Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest udzielenie licencji oraz dostępu do Platformy po uprzednim wdrożeniu, konfiguracji, integracji z ATS Zamawiającego, instruktaż, utrzymanie systemu klasy Human Capital Management (HCM), wspierającego zarządzanie zasobami ludzkimi oraz procesami HR w organizacji przez okres 12 miesięcy.

1. Przedmiot Zamówienia:

1.1. Przedmiotem zamówienia jest dostęp do platformy klasy Human Capital Management (HCM), wspierającej zarządzanie zasobami ludzkimi oraz procesami HR w organizacji (dalej: Platforma) oraz wdrożenie, konfiguracja, integracja z istniejącym systemem ATS Zamawiającego, instruktaż oraz serwis gwarancyjny Platformy.

1.2. Platforma musi umożliwiać dostęp do testów rekrutacyjnych i kompetencyjnych, 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. Warunki płatności: 30 dni od dnia doręczenia prawidłowo wystawionej faktury VAT do siedziby Zamawiającego.

1.4. Wykonawca zapewni Zamawiającemu dostęp do Platformy w zakresie testów rekrutacyjnych i kompetencyjnych w terminie 24 godzin od zawarcia Umowy.

1.5. Wdrożenie pozostałych funkcjonalności Platformy, w tym implementacja danych przekazanych przez Zamawiającego, nastąpi w terminie 3 dni roboczych od dnia ich przekazania Wykonawcy.

1.5.1. W ramach wdrożenia Platformy Wykonawca przeprowadzi analizę przedwdrożeniową o charakterze biznesowym, obejmującą identyfikację wymagań użytkowników, analizę procesów biznesowych oraz określenie sposobu wykorzystania Platformy przez Zamawiającego

1.5.2. W ramach wdrożenia Platformy Wykonawca przeprowadzi konfigurację Platformy, zgodnie z wymaganiami Zamawiającego, obejmującą dostosowanie parametrów, uprawnień, słowników oraz innych elementów niezbędnych do uruchomienia i eksploatacji Platformy.

1.5.3. W ramach wdrożenia Platformy Wykonawca przeprowadzi migrację danych otrzymanych od Zamawiającego, obejmującą przygotowanie, import oraz weryfikację poprawności danych przenoszonych z dotychczas wykorzystywanych przez Zamawiającego 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 wskazanego przez Zamawiającego. Pliki i kopie robocze wykorzystane do migracji Wykonawca usuwa niezwłocznie po jej zakończeniu i potwierdza ich usunięcie niezwłocznie po jego dokonaniu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

pracownikowi Zamawiającego wskazanemu w umowie. Potwierdzenie nastąpi poprzez pisemne potwierdzenie Wykonawcy przekazane Zamawiającemu w dniu zakończenia migracji i usunięcia danych.

1.6. W ramach realizacji zamówienia Wykonawca przeprowadzi instruktaż z zakresu korzystania z Platformy dla administratorów biznesowych wskazanych przez Zamawiającego. Liczba uczestników instruktażu nie przekroczy 100 osób.

1.7. W ramach realizacji zamówienia Wykonawca zapewni świadczenie usługi gwarancji. Gwarancja będzie realizowana w trybie zdalnym, z zachowaniem wymagań określonych w pkt 8.2. i 22.3. i obejmie obsługę zgłoszeń, konsultacje dla administratorów biznesowych oraz pomoc w rozwiązywaniu problemów związanych z eksploatacją wdrożonej Platformy.

1.8. Wsparcia gwarancyjne (Help Desk) dla użytkowników i administratorów biznesowych platformy, świadczone będzie w dni robocze od poniedziałku do piątku w godzinach 8:00-17:00.

2. Wymagania Funkcjonalne, platforma musi umożliwiać:

2.1. Integracja elektronicznych profili pracowników, umożliwiających implementację danych za pośrednictwem istniejącego systemu ATS Zamawiającego;

2.2. Gromadzenie danych osobowych i kompetencyjnych pracowników wyłącznie w zakresie niezbędnym do realizacji procesów kompetencyjnych, ocen pracowniczych, rozwoju, onboardingu i ścieżek kariery, a także danych organizacyjnych, danych dotyczących kompetencji, celów rozwojowych i ocen pracowniczych oraz wyników badań kompetencyjnych. System musi umożliwiać Zamawiającemu konfigurację katalogu pól, w tym wyłączenie pól zbędnych. System nie może wymagać wprowadzania danych kadrowo-płacowych ani danych szczególnych kategorii, z wyjątkiem danych dotyczących wynagrodzenia przekazywanych przez Zamawiającego wyłącznie w zakresie niezbędnym do realizacji funkcjonalności wartościowania stanowisk i monitorowania luki płacowej, o której mowa w pkt 4.6.;

2.3. Prezentowanie struktury organizacyjnej wraz z relacjami służbowymi;

2.4. Wyszukiwanie i filtrowanie danych pracowniczych zgodnie z nadanymi uprawnieniami (pkt 9.), z rejestrowaniem operacji w logach (pkt 10.4.);

2.5. Zaimportowanie danych osobowych i kompetencyjnych pracowników Zamawiającego;

2.6. Platforma musi zapewniać rozdzielenie panelu administracyjnego od panelu użytkownika.

3. Zarządzanie kapitałem ludzkim i kompetencjami pracowników

3.1. Badanie wiedzy, weryfikacja kompetencji, diagnostyka dopasowania kandydata w ramach procesu rekrutacji:

3.2. Platforma musi umożliwiać tworzenie testów wiedzy i kompetencji kandydatów oraz pracowników.

3.3. Platforma musi umożliwiać budowanie i zarządzanie bankami pytań.

3.4. Platforma musi umożliwiać definiowanie przez Zamawiającego limitów czasu na wykonanie testów i ocen. Limity dotyczą zarówno terminu na wykonanie testów i ocen, jak i samego czasu trwania poszczególnych testów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

3.5. Platforma 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.
3.6. Platforma musi umożliwiać generowanie raportów i analiz dla Zamawiającego oraz osób podlegających ocenie, określonych przez Zamawiającego; do wyniku porównania stosuje się zasady określone w pkt 3.9.
3.7. Platforma musi umożliwiać porównywanie profilu kompetencyjnego pracownika lub kandydata z profilem stanowiska.
3.8. Platforma musi wspierać procesy rekrutacji, adaptacji, rozwoju i planowania ścieżek kariery pracowników.
3.9. Platforma musi umożliwiać analizę potencjału, predyspozycji zawodowych oraz obszarów rozwojowych pracowników z wykorzystaniem metod zaakceptowanych przez Zamawiającego na etapie analizy przedwdrożeniowej; 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.

4. Zarządzanie kompetencjami pracowników Zamawiającego:

4.1. Platforma musi umożliwiać tworzenie słowników i profili kompetencyjnych.
4.2. Platforma musi umożliwiać definiowanie kategorii kompetencji.
4.3. Platforma musi umożliwiać przypisywanie kompetencji do stanowisk pracy.
4.4. Platforma musi umożliwiać definiowanie poziomów kompetencji.
4.5. Platforma musi umożliwiać określanie wymaganych poziomów kompetencji dla stanowisk pracy.
4.6. Platforma musi umożliwiać identyfikowanie luk kompetencyjnych.
4.7. Platforma musi umożliwiać analizę kompetencji zespołów.
4.8. Platforma musi umożliwiać wyszukiwanie pracowników według posiadanych kompetencji.
4.9 Platforma musi umożliwiać raportowanie poziomu kompetencji w organizacji.

5. Zarządzanie celami i oceną pracowników Zamawiającego

5.1. Platforma musi umożliwiać definiowanie celów indywidualnych i zespołowych;
5.2. Platforma musi umożliwiać określanie wag celów;
5.3. Platforma musi umożliwiać monitorowanie realizacji celów;
5.4. Platforma musi umożliwiać prowadzenie ocen okresowych dla wszystkich pracowników Zamawiającego dla wskazanej grupy pracowniczej;
5.5. Platforma musi umożliwiać tworzenie ocen dla różnych grup pracowników;
5.6. Platforma musi umożliwiać przechowywanie historii ocen przez okres określony przez Zamawiającego zgodnie z pkt 19.2, z automatycznym usunięciem lub anonimizacją po jego upływie;
5.7. Platforma musi umożliwiać raportowanie wyników ocen;
5.8. Platforma musi umożliwiać analizę pozyskanych wyników ocen;
5.9. Platforma musi umożliwiać automatyzację procesu zbierania odpowiedzi;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.10. Platforma musi umożliwiać generowanie raportów indywidualnych, zbiorczych;
5.11. Platforma musi umożliwiać analizę mocnych stron i obszarów rozwojowych;
5.12.Platforma musi umożliwiać identyfikację luk kompetencyjnych.

6. Wartościowanie stanowisk

6.1. Platforma musi umożliwiać definiowanie, zarządzanie i aktualizację opisów stanowisk pracy oraz wartościowania stanowisk.
6.2. Platforma powinna 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.
6.3. Platforma powinna umożliwiać przechowywanie historii zmian oraz generowanie raportów i zestawień dotyczących opisów i wartościowania stanowisk.
6.4. Platforma powinna umożliwić monitorowanie wskaźników luki płacowej, prezentację wyników w formie raportów i pulpitów menadżerskich oraz wspierać realizację obowiązków sprawozdawczych wynikających z przepisów prawa oraz polityk wewnętrznych Zamawiającego w tym poprzez możliwość tworzenia zestawień i analiz na potrzeby raportowania.
W celu realizacji tej funkcjonalności platforma 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.

7. Onboarding

7.1. Platforma musi zapewnić tworzenie słowników aktywności: zadań, spotkań, ankiet (stay/exit interview, feedback onboarding).

7.2. W ramach platformy muszą być dostępne materiały edukacyjne dla wszystkich użytkowników, którzy będą mieli dostęp do platformy (instrukcje, filmy, FAQ)

7.3. Platforma musi zapewniać automatyczną komunikację onboardingową (zaproszenia, przypomnienia, informacje o kolejnych etapach).

7.4. Platforma musi umożliwiać administratorowi biznesowemu analizę danych poszczególnych pracowników/departamentów/pionów w odniesieniu do oczekiwanych kryteriów Platforma musi umożliwiać wysyłanie rekomendacji działań rozwojowych oraz ścieżek rozwoju w organizacji, do wskazanych przez Zamawiającego na etapie analizy przedwdrożeniowej użytkowników, generowane na podstawie reguł określonych lub zaakceptowanych przez Zamawiającego; rekomendacje mają charakter pomocniczy, a ich zastosowanie wobec użytkownika wymaga decyzji upoważnionej osoby Zamawiającego. Do rekomendacji generowanych z użyciem AI stosuje się pkt 19.5.

7.5. Platforma musi umożliwiać definiowanie harmonogramu onboardingu oraz treści e-mail.

7.6 Platforma musi pokazywać statystyki osób na onboardingu, logowanie do platformy, ich zadowolenie lub niezadowolenie z przeprowadzonych szkoleń. Statystyki prezentowane są w formie

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

zagregowanej; informacja o zadowoleniu pochodzi wyłącznie z ankiet wypełnianych przez pracownika, a dane o logowaniu nie mogą być wykorzystywane do oceny pracownika.

7.7. Platforma musi umożliwić dodawanie komentarzy oraz załączników do aktywności. Platforma musi umożliwiać ograniczenie typów załączników, wyświetlanie ostrzeżenia o zakazie wprowadzania danych szczególnych kategorii oraz objęcie komentarzy i załączników mechanizmami retencji (pkt 19.4) i uprawnień (pkt 11).

8. Usługi gwarancyjne:

8.1. Wykonawca zobowiązuje się do świadczenia usług gwarancyjnych dla użytkowników platformy w zakresie jej obsługi i eksploatacji przez cały okres obowiązywania umowy;

8.2. Wykonawca zobowiązuje się do działań zapewniających bezawaryjną obsługę Platformy, obejmujących
w szczególności:

8.2.1. aktualizację Platformy i udostępnianie nowych wersji oprogramowania;

8.2.2 usuwanie awarii, błędów i nieprawidłowości w działaniu Platformy w nieprzekraczalnym terminie 24 godzin od chwili zgłoszenia;

8.2.3. przywracanie pełnej funkcjonalności Platformy po wystąpieniu incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

8.2.4. zapewnienie ciągłości działania i prawidłowego funkcjonowania Platformy;

8.2.5. zapewnienie pomocy technicznej dla użytkowników wskazanych przez Zamawiającego;

8.3. Platforma musi być dostępna i w pełni funkcjonalna z wykorzystaniem aktualnie wspieranych przez producentów wersji następujących przeglądarek internetowych:

8.3.1. Mozilla Firefox;

8.3.2. Google Chrome;

8.3.3. Microsoft EDGE;

8.3.4. Safari macOS;

8.4. Platforma musi być dostępna i w pełni funkcjonalna na następujących systemach operacyjnych:

8.4.1. Microsoft Windows 11,

8.4.2. macOS;

8.5. Wszelkie aktualizacje Platformy 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;

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

8.7. Platforma musi umożliwiać pracę w wielu językach, minimum polskim, angielskim, ukraińskim.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

9. Wymagania bezpieczeństwa Tożsamość i dostęp:

9.1. Tożsamość i dostęp SSO:

9.2. Platforma musi obsługiwać federacyjne uwierzytelnianie użytkowników zamawiającego za pomocą SAML 2.0 lub OpenID Connect;

9.3. Wykonawca musi zapewnić możliwość integracji platformy z Microsoft Entra ID Zamawiającego;

9.4. Platforma powinna obsługiwać automatyczne tworzenie, modyfikację i dezaktywację kont użytkowników za pomocą SCIM 2.0 albo równoważnego mechanizmu; Zamawiający dopuszcza stosowanie ręcznego procesu tworzenia, modyfikacji i dezaktywacji kont użytkowników wykonywanego przez upoważnionych pracowników Zamawiającego;

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

10. Tożsamość i dostęp MFA:

10.1. Platforma musi obsługiwać uwierzytelnianie wieloskładnikowe dla wszystkich kont administracyjnych;

10.2. Platforma musi umożliwiać wymuszenie MFA dla wszystkich użytkowników Zamawiającego, o ile uwierzytelnianie nie zostało zintegrowane i przekazane do realizacji po stronie Zamawiającego;

10.3. Platforma powinna obsługiwać co najmniej:

10.3.1. FIDO2/WebAuthn;

10.3.2. aplikację uwierzytelniającą z TOTP;

10.3.3. mechanizm MFA dostępny przez Microsoft Entra ID;

10.3.4 SMS może być stosowany wyłącznie jako mechanizm awaryjny, jeżeli system obsługuje silniejszą metodę uwierzytelniania;

10.4. Użytkownik nie może wyłączyć MFA bez uprawnienia administracyjnego i rejestracji takiej operacji w logu;

11.Tożsamość i dostęp RBAC:

11.1. Platforma musi zapewniać kontrolę dostępu opartą na rolach.

11.2. Zamawiający musi mieć możliwość definiowania ról niestandardowych.

11.3. Uprawnienia muszą być rozdzielone co najmniej na:

- przeglądanie danych;
- tworzenie i edycję danych;
- zmianę statusu pracownika;
- obsługę korespondencji;
- pobieranie załączników;
- eksport danych;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

- 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.

11.4. Platforma musi umożliwiać ograniczenie widoczności danych według organizacji, jednostki, lokalizacji, procesu obsługi i roli użytkownika;

11.5. Użytkownik nie może uzyskać dostępu do danych wyłącznie przez zmianę identyfikatora obiektu, parametru URL, numeru procesu lub identyfikatora API;

12. Tożsamość i dostęp, cykl życia kont:

12.1. Każde konto musi być imienne. Konta współdzielone są niedopuszczalne.

12.2. Platforma musi umożliwiać natychmiastową dezaktywację konta.

12.3. Po dezaktywacji użytkownik musi utracić dostęp do platformy i aktywnych sesji nie później niż w ciągu 15 minut.

12.4. Platforma musi umożliwiać automatyczną dezaktywację kont nieaktywnych przez okres określony przez Zamawiającego.

12.5. Platforma musi rejestrować nadanie, zmianę i odebranie uprawnień.

12.6 Platforma musi umożliwiać cykliczny przegląd uprawnień oraz eksport listy aktywnych użytkowników, ról i uprawnień.

12.7. Wykonawca musi zapewnić możliwość przeglądu uprawnień co najmniej raz na kwartał.

13. Tożsamość i dostęp, Administratorzy Wykonawcy:

13.1. Dostęp administratorów i personelu wsparcia Wykonawcy do środowiska zamawiającego musi odbywać się z użyciem imiennych kont i MFA;

13.2. Dostęp do danych produkcyjnych może być udzielony wyłącznie na czas określonego zadania;

13.3. Każdy dostęp administratora Wykonawcy do danych zamawiającego musi być:

- autoryzowany;
- imienny;
- rejestrowany;
- ograniczony zakresem i czasem;
- możliwy do odtworzenia na podstawie logów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

13.4. Wykonawca nie może uzyskiwać dostępu do treści danych bez uzasadnionej potrzeby technicznej.

13.5. Wykonawca przekaże wykaz kategorii personelu mającego dostęp do danych osobowych wraz z lokalizacją wykonywania pracy najpóźniej przed zawarciem umowy, w formie elektronicznej (np. tabeli).

13.6. Wykonawca powinien również zobowiązać się do aktualizacji wykazu przed wprowadzeniem zmian, w szczególności przed umożliwieniem dostępu do danych personelowi pracującemu z państwa trzeciego.

13.7. Samo przedstawienie wykazu nie oznacza zgody na transfer danych poza EOG. Ewentualny dostęp z państwa trzeciego wymaga uprzedniej weryfikacji spełnienia wymagań rozdziału V RODO oraz postanowień pkt 19 OPZ.

14. Wymagania bezpieczeństwa: Szyfrowanie i separacja

14.1. Szyfrowanie i separacja, Transmisja:

14.1.1. Wszystkie połączenia użytkowników, administratorów, API i integracji z platformą muszą być szyfrowane.

14.1.2. Wykonawca musi stosować TLS 1.2 jako minimum, przy czym TLS 1.3 powinien być preferowany, jeżeli jest obsługiwany przez obie strony komunikacji. Wykonawca powinien stosować się do rekomendacji opisanych w dokumencie RFC 9325.

14.1.3. Niedopuszczalne jest stosowanie SSL, TLS 1.0, TLS 1.1, anonimowych zestawów szyfrów, zestawów szyfrów niezapewniających szyfrowania danych (NULL encryption), przestarzałych algorytmów (zgodnie z dokumentem RFC 10015), a także zestawów szyfrów niezapewniających PFS (Perfect Forward Secrecy).

14.1.4. Wykonawca musi zapewnić poprawną walidację certyfikatów oraz ochronę przed obniżeniem poziomu zabezpieczeń połączenia.

14.2. Szyfrowanie i separacja, dane w spoczynku:

14.2.1. Dane osobowe, załączniki, bazy danych, kopie zapasowe i logi zawierające dane osobowe muszą być szyfrowane w spoczynku.

14.2.2. Dla szyfrowania danych Wykonawca musi stosować algorytmy uznane za bezpieczne i aktualne, nie słabsze niż AES-256 lub równoważne.

14.2.3. Klucze szyfrujące muszą być przechowywane i zarządzane niezależnie od zaszyfrowanych danych.

14.3. Wykonawca musi wskazać, czy Zamawiający ma możliwość kontroli lub zarządzania własnymi kluczami szyfrującymi. Zamawiający zaakceptuje oba rozwiązania.

14.4. Szyfrowanie i separacja, Separacja danych:

14.4.1. Dane Zamawiającego muszą być logicznie odseparowane od danych innych klientów.

14.4.2. Mechanizm separacji musi obejmować bazy danych, obiekty plikowe, cache, indeksy wyszukiwania, kopie zapasowe i mechanizmy eksportu.

14.4.4. Wykonawca na etapie analizy przedwdrożeniowej musi wykazać, że użytkownik jednego klienta nie może uzyskać dostępu do danych innego klienta poprzez interfejs aplikacyjny, API, wyszukiwanie, eksport lub manipulację identyfikatorem obiektu. Przy czym wykazanie może

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

nastąpić w formie wyników testów penetracyjnych nie starszych niż rok od momentu przekazania Zamawiającemu.

14.4.5. Wykonawca musi wykonywać testy kontroli separacji danych po zmianach architektury i aplikacji. Informacja o tych zmianach powinna zostać przekazana do Zamawiającego niezwłocznie po dokonaniu zmiany na adres Zamawiajacego wskazany w umowie.

15. Wymagania bezpieczeństwa, logi i monitoring:

15.1. Zakres rejestrowanych zdarzeń:

15.1.1. Platforma 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 platformy;
- działania administratorów Wykonawcy;
- użycie API i tokenów technicznych;
- zmiany konfiguracji integracji;
- zdarzenia bezpieczeństwa i blokady kont.

15.1.2. 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.

15.2. Integralność i retencja:

15.2.1. Użytkownik nie może modyfikować ani usuwać logów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

15.2.2. Administrator platformy nie może usuwać śladów własnych działań bez wygenerowania nieusuwalnego zdarzenia audytowego.

15.2.3. Logi muszą być chronione przed nieautoryzowaną modyfikacją i przedwczesnym usunięciem.

15.2.4. Logi muszą być przechowywane przez minimum 12 miesięcy. Logi mogą być wykorzystywane wyłącznie do celów bezpieczeństwa, rozliczalności i obsługi incydentów, a nie do oceny pracowników.

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

15.2.6. Wykonawca musi udostępnić dokumentację formatów i pól logów.

15.3. Alerty:

15.3.1. Platforma 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 i odebrania uprawnień administracyjnych;
- próby użycia konta po jego dezaktywacji;
- dostępu administratora Wykonawcy;
- zmiany konfiguracji bezpieczeństwa;
- nietypowej aktywności API.

16. Wymagania bezpieczeństwa, bezpieczeństwo aplikacji:

16.1. Bezpieczne wytwarzanie:

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

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

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

- SAST;
- DAST;
- SCA;
- skanowanie obrazów kontenerów;
- skanowanie infrastruktury jako kodu;
- testy konfiguracji chmurowej.

16.1.4. Wyniki testów muszą być analizowane przed wdrożeniem aktualizacji do produkcji w celu zapewnienia braku podatności w systemie produkcyjnym.

16.1.5. Podatności w szczególności te krytyczne i wysokie muszą być usuwane przed wdrożeniem do produkcji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

16.2. Załączniki:

16.2.1. Platforma musi ograniczać typy i rozmiary przesyłanych plików.

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

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

16.2.4. Platforma musi chronić przed:

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

16.2.5. Załącznik musi być dostępny wyłącznie użytkownikom posiadającym uprawnienie do danego procesu i pracownika.

17. Wymagania bezpieczeństwa, Backup i ciągłość działania:

17.1. SLA:

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

17.1.2. Maksymalny RTO (Recovery Time Objective) nie może przekroczyć 8 godzin.

17.1.3. Maksymalny RPO (Recovery Point Objective) nie może przekroczyć 4 godzin.

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

17.2. Backup:

17.2.1. Wykonawca musi wykonywać automatyczne kopie zapasowe baz danych, załączników, konfiguracji i niezbędnych metadanych, jak również historię zmian, zgody i konfigurację platformy

17.2.2. Kopie muszą być szyfrowane.

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

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

17.2.5. Wykonawca musi wykonywać test odtworzenia co najmniej raz na 12 miesięcy.

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

17.4. Na żądanie Zamawiającego Wykonawca musi przekazać raport z ostatniego testu odtworzeniowego.

18. Wymagania bezpieczeństwa, Incydenty i podatności:

18.1. Zgłaszanie Incydentów:

18.1.1.Wykonawca musi poinformować Zamawiającego o każdym incydencie lub podejrzeniu naruszeniu bezpieczeństwa danych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

18.1.2. Zgłoszenie musi nastąpić:

- w ciągu 1 godziny — dla incydentu krytycznego lub podejrzenia naruszenia danych;

18.1.3. Zgłoszenie musi być przekazane przez wskazany kanał alarmowy oraz kanał pisemny.

18.1.4. 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.

18.2. Współpraca powłamaniowa:

18.2.1. Wykonawca musi współpracować z Zamawiającym przy analizie incydentu.

18.2.2. Wykonawca musi zabezpieczyć i udostępnić Zamawiającemu logi, konfiguracje, dane sesyjne, informacje o kontach, adresach IP, tokenach i wykonanych czynnościach.

18.2.3. Wykonawca nie może usuwać ani modyfikować danych dowodowych bez uzgodnienia z Zamawiającym.

18.2.4. W terminie 10 dni roboczych od zakończenia obsługi incydentu Wykonawca musi przekazać pracownikowi Zamawiającemu wskazanemu w umowie raport RCA obejmujący:

- przyczynę źródłową;
- przebieg zdarzenia;
- zakres wpływu;
- działania ograniczające;
- działania naprawcze;
- działania zapobiegawcze;
- odpowiedzialne osoby i terminy.

19. Wymagania bezpieczeństwa, RODO i podwykonawcy:

19.1. Powierzenie:

19.1.1. 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.

19.1.2. Wykonawca może przetwarzać dane wyłącznie na udokumentowane polecenie Zamawiającego.

19.1.3. 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;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

- 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.

19.1.4. Wykonawca musi zapewnić pomoc przy:

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

19.1.5. Pomoc, o której mowa w pkt 19.1.4, musi być udzielana bez zbędnej zwłoki, nie później niż w terminie 5 dni roboczych od dnia otrzymania zgłoszenia Zamawiającego, z zastrzeżeniem spraw wymagających pilnego działania, w szczególności związanych z naruszeniem ochrony danych osobowych lub realizacją praw osób, których dane dotyczą. W takich przypadkach Wykonawca zobowiązany jest do udzielenia pomocy w terminie wskazanym przez Zamawiającego, uwzględniającym charakter sprawy oraz obowiązujące terminy wynikające z RODO.

19.1.6. Wykonawca musi zgłaszać Zamawiającemu stwierdzone naruszenia ochrony danych osobowych bez zbędnej zwłoki, na zasadach i w terminach określonych w umowie powierzenia przetwarzania danych osobowych.

19.1.7. Wykonawca musi prowadzić rejestr kategorii czynności przetwarzania danych osobowych zgodnie z art. 30 ust. 2 RODO, z uwzględnieniem przewidzianych w RODO wyjątków.

19.2. Retencja:

19.2.1. Platforma musi umożliwiać konfigurację okresów przechowywania danych, określonych przez Zamawiającego, według procesu i kategorii osób (pracownik, były pracownik, kandydat) oraz kategorii danych.

19.2.2. Platforma musi umożliwiać automatyczne usuwanie albo skuteczną nieodwracalną anonimizację danych po upływie okresu retencji.

19.2.3. Usunięcie lub anonimizacja danych osobowych musi obejmować wszystkie dane osobowe przetwarzane w aktywnych środowiskach Platformy, w szczególności dane znajdujące się w bazach produkcyjnych, załącznikach, indeksach wyszukiwania, pamięci podręcznej (cache) oraz innych kopiach pomocniczych. Dane te muszą zostać trwale usunięte w sposób uniemożliwiający ich dalsze przetwarzanie i odtworzenie w ramach aktywnych środowisk Platformy albo poddane skutecznej i nieodwracalnej anonimizacji uniemożliwiającej identyfikację osób, których dane dotyczą.

19.2.4. Wykorzystywanie rzeczywistych danych osobowych Zamawiającego w środowiskach testowych lub deweloperskich wymaga uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej lub elektronicznej. Po zakończeniu testów dane muszą zostać usunięte lub nieodwracalnie zanonimizowane.

19.2.5. Dane osobowe w kopiach zapasowych muszą być usuwane zgodnie z cyklem retencji określonym w umowie. W przypadku odtworzenia kopii zapasowej dane, których okres retencji upłynął, muszą zostać ponownie usunięte lub zanonimizowane.

19.2.6. Wykonawca musi wskazać przed zawarciem umowy maksymalny czas usunięcia lub nieodwracalnej anonimizacji danych osobowych ze środowiska produkcyjnego, kopii pomocniczych oraz kopii zapasowych, z uwzględnieniem cyklu ich retencji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

19.2.7. Platforma musi generować raport potwierdzający usunięcie lub anonimizację danych osobowych, zawierający datę wykonania operacji, zakres danych oraz jej wynik.

19.3. Dalsi podwykonawcy:

19.3.1. Wykonawca musi przedstawić Zamawiającemu, najpóźniej przed zawarciem umowy, aktualny wykaz wszystkich dalszych podmiotów przetwarzających dane osobowe, również na kolejnych poziomach powierzenia. Wykaz musi zawierać nazwę i siedzibę podmiotu, zakres i cel przetwarzania, lokalizację przetwarzania danych. Obowiązek obejmuje w szczególności dostawców infrastruktury chmurowej, platformy, wsparcia technicznego, usług komunikacyjnych oraz rozwiązań AI, jeżeli uczestniczą w przetwarzaniu danych osobowych Zamawiającego.

19.3.2. Wykonawca zobowiązany jest do poinformowania Zamawiającego w formie elektronicznej o planowanym dodaniu lub zmianie dalszego podmiotu przetwarzającego, co najmniej 30 dni kalendarzowych przed planowaną zmianą, wraz z przekazaniem zaktualizowanego wykazu dalszych podmiotów przetwarzających.

19.3.3. 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 dodatkowych roszczeń od Zamawiającego w szczególności roszczenia o zapłatę kar, dodatkowych opłat, rekompensat, odszkodowania lub zwrotu kosztów, z zastrzeżeniem wynagrodzenia należnego za świadczenia prawidłowo wykonane do dnia rozwiązania Umowy.

19.3.4 Wykonawca musi nałożyć na dalszych podwykonawców wymagania w zakresie ochrony danych osobowych co najmniej równoważnych obowiązkom wynikającym z umowy powierzenia przetwarzania danych osobowych zawartej z Zamawiającym, zgodnie z art. 28 ust. 4 RODO oraz OPZ.

19.3.5. Wykonawca ponosi odpowiedzialność za działania dalszych podwykonawców jak za własne działania.

19.4. Zakres danych, kategorie osób i operacje przetwarzania

19.4.1. Wykonawca może przetwarzać wyłącznie dane osobowe pracowników i kandydatów do pracy u Zamawiającego, w zakresie niezbędnym do realizacji przedmiotu zamówienia, obejmujące:

- dane identyfikacyjne i kontaktowe – imię, nazwisko, służbowy adres e-mail, prywatny adres e-mail kandydatów do pracy oraz identyfikator użytkownika w Platformie;
- dane organizacyjne – jednostka organizacyjna, stanowisko, przełożony;
- dane dotyczące wynagrodzenia – wyłącznie w zakresie niezbędnym do realizacji funkcjonalności wartościowania stanowisk i monitorowania luki płacowej, określonej w pkt 64 OPZ;
- dane dotyczące rozwoju zawodowego – kompetencje, cele i działania rozwojowe, ścieżki kariery oraz onboarding;
- dane dotyczące ocen pracowniczych – oceny pracownicze i wyniki badań kompetencyjnych;
- dane techniczne – dane użytkowników Platformy zawarte w logach systemowych.

19.4.2. 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 6.4.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

19.4.3. 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.

19.4.4. 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).

19.4.5. Ustawienia domyślne platformy muszą zapewniać, że dane pracownika, w szczególności wyniki ocen i badań kompetencyjnych, są dostępne wyłącznie dla ocenianego, jego bezpośredniego przełożonego oraz upoważnionych pracowników Zamawiającego wskazanych w umowie (art. 25 ust. 2 RODO).

19.5. Sztuczna inteligencja i zautomatyzowane przetwarzanie:

19.5.1. Wykonawca zobowiązany jest do wskazania w ofercie wszystkich funkcjonalności Platformy wykorzystujących sztuczną inteligencję (AI) lub uczenie maszynowe, w szczególności w zakresie rekomendacji, oceny kompetencji, scoringu, analizy potencjału oraz generowania i podsumowywania treści.

19.5.2. Dla każdej funkcjonalności Wykonawca musi przedstawić jej przeznaczenie, ogólny sposób działania, zakres wykorzystywanych danych wejściowych i generowanych wyników, dostawcę rozwiązania AI oraz lokalizację przetwarzania danych osobowych.

19.5.3. Funkcje, o których mowa w pkt.19.5.1., muszą być domyślnie wyłączone i mogą zostać uruchomione wyłącznie po akceptacji Zamawiającego, odrębnie dla każdej funkcji.

19.5.4. Platforma 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; platforma musi umożliwiać ich weryfikację, zmianę przez upoważnioną osobę Zamawiającego oraz odnotowanie uzasadnienia.

19.5.5. Platforma 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).

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

19.5.7. Jeżeli funkcja platformy stanowi platforma 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).

19.5.8. Dostawcy modeli AI są dalszymi podmiotami przetwarzającymi w rozumieniu pkt 19.1.3. Dane wejściowe i wyjściowe funkcji AI nie mogą być przechowywane przez dostawcę modelu dłużej, niż jest to niezbędne do obsługi zapytań, ani wykorzystywane w celach, o których mowa w pkt 19.1.3.

19.6. Prawa osób, przejrzystość i ocena skutków:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

19.6.1. Platforma 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.

19.6.2.Platforma 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.

19.6.3. 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, a także będzie współpracował przy jej aktualizacji. Uruchomienie produkcyjne funkcjonalności, o których mowa w pkt 1.1, 1.2 i 1.5.2 i 1.5.3., nastąpi po zakończeniu przez Zamawiającego oceny skutków dla ochrony danych.

19.6.4. Wykonawca zobowiązany jest również do współpracy przy przeprowadzaniu i aktualizacji DPIA.

20. Wymagania bezpieczeństwa, Lokalizacja i transfer danych:

20.1. Wykonawca w terminie 5 dni roboczych od podpisania umowy musi wskazać wszystkie lokalizacje:

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

20.2. Wszystkie lokalizacje przetwarzania danych, o których mowa w pkt 20.1 (w tym środowiska zapasowe, kopie zapasowe, wsparcie techniczne, logi i telemetria), muszą znajdować się na terytorium EOG,

20.3. Wymagania bezpieczeństwa, audyt i dowody zgodności:

20.3.1. Wykonawca w terminie 5 dni roboczych od podpisania umowy mus przedstawić:

- certyfikat ISO/IEC 27001 albo równoważne dowody funkcjonowania SZBI;
- zakres certyfikacji;
- ostatni raport z testu penetracyjnego
- listę podmiotów przetwarzających;
- wyniki ostatnich testów odtworzenia;
- macierz shared responsibility;
- opis funkcjonalności wykorzystujących AI lub mechanizmy uczenia maszynowego (pkt 19.5);

Dokumenty muszą być nie starsze niż 12 miesięcy, chyba że charakter dokumentu uzasadnia inny okres.

20.3.2. Zamawiający ma prawo żądać wyjaśnień, dodatkowych dowodów i aktualizacji dokumentów w okresie obowiązywania umowy.

20.3.3. Zamawiający ma prawo przeprowadzić audyt dokumentacyjny, audyt po incydencie oraz audyt zgodności z wymaganiami bezpieczeństwa.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

20.3.4. Wykonawca musi usunąć niezgodności w terminie wskazanym przez Zamawiającego, nie dłuższym niż 30 dni dla niezgodności wysokiego ryzyka.

21. Wymagania bezpieczeństwa, zakończenie współpracy:

21.1.Wykonawca musi zapewnić eksport wszystkich danych zamawiającego bez dodatkowych ograniczeń technicznych,w sposób i na warunkach uzgodnionych z Zamawiającym.

21.1.1. 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.

21.1.2. Eksport musi być wykonany w otwartym, udokumentowanym formacie.

21.1.3. Załączniki muszą być eksportowane wraz z jednoznacznym powiązaniem z kandydatem, pracownikiem (osobą, której dane dotyczą) i procesem.

21.2. Wykonawca musi zapewnić wsparcie migracji przez minimum 60 dni od zgłoszenia zamiaru zakończenia korzystania z Platformy.

21.2.1. 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 19.2.5

21.2.2.Wykonawca musi przekazać pracownikowi Zamawiającego wskazanemu w umowie pisemne potwierdzenie usunięcia danych niezwłocznie po zakończeniu migracji

21.3.Wykonawca musi zapewnić poprzez pisemne oświadczenie Zamawiającemu, że po zakończeniu umowy pozostaną wyłączone wszystkie:

- konta;
- tokeny;
- integracje;
- klucze API;
- webhooki;
- mechanizmy dostępu serwisowego.

21.4. Wykonawca nie może uzależniać eksportu danych od zawarcia dodatkowej umowy ani od uiszczenia opłat innych niż wskazane w ofercie.

22. Odbiór przedmiotu Zamówienia:

Odbiór przedmiotu zamówienia następuje po spełnieniu łącznie następujących warunków:

22.1. Udzielenia Zamawiającemu dostępu do Platformy zgodnie z OPZ;

22.2. Potwierdzeniu zgodności funkcjonalnej Platformy z OPZ; weryfikacja będzie polegała na sprawdzeniu aktywowanych kont oraz dostępności funkcjonalności wymaganych w OPZ przez osoby

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

wskazane przez Zamawiającego. Przekazaniu Zamawiającemu wszystkich wymaganych dokumentów oraz danych dostępowych;
22.3. Potwierdzenie warunków świadczenia usługi gwarancji
22.4. Warunkiem dokonania odbioru jest potwierdzenie zgodności realizacji przedmiotu zamówienia z OPZ oraz Umową;
22.5. Z czynności odbioru sporządza się protokół odbioru podpisany przez upoważnionych przedstawicieli Stron;
22.6. W przypadku stwierdzenia braków, wad lub niezgodności Zamawiający może odmówić podpisania protokołu odbioru albo podpisać go z uwagami, wyznaczając termin ich usunięcia;
22.7. 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 platformy;
- aktualne zestawienie w formacie edytowalnym (np. XLS) wszystkich dostarczonych pozycji, zawierające co najmniej: oznaczenie producenta (tzw. part numer), pełną nazwę produktu, wersję i edycje platformy, okres obowiązywania rozwiązania, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem