

ROZDZIAŁ III do SWZ

Opis Przedmiotu Zamówienia

Budowa i wdrożenie Systemu e-ATESTY

Spis treści

<u>1. DEFINICJE.....</u>	<u>3</u>
<u>2. WPROWADZENIE.....</u>	<u>6</u>
<u>3. OGÓLNA ARCHITEKTURA SYSTEMU E-ATESTY</u>	<u>7</u>
<u>4. WYMAGANIA DLA SYSTEMU E-ATESTY</u>	<u>12</u>
<u>5. WYMAGANIA DLA PORTALU WWW I APLIKACJI MOBILNEJ</u>	<u>15</u>
<u>6. WYMAGANIA DLA SYSTEMU CONTENT MANAGEMENT SYSTEM (CMS)</u>	<u>20</u>
<u>7. POZOSTAŁE WYMAGANIA ADMINISTRACYJNE</u>	<u>23</u>
<u>8. PROJEKT TECHNICZNY</u>	<u>27</u>
<u>9. PROJEKT GRAFICZNY</u>	<u>27</u>
<u>10. HARMONOGRAM WDROŻENIA SYSTEMU</u>	<u>28</u>
<u>11. WYDANIE</u>	<u>28</u>
<u>12. WDROŻENIE</u>	<u>29</u>
<u>13. PLAN TESTÓW.....</u>	<u>29</u>
<u>14. DOKUMENTACJA.....</u>	<u>30</u>
<u>15. KODY ŹRÓDŁOWE SYSTEMU</u>	<u>33</u>
<u>16. ASYSTA I KONSERWACJA TECHNICZNA</u>	<u>34</u>
<u>17. SZKOLENIA.....</u>	<u>35</u>
<u>18. UWARUNKOWANIA PRAWNE, NORMY I SYSTEMY</u>	<u>36</u>
<u>19. ZAŁĄCZNIKI DO DOKUMENTU</u>	<u>38</u>

1. Definicje

Administrator IT – Użytkownik Wewnętrzny z najwyższymi uprawnieniami do Systemu, umożliwiającymi dostęp do wszystkich funkcjonalności Systemu.

Atest – Atest Higieniczny lub Świadczenie Jakości Zdrowotnej wydawane dla Produktu przez NIZP PZH-PIB.

Błąd krytyczny - całościowy brak dostępu do Systemu lub jego kluczowych podzespołów uniemożliwiający jakąkolwiek pracę z Systemem bądź zatrzymanie lub poważne zakłócenie pracy Systemu, polegające na niemożliwości wykonania jednej z funkcji mającej wpływ na kluczowe procesy biznesowe aplikacji bez możliwości obejścia problemu, kontynuowania prac.

Błąd niekrytyczny – błąd mający wpływ na działanie funkcji Systemu, jednak nie ograniczający jego zdolności operacyjnych i nie mający wpływu na kluczowe procesy biznesowe Systemu.

Błędy - każda nieprawidłowość w działaniu Systemu, w szczególności wobec wymagań opisanych w niniejszym dokumencie i załącznikach, w tym w OPZ.

CAPTCHA - rodzaj zabezpieczenia, które jest znane jako uwierzytelnianie typu wywołanie – reakcja. Ułatwia ono ochronę przed spamem i odszyfrowywaniem haseł. CAPTCHA polega na wyświetlaniu prośby o wykonanie prostego testu potwierdzającego, że jesteś człowiekiem, a nie komputerem próbującym włamać się na konto chronione hasłem.

CMS (Content Management System) - oprogramowanie pozwalające na łatwe utworzenie i zarządzanie treścią, a także jego późniejszą aktualizację i rozbudowę, również przez redakcyjny personel nietechniczny.

Dokumentacja - Wszelka dokumentacja dotycząca Systemu, kodów źródłowych lub jakichkolwiek innych rezultatów prac Wykonawcy, w tym też ich zmiany lub modyfikacji, która powstanie i zostanie przekazana Zamawiającemu w ramach realizacji Umowy. Dokumentacja obejmuje w szczególności: dokumentację administratora, dokumentację techniczną, dokumentację użytkownika, dokumentację powykonawczą, politykę bezpieczeństwa oraz dokumentację w wersji elektronicznej wbudowaną w System, dotyczącą stworzonego i wdrożonego Systemu. Szczegółowe wymagania dla Dokumentacji są uszczegółowione w rozdziale 14. Dokumentacja.

Dystrybutor – podmiot gospodarczy, który odpowiada za dostępność produktu na rynku.

Dzień roboczy – dzień od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.

Konsument - osoba korzystająca z Aplikacji Mobilnej lub Portalu www, zainteresowana atestowanymi produktami w kontekście bezpieczeństwa dla zdrowia

Modyfikacje Systemu - zmiana Systemu wynikająca ze zmian powszechnie obowiązujących przepisów prawnych, prawnych regulacji dotyczących Zamawiającego, prawnych regulacji do których Zamawiający się stosuje oraz dodania nowych funkcjonalności na wniosek Zamawiającego

NIZP PZH-PIB - Narodowy Instytut Zdrowia Publicznego PZH – Państwowy Instytut Badawczy

Numer CAS - oznaczenie numeryczne przypisane substancji chemicznej przez amerykańską organizację Chemical Abstracts Service (CAS), pozwalające na identyfikację substancji.

Oprogramowanie dedykowane - Oprogramowanie Systemu, stworzone i wdrożone na potrzeby realizacji Umowy, obejmujące też wszelkie modyfikacje i rozszerzenia Oprogramowania Standardowego (może być indywidualizowane), lecz nie będące Oprogramowaniem Standardowym.

Oprogramowanie standardowe - Oprogramowanie stworzone przez podmioty inne niż Wykonawca, niezbędne do zbudowania, uruchomienia i przetestowania Systemu oraz zagwarantowania prawidłowego funkcjonowania środowiska Systemu, które musi być zapewnione przez Wykonawcę w ramach wykonywania Umowy celem prawidłowego działania Systemu, zgodnie z wszelkimi wymaganiami Zamawiającego. Za Oprogramowanie Standardowe uznaje się również oprogramowanie niezbędne do zbudowania, uruchomienia i przetestowania Wdrożenia oraz zagwarantowania prawidłowego funkcjonowania środowiska Systemu, wytworzone przez Wykonawcę, posiadające oznaczenia: nazwę producenta, numer wersji, nazwę handlową lub znak towarowy, jak też to, które było oprogramowaniem skutecznie wdrożonym i opisanym w dokumentacji technicznej, w tym użytkownika i administratora, udostępnionej na każde wezwanie Zamawiającego, jak też będące w obrocie w wersji pierwotnej przed zawarciem Umowy. Do Oprogramowania Standardowego jest zapewniona pełna dostępność usług z nim związanych na zasadach rynkowych, poprzez powszechnie jawne informacje.

Producent – podmiot gospodarczy, który prawnie odpowiada za wytworzenie produktu.

Produkt – wyrób / produkt objęty atestacją. W Systemie e-ATESTY występują tylko produkty, które są objęte lub były objęte atestacją.

PWA – (Progressive web application) progresywna aplikacja internetowa uruchamiana tak jak zwykła strona internetowa, ale umożliwiająca stworzenie wrażenia działania jak natywna aplikacja mobilna lub aplikacja desktopowa

SEM - (Marketing w wyszukiwarkach internetowych, ang. Search Engine Marketing) ogół działań promocyjnych w Internecie, które mają na celu uzyskanie jak najlepszych pozycji serwisu w wynikach wyszukiwania, na wybrane słowa / frazy kluczowe wpisywane przez użytkowników w zapytaniu do wyszukiwarki.

SEO – (Optymalizacja dla wyszukiwarek internetowych, ang. Search Engine Optimization) działania mające na celu wypozycjonowanie witryny internetowej na szczycie listy wyników wyszukiwania (SERP) w tym tzw. optymalizacja techniczna SEO obejmująca m.in. edycję kodu źródłowego serwisu internetowego, która ma za zadanie dostosować go do wymogów wyszukiwarek internetowych oraz wyeliminować błędy techniczne powodujące problemy z poprawnym funkcjonowaniem i indeksowaniem strony internetowej przez roboty sieciowe.

Testy swobodne - testy, w których tester wykonuje działania w Systemie bez używania jakiegokolwiek przypadku testowego, który opisywałby jego przebieg. W testach swobodnych możliwe powinno być nie tylko wprowadzanie przez testera dowolnych danych na których jest wykonywany test, ale również wybieranie dowolnych ścieżek testowania (wybór kolejnych

kroków testowych). Jedyńm warunkiem jaki musi być spełniony podczas testów swobodnych jest konieczność wykonywania przez testera działań/ kroków, które będą weryfikować prawidłowość przebiegów zatwierdzonych procesów. Zakres testów stanowią sformułowane zadania do przeprowadzenia testów swobodnych w odpowiednich obszarach systemu.

Usprawnienia Systemu - zmiana Systemu wynikająca z usuwania Błędów

Użytkownik Wewnętrzny – pracownik Zamawiającego posiadający uprawnienia do pracy w Systemie e-ATESTY

Webhook - powiadomienie o wydarzeniu przesyłane za pośrednictwem HTTP

Wersje Systemu - zmiana Systemu wynikająca z postępu technologicznego i technicznego

Wnioskodawca - podmiot, który składa wniosek (np. Użytkownik produktu, Dystrybutor, Producent, Pełnomocnik wnioskodawcy). Może składać wniosek w imieniu własnym lub Producenta/ Dystrybutora

2. Wprowadzenie

Projektowany System e-ATESTY obejmuje udostępniane publicznie Aplikację Mobilną oraz Portal WWW dostępny w przeglądarce internetowej. Celem Systemu jest udostępnienie dla Konsumentów możliwości przeglądania i wyszukiwania Atestów Higienicznych i Świadectw Jakości Zdrowotnej wydanych przez Instytut NIZP PZH-PIB.

Dane nt. atestów będą zasilać bazę Systemu e-ATESTY z systemów wewnętrznych Instytutu NIZP PZH-PIB. Wykonawca jest zobowiązany do dostarczenia usług sieciowych umożliwiających zarządzanie tymi danymi.

System e-ATESTY dostarczy statystyki przeglądania produktów z Atestami oraz sposobu używania Systemu przez Konsumentów w celu usprawnienia jakości dostarczanych przez Instytut usług.

We wszystkich zapisach SWZ oraz jej załącznikach, w tym w niniejszym OPZ, w których Zamawiający odwołuje się do norm, aprobat, specyfikacji technicznych lub systemów odniesienia Zamawiający dopuszcza rozwiązania równoważne. W przypadku, gdy w opisie przedmiotu zamówienia podano nazwy rozwiązań, oprogramowania lub urządzeń konkretnych producentów to należy traktować to jedynie jako określenie pożądanego standardu i jakości. We wszystkich takich sytuacjach Wykonawca może zaoferować równoważne rozwiązania o co najmniej takich samych parametrach. Przez równoważność rozumie się zaoferowanie rozwiązania, którego parametry techniczne i funkcjonalności są co najmniej takie same jak opisanych w SWZ. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca zobowiązany jest wykazać równoważność zastosowanych rozwiązań. Wdrożenie rozwiązania równoważnego wymaga zatwierdzenia przez Zamawiającego.

Zakres zamówienia

Zaprojektowanie i wybudowanie oprogramowania spełniającego wskazane w niniejszym dokumencie wymagania funkcjonalne. Oprogramowanie dedykowane będzie wdrożone na platformie oprogramowania/podsystemów/bibliotek zgodnych z wymaganiami wskazanymi w niniejszym opracowaniu. Wykonawca przekaze pełne niezaciemnione (ang. „obfuscation”) kody źródłowe oprogramowania dedykowanego opisanego wraz z nieusuniętymi komentarzami oraz autorskie prawa majątkowe w zakresie pól eksploatacji i na zasadach określonych w Umowie.

Zakres zamówienia obejmuje:

1. Wykonanie szczegółowego Projektu Technicznego Systemu.
2. Projekt Graficzny Systemu.
3. Dostarczenie i wdrożenie Systemu e-ATESTY.
4. Dostarczenie oprogramowania dedykowanego wraz kodami źródłowymi i prawami autorskimi.
5. Dostarczenie oprogramowania standardowego wraz z odpowiednimi licencjami.
6. Publikację Aplikacji Mobilnej w marketach Google Play Store oraz Apple App Store.

7. Dostarczenie strategii dotyczącej pozycjonowania strony z użyciem narzędzi SEO (Search Engine Optimization) i SEM (Search Engine Marketing) – w tym SEO on-site: techniczne, UX’owe i dotyczące treści oraz SEO off-site (content marketing i link building)
8. Dostawę Dokumentacji.
9. Przeprowadzenie Szkoleń.
10. Prace rozwojowe dla Systemu e-ATESTY w wymiarze 40 roboczogodzin, realizowane na zlecenie Zamawiającego bez dodatkowych kosztów, możliwe do wykorzystania na każdym etapie realizacji Umowy.
11. Udzielenie Gwarancji na wdrożony System i świadczenie usług w zakresie Gwarancji:
 - a. Okres gwarancji minimum 12 miesięcy od zakończenia wdrożenia (odbioru końcowego Systemu)
 - b. W każdym przypadku, w którym będzie to możliwe, Wykonawca będzie świadczył opiekę serwisową/gwarancyjną w sposób zdalny.
 - c. Usługi gwarancyjne świadczone na zasadach SLA określonych w Umowie
12. Dostarczanie nowych wersji Systemu w okresie gwarancji wraz z ich instalacją i konfiguracją w celu zapewnienia zgodności z aktualnym stanem prawnym.
13. Aktualizację dokumentacji będącą wynikiem aktualizacji komponentów Systemu.

Termin realizacji

Realizacja przedmiotu zamówienia podzielona została na następujące etapy:

Etap 1 – Projekt techniczny nie później niż 1 miesiąc od podpisania umowy.

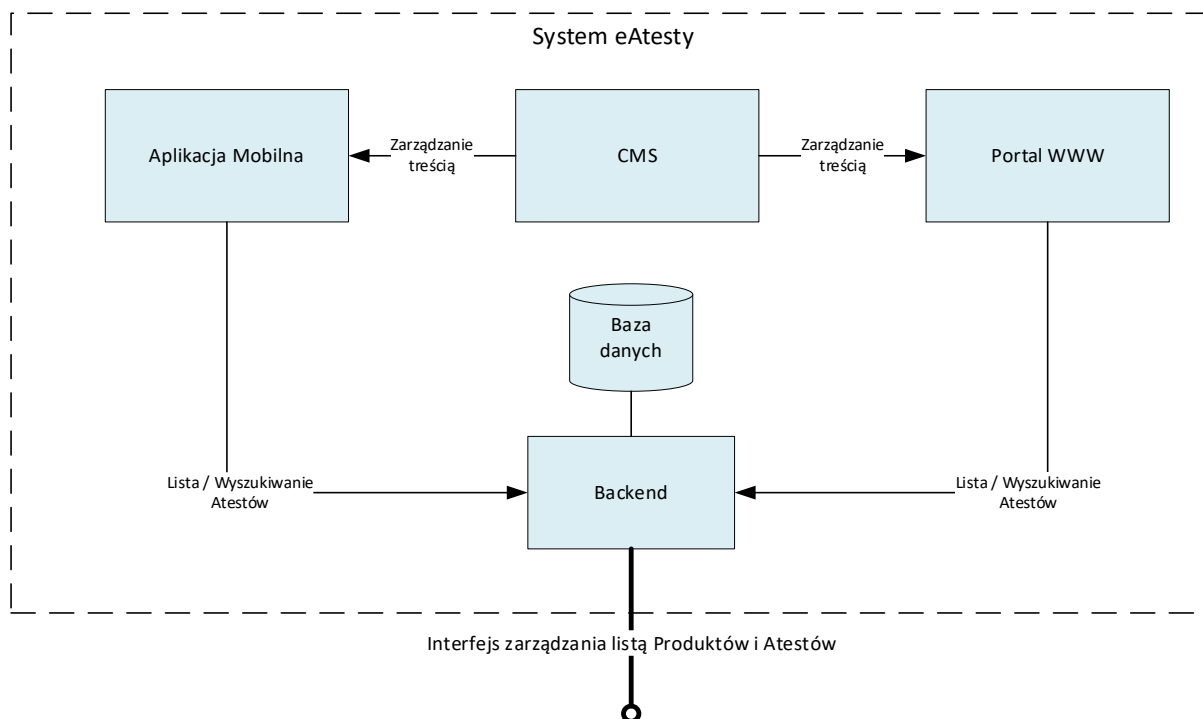
Etap 2 – Dostarczanie systemu e-ATESTY wraz z wymogiem okresowych odbiorów częściowych Systemu w postaci Wydań. Wykonawca powinien samodzielnie określić zakres i daty Wydań, które będą odbierane przez NIZP PZH-PIB.
Etap realizowany nie dłużej niż do dnia 13 października 2023 r.

Etap 3 – Stabilizacja Systemu e-Atesty – od zakończenia Etapu 2 do 15 listopada 2023 r.

3. Ogólna architektura Systemu e-ATESTY

Środowisko Systemu e-ATESTY zlokalizowane będzie w wydzielonej infrastrukturze NIZP PZH-PIB. Architekturę Systemu na ogólnym poziomie przedstawia poniższy schemat. Szczegółowy opis architektury musi zostać opracowany na etapie Projektu Technicznego.

Ogólna koncepcja architektury Systemu e-ATESTY



Elementy przedstawione na diagramie architektury to:

1. Aplikacja Mobilna – dostępna dla Użytkowników Zewnętrznych aplikacja dla konsumenta służąca do przeglądania i wyszukiwania Atestów produktów oraz pozyskiwania informacji na temat certyfikacji produktów.
2. Portal www – dostępny dla Użytkowników Zewnętrznych portal w przeglądarce internetowej służący do przeglądania i wyszukiwania Atestów produktów oraz pozyskiwania informacji na temat certyfikacji produktów.
3. CMS – system zarządzania treścią dla Portalu www oraz Aplikacji Mobilnej.
4. Baza danych – baza danych Produktów, obecnych i historycznych atestów oraz pozostałych danych przechowywanych w Systemie e-ATESTY.
5. Backend – ogólny komponent mający na celu zarządzanie warstwą biznesową Systemu e-ATESTY.
6. Interfejs zarządzania listą Produktów i Atestów – interfejs usługi sieciowej umożliwiający dodawanie, edytowanie, odczytywanie rekordów Produktów i Atestów z Bazy danych. Głównym celem interfejsu jest udostępnienie możliwości zasilania bazy danych Systemu e-ATESTY przez systemy NIZP PZH-PIB.

Aplikacja Mobilna i Portal www pokrywają się funkcjonalnościami z wyjątkami (wskazane w rozdziale *Wymagania dla Portalu WWW i Aplikacji Mobilnej*). Celem biznesowym Zamawiającego jest udostępnienie Systemu e-ATESTY zarówno w wersji w przeglądarce oraz dostępnej na urządzeniach mobilnych. Aplikacja Mobilna musi być możliwa do pobrania ze

sklepów platform Android i iOS. Dopuszczalne jest wykorzystanie technologii PWA (Progressive web application).

Szczegółowy zakres udostępnianych danych i usług oraz szczegółowy opis architektury Systemu powinien być przedmiotem Projektu Technicznego będącego częścią wdrożenia poszczególnych systemów.

Licencje

Zamawiający preferuje wykorzystanie licencji typu open-source w komponentach Systemu (systemy operacyjne, bazy danych, serwery WWW, platformy programistyczne, biblioteki itp.). W przypadku wyboru licencji płatnej Wykonawca zobowiązany jest udzielić Zamawiającemu licencji (permanentnej, nie jako subskrypcja) na dany komponent.

W przypadku, gdy to zasadne licencja powinna obowiązywać w oparciu o liczbę rdzeni procesora (CORE) minimum 16 rdzeni, z zastrzeżeniem, że Zamawiający udostępni środowisko zwirtualizowane, oparte o klastr składający się z 3 nodów, każdy po 2 procesory 16-rdzeniowe. Wykonawca dostarczy licencje umożliwiające instalację na maszynie wirtualnej udostępnionej na powyższym klastrze w sposób nienaruszający zasad licencyjnych, w szczególności dotyczących środowisk zwirtualizowanych. oraz umożliwi instalację dowolnej liczby instancji w ramach licencji udzielonej na daną liczbę rdzeni procesora (CORE).

Wykonawca przekaze autorskie prawa majątkowe w zakresie pól eksploatacji i na zasadach określonych w Umowie na Oprogramowanie wraz z kodami źródłowymi.

Dostarczane przez Wykonawcę licencje obejmują wszystkie komponenty i biblioteki Systemu, w tym stosowane przez Wykonawcę komponenty OpenSource i komponenty firm trzecich. Licencje muszą umożliwiać integrację z Nielimitowaną liczbą usług i systemów poprzez interfejsy integracyjne REST oraz połączenia ODBC/JDBS/ADO.NET.

System operacyjny

Oprogramowanie musi zostać zainstalowane na udostępnionej przez Zamawiającego platformie sprzętowo-programowej opartej o jeden ze wskazanych niżej systemów operacyjnych:

1. Linux – preferowany wybór Zamawiającego
2. Windows Server – Zamawiający posiada licencje na system operacyjny Windows Server

Wykorzystanie baz danych

W przypadku korzystania przez System z platformy bazy danych będzie ona oparta o jedną ze wskazanych niżej platform danych w wersji stabilnej i najbardziej aktualnej na dzień zawarcia Umowy:

1. MySQL,
2. Microsoft SQL Server,
3. PostgreSQL.

Wykorzystanie serwerów WWW

Dla elementów Systemu stosować można alternatywnie następujące serwery www w wersji stabilnej i najbardziej aktualnej na dzień zawarcia Umowy:

1. Nginx
2. WildFly,
3. Apache
4. Tomcat
5. IIS Microsoft,

Usługi sieciowe

Usługi sieciowe (Web Serwis) powinny być udostępniane w oparciu o udokumentowane interfejsy programistyczne REST API.

Metadane, będące parametrami wywołania lub rezultatem wywołania poszczególnych usług powinny być zapisywane w powszechnie stosowanym standardzie przeznaczonym do otwartych typów danych (np. JSON).

W poniższej tabeli zamieszczono listę standardowych usług charakterystycznych dla systemów integrowanych w NIZP PZH-PIB.

Id	Usługa	Charakterystyka i rezultat
U.BO.1	getBusinessObject(ObjectId): Data	Usługa pozwalająca na pobranie danych obiektu biznesowego o zadanym identyfikatorze. Parametrem wywołania jest identyfikator obiektu, opcjonalnie wersja obiektu. Rezultatem są metadane zawierające opis obiektu w tym, jeśli obiekt biznesowy reprezentuje fizyczny plik, dynamicznie generowany adres URL pozwalający na pobranie pliku w ramach aktywnej sesji.
U.BO.2	putBusinessObject(Data): ObjectID	Usługa pozwalająca na aktualizację obiektu biznesowego. Parametrami wywołania są metadane obiektu, rezultatem – identyfikator obiektu w systemie docelowym lub kod błędu.

U.BO.3	deleteBusinessObject(ID):result	Usługa pozwalająca na usunięcie obiektu biznesowego z systemu.
U.BO.4	getObjectList(ObjectId, Type): Data	Usługa pozwalająca na pobranie listy obiektów biznesowych powiązanych z obiektem o zadanym identyfikatorze relacją zadanego typu.

4. Wymagania dla Systemu e-ATESTY

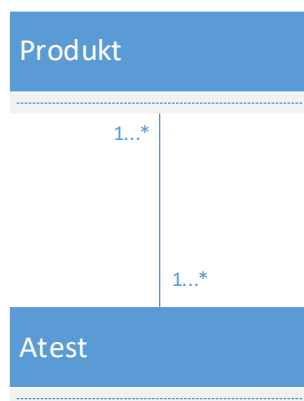
System e-ATESTY powinien spełniać poniższe wymagania:

1. **Modułowość** pozwalająca na wyłączenie bądź zastąpienie poszczególnych modułów Systemu bez utraty integralności danych oraz w sposób zapewniający poprawność działania pozostałych modułów Systemu.
2. **Trójwarstwowa architektura** z wydzieloną warstwą interfejsu użytkownika (frontend), warstwą logiki biznesowej (middleware) i warstwą danych (database).
3. **Udokumentowane interfejsy programistyczne (API)** pozwalające na integrację przez niezależnych dostawców (integratorów).
4. **Udokumentowana struktura bazy danych** pozwalająca na dostęp do danych przechowywanych w warstwie bazodanowej na potrzeby ich wirtualizacji i wykorzystania przez systemy zewnętrzne.
5. **Interfejs webowy** w języku polskim i angielskim pozwalający na dostęp przez najbardziej popularne przeglądarki internetowe (Microsoft Edge, Chrome, Mozilla Firefox, Opera, Safari) spełniający wymagania zgodnie z zapisami Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Dostęp realizowany przez szyfrowane połączenie HTTPS zabezpieczony powszechnie rozpoznawalnym certyfikatem SSL.
6. **Interfejs mobilny** realizowany przez dedykowaną aplikację dla systemów Android i iOS dla Aplikacji Mobilnej i przynajmniej webowy interfejs responsywny dla pozostałych elementów Systemu. Zamawiający dopuszcza wdrożenie aplikacji typu PWA w celu realizacji interfejsu mobilnego.
7. **Responsywność** – System musi być responsywny, a więc taki która dostosowuje swoją zawartość do urządzenia na której jest wyświetlany, ze szczególnym uwzględnieniem rozdzielczości ekranów urządzeń mobilnych (smartfonów i tabletów).
8. **Interfejs GUI** Systemu musi być w polskiej i angielskiej wersji językowej.
9. **Autentykacja** w pomiędzy Systemem a serwerami danych i usług zapleczka powinna odbywać się w sposób zapewniający bezpieczny delegowany dostęp zgodnie ze standardem OAuth w wersji 2.0 lub równoważnym dla wybranej technologii.
10. **Dostępność** - Muszą być spełnione wymagania dostępności cyfrowej dla Systemu e-ATESTY, zapisane w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (tj. Dz.U. 2023 poz. 82),
11. **Standardy** - wykonanie Systemu zgodnie z najnowszymi standardami, które wyznacza W3C.
12. **Bezpieczeństwo** – System musi spełniać standardy bezpieczeństwa (zgodnie z zał. 2 OPZ). W jego budowie nie mogą występować wady i podatności aplikacji webowych opisane w aktualnej wersji standardu OWASP TOP TEN (<https://www.owasp.org>).
13. **SLA** – dostarczony System powinien być objęty umową SLA. Zakres SLA opisany w rozdziale Asysta i Konserwacja Techniczna.
14. **Kopie zapasowe** zapewnienie przez Wykonawcę rozwiązania pozwalającego na tworzenie kopii zapasowych danych gromadzonych w Systemie z wykorzystaniem istniejącego u Zamawiającego narzędzia Veeam Enterprise Edition. Rozwiązanie powinno realizować następujące wymagania:

- a. możliwość zabezpieczenia danych przed ich celowym lub przypadkowym usunięciem
- b. zarządzanie kopiami zapasowymi z poziomu konsoli fizycznej (wiersz polecenia) oraz poprzez graficzny interfejs
- c. możliwość odtworzenia Systemu lub jego elementów po błędach.
- d. wykonywanie kopii zapasowych plików konfiguracyjnych, logów systemowych oraz dzienników zdarzeń.
- e. w ramach Dokumentacji Administratora, Wykonawca opracuje i przekaze instrukcję odtwarzania Systemu lub jego części na podstawie kopii zapasowych. W Dokumentacji Technicznej powinien znaleźć się proces tworzenia kopii zapasowych.
- f. podczas wykonywania kopii zapasowej będą tworzone każdorazowo po dwie kopie, które będą przechowywane w miejscach wskazanych przez Zamawiającego, w miejscu bezpiecznym, zapewniającym ochronę przed dostępem osób nieuprawnionych, modyfikacją, uszkodzeniem, zniszczeniem oraz wpływem środowiska.
- g. kopie zapasowe Systemu należy tworzyć przynajmniej w następującym cyklu:
 - pełny backup - raz w tygodniu
 - backup przyrostowy lub różnicowy – raz dziennie;
- h. kopie zapasowe powinny być zabezpieczone przed nieuprawnionym dostępem.
- i. okres przechowywania kopi zapasowych wynosi 3 miesiące od wytworzenia. Po ustaniu użyteczności kopii zapasowych są one usuwane. Po upływie okresu przechowywania nośnik może być wykorzystany ponownie po wcześniejszym upewnieniu się, iż wcześniejsze dane zostały w sposób trwały usunięte. Wykorzystując ponownie ten sam nośnik należy bezwzględnie weryfikować poprawność zapisu i możliwość odczytania jego zawartości. Za procedurę tworzenia kopii zapasowych i wady kopii zapasowych powstałe na skutek błędnej procedury, Wykonawca ponosi odpowiedzialność na zasadzie ryzyka.
- j. Wykonawca określi procedury wykonywania i odtwarzania kopii zapasowych. Zamawiający zgodnie z przekazaną Dokumentacją Administratora będzie wykonywał kopie zapasowe oraz okresowo sprawdzał poprawność wykonania kopii zapasowych.

Główne obiekty danych w Systemie

Poniższy diagram przedstawia główne obiekty danych przetwarzane w Systemie.



W Systemie występują dwa główne obiekty danych:

1. **Produkt**
2. **Atest**

Dla obiektów danych należy przyjąć następujące założenia:

3. Produkt może mieć wystawiony minimum jeden a maksymalnie wiele Atestów zarówno aktualnych jak i nieaktualnych.
1. Każdy Atest zostaje wydany dla minimum jednego do maksymalnie wielu Produktów.
2. Produkt nie pojawi się w bazie danych jeśli nie został wystawiony dla niego Atest. Tzn. nie będzie możliwości wyszukania Produktu bez przypisanego Atestu. Zawsze będzie to co najmniej jeden aktywny bądź nieaktywny Atest.
3. W Systemie wyszukujemy Produkty zarówno po danych Produktu jak i danych wystawionych dla niego Atestów. Wymagania funkcjonalne opisują dokładniej funkcję wyszukiwania.
4. Na etapie prac projektowych Zamawiający przekaże Wykonawcy listę przykładowych produktów oraz atestów (z kompletem metadanych ich opisujących) w celu wykonania poprawnego modelu danych
5. Obiekt Produktu jest zbudowany z około 15 (nie więcej niż 25) parametrów/pól różnego typu (liczba, ciąg znaków, data, data i czas, prawda/fałsz), w tym pola słownikowe i tabele (z pominięciem danych systemowych np. osoba/system dodający, data dodania do rejestru, data aktualizacji, osoba/system aktualizujący itp.)
6. Obiekt Atestu jest zbudowany z około 15 (nie więcej niż 25) parametrów/pól różnego typu (liczba, ciąg znaków, data, data i czas, prawda/fałsz), w tym pola słownikowe i tabele (z pominięciem danych systemowych np. osoba/system dodający, data dodania do rejestru, data aktualizacji, osoba/system aktualizujący itp.)

5. Wymagania dla Portalu WWW i Aplikacji Mobilnej

Z uwagi na fakt, że wymagania do Portalu WWW i Aplikacji Mobilnej są w większości tożsame zostały one umieszczone w jednym rozdziale. Specyficzne wymagania dla Portalu WWW i Aplikacji Mobilnej zostały umieszczone w odpowiednich sekcjach na liście wymagań poniżej.

Id wymagania	Treść wymagania
Ogólne	
WF.1	Możliwość wyświetlania treści w orientacji poziomej i pionowej preferowanej przez użytkownika.
WF.2	Dostępna „Deklaracja dostępności” zgodnie z WCAG 2.1.AA
WF.3	Wymagane rozróżnienie spośród Atestów - Atestów Higienicznych lub Świadectw Jakości Zdrowotnej. Wykonawca musi zastosować prawidłową nazwę przy dokumencie danego typu. Jeśli treść dotyczy zarówno Atestów Higienicznych jak i Świadectw Jakości Zdrowotnej powinien zostać zastosowany zapis typu „Atest / Świadectwo”
WF.4	System musi zawierać następujące strony/komponenty stron przygotowane przez Wykonawcę w projekcie graficznym, zaakceptowane przez Zamawiającego a następnie wdrożone w Systemie: <ol style="list-style-type: none"> 1. Strona główna 2. Menu/nawigacja strony 3. Stopka strony 4. Wyszukiwarka Produktów 5. Wyszukiwarka Atestów 6. Wyszukiwarka treści (poszczególne pola Atestów) 7. Instrukcja korzystania z Systemu 8. Strona z przykładowymi artykułami/publikacjami 9. Odwołanie do strony głównej atestacji PZH (https://www.pzh.gov.pl/uslugi/atestacja-atestation/) 10. Najczęściej zadawane pytania FAQ Wskazane powyżej strony za wyjątkiem wyszukiwarek produktów i atestów muszą być możliwe do edycji w systemie CMS.
WF.5	Przygotowana lista najczęstszych pytań z możliwością jej rozbudowy w systemie CMS
WF.6	Przygotowanie pomocy kontekstowej i odpowiedzi dla Konsumenta, w Aplikacji Mobilnej i Portalu www, dotyczącej poprawnej obsługi systemu, z możliwością edycji treści przez Użytkownika Wewnętrznego.
WF.7	Przygotowanie strony, która będzie instrukcją użytkownika Systemu e-ATESTY przeznaczoną dla Konsumenta.
WF.8	Konsument musi mieć możliwość zgłoszenia problemów, błędów występujących w Systemie bądź usprawnień. W tym celu w Systemie powinien znaleźć się odpowiedni formularz kontaktowy.
Wyszukiwanie Produktów	

WF.9	Możliwość przeszukiwania Produktów z wykorzystaniem wyszukiwania pełnotekstowego (np. wyszukiwanie naturalne) oraz wyszukiwania wieloznacznego.
a.	Wyszukiwanie (produktów lub atestów) powinno zostać zrealizowane za pomocą pojedynczego pola, gdzie użytkownik może wpisać dowolną ilość wyrazów.
b.	Każdy z wyrazów powinien brać udział w wyszukiwaniu rozdzielnie w każdym z pól/parametrów produktu i atestu.
c.	Wyniki wyszukiwania powinny być zaprezentowane w następującej kolejności (najbardziej dopasowany trafny rezultat wynik u góry) według największej ilości punktów zgromadzonych w wyszukiwaniu.
d.	Należy przyjąć taką punktację: <ul style="list-style-type: none"> - dopasowano numer atestu (10pkt.) - znaleziono wyraz/wyrazy w nazwie produktu (5pkt.) - znaleziono wyraz/wyrazy w nazwie producenta (4pkt.) - znaleziono wyraz/wyrazy w nazwie dystrybutora(3pkt.) - znaleziono wyraz/wyrazy w nazwie wnioskodawcy(2pkt.) - znaleziono wyraz/wyrazy w składzie produktu(1pkt.) W/w punktacja (dla poszczególnych pól) powinny być edytowalne minimum na poziomie bazy danych. Wyszukiwanie powinno się odbywać także po fragmencie wyrazów.
e.	Wymagania zdefiniowane w punktach WF.9: a, b, c oraz d są jedynie propozycją Zamawiającego, jednak Wykonawca może zaproponować inne rozwiązanie, które spełni potrzeby Zamawiającego pod względem ergonomii oraz UX użytkownika.
WF.10	Wyszukiwanie Produktu powinno uwzględniać następujące atrybuty Produktu: <ol style="list-style-type: none"> 1. nazwa wyrobu/produktu 2. nazwa producenta (czasem stosowany jest zapis np. "Wyprodukowano w Chinach/UE dla...") 3. nazwa Wnioskodawcy 4. numer kodu kreskowego Produktu (tam, gdzie dostępne) 5. skład chemiczny Produktu (na podstawie numerów CAS i nazw związków chemicznych/nazw materiałów) 6. zakres zastosowania 7. Dane dystrybutora (tam, gdzie dostępne)
WF.11	Wyszukiwanie Produktu powinno uwzględniać następujące atrybuty wystawionych dla niego Atestów: <ol style="list-style-type: none"> 1. Typ (Atest/Świadectwo) 2. numer Atestu 3. dane podmiotu (wnioskodawcy, producenta i dystrybutora), dla którego został wydany Atest 4. zakres stosowania 5. zastrzeżenia wyrobu/produktu
WF.12	Wyszukiwarka musi wspierać autouzupelnianie wpisywanej wyszukiwanej frazy (na podstawie danych w bazie eAtesty dla danego pola/parametru lub

	na podstawie rzeczowników w języku polskim i angielskim). Szczegółowe wymagania jaki mechanizm przyjęć do poszczególnych pól zostanie określony na etapie analizy technicznej z Wykonawcą.
WF.13	Wyszukiwarka wykrywa błędy polegające na pomyłkowej zamianie pojedynczych liter („literówki”) i dokonuje ich korekcji lub ostrzega o możliwym błędzie (na podstawie danych w bazie eAtesty dla danego pola/parametru lub na podstawie rzeczowników w języku polskim i angielskim). Szczegółowe wymagania jaki mechanizm przyjęć do poszczególnych pól zostanie określony na etapie analizy technicznej z Wykonawcą.
a.	Ze względu na wymagania WF.12 oraz WF.13 system powinien posiadać listę wszystkich unikalnych wyrazów przechowywanych w systemie w różnych polach (produkty, atesty) dostosowane do jednego formatu (np. wszystkie litery wielkie, brak białych znaków).
b.	Wykonawca musi przyjąć założenie, że wiele z pól w systemie będzie posiadało wiele wartości (wyrazów), które trzeba porozdzielać i zapisać jako osobne wyrazy w bazie (np. po znakach interpunkcyjnych, białych znakach, znakach specjalnych itp.).
c.	Wymagania zdefiniowane w punktach WF.13 a oraz b są jedynie propozycją Zamawiającego ze względu na przyszłą wydajność systemu, jednak Wykonawca może zaproponować inne rozwiązanie, które zaoferuje podobną lub lepszą wydajność.
WF.14	Wyszukiwarka pozwala na poprawne wyszukiwanie informacji, nawet jeśli wyszukiwany tekst został wpisany bez polskich znaków diakrytycznych.
WF.15	Możliwość filtrowania wyników wyszukiwania Produktu po następujących atrybutach: <ol style="list-style-type: none"> 1. grupy produktowe 2. data wydania Atestu 3. data ważności Atestu 4. producent 5. Wnioskodawca/dystrybutor 6. składzie chemicznym – numer CAS, nazwa związku chemicznego
WF.16	Możliwość sortowania wyników po: <ol style="list-style-type: none"> 1. grupy produktowe 2. data wydania Atestu 3. data ważności Atestu 4. producent 5. Wnioskodawca/dystrybutor <p>Wybór odpowiedniego sortowania powinien grupować podobne wyniki wyszukiwania.</p> <p>System musi pozwalać użytkownikowi na sortowanie danych dowolnego wymiaru w porządku rosnącym lub malejącym. W tabelach/listach proces wyszukiwania/filtrowania oraz sortowania musi się odbywać na całym zbiorze danych, a nie jedynie w obrębie jednej strony danych.</p>

WF.17	Wyszukiwanie powinno zwracać domyślnie najbardziej dopasowany wynik na bazie zgromadzonych danych o wyszukiwaniach.
WF.18	Możliwość wyszukania Produktu poprzez skanowanie kodu kreskowego produktu w aplikacji na urządzeniach mobilnych.
WF.19	Po każdej próbie wyszukiwania zakończonej brakiem wyników, powinien wyświetlać się komunikat typu „Spróbuj wyszukać produkt wskazując inne parametry wyszukiwania”.
Wyświetlanie Produktów i Atestów	
WF.20	<p>Konsument po wyszukaniu odpowiedniego Produktu powinien mieć możliwość wyświetlenia szczegółowych danych na temat tego Produktu. Wyświetlane dane (o ile nie są zastrzeżone):</p> <ol style="list-style-type: none"> 1. nazwa Produktu 2. grupa produktowa 3. nazwa Producenta (czasem stosowany jest zapis np. "Wyprodukowano w Chinach/UE dla...") 4. numer kodu kreskowego Produktu 5. skład chemiczny/materiałowy Produktu – składa się z numeru CAS, nazwy związku chemicznego, wartości % związku w składzie wyrobu. 6. lista aktualnych i nieaktualnych Atestów Produktu. Domyślnie najpierw aktualne Atesty sortowane po dacie wydania malejąco. Informacje, które mają zostać wyświetlone na Ateście będącym na liście: <ol style="list-style-type: none"> a. Typ (Atest/Świadectwo) i numer Atestu b. Informacja o aktualności wraz z informacją do kiedy Atest jest aktualny lub nieaktualności c. Data wydania d. Data ważności e. Dokument Atestu do podglądu i pobrania (w przypadku zgody na udostępnienie przez Przedsiębiorcę) f. Przejście do szczegółowego widoku Atestu
WF.21	<p>Konsument po wyszukaniu odpowiedniego Produktu powinien mieć możliwość wyświetlenia szczegółowych danych na temat Atestu tego Produktu Wyświetlane dane (o ile nie są zastrzeżone):</p> <ol style="list-style-type: none"> 1. numer Atestu, 2. typ Atestu (Atest/Świadectwo) 3. status Atestu 4. data wydania Atestu, 5. datę ważności Atestu, 6. dane podmiotu, dla którego został wydany Atest, 7. przeznaczenie / zakres stosowania 8. zastrzeżenia wyrobu/produktu, 9. dokument Atestu do podglądu i pobrania (w przypadku zgody na udostępnienie przez Przedsiębiorcę) 10. atestowane Produkty

WF.22	<p>Widok listy produktów z ostatnio wydanymi Atestami. W widoku powinno zostać uwzględnione, które Produkty zostały objęte Atestem oraz podstawowe dane Atestu:</p> <ol style="list-style-type: none"> 1. Typ (Atest/Świadczenie) i numer Atestu 2. Data wydania 3. Data ważności 4. atestowane Produkty 5. Dokument Atestu do podglądu i pobrania (w przypadku zgody na udostępnienie przez Przedsiębiorcę) 6. Przejście do szczegółowego widoku Atestu
WF.23	Każda lista/tabela obiektów, których liczba może przekroczyć 50 powinna posiadać mechanizm stronicowania.
WF.24	Użytkownik powinien mieć możliwość wyboru ilości elementów na stronie
WF.25	Użytkownik powinien mieć możliwość przejścia na konkretną stronę z zachowaniem aktualnego filtrowania i sortowania
Statystyki	
WF.26	<p>Aplikacja powinna zbierać i zapisywać dane na temat wyszukiwanych przez Konsumentów Produktów, takie jak:</p> <ol style="list-style-type: none"> 1. częstotliwość wyszukiwania danego Produktu 2. najczęściej wyszukiwane frazy 3. wyszukiwania zakończone brakiem wyniku 4. liczba i częstotliwość pobierania Atestów 5. stosowane w wyszukiwaniach filtry i sortowania

6. Wymagania dla systemu Content Management System (CMS)

System Zarządzania Treścią (CMS – system zarządzania treścią dla Portalu www oraz Aplikacji Mobilnej. System CMS preferowany przez Zamawiającego to Wordpress w wersji open-source (<https://pl.wordpress.org/>). System CMS, w przypadku korzystania z dodatkowych wtyczek do stworzenia systemu i spełnienia poniższych wymagań, musi mieć zakupione do nich licencje wg zasad z rozdziału **LICENCJE**.

W przypadku wyboru innego systemu niż Wordpress Wykonawca musi uzasadnić wybór alternatywnego rozwiązania, którego funkcjonalność jest co najmniej równoważna i spełnia poniższe wymagania.

Id wymagania	Treść wymagania
Ogólne	
CMS.1	System powinien umożliwiać jednoczesną pracę dla minimum 50 Użytkowników Wewnętrznych.
CMS.2	Możliwość ograniczenia dostępu do CMS dla konkretnych adresów IP.
CMS.3	System CMS wyłączony z wyszukiwania w wyszukiwarkach internetowych.
CMS.4	Możliwość prowadzenia statystyk, tj. ogólnej liczby odwiedzin, liczby unikatowych odwiedzin, najczęściej odwiedzanych stron Systemu, źródła odwiedzin (kraj, miasto, region itp.) za pomocą ogólnodostępnych narzędzi, typu Google Analytics, bądź równoważnych, oraz wyświetlania statystyk w systemie CMS.
Administracyjne	
CMS.5	System CMS musi umożliwiać zarządzanie zespołem redakcyjnym strony poprzez (konta, role, uprawnienia). Powinien uwzględniać minimum 2 role użytkowników: <ol style="list-style-type: none"> Administrator IT – dostęp do wszystkich funkcji systemu Redaktor – dostęp do tworzenia, edycji i wyświetlania treści ograniczonych uprawnieniami przez Administratora IT.
CMS.6	Autoryzacja administratora i redaktorów przy pomocy loginu i hasła.
CMS.7	System CMS musi zapewniać dalszy jego rozwój poprzez instalację dodatkowych modułów (Opensource lub dedykowanych do danego systemu CMS).
Zarządzanie treścią	
CMS.8	Kształtowanie treści i sposobu ich prezentacji w serwisie internetowym zarządzanym przez CMS odbywa się za pomocą prostych w obsłudze interfejsów użytkownika bez konieczności pracy na otwartym kodzie HTML i nie wymagające znajomości HTML.
CMS.9	Możliwość tworzenia treści w postaci: <ol style="list-style-type: none"> stron wraz z możliwością nadawania im unikalnych adresów URL, artykułów wraz z możliwością nadawania im unikalnych adresów URL oraz kategorii.

CMS.10	Przeptyw pracy nad stroną/artkułem ze statusami: w edycji, weryfikacja, zatwierdzony, opublikowany, z terminem publikacji, ukryty.
CMS.11	Wersjonowanie edycji stron/artkułów.
CMS.12	Możliwość ustalenia daty publikacji strony/artkułu.
CMS.13	Pod każdą treścią (strona, artykuł) musi być możliwość zamieszczenia przycisków/wtyczek udostępnienia treści do portali społecznościowych (facebook, linkedIn, twitter)
CMS.14	System CMS musi zawierać intuicyjny kreator treści pozwalający na bezpośrednie przeciąganie i upuszczanie komponentów do zdefiniowanych przez użytkownika bloków. Kreator musi zawierać następujące możliwości tworzenia nowych komponentów w ramach stron i artykułów: <ol style="list-style-type: none"> 1. siatka bloków zawierająca od 1 do 12 bloków 2. nagłówek generujący nagłówki od H1 do H6 3. tekst pozwalający na utworzenie bloku tekstowego przy pomocy edytora tekstu 4. obraz pozwalający na umieszczenie grafiki z galerii 5. galerii pozwalający na umieszczanie galerii obrazów 6. filmowy pozwalający na umieszczanie filmów bezpośrednio z co najmniej serwisów Youtube i Vimeo 7. mapy pozwalający na wyświetlanie map i umieszczanie znaczników z serwisów takich jak Google Maps 8. formularzy pozwalający na utworzenie i umieszczenie zdefiniowanych formularzy 9. linki zarówno dla wewnętrznych stron systemu jak i zewnętrznych stron 10. Pliki do pobrania 11. kod osadzony / niestandardowy (embedded / custom code) <p>Treść stron nie powinna być ograniczona co do ilości i rodzaju możliwych do wstawienia w niej komponentów.</p>
CMS.15	Edytor tekstu w kreatorze treści powinien mieć możliwość jego formatowania w zakresie: struktury, czcionki, stylu, koloru, list, nagłówek, edycji linków, wstawiania tabel. Sposób tworzenia treści musi pozwalać użytkownikowi zobaczyć na ekranie dokładnie to, co później zostanie przedstawione na stronie/artkule w Systemie.
CMS.16	Kreator treści musi posiadać wbudowaną funkcjonalność podglądu tworzonej strony/artkułu na komputerze, tablecie, telefonie komórkowym
CMS.17	Udostępnianie materiałów znajdujących się w CMS zarówno w przeglądarce internetowej (Portal www) jak i w Aplikacji Mobilnej.
CMS.18	Możliwość wersjonowania komponentów domyślnie w minimum dwóch wersjach językowych – polski, angielski wraz z możliwością dodania kolejnych wersji językowych.
CMS.19	Zarządzanie widocznością komponentów na poszczególnych stronach.
CMS.20	Możliwość dołączania na stronach plików do pobrania oraz dostęp do plików umieszczanych na stronie serwisu tj. możliwość podmiany lub dodawania nowych plików.
CMS.21	Możliwość definiowania i modyfikacji Deklaracji dostępności.

CMS.22	Repozytorium plików i elementów multimedialnych z możliwością dodania ich na stronę/artkuł lub podmiany już umieszczonych na stronie/artkule.
CMS.23	Tworzenie i zarządzanie nawigacją strony (menu, podmenu, stopka, min. do 3 poziomów)
CMS.24	Możliwość tworzenia i edycji komponentów wielokrotnego użytku, które zdefiniowane raz mogą być użyte wielokrotnie.
CMS.25	Możliwość zaawansowanej edycji komponentów CMS z wykorzystaniem: <ol style="list-style-type: none"> 1. HTML dla komponentów 2. CSS dla stylów komponentów 3. JavaScript dla skryptów
CMS.26	Możliwość wprowadzenia odpowiednich metadanych i wartości dla każdego z typów komponentów, aby spełnić wymagania WCAG 2.1.
CMS.27	Możliwość zdefiniowania wykonywanej akcji po zaakceptowaniu formularza w postaci: <ol style="list-style-type: none"> 1. wywołania skryptu, który pozwoli na przekazanie danych z pól formularza na zewnętrzne serwery w postaci zapytania http / webhook 2. informacji o poprawnym wypełnieniu formularza 3. informacji o niepoprawnym wypełnieniu formularza
CMS.28	Definiowanie formularzy musi umożliwiać dodanie CAPTCHA
Adresy URL	
CMS.29	Zarządzanie adresami URL stron i artykułów z możliwością zdefiniowania maski adresu URL dla stron i artykułów.
CMS.30	Zapewnienie unikalności wewnętrznych adresów URL.
CMS.31	Edycja istniejącego adresu URL powinna powodować jego aktualizację w komponentach w zakresie treści w CMS.
CMS.32	Wewnętrzne adresy URL powinny się podpowiadać w trakcie tworzenia lub edycji komponentu typu link.
Wyszukiwanie	
CMS.33	Możliwość uruchomienia funkcjonalności wyszukiwania na stronie internetowej. Wyszukiwarka na podstawie wyszukiwanej frazy musi zwracać w postaci listy pasujące strony i artykuły.
CMS.34	Możliwość edycji treści i wyglądu wyszukiwarki oraz listy wyszukanych stron i artykułów.
CMS.35	Wyszukiwarka musi mieć możliwość wyszukiwania po tytułach stron i artykułów oraz w treści stron i artykułów.
CMS.36	Wyszukiwanie powinno być również możliwe dla Użytkowników Wewnętrznych w ramach prac edycyjnych w systemie CMS.

7. Pozostałe wymagania administracyjne

Wymagania administracyjne, które mogą być wykonywane przez komponent Backend bądź inne Oprogramowanie.

Interfejsy programistyczne	
PA.1	<p>Przygotowanie interfejsów programistycznych umożliwiających zarządzanie (dodawanie, aktualizacja, usuwanie) bazą Produktów oraz wystawionych dla nich Atestów w celu zasilania Bazy danych Systemu e-ATESTY. Szczegółowy zakres interfejsów programistycznych umożliwiający efektywne zarządzanie listą powinien być elementem Projektu Technicznego.</p> <p>Dodatkowo system musi posiadać interfejsy API umożliwiające dla:</p> <ul style="list-style-type: none"> - pobieranie danych produktów - wyszukiwania produktów - wyszukiwania atestów - pobieranie listy atestów dla produktu - pobieranie danych atestu (po id oraz numerze atestu)
PA.2	<p>W ramach dostępu do listy Produktów musi zostać przygotowany również dostęp do zbieranych statystyk odnośnie Produktów i Atestów wskazanych w wymaganiu WF.26.</p>
Monitorowanie komunikatów, logów, usług sieciowych	
PA.3	<p>Komunikaty oraz logi systemowe muszą umożliwić Zamawiającemu przede wszystkim identyfikację i naprawę błędów dotyczących wydajności i bezpieczeństwa Systemu oraz monitorować aktywność w Systemie. Ponadto zgodnie z regulacjami wprowadzanymi przez ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, logi muszą umożliwiać identyfikowanie incydentów bezpieczeństwa oraz klasyfikację tych incydentów na podstawie:</p> <ul style="list-style-type: none"> • liczby użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług • czas trwania incydentu • zasięg geograficzny obszaru, którego dotyczy incydent • zakres zakłócenia funkcjonowania usługi • zakres wpływu incydentu na działalność gospodarczą i społeczną
PA.4	<p>Logowanie żądań przychodzących i wychodzących z Systemu oraz odpowiedzi do żądań. Mechanizm umożliwiający trwale zapisywanie wszystkich lub wybranych logów.</p>

PA.5	Obsługa logów, wyszukiwanie wg ustalonego kryterium, prezentacja rezultatów wyszukiwania w przejrzysty sposób.
PA.6	System umożliwia monitorowanie, powiadamianie i raportowanie incydentów zachodzących w Systemie.
PA.7	System posiada mechanizm audytowania zdarzeń, zapewnia logowanie wszystkich informacji z działalności Użytkowników Wewnętrznych i Zewnętrznych ze szczególnym uwzględnieniem dostępu do danych wrażliwych oraz umożliwia przygotowanie raportów w celu przeprowadzania audytów dotyczących danych wrażliwych.
Logi audytu	
PA.8	System musi posiadać rejestry audytowe, umożliwiać ich przeglądanie, sortowanie, filtrowanie, wyszukiwanie danych po dowolnych polach, eksport logów w formacie SysLog.
PA.9	System musi zawierać mechanizm do przeglądania logów bieżących (wstępnie wszystkie do 6 miesięcy; okres ustawiany parametrem) i archiwalnych (wstępnie wszystkie powyżej 6 miesięcy; okres ustawiany parametrem) w tym zapewniający możliwość: <ol style="list-style-type: none"> 1. wyszukiwania 2. filtrowania po wybranych przez Użytkownika typach zdarzeń i ich cechach. 3. sortowania po wybranych przez Użytkownika typach zdarzeń i ich cechach. oraz musi zapewnić mechanizm eksportu pliku logów do serwera zewnętrznego przy użyciu standardowych protokołów i mieć możliwość synchronizacji z serwerem czasu (protokół NTP).
PA.10	W zakresie przeglądania logów musi być możliwość dostępu co najmniej do następujących danych: <ol style="list-style-type: none"> 1. Historii zmian uprawnień Użytkowników (z dokładnością do roli): login, nazwisko, imię, komórka organizacyjna, rola, data nadania roli, data odebrania roli. 2. Historia Lista sesji Użytkowników: zawierać będzie listę wszystkich sesji Użytkowników, wraz z informacjami: login, nazwisko, imię, jednostka, komórka organizacyjna, data i godzina początku sesji, data i godzina zakończenia sesji (jeżeli sesja już została zakończona), adresie IP komputera, na którym powstała sesja. 3. Listy otwartych sesji: Login, nazwisko, imię, jednostka, komórka organizacyjna, data /godzina początku sesji (musi być możliwość wylogowania wszystkich Użytkowników). 4. Historii logowań: login, nazwisko, imię, komórka organizacyjna, data i godzina zalogowania, data i godzina wylogowania, czas logowania. 5. Kont Użytkowników Systemu: login, nazwisko, imię, komórka organizacyjna, data założenia konta, data dezaktywacji konta, czy aktywne, data ostatniego logowania.

	<p>6. Historii zmian dotyczących kont Użytkowników: zawiera wszystkie atrybuty konta Użytkownika (login, nazwisko, imię, komórka organizacyjna, data założenia konta, data zablokowania konta, czy aktywne) oraz powiązań konta Użytkownika z innymi obiektami (np. uprawnienia, sesje), wraz z datą i godziną zmiany oraz informacją o tym kto zmianę wykonał.</p> <p>7. Listy aktywnych Użytkowników wraz z przypisanymi rolami (imię, nazwisko, login, komórka organizacyjna, rola).</p> <p>8. Listy osób, które w zadanym okresie miały nadane uprawnienia, przy czym powinna być możliwość wyszukiwania po parametrach:</p> <ul style="list-style-type: none"> • okres (od, do) wraz z możliwością wyszukania listy osób, które miały nadane uprawnienia przez cały okres jak i w jego fragmencie, • rola (możliwe zaznaczenie kilku), • Lista osób powinna zawierać następujące informacje: login, nazwisko, imię, data nadania uprawnienia, data odebrania uprawnienia. <p>Zakres powyższych logów powinien zostać ostatecznie przedstawiony i uzgodniony z Zamawiającym.</p>
PA.11	<p>Wszystkie wskazane powyżej widoki muszą posiadać:</p> <ol style="list-style-type: none"> 1. nagłówek zawierający tytuł raportu. 2. zadane parametry wyszukiwania dla których został wygenerowany raport. 3. część zasadniczą z wygenerowanymi danymi wraz z nagłówkami kolumn. 4. możliwość wyszukiwania. 5. możliwość filtrowania po wybranych przez Użytkownika wartościach. 6. możliwość sortowania po wybranych przez Użytkownika wartościach.
PA.12	<p>W Systemie muszą być rejestrowane działania Użytkowników oraz zdarzenia związane z bezpieczeństwem informacji. Dane te muszą być przechowywane przez określony przez Zamawiającego czas dla potrzeb przyszłych postępowań wyjaśniających oraz monitorowania kontroli dostępu. Logi bieżące mają być przechowywane w Systemie, natomiast kwestie związane z przechowywaniem logów archiwalnych zostaną omówione na etapie Projektu Technicznego</p>
PA.13	<p>W Systemie muszą być logowane zdarzenia z dokładnością do każdego parametru określonego w PA.10. Komunikaty zdarzeń muszą być opisane w sposób czytelny dla użytkownika.</p>
PA.14	<p>W Systemie muszą być rejestrowane działania Użytkowników oraz zdarzenia związane z bezpieczeństwem informacji. Dane te muszą być przechowywane przez określony przez Zamawiającego czas dla potrzeb przyszłych postępowań wyjaśniających oraz monitorowania kontroli</p>

	dostępu. Logi bieżące mają być przechowywane w Systemie, natomiast kwestie związane z przechowywaniem logów archiwalnych zostaną omówione na etapie Projektu Technicznego.
PA.15	W przypadku, gdy w Aplikacji jest realizowany interfejs integracyjny obligatoryjne jest odnotowywanie działań związanych z uruchamianiem funkcji interfejsu integracyjnego wraz z możliwością włączenia powiadamiania mailowego o błędach.
PA.16	System musi umożliwiać eksport wyników wyszukiwania logów do plików formatu np. xlsx, csv w zależności od zapotrzebowania Użytkownika.
PA.17	W Systemie konieczne jest przygotowywanie raportu dostępu do danych osobowych zgodnie z obowiązującymi regulacjami prawnymi.

8. Projekt Techniczny

Projekt techniczny zawierający w szczególności:

1. Zdalne dostępy do systemów i baz danych Zamawiającego w tym środowiska testowego oraz produkcyjnego za pośrednictwem VPN.
2. Harmonogram wdrożenia Systemu.
3. Szczegółowy plan pierwszego Wydania oraz ogólny plan dla pozostałych Wydań.
4. Sposób komunikacji Zamawiającego z Wykonawcą oraz wspomagające narzędzia informatyczne.
5. Harmonogramu i zakres szkoleń.
6. Plan testów.
7. Zakres i sposób przeprowadzenia audytu bezpieczeństwa kodu.
8. Jednoznacznie ustalone zasady konfiguracji Systemu.
9. Schematy i opisy architektury logicznej i fizycznej zawierające również rozmieszczenie oraz powiązanie jej poszczególnych elementów, na poziomie sprzętowym oraz oprogramowania, z uwzględnieniem wersji produkcyjnej i testowej.
10. Wykaz komponentów wchodzących w skład Systemu (w tym bibliotek zewnętrznych oraz oprogramowania firm trzecich) wraz z informacją o wersji.
11. Szczegółowy zakres udostępnianych danych i usług.
12. Projekt Techniczny musi być aktualizowany o zmiany w projekcie do końca czasu trwania wdrożenia tj. końca Etapu 3 Umowy.
13. Dokumentacja interfejsów API.

9. Projekt Graficzny

1. Projekt Graficzny musi być sporządzony dla komponentów Systemu będących Oprogramowaniem dedykowanym.
2. Projekt graficzny Portalu musi być zgodny z Systemem Identyfikacji Wizualnej NIZP PZH-PIB.
3. Projekt Graficzny musi być sporządzony dla 3 grup urządzeń: dla komputerów, dla tabletów oraz dla smartfonów, uwzględniając wytyczne i założenia responsywnego interfejsu webowego.
4. Projekt Graficzny dla każdej z tych grup urządzeń musi zawierać wszystkie podstrony (strona główna oraz wszystkie podstrony, które wyglądają inaczej niż pozostałe).
5. Projekt Graficzny musi zostać przygotowany i przedstawiony Zamawiającemu przez Wykonawcę oraz zaakceptowany przez Zamawiającego dla każdego Wydania zgodnie z zakresem Wydania. Do każdego wydania muszą zostać dołączone pliki źródłowe.
6. Projekt Graficzny musi zostać przygotowany przez Wykonawcę w formacie umożliwiającym nanoszenie komentarzy i próśb o zmianę przez Zamawiającego.
7. Praca z Projektem Graficznym nie może obciążać Zamawiającego koniecznością ponoszenia dodatkowych kosztów, np. przez konieczność dokupienia dodatkowych licencji na oprogramowanie. Dopuszczalne jest uwzględnienie licencji na dodatkowe oprogramowanie w ofercie.

8. Projekt Graficzny będzie zawierał pliki wyjściowe w formacie, umożliwiającym otwarcie w standardowych narzędziach systemu Windows (pakiet MS Office 365) oraz pliki wektorowe w standardzie ustalonym z Zamawiającym na etapie akceptacji projektu graficznego.
9. Projekt graficzny, po zaakceptowaniu przez Zamawiającego, powinien zostać wyeksportowany do formatu.pdf i przekazany Zamawiającemu.
10. Projekt graficzny musi uwzględniać standardy UX Zamawiającego opisane w dokumencie będącym załącznikiem nr 1 oraz standard **WCAG 2.1. AA**.
11. Projekt graficzny powinien uwzględniać deklaracje dostępności (zgodnie z wymogiem WF.2)

10. Harmonogram wdrożenia Systemu

1. Harmonogram musi zawierać kamienie milowe i produkty.
2. Harmonogram musi zawierać sekwencję zdarzeń.
3. Harmonogram musi uwzględniać wykorzystanie odpowiednich zasobów ludzkich po stronie Zamawiającego.
4. Harmonogram musi określać rozłożone w czasie Wydania.
5. W harmonogramie muszą zostać w szczególności uwzględnione następujące elementy:
 - a. Dostarczenie Projektu Technicznego
 - b. Przygotowanie środowiska przez Wykonawcę z podziałem na środowisko testowe i produkcyjne
 - c. Dostarczenie, instalacja i konfiguracja przez Wykonawcę Systemu w środowisku testowym
 - d. Dostarczenie Dokumentacji
 - e. Dostarczenie, instalacja i konfiguracja przez Wykonawcę Systemu w środowisku produkcyjnym
 - f. Szkolenia dla Administratorów IT i Użytkowników Wewnętrznych
 - g. Rozpoczęcia i zakończenia poszczególnych Wydań
6. Harmonogram musi zawierać terminy, czas trwania poszczególnych elementów wymienionych w pkt 5)

11. Wydanie

1. Wydanie jest okresem czasu w trakcie trwania projektu wdrożenia Systemu, w którym realizowane są określone przez Wykonawcę wymagania funkcjonalne i pozafunkcjonalne z zakresu wszystkich wymagań OPZ. Następnie wskazany przez Wykonawcę zakres jest odbierany przez Zamawiającego.
2. Plan wydania wskazuje, które wymagania OPZ zostaną zrealizowane w danym Wydaniu.
3. Minimalna ilość planowanych wydań w projekcie to 3. Minimalny czas trwania Wydania to 1 miesiąc. Zakres ostatniego wydania przed etapem stabilizacji Systemu może realizować maksymalnie 20% wszystkich wymagań z OPZ.

4. Wydanie składa się z odbioru następujących produktów dla określonego w wydaniu zakresu wymagań z OPZ.
 - Zaktualizowany Projekt Techniczny
 - Projekt Graficzny
 - Scenariusze testowe
 - Wdrożony testowo System
 - Procedura testów wg Planu testów w tym testy akceptacyjne Zamawiającego
5. Każde wydanie musi dostarczać działającą i możliwą do przetestowania przez Zamawiającego część Systemu.
6. Każde kolejne wydanie powinno rozwijać w sposób narastający System e-ATESTY.

12. Wdrożenie

Wdrożenie Systemu musi obejmować:

1. Uruchomienie środowiska testowego z dostępem dla Zamawiającego
2. Dostarczenie Systemu e-ATESTY.
3. Udzielenie Zamawiającemu wsparcia podczas testów Systemu przeprowadzanych przez Zamawiającego.
4. Uruchomienie produkcyjne Systemu.
5. Przeprowadzenie audytu bezpieczeństwa kodu oraz testów swobodnych

13. Plan testów

Plan testów oraz scenariusze testowe:

1. Plan testów określa koncepcje wykonania testów i audytów na przestrzeni całego projektu. Natomiast w poszczególnych Wydaniach Plan testów jest implementowany, przygotowywane są scenariusze testowe i na ich podstawie wykonywane są wszystkie rodzaje testów/audytów dla danego zakresu wydania.
2. Plan testów w zakresie wdrożenia Systemu musi zawierać co najmniej:
 - a. Testy funkcjonalne,
 - b. Testy wydajności,
 - c. Testy bezpieczeństwa,
 - d. Testy spójności danych
 - e. Testy akceptacyjne.
 - f. Testy swobodne
 - g. Audyt bezpieczeństwa kodu (w tym jakości i kompletności)
 - h. Audyt bezpieczeństwa (w tym Testy penetracyjne)
 - i. Audyt dostępności cyfrowej (WCAG)
 - j. Audyt użyteczności (UX)
3. Plan testów zawiera listę wymagań funkcjonalnych i jakościowych Systemu wynikających z OPZ, które mają zostać poddane testom.
4. Wyłączenia – Zamawiający dopuszcza, aby testy nie obejmowały wybranych elementów w zakresie i obszarze testów, jednak w takiej sytuacji, fragmenty te muszą być jasno i precyzyjnie określone wraz z podaniem przyczyny, dla której następuje

- wyłaczenie. Wyłączenia muszą być zatwierdzone przez Zamawiającego. Brak zgody Zamawiającego skutkuje koniecznością przeprowadzenia testów w tym zakresie.
5. Plan testów zawiera harmonogram ich realizacji, tj. określa w jaki sposób testy będą realizowane dla poszczególnych Wydań.
 6. Plan testów zawiera spis środowisk przeznaczonych do wykorzystania w trakcie testów.
 7. Plan testów i scenariusze testowe zostaną opracowane przez Wykonawcę.
 8. Plan testów musi zostać zaakceptowany przez Zamawiającego w zakresie zgodności z wymogami wskazanymi w Umowie.
 9. Scenariusze testowe mają określone warunki których spełnienie pozwala na rozpoczęcie testów
 10. Scenariusze testowe zawierają zestaw kryteriów pozwalających uznać test za zakończony z wynikiem pozytywnym. Zestaw kryteriów podlega akceptacji Zamawiającego.
 11. Audyt bezpieczeństwa i testy penetracyjne, audyt bezpieczeństwa kodu, audyt użyteczności i audyt dostępności cyfrowej (WCAG) powinny zostać wykonane wraz ze sporządzeniem odpowiednich Raportów.
 12. Test spójności danych dotyczyć będzie metod i procesów wykorzystywanych do weryfikacji i zarządzania danymi oraz samą bazą danych. Celem testu będzie sprawdzenie metod dostępu do danych, sprawdzenia poprawności wdrożonych funkcji procesu i potwierdzenie, że korzystanie z bazy danych przez użytkowników zewnętrznych, nie powoduje zmiany danych, niepożądanych modyfikacji bazy oraz innych podobnych problemów.
 13. Zakres, wykorzystywane standardy i metody prowadzenia testów/audytów podlegają akceptacji Zamawiającego na etapie Projektu Technicznego.

14. Dokumentacja

Ogólne

1. Dokumentacja sporządzona na potrzeby Zamówienia musi być zgodna ze stanem prawnym aktualnym na dzień przedstawienia jej do odbioru Zamawiającemu.
2. Dokumentacja powinna obejmować wszystkie komponenty Systemu e-ATESTY.
3. Dostarczona Dokumentacja musi być w języku polskim, być spójna i nie może zawierać sprzeczności. Wykonawca musi zapewnić wzajemną zgodność pomiędzy wszystkimi rodzajami informacji umieszczonymi w Dokumentacji, brak logicznych sprzeczności oraz spójność pomiędzy informacjami zawartymi w Dokumentacji.
4. Dostarczona Dokumentacja ma charakteryzować się:
 - a. Jednolitą strukturą, rozumianą jako podział danego dokumentu na rozdziały, podrozdziały i sekcje w czytelny i zrozumiały sposób.
 - b. Jednolitym sposobem opisywania rozumianym jako zachowanie spójnej struktury, formy i sposobu pisania.
 - c. Poprawnością ortograficzną.
 - d. Aktualnymi odnośnikami do innych dokumentów, rozdziałów lub fragmentów Dokumentacji.
 - e. Musi w całości opisywać funkcjonalności Systemu.

- f. Musi zawierać pełne przedstawienie omawianego problemu obejmujące całość rozpatrywanego zakresu zagadnienia i nie zawierać zbędnej treści.
- g. Musi zawierać uzgodnienia poczynione z Zamawiającym w trakcie realizacji przedmiotu Umowy.
- h. Musi być spójna z Systemem Identyfikacji Wizualnej NIZP PZH-PIB.

Dokumentacja Użytkownika

Dokumentacja Użytkownika powinna zawierać:

1. Instrukcję użycia Sytemu krok po kroku dla wszystkich wymaganych funkcjonalności.
2. Komplet zrzutów ekranu z komponentów Systemu dla każdego indywidualnego ekranu/okna systemu, w celu obrazowego zaprezentowania użytkownikowi koniecznych kroków.
3. Wyjaśnienie zasady komunikacji systemu z użytkownikiem – kolory błędów, zasady walidacji, schemat rozwiązywania problemów.
4. Opis zastosowania wszystkich użytych słowników.
5. Listę i opis ikon, przycisków i skrótów klawiaturowych.
6. Opis wszystkich parametrów Systemu związanych z jego ustawieniami i funkcjonalnościami.
7. Zawierać wykaz możliwych do przyznania uprawnień do Systemu wraz z ich opisem.

Dokumentacja Administratora

Dokumentacja Administratora powinna zawierać:

1. Opis konfiguracji Systemu, w tym wykaz wdrożonych komponentów, relacji pomiędzy nimi, opis ich konfiguracji, implementacji w środowiskach, implementacji integracji.
2. Kompletną instrukcję instalacji i konfiguracji:
 - a. systemów
 - b. baz danych
 - c. kolejek
3. Opis postępowania w przypadku sytuacji awaryjnych – lista poleceń potrzebnych do uruchomienia wszystkich komponentów Systemu.
4. Komplet skryptów bazodanowych do odtworzenia baz danych.
5. Instrukcje start/stop dla całego środowiska.
6. Instrukcje eksploatacyjne dla administratorów.
7. Instrukcje wykonywania kopii zapasowych i odtwarzania Systemu z kopii.

Dokumentacja Techniczna

Dokumentacja Techniczna powinna zawierać:

1. Pełną dokumentację API oraz strukturę baz danych w formacie dokumentu DOC(X) lub PDF
2. Schemat architektury Oprogramowania wraz z opisem.
3. Diagramy klas i struktura bazy danych wraz z opisem uwzględniająca powiązania i zależności między elementami w formacie zgodnym z Enterprise Architect w wersji 15 lub nowszej (XML).
4. Wymagania techniczne dotyczące sprzętu i środowiska (z dokładnością do wersji środowiska).

5. Ustawienia konfiguracyjne środowiska, w którym pracuje System, w tym również opis implementacji w środowisku wraz z procedurami start/stop dla wszystkich komponentów Systemu.
6. Opis parametrów konfiguracji Systemu i sposób ich wykorzystania.
7. Opis techniczny rodzajów i zastosowanych protokołów komunikacji (w tym certyfikatów).
8. Sposób wykonania instalacji Systemu, instalacji poprawek i kolejnych wersji.
9. Procedurę odtworzenia danych i konfiguracji.
10. Proces tworzenia kopii zapasowych.
11. Diagram przepływu danych pomiędzy Systemem, a wszystkimi aplikacjami mającymi się integrować.
12. Diagram przepływu danych pomiędzy poszczególnymi modułami wewnątrz Systemu.
13. Instrukcję dla integratorów, w wersji do udostępniania osobom trzecim w celu właściwego zintegrowania się z Systemem zawierająca:
 - o opis usługi, interfejsów i wytyczne umożliwiające integrację Systemu.
 - o pliki z techniczną definicją i opisem poszczególnych Endpoint (np. OpenAPI JSON, Json-Schema, WSDL, GML, itp.).
 - o opis metod i struktur danych interfejsów.
14. Słownik danych – zaleca się taki, w którym dla danych w formatkach i raportach Systemu przywołano odpowiednie pole w tabeli lub widoku w bazie.
15. Wykaz danych podlegających kontroli poprawności wraz z informacją o sposobie kontroli poprawności.
16. Wykaz komunikatów diagnostycznych i standardowych błędów (opis błędu, warunki jego powstania).

Dokumentacja Powykonawcza

Dokumentacja Powykonawcza powinna zawierać:

1. Kompletny opis środowiska produkcyjnego i testowego.
 - a. Opis maszyn wirtualnych i ich rozmieszczenia na serwerze/serwerach.
 - b. Opis zainstalowanych komponentów/systemów/aplikacji, ich lokalizacji, roli, uprawnieniach.
2. Spis wszystkich użytkowników administracyjnych (serwerowych, bazodanowych, aplikacyjnych itp.) wraz z danymi autoryzacyjnymi.
3. Spis wszystkich utworzonych użytkowników (serwerowych, bazodanowych, aplikacyjnych itp.) z zakresem praw jakie posiadają oraz opisem.
4. Raporty zawierające wyniki testów akceptacyjnych, funkcjonalnych, swobodnych, wydajności, bezpieczeństwa, spójności danych.
5. Protokoły zdawczo – odbiorcze dla poszczególnych składowych systemu.
6. Raport z przeprowadzenia audytu bezpieczeństwa kodu.

Polityka bezpieczeństwa

Polityka Bezpieczeństwa musi być opracowana zgodnie z obowiązującymi przepisami prawa Rzeczypospolitej Polskiej oraz prawem Unii Europejskiej, w tym zgodnie z wymaganiami Krajowych Ram Interoperacyjności, Krajowym Systemie Cyberbezpieczeństwa, normą PN-

EN ISO/IEC 27001 jak również z obowiązującymi przepisami w zakresie ochrony danych osobowych.

Polityka bezpieczeństwa musi obejmować cały wdrażany System wraz z poszczególnymi modułami. Powinna zawierać m.in:

1. Regulamin Ochrony Danych Osobowych,
2. Regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji zgodne z regulacjami RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679);
3. Regulamin Ciągłości Działania,
4. Instrukcję bezpiecznego administrowania systemami teleinformatycznymi,
5. Listy wymagań minimalnych dla głównych klas zbiorów danych,
6. Instrukcję bezpiecznego użytkowania systemów teleinformatycznych,
7. Procedurę okresowych wewnętrznych audytów bezpieczeństwa,
8. Plan audytów wewnętrznych i zewnętrznych,
9. Instrukcję sporządzania cyklicznych raportów dla właścicieli kluczowych zbiorów danych i kadry zarządzającej,
10. Procedury eksploatacyjne dla głównych klas zbiorów danych,
11. Szablony rejestrów przewidzianych w regulaminach, instrukcjach i procedurach,
12. Wymagane procedury bezpieczeństwa i instrukcje wynikających z regulaminów bezpieczeństwa obszarów.
13. Określenie sposobu kwalifikacji incydentów włączając w to parametry je określające i poziomy/istotność incydentów
14. Określanie konkretnych środków i miar mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w kontekście oferowania usług objętych wdrażanym Systemem.

Wraz z Polityką bezpieczeństwa opracowana zostanie metodyka szacowania ryzyka oraz na jej podstawie przeprowadzony proces szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w systemie.

15. Kody źródłowe Systemu

Kody źródłowe muszą być przekazane w formie elektronicznej (przed kompilacją), umożliwiającej analizę i rozbudowę zarówno przez Zamawiającego jak i firmy trzecie działające na potrzeby Zamawiającego. Wykonawca musi przekazać informację o:

1. Wszystkich bibliotekach i dodatkach niezbędnych do kompilacji i uruchomienia kodu.
2. Rekomendowanym środowisku programistycznym wraz ze wskazaniem niezbędnych dodatków.
3. Parametrach i zmiennych środowiska programistycznego koniecznych do kompilacji i uruchomienia Systemu, instrukcji minimalnych czynności pozwalających na uruchomienie Systemu (wraz z kompilacją, jeżeli jest potrzebna).

4. Rekomendacji w zakresie kompilatora i jego ustawień.
5. W przypadku przekazywania kodu źródłowego Systemu, musi być on przekazany w taki sposób, aby było możliwe umieszczenie kodu w lokalnym repozytorium Zamawiającego.
6. Kod skryptów do obsługi/wdrażania (CI/CD) np. pliki JenkinsFile.

Kody źródłowe wytwarzane i dostarczane przez Wykonawcę będą gromadzone w repozytorium udostępnionym przez Wykonawcę. Wykonawca zapewni wymagane dostępy dla Zamawiającego do tego repozytorium.

W przypadku kodów źródłowych wytwarzanych przez Wykonawcę po ich akceptacji i/lub odbiorze przez Zamawiającego, Wykonawca zobowiązany będzie do ich utrzymywania i zapewnienia aktualności w ramach prowadzonych prac projektowych.

Kody źródłowe powinny zawierać wskazanie:

1. Wersji i dystrybucji wszystkich niezbędnych komponentów.
2. Sposobu instalacji bibliotek i dodatków.
3. Sposobu ustawiania parametrów i zmiennych środowiskowych.

W celu dokonania weryfikacji kompletności i czytelności kodu źródłowego, w obecności Zamawiającego, Wykonawca ma dokonać kompilacji i sprawdzenia poprawności działania kodu źródłowego o ile na etapie projektu technicznego nie zostanie ustalony inny tryb weryfikacji kodu źródłowego.

16. Asysta i Konserwacja Techniczna

1. W ramach świadczenia ATiK Wykonawca:
 - a. zapewni prawidłowe funkcjonowanie Systemu zgodne z warunkami Umowy oraz Dokumentacją,
 - b. usunie Błędy na zasadach określonych w Umowie,
 - c. dostarczy Modyfikacje Systemu,
 - d. dostarczy Usprawnienia Systemu,
 - e. dostarczy Wersje Systemu,
 - f. zapewni usługę konsultacji elektronicznych polegających na udzielaniu porad i wyjaśnień dotyczących zasad działania Systemu oraz możliwości i warunków jego rozbudowy,
 - g. przeniesie dane ze struktur poprzedniej Wersji Systemu do struktur nowej Wersji Systemu, jeżeli Wersja Systemu tego wymaga,
 - h. utrzyma sprawność Systemu na co najmniej takim poziomie jaki był przed zainstalowaniem Usprawnień, Modyfikacji i Wersji Systemu, przy zabezpieczeniu przez Zamawiającego odpowiedniej konfiguracji sprzętowo-systemowej,
 - i. zapewni Zamawiającemu wsparcie i pomoc w usuwaniu nieprawidłowości działania Systemu wynikających z instalacji Oprogramowania Standardowego,

- j. zapewni konserwację Systemu obejmującą prace związane z rekonfiguracją Systemu,
 - k. zapewni wsparcie i pomoc w zakresie zarządzania Systemem.
2. Wykonawca zobowiązany jest do dostarczenia Modyfikacji Systemu przed terminem wejścia w życie zmian w przepisach prawnych, jeżeli zostały one opublikowane co najmniej 14 dni roboczych przed ich wejściem w życie, a jeżeli warunek ten nie jest spełniony – w terminie 14 dni roboczych od dnia ich opublikowania. W uzasadnionych przypadkach Strony mogą ustalić inny termin wykonania Modyfikacji Systemu.
3. Wykonawca zobowiązany jest do przeprowadzenia przed dostarczeniem do Zamawiającego testów Usprawnień Systemu, Wersji Systemu oraz Modyfikacji Systemu we własnym środowisku testowym, które składa się co najmniej z takiej samej wersji Systemu, jaką posiada Zamawiający w tym również pod kątem:
 - a. poprawnego działania dostarczonego rozwiązania,
 - b. poprawnego działania wszystkich pozostałych funkcjonalności Systemu, której dotyczy dostarczone rozwiązanie.
4. Wykonawca zobowiązany jest do dostarczenia Zamawiającemu do 10 dni roboczych po instalacji każdej Modyfikacji, każdego Usprawnienia, każdej Wersji Systemu zaktualizowanej Dokumentacji (jeżeli taka aktualizacja jest konieczna) w wersji elektronicznej w formacie umożliwiającym jej wydruk i modyfikację.
5. W ramach ATiK Wykonawca przystąpi niezwłocznie do usunięcia Błędów i udzielenia odpowiedzi w ramach konsultacji elektronicznych. Powyższe czynności będą trwać nie dłużej niż:
 - a. usunięcie Błędów krytycznych – do 1 Dnia roboczego od momentu zgłoszenia,
 - b. usunięcie Błędów niekrytycznych – do 5 dni roboczych od momentu zgłoszenia,
 - c. udzielenie odpowiedzi w ramach konsultacji elektronicznych – do 10 dni roboczych od momentu zgłoszenia.
6. Czas usunięcia Błędu/udzielenia konsultacji elektronicznych, o którym mowa w pkt. 5, jest liczony od momentu przekazania zgłoszenia Błędu/potrzeby udzielenia konsultacji elektronicznych przez Zamawiającego do momentu usunięcia Błędu/udzielenia odpowiedzi w ramach konsultacji elektronicznej.

17. Szkolenia

1. Terminy realizacji oraz zakres szkoleń zostaną uzgodnione z Zamawiającym na etapie Projektu Technicznego.
2. Wykonawca musi uwzględnić ciągłość pracy Zamawiającego
3. Wykonawca utrwali w formie audio-video wszystkie przeprowadzane szkolenia.
4. Zakres szkoleń:
 - a. Ogólne szkolenie wyjaśniające działanie Systemu e-ATESTY. Wymagana forma zdalna. Łącznie dla 50 osób.
 - b. Szkolenie Użytkowników Wewnętrznych dla systemu CMS. Łącznie dla 30 osób.
 - c. Szkolenia Administratorów IT dla systemu CMS i konfiguracji całego Systemu e-ATESTY. Łącznie dla 20 osób.

18. Uwarunkowania prawne, normy i systemy

Oprogramowanie powinno spełniać wymagania prawne obowiązujące w Rzeczypospolitej Polskiej, w szczególności:

1. RODO (Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679) z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - ogólne unijne rozporządzenie zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
2. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych – Ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. i Sprostowanie do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 23 maja 2018r.
3. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz.U. 2019 poz. 730)
4. Ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz.U. 2018 poz. 1544 z późn. zm.)
5. Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019 poz. 125 z późn. zm.).
6. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. 2019 poz. 742 z późn. zm.)
7. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (t.j. Dz.U. 2023 poz. 82).
8. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023r. poz. 57) , w szczególności minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych.
9. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2022 poz. 1863 z późn. zm.).
10. Norma PN-ISO/IEC 27001:2017-06 – Systemy zarządzania bezpieczeństwem informacji.
11. Standardy wynikające z wytycznych horyzontalnych MiiR.
12. Rozporządzenie rady ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U.2017 poz. 2247 z późn. zm.).
13. System ma być zgodny z zapisami dokumentów NIZP PZH-PIB (chyba, że OPZ stanowi inaczej):

- a. Załącznik nr 1 – Rekomendacje UX
- b. Załącznik nr 2 – Strategia bezpieczeństwa
- c. Załącznik nr 3 – Plan zapewnienia jakości

19. Załączniki do dokumentu

Załącznik nr 1 – Rekomendacje UX

Załącznik nr 2 – Strategia bezpieczeństwa

Załącznik nr 3 – Plan zapewnienia jakości