

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest usługa dostępu do platformy do badania: kompetencji miękkich, oceny pracowniczej, ścieżki kariery wraz ze wsparciem technicznym dla Centrum e-Zdrowia.

1. Przedmiot Zamówienia:

- 1.1. Przedmiotem zamówienia jest usługa dostępu do Platformy, wdrożenie, konfiguracja, integracja z ATS Zamawiającego, utrzymanie systemu klasy Human Capital Management (HCM), wspierającego zarządzanie zasobami ludzkimi oraz procesami HR w organizacji.
- 1.2. System musi umożliwiać centralne zarządzanie danymi pracowniczymi, kompetencjami, procesami rozwojowymi, oceną pracowników oraz dostarczać dane analityczne wspierające podejmowanie decyzji kadrowych i organizacyjnych, podejmowanych wyłącznie przez upoważnione osoby Zamawiającego, bez zautomatyzowanego podejmowania decyzji w rozumieniu art. 22 RODO.
- 1.3. Cena nie może ulec zmianie podczas trwania umowy, bez względu na ilość użytkowników.
- 1.4. Warunki płatności: 30 dni od dnia doręczenia prawidłowo wystawionej faktury VAT lub rachunku do siedziby Zamawiającego.
- 1.5. Świadczenie usługi przez okres 12 miesięcy z możliwością przedłużenia na kolejne 12 miesięcy w ramach prawa opcji.
- 1.6. Uruchomienie platformy nastąpi po 24 godzinach od podpisania umowy.
- 1.7. Wdrożenie systemu, system musi zapewniać:
 - 1.7.1. Przeprowadzenie analizy przedwdrożeniowej o charakterze biznesowym, obejmującej identyfikację wymagań użytkowników, analizę procesów biznesowych oraz określenie sposobu wykorzystania systemu w organizacji.
 - 1.7.2. Konfigurację systemu, zgodnie z wymaganiami Zamawiającego, obejmującą dostosowanie parametrów, uprawnień, słowników oraz innych elementów niezbędnych do uruchomienia i eksploatacji rozwiązania.
 - 1.7.3. Migrację danych, obejmującą przygotowanie, import oraz weryfikację poprawności danych przenoszonych z dotychczas wykorzystywanych systemów lub źródeł danych. Migracji podlegają wyłącznie dane wskazane przez Zamawiającego, niezbędne do realizacji procesów kompetencyjnych, ocen pracowniczych, rozwoju, onboardingu i ścieżek kariery. Dane przekazywane są z wykorzystaniem szyfrowanego kanału. Pliki i kopie robocze wykorzystane do migracji Wykonawca usuwa niezwłocznie po jej zakończeniu i potwierdza ich usunięcie Zamawiającemu
- 1.8. Wykonawca przeprowadzi instruktaż z zakresu korzystania z narzędzia dla administratorów biznesowych. Liczba uczestników szkolenia nie przekroczy 100 osób.
- 1.9. W ramach realizacji zamówienia Wykonawca zapewni wsparcie powdrożeniowe świadczone po uruchomieniu produkcyjnym rozwiązania. Wsparcie będzie realizowane w trybie zdalnym, z zachowaniem wymagań określonych w pkt 7.5 i 14,

i obejmie obsługę zgłoszeń, konsultacje dla administratorów biznesowych oraz pomoc w rozwiązywaniu problemów związanych z eksploatacją wdrożonego narzędzia.

- 1.10. Zapewnienie usług wsparcia technicznego (Help Desk) oraz opieki serwisowej dla użytkowników i administratorów systemu, świadczonych w dni robocze od poniedziałku do piątku w godzinach 8:00-17:00.

2. Wymagania Funkcjonalne, system musi umożliwiać:

- 2.1. Prowadzenie elektronicznych profili pracowników, umożliwiającą implementację danych za pośrednictwem ATS Zamawiającego;
- 2.2. Gromadzenie danych osobowych i kompetencyjnych i kompetencyjnych pracowników wyłącznie w zakresie niezbędnym do realizacji procesów kompetencyjnych, ocen pracowniczych, rozwoju, onboardingu i ścieżek kariery, dane organizacyjne, dane dotyczące kompetencji, celów rozwojowych i ocen pracowniczych oraz wyniki badań kompetencyjnych. System musi umożliwiać Zamawiającemu konfigurację katalogu pól, w tym wyłączenie pól zbędnych, i nie może wymagać wprowadzenia danych kadrowo-płacowych ani danych szczególnych kategorii;
- 2.3. Prezentowanie struktury organizacyjnej wraz z relacjami służbowymi;
- 2.4. Wyszukiwanie i filtrowanie danych pracowniczych zgodnie z nadanymi uprawnieniami (pkt 7.3), z rejestrowaniem operacji w logach (pkt 9.1);
- ;
- 2.5. Musi umożliwiać zaimportowanie danych osobowych i kompetencyjnych pracowników Zamawiającego;
- 2.6. System musi zapewniać rozdzielenie panelu administracyjnego od panelu pracownika

3. Zarządzanie kapitałem ludzkim i kompetencjami pracowników

- 3.1. **Badanie wiedzy, weryfikacja kompetencji, diagnostyka dopasowania kandydata w ramach procesu rekrutacji:**
 - 3.1.1. System musi umożliwiać tworzenie testów wiedzy i kompetencji kandydatów oraz pracowników.
 - 3.1.2. System musi umożliwiać budowanie i zarządzanie bankami pytań.
 - 3.1.3. System musi umożliwiać definiowanie przez Zamawiającego limitów czasu na wykonanie testów i ocen.
 - 3.1.4. System musi umożliwiać automatyczną ocenę wyników testów i ankiet, przy czym wynik automatycznej oceny ma mieć charakter pomocniczy, podlegać weryfikacji przez upoważnioną osobę Zamawiającego i nie może stanowić wyłącznej podstawy decyzji wywołującej wobec osoby skutki prawne lub w podobny sposób istotnie na nią wpływającej (art. 22 RODO). Wykonawca musi udokumentować zasady automatycznej oceny w sposób umożliwiający ich wyjaśnienie osobie ocenianej.
 - 3.1.5. System musi umożliwiać generowanie raportów i analiz dla Zamawiającego oraz osób podlegających ocenie, określonym przez Zamawiającego; do wyniku porównania stosuje się zasady określone w pkt 3.1.4.
 - 3.1.6. System musi umożliwiać porównywanie profilu kompetencyjnego pracownika lub kandydata z profilem stanowiska.

3.1.7. System musi wspierać procesy rekrutacji, adaptacji, rozwoju i planowania ścieżek kariery pracowników.

3.1.8. System musi umożliwiać analizę potencjału, predyspozycji zawodowych oraz obszarów rozwojowych pracowników z wykorzystaniem metod zaakceptowanych przez Zamawiającego; analiza nie może obejmować wnioskowania o stanie zdrowia (w tym zdrowia psychicznego) ani o innych danych, o których mowa w art. 9 ust. 1 RODO, ani wykorzystywać rozpoznawania emocji; do wyników stosuje się zasady określone w pkt 3.1.4.

3.2. Zarządzanie kompetencjami pracowników Zamawiającego:

3.2.1. System musi umożliwiać tworzenie słowników i profili kompetencyjnych.

3.2.2. System musi umożliwiać definiowanie kategorii kompetencji.

3.2.3. System musi umożliwiać przypisywanie kompetencji do stanowisk pracy.

3.2.4. System musi umożliwiać definiowanie poziomów kompetencji.

3.2.5. System musi umożliwiać określanie wymaganych poziomów kompetencji dla stanowisk pracy.

3.2.6. System musi umożliwiać identyfikowanie luk kompetencyjnych.

3.2.7. System musi umożliwiać analizę kompetencji zespołów.

3.2.8. System musi umożliwiać wyszukiwanie pracowników według posiadanych kompetencji.

3.2.9. System musi umożliwiać raportowanie poziomu kompetencji w organizacji.

3.3. Zarządzanie celami i oceną pracowników Zamawiającego

3.3.1. System musi umożliwiać definiowanie celów indywidualnych i zespołowych;

3.3.2. System musi umożliwiać określanie wag celów;

3.3.3. System musi umożliwiać monitorowanie realizacji celów;

3.3.4. System musi umożliwiać prowadzenie ocen okresowych 180 dla pracowników oraz 270 dla wskazanej grupy pracowniczej;

3.3.5. System musi umożliwiać tworzenie ocen dla różnych grup pracowników;

3.3.6. System musi umożliwiać przechowywanie historii ocen przez okres określony przez Zamawiającego zgodnie z pkt 13.2, z automatycznym usunięciem lub anonimizacją po jego upływie;

3.3.7. System musi umożliwiać raportowanie wyników ocen;

3.3.8. System musi umożliwiać analizę pozyskanych wyników ocen;

3.3.9. System musi umożliwiać automatyzację procesu zbierania odpowiedzi;

3.3.10. System musi umożliwiać generowanie raportów indywidualnych, zbiorczych;

3.3.11. System musi umożliwiać analizę mocnych stron i obszarów rozwojowych;

3.3.12. System musi umożliwiać identyfikację luk kompetencyjnych.

4. Wartościowanie stanowisk

4.1.1. System musi umożliwiać definiowanie, zarządzanie i aktualizację opisów stanowisk pracy oraz wartościowania stanowisk.

4.1.2. Rozwiązanie powinno zapewniać możliwość tworzenia i edycji kart stanowisk, przypisywania kompetencji, obowiązków i wymagań do stanowisk, a także definiowania metodologii wartościowania stanowisk wraz z nadawaniem wag, punktacji oraz klasyfikacją stanowisk zgodnie z przyjętymi w organizacji zasadami.

- 4.1.3. System powinien umożliwiać przechowywanie historii zmian oraz generowanie raportów i zestawień dotyczących opisów i wartościowania stanowisk.
- 4.1.4. System powinien umożliwić monitorowanie wskaźników luki płacowej, prezentację wyników w formie raportów i dashboardów oraz wspierać realizację obowiązków sprawozdawczych wynikających z przepisów prawa oraz polityk wewnętrznych organizacji w tym poprzez możliwość tworzenia zestawień i analiz na potrzeby raportowania. W celu realizacji tej funkcjonalności system może przetwarzać indywidualne dane o wynagrodzeniu pracowników, w zakresie określonym przez Zamawiającego. Dostęp do jednostkowych danych o wynagrodzeniu musi być ograniczony do upoważnionych użytkowników zgodnie z nadanymi rolami i uprawnieniami. Dane prezentowane pracownikom w ramach porównań wynagrodzeń nie mogą umożliwiać ustalenia wynagrodzenia innego, konkretnego pracownika i powinny być prezentowane w postaci odpowiednio zagregowanych wartości, w szczególności średnich lub median.

5. Onboarding

- 5.1.1. System musi zapewnić tworzenie słowników aktywności: zadań, spotkań, ankiet (stay/exit interview, feedback onboarding).
- 5.1.2. W ramach systemu powinny być dostępne materiały edukacyjne dla uczestników (instrukcje, filmy, FAQ)
- 5.1.3. System powinien zapewniać automatyczną komunikację onboardingową (zaproszenia, przypomnienia, informacje o kolejnych etapach).
- 5.1.4. System powinien pokazywać proces wielu pracowników jednocześnie, dając możliwość śledzenia postępu pracownika w ścieżce.
- 5.1.5. System powinien wysyłać rekomendacje działań rozwojowych oraz ścieżek adaptacji w organizacji, generowane na podstawie reguł określonych lub zaakceptowanych przez Zamawiającego; rekomendacje mają charakter pomocniczy, a ich zastosowanie wobec pracownika wymaga decyzji upoważnionej osoby Zamawiającego. Do rekomendacji generowanych z użyciem AI stosuje się pkt 13.5.
- 5.1.6. System powinien definiować harmonogram oraz treść e-mail.
- 5.1.7. System powinien pokazywać statystyki osób na onboardingu, logowanie do systemu, ich zadowolenie lub niezadowolenie z przeprowadzonych szkoleń. Statystyki prezentowane są w formie zagregowanej; informacja o zadowoleniu pochodzi wyłącznie z ankiet wypełnianych przez pracownika, a dane o logowaniu nie mogą być wykorzystywane do oceny pracownika.
- 5.1.8. System powinien umożliwić dodawanie komentarzy oraz załączników do aktywności system musi umożliwiać ograniczenie typów załączników, wyświetlanie ostrzeżenia o zakazie wprowadzania danych szczególnych kategorii oraz objęcie komentarzy i załączników mechanizmami retencji (pkt 13.2) i uprawnień (pkt 7.3).

6. Wymagania techniczne i utrzymanie systemu:

- 6.1. Wykonawca zobowiązuje się do zapewnienia bieżącego wsparcia użytkowników systemu w zakresie jego obsługi i eksploatacji przez cały okres obowiązywania umowy;

6.2. Wykonawca zobowiązuje się do świadczenia usług utrzymaniowych obejmujących w szczególności:

6.2.1. aktualizację systemu i udostępnianie nowych wersji oprogramowania;

6.2.2. usuwanie awarii, błędów i nieprawidłowości w działaniu systemu;

6.2.3. przywracanie pełnej funkcjonalności systemu po wystąpieniu incydentów;

6.2.4. zapewnienie ciągłości działania i prawidłowego funkcjonowania systemu;

6.2.5. zapewnienie pomocy technicznej dla użytkowników wskazanych przez Zamawiającego;

6.2.6. System musi być dostępny i w pełni funkcjonalny z wykorzystaniem aktualnie wspieranych przez producentów wersji następujących przeglądarek internetowych:

6.2.6.1. Mozilla Firefox;

6.2.6.2. Google Chrome;

6.2.6.3. Microsoft EDGE;

6.2.6.4. Safari macOS;

6.2.7. System musi być dostępny i w pełni funkcjonalny na następujących systemach operacyjnych:

6.2.7.1. Microsoft Windows 11,

6.2.7.2. macOS;

6.2.8. Wszelkie aktualizacje systemu udostępniane przez Wykonawcę w okresie obowiązywania umowy muszą być dostarczane bez dodatkowych opłat i nie mogą powodować utraty danych ani ograniczenia funkcjonalności wykorzystywanych przez Zamawiającego;

6.2.9. Korzystanie z systemu nie może wymagać instalacji dodatkowego oprogramowania klienckiego, wtyczek ani komponentów innych niż standardowa przeglądarka internetowa, z zastrzeżeniem powszechnie stosowanych mechanizmów bezpieczeństwa i uwierzytelniania;

6.2.10. System musi umożliwiać pracę w wielu językach, minimum polskim, angielskim, ukraińskim.

7. Wymagania bezpieczeństwa Tożsamość i dostęp:

7.1. Tożsamość i dostęp SSO:

7.1.1. System musi obsługiwać federacyjne uwierzytelnianie użytkowników zamawiającego za pomocą SAML 2.0 lub OpenID Connect;

7.1.2. Wykonawca musi zapewnić możliwość integracji systemu z Microsoft Entra ID zamawiającego;

7.1.3. System musi obsługiwać automatyczne tworzenie, modyfikację i dezaktywację kont użytkowników za pomocą SCIM 2.0 albo równoważnego mechanizmu;

7.1.4. Zamawiający musi mieć możliwość wyłączenia logowania lokalnego dla użytkowników federacyjnych;

7.2. Tożsamość i dostęp MFA:

7.2.1. System musi obsługiwać uwierzytelnianie wieloskładnikowe dla wszystkich kont administracyjnych;

7.2.2. System musi umożliwiać wymuszenie MFA dla wszystkich użytkowników zamawiającego;

7.2.3. System powinien obsługiwać co najmniej:

- FIDO2/WebAuthn;
- aplikację uwierzytelniającą z TOTP;
- mechanizm MFA dostępny przez Microsoft Entra ID.

- 7.2.4. SMS może być stosowany wyłącznie jako mechanizm awaryjny, jeżeli system obsługuje silniejszą metodę uwierzytelniania;
- 7.2.5. Użytkownik nie może wyłączyć MFA bez uprawnienia administracyjnego i rejestracji takiej operacji w logu;
- 7.2.6. Wykonawca musi opisać procedurę resetu lub obejścia MFA, w tym wymagane czynności weryfikacyjne i sposób rejestrowania operacji.
- 7.3. Tożsamość i dostęp RBAC:
- 7.3.1. System musi zapewniać kontrolę dostępu opartą na rolach.
- 7.3.2. Zamawiający musi mieć możliwość definiowania ról niestandardowych.
- 7.3.3. Uprawnienia muszą być rozdzielone co najmniej na:
- przeglądanie danych;
 - tworzenie i edycję danych;
 - zmianę statusu pracownika;
 - obsługę korespondencji;
 - pobieranie załączników;
 - eksport danych;
 - usuwanie i anonimizację danych;
 - zarządzanie użytkownikami;
 - zarządzanie konfiguracją;
 - dostęp do logów;
 - administrację techniczną;
 - dostęp do wyników ocen pracowniczych i badań kompetencyjnych;
 - dostęp do raportów i analiz zbiorczych;
 - korzystanie z funkcji wykorzystujących AI.
- 7.3.4. System musi umożliwiać ograniczenie widoczności danych według organizacji, jednostki, lokalizacji, procesu obsługi i roli użytkownika;
- 7.3.5. Użytkownik nie może uzyskać dostępu do danych wyłącznie przez zmianę identyfikatora obiektu, parametru URL, numeru procesu lub identyfikatora API;
- 7.3.6. Wykonawca musi przedstawić kompletną macierz ról i uprawnień oraz opisać mechanizmy zapobiegania nieautoryzowanemu dostępowi typu IDOR/BOLA.
- 7.4. Tożsamość i dostęp, cykl życia kont:
- 7.4.1. Każde konto musi być imienne. Konta współdzielone są niedopuszczalne.
- 7.4.2. System musi umożliwiać natychmiastową dezaktywację konta.
- 7.4.3. Po dezaktywacji użytkownik musi utracić dostęp do systemu i aktywnych sesji nie później niż w ciągu 15 minut.
- 7.4.4. System musi umożliwiać automatyczną dezaktywację kont nieaktywnych przez okres określony przez zamawiającego.
- 7.4.5. System musi rejestrować nadanie, zmianę i odebranie uprawnień.
- 7.4.6. System musi umożliwiać cykliczny przegląd uprawnień oraz eksport listy aktywnych użytkowników, ról i uprawnień.
- 7.4.7. Wykonawca musi zapewnić możliwość przeglądu uprawnień co najmniej raz na kwartał.
- 7.5. Tożsamość i dostęp, Administratorzy Wykonawcy:

