Znak postępowania: CUI-ZZ.3200.29.2024

Załącznik nr 8 do projektu umowy

Zakres wymagań dotyczący dokumentacji

1 Uwagi i wymagania ogólne

1.1 Dokumentacja powinna zostać dostarczona w wersji elektronicznej edytowalnej i dodatkowo w wersji papierowej. W związku z powyższym wersja elektroniczna powinna być dostarczona dla:

dokumentów tekstowych w formacie PDF z możliwością przeszukiwania, również wyrazów z polskimi znakami i możliwością zaznaczania kopiowania treści,
dokumentów tekstowych w formacie DOC (lub innym ogólnie dostępnym formacie edytowalnym),
w przypadku dokumentacji zamieszczonej w systemie/aplikacji, zawartość musi być zgodna z wymaganiami wynikającymi z przepisów prawa – Ustawa z dn. 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U.2019 poz. 848 z pózn. zm..

W przypadku diagramów, schematów dostarczonych w ramach dokumentacji powinny one być dostarczone w narzędziu zgodnym
z notacjami UML, BPMN, Archimate i zapisane w formacie umożliwiającym ich przeglądanie w dostępnych publicznie i darmowych narzędziach, wraz ze wskazaniem źródła ich pobrania lub poprzez dostarczenie niezbędnego do przeglądania oprogramowania w ramach projektu. Zamawiający dopuszcza zamieszczenie diagramów i schematów w dokumentach .pdf, .doc, .docx i innych powszechnie używanych, pod warunkiem zapewnienia przez Wykonawcę czytelności zamieszczonych schematów i diagramów.

Dokumentacja powinna uwzględniać zarówno środowisko produkcyjne, testowe/szkoleniowe, jak i deweloperskie systemu.

Zawartość dokumentacji powinna być czytelna (dotyczy grafik, wykresów, diagramów).

W odniesieniu do wymagań edytorskich:

a) preferowany format dokumentacji (wielkość strony) –A4,
b) dla dokumentów .docx, .pdf czcionka o kroju Verdana, 11 pkt, interlinia co najmniej 1,15, w przypadku dokumentacji zamieszczonej w systemie/aplikacji, zawartość musi być zgodna z wymaganiami wynikającymi z przepisów prawa – Ustawa z dn. 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U.2019 poz. 848 z pózn. zm.,
c) wersjonowanie dokumentacji – format wersji n.xx gdzie n oznacza numer kolejnej zatwierdzonej wersji dokumentu, xx – numer kolejnej wersji opiniowanej, roboczej.

W ramach dokumentacji dostarczone powinny być:

zestawienie wszystkich uzgodnień i protokołów podpisanych na etapie realizacji, globalny rejestr zmian dotyczący dokumentacji powykonawczej,

2 Dokumentacja administratora

2.1 Opis systemu

Opis techniczny systemu powinien obejmować:

a) Schemat blokowy systemu wraz z opisem jego składowych oraz przepływu i przetwarzania danych w systemie.

b) graficzne odwzorowanie modułów funkcjonalnych systemu i ich komponentów logicznych,
c) punkty styku komponentów w obrębie modułów oraz punkty styku pomiędzy modułami (nazwy i definicje punktów styku wyjaśniające ich rolę i zasady działania),
d) rzeczywiste lub potencjalne zewnętrzne punkty styku Systemu do komunikacji z innymi systemami/aplikacjami, z którymi powinien współpracować (w przypadku gdy taka komunikacja została wdrożona lub system ma taką możliwość),
e) kierunki przepływu danych/informacji pomiędzy modułami w obrębie Systemu, diagram struktur bazodanowych systemu zawierający graficzne odzwierciedlenie tabel wraz z kolumnami, kluczami, relacjami pomiędzy tabelami oraz opisem danych (nazwy tabel, nazwy pól, typ danych, opis danych, opis kluczy głównych i/lub obcych).

