

## **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 podlegającym modyfikacji.

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

#### **1. Uwagi i wymagania ogólne**

1. Dokumentacja powinna zostać dostarczona w wersji elektronicznej, w tym w postaci plików .pdf lub innych powszechnie używanych formatach dokumentów tekstowych, np. .doc, .docx. Dostarczona dokumentacja musi mieć możliwość otwarcia w powszechnie dostępnym oprogramowaniu oraz przeszukiwania tekstu, w tym przeszukiwania wyrazów z polskimi znakami.
2. W przypadku diagramów, schematów dostarczonych w ramach dokumentacji powinny one być dostarczone i zapisane w formacie umożliwiającym ich przeglądanie w dostępnych publicznie i darmowych narzędziach lub w formacie Office.

Zamawiający oczekuje, że w przypadku gdy Wykonawca dostarczy diagramy, schematy w ramach dostarczonej dokumentacji, to Zamawiający będzie miał możliwość zapoznania się z ich treścią oraz będzie mógł je wykorzystać w trakcie obowiązywania usług utrzymania do wykonywania działań leżących po stronie Zamawiającego. Zamawiający nie dysponuje każdym oprogramowaniem dostępnym na rynku, które pozwoli otworzyć każdy format dokumentu.

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.

3. Dokumentacja powinna uwzględniać zarówno środowisko produkcyjne, testowe/szkoleniowe, jak i deweloperskie systemu o ile dane środowisko zostanie dostarczone. W przypadku braku środowiska testowego/szkoleniowego, deweloperskiego, dokumentacja powinna uwzględniać wyłącznie środowisko produkcyjne.
4. Zawartość dokumentacji powinna być czytelna (dotyczy grafik, wykresów, diagramów).
5. W odniesieniu do wymagań edytorskich dostarczona dokumentacja będzie zgodna z zaleceniami przygotowywania dokumentów dostępnych cyfrowo w oparciu o wytyczne: <https://www.gov.pl/attachment/62e46d8f-8472-4c05-87b9-00eecbec6374>, w tym obowiązującymi przepisami dot.

dostępności cyfrowej, w celu zapewnienia możliwości przeglądania dokumentacji przez osoby z niepełnosprawnościami.

## 2. Opis systemu

Opis techniczny Systemu zawierający minimum schemat blokowy Systemu z opisem modułów i przepływu danych pomiędzy modułami.

## 3. Dokumentacja administratora

3.1. Opis zarządzania użytkownikami i uprawnieniami w systemie w warstwie aplikacyjnej uwzględniający wszelkie zmiany dokonane w systemie.

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 stacji roboczej lub urządzenia klienckiego dla użytkownika systemu

Opis konfiguracji stacji roboczej lub urządzenia klienckiego dla użytkownika Systemu. Opis konfiguracji powinien określać minimalne wymagania dla stacji roboczych, niezbędne do korzystania z oprogramowania oraz wykaz niezbędnych, zainstalowanych na stacji roboczej komponentów (wraz z ich minimalną wersją) w celu możliwości wykonania czynności przez użytkowników (w tym wygenerowania, otworzenia i drukowania raportów).

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

Opis powinien uwzględniać wymagania zawarte w Rozporządzeniu w sprawie Krajowych Ram Interoperacyjności z dnia 05.12.2017 r., (Dz.U.2017,2247 z późn. zm.) i 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. Nazwy systemów kodowania znaków stosowanych w dokumentach generowanych z wdrażanego Systemu oraz w przypadku, gdy dane są wymieniane z innymi systemami na drodze teletransmisji nazwy systemów kodowania znaków w odniesieniu do informacji wymienianych pomiędzy systemami.

Zamawiający oczekuje wskazania przez Wykonawcę systemu lub systemów kodowania znaków jakie Wykonawca zaimplementował w

systemie w zakresie wymiany informacji pomiędzy innymi systemami oraz w dokumentach generowanych z systemu.

Systemy, pomiędzy którymi Zamawiający zamierza wymieniać dane zostały wskazane w OPZ. Wymiana danych wskazana jest m.in. w OPZ w wymaganiu FK.02, FK.03, WT.24, SP.13, SP.85, SP.88, SP.89, SP.95, SP.38, FK.56, FK.92.

Wymagania w zakresie standardów kodowania znaków określa Rozporządzenie w sprawie Krajowych Ram Interoperacyjności z dnia 05.12.2017 r., Dz.U.2017,2247 z późniejszymi zmianami.

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,

## 5. Procedury

### 5.1. Procedury eksploatacyjne

Procedury eksploatacyjne - instrukcja sposobu bezpiecznej zmiany przekazanych haseł inicjalnych do Systemu.

## 6. Dokumentacja użytkownika – minimalny zakres

1. Sposób logowania i wylogowania się użytkownika z Systemu, opis zmiany hasła przez użytkownika do Systemu.
2. Instrukcja (lub podręcznik) użytkownika zawierająca opis wykonywania zadań w systemie z uwzględnieniem różnych wariantów ich wykonania.
3. Opis wykonania czynności przez użytkownika w Systemie (opis dostępnych funkcjonalności w Systemie) oraz opis ścieżek wykonania procesów w Systemie.
4. Wykaz i opis dostępnych dla użytkownika raportów w Systemie wraz z informacjami dot. ich parametryzacji (opisane warunki początkowe), filtrowania i innych parametrów personalizacyjnych, dostępnych dla użytkownika w Systemie. W przypadku gdy opis parametrów jest wskazany w formacie raportu, wymaganie będzie spełnione.

## 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 w których przetwarzane są dane osobowe wraz ze wskazaniem programów/modułów/podsystemów zastosowanych do przetwarzania tych danych.
3. Opis struktury 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 szczegółowości 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 modyfikacje w systemie,

- informacji o odbiorcach, w rozumieniu art. 4pkt 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 urządzenia 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).
6. Opis zastosowanych metod i środków uwierzytelniania.
7. Opis elementów programowych i sprzętowych zabezpieczający system informatyczny przed działaniem szkodliwego oprogramowania oraz oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.
8. Opis zabezpieczeń chroniących przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

## 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. 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.
3. Procedurę raportowania incydentów bezpieczeństwa w zakresie powierzonych danych.