

## **Szczegółowe wymagania dotyczące dokumentacji systemu informatycznego**

### **I. Cel dokumentu**

Dokument zawiera szczegółowe wymagania dotyczące formy oraz zawartości dokumentacji dostarczanej przez Wykonawcę wraz z systemem informatycznym.

### **II . Zakres wymagań dotyczący dokumentacji**

#### **1. Uwagi i wymagania ogólne**

1. Dokumentacja powinna zostać dostarczona w wersji elektronicznej edytowalnej i dodatkowo w wersji papierowej. W związku z powyższym wersja elektroniczna powinna być dostarczona dla:
  - a) dokumentów tekstowych w formacie PDF z możliwością przeszukiwania, również wyrazów z polskimi znakami i możliwością zaznaczania kopiowania treści,
  - b) dokumentów tekstowych w formacie DOC (lub innym ogólnie dostępnym formacie edytowalnym).
2. 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.
3. Dokumentacja powinna uwzględniać zarówno środowisko produkcyjne, testowe/szkoleniowe, jak i deweloperskie systemu.
4. Zawartość dokumentacji powinna być czytelna (dotyczy grafik, wykresów, diagramów).
5. Zalecenia Zamawiającego w odniesieniu do wymagań edytorskich:
  - a) szablon dokumentu z wymaganymi elementami zgodny z standardem obowiązującym u Zamawiającego (zostanie przekazany Wykonawcy),
  - b) preferowany format dokumentacji (wielkość strony) –A4,
  - c) czcionka o kroju Verdana,
  - d) wersjonowanie dokumentacji – format wersji n.xx gdzie n oznacza numer kolejnej zatwierdzonej wersji dokumentu, xx – numer kolejnej wersji opiniowanej, roboczej.
6. W ramach dokumentacji dostarczone powinny być:
  - a) zestawienie wszystkich uzgodnień i protokołów podpisanych na etapie realizacji – Załącznik 2,
  - b) globalny rejestr zmian dotyczący dokumentacji powykonawczej – Załącznik 3,

#### **2. Opis systemu**

Opis techniczny systemu powinien obejmować:

1. Schemat blokowy systemu wraz z opisem jego składowych oraz przepływu i przetwarzania danych w systemie.
2. 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.

### 3. Dokumentacja administratora

#### 3.1. 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 użytkownika i przywilejów zdefiniowanych w systemie wraz z opisem.
3. Raportowanie uprawnień użytkowników.
4. Opis dotyczący implementacji audytu historii aktywności użytkownika.

#### 3.2. Opis konfiguracji systemu oraz parametrów systemu w warstwie aplikacyjnej (o ile występują)

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

1. Specyfikacja parametrów systemu wraz z ich opisem.
2. Opis wpływu parametrów na działanie systemu.
3. Procedura restartu umożliwiająca bezpieczne wyłączenie (zablokowanie) i włączenie (odblokowanie) systemu wraz z informacją o wpływie restartu na pozostałe elementy/moduły systemu.
4. Opis dotyczący diagnozowania błędów programowych, sposoby śledzenia działania systemu.
5. Opis logów powstających podczas pracy, wskazanie sposobu interpretacji informacji zawartej w zapisach.
6. Wykaz komunikatów błędów, ostrzeżeń oraz ich opisy.

#### 3.3. Opis słowników wykorzystywanych w systemie (o ile występują)

Opis słowników powinien zawierać:

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

#### 3.4. 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.

3.5. 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. 16.05.2016 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. Opis kodowania 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.
2. Opis formatów danych w jakim udostępniane są zasoby informacyjne zgodnie z załącznikiem nr 2 do rozporządzenia.
3. 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.
4. 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,
  - c) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny.
5. 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 późn. zm.) o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

3.6 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.

## 4. Licencje i gwarancje

### 4.1. Licencje

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:

1. Nazwę oprogramowania.
2. Sposób licencjonowania (np. procesor, użytkownik; informacje o metryce, uprawnieniach, ograniczeniach).
3. Ilości, rodzaje licencji (np. enterprise, standard) oraz poziom licencji.
4. Numer licencji.

### 4.2. Gwarancje i serwis

W ramach dokumentacji, wykonawca powinien umieścić informacje dotyczące zasad gwarancyjnych na dostarczany sprzęt/urządzenia i oprogramowanie. Dokumentacja powinna zawierać informacje dotyczące udzielanego wsparcia producenta w tym: terminy obowiązywania gwarancji, numer asysty technicznej, sposób korzystania z asysty technicznej.

Dokumentacja powykonawcza powinna zawierać opis usługi serwisowej który obejmuje:

1. Klasyfikację, kategoryzację błędów i awarii.
2. Opis procesu zgłaszania błędów i awarii.
3. Parametry świadczenia usługi serwisowej
  - a) okres dostępności serwisu gwarancyjnego,
  - b) czas reakcji serwisu w odniesieniu do poszczególnych kategorii błędów i awarii,
  - c) czas realizacji/usunięcia błędu (dla awarii czas przywrócenia funkcjonalności oraz czas przywrócenia stanu z przed awarii).

## 5. Procedury

### 5.1. Procedury eksploatacyjne

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

1. Przekazanie inicjalnych haseł do kont administracyjnych systemu wraz z procedurą bezpiecznej zmiany haseł (bez wpływu na funkcjonowanie systemu).

## 6. Dokumentacja użytkownika

W przypadku dokumentacji eksploatacyjnej, w której przewidziane są różne kategorie użytkowników, należy uwzględnić instrukcje dla wszystkich grup użytkowników. Minimalna zawartość dokumentacji dla użytkownika powinna obejmować:

1. Instrukcję rozpoczęcia, zawieszania i zakończenia pracy w systemie.
2. Instrukcję użytkownika zawierającą opis wykonywania zadań w systemie z uwzględnieniem różnych wariantów ich wykonania.
3. Szczegółowy opis funkcjonalności systemu.

4. Opis ścieżek obsługi procesów.
5. Dokładny opis raportów generowanych w systemie. Opis powinien zawierać informacje dotyczące parametryzacji, filtrowania i innych elementów personalizacyjnych dostępnych dla użytkownika oraz proces eksportowania raportów do narzędzi zewnętrznych.
6. Opis komunikatów błędów wraz z podaniem rozwiązań.
7. Przedstawienie systemu pomocy.
8. Instrukcja pracy awaryjnej.
9. Szkolenie w wersji elektronicznej, w formie pozwalającej na przeprowadzenie szkolenia w oprogramowaniu (Moodle), wraz z prawem licencyjnym pozwalającym w szczególności na:
  - a) swobodne wykorzystanie przekazanych materiałów w ramach kursu na potrzeby szkoleniowe, w zakresie w jakim CUI uzna za stosowne,
  - b) swobodną ingerencję dotyczącą zawartości kursu w tym zawartości merytorycznych jak i treści, materiałów graficznych i audiowizualnych zawartych w przekazanym kursie.

#### 7. Wymogi dokumentacji w odniesieniu do danych osobowych

Informacje dotyczące przetwarzanych danych osobowych powinny zostać zebrane w osobnym dokumencie poświęconemu temu zagadnieniu.

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. Wykaz lokalizacji tworzących obszar, w których przetwarzane są dane osobowe (wykaz budynków, pomieszczeń lokalizacji serwerów i stacji roboczych).
2. Wykaz zasobów/procesów/zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
3. Opis struktury zasobów/procesów/zbiorów danych wraz ze schematem wskazującym zawartość poszczególnych pól informacyjnych i powiązania między nimi. Minimalny zakres powinien zawierać:
  - schemat bazy danych,
  - nazwy tabel,
  - nazwy pól,
  - właściwości pól,
  - opisane klucze główne i/lub obce.
4. Logiczną interpretacją danych jak również sposób przepływu danych pomiędzy poszczególnymi systemami/podsystemami na poziomie szczegółowości określonej w podpunkcie 2.
5. Opis dostarczonych rozwiązań technicznych oraz organizacyjnych zapewniających realizację praw podmiotu danych opisanych w art.12-18 i 20-22 RODO w tym poufność, integralność i rozliczalność przetwarzanych danych z uwzględnieniem:

- a) Opisu zawierającego implementację realizacji przez system automatycznego zapisywania zatwierdzonych w systemie danych wraz z wskazaniem miejsca przechowywania informacji w systemie (na poziomie szczególności określonym w podpunkcie 2):
- realizacja zasady rozliczalności w systemach informatycznych,
    - daty pierwszego wprowadzenia danych do systemu oraz kolejnych dat ich modyfikacji,
    - identyfikatora użytkownika wprowadzającego oraz modyfikującego dane,
    - informacji audytowych zawierających historię poszczególnych wartości zmodyfikowanych z jednoznacznym przypisaniem ich do identyfikatora użytkownika przeprowadzającego modyfikację w systemie,
  - informacji o odbiorcach, w rozumieniu art. 4 pkt 9) RODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
  - funkcjonalności systemu służące do wersjonowania różnych treści zgód, treści klauzul informacyjnych, regulaminów itp.,
  - dokumentowanie źródła pozyskania danych w systemie.
  - możliwości realizacji prawa ograniczenia przetwarzania (prawa do sprzeciwu),
  - możliwości realizacji prawa do bycia zapomnianym,
  - możliwość realizacji prawa do otrzymania kopii danych w maszynowym formacie,
  - wbudowania w system funkcjonalności obejmujących szyfrowanie, anonimizację danych, pseudonimizację danych, zabezpieczenia dotyczące pseudonimizacji,
  - funkcjonalności „archiwum”, sposób realizacji w systemach informatycznych zakończenia przetwarzania w podstawowym celu, (okresy retencji),
- b) Opisu zawierającego mechanizm logowania do systemu i przechowywania historii logowań do systemu zawierający wskazanie miejsca przechowywania informacji dotyczących:
- Datę prób logowań do systemu z informacją o udanym lub nie procesie logowania przez użytkownika,
  - Identyfikator użytkownika,
  - Adres IP urzędnika z którego nastąpiło zalogowanie/próba logowania.
- c) Wykaz uprawnień – ról, profili dających dostęp do danych osobowym lub wrażliwych z wyszczególnieniem praw dostępowych do danych (odczyt, zapis, modyfikacja).
- d) Zapis potwierdzający implementację w systemie automatycznego mechanizmu wymuszającego zmianę hasła przez użytkownika co 30 dni.
- e) Opis zawierający dostęp do funkcjonalności umożliwiającej sporządzenie raportu i jego wydruk w zakresie informacji wskazanych w podpunktach a, b oraz c (w przypadku podpunktu c raport umożliwiający wygenerowanie raportu na poziomie poszczególnych użytkowników).
- f) Opis elementów programowych i sprzętowych zabezpieczający system informatyczny przed działaniem szkodliwego oprogramowania oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.

g) Opis zawierający wyszczególnienie realizacji pozostałych wymogów odnoszących się do środków technicznych i organizacyjnych dla poziomu bezpieczeństwa zdefiniowanym na poziomie wysokim:

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:
  - a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
  - b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

#### 8. 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:

1. Informację o lokalizacjach serwerów na których przetwarzane są lub mogą być przetwarzane dane, z uwzględnieniem CPD głównych i zapasowych.
2. Wskazanie sposobu oraz zasad dostępu do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych.
3. 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.
4. Procedurę raportowania incydentów bezpieczeństwa w zakresie powierzonych danych.