f) Diagram wdrożenia (deployment diagram) obejmujący wszystkie składowe systemu (w nomenklaturze UML: węzły, środowiska wykonawcze, komponenty/artefakty), wraz ze ścieżkami komunikacji pomiędzy składowymi oraz systemami zewnętrznymi z opisem wykorzystywanych protokołów i portów wszystkich uruchomionych w systemie usług.

g) Opis stosowanych zabezpieczeń, w tym zabezpieczeń przed wystąpieniem podatności (protokoły szyfrujące, algorytmy szyfrowania, nagłówki bezpieczeństwa, zabezpieczenia mechanizmów logowania przed m.in. nieautoryzowanym dostępem, ilość prób logowania itp.) W przypadku zastosowania mechanizmów dwuetapowych, także opis takiego logowania (MFA/2FA).

h) Opis zarządzania sesjami użytkownika oraz zastosowanych tokenów sesyjnych.
i) Opis częstotliwości i zakresu przeprowadzania testów penetracyjnych.
j) Opis środków uniemożliwiających nieautoryzowany dostęp na poziomie baz danych, usług sieciowych oraz aplikacji wraz z elementami zabezpieczającymi system przed działaniem szkodliwego oprogramowania.
k) Opis realizacji bezpiecznej migracji danych do innej chmury oraz narzędzi do samodzielnej migracji danych.
l) Opis dot. raportowania incydentów bezpieczeństwa w zakresie obsługiwanego systemu, w tym wykaz minimalnych informacji niezbędnych do obsługi incydentu bezpieczeństwa. Dokumentacja powinna zawierać także opis procesu usuwania zgłaszanych podatności oraz raportowanie incydentów bezpieczeństwa w zakresie obsługiwanego systemu.
m) Lista oprogramowania niezbędnego do uruchomienia systemu/aplikacji, zawierająca nazwę oprogramowania, producenta, wersję, źródło pakietów instalacyjnych (o ile takie oprogramowanie jest wymagane).

2.2 Opis konfiguracji systemu oraz parametrów systemu w warstwie aplikacyjnej

W ramach opisu powinny zostać umieszczone informacje dotyczące parametryzacji systemu w jego warstwie aplikacyjnej, w tym:

1. Specyfikacja parametrów systemu wraz z ich opisem.
    a. Opis wpływu parametrów na działanie systemu.
    b. Opis dotyczący diagnozowania błędów programowych, sposoby śledzenia działania systemu.
2. Logowanie zdarzeń:
    a. opis dostępu do logów w warstwie aplikacji i monitorowania zdarzeń,
    b. opis dotyczący implementacji audytu historii aktywności użytkownika – szczegółowy opis zdarzeń logowanych przez system/aplikację (wykaz pól z opisem),
    c. opis możliwości eksportu logów
3. Wykaz komunikatów błędów, ostrzeżeń oraz ich opisy.
4. Opis logów, dzienników systemów zawierających odnotowanie działań użytkowników lub obiektów systemowych polegające na dostępie do:
    a. systemu z uprawnieniami administracyjnymi;
    b. konfiguracji systemu, w tym konfiguracji zabezpieczeń (w zakresie jakim dotyczy);
    c. przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
5. Opis logów, dzienników systemów zawierający działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
    a. działań użytkowników nieposiadających uprawnień administracyjnych,
    b. zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu (o ile dotyczy),
    c. zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny (o ile dotyczy).
6. Opis mechanizmu uwierzytelnienia do systemu/aplikacji przez różne grupy osób korzystających z systemu/aplikacji, wraz z opisem zabezpieczeń.

2.2. Opis zarządzania użytkownikami i uprawnieniami w systemie w warstwie aplikacyjnej

Zapisy dotyczące zarządzania użytkownikami i uprawnieniami w warstwie aplikacyjnej powinny zawierać opis zawierający:

1. Proces tworzenia i usuwania użytkowników oraz modyfikacji i odbierania uprawnień (w formie instrukcji) w warstwie oprogramowania funkcjonalnego systemu.
2. Wykaz ról, profili użytkowników (w tym administratorów) i przywilejów zdefiniowanych w systemie wraz z wykazem funkcjonalności przypisanych do danych danych ról i prawami dostępu do danych (odczyt, zapis, modyfikacja).
3. Raportowanie uprawnień użytkowników – instrukcja generowania raportów uprawnień z systemu/aplikacji jak i z poszczególnych modułów merytorycznych (o ile występują), instrukcja powinna zawierać minimum wykaz wszystkich raportów w zakresie uprawnień oraz opis sposobu ich generowania wraz z informacją o danych jakie dany raport prezentuje.
4. Opis dotyczący implementacji audytu historii aktywności użytkownika.

2.3. Opis słowników wykorzystywanych w systemie

Opis słowników powinien zawierać:

1. Listę wszystkich słowników.
2. Opis zarządzania danymi słownikowymi.
3. Opis procedury aktualizacji danych słownikowych.

2.4. Opis konfiguracji stacji roboczej lub urządzenia klienckiego dla użytkownika systemu

Opis powinien zawierać proces przygotowania i konfiguracji stacji roboczej lub urządzenia klienckiego dla użytkownika pracującego w systemie.

Opis przygotowania i konfiguracji stacji roboczej przeznaczonej do pracy w systemie powinien zawierać:

1. Listę oprogramowania, zawierającą nazwę oprogramowania, producenta, wersję, źródło pakietów instalacyjnych.
2. Wymagania sprzętowe.
3. Wymagania dotyczące systemu operacyjnego oraz dodatkowego oprogramowania ze wskazaniem wersji minimalnej.
4. Instrukcję instalacji oprogramowania.

2.3 Opis wymagań dla systemów teleinformatycznych w odniesieniu do rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Opis powinien uwzględniać wymagania zawarte w Rozporządzeniu Rady Ministrów z dn. 21.05.2024 z póz. zm. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dokumentacja systemu teleinformatycznego powinna zawierać m.in.:

1. Kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą
2. Opis formatów danych w jakim udostępniane są zasoby informacyjne zgodnie z załącznikiem nr 2 do rozporządzenia oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym.
3. Opis spełnienia wymagań Web Content Accessibility Guidelines (WCAG 2.1), z uwzględnieniem poziomu AA, określonych w określonych w Ustawie z dnia 4 kwietnia 2019 r. (z pózn. zm.) o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
4. Opis logów, dzienników systemów zawierających odnotowanie działań użytkowników lub obiektów systemowych polegające na dostępie do:
    a) systemu z uprawnieniami administracyjnymi;
    b) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
    c) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.
5. Opis logów, dzienników systemów zawierający działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
6. działań użytkowników nieposiadających uprawnień administracyjnych,
7. zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,

8. zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny.

2.4 Opis wymagań dla teleinformatycznych stron internetowych i aplikacji mobilnych w odniesieniu do Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych

1. Opis spełnienia wymagań dla aplikacji w odniesieniu do ustawy o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych w zakresie: nawigacji, funkcjonalności, kompatybilności, , postrzegalności, zrozumiałości, deklaracji dostępności, obsługi żądania zapewnienia dostępności cyfrowej.
2. Przygotowanie przez wykonawcę raportu dostępności cyfrowej dla strony internetowej lub aplikacji zgodnie z wytycznymi:
3. Raport dwóch z narzędzi weryfikujących tak zwanych walidatorów potwierdzający brak błędów w poziomach A oraz AA uwzględniających również typ błędu ARIA.
4. Raport manualny oraz wzrokowy zgodnie z wytycznymi Ministerstwa zawartymi na stronie https://www.gov.pl/web/dostepnosc-cyfrowa/jak-zbadac-czy-strona-www-jest-dostepna-cyfrowo.
5. Raport przygotowany w formie dostępnego cyfrowo pliku PDF. będzie opublikowany na stronie aplikacji jako załącznik do Deklaracji Dostępności, która musi znajdować się na stronie/aplikacji i być pierwszym elementem strony/aplikacji.

3 Licencje i gwarancje

3. 1 Licencje

Dokumentacja zawiera pełną charakterystykę licencjonowania elementów aplikacji i środowiska wykorzystanych do funkcjonowania systemu.
W dokumentacji, wykonawca zobowiązany jest przedstawić listę wszystkich licencji na dostarczone oprogramowanie wraz z opisem sposobu licencjonowania. Opis powinien dotyczyć wszystkich aplikacji wymagających licencjonowania (aplikacje, systemy operacyjne, bazy danych, urządzenia i inne).
Lista licencji na oprogramowanie powinna zawierać:

a) Producenta i nazwę oprogramowania;
b) Sposób licencjonowania (np. procesor, użytkownik; informacje o metryce, uprawnieniach, ograniczeniach),
c) Ilości, rodzaje licencji (np. enterprise, standard) oraz poziom licencji,
d) Numer licencji,
e) Termin ważności licencji,
f) Sposób odnawiania licencji

4 Procedury

4.1 Procedury eksploatacyjne

Procedury mające na celu zabezpieczenie, bieżące utrzymanie i zapewnienie wysokiej niezawodności działania systemu.

a) Przekazanie inicjalnych haseł do kont administracyjnych systemu wraz z procedurą bezpiecznej zmiany haseł (bez wpływu na funkcjonowanie systemu).
b) Procedura administracyjna zawierająca informację o okresowych zadaniach, które muszą być wykonane przez administratora itp. wraz ze ścieżkami czynności i opisem ich realizacji.

5 Dokumentacja użytkownika

Dokumentacja powinna zawierać szczegółowy opis wszelkich funkcjonalności i właściwości dostarczonego rozwiązania informatycznego, pozwalający na poprawną eksploatację aplikacji zgodnie z jej przeznaczeniem.

Instrukcja użytkownika może obejmować szereg dokumentów, z których każdy jest wydzieloną całością obejmującą obsługę albo procesu, albo modułu, albo czynności przewidziane dla roli/kategorii użytkownika.
W przypadku dokumentacji eksploatacyjnej, w której przewidziane są różne kategorie użytkowników, należy uwzględnić w instrukcji wszystkie grupy użytkowników. W przypadku dokumentacji dla użytkownika specjalnego - administratora, jej szczegółowa specyfikacja została określona w części Dokumentacja administratora.

5.1 Minimalna zawartość dokumentacji dla użytkownika powinna obejmować:

a) Wytyczne dotyczące rozpoczęcia, zawieszania i zakończenia pracy w systemie- opis uwierzytelnienia i wylogowania się z systemu, informacja o czasie trwania sesji zalogowanego użytkownika oraz blokowania systemu w czasie bezczynności
b) Instrukcję użytkownika zawierającą opis wykonywania zadań w systemie z uwzględnieniem różnych wariantów ich wykonania.
c) Szczegółowy opis funkcjonalności systemu, ścieżek obsługi procesów, z uwzględnieniem różnych wariantów ich wykonania
d) Opis ścieżek obsługi procesów.
e) Opis raportów generowanych w systemie, który powinien zawierać informacje dotyczące:
   - parametryzacji, filtrowania i innych elementów możliwych do spersonalizowania dostępnych dla użytkownika
   - proces eksportowania raportów do narzędzi zewnętrznych
f) Opis komunikatów błędu wraz z podaniem rozwiązań.
g) Przedstawienie systemu pomocy.
h) Instrukcja pracy awaryjnej.

6 Wymogi dokumentacji w odniesieniu do danych osobowych

Dokument powinien zawierać elementy odnoszące się do przetwarzania, w tym przechowywania danych osobowych (tzw. zwykłych bądź szczególnych kategorii) w rozumieniu 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 lub RODO) oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

W przypadku przetwarzania w systemie danych osobowych wymagane jest opisanie następujących elementów

1. Nazwa procesu przetwarzania danych osobowych
2. Opis celu przetwarzania danych osobowych
3. Opis kategorii danych osobowych
4. Wykaz przetwarzanych danych osobowych wraz z krótkim opisem przepływów, którym podlegają dane osobowe w bazie danych/aplikacji
5. Podstawa prawna przetwarzania
6. Wykaz lokalizacji tworzących obszar w których przetwarzane są dane osobowe (wykaz budynków, pomieszczeń lokalizacji serwerów i stacji roboczych).
7. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację praw podmiotu danych opisanych w art.12-18 i 20-22 RODO

a) udostępnienie danych podmiotowi danych,
b) możliwości realizacji prawa ograniczenia przetwarzania (prawa do sprzeciwu),
c) możliwości realizacji prawa do bycia zapomnianym,
d) możliwość realizacji prawa do otrzymania kopii danych w maszynowym formacie,
e) oznaczenia rekordów, dla których realizowane zostały wymienione wyżej prawa

8. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację
   a) informacji o odbiorcach, w rozumieniu art. 4pkt 9)RODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
   b) funkcjonalności systemu służące do wersjonowania rożnych treści zgód, treści klauzul informacyjnych, regulaminów itp.,
   c) dokumentowanie źródła pozyskania danych w systemie.
   d) wbudowania w system funkcjonalności obejmujących szyfrowanie, anonimizację danych, pseudonimizację danych, zabezpieczenia dotyczące pseudonimizacji (przechowywanie kluczy szyfrujących),
9. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację bezpieczeństwa informacji w tym poufność, integralność i rozliczalność przetwarzanych danych (ze szczególnym uwzględnieniem logów, ich zawartości, dostępu i zabezpieczeń)
10. Realizacja zasady rozliczalności w systemach informatycznych,
    a) daty pierwszego wprowadzenia danych do systemu oraz kolejnych dat ich modyfikacji,
    b) identyfikatora użytkownika wprowadzającego oraz modyfikującego dane,
    c) informacji audytowych zawierających historię poszczególnych wartości zmodyfikowanych z jednoznacznym przypisaniem ich do identyfikatora użytkownika przeprowadzającego modyfikacje w systemie
11. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację obsługi zgód (jeżeli dotyczy)
12. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację funkcjonalności „archiwum" i retencji danych, sposób realizacji w systemach informatycznych zakończenia przetwarzania w podstawowym celu,
13. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających oznaczanie podstaw prawnych przetwarzania.
14. Opisanie sposobów szyfrowania danych w transferze i spoczynku (jeżeli występuje),
15. Opisanie usuwania danych po okresie retencji danych.

7 Wymagania dodatkowe dla dokumentacji dotyczącej usług w architekturze chmury obliczeniowej

W przypadku rozwiązań opartych na modelu przetwarzania w chmurze obliczeniowej gdzie przetwarzane są dane osobowe, dostarczona dokumentacja powinna zawierać między innymi:

a) Informację o lokalizacjach serwerów na których przetwarzane są lub mogą być przetwarzane dane, z uwzględnieniem CPD głównych i zapasowych.
b) Wskazanie sposobu oraz zasad dostępu do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych.
c) Listę zawierającą podwykonawców i współpracujących instytucji mających udział w realizacji usługi chmurowej wraz ze wskazaniem roli każdego z tych podmiotów w procesie przetwarzania danych osobowych.
d) Procedurę raportowania incydentów bezpieczeństwa w zakresie powierzonych danych.

8 Wymagania dotyczące dokumentacji dla systemów w których prowadzone są księgi rachunkowe

W odniesieniu do wymagań dokumentacji odnoszącej się do systemów w których prowadzone są się księgi rachunkowe, muszą one spełniać warunki określone w Ustawie o rachunkowości (Dz. U. z 2019r. poz. 351), w szczególności w zakresie określonym w art. 10 ww. ustawy.

Wymagany minimalny zakres dokumentacji powinien obejmować:

a) Wykaz zbiorów danych tworzących księgi rachunkowe w systemie, zawierający opis ich struktury, wzajemnych powiązań oraz ich funkcji w organizacji całości ksiąg rachunkowych i w procesach przetwarzania danych.
b) Opis systemu informatycznego, zawierający wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów oraz programowych zasad ochrony danych, w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania oraz informację dotyczącą wersji oprogramowania i daty rozpoczęcia jego eksploatacji.
c) Opis systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów.