

**Opis przedmiotu zamówienia na:**  
**SYSTEM DO WSPARCIA PROCESÓW RODO ORAZ ZARZĄDZANIA UPRAWNIENIAM**  
zgodny z

ROZPORZĄDZENIEM 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)

**1. System posiada następującą architekturę:**

- 1.1. Konsola administracyjna – w postaci w pełni funkcjonalnej aplikacji internetowej (webowej) pozwalająca na realizację pełnego zarządzania aplikacją oraz wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca wbudowane mechanizmy raportowania.
- 1.2. System aktualizuje konsolę administracyjną, bazę danych, słowniki, raporty i inne komponenty w sposób w pełni automatyczny za pośrednictwem bezpiecznego połączenia z serwerami aktualizacji producenta systemu w czasie nie dłuższym niż 24h od wydania przez producenta nowej wersji. W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne jest możliwość dokonania aktualizacji manualnej poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
- 1.3. System umożliwia logowanie do konsoli w sieciach lokalnych i rozległych.
- 1.4. System umożliwia bezproblemową i stabilną obsługę co najmniej 100 jednocześnie zalogowanym administratorom/ użytkownikom (osoby uzyskujące dostęp do danych w systemie).
- 1.5. System pozwala na instalację z poziomu pojedynczego instalatora MSI.
- 1.6. System umożliwia instalację w środowisku Windows oraz Linux.
- 1.7. System umożliwia instalację rozłożoną na dwa osobne serwery – aplikacyjny i bazodanowy.
- 1.8. System nie wymaga instalacji na urządzeniach końcowych.
- 1.9. System umożliwia przeniesienie instalacji do chmury.

**2. Wymagania systemowe:**

- 2.1. Konsola administracyjna działa na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).
- 2.2. Serwer www jest oparty o platformę: Linux Debian 11, oraz Java 8 (JRE lub JDK), Apache Tomcat 8.5.
- 2.3. Baza danych działa na silniku PostgreSQL w wersji 10 lub wyższej.

**3. Interfejs**

- 3.1. System umożliwia wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- 3.2. Import obiektów z MS Active Directory jest odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas importu zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
- 3.3. System umożliwia import danych z zewnętrznego pliku CSV, Excel, Microsoft SQL, MySQL, PostgreSQL. System umożliwia zaimportowanie : jednostek organizacyjnych, użytkowników, wnioskodawców, zbiorów, podmiotów, programów i zasobów, rejestru czynności przetwarzania,

rejestru klauzul informacyjnych, rejestru zgód, rejestru żądań podmiotów danych, rejestru upoważnień.

- 3.4. System posiada wbudowany, w pełni definiowalny przez administratora interfejs do importu danych. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.

