Opis przedmiotu zamówienia

System do prowadzenia dokumentacji zgodności (wzór)

Zamawiający: ……. Postępowanie nr ……. Opis sporządzono na podstawie art. 99 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa licencji na system informatyczny wspierający prowadzenie dokumentacji zgodności Zamawiającego (dalej „System"), jego wdrożenie w infrastrukturze Zamawiającego, przeszkolenie użytkowników oraz świadczenie usług utrzymania, obejmujących aktualizacje, poprawki bezpieczeństwa i wsparcie techniczne przez okres …… miesięcy.

Zamawiający wymaga wykonania zakresów oznaczonych poniżej. Zakres podstawowy obejmuje prowadzenie dokumentacji ochrony danych osobowych. Pozostałe zakresy Zamawiający wybiera przez zaznaczenie.

	Zakres funkcjonalny	**Pkt dokumentu**
☐	A. Ochrona danych osobowych (wymagany)	3.2
☐	B. System zarządzania bezpieczeństwem informacji	3.3
☐	C. Rejestr umów i Centralny Rejestr Umów	3.4
☐	D. Kadry (bez naliczania wynagrodzeń)	3.5
☐	E. Obowiązki z ustawy o krajowym systemie cyberbezpieczeństwa	3.6

2. Określenia

– **Dzień roboczy** – dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy.

– **Godziny robocze** – godziny od …… do …… w dni robocze.

– **Awaria krytyczna** – brak możliwości korzystania z Systemu przez użytkowników, utrata lub uszkodzenie danych albo incydent bezpieczeństwa dotyczący Systemu.

– **Poprawka bezpieczeństwa** – aktualizacja usuwająca podatność Systemu.

3. Wymagania funkcjonalne

Spełnienie wymagań weryfikuje się w sposób wskazany w tabelach: przez demonstrację na środowisku Wykonawcy, na podstawie dokumentacji albo oświadczenia Wykonawcy (pkt 11).

3.1. Wymagania ogólne

Lp.	**Wymaganie**	**Sposób weryfikacji**
F-01	System jest aplikacją dostępną przez przeglądarkę internetową i nie wymaga instalowania oprogramowania na stanowiskach użytkowników. Działa w aktualnych wersjach powszechnie używanych przeglądarek.	demonstracja
F-02	Dostęp odbywa się na kontach imiennych. System udostępnia role o zróżnicowanym zakresie uprawnień (co najmniej: administrator, inspektor ochrony danych, kierownik, pracownik) oraz pozwala nadać wybranej osobie odmienne uprawnienia do poszczególnych rejestrów.	demonstracja

Lp.	Wymaganie	Sposób weryfikacji
F-03	Uprawnienia do rejestrów mają co najmniej poziomy: brak dostępu, odczyt, edycja. Konfigurację uprawnień wykonuje administrator Zamawiającego bez udziału Wykonawcy.	demonstracja
F-04	System prowadzi dziennik zdarzeń obejmujący co najmniej logowania, zmiany danych, zmiany uprawnień i pobrania dokumentów, z możliwością eksportu przez uprawnione osoby.	demonstracja
F-05	Do wpisów można dołączać pliki. Pliki są dostępne wyłącznie po zalogowaniu i z uwzględnieniem uprawnień użytkownika. Administrator może ustawić limit rozmiaru załącznika.	demonstracja
F-06	Rejestry można przeszukiwać, filtrować i sortować.	demonstracja
F-07	System wysyła przypomnienia e-mail o zbliżających się terminach przeglądów lub zakończenia, z konfigurowalnymi progami czasowymi i adresatem.	demonstracja
F-08	Moduły funkcjonalne można włączać i wyłączać w konfiguracji bez utraty zapisanych danych. Interfejs i komunikaty są w języku polskim.	demonstracja

3.2. Zakres A: ochrona danych osobowych

Lp.	Wymaganie	Sposób weryfikacji
A-01	Rejestr czynności przetwarzania danych osobowych zawierający co najmniej: cel przetwarzania, podstawę prawną, kategorie osób i danych, odbiorców, przekazywanie do państw trzecich, okres przechowywania i opis środków bezpieczeństwa (art. 30 ust. 1 RODO).	demonstracja
A-02	Rejestr kategorii czynności przetwarzania wykonywanych w imieniu administratora (art. 30 ust. 2 RODO).	demonstracja
A-03	Rejestr naruszeń ochrony danych z datą wykrycia, oceną ryzyka i informacją o zgłoszeniu do organu nadzorczego.	demonstracja
A-04	Rejestr wniosków osób, których dane dotyczą, z rodzajem żądania (art. 15–21 RODO) i datą wpływu.	demonstracja
A-05	Rejestr zgód i podstaw przetwarzania oraz rejestr umów powierzenia przetwarzania.	demonstracja
A-06	Ewidencja analiz ryzyka i oceny skutków dla ochrony danych, ze wskazaniem, czy ocena jest wymagana, i jej statusu.	demonstracja
A-07	Pulpit inspektora ochrony danych oraz cykl przeglądów rejestrów z przypomnieniami.	demonstracja

3.3. Zakres B: system zarządzania bezpieczeństwem informacji

Lp.	Wymaganie	Sposób weryfikacji
B-01	Prowadzenie dokumentacji bezpieczeństwa informacji obejmującej co najmniej politykę bezpieczeństwa informacji, politykę ochrony danych osobowych, zarządzanie incydentami, zarządzanie systemem teleinformatycznym i zarządzanie ciągłością działania, wraz z załącznikami.	demonstracja
B-02	Dla każdego dokumentu zapisywane są co najmniej: rodzaj, status, wersja, właściciel i data zatwierdzenia.	demonstracja

Lp.	Wymaganie	Sposób weryfikacji
B-03	Rejestry upoważnień do przetwarzania danych, audytów i sprawdzeń oraz szkoleń i oświadczeń.	demonstracja
B-04	Inwentaryzacja zasobów, usług i sprzętu informatycznego.	demonstracja

3.4. Zakres C: rejestr umów i Centralny Rejestr Umów

Lp.	Wymaganie	Sposób weryfikacji
C-01	Kartoteka umowy zawierająca co najmniej: numer, rodzaj, status, kontrahenta, przedmiot, okres obowiązywania, zasady odnowienia i wypowiedzenia, wartość netto i brutto, walutę oraz załączniki. Numer umowy jest unikalny.	demonstracja
C-02	Historia zmian kartoteki z zachowaniem poprzednich wersji, autorem i datą zmiany. Umowy są archiwizowane, a nie usuwane.	demonstracja
C-03	Pulpit terminów i przypomnienia e-mail o kończących się umowach; eksport przefiltrowanej listy do formatu CSV.	demonstracja
C-04	Ocena, czy umowa podlega udostępnieniu w CRU (art. 34a ustawy o finansach publicznych), z zapisem decyzji, uzasadnienia i osoby, która ją podjęła.	demonstracja
C-05	Kontrola terminu udostępnienia umowy w CRU (30 dni od zawarcia lub zmiany), z uwzględnieniem dni awarii CRU ogłoszonych przez ministra, oraz ostrzeżenia o terminach.	demonstracja
C-06	Przygotowanie danych umowy w układzie odpowiadającym formularzowi CRU do ręcznego wpisu.	demonstracja
C-07	Opcjonalne przekazywanie danych do CRU przez interfejs udostępniony przez Ministra Finansów, wyłącznie po zatwierdzeniu przez uprawnioną osobę, z zabezpieczeniem przed wysłaniem tej samej umowy dwukrotnie oraz dziennikiem komunikacji niezawierającym klucza dostępowego.	demonstracja
C-08	Import zbiorczy umów z pliku CSV z raportem błędów dla każdego wiersza.	demonstracja
C-09	Kontrola identyfikatorów kontrahenta (NIP, REGON) oraz, w jednostkach samorządu gminnego, ostrzeżenie o umowie cywilnoprawnej z radnym (art. 24d ustawy o samorządzie gminnym).	demonstracja

3.5. Zakres D: kadry

Lp.	Wymaganie	Sposób weryfikacji
D-01	Kartoteka pracownika i współpracownika z historią zatrudnienia i zmian warunków, bez przetwarzania stawek i wynagrodzeń. System nie musi naliczać płac, podatków, składek ani zasiłków.	demonstracja
D-02	Ewidencje: nieobecności i urlopy, szkolenia, BHP, badania medycyny pracy (bez diagnoz i dokumentacji medycznej), uprawnienia i kwalifikacje, oceny okresowe, wyposażenie i mienie powierzone.	demonstracja
D-03	Kontrola terminów i przypomnienia e-mail. Każda zmiana kartoteki zapisuje wersję z autorem i datą; archiwizacja nie usuwa danych ani załączników.	demonstracja

Lp.	Wymaganie	Sposób weryfikacji
D-04	Katalog stanowisk oraz kreator zatrudnienia prowadzący przez kolejne czynności i terminy, z generowaniem dokumentów w formatach DOCX i PDF z edytowalnych wzorów.	demonstracja
D-05	Akta osobowe w postaci elektronicznej, w częściach A i B, z numeracją, datą i osobą sporządzającą oraz kontrolą integralności dokumentów.	demonstracja

3.6. Zakres E: obowiązki z ustawy o krajowym systemie cyberbezpieczeństwa

Lp.	Wymaganie	Sposób weryfikacji
E-01	Wykaz obowiązków kierownika jednostki, z podziałem na podmiot kluczowy i ważny, zawierający podstawę prawną, status, osobę odpowiedzialną, termin i dowody realizacji.	demonstracja
E-02	Rejestr incydentów kontrolujący terminy: wczesnego ostrzeżenia (24 godziny), zgłoszenia incydentu (72 godziny) i sprawozdania końcowego, a także zgłoszenia naruszenia ochrony danych organowi nadzorczemu (72 godziny), z alarmami e-mail.	demonstracja
E-03	Lista osób dopuszczonych do realizacji zadań wymagających szczególnego zaufania, bez przechowywania treści informacji z rejestru karnego.	demonstracja
E-04	Raport dla kierownika jednostki w formacie PDF, z zapisem potwierdzenia zapoznania się z nim.	demonstracja

4. Wymagania pozafunkcjonalne

Lp.	Wymaganie	Sposób weryfikacji
N-01	System jest instalowany w infrastrukturze Zamawiającego (on-premise). Dane, załączniki i kopie zapasowe są przechowywane wyłącznie w tej infrastrukturze. Wykonawca nie przechowuje ich na własnych systemach.	oświadczenie
N-02	Instalacja i praca Systemu nie wymagają stałego dostępu do internetu. Połączenia wychodzące są nawiązywane wyłącznie w ramach integracji włączanych przez administratora (poczta e-mail, CRU). Wykonawca wskaże w ofercie wszystkie połączenia wychodzące Systemu.	dokumentacja
N-03	Wykonawca poda w ofercie wymagania środowiskowe: system operacyjny, procesor, pamięć, miejsce na dysku, porty sieciowe i wymagane pakiety. Zamawiający zapewni maszynę wirtualną z systemem Linux o parametrach nie większych niż …… vCPU, …… GB RAM i …… GB dysku.	oferta
N-04	Transmisja danych między przeglądarką a Systemem jest szyfrowana (TLS), a System wymusza połączenie szyfrowane. Wykonawca zapewnia zarządzanie certyfikatami w środowisku bez dostępu do publicznych urzędów certyfikacji.	demonstracja
N-05	Hasła są przechowywane wyłącznie w postaci skrótów. System wymusza zmianę hasła startowego, blokuje logowanie po serii nieudanych prób i kończy bezczynne sesje.	dokumentacja
N-06	Składniki Systemu działają bez uprawnień administratora systemu operacyjnego (zasada najmniejszych uprawnień). Wykonawca opisze zastosowane ograniczenia.	dokumentacja

Lp.	Wymaganie	Sposób weryfikacji
N-07	System chroni przed typowymi atakami na aplikacje internetowe (w szczególności z klasyfikacji OWASP Top 10) i stosuje nagłówki bezpieczeństwa, w tym politykę ograniczającą źródła zasobów.	oświadczenie
N-08	Wydania Systemu są podpisane cyfrowo. Mechanizm instalacji weryfikuje podpis i integralność wydania przed wprowadzeniem zmian i odrzuca wydanie niepodpisane lub zmienione.	demonstracja
N-09	Do każdego wydania dołączony jest wykaz składników oprogramowania (SBOM) w powszechnie stosowanym formacie, np. CycloneDX lub SPDX.	dokumentacja
N-10	Proces wytwarzania obejmuje testy automatyczne oraz skanowanie zależności i obrazów wdrożeniowych pod kątem znanych podatności przed każdym wydaniem. Podatności krytyczne i wysokie są usuwane przed wydaniem albo uzasadniane i ograniczane udokumentowanym środkiem zaradczym.	oświadczenie
N-11	Wykonawca posiada i stosuje procedurę przyjmowania zgłoszeń podatności oraz powiadamiania użytkowników, zgodną z obowiązkami wytwórcy wynikającymi z rozporządzenia (UE) 2024/2847 (Cyber Resilience Act) od terminów jego stosowania.	dokumentacja
N-12	Wykonawca zapewnia poprawki bezpieczeństwa dla dostarczonej linii wersji przez co najmniej 5 lat od dnia pierwszego wydania tej linii i wskaże w ofercie datę końca wsparcia. Zakończenie wsparcia ogłasza co najmniej 12 miesięcy wcześniej.	oświadczenie

4.1. Kopie zapasowe i aktualizacje

Lp.	Wymaganie	Sposób weryfikacji
N-13	System ma wbudowany mechanizm automatycznych kopii zapasowych wykonywanych co najmniej raz na dobę, obejmujący bazę danych, załączniki oraz dane konfiguracyjne niezbędne do odtworzenia (w tym certyfikaty). Liczba przechowywanych kopii jest konfigurowalna. Administrator może wykonać kopię na żądanie.	demonstracja
N-14	Dokumentacja zawiera procedurę odtworzenia Systemu z kopii zapasowej. Kopie są zapisywane w sposób umożliwiający replikację poza serwer.	dokumentacja
N-15	Aktualizacje są instalowane przez administratora Zamawiającego z pliku wydania, bez kompilowania oprogramowania. Przed aktualizacją System tworzy kopię danych i konfiguracji, a w razie niepowodzenia automatycznie przywraca poprzednią wersję.	demonstracja
N-16	Po aktualizacji możliwy jest powrót do poprzedniej wersji w okresie wskazanym w dokumentacji, nie krótszym niż 48 godzin. Wykonawca opisze zasady powrotu dla wydań zmieniających strukturę bazy danych.	dokumentacja
N-17	W razie zakończenia współpracy Wykonawca wyda wszystkie dane Zamawiającego w formacie otwartym i opisanym (np. zrzut bazy danych i pliki załączników).	oświadczenie

5. Licencja

1) Wykonawca udziela Zamawiającemu niewyłącznej, bezterminowej licencji na korzystanie z Systemu, bez ograniczenia liczby użytkowników i kont.
2) Licencja obejmuje instalowanie, uruchamianie i używanie Systemu w jednej instalacji produkcyjnej oraz w jednej instalacji testowej lub szkoleniowej, wykonywanie kopii zapasowych i przeniesienie instalacji na inny serwer Zamawiającego.
3) Zamawiający może powierzyć instalację i administrowanie Systemem podmiotowi trzeciemu działającemu na jego rzecz.
4) Licencja obejmuje wersję Systemu dostarczoną w dniu odbioru oraz wszystkie aktualizacje udostępnione w okresie utrzymania.

6. Wdrożenie

Wdrożenie obejmuje w szczególności:

1) instalację Systemu w infrastrukturze Zamawiającego oraz instalację testową lub szkoleniową;
2) konfigurację połączenia szyfrowanego i instalację certyfikatu na stanowiskach wskazanych przez Zamawiającego;
3) konfigurację struktury organizacyjnej, ról i kont użytkowników oraz wybranych zakresów funkcjonalnych;
4) konfigurację poczty e-mail oraz, jeżeli Zamawiający tego zażąda, integracji z CRU;
5) import danych z plików wskazanych przez Zamawiającego w zakresie ……;
6) konfigurację kopii zapasowych i wykonanie próbnego odtworzenia;
7) przekazanie dokumentacji powykonawczej.

Wdrożenie zostanie zakończone w terminie …… dni od dnia zawarcia umowy. Odbiór następuje na podstawie protokołu podpisanego przez przedstawicieli Stron. Zamawiający dokonuje odbioru w terminie …… dni roboczych od zgłoszenia gotowości.

7. Szkolenia

– Szkolenie administratora Systemu w wymiarze …… godzin, obejmujące konfigurację, zarządzanie użytkownikami, kopie zapasowe, aktualizacje i diagnostykę.
– Szkolenie użytkowników w wymiarze …… godzin dla …… osób, w miejscu wskazanym przez Zamawiającego lub zdalnie.
– Wykonawca przekaże materiały szkoleniowe w postaci elektronicznej.

8. Utrzymanie i poziom usług

Utrzymanie obejmuje udostępnianie aktualizacji i poprawek bezpieczeństwa, instalację aktualizacji na zlecenie Zamawiającego, konsultacje telefoniczne i mailowe w wymiarze do …… godzin miesięcznie oraz dostosowywanie funkcji Systemu do zmian przepisów będących podstawą jego działania, w terminie umożliwiającym ich stosowanie. Poprawki bezpieczeństwa są udostępniane niezwłocznie po ich przygotowaniu. O podatności aktywnie wykorzystywanej Wykonawca informuje

Zamawiającego bez zbędnej zwłoki, nie później niż w ciągu …… godzin od uzyskania informacji.

Kategoria zgłoszenia	Opis	Czas reakcji	Czas naprawy
Awaria krytyczna	System nie działa lub żaden użytkownik nie może się zalogować; utrata lub uszkodzenie danych spowodowane działaniem Systemu; incydent bezpieczeństwa wynikający z podatności Systemu	do 4 godzin roboczych	do 10 dni roboczych
Błąd	funkcja działa niezgodnie z dokumentacją, co utrudnia pracę, ale nie uniemożliwia korzystania z Systemu	do …… dni roboczych	do …… dni roboczych
Usterka	nieprawidłowość niewpływająca na korzystanie z Systemu	do …… dni roboczych	w najbliższej aktualizacji

Czas reakcji liczy się od przyjęcia zgłoszenia do podjęcia czynności przez specjalistę Wykonawcy, a czas naprawy od przyjęcia zgłoszenia do trwałego usunięcia przyczyny przez udostępnienie poprawki lub aktualizacji. Czasy liczy się w godzinach roboczych. Zgłoszenia przyjmowane są pod adresem e-mail i numerem telefonu wskazanymi przez Wykonawcę. Czasy nie obowiązują, gdy przyczyna leży w środowisku Zamawiającego albo wynika z niezainstalowania udostępnionej poprawki bezpieczeństwa.

9. Dokumentacja

Wykonawca dostarczy w języku polskim, w postaci elektronicznej:

1) dokumentację instalacyjną i administracyjną (wymagania, instalacja, konfiguracja, kopie zapasowe i odtwarzanie, aktualizacje, rozwiązywanie problemów);
2) dokumentację użytkownika, dostępną także w samym Systemie;
3) opis zmian dla każdego wydania;
4) wykaz składników oprogramowania (SBOM) dla dostarczonej wersji;
5) dokumentację powykonawczą zawierającą parametry instalacji i konfiguracji.

10. Dane osobowe i dostęp zdalny

Jeżeli realizacja zamówienia wymaga dostępu Wykonawcy do danych osobowych przetwarzanych w Systemie, Strony zawrą umowę powierzenia przetwarzania zgodnie z art. 28 RODO przed uzyskaniem takiego dostępu. Dostęp zdalny do infrastruktury Zamawiającego odbywa się wyłącznie za zgodą Zamawiającego, przez wskazane przez niego połączenie, a każdy dostęp Wykonawca odnotowuje, podając datę, godzinę, osobę i zakres czynności.

11. Rozwiązania równoważne i potwierdzenie zgodności

Opis nie odwołuje się do znaków towarowych, patentów ani pochodzenia. Wymagania opisują cechy funkcjonalne i jakościowe, a Zamawiający dopuszcza rozwiązania równoważne, które spełniają je w sposób inny niż opisany, o ile zapewniają osiągnięcie tego samego rezultatu (art. 99 ust. 4 i 5 Pzp). Wykonawca powołujący się na rozwiązanie równoważne jest obowiązany wykazać w ofercie, że spełnia ono wymagania Zamawiającego.

Spełnienie wymagań Wykonawca potwierdza w ofercie wypełnioną tabelą zgodności (kolumna „Spełnia: tak/nie” dla każdego wymagania) wraz z opisem, a na wezwanie Zamawiającego, w terminie

…… dni, przeprowadza demonstrację Systemu na środowisku demonstracyjnym, obejmującą wymagania oznaczone w tabelach jako „demonstracja”.

Uwagi do stosowania wzoru (do usunięcia przed publikacją)

– Zakresy A–E należy dostosować do potrzeb jednostki. Wymagania, których Zamawiający nie potrzebuje, trzeba usunąć, a nie pozostawiać, żeby nie zawyżać wartości zamówienia.

– Wartości oznaczone wykropkowaniem (terminy, liczby godzin, parametry serwera) powinny wynikać z rzeczywistych potrzeb i oszacowania wartości zamówienia.

– Przed zastosowaniem opisu należy sprawdzić jego zgodność z regulaminem zamówień oraz przepisami obowiązującymi w dniu wszczęcia postępowania, w tym w zakresie umów podlegających CRU i ustawy o krajowym systemie cyberbezpieczeństwa.