- 7.5.1. Dostęp administratorów i personelu wsparcia Wykonawcy do środowiska zamawiającego musi odbywać się z użyciem imiennych kont i MFA;
- 7.5.2. Dostęp do danych produkcyjnych może być udzielony wyłącznie na czas określonego zadania;
- 7.5.3. Każdy dostęp administratora Wykonawcy do danych zamawiającego musi być:
- autoryzowany;
 - imienny;
 - rejestrowany;
 - ograniczony zakresem i czasem;
 - możliwy do odtworzenia na podstawie logów.
- 7.5.4. Wykonawca nie może uzyskiwać dostępu do treści danych bez uzasadnionej potrzeby technicznej.
- 7.5.5. Wykonawca musi przedstawić listę kategorii personelu, który może mieć dostęp do danych, wraz z lokalizacją wykonywania pracy. Dostęp personelu Wykonawcy lub dalszych podmiotów przetwarzających z państwa trzeciego stanowi przekazanie danych w rozumieniu rozdziału V RODO i podlega wymaganiom pkt 14.

8. Wymagania bezpieczeństwa: Szyfrowanie i separacja

8.1. Szyfrowanie i separacja, Transmisja:

- 8.1.1. Wszystkie połączenia użytkowników, administratorów, API i integracji z systemem muszą być szyfrowane.
- 8.1.2. Wykonawca musi stosować TLS 1.2 jako minimum oraz preferencyjnie TLS 1.3.
- 8.1.3. Niedopuszczalne jest stosowanie SSL, TLS 1.0, TLS 1.1, anonimowych zestawów szyfrów i przestarzałych algorytmów.
- 8.1.4. Wykonawca musi zapewnić poprawną walidację certyfikatów oraz ochronę przed obniżeniem poziomu zabezpieczeń połączenia.
- 8.1.5. Wykonawca musi przedstawić konfigurację TLS, w tym obsługiwane wersje protokołu, zestawy szyfrów i sposób zarządzania certyfikatami.

8.2. Szyfrowanie i separacja, dane w spoczynku:

- 8.2.1. Dane osobowe, załączniki, bazy danych, kopie zapasowe i logi zawierające dane osobowe muszą być szyfrowane w spoczynku.
- 8.2.2. Dla szyfrowania danych Wykonawca musi stosować algorytmy uznane za bezpieczne i aktualne, nie słabsze niż AES-256 lub równoważne.
- 8.2.3. Klucze szyfrujące muszą być przechowywane i zarządzane niezależnie od zaszyfrowanych danych.
- 8.2.4. Wykonawca musi opisać:
- sposób generowania kluczy;
 - sposób ich przechowywania;
 - kontrolę dostępu do kluczy;
 - rotację kluczy;
 - unieważnianie kluczy;
 - procedurę postępowania w przypadku kompromitacji klucza.
- 8.2.5. Wykonawca musi wskazać, czy zamawiający ma możliwość kontroli lub zarządzania własnymi kluczami szyfrującymi.

8.3. Szyfrowanie i separacja, Separacja danych:

- 8.3.1. Dane zamawiającego muszą być logicznie odseparowane od danych innych klientów.
- 8.3.2. Mechanizm separacji musi obejmować bazy danych, obiekty plikowe, cache, indeksy wyszukiwania, kopie zapasowe i mechanizmy eksportu.
- 8.3.3. Wykonawca musi przedstawić opis modelu izolacji wielodzierżawnej.
- 8.3.4. Wykonawca musi wykazać, że użytkownik jednego klienta nie może uzyskać dostępu do danych innego klienta poprzez interfejs aplikacyjny, API, wyszukiwanie, eksport lub manipulację identyfikatorem obiektu.
- 8.3.5. Wykonawca musi wykonywać testy kontroli separacji danych po zmianach architektury i aplikacji. Informacja o tych zmianach powinna zostać przekazana do Zamawiającego.

9. Wymagania bezpieczeństwa, logi i monitoring:

9.1. Zakres rejestrowanych zdarzeń:

9.1.1. System musi rejestrować co najmniej:

- udane i nieudane logowania;
- użycie i nieudane próby użycia MFA;
- utworzenie, modyfikację, dezaktywację i usunięcie konta;
- nadanie, zmianę i odebranie uprawnień;
- dostęp do profilu pracownika;
- pobranie załącznika;
- eksport danych;
- masowe wyszukiwanie i pobieranie danych;
- zmianę statusu, danych i zgód pracownika lub kandydata;
- usunięcie lub anonimizację danych;
- zmiany konfiguracji systemu;
- działania administratorów Wykonawcy;
- użycie API i tokenów technicznych;
- zmiany konfiguracji integracji;
- zdarzenia bezpieczeństwa i blokady kont.

9.1.2. Każdy log musi zawierać co najmniej:

- znacznik czasu zsynchronizowany z UTC;
- identyfikator użytkownika lub konta technicznego;
- adres IP lub identyfikator źródła;
- rodzaj operacji;
- identyfikator obiektu, którego dotyczyła operacja;
- wynik operacji;
- identyfikator sesji lub żądania, jeżeli jest dostępny.

9.2. Integralność i retencja:

- 9.2.1. Zwykły użytkownik nie może modyfikować ani usuwać logów.
- 9.2.2. Administrator systemu nie może usuwać śladów własnych działań bez wygenerowania nieusuwalnego zdarzenia audytowego.
- 9.2.3. Logi muszą być chronione przed nieautoryzowaną modyfikacją i przedwczesnym usunięciem.
- 9.2.4. Logi muszą być przechowywane przez minimum 12 miesięcy, chyba że zamawiający określi dłuższy okres, po upływie okresu określonego przez Zamawiającego logi są usuwane. Logi

mogą być wykorzystywane wyłącznie do celów bezpieczeństwa, rozliczalności i obsługi incydentów, a nie do oceny pracowników.

9.2.5. Wykonawca musi zapewnić eksport logów w formacie umożliwiającym dalszą analizę.

9.2.6. Wykonawca musi udostępnić dokumentację formatów i pól logów.

9.3. Alerty:

9.3.1. System musi umożliwiać generowanie lub przekazywanie alertów dotyczących:

- wielokrotnych nieudanych logowań;
- nietypowej lokalizacji lub urządzenia logowania;
- masowego pobrania danych pracowników, w tym wyników ocen i badań kompetencyjnych oraz CV;
- masowego eksportu danych;
- nadania uprawnień administracyjnych;
- użycia konta po jego dezaktywacji;
- dostępu administratora Wykonawcy;
- zmiany konfiguracji bezpieczeństwa;
- nietypowej aktywności API.

10. Wymagania bezpieczeństwa, bezpieczeństwo aplikacji:

10.1. Bezpieczne wytwarzanie:

10.1.1. Wykonawca musi utrzymywać udokumentowany proces bezpiecznego wytwarzania i utrzymania oprogramowania.

10.1.2. Proces musi obejmować analizę wymagań bezpieczeństwa, przeglądy kodu, testy, zarządzanie podatnościami i kontrolę zmian.

10.1.3. Wykonawca musi stosować OWASP ASVS albo równoważny, udokumentowany standard weryfikacji bezpieczeństwa aplikacji.

10.1.4. Wykonawca musi wykorzystywać n/w metody testowania bezpieczeństwa oprogramowania, odpowiednio do architektury systemu:

- SAST;
- DAST;
- SCA;

10.1.5. skanowanie obrazów kontenerów;

10.1.6. skanowanie infrastruktury jako kodu;

10.1.7. testy konfiguracji chmurowej.

10.1.8. Wyniki testów muszą być analizowane przed wdrożeniem zmiany do produkcji.

10.1.9. Podatności krytyczne i wysokie muszą być usuwane przed wdrożeniem do produkcji, chyba że zamawiający zaakceptuje udokumentowane ryzyko i plan redukcji.

10.2. Załączniki:

10.2.1. System musi ograniczać typy i rozmiary przesyłanych plików.

10.2.2. Każdy przesłany plik musi być skanowany pod kątem złośliwego oprogramowania przed udostępnieniem użytkownikowi.

10.2.3. System musi blokować pliki zawierające wykonywalny kod lub aktywną zawartość, jeżeli nie jest ona niezbędna do realizacji funkcji.

10.2.4. System musi chronić przed:

- path traversal;
- uploadem plików wykonywalnych;
- spoofingiem typu MIME;
- złośliwymi makrami;
- zip bomb;
- przejęciem ścieżki pliku;
- nieautoryzowanym dostępem do załącznika.

10.2.5. Załącznik musi być dostępny wyłącznie użytkownikom posiadającym uprawnienie do danego procesu i kandydata.

11. Wymagania bezpieczeństwa, Backup i ciągłość działania:

11.1. SLA:

11.1.1. Wykonawca musi zapewnić dostępność usługi na poziomie nie niższym niż 99,8% w każdym miesiącu kalendarzowym, z wyłączeniem uzgodnionych okien serwisowych.

11.1.2. Wykonawca musi określić:

- RTO;
- RPO;
- czas reakcji;
- czas usunięcia awarii;
- zasady eskalacji;
- rekompensaty za niedotrzymanie SLA.

11.1.3. Maksymalny RTO nie może przekroczyć 8 godzin.

11.1.4. Maksymalny RPO nie może przekroczyć 4 godzin.

11.1.5. Dla awarii krytycznej Wykonawca musi rozpocząć obsługę nie później niż w ciągu 30 minut od zgłoszenia lub wykrycia.

11.2. Backup:

11.2.1. Wykonawca musi wykonywać automatyczne kopie zapasowe baz danych, załączników, konfiguracji i niezbędnych metadanych.

11.2.2. Kopie muszą być szyfrowane.

11.2.3. Co najmniej jedna kopia musi być przechowywana w lokalizacji geograficznie odseparowanej od środowiska podstawowego, na terytorium EOG..

11.2.4. Kopie muszą być chronione przed nieautoryzowanym usunięciem i modyfikacją.

11.2.5. Wykonawca musi wykonywać test odtworzenia co najmniej raz na kwartał.

11.2.6. Wynik testu musi obejmować czas odtworzenia, zakres odtworzonych danych, wykryte błędy i działania korygujące.

11.2.7. Na żądanie zamawiającego Wykonawca musi przekazać raport z ostatniego testu odtworzeniowego.

11.2.8. Backup musi obejmować również załączniki, historię zmian, zgody i konfigurację systemu.

12. Wymagania bezpieczeństwa, Incydenty i podatności:

12.1. Zgłaszanie Incydentów:

12.1.1. Wykonawca musi poinformować zamawiającego o każdym incydencie lub podejrzeniu incydentu mogącego wpływać na poufność, integralność, dostępność lub autentyczność danych albo usługi.

12.1.2. Zgłoszenie musi nastąpić:

- w ciągu 1 godziny — dla incydentu krytycznego lub podejrzenia naruszenia danych;
 - w ciągu 4 godzin — dla pozostałego incydentu wpływającego na bezpieczeństwo lub dostępność;
 - w ciągu 24 godzin — dla podatności krytycznej dotyczącej usługi zamawiającego.
- 12.1.3. Zgłoszenie musi być przekazane przez wskazany kanał alarmowy oraz kanał pisemny.
- 12.1.4. Zgłoszenie musi zawierać, o ile informacje są dostępne:
- datę i czas wykrycia;
 - opis zdarzenia;
 - zakres i wpływ;
 - dotknięte komponenty;
 - kategorie danych;
 - działania podjęte przez Wykonawcę;
 - wskaźniki kompromitacji;
 - rekomendowane działania zamawiającego;
 - osobę odpowiedzialną za obsługę incydentu.
- 12.1.5. Wykonawca nie może uznać zdarzenia za nieistotne bez przekazania zamawiającemu informacji umożliwiających niezależną ocenę.
- 12.2. Współpraca powłamaniowa:
- 12.2.1. Wykonawca musi współpracować z zamawiającym przy analizie incydentu.
- 12.2.2. Wykonawca musi zabezpieczyć i udostępnić logi, konfiguracje, dane sesyjne, informacje o kontach, adresach IP, tokenach i wykonanych czynnościach.
- 12.2.3. Wykonawca nie może usuwać ani modyfikować danych dowodowych bez uzgodnienia z zamawiającym.
- 12.2.4. W terminie 10 dni roboczych od zakończenia obsługi incydentu Wykonawca musi przekazać raport RCA obejmujący:
- przyczynę źródłową;
 - przebieg zdarzenia;
 - zakres wpływu;
 - działania ograniczające;
 - działania naprawcze;
 - działania zapobiegawcze;
 - odpowiedzialne osoby i terminy.

13. Wymagania bezpieczeństwa, RODO i podwykonawcy:

- 13.1. Powierzenie:
- 13.1.1. Przed rozpoczęciem przetwarzania danych Wykonawca musi zawrzeć z zamawiającym umowę powierzenia przetwarzania danych osobowych zgodną z art. 28 RODO, według wzoru Zamawiającego. Postanowienia umowy powierzenia i OPZ w zakresie ochrony danych mają pierwszeństwo przed ogólnymi warunkami świadczenia usługi, regulaminami i umowami licencyjnymi producenta.
- 13.1.2. Wykonawca może przetwarzać dane wyłącznie na udokumentowane polecenie zamawiającego.
- 13.1.3. Wykonawca nie może wykorzystywać danych:
- do własnych celów, w tym marketingowych, statystycznych i rozwojowych;

- do profilowania pracowników lub kandydatów na potrzeby Wykonawcy lub podmiotów trzecich;
- do trenowania, dostrajania, walidacji lub ulepszania modeli AI lub uczenia maszynowego – również w postaci zanonimizowanej, zagregowanej lub pochodnej (w tym treści zapytań, wyników, metadanych i telemetrii);
- do tworzenia produktów lub usług dla innych klientów oraz do świadczenia usług na rzecz innych klientów, w tym benchmarkingu;
- do analityki niezwiązanej ze świadczeniem usługi.

13.1.4. Wykonawca musi zapewnić pomoc przy:

- realizacji praw osób;
- obsłudze naruszeń;
- ocenie skutków dla ochrony danych;
- wykazaniu zgodności;
- przeprowadzeniu audytu.

13.1.5. Pomoc, o której mowa w pkt 13.1.4, musi być udzielana bez zbędnej zwłoki, nie później niż w terminie 5 dni roboczych od zgłoszenia Zamawiającego [DO USTALENIA], w sposób umożliwiający dochowanie terminów z art. 12 ust. 3 RODO. Wykonawca prowadzi rejestr kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO.

13.2. Retencja:

13.2.1. System musi umożliwiać konfigurację okresów przechowywania danych , określonych przez Zamawiającego, według procesu i i kategorii osób (pracownik, były pracownik, kandydat oraz kategorii danych. System musi umożliwiać automatyczne usuwanie albo anonimizację danych po upływie retencji.

13.2.2. Usunięcie musi obejmować dane aktywne, załączniki, indeksy wyszukiwania, cache i środowiska testowe, dane osobowe Zamawiającego nie mogą być wykorzystywane w środowiskach testowych i deweloperskich bez uprzedniej pisemnej zgody Zamawiającego.

13.2.3. .

13.2.4. Dane w backupach muszą być usuwane zgodnie z cyklem nadpisywania określonym w umowie.

13.2.5. Wykonawca musi wskazać maksymalny czas całkowitego usunięcia danych z systemów produkcyjnych i kopii pomocniczych.

13.2.6. System musi generować raport wykonania usunięcia lub anonimizacji.

13.3. Dalsi podwykonawcy:

13.3.1. Wykonawca musi przedstawić pełną listę dalszych podmiotów przetwarzających (na wszystkich poziomach), obejmującą nazwę i siedzibę, zakres i cel przetwarzania, lokalizację przetwarzania oraz podstawę transferu – w szczególności dostawców infrastruktury chmurowej, narzędzi wsparcia i komunikacji oraz modeli AI.

- 13.3.2. Zmiana dalszego podmiotu przetwarzającego wymaga uprzedniego powiadomienia zamawiającego co najmniej 30 dni przed zmianą.
- 13.3.3. Zamawiający ma prawo zgłosić sprzeciw wobec zmiany z przyczyn związanych z bezpieczeństwem lub ochroną danych. Zgłoszenie sprzeciwu skutkuje zakazem powierzenia danych danemu podmiotowi, a w przypadku braku możliwości świadczenia usługi bez jego udziału – prawem Zamawiającego do rozwiązania umowy bez kar i dodatkowych opłat.
- 13.3.4. Wykonawca musi nałożyć na dalszych podwykonawców wymagania co najmniej równoważne wymaganiom niniejszego OPZ.
- 13.3.5. Wykonawca ponosi odpowiedzialność za działania dalszych podwykonawców jak za własne działania.
- 13.4. Zakres danych, kategorie osób i operacje przetwarzania:
- 13.4.1. Przetwarzanie danych przez Wykonawcę obejmuje wyłącznie dane osobowe pracowników Zamawiającego (oraz kandydatów do pracy) w zakresie: danych identyfikacyjnych (imię, nazwisko, służbowy adres e-mail, identyfikator w systemie), dane dotyczące wynagrodzenia – w zakresie niezbędnym do realizacji funkcjonalności określonej w pkt 4.1.4., danych organizacyjnych (jednostka organizacyjna, stanowisko, przełożony), danych dotyczących kompetencji, celów i działań rozwojowych, ścieżek kariery i onboardingu, ocen pracowniczych, wyników badań kompetencyjnych, a także danych użytkowników systemu zawartych w logach.
- 13.4.2. Dane o wynagrodzeniu mogą być przetwarzane wyłącznie w zakresie niezbędnym do realizacji funkcjonalności dotyczącej wartościowania stanowisk i monitorowania luki płacowej, o której mowa w pkt 4.1.4.
- 13.4.3. Wykonawca może wykonywać na danych wyłącznie operacje niezbędne do świadczenia usługi, wdrożenia, migracji, utrzymania i wsparcia technicznego, w szczególności: przechowywanie, utrwalanie, organizowanie, porządkowanie, udostępnianie użytkownikom Zamawiającego, tworzenie kopii zapasowych, usuwanie oraz wgląd w dane w zakresie niezbędnym do obsługi zgłoszenia.
- 13.4.4. Zamawiający jest administratorem danych, a Wykonawca podmiotem przetwarzającym. Wykonawca, który z naruszeniem umowy określi cele i sposoby przetwarzania, jest uważany za administratora w odniesieniu do tego przetwarzania (art. 28 ust. 10 RODO).
- 13.4.5. Ustawienia domyślne systemu muszą zapewniać, że dane pracownika, w szczególności wyniki ocen i badań kompetencyjnych, są dostępne wyłącznie dla ocenianego, jego bezpośredniego przełożonego oraz upoważnionych pracowników komórki kadrowej (art. 25 ust. 2 RODO).
- 13.5. Sztuczna inteligencja i zautomatyzowane przetwarzanie:
- 13.5.1. Wykonawca musi wskazać w ofercie wszystkie funkcje systemu wykorzystujące sztuczną inteligencję lub mechanizmy uczenia maszynowego (w tym rekomendacje, scoring, analizę potencjału, generowanie lub podsumowywanie treści), wraz z opisem ich logiki, danych wejściowych i wyjściowych, dostawcy modelu oraz miejsca przetwarzania.
- 13.5.2. Funkcje, o których mowa w pkt 13.5.1, muszą być domyślnie wyłączone i mogą zostać uruchomione wyłącznie po akceptacji Zamawiającego, odrębnie dla każdej funkcji.
- 13.5.3. System nie może podejmować wobec pracowników ani kandydatów decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, które wywołują skutki prawne lub w podobny sposób istotnie wpływają na te osoby (art. 22 RODO). Wyniki funkcji

automatycznych mają charakter pomocniczy; system musi umożliwiać ich weryfikację, zmianę przez upoważnioną osobę Zamawiającego oraz odnotowanie uzasadnienia.

13.5.4. System nie może wykorzystywać rozpoznawania emocji ani wnioskowania o stanie zdrowia, cechach psychicznych lub innych danych, o których mowa w art. 9 ust. 1 RODO (art. 5 ust. 1 lit. f rozporządzenia 2024/1689).

13.5.5. Wykonawca musi zapewnić możliwość przedstawienia osobie, której dane dotyczą, zrozumiałej informacji o czynnikach, które wpłynęły na wynik automatycznej oceny lub rekomendacji.

13.5.6. Jeżeli funkcja systemu stanowi system AI wysokiego ryzyka w rozumieniu załącznika III pkt 4 rozporządzenia 2024/1689, Wykonawca przekaże Zamawiającemu instrukcję obsługi oraz informacje niezbędne do wykonania obowiązków podmiotu stosującego, w tym do informowania pracowników i ich przedstawicieli oraz do przeprowadzenia oceny skutków dla praw podstawowych (art. 13, 26 i 27 rozporządzenia 2024/1689).

13.5.7. Dostawcy modeli AI są dalszymi podmiotami przetwarzającymi w rozumieniu pkt 13.3. Dane wejściowe i wyjściowe funkcji AI nie mogą być przechowywane przez dostawcę modelu dłużej, niż jest to niezbędne do obsługi zapytania, ani wykorzystywane w celach, o których mowa w pkt 13.1.3.

13.6. Prawa osób, przejrzystość i ocena skutków:

13.6.1. System musi umożliwiać realizację praw osób, o których mowa w art. 15–21 RODO, w szczególności wygenerowanie kompletnego zestawienia danych dotyczących wskazanej osoby (w tym wyników ocen, badań kompetencyjnych i rekomendacji) w formacie ustrukturyzowanym, sprostowanie, ograniczenie przetwarzania oraz usunięcie danych pojedynczej osoby.

13.6.2. System musi umożliwiać prezentowanie użytkownikom informacji o przetwarzaniu danych osobowych o treści określonej przez Zamawiającego (art. 13 RODO), w tym przed przystąpieniem do testu, badania kompetencyjnego lub oceny.

13.7. Wykonawca przekaże Zamawiającemu, przed uruchomieniem produkcyjnym, informacje niezbędne do przeprowadzenia oceny skutków dla ochrony danych (art. 35 RODO), w tym opis operacji i przepływów danych, zastosowanych zabezpieczeń oraz logiki funkcji automatycznych, oraz będzie współpracował przy jej aktualizacji.

- 13.6. Prawa osób, przejrzystość i ocena skutków:

- 13.6.1. System musi umożliwiać realizację praw osób, o których mowa w art. 15–21 RODO, w szczególności wygenerowanie kompletnego zestawienia danych dotyczących wskazanej osoby (w tym wyników ocen, badań kompetencyjnych i rekomendacji) w formacie ustrukturyzowanym, sprostowanie, ograniczenie przetwarzania oraz usunięcie danych pojedynczej osoby.

- 13.6.2. System musi umożliwiać prezentowanie użytkownikom informacji o przetwarzaniu danych osobowych o treści określonej przez Zamawiającego (art. 13 RODO), w tym przed przystąpieniem do testu, badania kompetencyjnego lub oceny.

13.6.3. Wykonawca przekaże Zamawiającemu, przed uruchomieniem produkcyjnym, informacje niezbędne do przeprowadzenia oceny skutków dla ochrony danych (art. 35 RODO), w tym opis operacji i przepływów danych, zastosowanych zabezpieczeń oraz logiki funkcji automatycznych, oraz będzie współpracował przy jej aktualizacji. Uruchomienie

produkcyjne funkcji, o których mowa w pkt 3.1, 3.3 i 5.1.5, następuje po zakończeniu oceny skutków przez Zamawiającego.

14. Wymagania bezpieczeństwa, Lokalizacja i transfer danych:

14.1. Wykonawca musi wskazać wszystkie lokalizacje:

- środowisk produkcyjnych;
- środowisk zapasowych;
- kopii backupowych;
- centrów operacji bezpieczeństwa;
- wsparcia technicznego;
- przetwarzania logów i telemetrii.

14.2. Wszystkie lokalizacje przetwarzania danych, o których mowa w pkt 14.1 (w tym środowiska zapasowe, kopie zapasowe, wsparcie techniczne, logi i telemetria), muszą znajdować się na terytorium EOG, z zastrzeżeniem pkt 14.3.

14.3. Transfer danych poza EOG wymaga uprzedniej pisemnej zgody Zamawiającego oraz zastosowania mechanizmu, o którym mowa w art. 45 lub 46 RODO, wraz z przedstawieniem oceny skutków transferu i opisu środków uzupełniających; Wykonawca niezwłocznie informuje Zamawiającego o każdym żądaniu dostępu do danych skierowanym przez organ publiczny państwa trzeciego, o ile nie jest to prawnie zakazane.

14.4. Wykonawca musi wskazać mechanizm transferu, dodatkowe zabezpieczenia oraz państwa, do których dane mogą być przekazywane.

14.5. Wykonawca nie może zmienić lokalizacji przetwarzania bez uprzedniego powiadomienia zamawiającego.

15. Wymagania bezpieczeństwa, audyt i dowody zgodności:

15.1. Wykonawca musi przedstawić przed podpisaniem umowy:

- certyfikat ISO/IEC 27001 albo równoważne dowody funkcjonowania SZBI;
- zakres certyfikacji;
- Statement of Applicability;
- ostatni raport z testu penetracyjnego;
- opis architektury usługi;
- listę podmiotów przetwarzających;
- lokalizację danych i backupów;
- opis zarządzania incydentami;
- opis zarządzania kluczami;
- opis procesu SDLC;
- wyniki ostatnich testów odtworzenia;
- wzór umowy powierzenia;
- wzór SLA;
- macierz shared responsibility;
- opis funkcjonalności wykorzystujących AI lub mechanizmy uczenia maszynowego (pkt 13.5);
- certyfikat ISO/IEC 27701 lub równoważny dowód funkcjonowania systemu zarządzania prywatnością jeżeli Wykonawca go posiada;
- ocenę skutków transferu jeżeli przewidziano przekazywanie danych poza EOG.
-

- 15.2. Dokumenty muszą być aktualne na dzień złożenia oferty lub nie starsze niż 12 miesięcy, chyba że charakter dokumentu uzasadnia inny okres.
- 15.3. Zamawiający ma prawo żądać wyjaśnień, dodatkowych dowodów i aktualizacji dokumentów w okresie obowiązywania umowy.
- 15.4. Zamawiający ma prawo przeprowadzić audyt dokumentacyjny, audyt po incydencie oraz audyt zgodności z wymaganiami bezpieczeństwa.
- 15.5. Wykonawca musi usunąć niezgodności w terminie wskazanym przez zamawiającego, nie dłuższym niż 30 dni dla niezgodności wysokiego ryzyka.

16. Wymagania bezpieczeństwa, zakończenie współpracy:

- 16.1. Wykonawca musi zapewnić eksport wszystkich danych zamawiającego bez dodatkowych ograniczeń technicznych.
- 16.2. Eksport musi obejmować co najmniej:
- profile pracowników;
 - załączniki;
 - historię zmian;
 - historię komunikacji;
 - zgody;
 - statusy procesów;
 - dane użytkowników i ról;
 - słowniki i konfigurację;
 - logi;
 - dane integracyjne.
- 16.3. Eksport musi być wykonany w otwartym, udokumentowanym formacie.
- 16.4. Załączniki muszą być eksportowane wraz z jednoznacznym powiązaniem z kandydatem, pracownikiem (osobą, której dane dotyczą) i procesem.
- 16.5. Wykonawca musi zapewnić wsparcie migracji przez minimum 60 dni od zgłoszenia zamiaru zakończenia usługi.
- 16.6. Po zakończeniu migracji Wykonawca musi zgodnie z decyzją Zamawiającego, usunąć dane Zamawiającego w tym ich kopie, dane pochodne, logi i dane przetwarzane przez dalsze podmioty przetwarzające, z systemów produkcyjnych i pomocniczych w terminie nie dłuższym niż 30 dni, a z kopii zapasowych w terminie określonym w pkt 13.2.4.
- 16.7. Wykonawca musi przekazać pisemne potwierdzenie usunięcia danych.
- 16.8. Wykonawca musi zapewnić, że po zakończeniu umowy pozostaną wyłączone wszystkie:
- konta;
 - tokeny;
 - integracje;
 - klucze API;
 - webhooki;
 - mechanizmy dostępu serwisowego.
- 16.9. Wykonawca nie może uzależniać eksportu danych od zawarcia dodatkowej umowy ani od uiszczenia opłat innych niż wskazane w ofercie.

17. Odbiór przedmiotu Zamówienia:

Odbiór przedmiotu zamówienia następuje po spełnieniu łącznie następujących warunków:

- 17.1. Aktywacji usługi SaaS dla wyznaczonej w pkt.2.1 ilości pracowników zamawiającego;
- 17.2. Potwierdzeniu zgodności ilościowej i funkcjonalnej z OPZ;
- 17.3. Przekazaniu Zamawiającemu wszystkich wymaganych dokumentów oraz danych dostępowych;
- 17.4. Uruchomieniu Wsparcia Technicznego – jeżeli dotyczy;
- 17.5. Warunkiem dokonania odbioru jest potwierdzenie zgodności przedmiotu zamówienia z OPZ oraz Umową;
- 17.6. Z czynności odbioru sporządza się protokół odbioru podpisany przez upoważnionych przedstawicieli Stron;
- 17.7. W przypadku stwierdzenia braków, wad lub niezgodności Zamawiający może odmówić podpisania protokołu odbioru albo podpisać go z uwagami, wyznaczając termin ich usunięcia;
- 17.8. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest przekazać Zamawiającemu, na adres e-mail: licencje@cez.gov.pl dane i dokumenty umożliwiające korzystanie z usługi w pełnym zakresie funkcjonalnym, w szczególności:
- nośniki lub pliki instalacyjne Oprogramowania – jeżeli dotyczy;
 - wszystkie wymagane klucze licencyjne i aktywacyjne – jeżeli dotyczy;
 - dokument potwierdzający dostawę przedmiotu zamówienia wraz ze wskazaniem okresu obowiązywania usługi;
 - umowę licencyjną producenta rozwiązania;
 - aktualne zestawienie w formacie edytowalnym (np. XLS) wszystkich dostarczonych pozycji, zawierające co najmniej: oznaczenie producenta (tzw. part numer), pełną nazwę produktu, wersję i edycję rozwiązania, okres obowiązywania rozwiązania, okres obowiązywania Wsparcia Technicznego, poziom Wsparcia Technicznego, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto.