        1. Statusu wniosku.

        2. Typu instalacji.

        3. Obszarów przyspieszonego rozwoju OZE.

        4. Innych kryteriów, takich jak moc instalacji czy data uruchomienia.

    3. Możliwość generowania raportów lub eksportowania danych formatów CSV, XLSX, GeoJSON.

- **Integracja z systemem wnioskowania**

    1. Dane o wnioskach i instalacjach są (opcja konfiguracyjna):

        1. aktualizowane w czasie rzeczywistym lub

        2. według harmonogramu synchronizacji z portalem wraz z funkcją autoryzacji przez użytkownika wewnętrznego zmian w mapie.

2. System monitoruje zmiany statusu wniosków i automatycznie aktualizuje dane na warstwie mapowej do publikacji.

3. **Wyszukiwarka treści:**

   - **Intuicyjne filtrowanie:**

     1. Kategorie: Użytkownicy mogą ograniczyć wyniki wyszukiwania do określonych kategorii, takich jak artykuły, dokumenty, multimedia, raporty lub ogłoszenia.

     2. Daty publikacji: Możliwość filtrowania wyników według zakresu czasowego (np. ostatnie 7 dni, miesiąc, rok lub określone daty). Umożliwia to łatwe znalezienie najnowszych informacji lub danych archiwalnych.

     3. Słowa kluczowe: Wprowadzenie dowolnego słowa lub frazy, które są automatycznie dopasowywane do treści w bazie danych. Wyszukiwarka obsługuje zaawansowane operatory (np. AND, OR, NOT).

   - **Sugestie autouzupełniania:**

     1. System dynamicznie generuje podpowiedzi w miarę wpisywania tekstu przez użytkownika.

     2. Podpowiedzi są oparte na:

        1. Najczęściej wyszukiwanych frazach przez innych użytkowników.

        2. Popularnych słowach kluczowych w treściach dostępnych w systemie.

        3. Historycznych wyszukiwaniach (dla zalogowanych użytkowników, z opcją personalizacji).

        4. Funkcja ta znacząco przyspiesza proces wyszukiwania i pomaga użytkownikom sformułować precyzyjne zapytania.

   - **Dodatkowe funkcje:**

     1. Filtrowanie wielokryterialne: Umożliwia jednoczesne stosowanie kilku filtrów, np. „*kategoria: raporty*” + „*data*: *ostatnie 30 dni*” + „słowo *kluczowe: energia odnawialna*”.

2. Podgląd wyników: Każdy wynik zawiera fragment treści (tzw. *snippet*), który pozwala użytkownikowi ocenić, czy dana pozycja jest istotna, jeszcze przed jej otwarciem.

3. Sortowanie wyników: Opcje sortowania według trafności, daty publikacji, liczby odsłon lub innych zdefiniowanych kryteriów.

4. Obsługa błędów i synonimów: System automatycznie sugeruje poprawne zapytania w przypadku literówek lub braku wyników oraz obsługuje wyszukiwanie powiązanych pojęć (np. „*energia słoneczna*" -> „*fotowoltaika*").

- **Personalizacja wyszukiwania:**

  1. Dla zalogowanych użytkowników wyszukiwarka może zapamiętywać preferencje, takie jak najczęściej stosowane filtry lub ulubione kategorie.

  2. Funkcjonalność pozwala na tworzenie zapisanych zapytań, które mogą być automatycznie aktualizowane i wysyłane jako powiadomienia.

- **Zaawansowane wyszukiwanie:**

  1. Wprowadzenie zaawansowanych opcji, takich jak przeszukiwanie pełnego tekstu w dokumentach *PDF*, *.doc*, *.docx*, lub zawężenie wyników do treści pochodzących od wybranych autorów lub źródeł.

4. **Materiały edukacyjne i promocyjne:**

   - Publikacja artykułów, poradników i infografik.

   - Możliwość pobierania dokumentów, takich jak teksty ustaw, rozporządzeń, regulaminy, wzory formularzy czy prezentacje.

   - Wideo i animacje tłumaczące kluczowe procesy.

5. **Dostosowanie do potrzeb użytkownika:**

   - Responsywny interfejs użytkownika zapewniający czytelność na urządzeniach mobilnych.

   - Funkcje dostępności, takie jak opcje zwiększania czcionki, tryb wysokiego kontrastu oraz możliwość odczytu ekranowego.

6. **Aktualności i powiadomienia:**

- Sekcja z aktualnościami na temat dostępnych programów i terminów składania wniosków.
- Możliwość subskrypcji newslettera.

F2A.02: **Funkcjonalności modułu newslettera:**

1. Zarządzanie subskrybentami:

- Rejestracja użytkowników do newslettera poprzez dedykowany formularz (w tym wyrażenie zgody RODO na przetwarzanie danych osobowych),
- Możliwość edycji danych kontaktowych subskrybenta (np. aktualizacja adresu e-mail),
- Możliwość rezygnacji z subskrypcji przez użytkownika w dowolnym momencie (link rezygnacji w każdej wiadomości).

2. Tworzenie i zarządzanie treścią newslettera:

- Kreator wiadomości (tekstowych i HTML) umożliwiający przygotowanie szablonów newsletterów,
- Możliwość załączania grafik, linków oraz materiałów informacyjnych,
- Opcja segmentacji treści (np. dostosowanie treści do wybranych grup odbiorców).

3. Wysyłka newsletterów:

- Planowanie wysyłki na określony dzień i godzinę (scheduler),
- Możliwość natychmiastowej wysyłki wiadomości lub ustawienia kampanii cyklicznych (np. newsletter miesięczny, kwartalny),
- Obsługa masowej wysyłki z zapewnieniem zgodności z zasadami wysyłek bulk e-mail (np. limity dzienne, kontrola bounce rate).

4. Personalizacja:

- Możliwość personalizacji treści wiadomości na podstawie danych użytkownika (np. imię, rodzaj usług, które użytkownik zamówił),
- Dynamiczne treści w newsletterze w zależności od preferencji lub historii aktywności użytkownika.

5. Śledzenie skuteczności:

- Rejestrowanie podstawowych statystyk:

- liczba dostarczonych wiadomości,
- liczba otwartych wiadomości (open rate),
- liczba kliknięć w linki (click-through rate),
- liczba rezygnacji (unsubscribe rate),

- Raportowanie skuteczności kampanii w formie wykresów i tabel.

6. Zgodność z prawem i bezpieczeństwo:

- Wbudowane mechanizmy zgodności z RODO (rejestrowanie zgód, zarządzanie cofnięciem zgody),
- Zapewnienie bezpiecznego przetwarzania adresów e-mail (szyfrowanie w bazie danych),
- Mechanizm dwuetapowego potwierdzenia zapisu (double opt-in),
- Obowiązkowe linki do polityki prywatności i zasad przetwarzania danych.

7. Integracja z innymi modułami systemu:

- Automatyczna aktualizacja bazy subskrybentów na podstawie profilu użytkownika systemu PIOZE (jeżeli użytkownik wyraził zgodę na komunikację marketingową),
- Możliwość powiązania wysyłki newsletterów z wydarzeniami w systemie (np. informacja o nowych programach OZE, nowych możliwościach składania wniosków).

CHAT. Funkcjonalność Chatbota oraz Email dla Obywatela

CHAT.01: Część ogólnodostępna zostanie wyposażona w funkcjonalność Chatbot, która będzie się składać z następujących elementów:

A. Informacyjna obsługa użytkownika (FAQ)

- **Automatyczne odpowiedzi** na najczęściej zadawane pytania dotyczące:
  - Procedur składania wniosków o instalacje OZE.
  - Wymagań formalnych i technicznych dla różnych typów instalacji (fotowoltaika, pompy ciepła itp.).
  - Czasu oczekiwania na decyzje administracyjne.
  - Statusu wniosków i dalszych kroków po złożeniu dokumentów.

- **Wsparcie w nawigacji** po portalu PIOZE: pomoc w znalezieniu odpowiednich formularzy i sekcji w serwisie.
- **Przełączanie na obsługę** przez operatora w przypadku braku satysfakcjonującej odpowiedzi.
- **Podsumowanie interakcji przesyłanej na email** po jej zakończeniu (dla użytkowników zalogowanych).

B. Wsparcie techniczne

- **Zgłaszanie problemów technicznych**: chatbot będzie przyjmować zgłoszenia dotyczące problemów z portalem (logowanie, błędy formularzy) i przekierowywać je do odpowiednich działów wsparcia.
- **Integracja z systemem zgłoszeń** (np. JIRA lub inny bug tracker) w celu monitorowania statusu zgłoszonych problemów.

CHAT.02: Część ogólnodostępna zostanie wyposażona w funkcjonalność Email, która będzie się składać z następujących elementów:

A. Automatyczne powiadomienia email

- **Potwierdzenie złożenia wniosku** z unikalnym numerem referencyjnym.
- **Powiadomienia o zmianach statusu wniosku** (przyjęty, w trakcie weryfikacji, wymagane uzupełnienia, decyzja wydana).
- **Przypomnienia o terminach** (np. konieczność dostarczenia dodatkowych dokumentów lub zbliżający się koniec ważności certyfikatu).

B. Personalizowane odpowiedzi na zapytania

- **System ticketowy dla zapytań emailowych**: każde zapytanie od obywatela generuje numer zgłoszenia, co umożliwia śledzenie odpowiedzi.
- **Szablony odpowiedzi** dostosowane do najczęstszych pytań, z automatycznym uzupełnianiem danych (np. nazwisko użytkownika, numer wniosku).

C. Bezpieczeństwo i poufność

- **Szyfrowanie korespondencji**: wszystkie emaile zawierające dane osobowe lub poufne są szyfrowane zgodnie z wymaganiami RODO.

CHAT.02: Dodatkowe funkcjonalności dla obu kanałów:

1. **Integracja z bazą wiedzy**: zarówno chatbot, jak i system email będą korzystać z artykułów publikowanych w PIOZE, co zapewni spójność udzielanych odpowiedzi.
2. **Ocena jakości obsługi**: po zakończeniu interakcji użytkownik może ocenić jakość otrzymanej pomocy (skala ocen, komentarze).
3. **Statystyki i raportowanie**: analiza najczęściej zadawanych pytań, monitorowanie czasu reakcji na zgłoszenia oraz generowanie raportów dotyczących efektywności obsługi.

GEO. Integracja z Geoportalem Infrastruktury Informacji Przestrzennej

GEO.01: System musi obsługiwać integrację z Geoportalem Infrastruktury Informacji Przestrzennej za pomocą standardowych usług sieciowych:

- **WMS (Web Map Service)** – wyświetlanie map warstwowych.
- **WFS (Web Feature Service)** – pobieranie i edycja danych wektorowych.
- **WMTS (Web Map Tile Service)** – szybkie renderowanie dużych zestawów danych rastrowych.
- **CSW (Catalogue Service for the Web)** – wyszukiwanie i rejestrowanie metadanych.

GEO.02: System musi wspierać automatyczną synchronizację warstw mapowych publikowanych w Geoportalu Infrastruktury Informacji Przestrzennej podstawie:

- Harmonogramów aktualizacji.
- Zmian danych na poziomie wniosków lub dokumentacji. Dane o wnioskach muszą być aktualizowane w czasie rzeczywistym lub w ustalonych interwałach czasowych.

GEO.03: Warstwy publikowane w Geoportalu Infrastruktury Informacji Przestrzennej muszą zawierać:

- Lokalizację instalacji *OZE*.
- Status wniosków (np. złożony, w trakcie rozpatrywania, zatwierdzony, odrzucony).
- Typy technologii (fotowoltaika, energetyka wiatrowa, itp.).
- Szczegóły techniczne, takie jak moc instalacji i data uruchomienia.

Warstwy muszą być interaktywne i umożliwiać filtrowanie danych według kryteriów (np. status, typ technologii, moc instalacji). Powinny być przygotowane zgodnie z powyższym

podziałem, umożliwiając publikację poprzez grupowanie obiektów o danym statusie w ramach jednej warstwy usługi lub ich rozróżnienie na poziomie symbolizacji. Warstwy powinny być znormalizowane oraz wykorzystywać słowniki kontrolne..

GEO.04: System musi umożliwiać użytkownikom wewnętrznym (np. administratorom) dodawanie nowych warstw do Geoportalu Infrastruktury Informacji Przestrzennej z poziomu systemu PIOZE, w tym:

- Import danych geoprzestrzennych (*SHP*, *GeoJSON*, *GML*).
- Stylizację warstw za pomocą predefiniowanych szablonów lub edytorów styli (*SLD*).

GEO.06: System musi zapewniać zgodność z dyrektywą *INSPIRE* w zakresie udostępniania danych geoprzestrzennych.

GEO.07: Warstwy z Geoportalu Infrastruktury Informacji Przestrzennej muszą umożliwiać generowanie raportów oraz eksport danych w formatach takich jak *CSV*, *XLSX*, *GeoJSON*. Administrator powinien mieć możliwość udostępniania lub wyłączenia udostępniania raportów dla użytkowników, niezależnie od ich skonfigurowania w systemie.

GEO.09: Interfejs użytkownika Geoportalu Infrastruktury Informacji Przestrzennej powinien umożliwiać:

- Przeszukiwanie warstw danych na podstawie lokalizacji.
- Wyświetlanie szczegółów wniosków w formie pop-upów mapowych.
- Intuicyjną nawigację i filtrowanie.

REJ. Rejestracja w Portalu

REJ.01: System musi zapewniać możliwość dwupoziomowej **za pomocą login.gov.pl**, z integracją następujących metod uwierzytelnienia:

- Profil Zaufany,
- e-dowód,
- Bankowość elektroniczna.

REJ.02: System musi umożliwiać aktywację konta użytkownika poprzez wysłanie wiadomości e-mail zawierającej unikalny link aktywacyjny. Link musi być ważny przez określony czas (np. 24 godziny), który może być konfigurowany przez administratora systemu.

REJ.03: System powinien pozwalać na ponowne wysyłanie linku w przypadku braku aktywacji. W systemie powinna istnieć możliwość zdefiniowania czasu (*cool down time*) po jakim możliwe jest ponowne wygenerowanie linku aktywacyjnego.

REJ.04: W procesie rejestracji system musi wymagać od użytkownika:

- Zapoznania się z aktualnym regulaminem portalu,
- Wyrażenia zgody na jego akceptację przed zakończeniem procesu rejestracji.

REJ.05: Po rejestracji w systemie użytkownik jest przekierowywany na stronę pozwalającą na uzupełnienie danych użytkownika niezbędnych dla procesu wnioskowania:

Dane identyfikacyjne:

- Imię i nazwisko
- Numer *PESEL*
- Numer i seria dowodu osobistego
- Numer *NIP*
- Numer telefonu
- Adres *e-mail*

Dane adresowe:

- Adres zamieszkania
- Adres korespondencyjny

Dane pełnomocnika (jeśli dotyczy):

- Imię i nazwisko
- Numer *PESEL*
- Adres
- Dane kontaktowe

Dane dotyczące komunikacji elektronicznej:

- Adres skrzynki *ePUAP,*
- Adres skrzynki *eDoręczeń* (o ile zdefiniowano).

REJ.06: W przypadku zarejestrowania się z wykorzystaniem mechanizmów **login.gov.pl** system automatycznie wypełnia dane, które są udostępniane przez **login.gov.pl.** Dane te nie powinny być możliwe do zmiany przez użytkownika w toku pracy w systemie.

WRJ. Wyrejestrowanie z Portalu

WRJ.01: System musi umożliwiać użytkownikowi samodzielne usunięcie konta poprzez funkcjonalność dostępną w panelu użytkownika.

WRJ.02: Konto użytkownika wraz z wszystkimi danymi osobowymi i powiązaną dokumentacją musi być automatycznie usuwane z systemu po upływie 2 lat od ostatniego logowania, zgodnie z przepisami prawa.

WRJ.03: Użytkownik musi mieć możliwość usunięcia swojego konta z poziomu ustawień profilu lub innego dedykowanego miejsca w systemie.

WRJ.04: System musi zapewnić jasne instrukcje dotyczące procesu usunięcia konta, w tym:

- Ostrzeżenie o nieodwracalności procesu.
- Informację o konieczności pobrania kopii dokumentów przed usunięciem konta.

WRJ.05: Użytkownik musi potwierdzić chęć usunięcia konta poprzez dodatkowe zabezpieczenie, takie jak ponowne podanie hasła lub potwierdzenie poprzez e-mail.

WRJ.06: System musi trwale usuwać wszystkie dane osobowe użytkownika, w tym:

- Dane identyfikacyjne (np. imię, nazwisko, PESEL).
- Dokumenty powiązane z kontem.
- Informacje o aktywnościach użytkownika w portalu.

WRJ.07: Dane muszą być usuwane w sposób zgodny z wymogami RODO.

WRJ.08: Użytkownik musi otrzymać potwierdzenie usunięcia konta w formie wiadomości e-mail.

WRJ.09: System musi automatycznie usuwać konta nieaktywne przez okres 2 lat od ostatniego logowania.

WRJ.10: Administrator systemu powinien mieć możliwość konfigurowania tego okresu w panelu zarządzania.

WRJ.11: System powinien generować automatyczne informacje o zamiarze usunięcia konta kierowane na adres e-mail powiązany z kontem.

WRJ.12: W przypadku problemów z usunięciem konta, użytkownik musi mieć możliwość kontaktu z pomocą techniczną portalu.

WRJ.12: System musi zawierać sekcję pomocy z instrukcją dotyczącą procesu usuwania konta.

WRJ.13: Proces wyrejestrowania musi być zabezpieczony przed nieuprawnionym dostępem, np. przez wymaganie ponownej weryfikacji tożsamości użytkownika przed rozpoczęciem procedury poprzez wysłanie wiadomości e-mail z linkiem aktywującym usuniecie konta.

LOG. Logowanie w Portalu

LOG.01: System musi zapewniać **logowanie za pomocą login.gov.pl**:

- Integracja z metodami uwierzytelnienia oferowanymi przez login.gov.pl:
    - Profil Zaufany,
    - e-dowód,
    - Bankowość elektroniczna.
- Po zalogowaniu użytkownik musi zostać przekierowany do odpowiedniego obszaru w portalu.

LOG.02: System musi wymagać od użytkownika ponownej akceptacji regulaminu w przypadku jego zmiany.

- Przy kolejnym logowaniu po zmianie regulaminu, użytkownik musi zostać poinformowany o konieczności zapoznania się z nową treścią regulaminu.
- Proces logowania nie może zostać zakończony, dopóki użytkownik nie wyrazi zgody na nowy regulamin.
- System powinien umożliwiać dostęp do pełnej treści nowego regulaminu w formacie elektronicznym (PDF lub link do strony).

LOG.03: Administrator portalu musi mieć możliwość zarządzania komunikatami dotyczącymi zmiany regulaminu, w tym:

- Data wprowadzenia zmiany,
- Opcjonalna wiadomość informacyjna dla użytkowników.

LOG.05: System zapewnia opcjonalne (konfigurowane przez administratora) wsparcie dla dwuetapowego uwierzytelniania (2FA), z wykorzystaniem:

- Kodów SMS,
- Linków wysyłanych na adres e-mail powiązany z kontem,
- Aplikacji mobilnych generujących kody jednorazowe (np. Google Authenticator, Free OTP, OTP Auth – do konfiguracji przez Administratora).

LOG.08: System musi rejestrować szczegóły dotyczące każdego logowania, w tym:

- Datę i godzinę logowania,
- Identyfikator użytkownika (np. ID konta lub e-mail użytkownika),
- Adres IP urządzenia, z którego dokonano logowania.,
- Używaną metodę logowania (login.gov.pl, e-mail i hasło).
- Zapisane logi muszą być dostępne dla administratorów w celach audytowych.

Dodatkowo, system powinien oferować mechanizm opcjonalnego powiadamiania użytkownika o zalogowaniu na jego konto, np. poprzez wiadomość e-mail lub SMS.

PHI. Zabezpieczenia formularza rejestracyjnego oraz logowania

PHI.01: Mechanizm wykrywania wielu nieudanych prób

- System musi automatycznie rejestrować liczbę nieudanych prób rejestracji lub logowania podejmowanych przez użytkownika w określonym czasie.
- Administrator powinien mieć możliwość konfiguracji parametrów takich jak:
    - Maksymalna liczba nieudanych prób.
    - Okres, w którym liczone są nieudane próby.

PHI.02: Blokowanie konta użytkownika

- Po osiągnięciu określonej liczby nieudanych prób logowania na to samo konto, system musi automatycznie zablokować konto na czas określony w konfiguracji.
- System musi wysłać użytkownikowi powiadomienie (np. e-mail) z informacją o blokadzie konta oraz instrukcją odblokowania.

PHI.03: Blokowanie adresu IP

- W przypadku wykrycia wielu nieudanych prób rejestracji lub logowania z tego samego adresu IP, system musi automatycznie zablokować możliwość rejestracji lub logowania z tego adresu IP na określony czas.
- Administrator musi mieć możliwość skonfigurowania wyjątków dla zaufanych adresów IP (tzw. lista "whitelist").

PHI.04: Czasowa blokada

- System musi umożliwiać blokowanie konta lub IP na czas określony w konfiguracji (np. 10 minut, 1 godzina, 24 godziny).
- Administrator musi mieć możliwość natychmiastowego odblokowania konta lub IP w panelu zarządzania.

PHI.05: Powiadamianie administratora

- System musi automatycznie informować administratora o wykryciu podejrzanej aktywności, takiej jak:
  - Wielokrotne nieudane próby logowania z jednego konta.
  - Wielokrotne próby rejestracji z jednego IP.
- Powiadomienia mogą być wysyłane e-mailem lub wyświetlane w dedykowanym panelu administracyjnym.

PHI.07: Elastyczna konfiguracja

- Administrator musi mieć możliwość zmiany parametrów systemu, takich jak:
  - Maksymalna liczba nieudanych prób.
  - Długość blokady konta lub IP.
  - Dostosowanie wiadomości wysyłanych do użytkowników
  - Parametry mechanizmów ochronnych, takich jak CAPTCHA (np. liczba prób przed aktywacją)

PHI.08: Zabezpieczenie przed fałszywymi blokadami

- System musi uwzględniać mechanizmy zapobiegające blokowaniu użytkowników w przypadku potencjalnych fałszywych alarmów (np. zastosowanie CAPTCHA po określonej liczbie prób przed zablokowaniem).

PHI.09: System powinien posiadać funkcjonalność wylogowania użytkownika jeśli nastąpiło ponowne logowania na identyczne dane autoryzacyjne z innego adresu IP.

UDA. Dane użytkownika

UDA.01: System musi zapewniać dostęp do dedykowanego panelu użytkownika, w którym można przeglądać, edytować i aktualizować dane osobowe.

UDA.02: Panel użytkownika powinien być dostępny po zalogowaniu się do systemu.

UDA.03: Użytkownik musi mieć możliwość samodzielnej edycji danych, o których mowa w wymaganiu **REJ.05**:

UDA.04: System musi wymagać potwierdzenia zmian krytycznych (np. zmiana adresu e-mail) poprzez:

- Podanie bieżącego hasła użytkownika lub użycie 2FA przed wprowadzeniem zmiany.
- Weryfikację nowego adresu e-mail poprzez wysłanie linku potwierdzającego.
- (Opcjonalnie) Wykorzystanie pomocniczego adresu e-mail lub innego mechanizmu odzyskiwania dostępu, aby zapewnić użytkownikowi możliwość reakcji w razie błędnej zmiany.

UDA.05: Użytkownik musi mieć możliwość:

  - Zmiany hasła do konta,
  - Ustawienia opcji związanych z dwuetapowym uwierzytelnianiem (2FA) – o ile jest stosowane,
  - Przeglądania historii logowań i sesji.

UDA.06: Dla danych pobieranych z zewnętrznych źródeł, takich jak:

  - rejestry administracji publicznej,
  - systemy ePUAP,
  - system eDoręczeń

  zmiany muszą być możliwe wyłącznie po ich uprzedniej aktualizacji w źródłowym rejestrze.

UDA.07: System powinien automatycznie synchronizować zaktualizowane dane z zewnętrznych rejestrów w czasie rzeczywistym lub w określonych odstępach czasu.

UDA.08: Po każdej zmianie danych system musi automatycznie generować powiadomienie e-mail na podany przez użytkownika adres, zawierające informacje o dokonanych zmianach.

UDA.09: W przypadku trudności w edycji danych użytkownik powinien mieć możliwość skontaktowania się z pomocą techniczną portalu poprzez formularz kontaktowy, czat lub infolinię.

UDA.10: Wszystkie zmiany w danych osobowych muszą być zgodne z przepisami RODO i ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781, z późn. zm.).

UDA.11: System musi zapewniać użytkownikom dostęp do polityki prywatności oraz możliwości zarządzania zgodami na przetwarzanie danych.

UDA.12: System musi przechowywać historię zmian danych użytkownika, w tym:

  - Datę i czas modyfikacji,
  - Rodzaj zmienionych danych,
  - Identyfikator użytkownika dokonującego zmian (w przypadku administracyjnej modyfikacji).

- Historia zmian powinna być dostępna dla administratorów w celach audytowych.

L2A. Część PIOZE dostępna po zalogowaniu

L2A.01: Portal powinien zawierać **menu nawigacyjne** z sekcjami:

- Moje wnioski.
- Formularze.
- Baza adresowa.
- Certyfikaty.
- Raporty.
- Pomoc techniczna.

L2A.02: Dashboard użytkownika powinien prezentować kluczowe informacje w formie widgetów:

- Statusy wniosków (liczba wniosków w toku, zatwierdzonych, odrzuconych).
- Powiadomienia (terminy, zmiany statusów, wezwania do uzupełnienia dokumentacji).
- Projekty w toku z możliwością filtrowania i sortowania.

L2A.03: Wymagana jest funkcjonalność wyszukiwania oraz filtrowania wniosków i projektów według takich kryteriów jak:

- Typ wniosku.
- Etap procesu.
- Data złożenia lub decyzji.

ENG. Silnik obsługi wniosków

ENG.01: Silnik systemu musi działać w oparciu o uniwersalne zasady przetwarzania danych i obsługi wniosków, niezależne od specyfiki procedur.

ENG.02: Procedury (rozumiane jako definiowanie formularzy oraz sekwencji formularzy adekwatnych w danej sprawie) muszą być definiowane jako odrębne jednostki konfiguracji, które administratorzy biznesowi mogą samodzielnie tworzyć, modyfikować lub usuwać bez potrzeby ingerencji zespołu technicznego.

ENG.03: Procedury muszą być definiowane za pomocą:

- **Języka definiowania procedur** – uproszczonego języka opisu reguł i kroków procedur, umożliwiającego tworzenie logiki biznesowej.
- **Edytora WYSIWYG** – interfejsu graficznego do intuicyjnego definiowania procedur, kroków, zależności oraz wymaganych danych.

ENG.04: Język definiowania procedur musi umożliwiać:

- Definicję kroków procedur i ich zależności.
- Określenie parametrów wejściowych i warunków przejścia między krokami.
- Wskazanie wymaganych dokumentów dla każdego etapu procedury.

ENG.05: Edytor WYSIWYG musi zapewniać graficzną reprezentację procedur, w tym:

- Diagramy przepływu pracy (workflow).
- Funkcję Drag & Drop do edycji kroków i zależności.
- Podgląd w czasie rzeczywistym umożliwiający testowanie procedur przed ich publikacją.

ENG.06: System musi umożliwiać definiowanie:

- Sekwencji kroków procedur oraz warunków przejścia między nimi.

- Ewentualnej równoległości działań.
- Wymagań dokumentacyjnych w zależności od parametrów wniosku.
- Powiązania procedur z właściwymi organami administracyjnymi.

ENG.07: Silnik systemu musi wspierać dynamiczne decyzje w ramach procedur, takie jak:

- Weryfikacja danych użytkownika.
- Dostosowywanie etapów procedury w oparciu o wybrane parametry inwestycji.

ENG.08: System musi umożliwiać:

- Publikację procedur po zakończeniu ich definiowania.
- Wersjonowanie procedur, z możliwością powrotu do poprzednich wersji.
- Obsługę wielu równoległych procedur.

ENG.09: Administratorzy muszą mieć możliwość zarządzania zmianami regulacyjnymi poprzez:

- Aktualizację kroków procedur.
- Modyfikację wymagań dokumentacyjnych i warunków przejścia.
- Natychmiastowe publikowanie zmian.

ENG.10: Administratorzy muszą mieć możliwość dodawania nowych procedur, które stają się dostępne dla użytkowników natychmiast po publikacji.

ENG.11: System musi zapewniać walidację procedur pod kątem poprawności logicznej (np. brak zapętleń w sekwencji kroków).

ENG.12: System musi umożliwiać definiowanie procedur bieżących (obowiązujących) oraz przyszłych (zaplanowanych).

- Procedury przyszłe muszą mieć możliwość ustawienia daty rozpoczęcia obowiązywania.
- Po osiągnięciu daty rozpoczęcia obowiązywania, procedura przyszła automatycznie staje się procedurą bieżącą, a nowe wnioski są składane zgodnie z jej zasadami.

ENG.13: System musi automatycznie generować wnioski niesfinalizowane przed zmianą procedury jako dokumenty PDF, zawierające dane wprowadzone przez użytkownika oraz wersję procedury.

- Wnioski niesfinalizowane po zmianie procedury muszą być zablokowane do edycji i oznaczone jako „Zablokowane – procedura wygasła".
- Użytkownik musi mieć możliwość pobrania zarchiwizowanego wniosku w formacie PDF.

ENG.18: System musi informować użytkowników o nadchodzących zmianach w procedurach za pomocą:

  - Powiadomień e-mail lub SMS.
  - Informacji wyświetlanych w panelu użytkownika.

ENG.19: Powiadomienia muszą zawierać szczegóły, takie jak data wygaśnięcia procedury i konieczność zakończenia wniosku przed tym terminem.

ENG.20: Edytor WYSIWYG musi umożliwiać tworzenie procedur z użyciem graficznego interfejsu, w tym:

  - Przeciąganie i upuszczanie elementów procedury.
  - Ustalanie zależności między krokami.

ENG.21: Edytor musi wspierać dynamiczne dodawanie wymagań dokumentacyjnych i powiązań z organami administracyjnymi.

ENG.22: Po aktywacji procedury przyszłej:

  - Wszystkie nowe wnioski muszą być zgodne z nową procedurą.
  - Wnioski niesfinalizowane zgodne z poprzednią procedurą muszą być możliwe do sfinalizowania zgodnie z poprzednim stanem prawnym.

SEL. Moduł wyboru formularzy („Formularze")

SEL01: Moduł wyboru formularzy musi umożliwiać użytkownikom dopasowanie odpowiednich formularzy oraz wskazać właściwą kolejność składania wniosków na ich podstawie - na podstawie parametrów inwestycji, takich jak:

- Rodzaj technologii OZE.
- Wielkość instalacji.
- Etap procesu inwestycyjnego.
- Moc instalacji (mikroinstalacje, małe instalacje, instalacje wielkoskalowe/przemysłowe).

- Umiejscowienie (np. grunt, dachy),
- Lokalizacja (np. obszary Natura 2000, obszar przyspieszonego rozwoju OZE – automatyczne przypisanie na podstawie zdefiniowanych w systemie granic obszarów oraz podanej lokalizacji inwestycji).

Szczegółowe wytyczne w tym zakresie opisano w Załączniku nr 1.

SEL.02: System musi zapewniać intuicyjny interfejs z możliwością filtrowania, wyszukiwania oraz wyświetlania rekomendacji.

SEL.03: Moduł musi wyświetlać wyłącznie formularze odpowiednie do zadanych parametrów, eliminując nieadekwatne opcje.

SEL.04: System musi prezentować formularze w czytelnej formie, zawierając informacje takie jak:

- Nazwa formularza.
- Krótki opis celu i zastosowania.
- Wymagania dotyczące załączników.
- Przewidywany czas wypełnienia.

SEL.05: Formularze muszą być dostępne w trybie podglądu, umożliwiając użytkownikowi zapoznanie się z ich treścią przed rozpoczęciem wypełniania.

ORG. Moduł wyboru organów właściwych w danej sprawie

ORG.01. Moduł musi umożliwiać automatyczne dopasowanie właściwego organu administracyjnego na podstawie:

- Rodzaju instalacji (fotowoltaika, lądowe instalacje wiatrowe, morskie instalacje wiatrowe, biogazownie, instalacje biomasowe, instalacje geotermalne, magazyny energii).
- Mocy instalacji (mikroinstalacje (do 50 kW), małe instalacje (pow. 50 kW–1 MW), wielkoskalowe instalacje (pow. 1 MW)).
- Etapu procesu inwestycyjnego (np. decyzje o środowiskowych uwarunkowaniach, pozwolenia budowlane, koncesje).
- Lokalizacji inwestycji (np. obszary sztuczne i przekształcone - np. dachy, obszary chronione – np. Natura 2000, obszary morskie).

- Właściwości terytorialnej organu dla lokalizacji inwestycji.

Szczegółowe wymagania w tym zakresie opisano w Załączniku nr 2.

ORG.02: System musi automatycznie przypisywać właściwe organy dla konkretnych zadań, takich jak np.:

- Decyzje o środowiskowych uwarunkowaniach (regionalny dyrektor ochrony środowiska, wójt/burmistrz/prezydent miasta, inny zdefiniowany przez administratora podmiot).
- Pozwolenia wodnoprawne (Państwowe Gospodarstwo Wodne Wody Polskie, inny zdefiniowany przez administratora podmiot).
- Pozwolenia na budowę (starosta, wojewoda, inny zdefiniowany przez administratora podmot).
- Zgłoszenia mikroinstalacji (OSD, inny zdefiniowany przez administratora podmot).

Szczegółowe wymagania w tym zakresie znajdują się w Załączniku nr 2.

ORG.03: Moduł musi uwzględniać dodatkowe organy dla specyficznych przypadków, takich jak np.:

- Obszary morskie (Minister Infrastruktury, dyrektor urzędu morskiego, inny zdefiniowany przez administratora podmiot).
- Tereny górnicze (Dyrektor Okręgowego Urzędu Górniczego, inny zdefiniowany przez administratora podmiot).

Szczegółowe wymagania w tym zakresie znajdują się w Załączniku nr 2.

ORG.04: Moduł musi wyświetlać listę przypisanych organów z możliwością podglądu wymagań formalnych.

FOR. Formularze dostępne w systemie

FOR.01: Formularze dostępne w systemie muszą być podzielone na sekcje logiczne:

- Informacje ogólne o danym wniosku – do akceptacji.
- Dane podstawowe (np. nazwa firmy, dane kontaktowe, numer identyfikacyjny użytkownika).

- Szczegóły projektu niezbędne na potrzeby wniosku (opis celu projektu, lokalizacja, oczekiwane rezultaty).
- Dokumenty załączane (możliwość dodawania plików, np. PDF, JPG, DOCX) wraz z określeniem zasad walidacji (patrz sekcja VAL).
- Oświadczenia (np. akceptacja regulaminu, potwierdzenie zgodności danych, oświadczenia związane z obsługiwaną procedurą).

FOR.02: Dany formularz może zawierać więcej sekcji danego typu – w zależności od typu wniosku oraz potrzeb związanych z ergonomią użytkowania.

FOR.03: Formularze powinny wspierać:

- **Dynamiczne podpowiedzi kontekstowe** w czasie wypełniania pól.
- **Automatyczną walidację danych** w czasie rzeczywistym z podświetlaniem błędnych pól.

FOR.04: Portal musi umożliwiać załączanie plików w formacie PDF, JPG, DOCX przy pomocy funkcji:

- **Przeciągnij i upuść**.
- Tradycyjnego wyboru pliku z dysku.

FOR.05: System powinien zapewniać listę kontrolną załączników z możliwością oznaczania tych już dodanych dla danego etapu wnioskowania.

EF. Edytor formularzy

EF.01: Edytor musi umożliwiać intuicyjne tworzenie formularzy o minimalnej funkcjonalności opisanej w sekcji FOR oraz walidacji opisanych w sekcji VAL za pomocą metody „przeciągnij i upuść” (drag-and-drop).

EF.02: Edytor musi wspierać dodawanie różnych typów pól formularza, takich jak:

- Pola tekstowe (krótkie/długie).
- Pola wyboru (checkbox)
- Listy wielokrotnego wyboru.
- Przyciski radiowe (radio buttons).
- Listy rozwijane (dropdown).

- Pola daty i czasu.
- Przesyłanie plików.

EF.03: Musi umożliwiać grupowanie i hierarchiczne układanie pól.

EF.04: Musi wspierać definiowanie pól obowiązkowych oraz walidacji danych (np. format e-maila, numer telefonu).

EF.05: Musi wspierać dynamiczne reguły wyświetlania pól (np. warunkowe pokazywanie ukrytych pól w zależności od odpowiedzi użytkownika).

EF.06: Musi umożliwiać predefiniowane szablony formularzy z możliwością ich modyfikacji.

EF.07: Musi umożliwiać integrację formularzy z innymi komponentami portalu (np. API, słowniki).

EF.08: Edytor musi umożliwiać wersjonowanie formularzy, zapewniając dostęp do historii zmian i możliwość przywracania poprzednich wersji.

EF.09: Musi wspierać zarządzanie dostępem do formularzy poprzez role i uprawnienia (np. administratorzy, edytorzy, użytkownicy).

EF.10: Musi zapewniać możliwość publikacji formularza w portalu po jego zatwierdzeniu.

EF.11: Musi umożliwiać klonowanie istniejących formularzy jako podstawy do tworzenia nowych.

EF.12: Musi zapewniać podgląd formularza w czasie rzeczywistym w różnych rozdzielczościach ekranu.

EF.13: Edytor musi umożliwiać testowanie formularza przed jego publikacją, w tym walidację pól i reguł dynamicznych.

EF.14: Musi zapewniać możliwość wysyłania formularza testowego do symulacji procesu składania wniosku.

EF.15 – Zarządzanie formularzami i procedurami wnioskowania:

- System powinien umożliwiać **dodawanie, modyfikowanie i usuwanie formularzy oraz procedur składania wniosków** w sposób konfigurowalny, z poziomu GUI lub dedykowanego modułu administracyjnego.
- Wprowadzanie zmian w formularzach i procedurach **nie może wymagać ingerencji w strukturę bazy danych ani zmian architektury systemu**.

- System musi zapewniać **ciągłość działania** w czasie modyfikacji i **minimalizować ryzyko przerw w dostępności usług**.
- Wymagana jest możliwość wdrażania zmian bez konieczności restartu systemu oraz bez wpływu na bieżąco obsługiwane wnioski.

WNI. Wsparcie składania wniosków

WNI.01: System musi automatycznie generować treść pisma zawierającego dany wniosek w ramach procedury w oparciu o:

- Dane podane przez użytkownika w formularzu (np. informacje o wnioskodawcy, charakterystyka instalacji, wymagania dokumentacyjne).
- Struktury logiczne i wzory dokumentów zdefiniowane w systemie, zgodne z wymaganiami prawnymi i regulacjami.
- Specyfikę właściwego organu administracyjnego (np. sposób adresowania, wymagany format dokumentu).

WNI.02: Każdy wygenerowany wniosek musi być oznaczony unikalnym identyfikatorem w systemie, który będzie zawierał:

- Numer wniosku.
- Datę i czas jego utworzenia.
- Kod identyfikujący formularz oraz etap procesu.

WNI.04: System musi umożliwiać wysyłkę wniosku do właściwego organu w zależności od wyboru użytkownika:

- Za pomocą platformy ePUAP lub eDoręczeń
- Samodzielnie przez użytkownika – wysyłka na adres e-mail użytkownika (z pomięciem załączników).
- Pobranie wersji pdf wniosku (z pomięciem załączników).

WNI.05: Wysyłka musi obejmować:

- Automatyczne zaadresowanie wniosku do właściwego organu na podstawie parametrów instalacji i lokalizacji.
- Dołączenie wymaganych załączników w odpowiednich formatach (np. PDF, JPG, DOCX).

- Weryfikację poprawności danych i kompletności załączników przed wysłaniem.

WNI.06: System musi generować powiadomienia e-mail dla użytkownika o statusie wniosku:

- Potwierdzenie złożenia wniosku, zawierające:
  - Unikalny identyfikator wniosku.
  - Datę i czas wysyłki.
  - Kopię wygenerowanego pisma w formacie PDF.
- Informację o ewentualnych błędach lub brakach, które uniemożliwiają wysłanie wniosku.

WNI.07: System musi przechowywać w historii aktywności użytkownika informacje o wszystkich złożonych wnioskach wraz z ich statusami.

WNI.08: System musi być zintegrowany z platformą *ePUAP* w zakresie:

- Weryfikacji dostępu do konta użytkownika na *ePUAP*.
- Automatycznego przesyłania wniosku jako pisma urzędowego do wskazanego organu.
- Generowania urzędowego potwierdzenia odbioru (UPO) i jego zapisania w systemie.

WNI.08.01: System musi być zintegrowany z platformą *eDoręczeń* w zakresie:

- Obsługi doręczeń elektronicznych przez Krajowy System *eDoręczeń* zgodnie z ustawą.
- Możliwości automatycznego wysyłania dokumentów do urzędów i użytkowników.
- Integracji ze skrzynkami doręczeń elektronicznych.
- Mechanizmów śledzenia doręczeń i potwierdzeń odbioru.
- W przypadku, gdy wnioskodawca posiada aktywną skrzynkę eDoręczeń (adres do doręczeń elektronicznych), system musi domyślnie używać kanału eDoręczeń do przekazania pisma.
- Wyłącznie w przypadku braku aktywnej skrzynki eDoręczeń, dopuszcza się wykorzystanie ePUAP jako alternatywnego kanału doręczeń.

- System musi automatycznie rozpoznać dostępność skrzynki eDoręczeń (np. poprzez rejestr adresów elektronicznych) i odpowiednio przekierować wysyłkę dokumentu.
- W przypadku, gdy adresatem jest urząd posiadający skrzynkę eDoręczeń, system musi kierować korespondencję przez kanał eDoręczeń.
- Korzystanie z ePUAP jest dopuszczalne wyłącznie w przypadku, gdy dany urząd nie figuruje w rejestrze podmiotów zobowiązanych do odbioru eDoręczeń lub nie posiada aktywnej skrzynki w systemie.

WNI.09: System musi przechowywać kopie wszystkich wygenerowanych wniosków w formie elektronicznej, w tym:

- Wersję pisma w formacie *PDF*.
- Wersję elektroniczną załączników przesłanych razem z wnioskiem.

WNI.10: Użytkownik musi mieć możliwość pobrania kopii wniosku i załączników z historii aktywności.

VAL. Walidacje wprowadzanych danych

VAL.01: System musi umożliwiać automatyczną walidację danych wprowadzanych przez użytkowników na każdym etapie wnioskowania, generowania certyfikatów i innych procesów – zgodnie z regułami zaprojektowanymi w formularzu.

VAL.02: Walidacja danych musi być zgodna z obowiązującymi przepisami prawa oraz wymaganiami proceduralnymi dotyczącymi instalacji OZE.

VAL.03: System musi obsługiwać następujące typy walidacji:

VAL.03.01: Walidacja strukturalna – sprawdzanie poprawności formatów danych, np.:

- Numer NIP, PESEL, REGON.
- Kody pocztowe, numery telefonów.
- Adresy e-mail.

VAL.03.02: Walidacja logiczna – weryfikacja spójności danych, np.:

- Rodzaj instalacji (np. instalacja fotowoltaiczna, lądowa instalacja wiatrowa).

- Moc instalacji zgodna z typem technologii (mikroinstalacja, mała instalacja, instalacja wielkoskalowa).
- Lokalizacja (np. na obszarze Natura 2000 wymagająca dodatkowych dokumentów).

VAL.03.03: Walidacja zakresowa – sprawdzanie czy dane mieszczą się w wymaganych przedziałach, np.:

- Moc instalacji (np. od 1 kW do 10 MW).
- Daty (np. data rozpoczęcia inwestycji nie może być wcześniejsza niż data zgłoszenia).

VAL.03.04: Walidacja zależności – weryfikacja powiązań między danymi, np.:

- Wymagania dokumentacyjne zależne od typu instalacji.
- Powiązanie inwestycji z właściwym organem na podstawie lokalizacji.

VAL.04: System musi weryfikować dane w czasie rzeczywistym podczas ich wprowadzania w formularzach.

VAL.04.01: System musi umożliwiać automatyczną walidację danych wprowadzanych przez użytkownika, wykorzystując integracje z zewnętrznymi bazami referencyjnymi, takimi jak:

- Węzeł Krajowy (PESEL, dane osobowe).
- TERYT (spis miejscowości, ulic, kodów pocztowych).
- REGON (nazwa firmy, NIP, forma prawna, siedziba).

VAL.03.02: W przypadku rozbieżności system powinien umożliwić użytkownikowi:

- Potwierdzenie zgodności danych z danym rejestrem.
- Intencjonalne wprowadzenie danych odmiennych, spełniających kryteria walidacji (np. inny adres korespondencyjny).

VAL.04.02: Walidacja musi działać w czasie rzeczywistym, weryfikując poprawność danych na etapie ich wprowadzania do formularzy.

VAL.05: Użytkownik musi otrzymywać informacje zwrotne o błędach w formie:

- Podświetlenia pól z błędami.
- Komunikatów wyjaśniających, co należy poprawić.

VAL.06: System musi umożliwiać walidację danych przed przesłaniem formularza, aby użytkownik mógł skorygować wszystkie błędy przed złożeniem wniosku.

VAL.07: System musi weryfikować załączniki pod kątem:

- Poprawności formatów plików (np. PDF, JPG, DOCX).
- Maksymalnej wielkości plików (zgodnie z ograniczeniami platformy, np. ePUAP, eDoręczeń).
- Kompletu wymaganych dokumentów na podstawie typu wniosku.
- Użytkownik powinien otrzymywać czytelny komunikat dotyczący przyczyn ewentualnej niezgodności ze standardami systemu oraz wymaganiami w tym zakresie.

VAL.08: W przypadku brakujących lub błędnych załączników system musi generować szczegółowy komunikat z listą braków.

VAL.09: System musi umożliwiać weryfikację danych wprowadzonych przez użytkownika w porównaniu z bazami referencyjnymi, np.:

  - Weryfikacja numeru NIP w bazie CEIDG/KRS.
  - Sprawdzenie lokalizacji w bazie terenów Natura 2000.
  - Weryfikacja zgodności danych kontaktowych (np. e-mail, telefon) z wcześniej wprowadzonymi informacjami.

VAL.10: System musi obsługiwać proces walidacji w przypadku zmiany danych w istniejącym wniosku, w tym:

- Sprawdzenie spójności zmienionych danych z wcześniej podanymi informacjami.
- Weryfikacja czy zmiany wymagają dodatkowych dokumentów lub zgód.

VAL.11: W przypadku błędów walidacyjnych system musi:

- Uniemożliwić przesłanie formularza, dopóki wszystkie błędy nie zostaną poprawione – chyba że użytkownik podejmie świadomą i potwierdzoną w systemie decyzje o wysłaniu Wniosku z błędami walidacji.
- Wyświetlić pełną listę błędów z możliwością ich szybkiego lokalizowania i poprawiania.

VAL.12: System musi umożliwiać użytkownikowi zapisanie formularza z błędami jako wersji roboczej i powrót do jego edycji w późniejszym czasie.

BA Baza adresowa

BA.01: System musi zawierać kompletną bazę adresową jednostek zaangażowanych w procesy wydawania decyzji związanych z instalacjami OZE.

BA.02: Baza adresowa musi obejmować wszystkie jednostki administracyjne, w tym:

- Urzędy miast lub gmin
- Urzędy wojewódzkie
- Urzędy dzielnicowe m. st. Warszawy
- Starostwa powiatowe
- Regionalne dyrekcje ochrony środowiska
- Regionalne dyrekcje lasów państwowych
- Generalna Dyrekcja Ochrony Środowiska
- Wojewódzkie inspektoraty nadzoru budowlanego
- Powiatowe inspektoraty nadzoru budowlanego
- Państwowa Straż Pożarna
- Stacje sanitarno-epidemiologiczne
- Graniczne stacje sanitarno-epidemiologiczne
- Krajowy Ośrodek Wsparcia Rolnictwa
- Urząd Regulacji Energetyki
- Regionalne zarządy gospodarki wodnej
- Zarządy zlewni
- Ministerstwo Infrastruktury
- Ministerstwo Rolnictwa i Rozwoju Wsi
- Urzędy marszałkowskie

BA.03: Każda jednostka w bazie musi zawierać następujące dane:

- Nazwę jednostki.

- Adres korespondencyjny (w tym ulica, numer, kod pocztowy, miejscowość).
- Adres ePUAP (jeśli dotyczy).
- Adres eDoręczeń (jeśli dotyczy).
- Adres e-mail i numer telefonu do kontaktu oraz opcjonalnie osobę kontaktową
- Obszar kompetencji jednostki (np. gmina, powiat, województwo).
- Typ decyzji, które jednostka wydaje (np. pozwolenie na budowę, decyzja o środowiskowych uwarunkowaniach).
- Link do odpowiedniej istniejącej strony docelowej, z której można rozpocząć proces składania wniosku, lub do aplikacji internetowej w danej jednostce.

BA.04: System musi umożliwiać automatyczne powiązanie jednostek z wnioskami na podstawie:

- Lokalizacji inwestycji (np. gmina, powiat, województwo).
- Typu instalacji (mikroinstalacja, mała instalacja, instalacja wielkoskalowa).
- Rodzaju decyzji wymaganej dla danej procedury.

BA.05: Moduł bazy adresowej musi współpracować z modułem formularzy, umożliwiając automatyczne uzupełnienie adresu właściwego organu w pismach i dokumentach.

BA.06: Administratorzy systemu muszą mieć możliwość:

- Dodawania nowych jednostek.
- Edytowania istniejących danych (np. zmiana adresu, aktualizacja danych kontaktowych).
- Usuwania jednostek z bazy (po potwierdzeniu przez administratora).
- Importowania i eksportowania danych jednostek w formatach CSV lub XLSX.

BA.07: System musi umożliwiać automatyczną aktualizację bazy adresowej z centralnych źródeł danych (np. TERYT, rejestry państwowe). Ewentualne nadpisanie danych wymaga potwierdzenia przez Administratora.

BA.08: Użytkownicy muszą mieć możliwość wyszukiwania jednostek w bazie według:

- Nazwy jednostki.

- Lokalizacji (np. gmina, powiat, województwo).
- Typu decyzji (np. pozwolenie na budowę, decyzja o środowiskowych uwarunkowaniach).
- Zakresu kompetencji (np. ochrona środowiska, budownictwo).

BA.09: System musi umożliwiać filtrowanie wyników na podstawie wybranych kryteriów.

BA.10: System musi umożliwiać użytkownikowi:

- Wyświetlenie szczegółowych informacji o jednostkach odpowiedzialnych za rozpatrywanie jego wniosku.
- Pobranie pełnych danych kontaktowych jednostek właściwych dla danej lokalizacji i typu decyzji.
- Automatyczne wysyłanie wniosków i korespondencji do odpowiednich jednostek poprzez ePUAP, eDoręczenia lub e-mail.

BA.11: System musi zapewniać administratorom:

- Walidację danych jednostek przy ich dodawaniu lub edycji (np. poprawność kodów pocztowych, formatów e-mail).
- Możliwość ręcznej i automatycznej aktualizacji danych w bazie.
- Informowanie administratorów o brakach lub niezgodnościach w danych jednostek.

BA.12: System musi rejestrować historię zmian wprowadzonych w bazie adresowej, w tym:

- Kto i kiedy dokonał zmiany.
- Zakres wprowadzonych modyfikacji.

BA.13: Administratorzy muszą mieć dostęp do logów zmian w celu audytu.

MON. Monitorowanie odpowiedzi organów oraz uzupełnień

MON01: Moduł musi automatycznie analizować pisma przychodzące na skrzynkę ePUAP lub eDoręczenia.

MON.02: System musi identyfikować pisma na podstawie:

- Numeru sprawy związanego z wysłanym wnioskiem.

- Danych w metadanych pisma (np. identyfikator nadawcy, data, treść nagłówka).

MON.03: Każde pismo przychodzące musi być automatycznie powiązane z odpowiednim wnioskiem na podstawie:

- Unikalnego identyfikatora wniosku (założenie: nadawca musi się nim posłużyć w piśmie zgodnie z wezwaniem).
- Numeru sprawy wygenerowanego podczas wysyłki wniosku (założenie: nadawca musi się nim posłużyć w piśmie zgodnie z wezwaniem).

MON.04: System musi umożliwiać obsługę pism przychodzących, które nie mogą być automatycznie powiązane z żadnym wnioskiem, w tym:

- Wyświetlanie informacji o piśmie nierozpoznanym, w tym:
  - Nadawca (organ administracyjny).
  - Data otrzymania.
  - Numer sprawy podany w piśmie (jeśli dostępny).
  - Treść pisma lub podgląd załącznika.
- Funkcjonalność ręcznego przypisania pisma do istniejącego wniosku przez użytkownika.

MON.05: System musi umożliwiać przypisywanie nierozpoznanych pism do istniejących wniosków z listy.

MON.06: System musi automatycznie powiadamiać użytkownika o odpowiedziach od organów, w tym:

- Odpowiedziach powiązanych z wnioskiem.
- Pismach nierozpoznanych z możliwością ręcznego przypisania.

MON.07: Powiadomienia muszą być dostępne w formie:

- Komunikatów w panelu użytkownika.
- Powiadomień e-mail lub SMS (opcjonalnie, w zależności od ustawień użytkownika).

MON.08: System musi rozpoznawać pisma z prośbami o korekty i uzupełnienia, w tym:

- Automatyczne identyfikowanie, że pismo dotyczy korekty lub uzupełnienia na podstawie:
  - Analizy treści pisma.
  - Słowników kluczowych (np. "korekta", "uzupełnienie", "braki formalne").
- Przypisywanie takich pism do odpowiednich wniosków.

MON.09: System musi umożliwiać użytkownikowi:

- Szybki podgląd pisma dotyczącego korekty lub uzupełnienia.
- Udzielenia odpowiedzi z możliwością załączania brakujących dokumentów – w tym ponownego wypełnienia formularza podlegającego korekcie.
- Automatyczne przesłanie odpowiedzi do organu za pomocą ePUAP, eDoręczeń lub e-maila.

MON.10: Moduł musi przechowywać pełną historię korespondencji między użytkownikiem a organem dla każdego wniosku, w tym:

- Wszystkie pisma wychodzące i przychodzące.
- Odpowiedzi na korekty i uzupełnienia.
- Informacje o ręcznie przypisanych pismach nierozpoznanych.

MON.11: Historia korespondencji musi być dostępna w formie chronologicznej, z możliwością filtrowania według:

- Daty.
- Nadawcy.
- Statusu (np. rozpoznane, nierozpoznane, zrealizowane).

MON.12: Moduł monitorowania odpowiedzi musi być zintegrowany z:

- Modułem składania wniosków, aby automatycznie powiązać odpowiedzi z wysłanymi wnioskami.
- Modułem generowania odpowiedzi, aby umożliwić szybkie przygotowanie pism na żądanie organów.

MON.13: System musi automatycznie aktualizować status sprawy w oparciu o:

- Otrzymane odpowiedzi od organu.
- Zrealizowane korekty lub uzupełnienia.

MON.14: Status sprawy musi być widoczny dla użytkownika w panelu zarządzania wnioskami.

MWN. Zarządzanie złożonymi wnioskami („Moje Wnioski")

MWN.01: Moduł musi umożliwiać wyświetlanie szczegółów każdego wniosku, w tym:

- Status wniosku (np. w toku, zakończony, odrzucony).
- Numer wniosku i jego unikalny identyfikator.
- Etap procesu (np. weryfikacja, ocena, decyzja).
- Datę złożenia wniosku.

MWN.02: Użytkownik musi mieć możliwość:

- Podglądu treści wniosku w formacie PDF.
- Pobrania załączonych dokumentów.
- Anulowania wniosku (jeśli jest to możliwe na danym etapie procedury).

MWN.03: Moduł musi prezentować wnioski w formie listy lub tabeli z możliwością:

- Filtrowania wniosków według statusu, typu instalacji, daty złożenia.
- Sortowania wniosków według daty złożenia, numeru wniosku, etapu procesu.

MWN.07: System musi umożliwiać grupowanie wniosków według:

- Typu inwestycji (np. fotowoltaika, biogazownie, magazyny energii).
- Statusu (np. złożone, oczekujące na decyzję, zakończone).

MWN.08: System musi przechowywać historię działań dla każdego wniosku, w tym:

- Daty i godziny zmian statusów.
- Szczegóły o działaniach podjętych przez organy (np. wezwania do uzupełnienia dokumentów).
- Odpowiedzi użytkownika na prośby o uzupełnienia.

MWN.09: Moduł musi generować powiadomienia dla użytkownika o:

- Zmianach statusu wniosku.
- **MW.09.02:** Wezwaniach do uzupełnienia dokumentów.
- Terminach związanych z realizacją wniosku.

MWN.10: Powiadomienia muszą być dostępne w formie:

- Komunikatów w systemie.
- Opcjonalnych powiadomień e-mail lub SMS (w zależności od ustawień użytkownika).

CER. Zarządzanie certyfikatami („Certyfikaty")

CERT.01: Moduł certyfikatów musi umożliwiać obsługę procesu zarządzania certyfikatami (tj. wszelkiego rodzaju pozwoleniami, decyzjami, koncesjami itp. – czyli decyzjami organów administracji dotyczącymi danego wniosku wraz z określonym zakresem oraz terminem ważności), związanymi z instalacjami **OZE**, w tym ich generowanie, przechowywanie i udostępnianie użytkownikom.

CERT.02: System musi zapewniać zgodność z obowiązującymi przepisami prawa dotyczącymi certyfikacji instalacji OZE oraz certyfikatów energetycznych.

CERT.03: Moduł musi umożliwiać automatyczne rejestrowanie certyfikatów na podstawie uzyskanych decyzji organów.

CERT.04: Zapisy dotyczące certyfikatów muszą zawierać:

- Dane identyfikacyjne wnioskodawcy i instalacji.
- Numer certyfikatu.
- Datę wydania i okres ważności certyfikatu.
- Dane techniczne instalacji (np. moc, rodzaj technologii OZE).
- Oryginalny dokument zawierający dokument w wersji elektronicznej.

CERT.05: Moduł musi umożliwiać przechowywanie certyfikatów w systemie w sposób zaszyfrowany.

CERT.06: Certyfikaty muszą być dostępne dla użytkowników w formie:

- Podglądu online w panelu użytkownika.

- Plików PDF do pobrania.

CERT.07: Moduł musi umożliwiać wyszukiwanie i filtrowanie certyfikatów według:

- Daty wydania.
- Numeru certyfikatu.
- Nazwy instalacji.
- Typu instalacji i lokalizacji.

CERT.08: System musi generować powiadomienia dla użytkowników w przypadku:

- Zbliżającego się końca okresu ważności certyfikatu.
- Możliwości przedłużenia certyfikatu lub konieczności ponownego procesu certyfikacji.

CERT.09: Powiadomienia muszą być dostępne w formie:

- Komunikatów w systemie.
- Opcjonalnych powiadomień e-mail lub SMS.

CERT.10: Moduł musi obsługiwać proces przedłużania certyfikatów, w tym:

- Automatyczne generowanie powiadomień o konieczności przedłużenia.
- Rejestrowania nowego certyfikatu lub wydłużenia terminu jego ważności.

CERT.11: System musi umożliwiać użytkownikowi samodzielną aktualizację certyfikatu w przypadku otrzymania odpowiedniej decyzji organu administracyjnego.

CERT.12: Moduł musi przechowywać certyfikaty archiwalne i umożliwiać ich podgląd oraz pobranie.

CERT.13: Certyfikaty archiwalne muszą być oznaczone jako „Nieważne" lub „Zastąpione" w przypadku ich wygaśnięcia lub zastąpienia nowym dokumentem.

REP. Raportowanie („Raporty")

REP.01: System musi umożliwiać generowanie raportów w oparciu o dane zgromadzone w systemie, dotyczące m.in. wniosków, certyfikatów, załączników oraz aktywności użytkowników.

REP.02: Raporty muszą być dostępne w formie interaktywnej w systemie oraz eksportowalne w formatach:

- CSV.
- PDF.
- XLSX.

REP.03.01: System musi umożliwiać użytkownikom generowanie następujących typów raportów:

- **Raporty dotyczące wniosków:**
  - Liczba złożonych wniosków w wybranym okresie.
  - Statusy wniosków (np. w toku, zakończone, odrzucone).
  - Wnioski przypisane do poszczególnych organów.
- **Raporty dotyczące certyfikatów:**
  - Liczba zarejestrowanych certyfikatów.
  - Certyfikaty o wygasającym terminie ważności.
  - Certyfikaty nieważne i archiwalne.

REP.03.02: System musi umożliwiać administratorom generowanie następujących typów raportów:

- **Raporty dotyczące wniosków:**
  - Łączna liczba złożonych wniosków w wybranym okresie.
  - Statusy wniosków (np. w toku, zakończone, odrzucone).
  - Wnioski przypisane do poszczególnych organów.
- **Raporty dotyczące certyfikatów:**
  - Łączna liczba zarejestrowanych certyfikatów.
  - Certyfikaty o wygasającym terminie ważności.
  - Certyfikaty nieważne i archiwalne.
- **Raporty dotyczące załączników:**

- Średnia i maksymalna wielkość załączników.
- Liczba brakujących lub niewłaściwie dodanych dokumentów.

- **Raporty dotyczące użytkowników:**
  - Aktywność użytkowników w systemie (logowania, edycje wniosków, przesyłanie załączników).
  - Lista użytkowników z najwyższą liczbą złożonych wniosków.
- **Raporty wydajności systemu:**
  - Czas realizacji wniosków na różnych etapach.
  - Liczba błędów walidacyjnych zgłaszanych przez użytkowników.
  - Liczba problemów z załącznikami (np. przekroczona wielkość plików).

REP.04: System musi umożliwiać użytkownikowi personalizację raportów, w tym:

- Wybór zakresu danych (np. przedziały czasowe, wybrane organy, typy wniosków).
- Dodawanie i usuwanie kolumn z danymi w tabelach raportowych.
- Tworzenie własnych szablonów raportów z możliwością ich zapisania do ponownego użycia.

SUP. Pomoc techniczna

SUP.01: Moduł „Pomoc Techniczna" musi umożliwiać użytkownikom uzyskanie wsparcia technicznego w zakresie korzystania z systemu oraz procesów wnioskowania.

SUP.02: System musi wspierać różne kanały kontaktu użytkownika z pomocą techniczną:

- Formularz kontaktowy w systemie.
- Pomoc w czasie rzeczywistym (czat online).
- Dostęp do bazy wiedzy i FAQ.

SUP.03: Użytkownik musi mieć możliwość zgłaszania problemów technicznych za pomocą:

- Formularza zgłoszeniowego zawierającego:
  - Opis problemu.

- Zrzuty ekranu lub inne załączniki ilustrujące problem.
- Informację o kroku, na którym wystąpił problem.

SUP.04: System musi automatycznie przypisywać zgłoszenia do odpowiednich kategorii, takich jak:

- Problemy techniczne.
- Błędy walidacji danych.
- Problemy z załącznikami.
- Pytania dotyczące procedur administracyjnych.

SUP.05: Każde zgłoszenie musi być rejestrowane w systemie wraz z:

- Datą i godziną zgłoszenia.
- Unikalnym numerem identyfikacyjnym zgłoszenia.
- Statusami zgłoszenia (np. nowe, w trakcie rozwiązywania, rozwiązane, odrzucone).

SUP.06: System musi umożliwiać użytkownikowi podgląd historii jego zgłoszeń, w tym:

- Status zgłoszenia.
- Odpowiedzi udzielone przez zespół wsparcia.
- Możliwość zamknięcia zgłoszenia przez użytkownika po jego rozwiązaniu.

SUP.07: Moduł musi umożliwiać użytkownikom zgłaszanie zastrzeżeń lub propozycji usprawnień w procedurach wydawania pozwoleń za pomocą:

- Dedykowanego formularza do kontaktu z centralnym organem krajowym.
- Opcji przesłania propozycji lub zastrzeżeń z załącznikami (np. dokumenty, raporty, uwagi).

SUP.08: System musi umożliwiać klasyfikację takich zgłoszeń jako:

- Zastrzeżenia dotyczące procedur administracyjnych.
- Propozycje usprawnień w procesach wydawania pozwoleń.

SUP.09: Zgłoszenia przesyłane do centralnego organu krajowego nie mogą zastępować ani stanowić alternatywy dla istniejących możliwości kontroli administracyjnej lub sądowej, a system musi wyświetlać stosowną informację użytkownikowi przed wysłaniem zgłoszenia.

SUP.10: System musi zawierać bazę wiedzy i FAQ dostępne bez konieczność logowania obejmującą:

- Instrukcje korzystania z systemu.
- Najczęściej zadawane pytania dotyczące procedur administracyjnych i technicznych.
- Opisy rozwiązań dla typowych problemów technicznych.

SUP.11: Użytkownik musi mieć możliwość przeszukiwania bazy wiedzy według słów kluczowych oraz przeglądania kategorii tematycznych bez konieczności logowania.

SUP.12: System musi powiadamiać użytkownika o statusie jego zgłoszenia za pomocą:

- Powiadomień w systemie.
- E-maila z informacją o zmianach statusu zgłoszenia (np. odpowiedź, rozwiązanie problemu).

SUP.13: Powiadomienia o przyjęciu zgłoszenia przez centralny organ krajowy muszą zawierać:

- Numer zgłoszenia.
- Przewidywany czas odpowiedzi (jeśli został określony przez organ).

SUP.14: System musi umożliwiać administratorom generowanie raportów dotyczących zgłoszeń użytkowników, w tym:

- Liczba zgłoszeń w podziale na kategorie.
- Średni czas rozwiązania zgłoszenia.
- Liczba zastrzeżeń/propozycji przesłanych do centralnego organu krajowego.
- Statystyki dotyczące najczęściej zgłaszanych problemów.

ADM. Funkcje administracyjne

ADM.01: System musi zapewniać panel administracyjny umożliwiający zarządzanie użytkownikami, konfigurację systemu, zarządzanie danymi i kontrolę nad wszystkimi modułami.

ADM.02: Panel administracyjny musi być dostępny wyłącznie dla uprawnionych administratorów z odpowiednimi poziomami dostępu.

ADM.03: Administratorzy muszą mieć możliwość zarządzania kontami użytkowników, w tym:

- Tworzenia, edytowania i usuwania kont użytkowników.
- Resetowania haseł i zarządzania metodami uwierzytelniania.
- Przypisywania ról i uprawnień użytkownikom.

ADM.04: System musi umożliwiać definiowanie ról użytkowników i przypisywanie im odpowiednich uprawnień dostępu do modułów i funkcji systemu, takich jak:

- Administratorzy systemowi.
- Administratorzy biznesowi.
- Użytkownicy końcowi.
- Operatorzy wsparcia technicznego.

ADM.05: Administratorzy muszą mieć możliwość konfiguracji podstawowych ustawień systemowych, w tym:

- Definiowania parametrów dla modułów, takich jak maksymalna wielkość załączników, limity czasu na realizację wniosków.
- Zarządzania szablonami formularzy i dokumentów (np. wniosków, certyfikatów).
- Aktualizacji danych referencyjnych (np. TERYT, bazy REGON, słowniki proceduralne).

ADM.06: System musi wspierać konfigurację dynamicznych procedur administracyjnych poprzez moduł definiowania kroków i zależności procesów.

ADM.07: Panel administracyjny musi umożliwiać monitorowanie działań użytkowników i operacji systemowych, w tym:

- Logów logowania i aktywności użytkowników.
- Historii edycji danych i wniosków.
- Informacji o błędach systemowych i zgłoszeniach problemów.

ADM.08: System musi zapewniać mechanizm audytowy umożliwiający administratorom śledzenie:

- Zmian wprowadzonych przez użytkowników.

- Aktualizacji konfiguracji systemu.
- Wysyłek danych do zewnętrznych organów.

ADM.09: Administratorzy muszą mieć możliwość zarządzania danymi systemowymi, w tym:

- Dodawania, modyfikowania i usuwania danych administracyjnych (np. dane organów administracyjnych, szablony procedur).
- Zarządzania archiwami danych, w tym wniosków, certyfikatów i dokumentów.

ADM.10: System musi umożliwiać eksport i import danych administracyjnych w formatach CSV, XLSX lub XML.

ADM.11: Administratorzy muszą mieć możliwość zarządzania systemem powiadomień i alertów, w tym:

- Konfiguracji treści i częstotliwości powiadomień.
- Monitorowania statusów wysyłanych powiadomień.
- Zarządzania powiadomieniami systemowymi dla użytkowników.

ADM.12: System musi umożliwiać konfigurację i kontrolę bezpieczeństwa, w tym:

- Zarządzanie dostępem do danych wrażliwych.
- Konfigurację polityki haseł (np. wymagana złożoność, okres ważności) – patrz SEC. 6.
- Obsługę dwuetapowego uwierzytelniania (2FA) dla wybranych ról.

ADM.13: System musi umożliwiać szybkie blokowanie lub ograniczanie dostępu dla wybranych użytkowników w przypadku podejrzenia nieautoryzowanego dostępu.

ADM.14: Administratorzy muszą mieć możliwość zarządzania modułami systemu, w tym:

- Włączania i wyłączania wybranych modułów.
- Aktualizacji treści w bazie wiedzy i FAQ.
- Dodawania i modyfikacji raportów oraz generowania statystyk systemowych.

ADM.15: System musi umożliwiać administratorom przeprowadzanie aktualizacji w zakresie:

- Wgrywania nowych wersji bazy referencyjnej (np. TERYT, REGON).

- Integracji z zewnętrznymi systemami (np. ePUAP, eDoręczenia, Węzeł Krajowy).

ADM.16: Panel administracyjny musi umożliwiać testowanie integracji z zewnętrznymi systemami przed ich wdrożeniem.

ADM.17: Panel administracyjny musi być dostępny wyłącznie przez zabezpieczone kanały komunikacji (HTTPS, VPN).

ADM.18: System musi zapewniać pełną zgodność z przepisami dotyczącymi ochrony danych osobowych (RODO).

ADM.19: System musi umożliwiać audyt operacji użytkowników i zapisywać logi w dedykowanej tabeli audytowej lub strukturze nierelacyjnej.

INIT. Inicjalne zasilenie systemu procedurami

INIT.01: Wykonawca jest zobowiązany do zasilenia systemu kompletnym zestawem formularzy i procedur w oparciu o załączone dokumenty oraz obowiązujący stan prawny na dzień składania oferty.

INIT.02: Zasilenie systemu obejmuje:

- Formularze zgłoszeń, decyzji i pozwoleń, zgodnie z etapami procesu inwestycyjnego opisanymi w Załącznikach 1 i 2.
- Procedury i zależności między poszczególnymi etapami inwestycji w różne typy instalacji *OZE* (mikroinstalacje, małe instalacje, wielkoskalowe instalacje) i technologii zgodnie z matrycą znajdującą się w Załączniku 2.

INIT.03: Formularze muszą obejmować, co najmniej:

- Formularze zgłoszeniowe dla mikroinstalacji, małych instalacji i wielkoskalowych instalacji OZE z uwzględnieniem technologii.
- Formularze wniosków o:
  - Decyzję środowiskową.
  - Warunki zabudowy (WZ) i wyrysy z miejscowego planu zagospodarowania przestrzennego (MPZP).
  - Pozwolenia na budowę.

- Koncesje na wytwarzanie energii elektrycznej z OZE.

Inne – według informacji w Załącznikach 1 i 2.

INIT.04: Każdy formularz musi być zintegrowany z systemem w sposób umożliwiający automatyczne generowanie dokumentów w oparciu o dane wprowadzone przez użytkowników.

INIT.05: Procedury muszą obejmować wszystkie wymagane w danym przypadku etapy inwestycji, w tym:

- Uzyskanie decyzji o środowiskowych uwarunkowaniach.
- Uzyskanie warunków zabudowy lub potwierdzenie lokalizacji inwestycji za sprawą innych narzędzi planistycznych.
- Uzyskanie pozwoleń środowiskowych.
- Uzyskanie pozwoleń wodnoprawnych.
- Uzyskanie pozwoleń budowlanych (pozwolenia na budowę, pozwolenia na użytkowanie) i zgłoszenia zakończenia robót budowlanych.
- Uzyskanie wpisu do rejestru małych instalacji OZE oraz wpisu do rejestru wytwórców biogazu rolniczego.
- Uzyskanie koncesji na wytwarzanie energii z OZE, koncesji na wytwarzanie ciepła oraz koncesji na magazynowanie energii.

Kompletna lista procedur wynika z Załączników 1 i 2.

INIT.06: Procedury muszą być powiązane z właściwymi organami, zgodnie z przypisaniem kompetencji zawartym w Załączniku 1.

INIT.07: Wykonawca musi zapewnić, że wszystkie wprowadzone formularze i procedury są:

- Zgodne z obowiązującym prawem.
- Zgodne z wymaganiami określonymi przez organy właściwe do wydawania decyzji.

INIT-ADDR. Inicjalne zasilenie bazy adresowej

INIT-ADDR.01: Wykonawca musi przeprowadzić inicjalne zasilenie bazy adresowej jednostek zaangażowanych w procesy wydawania decyzji administracyjnych dotyczących instalacji OZE.

INIT-ADDR.02: Zasilenie bazy musi być wykonane w oparciu o dane dostarczone w załącznikach, a także z uwzględnieniem aktualnych rejestrów publicznych, takich jak:

- TERYT (spis miejscowości, ulic, kodów pocztowych).
- Centralne rejestry organów administracyjnych (np. rejestry RDOŚ, urzędów gmin, powiatów, województw).

INIT-ADDR.03: Każdy rekord w bazie adresowej musi zawierać następujące informacje:

- Nazwa jednostki administracyjnej (np. RDOŚ w Katowicach, Starostwo Powiatowe w Krakowie).
- Adres korespondencyjny (ulica, numer, kod pocztowy, miejscowość).
- ePUAP (jeśli dotyczy).
- eDoręczenia (jeżeli dotyczy).
- Adres e-mail i numer telefonu do kontaktu.
- Typ decyzji, które jednostka jest uprawniona wydawać (np. decyzja o środowiskowych uwarunkowaniach, pozwolenie na budowę).
- Obszar kompetencji (np. gmina, powiat, województwo).

INIT-ADDR.04: Dane do zasilenia bazy muszą być pozyskane z następujących źródeł:

- Dokumentacja załączona do postępowania przetargowego (np. wykaz organów właściwych do wydawania decyzji).
- Centralne rejestry danych publicznych (np. TERYT, REGON).
- Weryfikacja danych kontaktowych jednostek na ich oficjalnych stronach internetowych.

INIT-ADDR.05: Przed wprowadzeniem danych do systemu, **Wykonawca** musi przeprowadzić walidację, w tym:

- Sprawdzenie poprawności i aktualności adresów, numerów telefonów, adresów e-mail i ePUAP, eDoręczeń.

- Weryfikację, czy jednostki są właściwe dla wskazanych typów decyzji i obszarów.
- Zgłaszanie brakujących lub niezgodnych danych Zamawiającemu wraz z propozycją ich uzupełnienia.

INIT-G3L. Uwzględnienie wymagań kamienia milowego G3L

INIT-G3L.0: Wykonawca skonfiguruje system zgodnie z wymaganiami reformy G3.1.1 „Usprawnienie procesu wydawania pozwoleń dotyczących odnawialnych źródeł energii" w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).

INIT-G3L.1: System musi udostępniać (lub linkować) do istniejących stron docelowych, aplikacji lub usług internetowych, umożliwiających użytkownikom rozpoczęcie procesu składania wniosków o pozwolenia dotyczące odnawialnych źródeł energii (OZE) lub do aplikacji internetowej) informacji lub danych, które mogą być udostępniane publicznie.
INIT-G3L.2: System musi integrować i prezentować dane wynikające z funkcjonalności narzędzi informatycznych wskazanych w kamieniach milowych **G10G** i **G11G** (narzędzie informatyczne na potrzeby stosowania nowego modelu regulacyjnego przez Urząd Regulacji Energetyki w ramach reformy G1.1.4 Wsparcie dla instytucji wdrażających reformy i inwestycje w ramach REPowerEU).
INIT-G3L.3: System musi udostępniać informacje wskazane w **lit. b) kamienia milowego G14G**, w szczególności dotyczące:

(i) regularnie aktualizowanych informacji na temat dostępnych zdolności przyłączeniowych do sieci;
(ii) informacji na temat odrzuconych wniosków o przyłączenie, w tym uzasadnienia odrzucenia oraz
(iii) jednolitego zbioru przepisów.

INIT-G3L.4: System musi uwzględniać mapowanie wymagane w ramach kamienia milowego **G1L** (odrębne od niniejszego zlecenie Ministerstwa Klimatu i Środowiska) oraz umożliwiać prezentację wyników tego mapowania, w tym:

- dostępność gruntów,
- sieci przesyłowe,
- lokalizacje zasobów energetycznych.

INIT-G3L.5: System musi zawierać informacje i funkcjonalności związane z obszarami przyspieszonego rozwoju energii ze źródeł odnawialnych wskazanymi w kamieniu milowym **G2L:**

(i) właściwe organy odpowiedzialne za wyznaczanie obszarów przyspieszonego rozwoju energii ze źródeł odnawialnych,
(ii) ich obowiązki, w tym w odniesieniu do zapewnienia, aby wyznaczenie obszarów przyspieszonego rozwoju energii ze źródeł odnawialnych nie miało negatywnego wpływu na ochronę przyrody i różnorodności biologicznej, oraz
(iii) procedury wydawania pozwoleń dotyczące lądowych instalacji wiatrowych i instalacji fotowoltaicznych, które mają zastosowanie do obszarów przyspieszonego rozwoju energii ze źródeł odnawialnych.

INIT-G3L.6: System musi umożliwiać transparentne udostępnianie danych publicznych wynikających z kamieni milowych, z zachowaniem zasad interoperacyjności i otwartości danych publicznych.
INIT-G3L.7: System musi zapewnić integrację funkcjonalności z narzędziami administracyjnymi wspierającymi proces decyzyjny dla jednostek administracji publicznej oraz inwestorów.

PRF. Wymagania wydajnościowe

Czas odpowiedzi systemu

- **PRF.1.1** Czas odpowiedzi systemu na zapytania w 95% przypadków, w szczególności na wygenerowanie strony WWW (przy założeniu wielkości strony 1 MB) na serwerze, nie może przekraczać 2 sekund przy maksymalnie 200 użytkownikach jednoczesnych.
- **PRF.1.2** System musi utrzymywać czas odpowiedzi na zapytania nieprzekraczający 3 sekund w 99% przypadków w scenariuszach z maksymalnym obciążeniem.
- **PRF.1.3** Czas generowania strony powinien być regularnie monitorowany i raportowany w czasie rzeczywistym, a wszelkie przekroczenia limitów wydajności muszą generować alerty.
- **PRF.1.4** Weryfikacja parametrów czasów odpowiedzi będzie przeprowadzana przy użyciu narzędzi takich jak JMeter lub innych równoważnych zatwierdzonych przez **Zamawiającego**.

Skalowalność

- **PRF.2.1** Platforma musi wspierać dynamiczną skalowalność, aby umożliwić obsługę dodatkowego obciążenia przekraczającego pierwotny limit 200 użytkowników. Skalowalność powinna być elastyczna, z możliwością automatycznego zwiększania zasobów.

- **PRF.2.2** System musi utrzymać czas odpowiedzi poniżej 2 sekund nawet w przypadku wzrostu obciążenia o 25% powyżej standardowej liczby użytkowników jednoczesnych (czyli do 250 użytkowników).
- **PRF.2.3** W celu zapewnienia skalowalności system powinien mieć opcję rozdzielania obciążenia na wiele serwerów lub instancji.

Zarządzanie pamięcią podręczną (cache)

- **PRF.3.1** Platforma musi umożliwiać konfigurację parametrów pamięci podręcznej, w szczególności czasu życia cache (TTL) oraz parametrów zależnych od typu informacji, takich jak treści statyczne (np. obrazy, style) oraz dynamiczne.
- **PRF.3.2** Dla treści dynamicznych (np. strony generowane na podstawie zapytań do bazy danych), system powinien umożliwiać ustawienia pozwalające na elastyczne, indywidualne dopasowanie TTL i odświeżania cache na poziomie poszczególnych zasobów.
- **PRF.3.3** System musi zapewniać mechanizmy monitorowania i zarządzania cache, tak aby użytkownicy mieli dostęp do najnowszych informacji, a jednocześnie by było zachowane odpowiednie wykorzystanie zasobów.

Monitorowanie i raportowanie wydajności

- **PRF.4.1** System powinien posiadać funkcje monitorowania i raportowania kluczowych parametrów wydajnościowych, takich jak średni czas odpowiedzi, liczba użytkowników jednoczesnych, obciążenie procesora i pamięci, z interwałem pomiarowym nie dłuższym niż 5 minut.
- **PRF.4.2** Narzędzia monitorujące powinny być w stanie przechowywać historyczne dane na temat wydajności przez co najmniej 3 miesiące, umożliwiając analizę trendów i podejmowanie działań optymalizacyjnych.
- **PRF.4.3** Wszelkie alerty o przekroczeniu wartości progowych (np. czasu odpowiedzi) powinny być przesyłane do administratora w formie powiadomień e-mail lub SMS, umożliwiając szybką reakcję na problem.

Diagnoza i rozwiązywanie problemów z wydajnością

- **PRF.5.1** System musi mieć zintegrowane mechanizmy logowania i diagnostyki, umożliwiające rejestrowanie zdarzeń związanych z wydajnością, takich jak przeciążenia lub błędy w cache, aby przyspieszyć proces analizy problemów.
- **PRF.5.2** System powinien umożliwiać dostęp do logów w czasie rzeczywistym oraz oferować wsparcie dla narzędzi analitycznych, które pozwalają na szybką lokalizację i identyfikację wąskich gardeł w procesach obsługi zapytań użytkowników.

Zgodność z narzędziami pomiarowymi

- **PRF.6.1** System musi być kompatybilny z narzędziami takimi jak *JMeter* lub równoważnymi, umożliwiającymi symulację obciążenia i monitorowanie wydajności zgodnie z wymaganymi wskaźnikami.
- **PRF.6.2** Narzędzia używane do testowania wydajności powinny pozwalać na generowanie raportów z testów obciążeniowych i wytrzymałościowych oraz udostępniać wyniki w formatach akceptowanych przez **Zamawiającego**.

SEC. Wymagania bezpieczeństwa

SEC.1: Zabezpieczenie przed atakami na systemy informatyczne

- **Walidacja danych**: System musi wykonywać szczegółową walidację wszystkich danych wprowadzanych przez użytkowników, zwłaszcza w polach formularzy i w adresach URL. Należy zapewnić ochronę przed atakami ujętymi w zestawieniach *OWASP*, w szczególności w odniesieniu do zagrożeń, takich jak SQL Injection, XSS, CSRF, oraz ataki spamowe.
- **Autoryzacja dostępu**: System może być dostępny tylko dla uwierzytelnionych użytkowników, z wyjątkiem anonimowych użytkowników, którzy mogą korzystać z części informacyjnej aplikacji.
- **Bezpieczne połączenie**: Komunikacja powinna być szyfrowana protokołem HTTPS z certyfikatem SSL dla bezpieczeństwa transmisji danych.

SEC.2: Resetowanie haseł

- **Bezpieczny proces resetowania haseł**: System musi umożliwiać resetowanie haseł użytkowników przez wysłanie linku na adres e-mail użytkownika oraz hasła na podany numer komórkowy, co pozwoli na zmianę hasła. Proces ten powinien uwzględniać zabezpieczenia przed nieuprawnionym dostępem.

SEC.3: Dostęp do logów zdarzeń

- **Interfejs administracyjny**: Administrator musi mieć dostęp do logów zdarzeń systemowych poprzez interfejs administracyjny. Logi powinny być segregowane według parametrów, takich jak data, przedział czasowy, użytkownik, identyfikator, oraz rodzaj czynności.
- **Eksport logów**: System musi umożliwiać administratorowi eksport logów w celu archiwizacji lub dalszej analizy.

SEC.4: Audyt operacji użytkowników

- **Rejestracja operacji**: System musi odnotowywać każdą operację wykonywaną przez użytkowników, w tym identyfikator użytkownika oraz datę i godzinę wykonania operacji. Dane te powinny być zabezpieczone przed nieautoryzowaną modyfikacją.

SEC.5: Zabezpieczenie logów zdarzeń

- **Niezmienność i ochrona logów**: System musi posiadać mechanizmy uniemożliwiające edycję oraz usuwanie plików z logami zdarzeń. Dodatkowo należy zapobiegać przepełnieniu logów, co mogłoby prowadzić do utraty danych.

SEC.6: Reguły dla haseł użytkowników

- **Definicja reguł haseł**: System musi umożliwiać definiowanie zasad dotyczących siły haseł dla różnych grup użytkowników, obejmujących:
    - Minimalną i maksymalną długość hasła,
    - Wymóg użycia znaków alfanumerycznych oraz specjalnych,
    - Okres ważności hasła,
    - Liczbę zapamiętanych haseł, które są zablokowane przed ponownym użyciem.

SEC.7: Monitorowanie prób naruszenia bezpieczeństwa

- **Wykrywanie prób nieuprawnionego dostępu**: System musi monitorować próby naruszenia bezpieczeństwa, rejestrując m.in. nieudane próby logowania, ostrzeżenia systemowe oraz błędy w celu odpowiedniej reakcji na potencjalne zagrożenia.

SEC.8: Monitorowanie operacji uprzywilejowanych

- **Audyt operacji administracyjnych**: System musi umożliwiać monitorowanie operacji uprzywilejowanych, takich jak wykorzystanie uprawnień administratora, uruchamianie, a także inne działania o wysokim poziomie dostępu.

SEC.9: Odporność na zagrożenia OWASP10

- **Odporność na zagrożenia**: System musi być odporny na zagrożenia wymienione w OWASP Top Ten, zapewniając ochronę przed najczęstszymi atakami bezpieczeństwa.
- **Przykłady zagrożeń**: System powinien być zabezpieczony przed zagrożeniami takimi jak:
    - Ataki semantyczne na adres URL,
    - Wstrzykiwanie kodu SQL,

- XSS (Cross-Site Scripting),
- CSRF (Cross-Site Request Forgery),
- Przechwytywanie i kradzież sesji oraz cookies,
- Trawersowanie katalogów,
- Wstrzykiwanie poleceń systemowych.

SEC.10: Zabezpieczenie formularzy publicznych

Captcha na formularzach: Wszystkie formularze dostępne dla użytkowników nieautoryzowanych, które zapisują dane do bazy, muszą posiadać zabezpieczenie typu CAPTCHA, aby zapobiec automatycznym, nieuprawnionym wprowadzaniom danych do systemu.

SEC.11: System musi zapewniać szyfrowanie przesyłanych danych za pomocą protokołu HTTPS.

SEC.12: Ochrona przed nieautoryzowanym dostępem: blokowanie adresów IP

System musi posiadać mechanizmy automatycznego reagowania na próby nieautoryzowanego dostępu, w tym funkcjonalność **blokowania adresów IP**, z których pochodzą podejrzane lub złośliwe działania. W szczególności:

SEC.12.1: Automatyczne wykrywanie nieautoryzowanego dostępu:

- System powinien monitorować próby logowania i inne działania związane z uwierzytelnianiem oraz dostępem do zasobów systemu,
- Detekcja powinna obejmować m.in.:
  - wielokrotne błędne logowania (brute-force),
  - próby dostępu do zastrzeżonych zasobów bez autoryzacji,
  - próby eskalacji uprawnień.

SEC.12.2:Zasady blokowania IP:

- Możliwość zdefiniowania reguł (np. blokada po 5 nieudanych próbach logowania w ciągu 10 minut),
- Możliwość blokady tymczasowej (np. 30 minut) lub trwałej – zgodnie z polityką bezpieczeństwa Zamawiającego,
- Możliwość konfiguracji wyjątków (whitelisting) dla zaufanych adresów IP.

SEC.12.3: Zarządzanie listą zablokowanych adresów IP:

- Interfejs administratora umożliwiający podgląd i zarządzanie listą zablokowanych IP,
- Możliwość ręcznego dodawania i usuwania adresów IP,
- Historia zablokowań i przyczyny (log aktywności bezpieczeństwa).

SEC.12.4: Powiadamianie i logowanie:

- Automatyczne logowanie każdego przypadku blokady IP do systemu audytowego,
- Możliwość konfiguracji powiadomień (e-mail/SIEM/webhook) dla administratorów o zdarzeniach związanych z bezpieczeństwem.

SEC.12.5: Zgodność z polityką bezpieczeństwa:

- Mechanizmy muszą być zgodne z polityką bezpieczeństwa Zamawiającego oraz zaleceniami OWASP i normą ISO/IEC 27001 w zakresie zarządzania dostępem i reagowania na incydenty.

12. Warunki równoważności

Zamawiający określa następujące warunki równoważności dla standardów i technologii, na które powołano się w niniejszej dokumentacji.

CISA	Ilekroć w specyfikacji zamówienia wskazano wymóg posiadania certyfikacji *CISA* (*Certified Information Systems Auditor*), dopuszcza się stosowanie certyfikacji równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny poziom wiedzy, umiejętności i doświadczenia w zakresie audytu systemów IT, zarządzania ryzykiem oraz ochrony zasobów informacyjnych. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym zakres certyfikacji oraz wymagania dotyczące doświadczenia zawodowego. Dopuszcza się stosowanie certyfikacji równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres wiedzy i egzaminu** Certyfikacja musi obejmować wiedzę i umiejętności w zakresie audytu systemów IT, zarządzania ryzykiem oraz ochrony zasobów informacyjnych, w szczególności: • **Planowanie i prowadzenie audytu systemów informatycznych** • **Zarządzanie ryzykiem i kontrola wewnętrzna** • **Zarządzanie cyklem życia systemów IT i ich infrastrukturą** • **Ochrona zasobów informacyjnych i bezpieczeństwo IT** • **Zarządzanie incydentami i ciągłością działania** Egzamin certyfikacyjny musi sprawdzać znajomość powyższych zagadnień oraz ich praktyczne zastosowanie. **1.2. Wymogi dotyczące doświadczenia** Certyfikacja musi wymagać od kandydata: • Minimum **5 lat doświadczenia zawodowego** w obszarze audytu systemów IT, zarządzania ryzykiem lub bezpieczeństwa informacji. • Możliwości skrócenia wymaganego doświadczenia o **1–2 lata**, jeśli kandydat posiada inne uznane certyfikaty branżowe lub wyższe wykształcenie w dziedzinie technologii informacyjnych, audytu lub cyberbezpieczeństwa. **1.3. Proces weryfikacji kompetencji** Certyfikacja musi spełniać następujące wymagania: • Egzamin musi być przeprowadzany przez **niezależną organizację certyfikującą**, posiadającą uznanie na rynku międzynarodowym. • Certyfikacja musi podlegać **procesowi odnawiania** (np. poprzez wymagane punkty CPE – Continuing

	Professional Education lub inne mechanizmy utrzymania wiedzy). **1.4. Kodeks etyczny** Certyfikacja musi zobowiązywać posiadacza do przestrzegania kodeksu etycznego w zakresie: • Zgodności z zasadami audytu i ochrony informacji. • Przeciwdziałania konfliktowi interesów w audycie IT. • Działania zgodnie z najlepszymi praktykami audytorskimi i standardami bezpieczeństwa informacji. **1.5. Przykładowe certyfikaty uznawane za równoważne** Za równoważne będą uznane certyfikaty, pod warunkiem spełnienia powyższych kryteriów. Certyfikaty niewymagające przeprowadzania dowodu: • **CIA (Certified Internal Auditor)** – The Institute of Internal Auditors (IIA) • **CRISC (Certified in Risk and Information Systems Control)** – ISACA • **GIAC Systems and Network Auditor (GSNA)** – SANS Institute **1.6. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. Opis certyfikacji, jej zakresu oraz wymagań egzaminacyjnych. 2. Dokument potwierdzający wymagania dotyczące doświadczenia zawodowego. 3. Informacje dotyczące akredytacji organizacji certyfikującej. 4. Kodeks etyczny obowiązujący posiadaczy certyfikacji. **1.7. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedstawionej dokumentacji pod kątem zgodności z wymaganiami. • Zasięgnięcia opinii eksperckiej w celu potwierdzenia równoważności certyfikacji. • Przeprowadzenia dodatkowych testów lub wywiadów weryfikujących kompetencje osoby wskazanej przez wykonawcę.
CISSP	Ilekroć w specyfikacji zamówienia wskazano wymóg posiadania certyfikacji *CISSP* (*Certified Information Systems Security Professional*), dopuszcza się stosowanie certyfikacji równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny poziom wiedzy, umiejętności i doświadczenia w zakresie bezpieczeństwa informacji. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym opis zakresu

	certyfikacji, wymagań dotyczących doświadczenia oraz kodeksu etycznego." Dopuszcza się stosowanie certyfikacji równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres wiedzy i egzaminu** Certyfikacja musi obejmować wiedzę i umiejętności w zakresie przynajmniej następujących obszarów: • **Bezpieczeństwo i zarządzanie ryzykiem** • **Bezpieczeństwo zasobów** • **Architektura i inżynieria bezpieczeństwa** • **Bezpieczeństwo komunikacji i sieci** • **Zarządzanie tożsamością i dostępem (IAM)** • **Ocena i testowanie bezpieczeństwa** • **Operacje bezpieczeństwa** • **Bezpieczeństwo w rozwoju oprogramowania** Certyfikat równoważny musi być oparty na egzaminie teoretycznym i/lub praktycznym sprawdzającym wiedzę w powyższych obszarach. **1.2. Wymogi dotyczące doświadczenia** Certyfikacja musi wymagać od kandydata: • Minimum **5 lat doświadczenia zawodowego** w co najmniej dwóch z wyżej wymienionych obszarów. • Możliwości skrócenia wymaganego doświadczenia o **1 rok**, jeśli kandydat posiada inne uznane certyfikaty branżowe lub wyższe wykształcenie w dziedzinie cyberbezpieczeństwa lub technologii informacyjnych. **1.3. Proces weryfikacji kompetencji** Certyfikacja musi spełniać następujące wymagania: • Egzamin powinien być nadzorowany przez **niezależną organizację certyfikującą**, posiadającą akredytację ISO/IEC 17024 lub równoważną. • Certyfikat musi podlegać **procesowi odnawiania** i wymagać od posiadacza **utrzymywania kompetencji** (np. poprzez zdobywanie punktów CPE – Continuing Professional Education). **1.4. Kodeks etyczny** Certyfikacja musi zobowiązywać posiadacza do przestrzegania kodeksu etycznego obejmującego co najmniej: • Ochronę interesu publicznego i zgodność z regulacjami prawnymi. • Przeciwdziałanie nadużyciom w zakresie cyberbezpieczeństwa. • Zobowiązanie do działania zgodnie z najlepszymi praktykami i standardami w dziedzinie bezpieczeństwa informacji. **1.5. Przykładowe certyfikaty uznawane za równoważne** Za równoważne będą uznane certyfikacje, pod warunkiem spełnienia powyższych kryteriów.

	Certyfikacje niewymagające przedstawiania dowodów: • **CISM (Certified Information Security Manager)** – ISACA • **GIAC Security Leadership (GSLC)** – SANS Institute **1.6. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność certyfikacji, w tym: 1. Opis certyfikacji, jej zakresu oraz wymagań egzaminacyjnych. 2. Dokument potwierdzający wymagania dotyczące doświadczenia zawodowego. 3. Informacje dotyczące akredytacji organizacji certyfikującej. 4. Kodeks etyczny obowiązujący posiadaczy certyfikacji. **1.7. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedstawionej dokumentacji pod kątem zgodności z wymaganiami. • Zasięgnięcia opinii eksperckiej w celu potwierdzenia równoważności certyfikacji. • Przeprowadzenia dodatkowych testów lub wywiadów weryfikujących kompetencje osoby wskazanej przez wykonawcę.
CMMI	Ilekroć w opisie przedmiotu zamówienia wskazano wymóg stosowania modelu *CMMI (Capability Maturity Model Integration*), dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny zakres i poziom zarządzania oraz doskonalenia procesów organizacyjnych. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym szczegóły dotyczące poziomów dojrzałości, obszarów procesów oraz metod oceny. Dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres i poziom zarządzania procesami** Równoważne rozwiązanie musi zapewniać: • **Podejście procesowe do zarządzania organizacją**, uwzględniające ciągłe doskonalenie i optymalizację działań. • **Strukturyzowaną metodę oceny dojrzałości procesów**, pozwalającą na ich mierzalną poprawę. • **Zgodność z międzynarodowymi standardami zarządzania jakością i procesami**, np. ISO 9001, ISO/IEC 33000, ITIL, COBIT. **1.2. Poziomy dojrzałości i ocena procesów**

	Równoważne rozwiązanie musi obejmować system oceny dojrzałości organizacji w zakresie procesów, który spełnia następujące wymagania: • Podział na co najmniej **pięć poziomów dojrzałości**, analogicznych do modelu CMMI: 1. **Poziom początkowy (Initial)** – nieustrukturyzowane, ad hoc podejście do zarządzania procesami. 2. **Poziom zarządzany (Managed)** – ustrukturyzowane i powtarzalne procesy zarządzania. 3. **Poziom zdefiniowany (Defined)** – standaryzowane procesy oparte na dokumentacji i najlepszych praktykach. 4. **Poziom ilościowo zarządzany (Quantitatively Managed)** – pomiar i kontrola procesów w oparciu o dane i wskaźniki. 5. **Poziom optymalizacyjny (Optimizing)** – ciągłe doskonalenie i innowacje w procesach. • Możliwość przeprowadzania audytów i ocen procesów zgodnie z metodologią oceny zgodną z CMMI Appraisal Method. **1.3. Obszary procesów** Równoważne rozwiązanie musi obejmować przynajmniej następujące obszary: • **Zarządzanie projektami i programami** – określenie standardów planowania, realizacji i monitorowania projektów. • **Zarządzanie ryzykiem** – identyfikacja, analiza i monitorowanie ryzyka w organizacji. • **Zarządzanie jakością i doskonalenie procesów** – wdrażanie działań zapewniających jakość oraz mechanizmów optymalizacji. • **Zarządzanie zasobami ludzkimi i kompetencjami** – rozwój i ocena kompetencji pracowników zgodnie z potrzebami organizacji. • **Inżynieria i rozwój produktów lub usług** – stosowanie najlepszych praktyk w zakresie wytwarzania i testowania rozwiązań. • **Bezpieczeństwo informacji** – zapewnienie odpowiedniego poziomu ochrony zasobów informacyjnych. **1.4. Metodologia oceny i certyfikacji** Równoważne rozwiązanie musi umożliwiać formalną ocenę poziomu dojrzałości procesów, przeprowadzaną przez:

	• **Niezależną jednostkę certyfikującą** lub audytora posiadającego uprawnienia do oceny modelu procesowego. • Metodologię oceny porównywalną do **CMMI Appraisal Method (np. SCAMPI)** lub inną, zapewniającą rzetelne i obiektywne wyniki. • Dokumentację procesów oraz raporty z przeprowadzonych audytów, potwierdzające poziom dojrzałości organizacji. **1.5. Przykładowe modele uznawane za równoważne** Za modele równoważne będą uznane standardy, pod warunkiem spełnienia powyższych kryteriów. Standardy uznane za równoważne (bez przeprowadzania dowodów): • **ISO/IEC 33000 (SPICE – Software Process Improvement and Capability Determination)** • **ITIL (Information Technology Infrastructure Library) – poziom Managed lub wyższy** • **COBIT (Control Objectives for Information and Related Technologies) – Governance & Management Framework** • **Lean Six Sigma – ocena poziomu dojrzałości organizacyjnej w zakresie doskonalenia procesów** **1.6. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. Opis modelu procesowego i systemu oceny dojrzałości. 2. Raporty z przeprowadzonych audytów lub certyfikat potwierdzający spełnienie wymagań. 3. Dokumentację potwierdzającą zakres stosowanych procesów oraz metod zarządzania nimi. 4. Szczegóły dotyczące poziomów dojrzałości, metodologii oceny oraz niezależnej jednostki certyfikującej. **1.7. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedstawionej dokumentacji pod kątem zgodności z wymaganiami. • Zasięgnięcia opinii eksperckiej w celu potwierdzenia równoważności zastosowanego modelu. • Przeprowadzenia audytu lub dodatkowych testów, weryfikujących zgodność stosowanego rozwiązania z wymaganiami.
ePUAP	Brak równoważności, ze względu na umocowanie prawne rozwiązania.
eDoręczenia	Brak równoważności, ze względu na umocowanie prawne rozwiązania.

Google Analytics	Aby usługa analityczna mogła być uznana za równoważną z Google Analytics, powinna spełniać następujące warunki: 1. **Funkcjonalność Analityczna**: ○ **Zbieranie danych o ruchu**: Możliwość śledzenia wizyt, unikalnych użytkowników, źródeł ruchu, zachowań na stronie, konwersji itp. ○ **Raportowanie i Analiza**: Dostęp do zaawansowanych narzędzi raportowania, segmentacji danych oraz analizy w czasie rzeczywistym. ○ **Integracje**: Możliwość integracji z innymi narzędziami marketingowymi i reklamowymi. 2. **Zgodność z RODO (GDPR)**: ○ **Ochrona danych osobowych**: Zapewnienie, że przetwarzanie danych odbywa się zgodnie z przepisami o ochronie danych osobowych. ○ **Anonimizacja danych**: Możliwość anonimizacji adresów IP i innych danych osobowych. ○ **Kontrola nad danymi**: Umożliwienie użytkownikom dostępu do swoich danych oraz ich usunięcia na żądanie. 3. **Bezpieczeństwo Danych**: ○ **Szyfrowanie**: Dane powinny być przesyłane i przechowywane w formie zaszyfrowanej. ○ **Certyfikacje**: Posiadanie certyfikatów bezpieczeństwa, takich jak ISO 27001. 4. **Lokalizacja Serwerów**: ○ **Przechowywanie danych w UE**: Dane powinny być przechowywane na serwerach zlokalizowanych w Unii Europejskiej lub w krajach uznanych za zapewniające odpowiedni poziom ochrony danych. 5. **Transparentność**: ○ **Polityka prywatności**: Jasne i przejrzyste informacje o tym, jakie dane są zbierane i w jaki sposób są wykorzystywane. ○ **Zgody użytkowników**: Mechanizmy umożliwiające uzyskanie świadomej zgody od użytkowników na przetwarzanie ich danych. 6. **Interoperacyjność**: ○ **Otwarte standardy**: Wsparcie dla standardowych formatów danych i protokołów komunikacyjnych. ○ **API**: Dostępność interfejsów programistycznych umożliwiających integrację z innymi systemami.

	7. **Wsparcie Techniczne i Dokumentacja**: ○ **Pomoc techniczna**: Dostęp do wsparcia w języku polskim lub angielskim. ○ **Dokumentacja**: Pełna i aktualna dokumentacja użytkownika oraz deweloperska. 8. **Skalowalność i Wydajność**: ○ **Obsługa dużego ruchu**: Zdolność do efektywnego przetwarzania danych z witryn o wysokim natężeniu ruchu. ○ **Czas odpowiedzi**: Szybkie przetwarzanie i dostęp do danych. 9. **Koszty i Licencjonowanie**: ○ **Przejrzystość kosztów**: Jasne warunki cenowe, bez ukrytych opłat. ○ **Model licencyjny**: Warunki licencji powinny być porównywalne lub korzystniejsze niż w przypadku Google Analytics. 10. **Brak Konfliktu Interesów**: ○ **Niezależność**: Usługa nie powinna wykorzystywać danych do własnych celów marketingowych ani udostępniać ich stronom trzecim bez wyraźnej zgody. **Uwagi dodatkowe**: • **Transfer Danych do Krajów Trzecich**: Jeśli dane są przekazywane poza EOG, muszą być zastosowane odpowiednie mechanizmy prawne, takie jak standardowe klauzule umowne lub wiążące reguły korporacyjne. • **Aktualizacje i Rozwój**: Regularne aktualizacje systemu w celu zapewnienia bezpieczeństwa i zgodności z najnowszymi standardami. • **Doświadczenie Użytkownika**: Intuicyjny interfejs użytkownika oraz dostępność szkoleń i materiałów edukacyjnych.
HTTP/HTTPS	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
ISO 9001	Ilekroć w opisie przedmiotu zamówienia wskazano wymóg stosowania standardu *ISO 9001*: Systemy zarządzania jakością, dopuszcza się zastosowanie standardów równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny poziom zarządzania jakością, zgodnie z wymaganiami klientów, regulacji oraz zasadami ciągłego doskonalenia. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym opis wdrożonego systemu oraz certyfikacji. Dopuszcza się zastosowanie standardów równoważnych, pod warunkiem że spełniają one następujące kryteria:

	1.1. Zakres zarządzania jakością Równoważny system zarządzania jakością musi zapewniać: • **Orientację na klienta** – wdrożenie zasad zarządzania jakością zgodnie z wymaganiami klientów oraz interesariuszy. • **Zgodność z przepisami prawnymi i regulacyjnymi**, dotyczącymi jakości usług, produktów oraz procesów. • **Podejście procesowe** – identyfikację, monitorowanie i optymalizację procesów organizacyjnych. • **Ciągłe doskonalenie** – mechanizmy stałej poprawy jakości, analizę ryzyk i działań korygujących. • **Odpowiedzialność kierownictwa** – zobowiązanie do wdrażania polityki jakości oraz nadzorowania jej realizacji. • **Zaangażowanie pracowników** – określenie kompetencji, szkoleń i zakresu odpowiedzialności w zakresie jakości. • **Oparte na dowodach podejmowanie decyzji** – wykorzystanie audytów, analiz oraz danych do oceny skuteczności systemu jakości. **1.2. Wymogi dotyczące certyfikacji** Równoważny system zarządzania jakością musi: • Być **wdrożony i certyfikowany** przez niezależną organizację certyfikującą. • Obejmować **cykliczne audyty wewnętrzne i zewnętrzne**, zapewniające zgodność z wymaganiami jakościowymi. • Zapewniać mechanizmy identyfikacji, analizy oraz redukcji ryzyk wpływających na jakość usług i produktów. **1.3. Standardy uznawane za równoważne** Za systemy zarządzania jakością równoważne wobec ISO 9001 będą uznane, pod warunkiem spełnienia powyższych kryteriów. Standardy niewymagające postępowania dowodowego: • **EFQM (European Foundation for Quality Management)** – Model doskonałości organizacyjnej. • **TQM (Total Quality Management)** – Całościowe zarządzanie jakością. • **Malcolm Baldrige National Quality Award (MBNQA)** – Standard zarządzania jakością i doskonałością organizacyjną. **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. Opis wdrożonego systemu zarządzania jakością, obejmujący zakres działań oraz kluczowe zasady zarządzania.

	2. Certyfikat potwierdzający wdrożenie systemu, wydany przez niezależną jednostkę certyfikującą. 3. Raporty z audytów wewnętrznych lub zewnętrznych potwierdzające zgodność systemu z zasadami ISO 9001 lub innymi równoważnymi normami. 4. Dokumentację potwierdzającą metody oceny jakości, mechanizmy ciągłego doskonalenia oraz działania korygujące. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedłożonej dokumentacji pod kątem spełnienia wymagań. • Konsultacji eksperckiej w celu potwierdzenia równoważności zastosowanego systemu. • Przeprowadzenia audytu lub oceny zgodności metod zarządzania jakością z wymogami ISO 9001.
ISO/IEC 12207	Ilekroć w specyfikacji zamówienia wskazano wymóg stosowania standardu ISO/IEC 12207, dopuszcza się rozwiązania równoważne, pod warunkiem że oferowane rozwiązanie zapewnia zarządzanie cyklem życia oprogramowania w sposób zgodny z kluczowymi wymaganiami określonymi w normie ISO/IEC 12207. **Wykonawca** zobowiązany jest do przedstawienia dokumentacji potwierdzającej równoważność, w tym opisu procesów i ich zgodności z wymaganiami prawnymi oraz technicznymi. **Zapis dotyczący równoważności standardu ISO/IEC 12207** 1. **Stosowanie standardu ISO/IEC 12207 lub rozwiązania równoważnego** W przypadku, gdy w specyfikacji zamówienia wskazano wymóg stosowania standardu **ISO/IEC 12207: Systemy i inżynieria oprogramowania – procesy cyklu życia oprogramowania**, dopuszcza się zastosowanie standardów równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zarządzanie cyklem życia oprogramowania** Równoważne rozwiązanie musi zapewniać: • **Kompleksowe zarządzanie cyklem życia oprogramowania**, obejmujące rozwój, wdrażanie, utrzymanie i utylizację systemów informatycznych. • **Strukturyzowane podejście do procesów inżynierii oprogramowania**, uwzględniające zarówno rozwój dedykowany, jak i integrację gotowych komponentów. • **Zgodność z wymaganiami technicznymi i prawnymi**, w tym dotyczącymi bezpieczeństwa, interoperacyjności oraz jakości kodu. **1.2. Kluczowe procesy zarządzania oprogramowaniem**

	Równoważne rozwiązanie musi obejmować co najmniej następujące obszary: 1. **Procesy podstawowe**: ○ **Procesy wytwarzania oprogramowania** – od analizy wymagań po implementację i testowanie. ○ **Procesy eksploatacji i utrzymania** – zapewnienie działania i rozwoju systemów informatycznych po wdrożeniu. 2. **Procesy wspierające**: ○ **Zarządzanie konfiguracją** – identyfikacja i kontrola zmian w oprogramowaniu. ○ **Zarządzanie jakością** – zapewnienie zgodności produktu z wymaganiami oraz jego ciągłe doskonalenie. ○ **Zarządzanie dokumentacją** – organizacja i archiwizacja dokumentacji technicznej systemu. 3. **Procesy organizacyjne**: ○ **Zarządzanie projektami IT** – planowanie, nadzorowanie i kontrola projektów związanych z rozwojem oprogramowania. ○ **Zarządzanie ryzykiem IT** – identyfikacja, analiza i minimalizacja ryzyk związanych z oprogramowaniem. ○ **Zarządzanie bezpieczeństwem informacji** – stosowanie odpowiednich mechanizmów ochrony danych i kontroli dostępu. **1.3. Standardy uznawane za równoważne** Za równoważne mogą będą uznane standardy zarządzania cyklem życia oprogramowania, pod warunkiem że spełniają powyższe kryteria. Przykładowe standardy nie wymagające postępowania dowodowego: • **CMMI for Development (Capability Maturity Model Integration)** – model dojrzałości organizacyjnej w zakresie inżynierii oprogramowania. • **ISO 90003** – Wytyczne dotyczące stosowania ISO 9001 w inżynierii oprogramowania. **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis wdrożonego systemu zarządzania cyklem życia oprogramowania**, uwzględniający kluczowe procesy i ich zgodność z ISO/IEC 12207. 2. **Certyfikaty potwierdzające wdrożenie systemu zarządzania jakością w obszarze inżynierii oprogramowania**, jeśli dotyczy.

	3. **Raporty z audytów technicznych**, potwierdzające stosowanie praktyk zgodnych ze standardem ISO/IEC 12207. 4. **Dokumentację procesów inżynierii oprogramowania**, w tym procedury zarządzania zmianą, jakością i konfiguracją. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności zastosowanego standardu. • Przeprowadzenia dodatkowych testów lub audytów weryfikujących zgodność zarządzania cyklem życia oprogramowania z wymaganiami ISO/IEC 12207.
ISO/IEC 25010	Ilekroć w opisie przedmiotu zamówienia wskazano wymóg stosowania normy ISO/IEC 25010, dopuszcza się rozwiązania równoważne, pod warunkiem że oferowane rozwiązanie zapewnia ocenę jakości oprogramowania w sposób zgodny z cechami i zasadami opisanymi w normie ISO/IEC 25010. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym opis metod oceny, charakterystyk jakościowych oraz sposób raportowania wyników. Dopuszcza się zastosowanie standardów równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Kryteria jakości oprogramowania** Równoważne rozwiązanie musi zapewniać ocenę jakości oprogramowania w sposób zgodny z następującymi **charakterystykami jakościowymi**, określonymi w normie ISO/IEC 25010: 1. **Funkcjonalność (Functional Suitability)** o Poprawność działania funkcji o Kompleksowość i adekwatność funkcji względem wymagań 2. **Wydajność i efektywność (Performance Efficiency)** o Czas odpowiedzi i przepustowość systemu o Zużycie zasobów (CPU, pamięć, sieć) o Skalowalność 3. **Zgodność (Compatibility)** o Interoperacyjność z innymi systemami o Zgodność z wymaganymi standardami 4. **Użyteczność (Usability)** o Intuicyjność i łatwość obsługi o Dostępność dla użytkowników (zgodność z WCAG, ergonomia interfejsu) 5. **Niezawodność (Reliability)** o Odporność na błędy

	o Dostępność systemu o Odzyskiwanie po awarii 6. **Bezpieczeństwo (Security)** o Ochrona przed atakami i nieautoryzowanym dostępem o Szyfrowanie i uwierzytelnianie o Integralność danych 7. **Konserwowalność (Maintainability)** o Modułowość i łatwość wprowadzania zmian o Czytelność kodu i dokumentacji o Testowalność 8. **Przenaszalność (Portability)** o Możliwość migracji na inne środowiska o Niezależność od platformy **1.2. Metody oceny jakości oprogramowania** Równoważne rozwiązanie musi zapewniać systematyczne podejście do oceny jakości oprogramowania, obejmujące: • **Metody ilościowe i jakościowe** – analiza metryk jakościowych, testowanie oraz ocena zgodności z wymaganiami. • **Techniki oceny** – testy jednostkowe, testy wydajnościowe, audyty kodu, analiza statyczna i dynamiczna. • **Zastosowanie międzynarodowych standardów w zakresie testowania i oceny jakości** – np. ISTQB, ISO/IEC 29119. **1.3. Standardy uznawane za równoważne** Standardy równoważne będą uznane, pod warunkiem spełnienia powyższych kryteriów. Standardy równiważne niewymagające pełnego postępowania dowodowego: • **CISQ (Consortium for Information & Software Quality)** – standardy oceny jakości kodu. • **NIST Software Assurance Metrics** – metody oceny jakości i bezpieczeństwa oprogramowania. • **CMMI for Development** – modele oceny jakości i dojrzałości procesów tworzenia oprogramowania. **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis metod oceny jakości oprogramowania**, w tym metryki i podejść stosowanych w procesie weryfikacji. 2. **Dokumentację charakterystyk jakościowych**, które są analizowane w ramach systemu oceny. 3. **Raporty i procedury oceny jakości**, potwierdzające zgodność stosowanego systemu z normą ISO/IEC 25010 lub standardem równoważnym.

	4. **Certyfikaty lub wyniki audytów technicznych**, jeśli dotyczy, potwierdzające stosowanie określonych norm w procesie oceny jakości. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedłożonej dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności zastosowanej metodyki oceny jakości. • Przeprowadzenia dodatkowych testów lub audytów weryfikujących rzeczywistą jakość oprogramowania względem deklarowanych standardów.
ISO/IEC 27001	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
ISTQB Foundation Level	Jeżeli w opisie przedmiotu zamówienia wskazano wymóg posiadania certyfikacji ISTQB Foundation Level, dopuszcza się zastosowanie certyfikacji równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny poziom wiedzy, umiejętności i doświadczenia w zakresie testowania oprogramowania, w tym: - Znajomość podstawowych zasad, pojęć i technik testowania oprogramowania. - Umiejętność projektowania i realizacji testów zgodnie z wymaganiami oraz celami projektu. - Zrozumienie cyklu życia testowania oraz stosowania technik statycznych i dynamicznych. - Umiejętność zarządzania procesem testowym i oceny wyników testów. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym zakres certyfikacji, wymagania dotyczące egzaminu oraz praktycznego zastosowania w projektach testowych. **Dopuszcza się** zastosowanie certyfikacji równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres wiedzy i egzaminu** Certyfikacja równoważna musi obejmować wiedzę i umiejętności z zakresu testowania oprogramowania, w szczególności: • **Podstawowe zasady testowania** – cele testowania, psychologia testowania, siedem zasad testowania. • **Proces testowy** – planowanie, projektowanie, wykonywanie i ocena testów. • **Techniki testowania** – testowanie dynamiczne i statyczne, analiza wartości brzegowych, testowanie eksploracyjne. • **Zarządzanie testami** – planowanie, organizacja i kontrola testów w ramach projektu IT.

	• **Narzędzia wspierające testowanie** – automatyzacja testów, testowanie wydajnościowe, narzędzia do zarządzania przypadkami testowymi. Egzamin certyfikacyjny musi obejmować zarówno test teoretyczny, jak i praktyczne zastosowanie zdobytej wiedzy. **1.2. Wymogi dotyczące umiejętności i doświadczenia** Certyfikacja musi potwierdzać, że kandydat posiada: • Umiejętność **projektowania i realizacji testów** zgodnie z wymaganiami oraz celami projektu. • Znajomość **cyklu życia testowania** i umiejętność stosowania różnych metod testowych. • Zrozumienie **technicznych i organizacyjnych aspektów testowania oprogramowania**. **1.3. Standardy uznawane za równoważne** Certyfikaty będą uznane za równoważne, pod warunkiem spełnienia powyższych kryteriów: Przykłady certyfikacji równoważnych niewymagających pełnego postępowania dowodowego: • **Certified Software Tester (CST)** – QAI • **Certified Test Engineer (CTE)** – QAI • **CMST (Certified Manager of Software Testing)** – QAI • **ISTQB Agile Tester Foundation Level** – dla projektów Agile • **TMap Suite Test Engineer** – Sogeti • **CAT (Certified Agile Tester)** – iSQI • **ICST (International Certified Software Tester)** – IIST **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis certyfikacji, jej zakresu oraz wymagań egzaminacyjnych**. 2. **Dokument potwierdzający znajomość technik testowania oraz metod zarządzania testami**. 3. **Informacje dotyczące akredytacji organizacji certyfikującej**. 4. **Przykłady zastosowania certyfikacji w projektach testowych**, potwierdzające praktyczne umiejętności. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedstawionej dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności certyfikacji. • Przeprowadzenia dodatkowej oceny kompetencji wskazanych osób, np. poprzez rozmowę techniczną lub test praktyczny.

JSON	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
OAuth	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
OWASP	W przypadku, gdy **Wykonawca** proponuje rozwiązanie inne niż standardy, narzędzia lub wytyczne OWASP (Open Worldwide Application Security Project), **Zamawiający** uznaje je za równoważne pod warunkiem, że: 1. **Funkcjonalność i zakres:** o Proponowane rozwiązanie obejmuje co najmniej następujące obszary: ▪ Identyfikacja najważniejszych zagrożeń bezpieczeństwa aplikacji (np. zgodnie z OWASP Top Ten). ▪ Możliwość weryfikacji bezpieczeństwa aplikacji zgodnie z międzynarodowymi standardami (np. OWASP ASVS lub równoważnymi). ▪ Mechanizmy wsparcia dla zarządzania ryzykiem i procesami bezpieczeństwa aplikacji (np. OWASP SAMM lub równoważne). 2. **Zgodność z regulacjami:** o Rozwiązanie zapewnia zgodność z obowiązującymi przepisami prawa dotyczącymi bezpieczeństwa informacji, w szczególności: ▪ Rozporządzenie RODO (GDPR). ▪ Ustawa o Krajowym Systemie Cyberbezpieczeństwa. ▪ Normy ISO/IEC dotyczące bezpieczeństwa informacji (np. ISO 27001). 3. **Transparentność i otwartość:** o Dokumentacja techniczna oraz wytyczne dotyczące bezpieczeństwa są dostępne publicznie lub udostępniane Zamawiającemu w sposób zapewniający ich weryfikację. o Wdrożone mechanizmy ochrony bezpieczeństwa są audytowalne i umożliwiają przeprowadzenie weryfikacji przez podmioty zewnętrzne. 4. **Bezpieczeństwo techniczne:** o Proponowane rozwiązanie oferuje wsparcie dla analiz dynamicznych (DAST), statycznych (SAST) lub interaktywnych (IAST), umożliwiających identyfikację podatności w oprogramowaniu.

	○ Rozwiązanie wspiera szyfrowanie danych, zgodnie z najlepszymi praktykami w zakresie ochrony informacji. 5. **Edukacja i wsparcie:** ○ Oferowane narzędzie lub standard musi być wspierany przez dokumentację, szkolenia lub materiały edukacyjne, umożliwiające skuteczne wdrożenie w organizacji **Zamawiającego**. 6. **Raportowanie i analiza:** ○ Narzędzie umożliwia generowanie szczegółowych raportów dotyczących bezpieczeństwa aplikacji, w tym raportowania incydentów i działań naprawczych. 7. **Interoperacyjność i skalowalność:** ○ Rozwiązanie jest kompatybilne z narzędziami DevOps/DevSecOps, umożliwiając integrację z procesami CI/CD. ○ System wspiera różne typy aplikacji, w tym aplikacje webowe, mobilne i IoT. **Weryfikacja równoważności** **Wykonawca** zobowiązany jest do przedstawienia szczegółowej dokumentacji technicznej oraz innych materiałów potwierdzających spełnienie warunków równoważności. **Zamawiający** zastrzega sobie prawo do zasięgnięcia opinii eksperckiej lub przeprowadzenia testów weryfikacyjnych.
PDF, DOC/DOCX, ODT PPT/PPTX, ODP MP4, MP3, OGG, AVI, JPEG, PNG, GIF, BMP	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
PMP	Ilekroć w specyfikacji zamówienia wskazano wymóg posiadania certyfikacji *PMP* (*Project Management Professional*), dopuszcza się zastosowanie certyfikacji równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia wiedzę, umiejętności i doświadczenie w zarządzaniu projektami na poziomie równoważnym z *PMP*. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym zakres certyfikacji, standardy oraz uznanie międzynarodowe. **Dopuszcza się** zastosowanie certyfikacji równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres wiedzy i egzaminu** Certyfikacja równoważna musi potwierdzać wiedzę i umiejętności w zakresie: • **Zarządzania projektami zgodnie z uznanym standardem** (np. PMBOK Guide – Project

	Management Body of Knowledge lub innymi równoważnymi standardami). • **Procesów zarządzania projektem**, w tym inicjowania, planowania, realizacji, monitorowania i zamykania projektu. • **Metod i narzędzi zarządzania ryzykiem, harmonogramem, budżetem i jakością projektu**. • **Zarządzania zespołem projektowym, interesariuszami oraz komunikacją w projekcie**. • **Metodyk i podejść zarządzania projektami**, takich jak klasyczne (Waterfall), zwinne (Agile) i hybrydowe. Egzamin certyfikacyjny musi obejmować zarówno test teoretyczny, jak i praktyczne zastosowanie wiedzy w zarządzaniu projektami. **1.2. Wymogi dotyczące doświadczenia** Certyfikacja musi wymagać od kandydata: • **Minimum 3-5 lat doświadczenia** w prowadzeniu lub zarządzaniu projektami. • Udokumentowanej znajomości **zarządzania projektami w różnych środowiskach branżowych**. • Potwierdzenia umiejętności stosowania narzędzi i technik zarządzania projektami w praktyce. **1.3. Standardy uznawane za równoważne** Za równoważne będą uznane certyfikaty zarządzania projektami, pod warunkiem spełnienia powyższych kryteriów. Certyfikacje równoważne: • **PRINCE2 Practitioner (Projects IN Controlled Environments)** – Axelos • **IPMA Level B, C (International Project Management Association)** • **AgilePM Practitioner** – APMG International • **Scrum Master Certified (CSM, PSM I/II)** – dla projektów zwinnych • **SAFe Program Consultant (SPC) lub SAFe Agilist (SA)** – w przypadku zarządzania projektami w metodykach Agile i Scaled Agile Framework **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis certyfikacji**, jej zakresu oraz wymagań egzaminacyjnych. 2. **Dokumenty potwierdzające znajomość procesów i metod zarządzania projektami**. 3. **Informacje dotyczące akredytacji organizacji certyfikującej oraz uznania międzynarodowego certyfikatu**.

	4. **Przykłady zastosowania certyfikacji w projektach**, potwierdzające praktyczne umiejętności zarządzania projektami. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedstawionej dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności certyfikacji. • Przeprowadzenia dodatkowej oceny kompetencji wskazanych osób, np. poprzez rozmowę techniczną lub test praktyczny.
PRINCE2	Ilekroć w opisie przedmiotu zamówienia wskazano wymóg stosowania metodyki *PRINCE2* w zarządzaniu projektem, dopuszcza się stosowanie rozwiązań równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia zarządzanie projektami w sposób zgodny z kluczowymi zasadami i procesami metodyki PRINCE2, w szczególności w zakresie zarządzania etapowego, uzasadnienia biznesowego, struktury ról oraz zarządzania ryzykiem. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność proponowanej metodyki. **Zapis dotyczący równoważności metodyki PRINCE2** 1. **Stosowanie metodyki PRINCE2 lub rozwiązania równoważnego** W przypadku, gdy w opisie przedmiotu zamówienia wskazano wymóg stosowania metodyki **PRINCE2 (Projects IN Controlled Environments)** w zarządzaniu projektem, dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Kluczowe zasady zarządzania projektami** Równoważne rozwiązanie musi zapewniać zarządzanie projektami w sposób zgodny z następującymi kluczowymi zasadami metodyki PRINCE2: • **Zarządzanie etapowe** – podział projektu na kontrolowane etapy z określonymi punktami przeglądowymi. • **Stałe uzasadnienie biznesowe** – każda decyzja projektowa powinna być podejmowana w oparciu o analizę wartości biznesowej. • **Zdefiniowane role i obowiązki** – określenie ról uczestników projektu oraz ich odpowiedzialności. • **Zarządzanie ryzykiem** – systematyczna identyfikacja, analiza i monitorowanie ryzyka w projekcie. • **Ustalona struktura procesów** – od inicjacji, przez realizację, aż po zamknięcie projektu.

	• **Zarządzanie zmianą** – mechanizmy oceny i wdrażania zmian w projekcie. • **Dostosowanie do potrzeb projektu** – elastyczność w adaptacji metodyki do skali i specyfiki projektu. **1.2. Struktura ról i odpowiedzialności** Równoważne rozwiązanie musi obejmować: • **Jasny podział ról i obowiązków** w zespole projektowym, w tym odpowiedzialność sponsora, kierownika projektu oraz zespołu realizacyjnego. • **Mechanizmy monitorowania i raportowania** postępu projektu do interesariuszy. **1.3. Zarządzanie cyklem życia projektu** Równoważna metodyka powinna obejmować co najmniej następujące etapy: 1. **Inicjowanie projektu** – określenie celów, zakresu i uzasadnienia biznesowego. 2. **Planowanie** – definiowanie harmonogramu, zasobów i budżetu. 3. **Realizacja i kontrola** – monitorowanie postępów, zarządzanie ryzykiem i podejmowanie decyzji w oparciu o ustalone wskaźniki. 4. **Zamykanie projektu** – ocena efektów i raportowanie końcowe. **1.4. Standardy uznawane za równoważne** Za równoważne będą uznane metodyki zarządzania projektami, pod warunkiem spełnienia powyższych kryteriów. Metodyki i standardy nie wymagające pełnego postępowania dowodowego: • **PMP (Project Management Professional – PMBOK Guide)** – metodyka PMI • **IPMA Level B/C** – International Project Management Association • **AgilePM (Agile Project Management)** – APMG International • **SAFe (Scaled Agile Framework)** – zarządzanie projektami w środowisku Agile • **Scrum Master + Agile Practitioner** – zarządzanie projektami zwinnymi • **Lean Project Management** – podejście do optymalizacji projektów • **PM2** – Metodyka zarządzania projektami opracowana przez Komisję Europejską **1.5. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis metodyki zarządzania projektami** oraz jej zgodności z kluczowymi zasadami PRINCE2.

	2. **Dokumentację potwierdzającą stosowanie mechanizmów zarządzania etapowego, ryzykiem oraz uzasadnieniem biznesowym**. 3. **Informacje dotyczące uznania międzynarodowego danej metodyki oraz jej zgodności z najlepszymi praktykami**. 4. **Referencje z realizacji projektów** przy zastosowaniu danej metodyki jako potwierdzenie praktycznej zgodności z PRINCE2. **1.6. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedłożonej dokumentacji pod kątem spełnienia wymagań. • Konsultacji eksperckiej w celu potwierdzenia równoważności stosowanej metodyki. • Przeprowadzenia dodatkowych testów lub wywiadów technicznych, sprawdzających praktyczne zastosowanie metodyki w projektach.
PRINCE2 Practitioner	Ilekroć w specyfikacji zamówienia wskazano wymóg stosowania certyfikacji *PRINCE2 Practitioner* w zarządzaniu projektem, dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny poziom wiedzy, kompetencji i umiejętności w zarządzaniu projektami. **Wykonawca** zobowiązany jest do dostarczenia dokumentacji potwierdzającej równoważność, w tym opis procesów, struktury zarządzania oraz metod oceny projektów. **Dopuszcza się** zastosowanie certyfikacji równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres wiedzy i kompetencji** Certyfikacja równoważna musi potwierdzać wiedzę, umiejętności i kompetencje w zakresie: • **Zarządzania projektami w ustrukturyzowany sposób**, zgodnie z uznanymi metodykami. • **Zarządzania etapowego** – planowania, monitorowania i zamykania poszczególnych faz projektu. • **Zarządzania uzasadnieniem biznesowym** – stosowanie narzędzi do oceny celowości i opłacalności projektu. • **Określania i zarządzania rolami w projekcie** – struktura ról i odpowiedzialności w zespole projektowym. • **Zarządzania ryzykiem, jakością, zakresem i zmianami w projekcie**. • **Monitorowania i oceny postępów projektu** – stosowanie odpowiednich metryk i raportowania.

	• **Dostosowywania metodyki do specyfiki projektu** – umiejętność adaptacji w różnych środowiskach. **1.2. Metody oceny projektów** Certyfikacja równoważna musi obejmować systematyczne podejście do oceny projektów, w tym: • **Analizę skuteczności zarządzania projektem** na podstawie kluczowych wskaźników wydajności (KPI). • **Mechanizmy kontrolne** – stosowanie audytów projektowych, przeglądów i analiz ryzyka. • **Metodykę podejmowania decyzji na podstawie danych** – planowanie i realizacja działań korygujących. **1.3. Standardy uznawane za równoważne** Za równoważne będą uznane certyfikaty zarządzania projektami, pod warunkiem spełnienia powyższych kryteriów. Certyfikaty nie wymagające pełnego postępowania dowodowego: • **PMP (Project Management Professional)** – PMI • **IPMA Level B, C (International Project Management Association)** • **AgilePM Practitioner** – APMG International • **SAFe Program Consultant (SPC) lub SAFe Agilist (SA)** – dla zarządzania projektami w środowiskach Agile • **Scrum Master Certified (CSM, PSM II)** – dla projektów zwinnych • **PM² Advanced lub PM² Expert**– Metodyka zarządzania projektami opracowana przez Komisję Europejską. **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis certyfikacji**, jej zakresu oraz wymagań egzaminacyjnych. 2. **Dokumenty potwierdzające znajomość procesów, struktur zarządzania i metod oceny projektów**. 3. **Informacje dotyczące uznania międzynarodowego certyfikacji i jej zgodności z najlepszymi praktykami**. 4. **Przykłady zastosowania certyfikacji w praktyce**, potwierdzające umiejętności zarządzania projektami na poziomie Practitioner. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedłożonej dokumentacji pod kątem zgodności z wymaganiami.

	• Konsultacji eksperckiej w celu potwierdzenia równoważności certyfikacji. • Przeprowadzenia dodatkowej oceny kompetencji wskazanych osób, np. poprzez rozmowę techniczną lub analizę referencji projektowych.
PSOAP - Profil SOAP i odnosi się do profilu stosowania standardu SOAP (Simple Object Access Protocol)	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
REST API	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
RUP	Ilekroć w opisie przedmiotu zamówienia wskazano wymóg stosowania metodologii *RUP (Rational Unified Process*), dopuszcza się zastosowanie metodologii równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia iteracyjne i przyrostowe podejście do realizacji projektów, uwzględnia fazy cyklu życia projektu oraz wspiera zarządzanie wymaganiami, ryzykiem, weryfikację i walidację. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym opis stosowanej metodologii i przykładów jej zastosowania w projektach. **Dopuszcza się** zastosowanie metodologii równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Kluczowe założenia metodologii** Równoważna metodologia musi zapewniać: • **Iteracyjne i przyrostowe podejście do realizacji projektów**, umożliwiające stopniowe dostarczanie funkcjonalności. • **Podział cyklu życia projektu na etapy** zgodne z podejściem RUP: 1. **Inicjalizacja (Inception)** – definiowanie celów, zakresu i ryzyka projektu. 2. **Elaboracja (Elaboration)** – opracowanie szczegółowej architektury systemu i planowanie projektu. 3. **Konstrukcja (Construction)** – implementacja i rozwój oprogramowania. 4. **Przekazanie (Transition)** – wdrożenie, testowanie i dostarczenie produktu końcowego. • **Zarządzanie wymaganiami**, uwzględniające modelowanie, analizę oraz śledzenie zmian w wymaganiach. • **Zarządzanie ryzykiem**, poprzez identyfikację, analizę i wdrażanie strategii minimalizujących ryzyko. • **Silne wsparcie dla weryfikacji i walidacji** – testowanie na każdym etapie cyklu życia projektu.

	• **Adaptacyjność do różnych rozmiarów i rodzajów projektów IT**, zgodnie z najlepszymi praktykami inżynierii oprogramowania. **1.2. Struktura ról i odpowiedzialności** Równoważna metodologia musi obejmować: • **Zdefiniowane role w projekcie** – architekt, analityk, kierownik projektu, programista, tester, użytkownik końcowy. • **Określone przepływy pracy (workflows)** – zarządzanie wymaganiami, analizą, projektowaniem, implementacją, testowaniem i wdrażaniem. • **Procesy zapewniające dokumentację i śledzenie zmian** w projekcie. **1.3. Standardy uznawane za równoważne** Za równoważne będą uznane metodologie inżynierii oprogramowania i zarządzania projektami IT, pod warunkiem spełnienia powyższych kryteriów. Metodologie niewymagające pełnego postępowania dowodowego: • **Agile Unified Process (AUP)** – lekkie, zwinne podejście do RUP. • **Disciplined Agile Delivery (DAD)** – rozszerzona wersja Agile/RUP. • **Scrum z elementami zarządzania wymaganiami i ryzykiem**. • **SAFe (Scaled Agile Framework)** – iteracyjne zarządzanie dużymi projektami IT. • **Extreme Programming (XP)** – iteracyjne podejście do tworzenia oprogramowania, z naciskiem na jakość kodu. • **Lean Software Development** – iteracyjne podejście do wytwarzania oprogramowania. • **IBM Engineering Lifecycle Management (dawniej Rational Team Concert)** – zintegrowane zarządzanie projektami IT. **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis stosowanej metodologii** oraz jej zgodności z podejściem iteracyjnym i przyrostowym. 2. **Dokumentację procesów zarządzania wymaganiami, ryzykiem oraz weryfikacji i walidacji**. 3. **Informacje o uznaniu stosowanej metodologii w branży IT i jej zgodności z najlepszymi praktykami**. 4. **Przykłady zastosowania metodologii w projektach IT**, potwierdzające jej efektywność i skuteczność.

	1.5. Weryfikacja równoważności Zamawiający zastrzega sobie prawo do: • Weryfikacji przedłożonej dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności stosowanej metodologii. • Przeprowadzenia dodatkowych testów lub analiz eksperckich, weryfikujących zgodność metodologii z wymaganiami projektowymi.
SAML- Security Assertion Markup Language	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
TOGAF	Ilekroć w specyfikacji zamówienia wskazano wymóg stosowania ram architektonicznych *TOGAF* (*The Open Group Architecture Framework*), dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny zakres funkcjonalności, wspiera zarządzanie architekturą korporacyjną w sposób kompleksowy oraz dostarcza narzędzia do projektowania, planowania i zarządzania zmianą w architekturze organizacji. **Wykonawca** zobowiązany jest przedłożyć dokumentację potwierdzającą równoważności. **Dopuszcza się** zastosowanie rozwiązań równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres funkcjonalności i metodologia** Równoważne rozwiązanie musi zapewniać: • **Kompleksowe zarządzanie architekturą korporacyjną**, obejmujące planowanie, projektowanie, wdrażanie i nadzorowanie architektury organizacyjnej. • **Strukturyzowane podejście do projektowania architektury** zgodne z uznanymi standardami i najlepszymi praktykami. • **Proces zarządzania zmianą w architekturze organizacji** w sposób umożliwiający integrację strategii biznesowej i IT. • **Definiowanie i utrzymywanie architektonicznych standardów organizacyjnych**, wspierających interoperacyjność i zgodność systemów. **1.2. Wspierane obszary zarządzania architekturą** Równoważne rozwiązanie musi obejmować co najmniej następujące elementy: • **Metodykę zarządzania architekturą** – struktura procesów wspierających cykl życia architektury korporacyjnej. • **Architekturę biznesową** – definiowanie procesów biznesowych, modeli operacyjnych i wymagań strategicznych.

	• **Architekturę aplikacji** – modelowanie i planowanie systemów aplikacyjnych oraz ich integracji. • **Architekturę danych** – strategia zarządzania danymi, ich struktura, przepływy i standardy przechowywania. • **Architekturę technologiczną** – infrastruktura IT, systemy i standardy technologiczne wspierające architekturę organizacji. **1.3. Narzędzia do zarządzania architekturą** Równoważne rozwiązanie musi dostarczać: • **Mechanizmy analizy i planowania architektury** zgodnie z podejściem iteracyjnym. • **Zarządzanie repozytorium architektonicznym** – możliwość przechowywania i aktualizacji modeli architektury. • **Mapowanie strategii IT na wymagania biznesowe** – definiowanie powiązań między celami biznesowymi a rozwiązaniami IT. • **Procesy monitorowania zgodności architektury** – narzędzia do śledzenia wdrożenia i realizacji założeń architektonicznych. **1.4. Standardy uznawane za równoważne** Za równoważne będą uznane standardy i ramy architektoniczne, pod warunkiem spełnienia powyższych kryteriów. Rozwiązania niewymagające pełnego postępowania dowodowego: • **Zachman Framework** – struktura klasyfikacji komponentów architektury korporacyjnej. • **FEAF (Federal Enterprise Architecture Framework)** – model architektoniczny stosowany w administracji publicznej. • **DoDAF (Department of Defense Architecture Framework)** – standard architektury dla systemów wojskowych i rządowych. • **MODAF (Ministry of Defence Architecture Framework)** – brytyjski standard dla architektury korporacyjnej. • **ArchiMate** – modelowanie architektury korporacyjnej zgodnie z otwartym standardem The Open Group. **1.5. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis rozwiązania i jego metodologii**, potwierdzający zgodność z kluczowymi zasadami TOGAF. 2. **Dokumentację procesów zarządzania architekturą**, uwzględniającą planowanie, wdrażanie i nadzorowanie architektury organizacyjnej.

	3. **Informacje o uznaniu międzynarodowym stosowanej metodyki oraz jej zgodności z najlepszymi praktykami**. 4. **Przykłady praktycznego zastosowania rozwiązania**, w tym referencje z projektów obejmujących zarządzanie architekturą korporacyjną. **1.6. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedłożonej dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności stosowanej metodyki. • Przeprowadzenia dodatkowych testów, audytów lub wywiadów eksperckich w celu oceny praktycznego zastosowania rozwiązania.

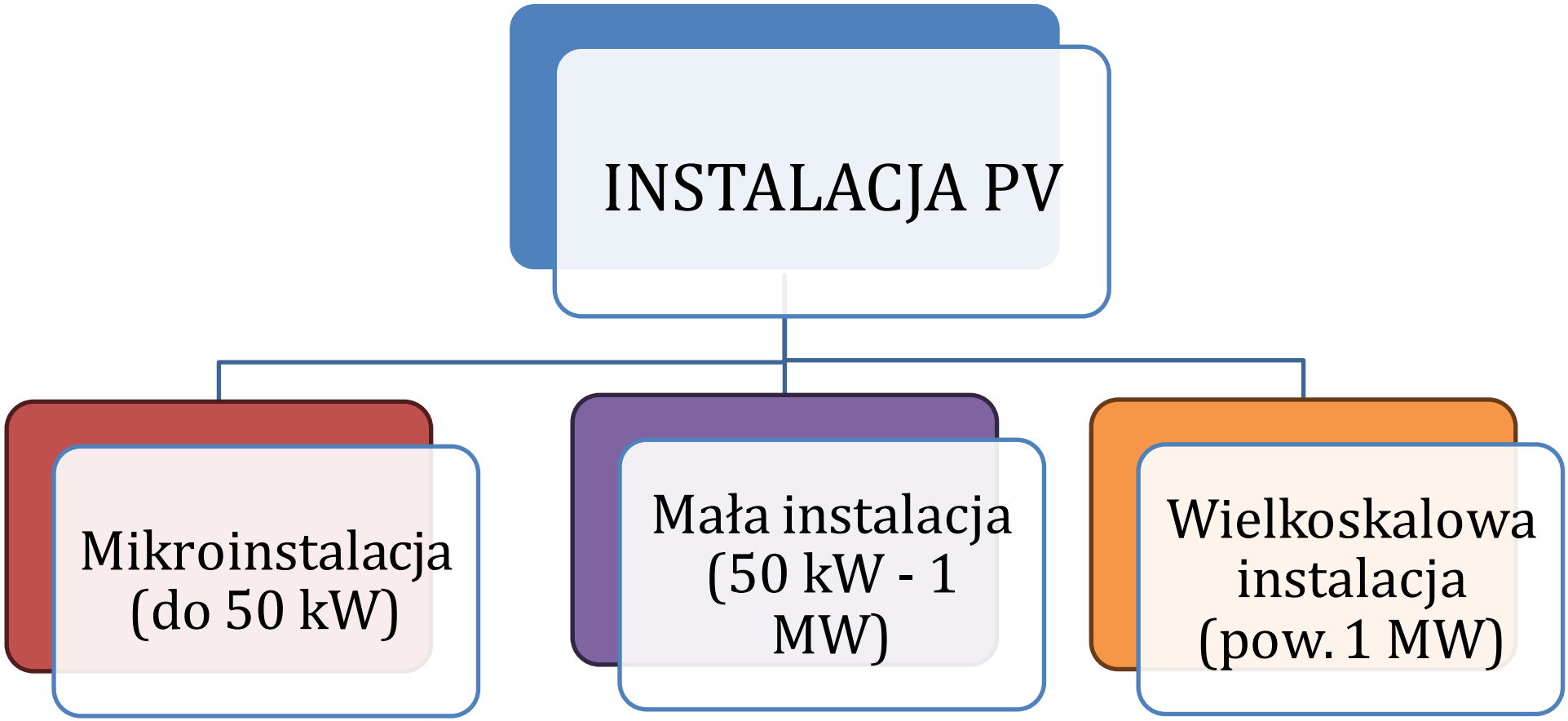
UML – Unified Modelling Language	Ilekroć w **SOPZ** wskazano wymaganie stosowania *UML* jako standardu modelowania, dopuszcza się zastosowanie rozwiązań równoważnych, które zapewniają możliwość tworzenia diagramów i modeli o funkcjonalności oraz strukturze odpowiadającej *UML*. **Wykonawca** zobowiązany jest do przedstawienia dokumentacji potwierdzającej równoważność oferowanego rozwiązania, w tym opis funkcjonalności, zgodności z normami oraz sposobu współpracy z narzędziami do modelowania *UML*.
	Dopuszcza się zastosowanie rozwiązań równoważnych, pod warunkiem że spełniają one następujące kryteria:
	1.1. Wymagania dotyczące funkcjonalności
	Równoważne rozwiązanie musi umożliwiać:
	• **Tworzenie diagramów i modeli o strukturze i funkcjonalności zgodnej z UML**, w tym co najmniej:
	  ○ Diagramy przypadków użycia (**Use Case Diagram**).
	  ○ Diagramy klas (**Class Diagram**).
	  ○ Diagramy sekwencji (**Sequence Diagram**).
	  ○ Diagramy aktywności (**Activity Diagram**).
	  ○ Diagramy komponentów (**Component Diagram**).
	  ○ Diagramy wdrożenia (**Deployment Diagram**).
	• **Obsługę modelowania strukturalnego, behawioralnego i interakcyjnego**, zgodnie z zasadami UML.
	• **Zachowanie standardowego notacji graficznej**, umożliwiającej jednoznaczną interpretację modeli.
	1.2. Wymagania dotyczące zgodności z normami
	Równoważne rozwiązanie musi:
	• **Spełniać normy OMG (Object Management Group) dotyczące modelowania oprogramowania** lub inne równoważne standardy.

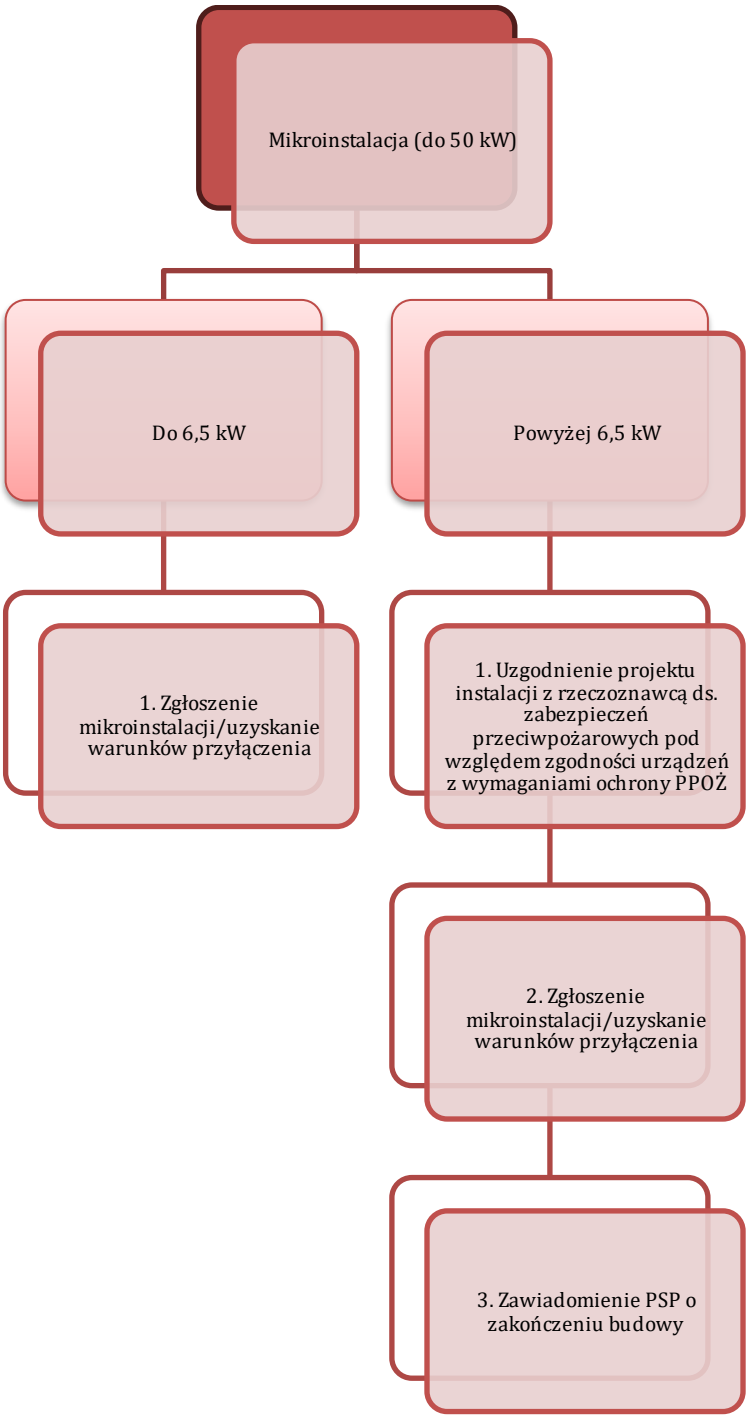
	• **Zapewniać możliwość eksportu i importu modeli** w formatach kompatybilnych z UML (np. XMI – XML Metadata Interchange). • **Umożliwiać interoperacyjność z narzędziami do modelowania UML**, np. Enterprise Architect, IBM Rational, Visual Paradigm, ArgoUML. **1.3. Standardy uznawane za równoważne** Za rozwiązania równoważne będą uznane metodyki i języki modelowania spełniające powyższe kryteria. Standardy nie wymagające pełnego postępowania: • **BPMN (Business Process Model and Notation)** – w zakresie modelowania procesów biznesowych. • **Archimate** – w zakresie modelowania architektury korporacyjnej. • **ERD (Entity-Relationship Diagram)** – w zakresie modelowania danych. • **SoaML (Service-Oriented Architecture Modeling Language)** – w zakresie modelowania architektury SOA. **1.4. Wymagane dokumenty potwierdzające równoważność** Wykonawca zobowiązany jest przedłożyć: 1. **Opis funkcjonalności oferowanego rozwiązania**, potwierdzający zgodność ze standardem UML. 2. **Dokumentację dotyczącą obsługi modelowania strukturalnego, behawioralnego i interakcyjnego**. 3. **Informacje dotyczące zgodności z normami OMG lub innymi równoważnymi standardami**. 4. **Przykłady zastosowania rozwiązania w projektach IT**, potwierdzające jego praktyczne wykorzystanie. 5. **Opis współpracy narzędzia z UML i innymi standardami modelowania**. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji dokumentacji pod kątem spełnienia wymagań funkcjonalnych i zgodności ze standardem UML. • Konsultacji eksperckiej w celu potwierdzenia równoważności oferowanego rozwiązania. • Przeprowadzenia testów praktycznych lub analizy zgodności eksportowanych modeli z UML.
UML Professional Foundation	Ilekroć w specyfikacji zamówienia wskazano wymóg posiadania certyfikacji *UML Professional Foundation*, dopuszcza się zastosowanie certyfikacji równoważnych, pod warunkiem że oferowane rozwiązanie zapewnia porównywalny poziom wiedzy, umiejętności i doświadczenia w zakresie modelowania w języku *UML* lub innym równoważnym wybranym przez **Wykonawcę** oraz jego

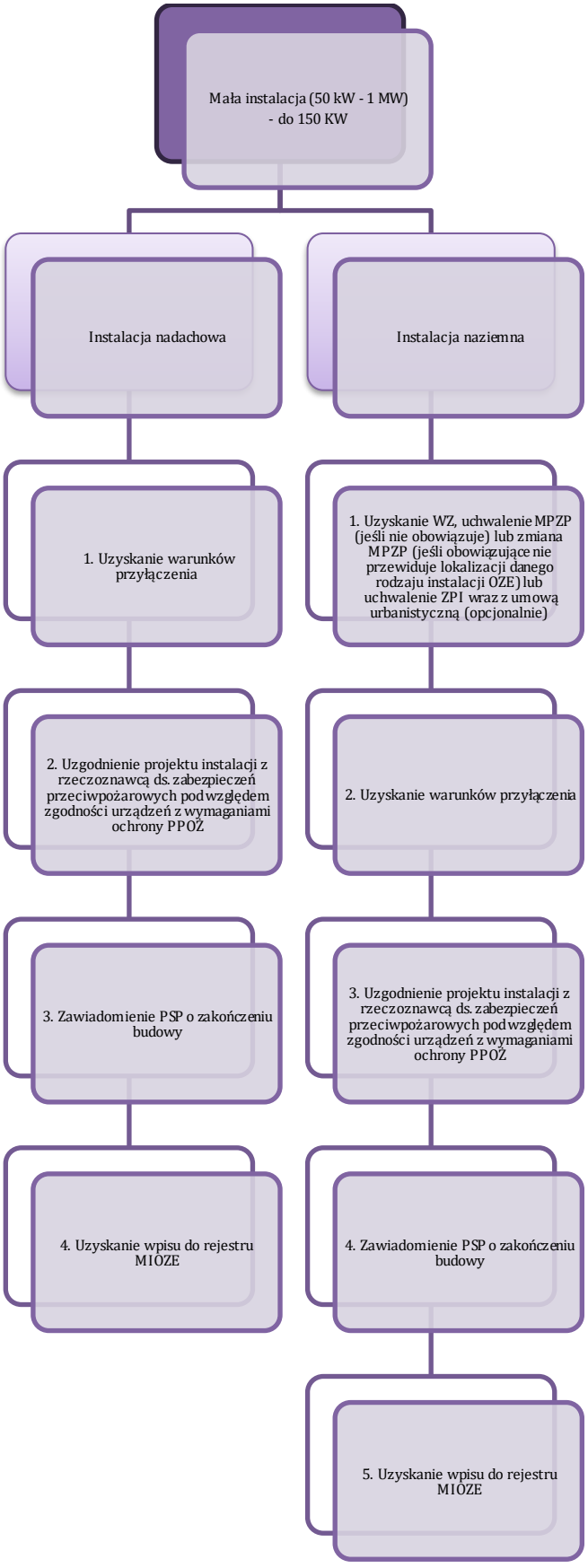
	zastosowania w projektach IT. Wykonawca zobowiązany jest przedłożyć dokumentację potwierdzającą równoważność, w tym opis zakresu certyfikacji oraz przykłady jej zastosowania. **Dopuszcza** się zastosowanie certyfikacji równoważnych, pod warunkiem że spełniają one następujące kryteria: **1.1. Zakres wiedzy i kompetencji** Certyfikacja równoważna musi potwierdzać wiedzę, umiejętności i doświadczenie w zakresie: • **Podstaw modelowania w UML**, w tym zastosowanie notacji i standardów OMG (Object Management Group). • **Tworzenia i interpretacji kluczowych diagramów UML**, takich jak: ○ **Diagramy strukturalne** (diagramy klas, komponentów, wdrożenia). ○ **Diagramy behawioralne** (diagramy przypadków użycia, aktywności, stanów). ○ **Diagramy interakcyjne** (diagramy sekwencji, komunikacji, interakcji). • **Zastosowania UML w analizie, projektowaniu i dokumentowaniu systemów IT**. • **Integracji UML z innymi standardami modelowania, takimi jak BPMN, ArchiMate czy ERD**. • **Narzędzi wspierających modelowanie UML**, np. Enterprise Architect, IBM Rational, Visual Paradigm, MagicDraw. **1.2. Wymogi dotyczące egzaminu i doświadczenia** Certyfikacja musi potwierdzać: • **Znajomość UML na poziomie profesjonalnym**, w tym zastosowanie w praktycznych projektach IT. • **Zdolność do modelowania systemów IT i tworzenia dokumentacji architektonicznej**. • **Doświadczenie w pracy z UML lub innym równoważnym językiem modelowania**. **1.3. Standardy uznawane za równoważne** Za równoważne będą uznane certyfikacje w zakresie modelowania i architektury systemów, pod warunkiem spełnienia powyższych kryteriów. Certyfikacje równoważne (te certyfikaty nie wymagają pełnej dokumentacji dowodowej): • **OCUP 2 (OMG Certified UML Professional 2)** – Object Management Group. • **ArchiMate Certification** – The Open Group. • **Software Modeling Certification (ISTQB Advanced Level Model-Based Tester)** – ISTQB. • **ICSM (International Certified Software Modeler)** – IIST.

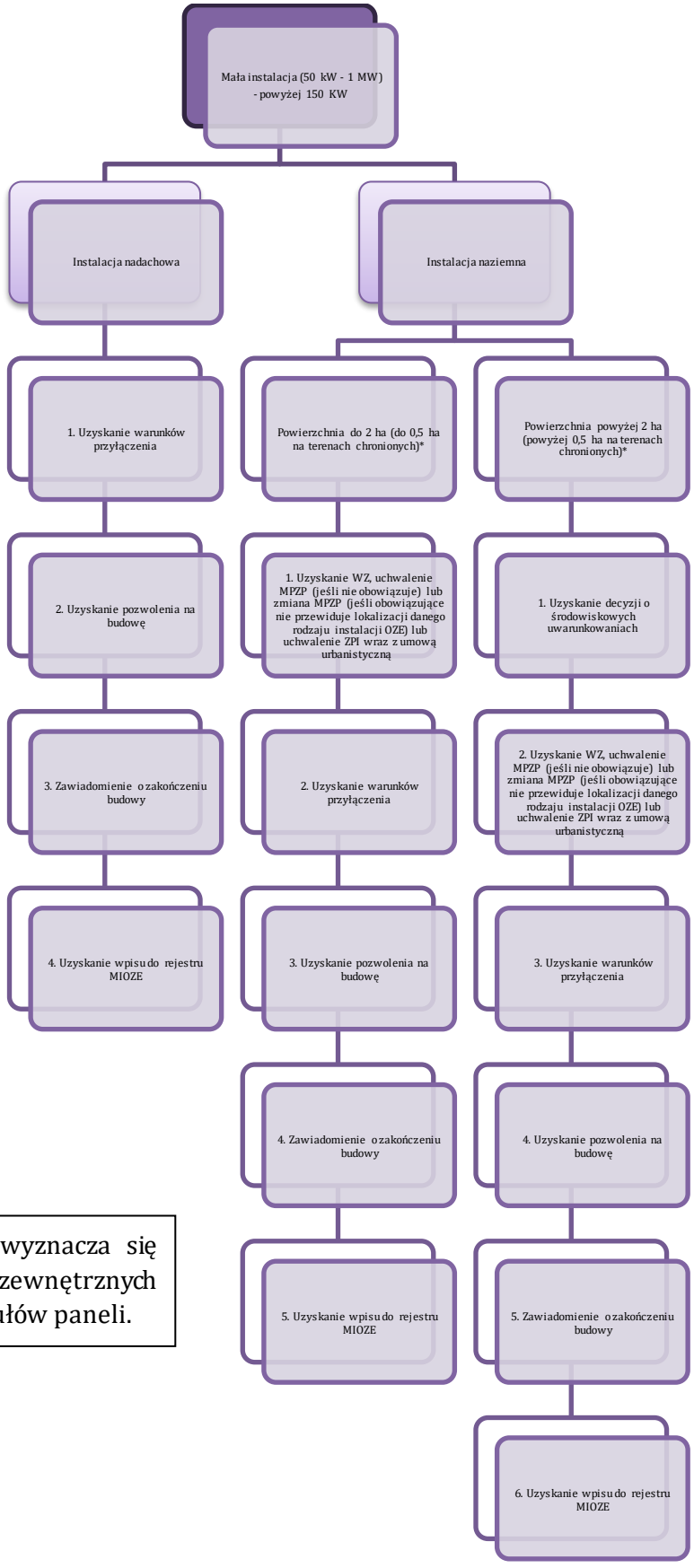
	1.4. Wymagane dokumenty potwierdzające równoważność Wykonawca zobowiązany jest przedłożyć: 1. **Opis certyfikacji**, jej zakresu oraz wymagań egzaminacyjnych. 2. **Dokument potwierdzający znajomość notacji UML i jej zastosowanie w praktyce**. 3. **Informacje dotyczące akredytacji organizacji certyfikującej i uznania międzynarodowego**. 4. **Przykłady zastosowania certyfikacji w projektach IT**, potwierdzające praktyczne umiejętności modelowania systemów. **1.5. Weryfikacja równoważności** Zamawiający zastrzega sobie prawo do: • Weryfikacji przedstawionej dokumentacji pod kątem zgodności z wymaganiami. • Konsultacji eksperckiej w celu potwierdzenia równoważności certyfikacji. • Przeprowadzenia dodatkowej oceny kompetencji wskazanych osób, np. poprzez test praktyczny lub analizę referencji projektowych.
WCAG 2.1	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
WFS (Web Feature Service).	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
WMS (Web Map Service)	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
WSDL - Web Services Description Language	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**
XML- Extensible Markup Language	**Zamawiający** nie określa warunków równoważności ze względu na wskazanie standardu w **KRI**

Załącznik 1. Taksonomia procedur OZE

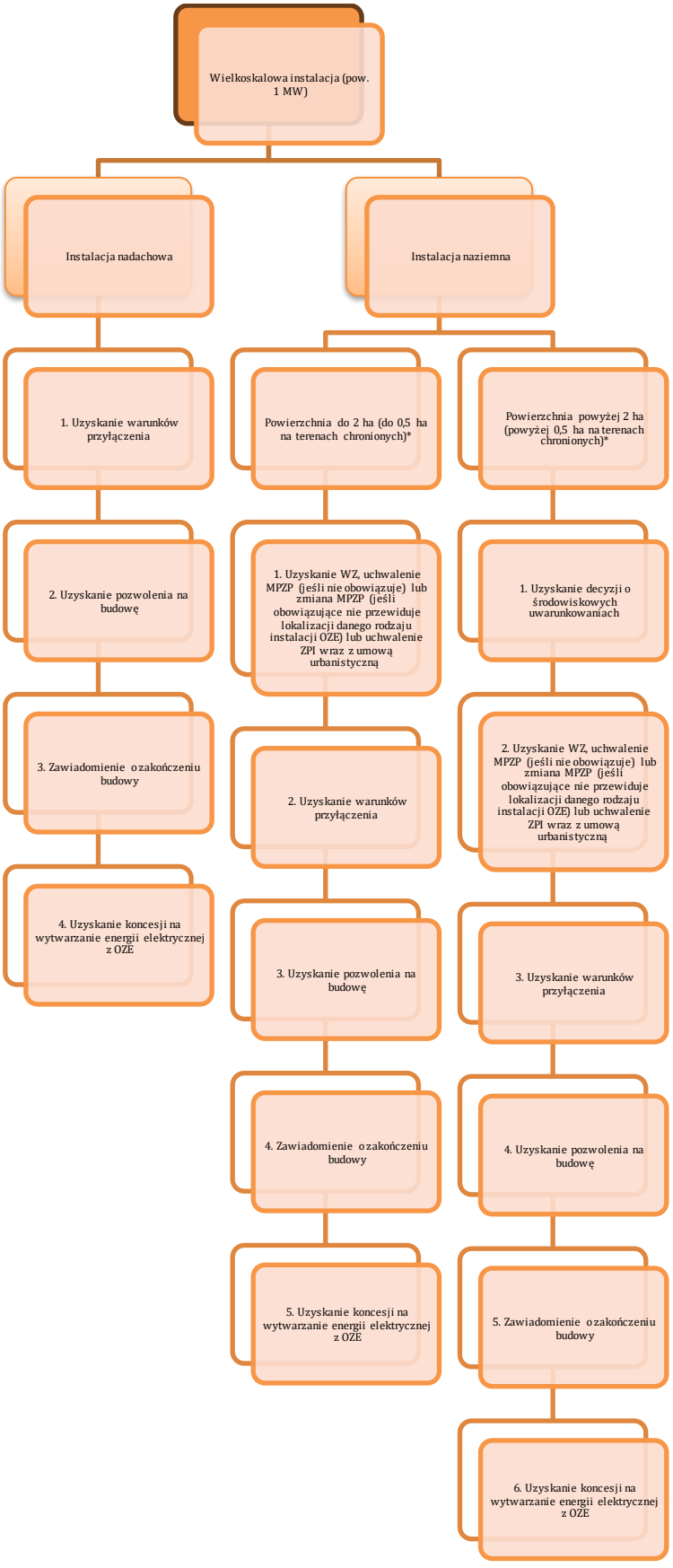


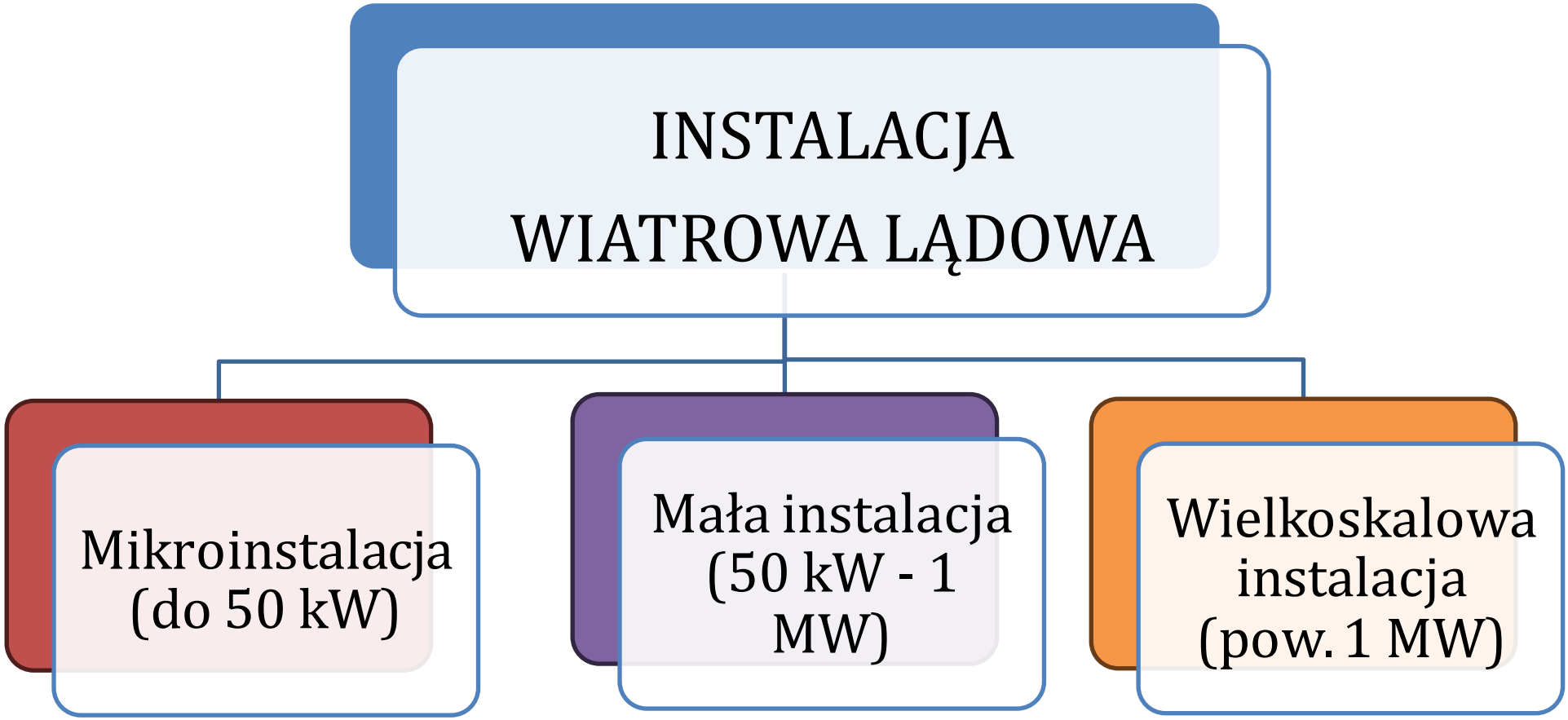

Mikroinstalacja (do 50 kW)
Do 6,5 kW
Powyżej 6,5 kW
1. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia
1. Uzgodnienie projektu instalacji z rzeczoznawcą ds. zabezpieczeń przeciwpożarowych pod względem zgodności urządzeń z wymaganiami ochrony PPOŻ
2. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia
3. Zawiadomienie PSP o zakończeniu budowy

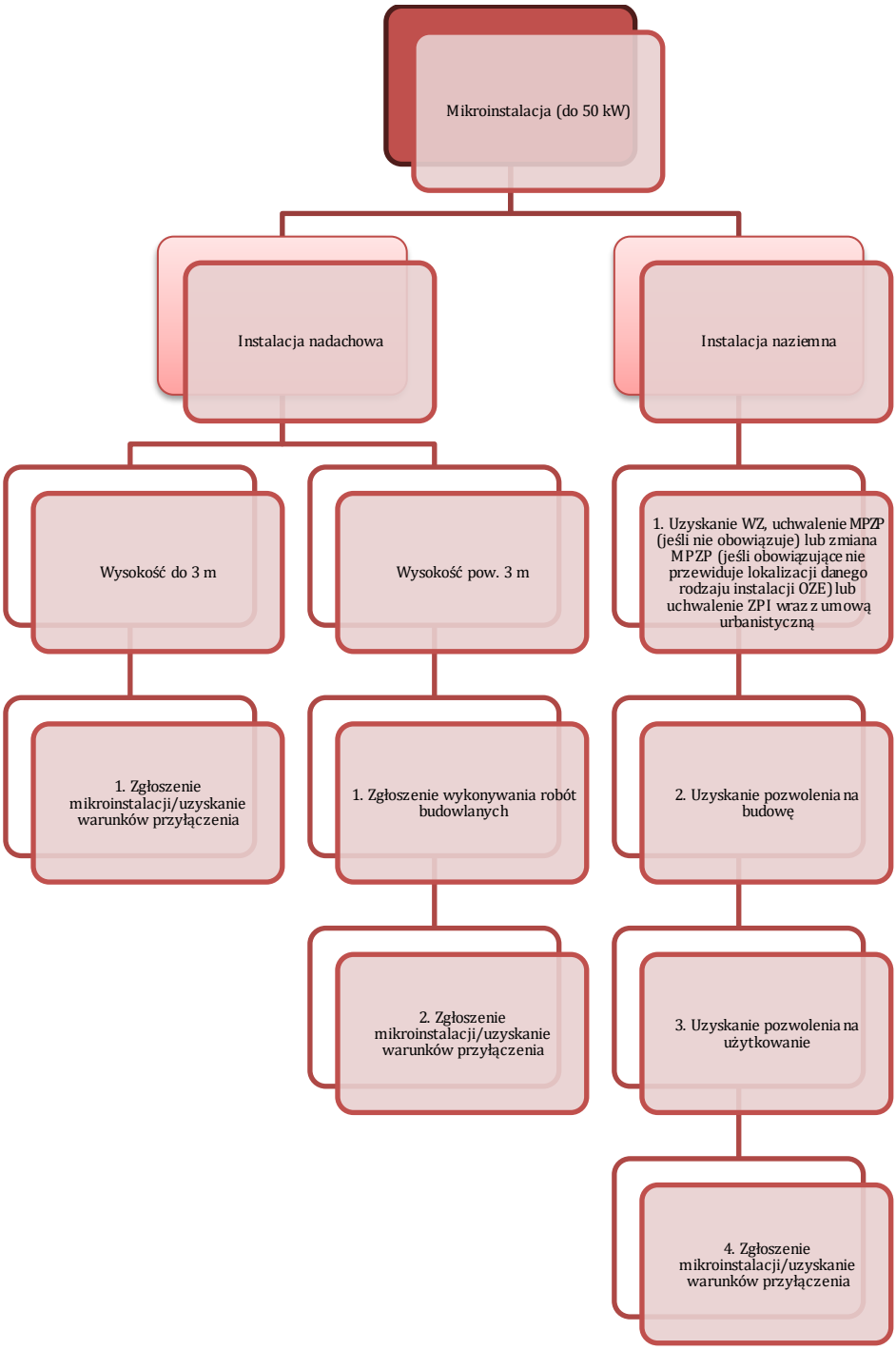

Mała instalacja (50 kW - 1 MW) - do 150 KW
Instalacja nadachowa
Instalacja naziemna
1. Uzyskanie warunków przyłączenia
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną (opcjonalnie)
2. Uzgodnienie projektu instalacji z rzeczoznawcą ds. zabezpieczeń przeciwpożarowych pod względem zgodności urządzeń z wymaganiami ochrony PPOŻ
2. Uzyskanie warunków przyłączenia
3. Zawiadomienie PSP o zakończeniu budowy
3. Uzgodnienie projektu instalacji z rzeczoznawcą ds. zabezpieczeń przeciwpożarowych pod względem zgodności urządzeń z wymaganiami ochrony PPOŻ
4. Uzyskanie wpisu do rejestru MIOZE
4. Zawiadomienie PSP o zakończeniu budowy
5. Uzyskanie wpisu do rejestru MIOZE

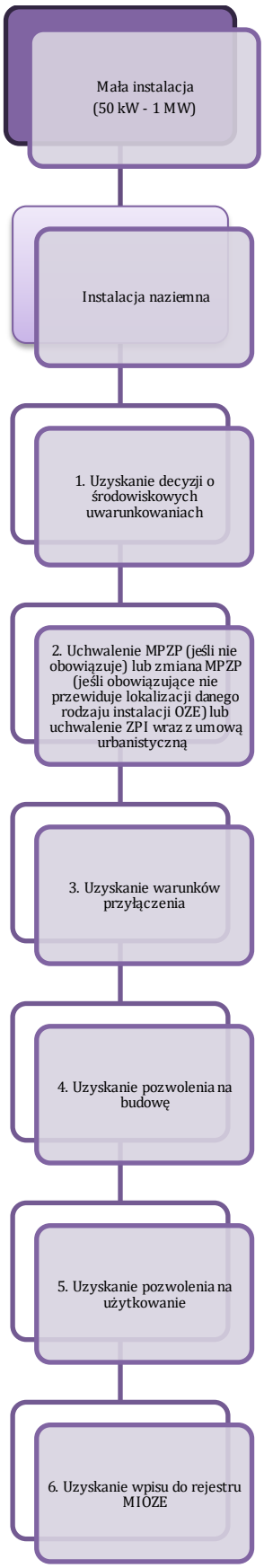


*Powierzchnie wyznacza się po obrysie zewnętrznych skrajnych modułów paneli.

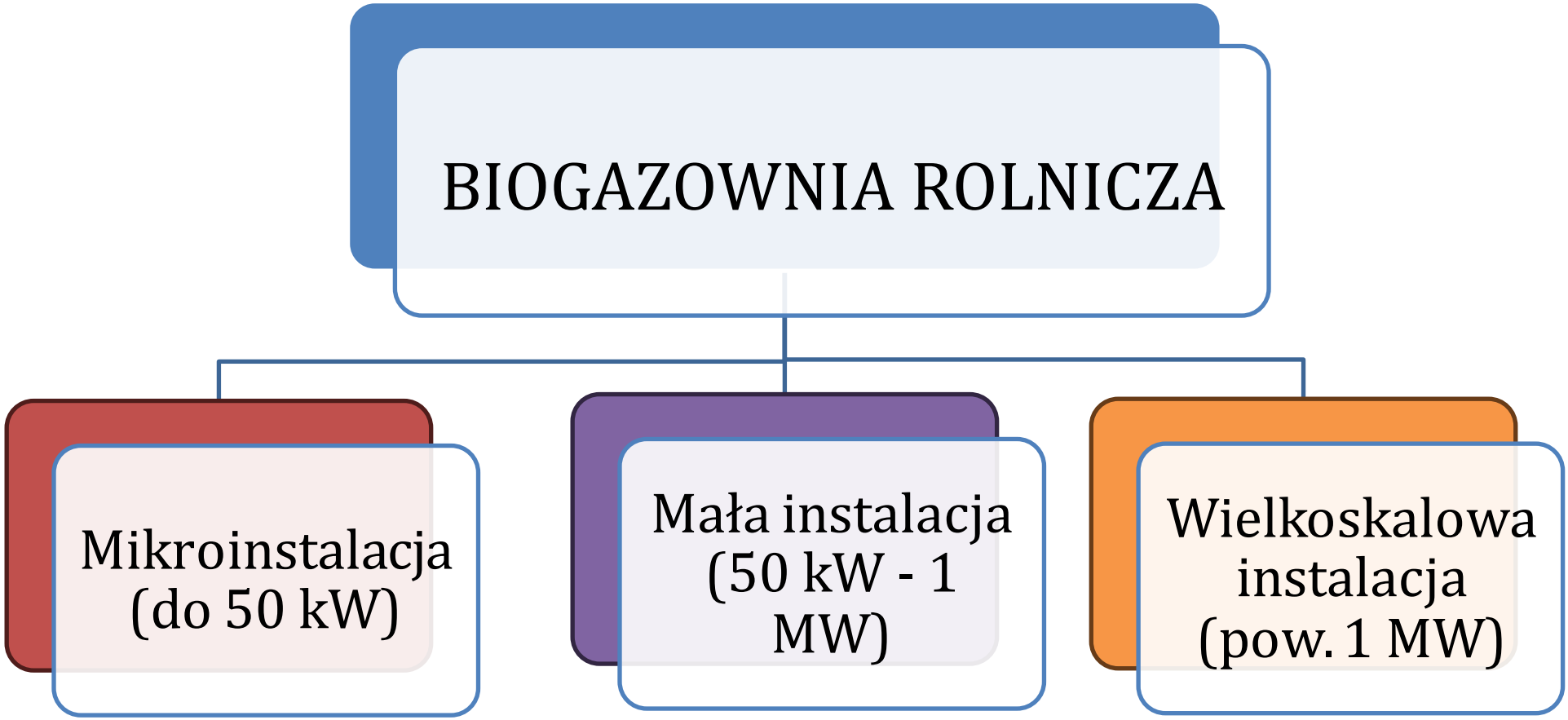

Wielkoskalowa instalacja (pow. 1 MW)
Instalacja nadachowa
Instalacja naziemna
1. Uzyskanie warunków przyłączenia
2. Uzyskanie pozwolenia na budowę
3. Zawiadomienie o zakończeniu budowy
4. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE
Powierzchnia do 2 ha (do 0,5 ha na terenach chronionych)*
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie warunków przyłączenia
3. Uzyskanie pozwolenia na budowę
4. Zawiadomienie o zakończeniu budowy
5. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE
Powierzchnia powyżej 2 ha (powyżej 0,5 ha na terenach chronionych)*
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie warunków przyłączenia
4. Uzyskanie pozwolenia na budowę
5. Zawiadomienie o zakończeniu budowy
6. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE

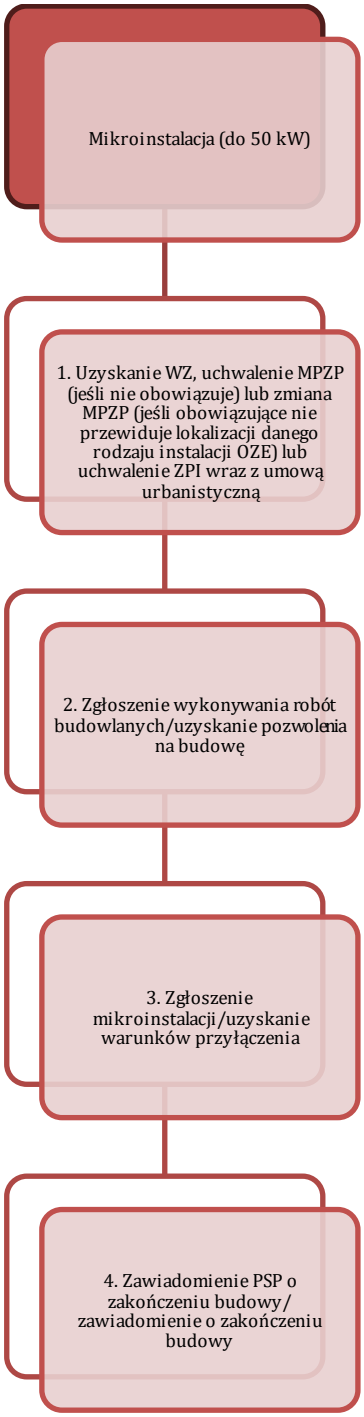

INSTALACJA WIATROWA LĄDOWA
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1 MW)

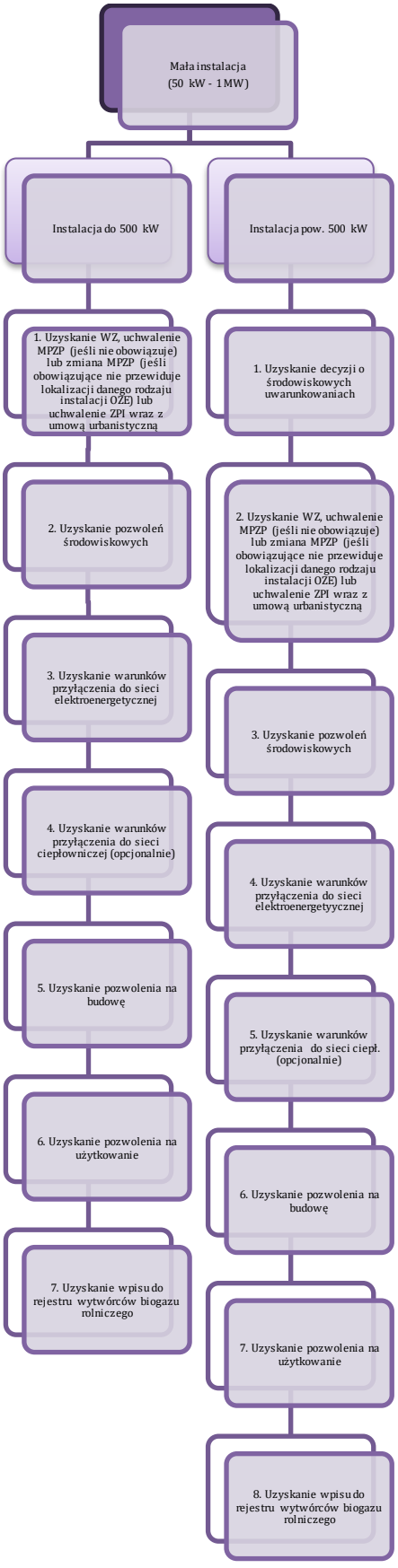

Mikroinstalacja (do 50 kW)
Instalacja nadachowa
Instalacja naziemna
Wysokość do 3 m
Wysokość pow. 3 m
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
1. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia
1. Zgłoszenie wykonywania robót budowlanych
2. Uzyskanie pozwolenia na budowę
2. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia
3. Uzyskanie pozwolenia na użytkowanie
4. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia

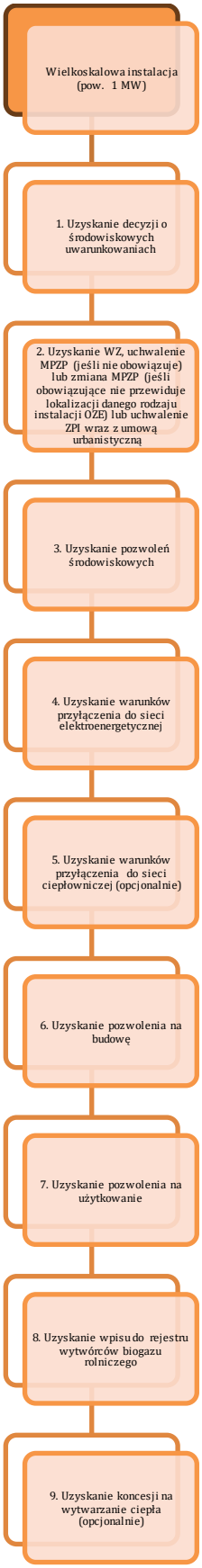

Mała instalacja
(50 kW - 1 MW)
Instalacja naziemna
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie warunków przyłączenia
4. Uzyskanie pozwolenia na budowę
5. Uzyskanie pozwolenia na użytkowanie
6. Uzyskanie wpisu do rejestru MIOZE

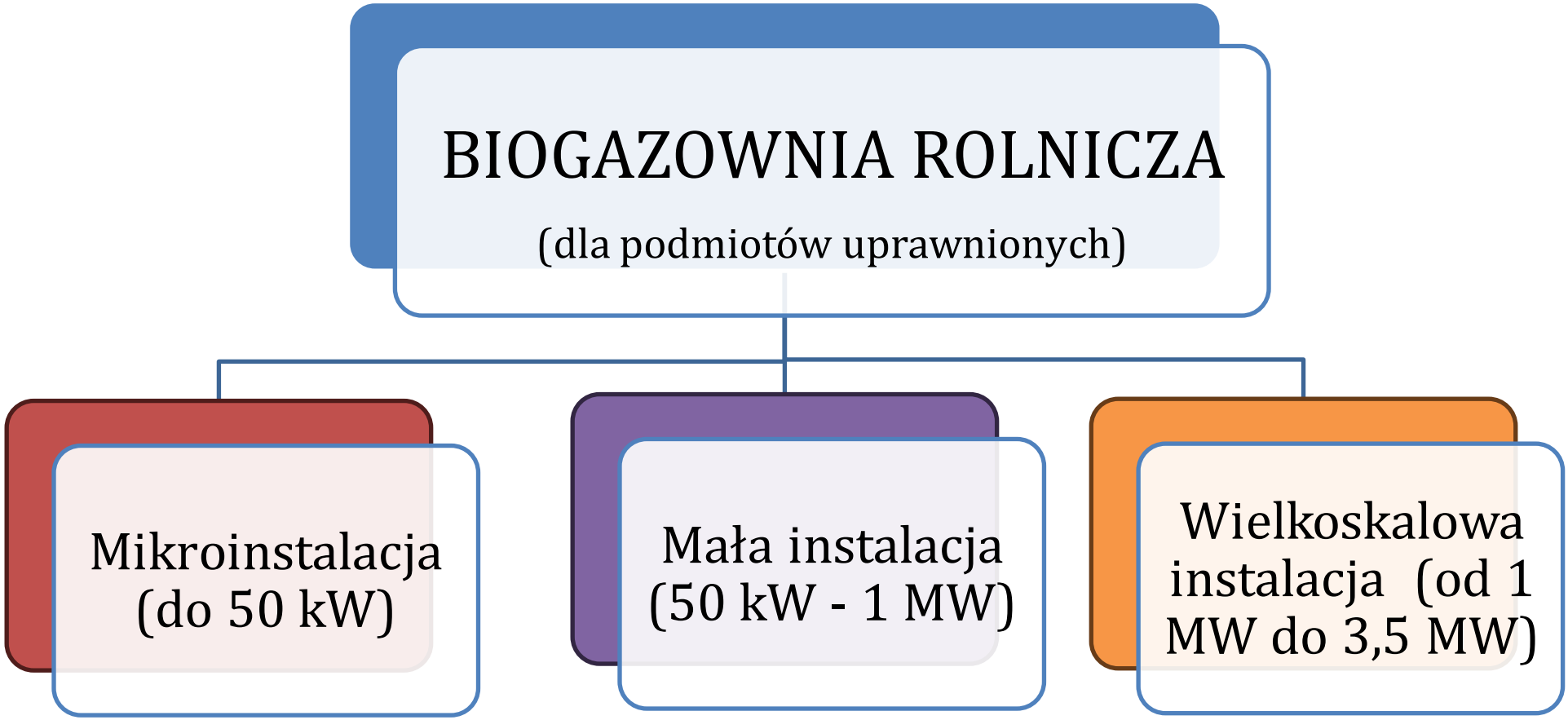
Uwaga:
w przypadku niektórych wiatrowych instalacji wielkoskalowych, przed etapem uzyskania pozwolenia na budowę, niezbędna może być także procedura zgłoszenia farmy wiatrowej jako przeszkody lotniczej (do Prezesa Urzędu Lotnictwa Cywilnego, Ministra Obrony Narodowej oraz ministra właściwego do spraw wewnętrznych).


BIOGAZOWNIA ROLNICZA
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1 MW)

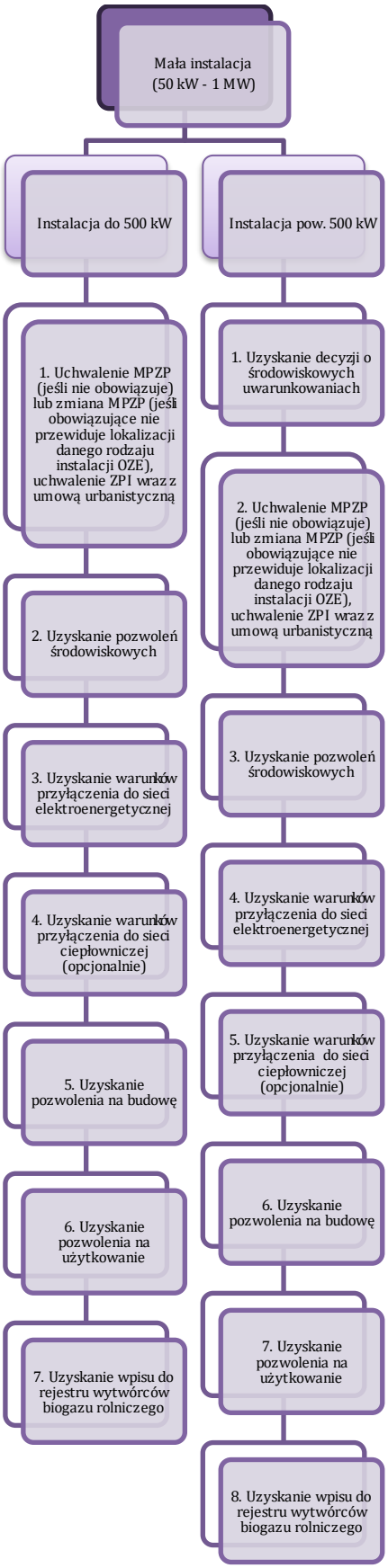

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Zgłoszenie wykonywania robót budowlanych/uzyskanie pozwolenia na budowę
3. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia
4. Zawiadomienie PSP o zakończeniu budowy/ zawiadomienie o zakończeniu budowy

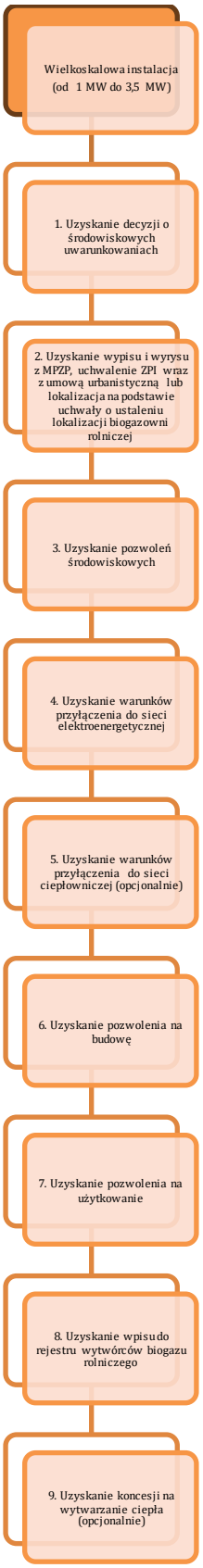

Mała instalacja
(50 kW - 1MW)
Instalacja do 500 kW
Instalacja pow. 500 kW
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwoleń środowiskowych
3. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
4. Uzyskanie warunków przyłączenia do sieci ciepłowniczej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci elektroenergetyycznej
5. Uzyskanie warunków przyłączenia do sieci ciepł. (opcjonalnie)
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego


Wielkoskalowa instalacja (pow. 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
5. Uzyskanie warunków przyłączenia do sieci ciepłowniczej (opcjonalnie)
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego
9. Uzyskanie koncesji na wytwarzanie ciepła (opcjonalnie)

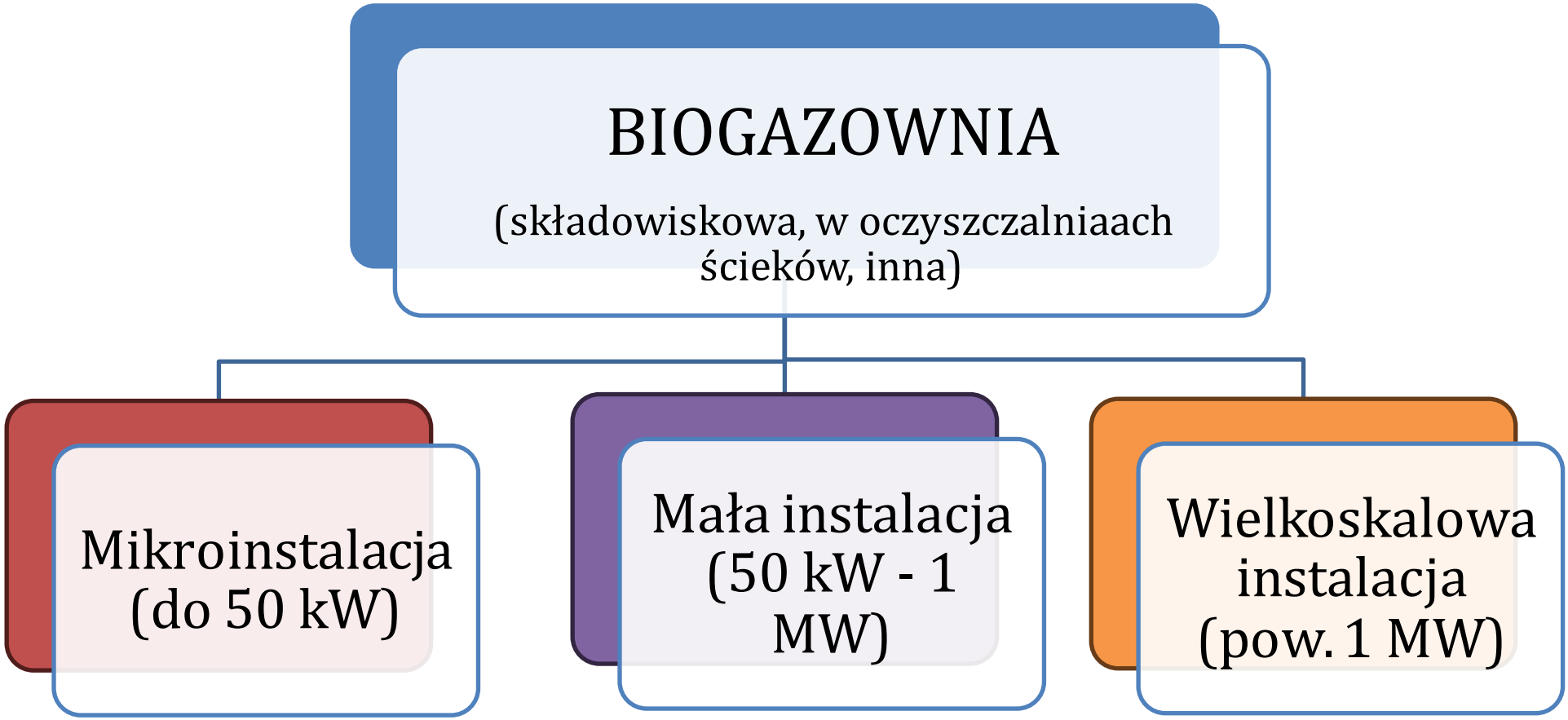

BIOGAZOWNIA ROLNICZA
(dla podmiotów uprawnionych)
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (od 1 MW do 3,5 MW)

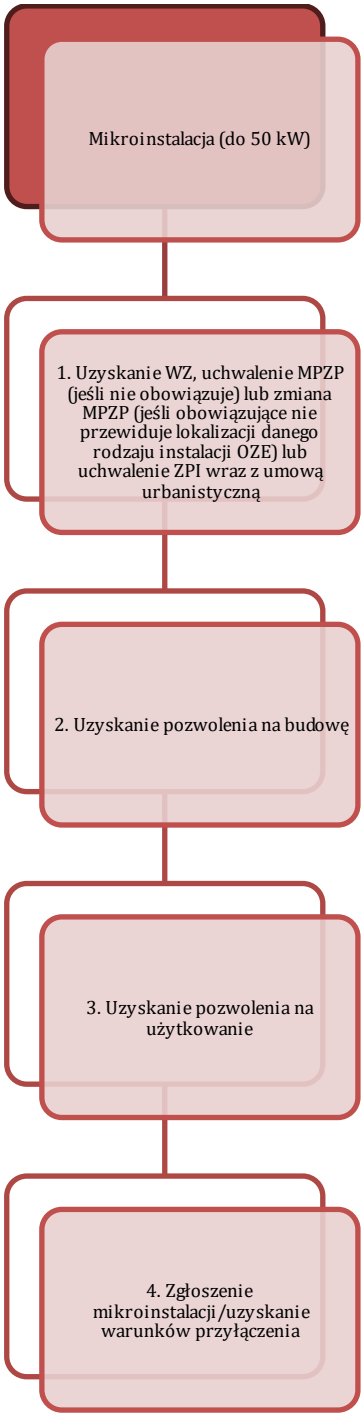

Mikroinstalacja
(do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Zgłoszenie wykonywania robót budowlanych/uzyskanie pozwolenia na budowę
3. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia
4. Zawiadomienie PSP o zakończeniu budowy/ zawiadomienie o zakończeniu budowy


Mała instalacja (50 kW - 1 MW)
Instalacja do 500 kW
1. Uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE), uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwoleń środowiskowych
3. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
4. Uzyskanie warunków przyłączenia do sieci ciepłowniczej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego
Instalacja pow. 500 kW
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE), uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
5. Uzyskanie warunków przyłączenia do sieci ciepłowniczej (opcjonalnie)
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego

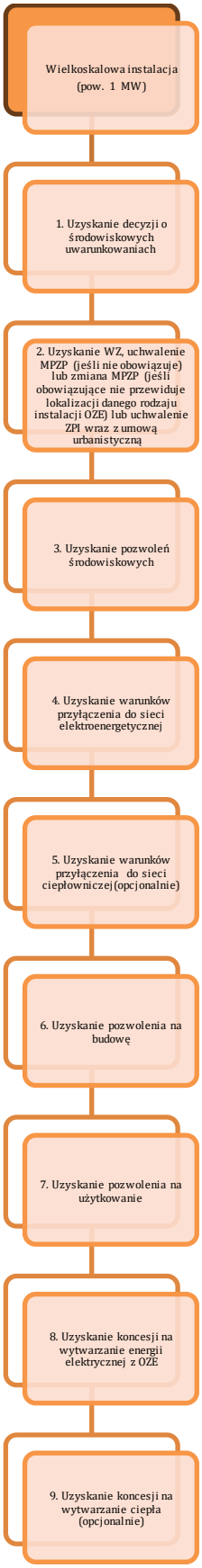


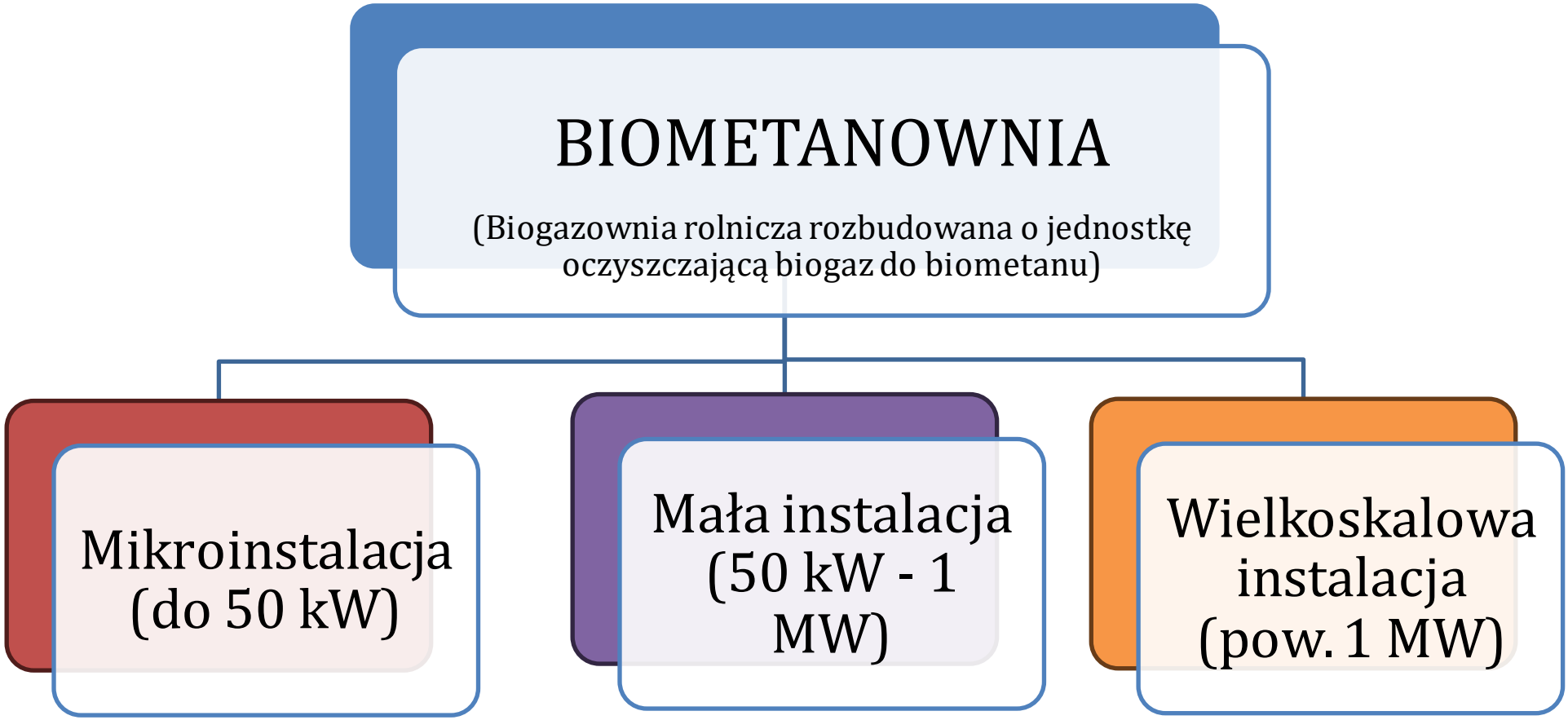
*Odrębna ścieżka dla podmiotów uprawnionych została wprowadzona ustawą z dnia 13 lipca 2023 r. o ułatwieniach w przygotowaniu i realizacji inwestycji w zakresie biogazowni rolniczych, a także ich funkcjonowaniu (Dz.U. 2023 poz. 1597)


BIOGAZOWNIA
(składowiskowa, w oczyszczalniaach ścieków, inna)
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1 MW)

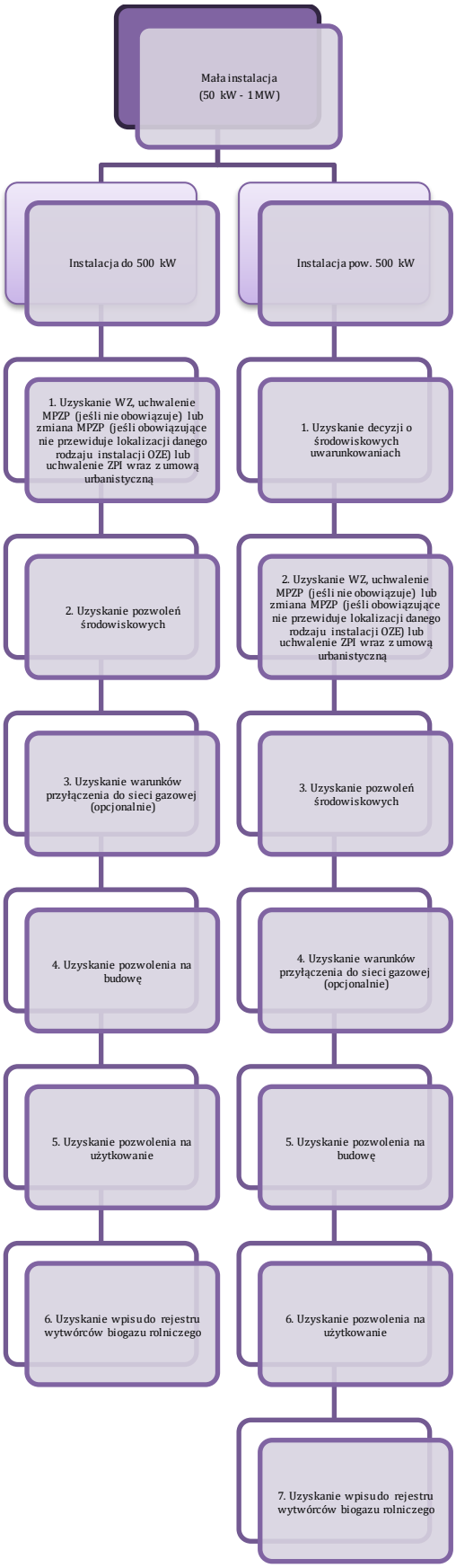

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwolenia na budowę
3. Uzyskanie pozwolenia na użytkowanie
4. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia

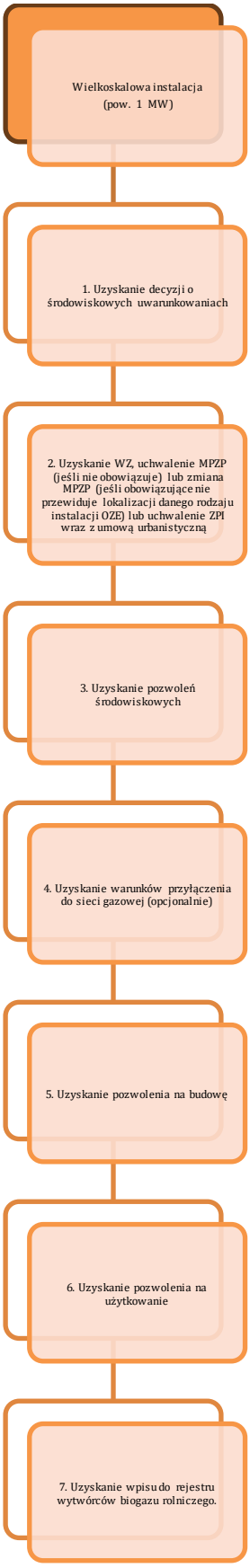

Mała instalacja
(50 kW - 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
5. Przyłączenie do sieci ciepłowniczej (opcjonalnie)
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie wpisu do rejestru MIOZE

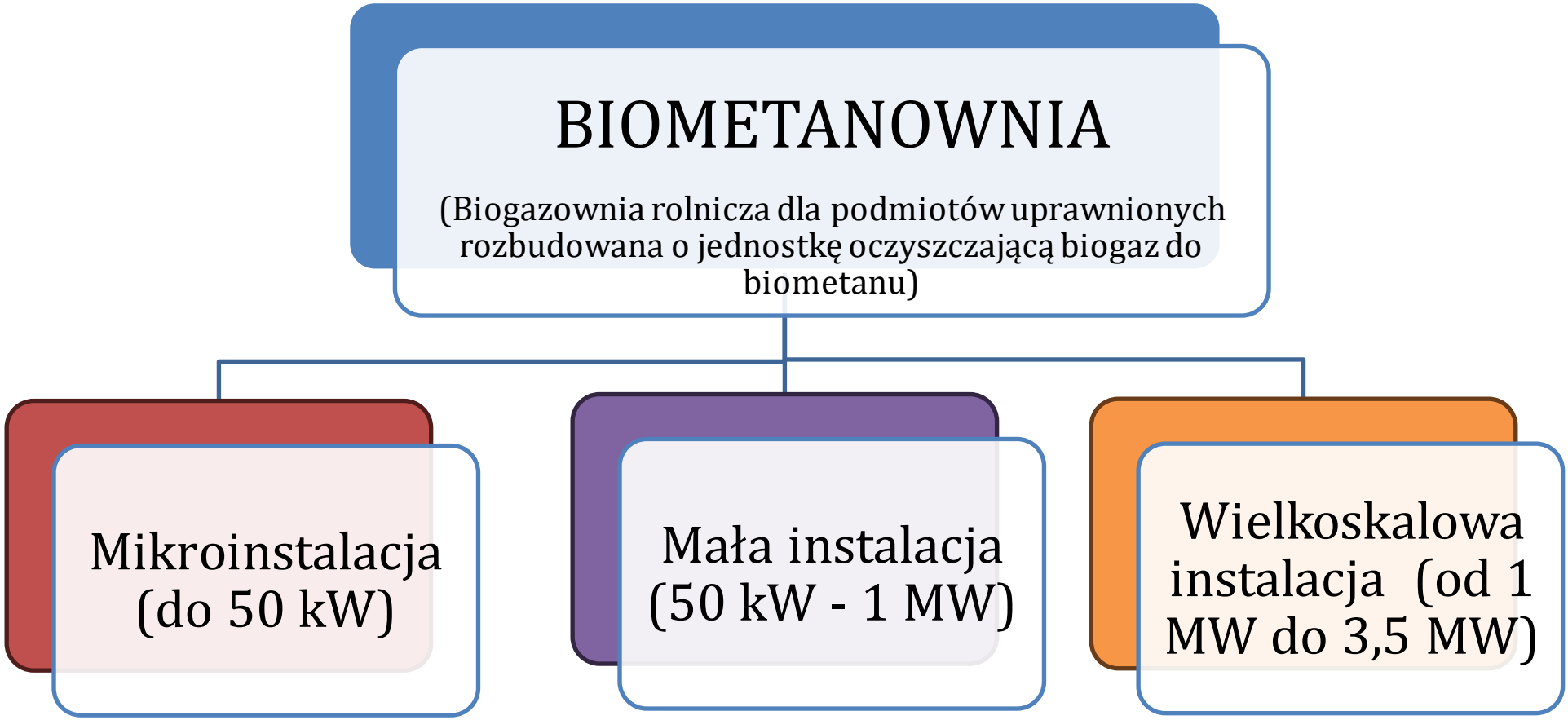

Wielkoskalowa instalacja (pow. 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
5. Uzyskanie warunków przyłączenia do sieci ciepłowniczej(opcjonalnie)
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE
9. Uzyskanie koncesji na wytwarzanie ciepła (opcjonalnie)


BIOMETANOWNIA
(Biogazownia rolnicza rozbudowana o jednostkę oczyszczającą biogaz do biometanu)
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1 MW)

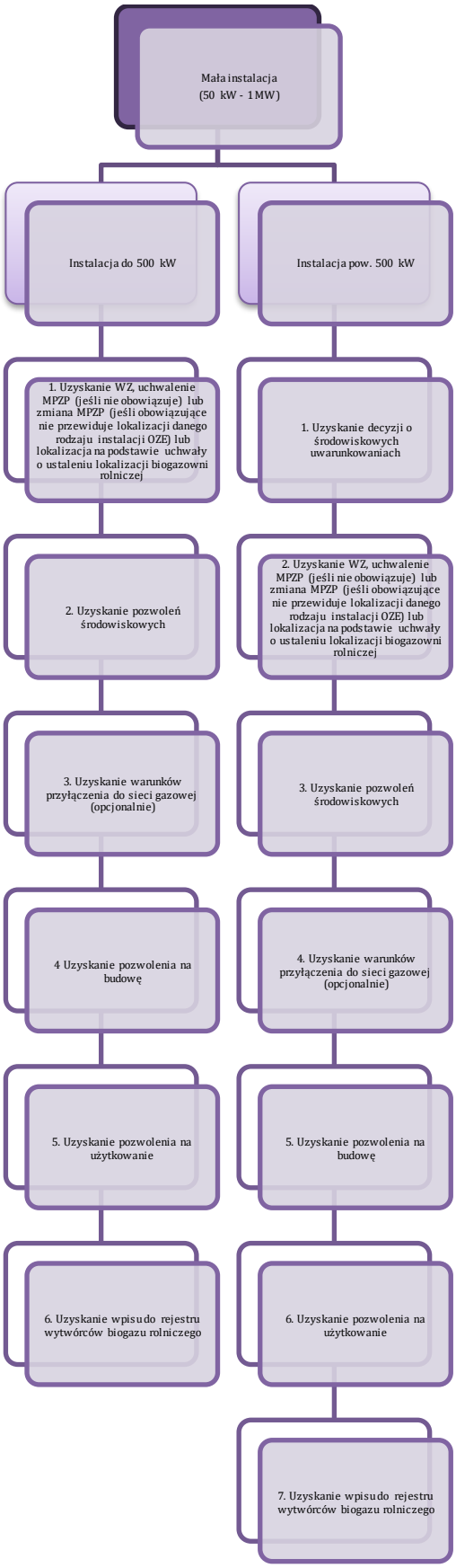

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Zgłoszenie wykonywania robót budowlanych/uzyskanie pozwolenia na budowę
3. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
4. Zawiadomienie PSP o zakończeniu budowy/ zawiadomienie o zakończeniu budowy

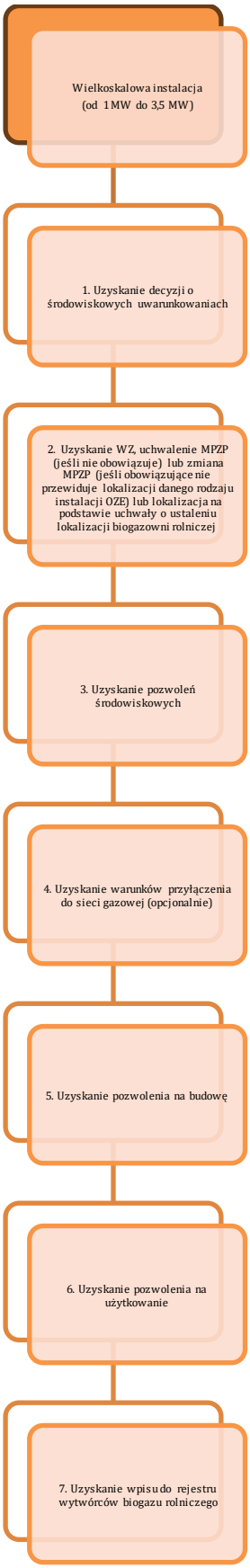

Mała instalacja (50 kW - 1 MW)
Instalacja do 500 kW
Instalacja pow. 500 kW
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwoleń środowiskowych
3. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
4. Uzyskanie pozwolenia na budowę
5. Uzyskanie pozwolenia na użytkowanie
6. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego

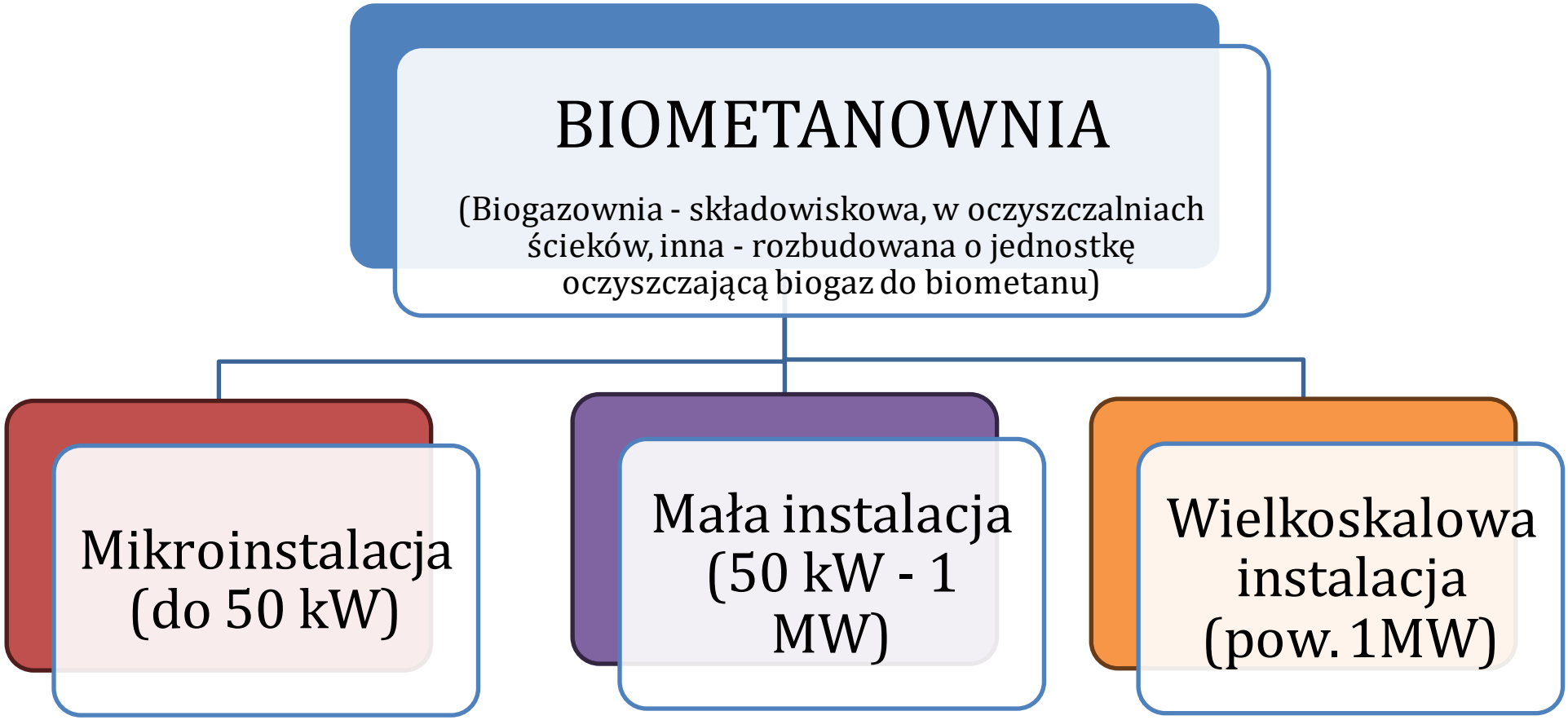

Wielkoskalowa instalacja (pow. 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego.

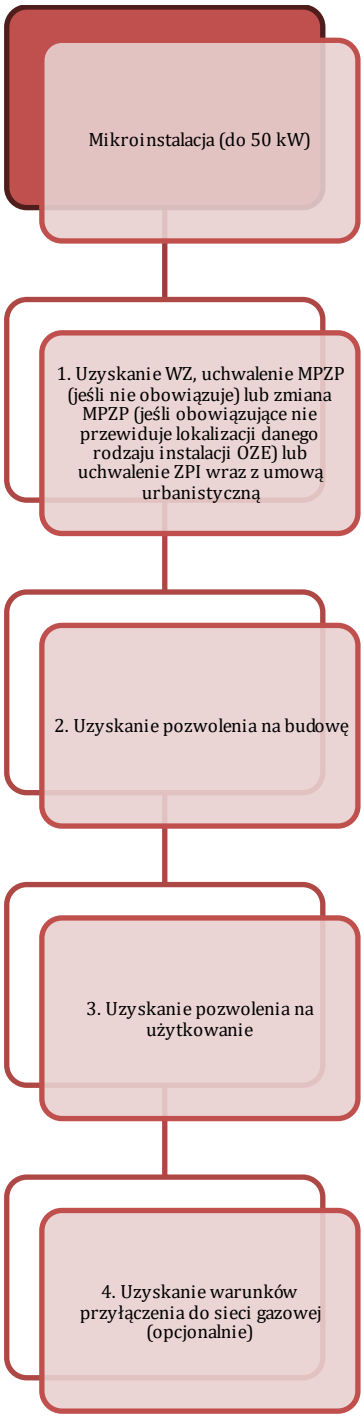

BIOMETANOWNIA
(Biogazownia rolnicza dla podmiotów uprawnionych rozbudowana o jednostkę oczyszczającą biogaz do biometanu)
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (od 1 MW do 3,5 MW)

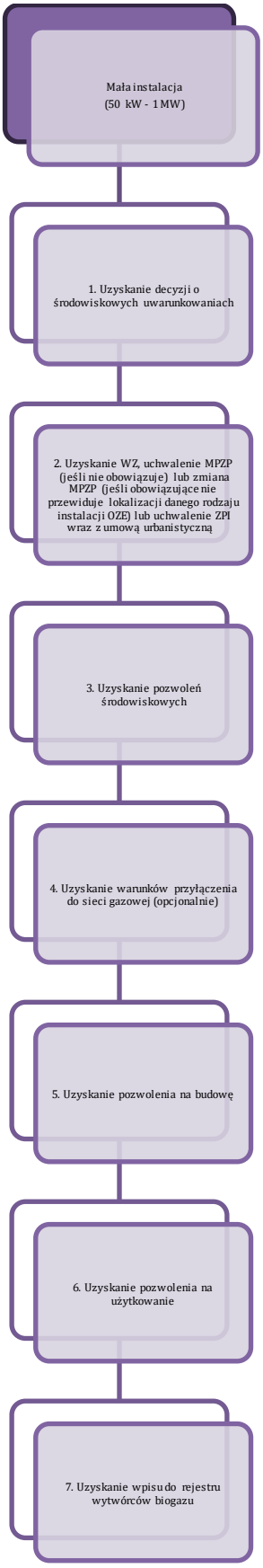

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Zgłoszenie wykonywania robót budowlanych/uzyskanie pozwolenia na budowę
3. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
4. Zawiadomienie PSP o zakończeniu budowy/ zawiadomienie o zakończeniu budowy

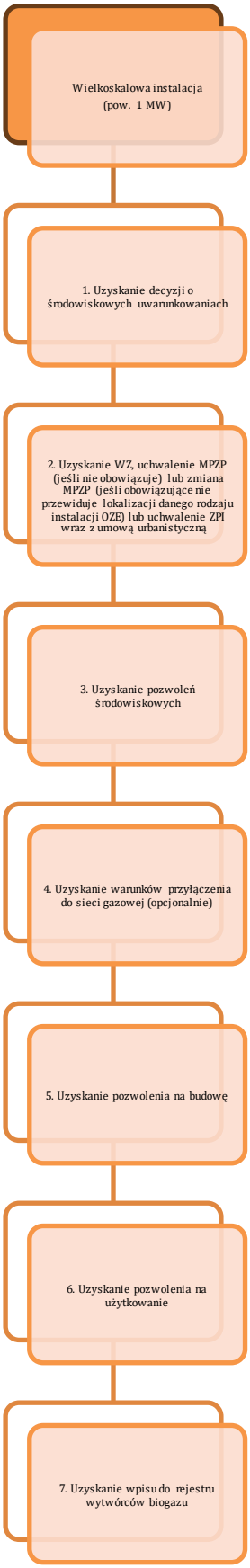

Mała instalacja
(50 kW - 1 MW)
Instalacja do 500 kW
Instalacja pow. 500 kW
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub lokalizacja na podstawie uchwały o ustaleniu lokalizacji biogazowni rolniczej
2. Uzyskanie pozwoleń środowiskowych
3. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
4 Uzyskanie pozwolenia na budowę
5. Uzyskanie pozwolenia na użytkowanie
6. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub lokalizacja na podstawie uchwały o ustaleniu lokalizacji biogazowni rolniczej
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego

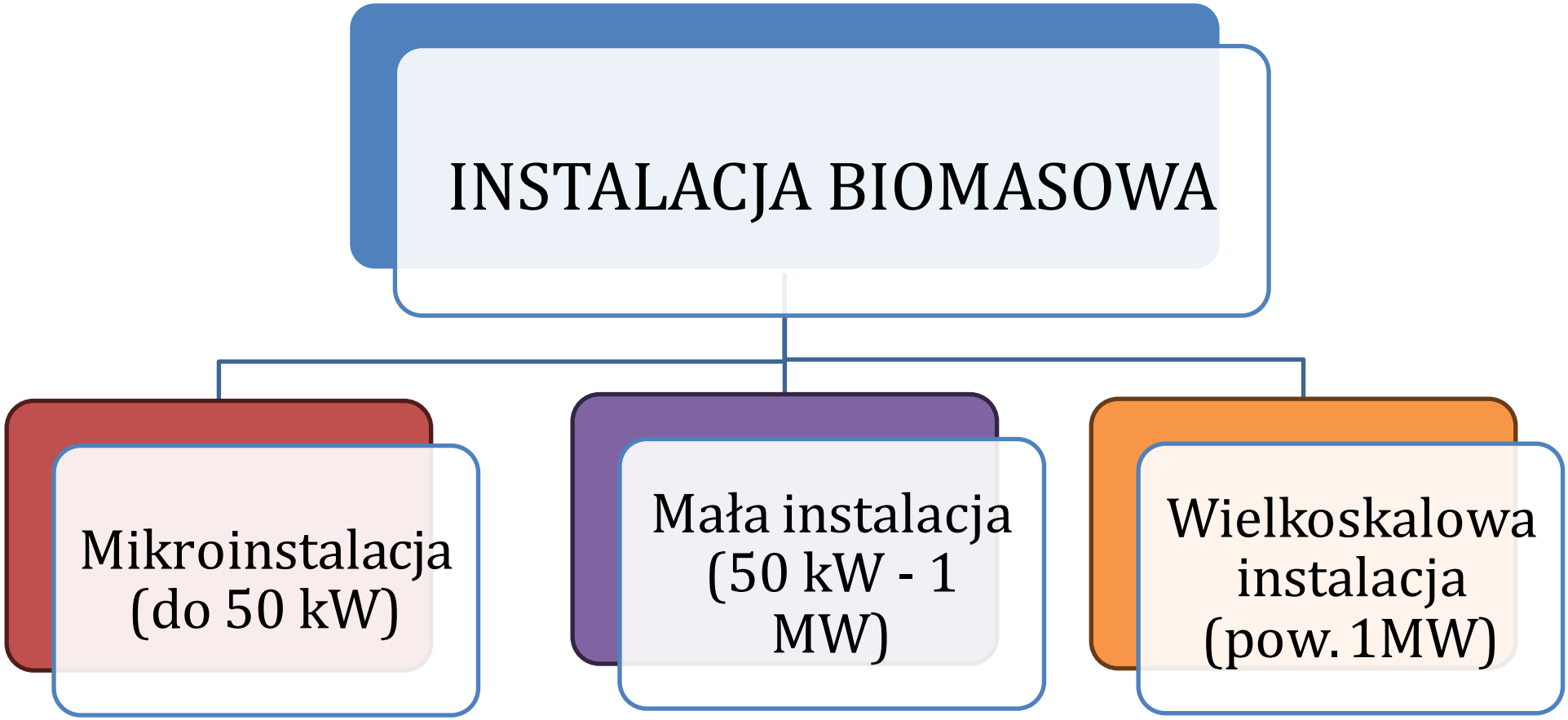

Wielkoskalowa instalacja (od 1 MW do 3,5 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub lokalizacja na podstawie uchwały o ustaleniu lokalizacji biogazowni rolniczej
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu rolniczego

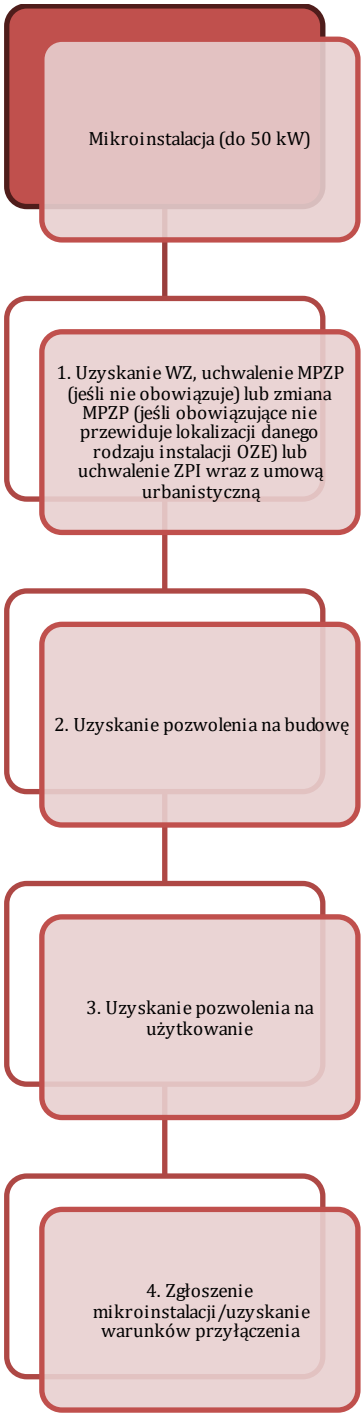

BIOMETANOWNIA
(Biogazownia - składowiskowa, w oczyszczalniach ścieków, inna - rozbudowana o jednostkę oczyszczającą biogaz do biometanu)
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1MW)

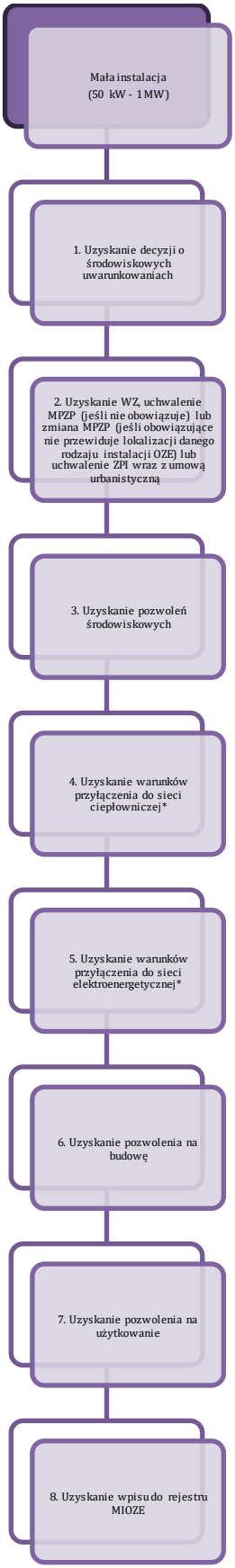

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwolenia na budowę
3. Uzyskanie pozwolenia na użytkowanie
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)


Mała instalacja
(50 kW - 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu

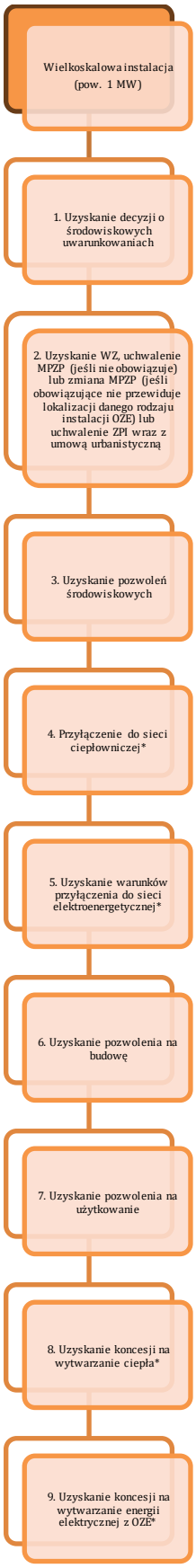

Wielkoskalowa instalacja (pow. 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwoleń środowiskowych
4. Uzyskanie warunków przyłączenia do sieci gazowej (opcjonalnie)
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Uzyskanie wpisu do rejestru wytwórców biogazu


INSTALACJA BIOMASOWA
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1MW)

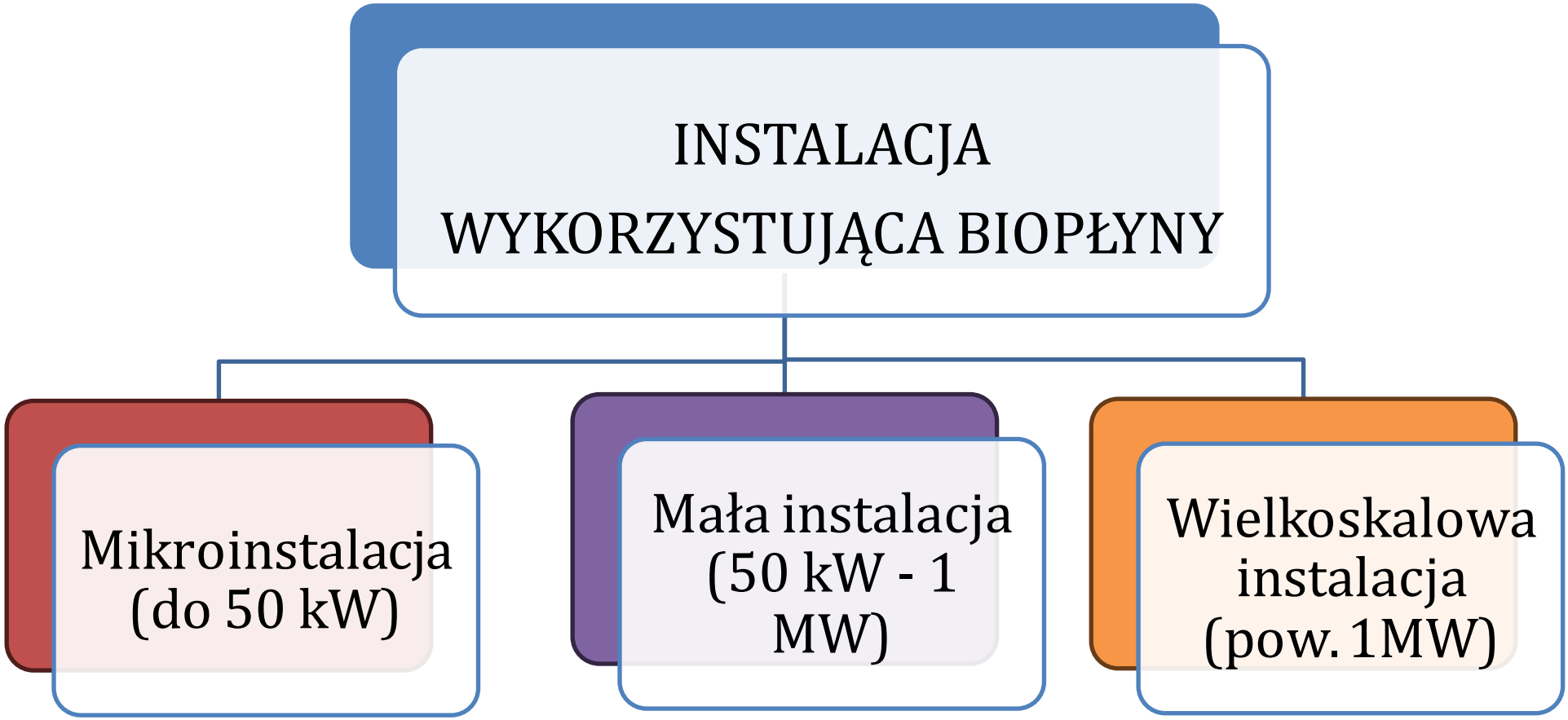

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwolenia na budowę
3. Uzyskanie pozwolenia na użytkowanie
4. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia

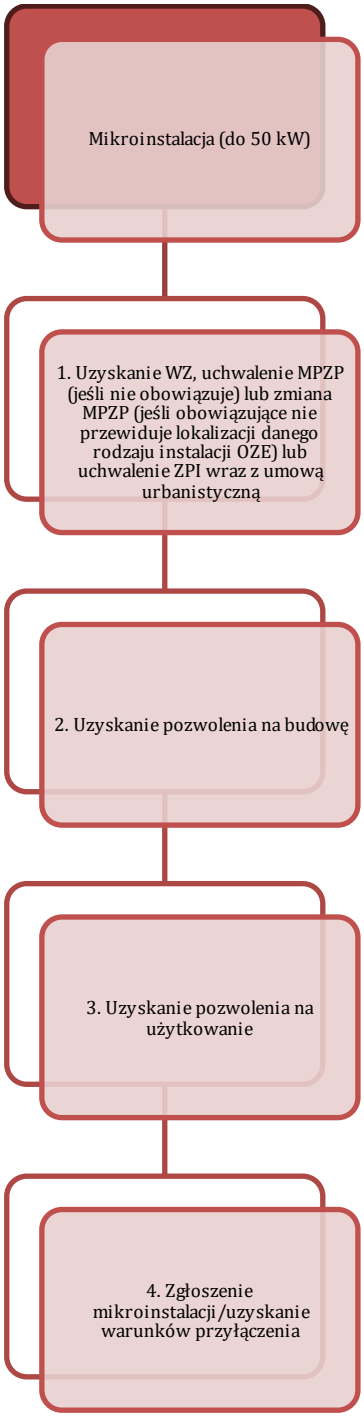


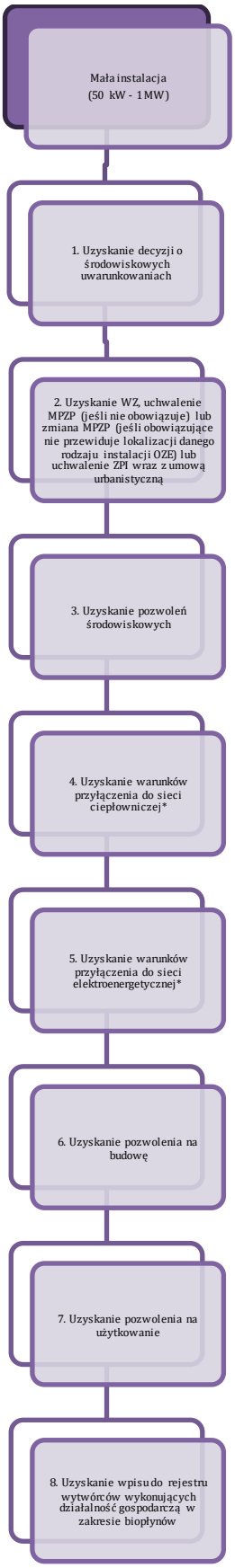
* Konieczność uzyskania warunków przyłączenia do sieci elektroenergetycznej lub/i ciepłowniczej uzależniona jest od rodzaju wytwarzanej energii przez poszczególną instalację.



* Konieczność uzyskania warunków przyłączenia do sieci elektroenergetycznej lub/i ciepłowniczej oraz koncesji na wytwarzanie ciepła lub/i energii elektrycznej z OZE uzależniona jest od rodzaju wytwarzanej energii przez poszczególną instalację.

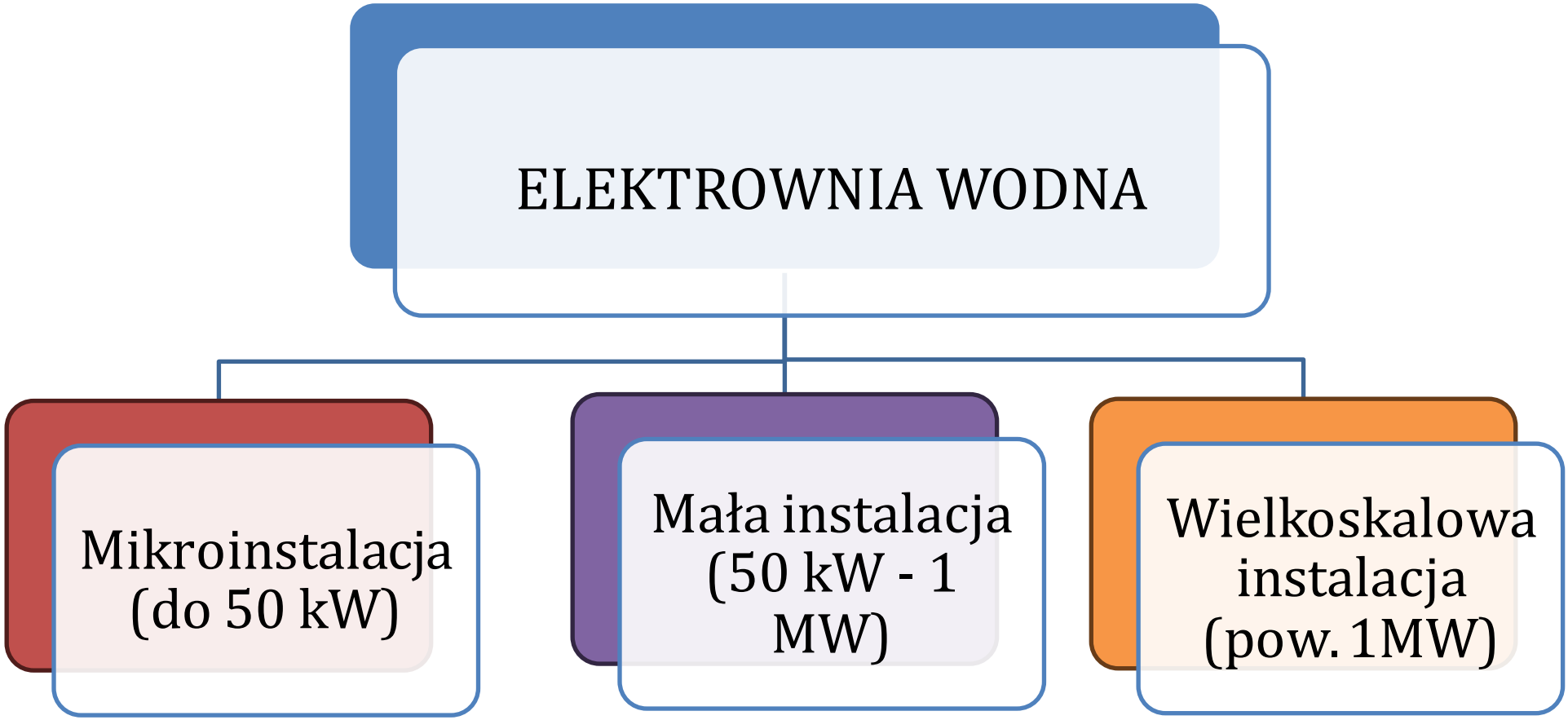

INSTALACJA WYKORZYSTUJĄCA BIOPŁYNY
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1MW)

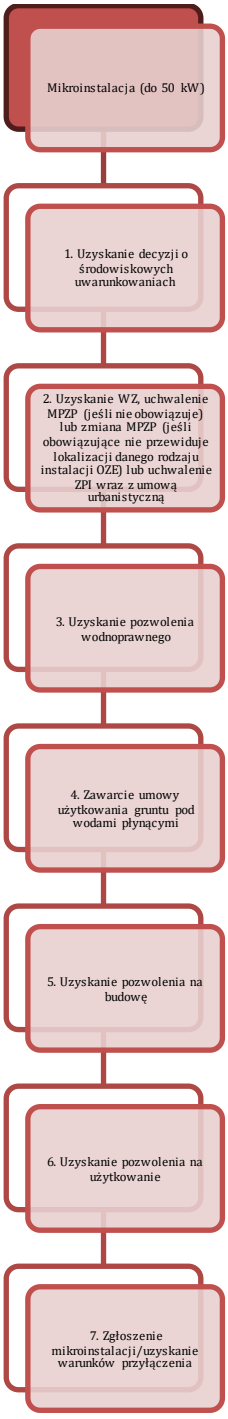

Mikroinstalacja (do 50 kW)
1. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
2. Uzyskanie pozwolenia na budowę
3. Uzyskanie pozwolenia na użytkowanie
4. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia

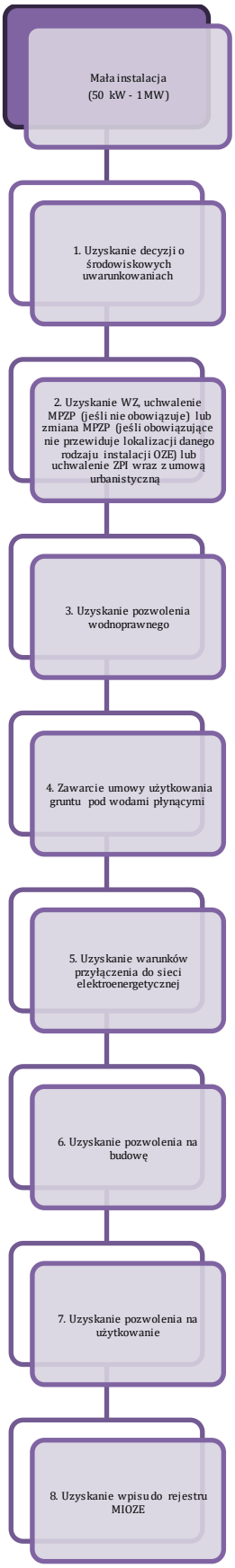


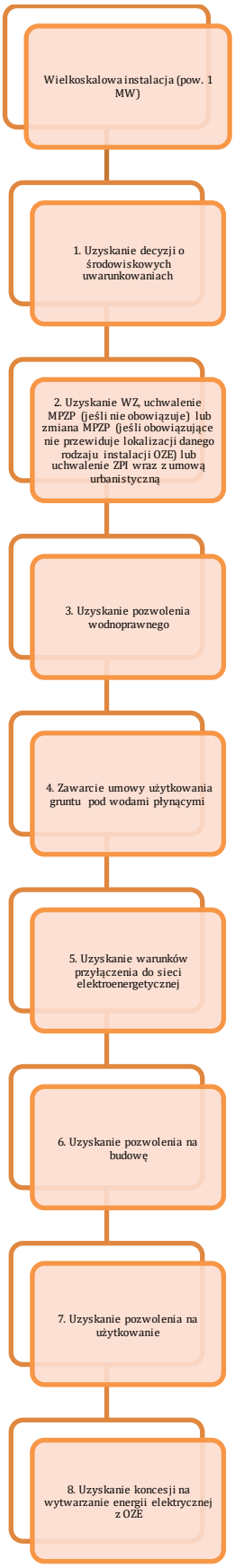
* Konieczność uzyskania warunków przyłączenia do sieci elektroenergetycznej lub/i ciepłowniczej uzależniona jest od rodzaju wytwarzanej energii przez poszczególną instalację.

* Konieczność uzyskania warunków przyłączenia do sieci elektroenergetycznej lub/i ciepłowniczej uzależniona jest od rodzaju wytwarzanej energii przez poszczególną instalację.


ELEKTROWNIA WODNA
Mikroinstalacja (do 50 kW)
Mała instalacja (50 kW - 1 MW)
Wielkoskalowa instalacja (pow. 1MW)


Mikroinstalacja (do 50 kW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwolenia wodnoprawnego
4. Zawarcie umowy użytkowania gruntu pod wodami płynącymi
5. Uzyskanie pozwolenia na budowę
6. Uzyskanie pozwolenia na użytkowanie
7. Zgłoszenie mikroinstalacji/uzyskanie warunków przyłączenia


Mała instalacja
(50 kW - 1MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwolenia wodnoprawnego
4. Zawarcie umowy użytkowania gruntu pod wodami płynącymi
5. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie wpisu do rejestru MIOZE


Wielkoskalowa instalacja (pow. 1 MW)
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach
2. Uzyskanie WZ, uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną
3. Uzyskanie pozwolenia wodnoprawnego
4. Zawarcie umowy użytkowania gruntu pod wodami płynącymi
5. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
6. Uzyskanie pozwolenia na budowę
7. Uzyskanie pozwolenia na użytkowanie
8. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE

INSTALACJA GEOTERMALNA

Poszukiwanie i rozpoznawanie wód termalnych

1. Wybór lokalizacji inwestycji (w tym położenie nieruchomości i złóż);
2. Uzyskanie zatwierdzenia projektu robót geologicznych;
3. Sporządzenie i zatwierdzenie planu ruchu zakładu górniczego;
4. Dokonanie zgłoszenia wodnoprawnego;
5. Uzyskanie decyzji o środowiskowych uwarunkowaniach;
6. Dokonanie zgłoszenia rozpoczęcia robót geologicznych;
7. Uzyskanie zatwierdzenia dokumentacji hydrogeologicznej;
8. Uzyskanie koncesji na eksploatację wód termalnych.

Realizacja inwestycji

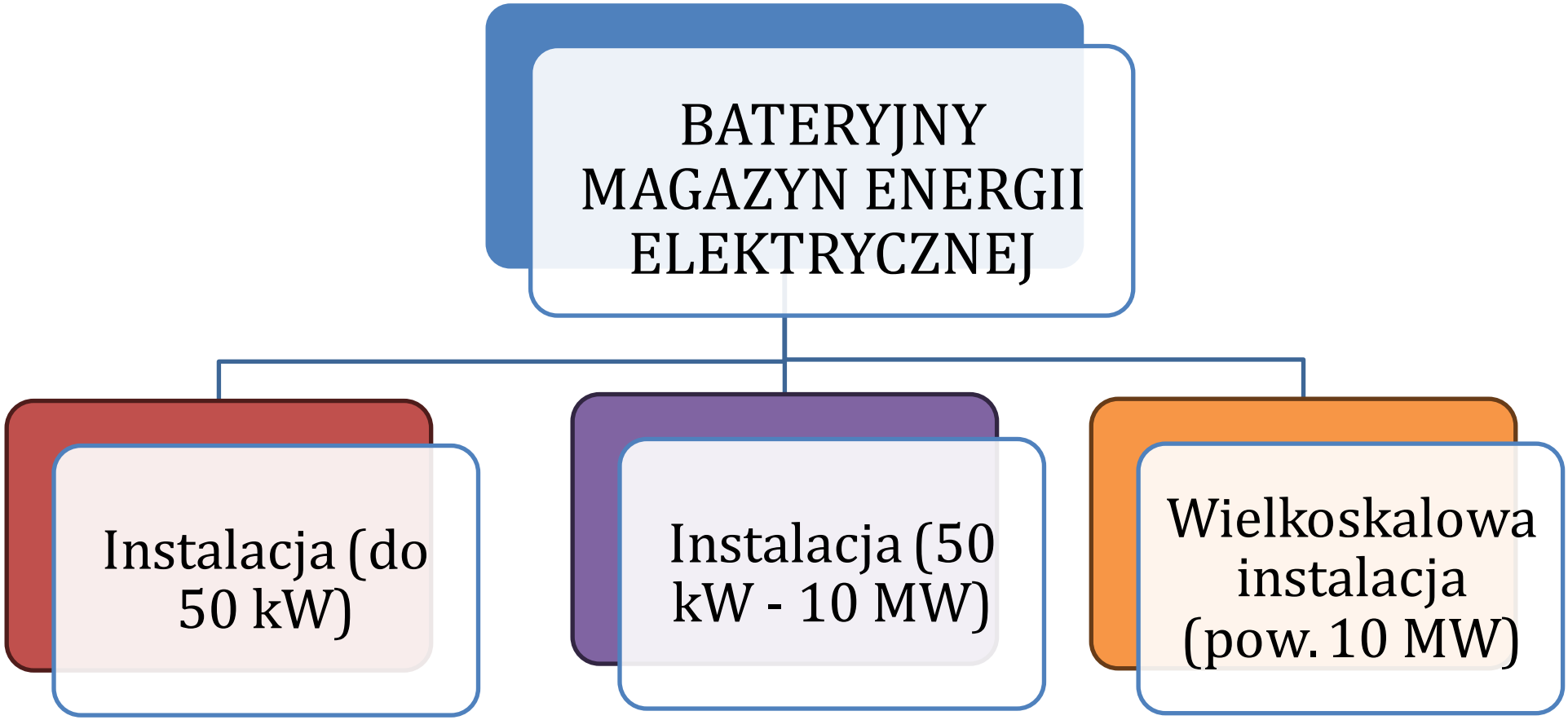
1. Uzyskanie decyzji o środowiskowych uwarunkowaniach;
2. Uzyskanie decyzji WZ (opcjonalnie o lokalizacji inwestycji celu publicznego), uchwalenie MPZP (jeśli nie obowiązuje) lub zmiana MPZP (jeśli obowiązujące nie przewiduje lokalizacji danego rodzaju instalacji OZE) lub uchwalenie ZPI wraz z umową urbanistyczną;
3. Uzyskanie warunków przyłączenia do sieci ciepłowniczej;
4. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej (opcjonalnie);
5. Uzyskanie pozwolenia na budowę;
6. Uzyskanie pozwolenia na użytkowanie;
7. Uzyskanie koncesji na wytwarzanie ciepła (opcjonalnie);
8. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE (opcjonalnie).

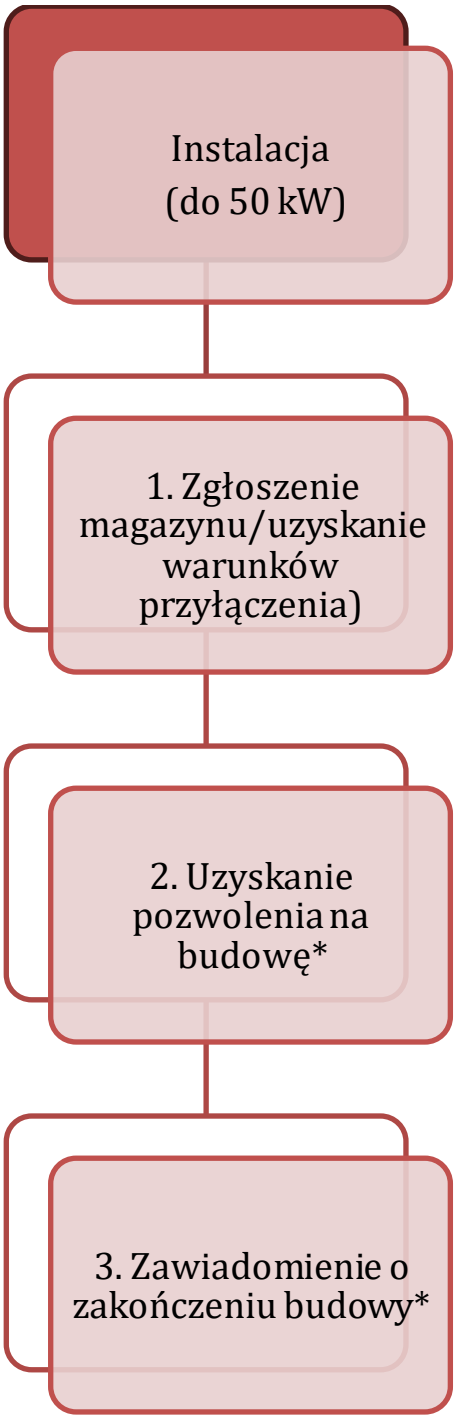
MORSKA FARMA WIATROWA

1. Sprawdzenie możliwości lokalizacji w planie zagospodarowania przestrzennego morskich wód wewnętrznych, morza terytorialnego i wyłącznej strefy ekonomicznej (PZPPOM) i załączniku 1 i 2 do ustawy offshore
2. Uzyskanie pozwolenia na wznoszenie lub wykorzystywanie sztucznych wysp, konstrukcji i urządzeń w polskich obszarach morskich (PSZW)
3. Uzyskanie warunków przyłączenia do sieci elektroenergetycznej
4. Uzyskanie pozwolenia na układanie i utrzymywanie kabli lub rurociągów na obszarach morskich wód wewnętrznych i morza terytorialnego (PUUK)
5. Uzyskanie uzgodnienia układania i utrzymywania kabli lub rurociągów w wyłącznej strefie ekonomicznej (UUUK)
6. Uzyskanie decyzji o środowiskowych uwarunkowaniach dla całej inwestycji
7. Uzyskanie decyzji geologicznych
8. Uzyskanie decyzji zatwierdzających ekspertyzy i plany wymagane ustawą o bezpieczeństwie morskim
9. Uzyskanie pozwolenia na budowę
10. Certyfikacja wymagana ustawą o bezpieczeństwie morskim
11. Przedłożenie wobec OSP ekspertyz zgodności projektowej i wykonawczej
12. Uzyskanie pozwolenia na użytkowanie
13. Uzyskanie koncesji na wytwarzanie energii elektrycznej z OZE

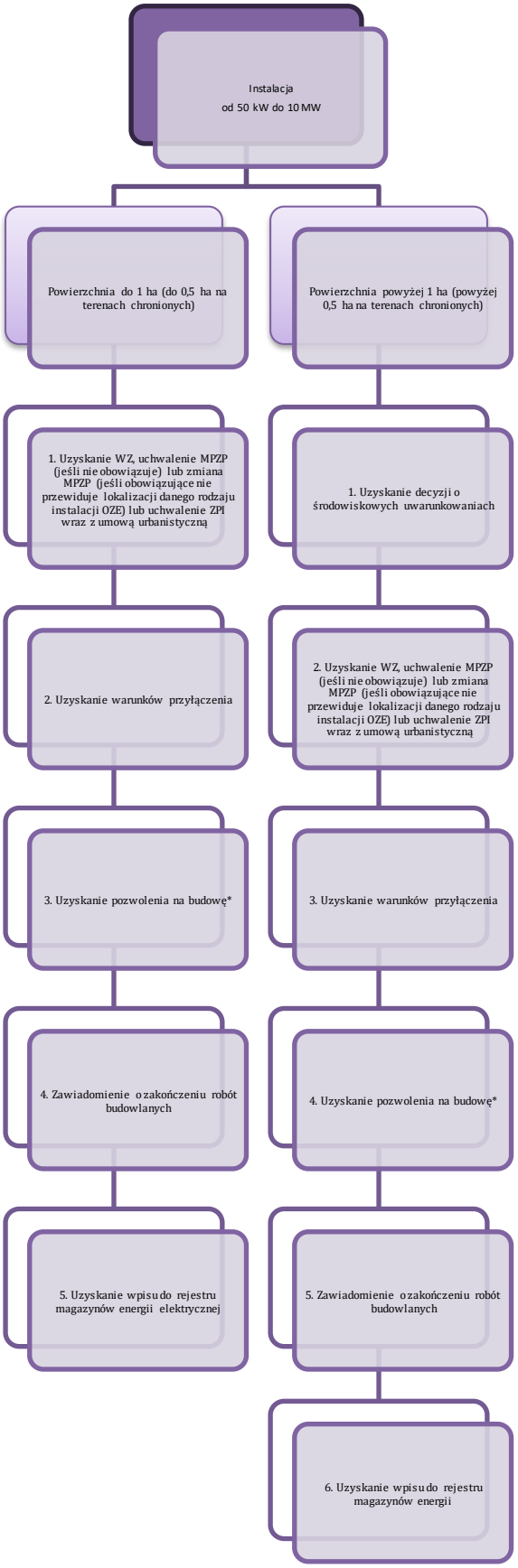
Uwaga:

w przypadku niektórych wielkoskalowych morskich elektrowni wiatrowych przed etapem uzyskania pozwolenia na budowę niezbędna może być także procedura zgłoszenia farmy wiatrowej jako przeszkody lotniczej (do Prezesa Urzędu Lotnictwa Cywilnego, Ministra Obrony Narodowej oraz ministra właściwego do spraw wewnętrznych).

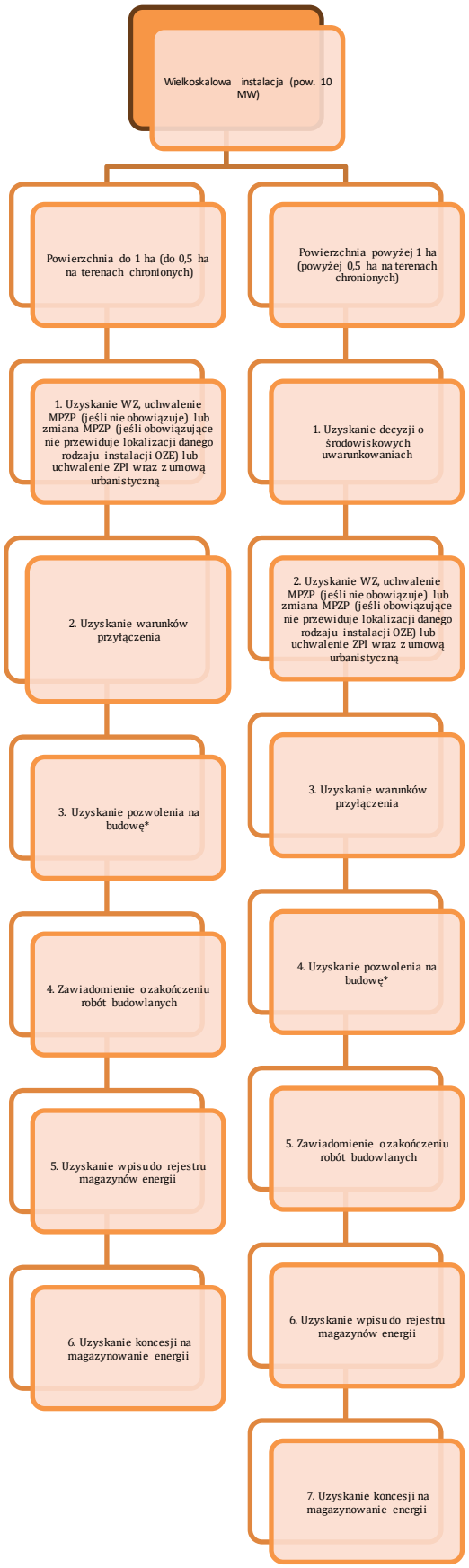

BATERYJNY MAGAZYN ENERGII ELEKTRYCZNEJ
Instalacja (do 50 kW)
Instalacja (50 kW - 10 MW)
Wielkoskalowa instalacja (pow. 10 MW)



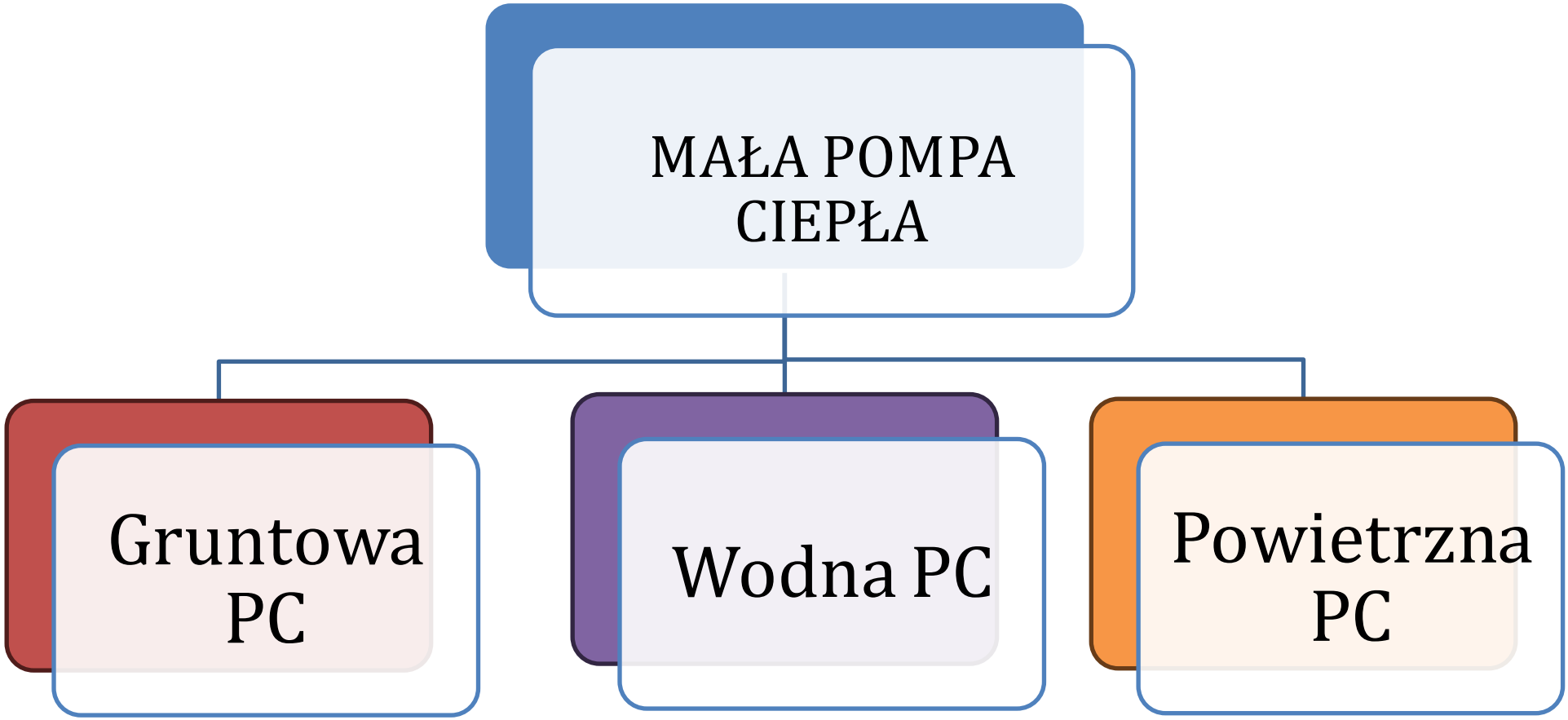
* Kwestia wymogów uzyskania pozwolenia na budowę dla magazynów energii elektrycznej nie jest obecnie wystarczająco uregulowana, stąd konieczność uzyskania pozwolenia na budowę oraz zgłoszenia rozpoczęcia robót budowlanych zależna jest od decyzji właściwego organu architektoniczno-budowlanego. Jednocześnie należy zauważyć, że obecnie procedowana jest zmiana ustawy - Prawo Budowlane, która przewiduje m. in. wprowadzenie możliwości lokalizacji magazynów energii elektrycznej o pojemności nominalnej nie większej niż 20 kWh bez konieczności uzyskiwania pozwolenia na budowę i zgłoszenia rozpoczęcia robót budowlanych.

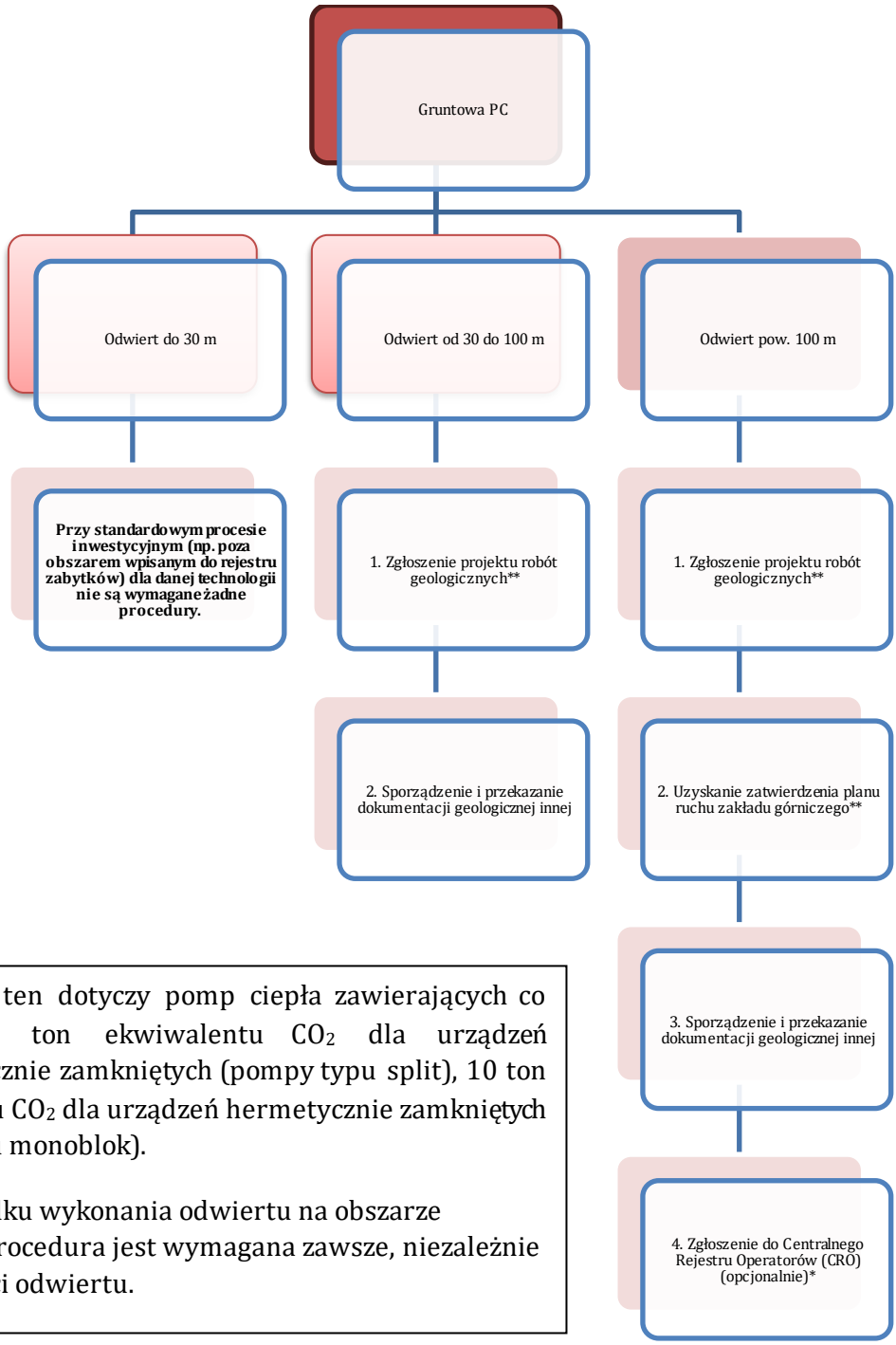


* Kwestia wymogów uzyskania pozwolenia na budowę dla magazynów energii elektrycznej nie jest obecnie wystarczająco uregulowana, stąd konieczność uzyskania pozwolenia na budowę oraz zgłoszenia rozpoczęcia robót budowlanych zależna jest od decyzji właściwego organu architektoniczno-budowlanego. Jednocześnie należy zauważyć, że obecnie procedowana jest zmiana ustawy - Prawo Budowlane, która przewiduje m. in. wprowadzenie możliwości lokalizacji magazynów energii elektrycznej o pojemności nominalnej nie większej niż 20 kWh bez konieczności uzyskiwania pozwolenia na budowę i zgłoszenia rozpoczęcia robót budowlanych.



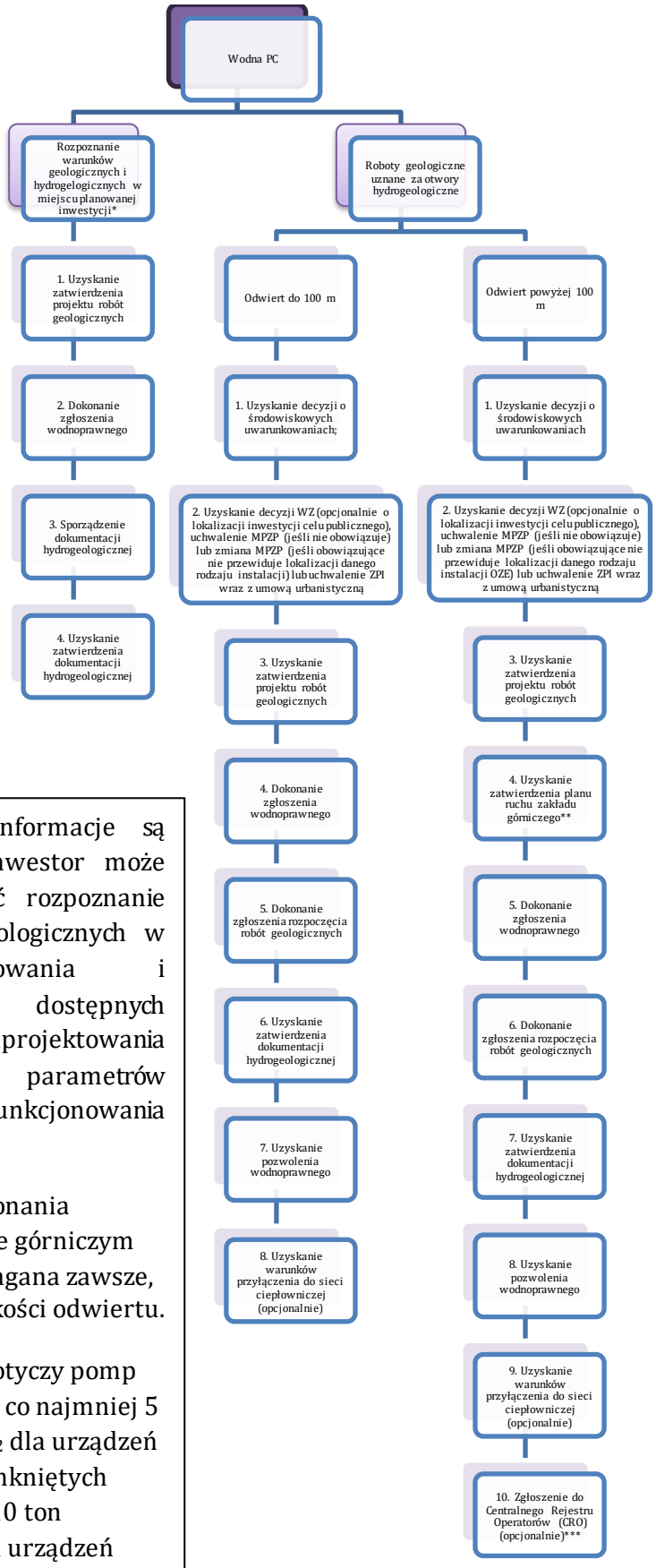
* Kwestia wymogów uzyskania pozwolenia na budowę dla magazynów energii elektrycznej nie jest obecnie wystarczająco uregulowana, stąd konieczność uzyskania pozwolenia na budowę oraz zgłoszenia rozpoczęcia robót budowlanych zależna jest od decyzji właściwego organu architektoniczno-budowlanego. Jednocześnie należy zauważyć, że obecnie procedowana jest zmiana ustawy - Prawo Budowlane, która przewiduje m. in. wprowadzenie możliwości lokalizacji magazynów energii elektrycznej o pojemności nominalnej nie większej niż 20 kWh bez konieczności uzyskiwania pozwolenia na budowę i zgłoszenia rozpoczęcia robót budowlanych.


MAŁA POMPA CIEPŁA
Gruntowa PC
Wodna PC
Powietrzna PC



*Obowiązek ten dotyczy pomp ciepła zawierających co najmniej 5 ton ekwiwalentu CO_2 dla urządzeń niehermetycznie zamkniętych (pompy typu split), 10 ton ekwiwalentu CO_2 dla urządzeń hermetycznie zamkniętych (pompy typu monoblok).

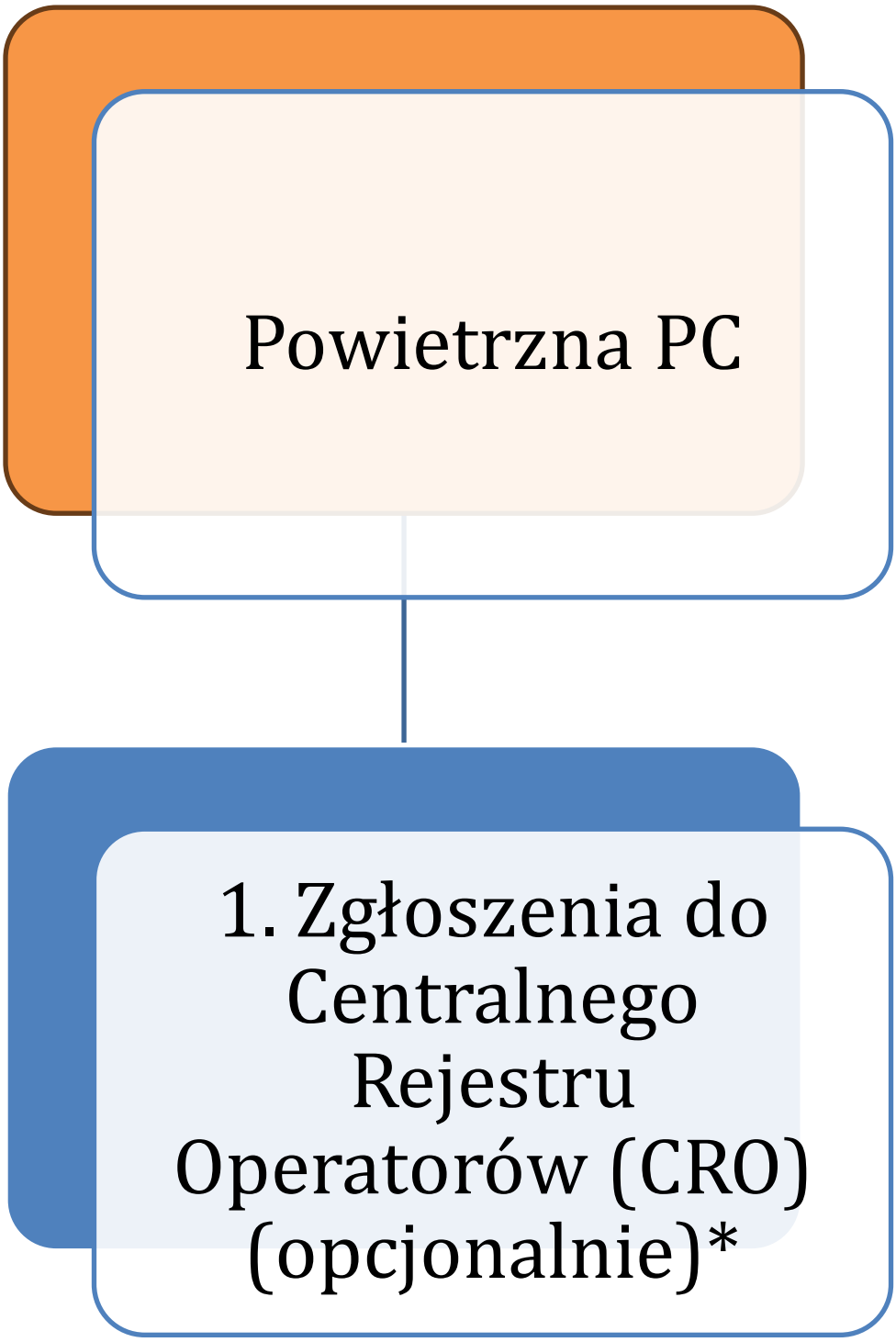
**W przypadku wykonania odwiertu na obszarze górniczym procedura jest wymagana zawsze, niezależnie od głębokości odwiertu.



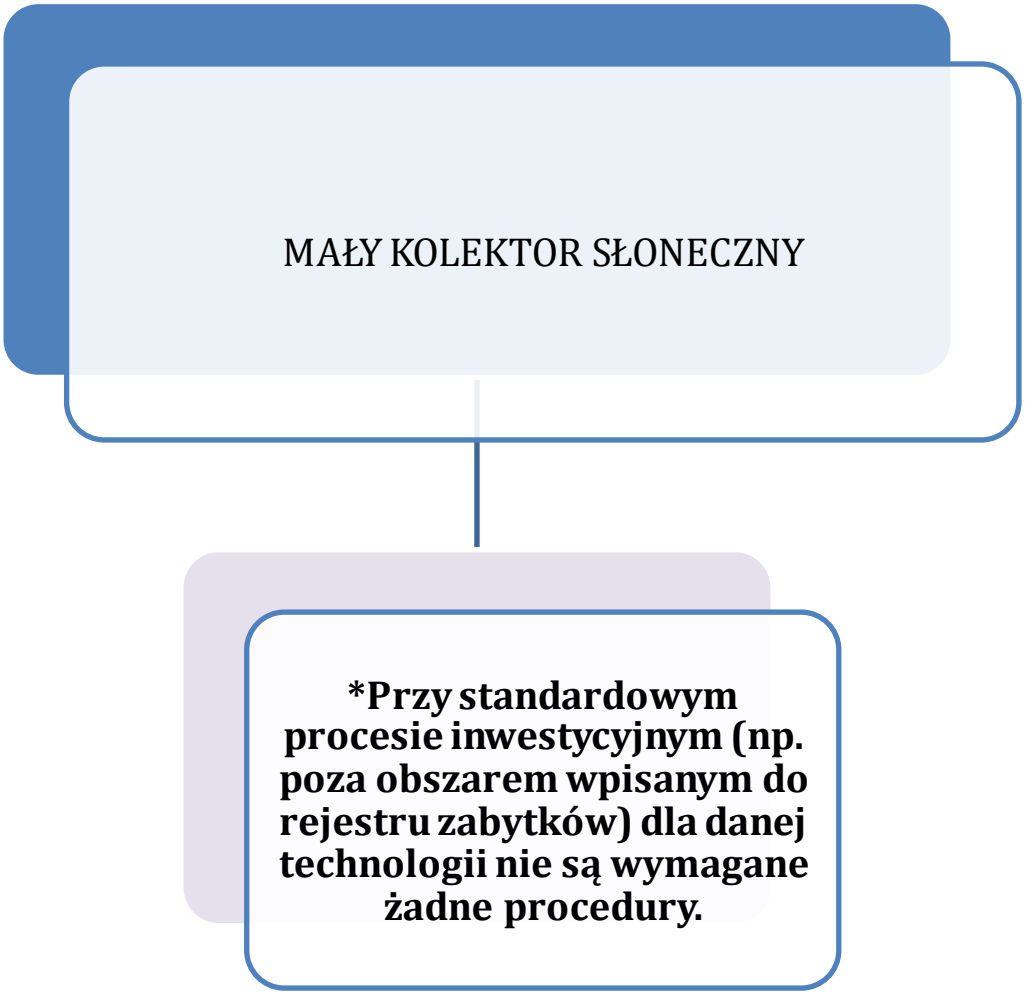
*Jeżeli dostępne informacje są niewystarczające, inwestor może sam przeprowadzić rozpoznanie warunków hydrogeologicznych w celu zweryfikowania i uszczegółowienia dostępnych danych dla zaprojektowania właściwych parametrów technicznych funkcjonowania systemu.

**W przypadku wykonania odwiertu na obszarze górniczym procedura jest wymagana zawsze, niezależnie od głębokości odwiertu.

*** Obowiązek ten dotyczy pomp ciepła zawierających co najmniej 5 ton ekwiwalentu CO_2 dla urządzeń niehermetycznie zamkniętych (pompy typu split), 10 ton ekwiwalentu CO_2 dla urządzeń hermetycznie zamkniętych (pompy typu monoblok).



*Obowiązek ten dotyczy pomp ciepła zawierających co najmniej 5 ton ekwiwalentu CO_2 dla urządzeń niehermetycznie zamkniętych (pompy typu split), 10 ton ekwiwalentu CO_2 dla urządzeń hermetycznie zamkniętych (pompy typu monoblok).


MAŁY KOLEKTOR SŁONECZNY
*Przy standardowym procesie inwestycyjnym (np. poza obszarem wpisanym do rejestru zabytków) dla danej technologii nie są wymagane żadne procedury.

Załącznik 2. Właściwość instytucjonalna w procedurach OZE

Lp.	Procedura	Organ właściwy
1. Procedury środowiskowe		
1.1.	Uzyskanie decyzji o środowiskowych uwarunkowaniach	Regionalny dyrektor ochrony środowiska, wójt/burmistrz/prezydent miasta
1.2.	Uzyskanie pozwolenia wodnoprawnego	Państwowe Gospodarstwo Wodne Wody Polskie
1.3.	Zgłoszenie wodnoprawne	Nadzory wodne, Ministerstwo Infrastruktury
1.4.	Ocena wodnoprawna	Dyrektor Regionalnego Zarządu Gospodarki Wodnej, Dyrektor Zarządu Zlewni
1.5.	Pozwolenie zintegrowane	Starosta, marszałek województwa, regionalny dyrektor ochrony środowiska
1.6.	Pozwolenie na wprowadzanie gazów lub pyłów do powietrza	Marszałek województwa, starosta
1.7.	Pozwolenie na wprowadzenie do obrotu nawozu albo środka wspomagającego uprawę roślin	Minister właściwy ds. rolnictwa
1.8.	Zezwolenie na przetwarzanie odpadów	Starosta, marszałek województwa, regionalny dyrektor ochrony środowiska
1.9.	Pozwolenie na wytwarzanie odpadów powstających podczas eksploatacji instalacji	Marszałek województwa, starosta
1.10.	Zagospodarowanie pofermentu	Minister Rolnictwa i Rozwoju Wsi, marszałek województwa
2. Procedury – zagospodarowanie przestrzenne		
2.1.	Ustalenie lokalizacji inwestycji celu publicznego	Wójt/burmistrz/prezydent miasta, marszałek województwa, wojewoda
2.2.	Uzyskanie decyzji o warunkach zabudowy (WZ)	Wójt/burmistrz/prezydent miasta, wojewoda

2.3.	Uchwała o ustaleniu lokalizacji biogazowni rolniczej	Wójt, burmistrz, prezydent miasta
2.4.	Wniosek o uchwalenie lub zmianę miejscowego planu zagospodarowania przestrzennego (MPZP)	Wójt, burmistrz lub prezydent miasta albo rada gminy
2.5.	Wniosek o wypis i wyrys z miejscowego planu zagospodarowania przestrzennego (MPZP)	Urząd miasta lub gminy
2.6.	Wniosek o wypis i wyrys ze studium uwarunkowań i kierunków zagospodarowania przestrzennego	Urząd miasta lub gminy
2.7.	Zaświadczenie o zgodności zamierzonego sposobu użytkowania z ustaleniami obowiązującego miejscowego planu zagospodarowania przestrzennego (MPZP)	Urząd miasta lub gminy
2.8.	Zaświadczenie o zgodności budowy z ustaleniami obowiązującego miejscowego planu zagospodarowania przestrzennego (MPZP)	Urząd miasta lub gminy
2.9.	Uchwalenie Zintegrowanego Planu Inwestycyjnego (ZPI) wraz z umową urbanistyczną	Wójt, burmistrz lub prezydent miasta
2.10.	Wyłączenie gruntów z produkcji rolniczej	Starosta lub prezydent miasta
3. Procedury przyłączeniowe		
3.1.	Zgłoszenie mikroinstalacji	Operator system dystrybucyjnego
3.2.	Wniosek o wydanie warunków przyłączenia do sieci ciepłowniczej	Operator systemu ciepłowniczego
3.3.	Wniosek o wydanie warunków przyłączenia do sieci elektroenergetycznej	Operator systemu dystrybucyjnego
3.4.	Wniosek o wydanie warunków przyłączenia do sieci gazowej	Operator systemu dystrybucyjnego lub przesyłowego, który jest właścicielem sieci gazowej

4. Procedury budowlane		
4.1.	Uzyskanie pozwolenia na budowę	Starosta, wojewoda
4.2.	Zgłoszenie wykonywania robót budowlanych z projektem budowlanym	Starosta, prezydent miasta lub wojewoda
4.3.	Zgłoszenie budowy lub robót budowlanych bez projektu budowlanego	Starosta, prezydent miasta lub wojewoda
4.4.	Uzyskanie pozwolenia na użytkowanie lub zawiadomienie o zakończeniu robót budowlanych	Powiatowy inspektor nadzoru budowlanego, wojewódzki inspektor nadzoru budowlanego
4.5.	Zawiadomienie o zakończeniu budowy	Powiatowy inspektor nadzoru budowlanego, wojewódzki inspektor nadzoru budowlanego
4.6.	Zawiadomienie Państwowej Straży Pożarnej o zakończeniu budowy	Państwowa Straż Pożarna
4.7.	Zawiadomienie Państwowej Inspekcji Sanitarnej o zakończeniu budowy	Państwowy Powiatowy/Wojewódzki/Graniczny Inspektor Sanitarny
5. Procedury geologiczne		
5.1.	Zatwierdzenie planu ruchu zakładu górniczego	Dyrektor okręgowego urzędu górniczego
5.2.	Zgłoszenie zamiaru rozpoczęcia robót geologicznych	Marszałek województwa, starosta lub Minister Klimatu i Środowiska
5.3.	Sporządzenie i zatwierdzenie dokumentacji hydrogeologicznej po zakończeniu robót geologicznych w zakresie wód podziemnych	Minister właściwy do spraw środowiska, marszałek województwa, starosta
5.4.	Informacja geologiczna	Marszałek województwa, Minister Środowiska
5.5.	Koncesja na wydobywanie kopalin ze złóż (na eksploatację wód termalnych)	Marszałek województwa lub starosta
5.6.	Zatwierdzenie projektu robót geologicznych	Minister właściwy do spraw środowiska, marszałek województwa, starosta
5.7.	Sporządzenie i przekazanie dokumentacji geologicznej innej	Dokumentację geologiczną inną przekazuje się odpowiednio organowi, który udzielił koncesji,

		zatwierdził projekt robót geologicznych lub któremu zgłoszono projekt robót geologicznych.
6. Procedury – morskie farmy wiatrowe		
6.1.	Pozwolenie na wznoszenie lub wykorzystywanie sztucznych wysp, konstrukcji i urządzeń w polskich obszarach morskich (PSZW)	Minister właściwy ds. gospodarki morskiej (Minister Infrastruktury)
6.2.	Pozwolenie na układanie i utrzymywanie kabli na obszarach morskich wód wewnętrznych i morza terytorialnego (PUUK)	Dyrektor urzędu morskiego
6.3.	Uzgodnienie na układanie i utrzymywanie kabli w wyłącznej strefie ekonomicznej (UUUK)	Minister właściwy ds. gospodarki morskiej (Minister Infrastruktury)
6.4.	Decyzje zatwierdzające ekspertyzy i plany z zakresu bezpieczeństwa żeglugi, bezpieczeństwa personelu oraz ochrony środowiska morskiego	Dyrektor Urzędu Morskiego
6.5.	Decyzje zatwierdzające ekspertyzy z zakresu systemów łączności, bezpieczeństwa morskiego, ochrony granicy państwowej oraz obronności	Minister Obrony Narodowej, Minister Spraw Wewnętrznych i Administracji
6.6.	Ekspertyza zgodności projektowej i wykonawczej składana operatorowi systemu przesyłowego	Operator systemu przesyłowego
6.7.	Certyfikacja morskich farm wiatrowych i zespołu urządzeń służących do wyprowadzania mocy	Zgodnie z obwieszczeniem Ministra Infrastruktury z dnia 12 lipca 2023 r. w sprawie wykazu uznanych organizacji upoważnionych do wydawania certyfikatów potwierdzających spełnienie wymagań określonych w art. 82 ust. 1 ustawy z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych (Dz.Urz.MI z 2023 r. poz. 33)

6.8.	Sprawdzenie możliwości lokalizacji w planie zagospodarowania przestrzennego morskich wód wewnętrznych, morza terytorialnego i wyłącznej strefy ekonomicznej (PZPPOM) i załączniku 1 i 2 do ustawy offshore	Nie dotyczy
7. Procedury – wpisy do rejestrów/sprawozdania		
7.1.	Wpis do rejestru wytwórców biopłynów	Dyrektor Generalny KOWR
7.2.	Wpis do rejestru wytwórców biogazu rolniczego	Dyrektor Generalny KOWR
7.3.	Wpis do rejestru wytwórców biogazu	Prezes Urzędu Regulacji Energetyki
7.4.	Wpis do rejestru magazynów energii elektrycznej	Operator systemu dystrybucyjnego albo przesyłowego
7.5.	Wpis do rejestru wytwórców energii w małej instalacji (MIOZE)	Prezes Urzędu Regulacji Energetyki
7.6.	Sprawozdanie wytwórcy energii w małej instalacji	Prezes Urzędu Regulacji Energetyki
8. Procedury koncesyjne		
8.1.	Koncesja na wytwarzanie energii elektrycznej w odnawialnych źródłach energii (OZE)	Prezes Urzędu Regulacji Energetyki
8.2.	Uzyskanie koncesji na wytwarzanie energii elektrycznej w kogeneracji (CHP)	Prezes Urzędu Regulacji Energetyki
8.3.	Koncesja na wytwarzanie ciepła (WCC)	Prezes Urzędu Regulacji Energetyki
8.4.	Koncesja na magazynowanie energii elektrycznej	Prezes Urzędu Regulacji Energetyki
9. Procedury inne		
9.1.	Zapewnienie tytułu prawnego do nieruchomości, na której ma być posadowiona elektrownia wodna	Dyrektor Regionalnego Zarządu Gospodarki Wodnej
9.2.	Wniosek o zawarcie umowy użytkowania gruntu pod wodami płynącymi	Dyrektor Regionalnego Zarządu Gospodarki Wodnej

9.3.	Zgłaszanie i oznakowanie farmy wiatrowej jako przeszkody lotniczej	Prezes Urzędu Lotnictwa Cywilnego, Minister Obrony Narodowej
9.4.	Zgłoszenie pompy ciepła do Centralnego Rejestru Operatorów (CRO)	Zgłoszenie składane jest w elektronicznym systemie CRO
9.5.	Zgłoszenie do Centralnej Ewidencji Emisyjności Budynków (CEEB)	Minister właściwy do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa
9.6.	Uzgodnienie projektu instalacji pod kątem wymagań PPOŻ (dla mikroinstalacji PV > 6,5 kW)	Rzeczoznawca ds. zabezpieczeń przeciwpożarowych, organ PSP
9.7.	Zaświadczenie o dopuszczeniu do aukcji	Prezes Urzędu Regulacji Energetyki
9.8.	Zawiadomienie Państwowej Straży Pożarnej o zakończeniu budowy	Państwowa Straż Pożarna