#### 4. Funkcjonalności systemu

- 4.1. System wspiera wszystkie procesy wymagane ROZPORZĄDZENIEM 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).
- 4.2. System zapewnia prowadzenie następujących rejestrów:
- a) rejestr czynności przetwarzania z możliwością wskazania : nazwy czynności przetwarzania, celu przetwarzania, kategorii osób, kategorii danych, podstawy prawnej przetwarzania, źródła danych, planowanego terminu usunięcia danych, nazwy administratora/ów wraz z danymi kontaktowymi, nazwy współadministratora/ów wraz z danymi kontaktowymi, danych IOD wraz z danymi kontaktowymi, danych przedstawiciela, kategorii odbiorców, nazwy systemów lub oprogramowania, zbiorów, analityki danych, ogólnych opisów środków bezpieczeństwa, transferu do kraju trzeciego lub org. międzynarodowej, załączników, możliwość importu archiwalnych rejestrów
  - b) rejestr kategorii czynności przetwarzania z możliwością wskazania : kategorii przetwarzania, ogólnych opisów środków bezpieczeństwa, nazwy administratora/ów wraz z danymi kontaktowymi, danych IOD wraz z danymi kontaktowymi, danych przedstawiciela, nazwy współadministratora/ów wraz z danymi kontaktowymi, danych podprocesora/ów wraz z danymi kontaktowymi, czasu trwania przetwarzania, nazwy państw trzecich lub org. Międzynarodowych do których dane są przekazywane, zbiorów, analityki danych, kategorii danych, kategorii osób, nazwy systemów lub oprogramowania, okresu przetwarzania, podstawy prawnej przetwarzania, planowanego terminu usunięcia danych, zasad zakończenia współpracy, załączników, możliwość importu archiwalnych rejestrów
  - c) ewidencja incydentów naruszenia ochrony danych osobowych : dostosowany pod formularz zgłoszeń incydentów przesyłany do Prezesa Urzędu Ochrony Danych z możliwością przeprowadzenia oceny wagi naruszenia.
  - d) rejestr umów powierzenia z możliwością wskazania : przedmiotu umowy powierzenia, daty umowy, numeru umowy, administratora danych powierzającego wraz z danymi kontaktowymi, danych IOD wraz z danymi kontaktowymi, danych przedstawiciela, podmiotu przetwarzającego, nazwy państw trzecich lub org. Międzynarodowych do których dane są przekazywane, okresu powierzenia, zbiorów, powierzonych czynności, analityki danych, kategorii danych, kategorii osób, kategorii odbiorców, ogólnych opisów środków bezpieczeństwa, planowanego terminu usunięcia danych, załączników, możliwość importu archiwalnych rejestrów
  - e) rejestr upoważnień z funkcją generowania upoważnień z możliwością wskazania : pracownika/ grupy pracowników, czynności przetwarzania, zbiorów, daty upoważnienia, daty ważności upoważnienia, podstawy zatrudnienia, zakresu upoważnienia, załączników. Rejestr upoważnień pozwala na : zbiorcze wygenerowanie zestawienia osób uprawnionych do przetwarzania danych osobowych, wygenerowanie upoważnienia do przetwarzania danych osobowych dla pojedynczego pracownika bądź grupy pracowników, odebranie upoważnienia w dowolnym momencie jego trwania ze wskazaniem na datę odebrania oraz jego powód, na wprowadzenie notatki ze sprawdzeń dokonanych przez IOD.
  - f) rejestr żądań podmiotów danych z możliwością wskazania : wnioskodawcy, danych pełnomocnika, bieżącego procesu, daty wpływu żądania, kanału wpływu, kodu żądania, podstawy prawnej, zbiorów danych, treści wniosku, kanału odpowiedzi, załączników.
  - g) rejestr udostępnień danych osobowych z możliwością wskazania : daty udostępnienia, podmiotu udostępniającego wraz z danymi kontaktowymi, sposobu udostępnienia,

- podmiotu któremu dane zostały udostępnione, zbiorów, zakresu udostępnienia, celu udostępnienia, podstawy prawnej, załączników
- h) rejestr zgód z możliwością wskazania : osoby/podmiotu od którego zgoda została pozyskana wraz z danymi kontaktowymi, kanału pozyskania zgody, nazwy zgody, kategorii zgody, treści zgody, podkategorii, daty udzielenia zgody, daty obowiązywania zgody, daty wycofania zgody, kanału wycofania zgody, powodu wycofania zgody, załączników
  - i) rejestr klauzul informacyjnych z możliwością wskazania : podstawy prawnej ,nazwy obowiązku, administratora/ów danych wraz danymi przedstawiciela oraz IOD, współadministratora/ów wraz z danymi kontaktowymi, celu przetwarzania, czynności przetwarzania, podstawy prawnej przetwarzania, kategorii danych, źródła pozyskania danych, źródła pochodzenia danych, zbiorów danych, okresu retencji, praw i konsekwencji, odbiorców danych, kategorii odbiorców, przekazania danych do państwa trzeciego lub org. Międzynarodowej, informacji odnośnie zautomatyzowanym podejmowaniu decyzji, profilowaniu.
- 4.3. System „pilnuje” terminów procesowania żądać podmiotów danych i przypomina o upływie terminów.
  - 4.4. „pilnuje” terminów ważności upoważnień do przetwarzania danych i przypomina o System upływie terminów.
  - 4.5. System pozwala na procesowanie : upoważnień do przetwarzania danych osobowych, dostępów do systemów informatycznych, zasobów z dowolnie zdefiniowaną ścieżką akceptacji.
  - 4.6. System zapewnia rejestrowanie zdarzeń o użytkownikach, które utworzyły np.: aktywo informacyjne, obszar przetwarzania, czynność przetwarzania, a także o osobach, które dokonywały modyfikacji każdego z tych obiektów.
  - 4.7. System zapewnia prezentowanie informacji o uprawnieniach osoby i ich zmianach w czasie.
  - 4.8. System zapewnia prezentowanie zmian wprowadzonych w obrębie rejestrów oraz incydentów.
  - 4.9. System pozwala na prowadzenie kalendarza zadań dla IOD oraz ASI.
  - 4.10. System umożliwia wykonanie analizy ryzyka oraz DPIA (ocena skutków przetwarzania danych osobowych). W systemie zastosowana została metoda zarządzania ryzykiem w systemach zarządzania bezpieczeństwem informacji w urzędach administracji rządowej w zakresie zagrożeń pochodzących z cyberprzestrzeni, rekomendowanej przez Komitet Rady Ministrów ds. Cyfryzacji w listopadzie 2015 r. oraz metoda rozszerzonej analizy ryzyka wg PN-ISO/IEC-27005. Definiowalny mechanizm ryzyka (prawdopodobieństwo oraz skutek) uwzględniają : zakres, cele przetwarzania, rodzaj danych, atrybut, zagrożenia, opis podatności, zabezpieczenia, decyzję, uzasadnienie akceptacji poziomu ryzyka oraz zalecenia.
  - 4.11. System posiada wbudowany system obsługi wniosków pozwalający na : zarządzanie obiegiem wniosków (wnioski o rejestrację/wyrejestrowanie pracownika, wnioski o nadanie dostępu do systemu informatycznego, wnioski o wydanie upoważnienia do przetwarzania danych, wnioski o odebranie uprawnień do systemu informatycznego, wnioski o odebranie upoważnień do przetwarzania danych osobowych), kontrolę uprawnień, powiadomienia e-mail o utworzonym wniosku, przegląd uprawnień bieżących i archiwalnych, akceptację wniosków przez e-mail.
  - 4.12. System posiada niezbędne słowniki pozwalające na wykorzystanie ich zawartości podczas eksploatacji systemu. Wbudowane słowniki posiadają w pełni modyfikowalne treści.  
Dostępne słowniki :
    - o administrator danych (nazwa administratora; imię i nazwisko; dane kontaktowe),
    - o współadministrator danych (nazwa administratora, imię i nazwisko, dane kontaktowe),
    - o analityka danych (podział danych ze względu na ich typ),
    - o analiza ryzyka: zagrożenia (nazwa zagrożenia, opis),
    - o cel przetwarzania (cel przetwarzania),
    - o charakter naruszenia (charakter naruszenia),
    - o czynności przetwarzania (nazwa czynności przetwarzania, opis)
    - o grupy lokalizacji (grupa lokalizacji, opis, lista lokalizacji objętych grupą),
    - o jednostki organizacyjne (z możliwością wskazania na dyrektora, kierownika, zastępcę oraz osobę wybraną do akceptacji, daty powstania jednostki, daty ustania jednostki),
    - o kanały (nazwa kanału, opis),
    - o kategorie danych (rodzaj kategorii danych, opis),

- o kategorie odbiorców (nazwa kategorii odbiorców, opis),
  - o kategorie osób (kategorie osób, opis),
  - o konsekwencje (konsekwencje),
  - o kontenery załączników (nazwa kontenera, opis),
  - o lokalizacje (z możliwością wskazania: lokalizacji nadrzędnej, zabezpieczeń fizycznych, organizacyjnych oraz technicznych stosowanych w lokalizacjach, grup lokalizacji, osób odpowiedzialnych za daną lokalizację, programów i zasobów wykorzystywanych w danej lokalizacji, informacji odnośnie sprawdzeń dokonanych przez IOD, wprowadzenia załączników),
  - o macierz ryzyka (poziom ryzyka - modyfikacja parametrów, prawdopodobieństwo – modyfikacja parametrów, skutki -modyfikacja parametrów),
  - o obowiązki (nazwa obowiązku, opis),
  - o okoliczności naruszenia (opis naruszenia),
  - o podprocesory danych (nazwa, imię i nazwisko, dane kontaktowe),
  - o podstawy do zaprzestania przetwarzania danych (podstawa prawna),
  - o podstawy prawne (podstawa prawna),
  - o procesy żądania (nazwa procesu, status, opis),
  - o przyczyny naruszenia (przyczyny naruszenia),
  - o rejestr upoważnień: form przetwarzania (forma przetwarzania, opis),
  - o rejestr zgód: kanały pozyskania (kanał pozyskania, opis),
  - o rejestr zgód: kategorie (kategoria, opis),
  - o rejestr zgód: podkategorie (kategoria, podkategoria, opis),
  - o rejestr zgód: treści zgód (kategoria, nazwa, treść),
  - o rodzaje programów i zasobów (rodzaj, opis),
  - o rodzaje żądań (kod, nazwa, kategoria, opis),
  - o sposoby udostępnienia (sposób udostępniania, opis),
  - o statusy incydentów (status, opis),
  - o środki bezpieczeństwa (środek bezpieczeństwa, opis),
  - o typy czynności przetwarzania (typ czynności, opis),
  - o typy danych (typ danych, opis),
  - o typy zabezpieczeń (typ zabezpieczeń, opis),
  - o typy załączników (typ, opis),
  - o wnioskodawcy (imię i nazwisko, pesel, kod pocztowy, miasto, ulica, adres korespondencyjny, telefon, e-mail, pełnomocnik, pełnomocnik-kod pocztowy, pełnomocnik-miasto, pełnomocnik-ulica, pełnomocnik-adres korespondencyjny, pełnomocnik-telefon, pełnomocnik-e-mail),
  - o zabezpieczenia (typ zabezpieczenia, zabezpieczenie, opis),
  - o zasady zakończenia współpracy (zasady zakończenia współpracy, opis),
  - o źródła pochodzenia danych (źródło pochodzenia danych, opis),
  - o źródła pozyskania danych (źródło, opis)
- 4.13. System umożliwia pracę na profilach – wersja IOD. Profil to wydzielony komplet danych związanych z prowadzeniem rejestrów wymaganych Rozporządzeniem, fizycznie odseparowanych i możliwych do przeniesienia oraz uruchomienia jako wydzielona instancja aplikacji RODOprotektor. W aplikacji RODOprotektor może być aktywowana dowolna liczba jednocześnie działających profili. Całkowita liczba profili jest ograniczona głównie kluczem subskrypcyjnym (licencyjnym).
- 4.14. System posiada panel administratora oraz panel użytkownika – tzw. dashboard pokazujący stan zadań do wykonania przypadający zalogowanemu administratorowi/użytkownikowi, liczbę incydentów bezpieczeństwa w różnych przekrojach czasowych, liczbę utworzonych rejestrów czynności, kategorii, umów powierzenia, żądań podmiotów danych oraz upoważnień wygasających i wygaśniętych w różnych przekrojach czasowych.
- 4.15. System umożliwia i zapamiętuje w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widżety, ich konfigurację i kolejność).

- 4.16. Dane prezentowane na wszystkich widokach/zakładkach w systemie mają możliwość dynamicznego filtrowania w oparciu o reguły utworzone przez dowolnego użytkownika systemu.
- 4.17. Konsola umożliwia wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).
- 4.18. Raportowanie i eksport danych
  - 4.18.1. System umożliwia wyeksportowanie wybranych lub wszystkich danych do formatu do PDF, XPS, HTML, pliku tekstowego, RTF, Word, OpenDocument, Excel, Calc oraz jako pliku z danymi lub obrazem.
  - 4.18.2. System ma możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
  - 4.18.3. System posiada możliwość modyfikacji i tworzenia nowych raportów w samej aplikacji za pośrednictwem przeglądarkowego edytora raportów.
  - 4.18.4. System posiada wbudowane wykresy, które można dostosować przy użyciu szerokiej gamy opcji, zarówno w wyglądzie jak i w działaniu.
  - 4.18.5. System umożliwia generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
  - 4.18.6. System pozwala na pełną dowolność w kreowaniu zapytań SQL wraz z parametrami.
  - 4.18.7. System umożliwia skomplikowane operacje na tekście i liczbach.
  - 4.18.8. Generowanie raportu odbywa się po stronie serwera a nie klienta.
  - 4.18.9. System umożliwia wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).
  - 4.18.10. System obsługuje raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
  - 4.18.11. System umożliwia grupowanie danych oparte o rodzaj nagłówek oraz stopek.
  - 4.18.12. System posiada możliwość obsługi i umieszczania podraportów wraz z możliwością przekazania parametrów.
  - 4.18.13. System posiada niezbędne raporty dotyczące kluczowych obszarów (rejestrów) RODO.

## **5. Dodatkowe wymagania funkcjonalne**

Korzystanie z systemu:

- 5.1. system zainstalowany na serwerze Zamawiającego (on-premise) (dostęp dla użytkowników przez przeglądarki internetowe),
- 5.2. Możliwość obsługi wielu kont podmiotów w ramach jednej instalacji. Każdy użytkownik może być przypisany do dowolnej liczby kont podmiotów i w każdym posiadać różne uprawnienia. Uprawnienia dla każdego z kont użytkownika zarządzane przez podmiot, dla którego założono konto bez konieczności ingerencji podmiotu, w którym zainstalowano system. Fizyczna separacja kont podmiotów z możliwością kopiowania danych między podmiotami.

## **6. Bezpieczeństwo**

- 6.1. System wyposażony jest w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
- 6.2. System umożliwia zablokowanie komunikacji z serwerem producenta w celu wyłączenia aktualizacji.
- 6.3. System umożliwia dostarczenie aktualizacji w formie offline.
- 6.4. Uwierzytelnianie do systemu jest realizowane:
  - 6.4.1. Z wykorzystaniem imiennego konta użytkownika i hasła;
  - 6.4.2. Z wykorzystaniem imiennego konta administratorów aplikacji i hasła;
  - 6.4.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej;

- 6.4.4. Za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory.
- 6.4.5. Za pośrednictwem kont LDAP
- 6.4.6. Za pośrednictwem kont CAS
- 6.5. System umożliwia definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, wyposażony jest w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
- 6.6. Lista użytkowników / administratorów systemu jest importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.
- 6.7. System udostępnia historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.
- 6.8. System posiada mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz może udostępniać informacje o rezultacie wykonania kopii.
- 6.9. System pobiera dane z widoków (ang. View) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
- 6.10. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
- 6.11. System zapewnia mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

## **7. Wdrożenie:**

- 7.1. Dostawca uruchomi System w wariantcie on-premise za zasobach Zamawiającego,
- 7.2. Wdrożenie powinno nastąpić w ciągu max 1 dnia roboczego od dnia podpisania umowy.

## **8. Szkolenia.**

W ramach 48 miesięcznej subskrypcji Wykonawca gwarantuje nie limitowe, na żądanie Zamawiającego zdalne szkolenia administracyjne oraz użytkowe.

## **9. Wsparcie**

- 9.1. Opieka serwisowa: 48 miesięcy od dnia podpisania protokołu odbioru bez zastrzeżeń.  
W ramach usługi opieki serwisowej Wykonawca zobowiązuje się do realizacji następujących usług:
  - 9.1.1. wsparcia telefonicznego oraz mailowego, Wykonawca gwarantuje telefoniczne oraz mailowe wsparcie w języku polskim dostępne w dni robocze od godziny 7:00 do 15:00 zapewnione przez producenta Oprogramowania
  - 9.1.2. usług serwisowych, które obejmują:
    - o możliwość zgłaszania przez Zamawiającego usterek lub nieprawidłowości w funkcjonowaniu Oprogramowania poprzez adres e mail;
    - o szczegółową analizę przypadków (logów) zgłoszonych przez Użytkownika,
    - o czas reakcji Wykonawcy na zgłoszenie Użytkownika nie dłuższy niż następny dzień roboczy,
    - o w przypadku problemu z aplikacją Wykonawca zapewnia rozwiązanie problemu nie później niż na 2 dzień roboczy od dnia zgłoszenia, przy czym dzień zgłoszenia nie podlega wliczeniu do ww. terminu.
  - 9.1.3 aktualizacji Oprogramowania na zasadzie możliwości użytkownika wszelkich aktualizacji oprogramowania Wykonawcy, które będą miały miejsce w czasie obowiązywania niniejszej Umowy, w tym aktualizacji Systemu.