289309

Opis Przedmiotu Zamówienia

1. **Przedmiotem zamówienia jest umożliwienie dostępu i konfiguracja do wymagań Zamawiającego systemu klasy ATS (ang. Applicant Tracking System) wspierającego obsługę procesów rekrutacyjnych Zamawiającego.**
2. **Wymagania Ogólne:**
   2.1 Wykonawca zobowiązuje się do:
   a) zapewnienia dostępu do systemu ATS dla conajmniej 4 użytkowników (rekruterów);
   b) zapewnienia dostępu do systemu ATS dla co najmniej 100 osób merytorycznych/hiring managerów;
   c) zapewnienia nielimitowanej ilości slotów rekrutacyjnych (jednocześnie otwartych rekrutacji).
   d) Wykonawca dostarczy i będzie świadczył usługę w modelu SaaS (Software as a Service), w ramach której system oraz infrastruktura chmurowa stanowią jedną, kompletną usługę. Oferowane rozwiązanie musi obejmować udostępnienie aplikacji, zasobów obliczeniowych, przestrzeni do przechowywania danych oraz wszelkich elementów infrastruktury wymaganych do prawidłowego funkcjonowania systemu. Odpowiedzialność za utrzymanie, aktualizację, zabezpieczenie i dostępność środowiska chmurowego spoczywa w całości na Wykonawcy.
   e) świadczenie usługi przez okres 12 miesięcy z możliwością przedłużenia na kolejne 12 miesięcy w ramach prawa opcji.
   2.2 System musi umożliwiać realizację procesów rekrutacyjnych, w szczególności:
   a) tworzenie, publikację i zarządzanie ogłoszeniami rekrutacyjnymi, w tym publikację na stronie internetowej Zamawiającego oraz zewnętrznych portalach rekrutacyjnych
   b) prowadzenie wielu procesów rekrutacyjnych jednocześnie;
   c) definiowanie i zarządzanie etapami procesu rekrutacyjnego;
   d) zarządzanie bazą kandydatów, w tym gromadzenie, przechowywanie i wyszukiwanie CV oraz pozostałej dokumentacji rekrutacyjnej;
   e) tworzenie i zarządzanie profilami kompetencyjnymi;
   f) ocenianie, filtrowanie, sortowanie i porównywanie kandydatów;
   g) planowanie i organizację rozmów rekrutacyjnych;
   h) zapraszanie kandydatów na rozmowy rekrutacyjne oraz przekazywanie informacji zwrotnej;
   i) wspomaganie i automatyzację komunikacji z kandydatami oraz uczestnikami procesu rekrutacyjnego po stronie Zamawiającego;

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

j) zapewnienie elektronicznego obiegu dokumentów pomiędzy rekruterami a osobami zaangażowanymi merytorycznie w proces rekrutacji;
k) raportowanie i analizę efektywności prowadzonych procesów rekrutacyjnych;
l) zapewnienie zgodności procesu rekrutacyjnego z obowiązującymi przepisami prawa, w szczególności przepisami o ochronie danych osobowych (RODO);
m) realizację funkcjonalności multipostingu, rozumianej jako nieograniczona możliwość jednoczesnej publikacji ogłoszeń rekrutacyjnych na portalach pracy, z którymi Zamawiający posiada aktywne umowy lub integracje, a także na stronie internetowej i stronie kariery Zamawiającego, z poziomu systemu ATS;
n) tworzenie formularzy i kwestionariuszy rekrutacyjnych zawierających dodatkowe pytania do kandydatów.
o) System musi umożliwić dodawanie notatek

2.3 System musi zapewniać funkcjonalność raportowania i analityki, obejmującą co najmniej:
a) tworzenie raportów dotyczących prowadzonych procesów rekrutacyjnych;
b) generowanie statystyk i zestawień dotyczących kandydatów;
c) filtrowanie danych według zdefiniowanych kryteriów;
d) eksport raportów i danych do formatów XLSX, CSV i PDF;
e) samodzielne tworzenie raportów przez uprawnionych użytkowników bez udziału Wykonawcy.

2.4 System musi zapewniać integrację z następującymi rozwiązaniami:
a) zakładką „Oferty pracy" na stronie internetowej Zamawiającego;
b) usługami Microsoft 365, w szczególności Microsoft Outlook oraz Microsoft Teams, umożliwiającą m.in. planowanie i wysyłanie zaproszeń na spotkania rekrutacyjne online, automatyczne generowanie linków do spotkań MS Teams oraz synchronizację terminów spotkań z kalendarzami uczestników procesu rekrutacyjnego;
c) portalami rekrutacyjnymi, z którymi Zamawiający posiada zawarte umowy na publikację ogłoszeń o pracę.

2.5 Wykonawca zobowiązuje się do konfiguracji systemu zgodnie z wymaganiami Zamawiającego, przeprowadzenia instruktażu stanowiskowego dla użytkowników wskazanych przez Zamawiającego, w liczbie odpowiadającej co najmniej liczbie użytkowników określonej w pkt 2.1;

2.6 Instruktaże, konsultacje oraz wsparcie mogą być realizowane w formie stacjonarnej lub zdalnej. W przypadku realizacji usług w formie zdalnej Wykonawca zobowiązany jest do zapewnienia i organizacji środowiska technicznego umożliwiającego przeprowadzenie spotkania, w tym dostarczenia kanału komunikacji, linków dostępowych oraz niezbędnego wsparcia technicznego dla uczestników;

2.7 Wykonawca zobowiązuje się do wyznaczenia dedykowanego opiekuna odpowiedzialnego za obsługę Zamawiającego przez cały okres obowiązywania umowy;

2.8 Wykonawca zobowiązuje się do zagwarantowania niezmienności cen za korzystanie z systemu ATS przez cały okres realizacji zamówienia, w tym w okresie realizacji zamówienia opcjonalnego, o ile zostanie ono uruchomione.

3. Wymagania techniczne i utrzymanie systemu ATS:

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

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

3.2 wykonawca zobowiązuje się do świadczenia usług utrzymaniowych obejmujących w szczególności:

a) aktualizację systemu i udostępnianie nowych wersji oprogramowania;
b) usuwanie awarii, błędów i nieprawidłowości w działaniu system;
c) przywracanie pełnej funkcjonalności systemu po wystąpieniu incydentów;
d) zapewnienie ciągłości działania i prawidłowego funkcjonowania system;
e) zapewnienie pomocy technicznej dla użytkowników wskazanych przez Zamawiającego;

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

a) Mozilla Firefox;
b) Google Chrome;
c) Microsofte EDGE;
d) Safari macOS;

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

a) Microsoft Windows 11,
b) macOS;

3.5 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;

3.6 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;

4. Wymagania bezpieczeństwa Tożsamość i dostęp:

4.1 Tożsamość i dostęp SSO:

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

b) Wykonawca musi zapewnić możliwość integracji systemu z Microsoft Entra ID zamawiającego;
c) System musi obsługiwać automatyczne tworzenie, modyfikację i dezaktywację kont użytkowników za pomocą SCIM 2.0 albo równoważnego mechanizmu;
d) Zamawiający musi mieć możliwość wyłączenia logowania lokalnego dla użytkowników federacyjnych;
e) Konto lokalne powinno być utrzymywane wyłącznie dla awaryjnego konta administracyjnego, którego użycie musi być rejestrowane i zgłaszane zamawiającemu (opcjonalnie);
f) Wykonawca musi przedstawić opis konfiguracji SSO, zakres obsługiwanych atrybutów, procedurę synchronizacji użytkowników oraz procedurę awaryjnego odzyskania dostępu.

4.2 Tożsamość i dostęp MFA:

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

a) System musi obsługiwać uwierzytelnianie wieloskładnikowe dla wszystkich kont administracyjnych;
b) System musi umożliwiać wymuszenie MFA dla wszystkich użytkowników zamawiającego;
c) System powinien obsługiwać co najmniej:
   - FIDO2/WebAuthn;
   - aplikację uwierzytelniającą z TOTP;
   - mechanizm MFA dostępny przez Microsoft Entra ID.
d) SMS może być stosowany wyłącznie jako mechanizm awaryjny, jeżeli system obsługuje silniejszą metodę uwierzytelniania;
e) Użytkownik nie może wyłączyć MFA bez uprawnienia administracyjnego i rejestracji takiej operacji w logu;
f) Wykonawca musi opisać procedurę resetu lub obejścia MFA, w tym wymagane czynności weryfikacyjne i sposób rejestrowania operacji.

4.3 Tożsamość i dostęp RBAC:
a) System musi zapewniać kontrolę dostępu opartą na rolach.
b) Zamawiający musi mieć możliwość definiowania ról niestandardowych.
c) Uprawnienia muszą być rozdzielone co najmniej na:
   - przeglądanie danych;
   - tworzenie i edycję danych;
   - zmianę statusu kandydata;
   - obsługę korespondencji;
   - pobieranie CV i załączników;
   - eksport danych;
   - usuwanie i anonimizację danych;
   - zarządzanie użytkownikami;
   - zarządzanie konfiguracją;
   - dostęp do logów;
   - administrację techniczną.
d) System musi umożliwiać ograniczenie widoczności danych według organizacji, jednostki, lokalizacji, procesu rekrutacyjnego i roli użytkownika;
e) Użytkownik nie może uzyskać dostępu do danych wyłącznie przez zmianę identyfikatora obiektu, parametru URL, numeru procesu lub identyfikatora API;
f) Wykonawca musi przedstawić kompletną macierz ról i uprawnień oraz opisać mechanizmy zapobiegania nieautoryzowanemu dostępowi typu IDOR/BOLA.

4.4 Tożsamość i dostęp, cyk życia kont:
a) Każde konto musi być imienne. Konta współdzielone są niedopuszczalne.
b) System musi umożliwiać natychmiastową dezaktywację konta.
c) Po dezaktywacji użytkownik musi utracić dostęp do systemu i aktywnych sesji nie później niż w ciągu 15 minut.
d) System musi umożliwiać automatyczną dezaktywację kont nieaktywnych przez okres określony przez zamawiającego.

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

e) System musi rejestrować nadanie, zmianę i odebranie uprawnień.
f) System musi umożliwiać cykliczny przegląd uprawnień oraz eksport listy aktywnych użytkowników, ról i uprawnień.
g) Wykonawca musi zapewnić możliwość przeglądu uprawnień co najmniej raz na kwartał.

4.5 Tożsamość i dostęp, Administratorzy Wykonawcy:

a) Dostęp administratorów i personelu wsparcia Wykonawcy do środowiska zamawiającego musi odbywać się z użyciem imiennych kont i MFA;
b) Dostęp do danych produkcyjnych może być udzielony wyłącznie na czas określonego zadania;
c) Każdy dostęp administratora Wykonawcy do danych zamawiającego musi być:
   - autoryzowany;
   - imienny;
   - rejestrowany;
   - ograniczony zakresem i czasem;
   - możliwy do odtworzenia na podstawie logów.
d) Wykonawca nie może uzyskiwać dostępu do treści danych bez uzasadnionej potrzeby technicznej.
e) Wykonawca musi przedstawić listę kategorii personelu, który może mieć dostęp do danych, wraz z lokalizacją wykonywania pracy.

5. Wymagania bezpieczeństwa: Szyfrowanie i separacja

5.1 Szyfrowanie i separacja, Transmisja:

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

5.2 Szyfrowanie i separacja, dane w spoczynku:

a) Dane osobowe, CV, załączniki, bazy danych, kopie zapasowe i logi zawierające dane osobowe muszą być szyfrowane w spoczynku.
b) Dla szyfrowania danych Wykonawca musi stosować algorytmy uznane za bezpieczne i aktualne, nie słabsze niż AES-256 lub równoważne.
   - Klucze szyfrujące muszą być przechowywane i zarządzane niezależnie od zaszyfrowanych danych.
   - Wykonawca musi opisać:
   - sposób generowania kluczy;
   - sposób ich przechowywania;
   - kontrolę dostępu do kluczy;
   - rotację kluczy;
   - unieważnianie kluczy;

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

c) procedurę postępowania w przypadku kompromitacji klucza.
d) Wykonawca musi wskazać, czy zamawiający ma możliwość kontroli lub zarządzania własnymi kluczami szyfrującymi.

5.3 Szyfrowanie i separacja, Separacja danych:

a) Dane zamawiającego muszą być logicznie odseparowane od danych innych klientów.
b) Mechanizm separacji musi obejmować bazy danych, obiekty plikowe, cache, indeksy wyszukiwania, kopie zapasowe i mechanizmy eksportu.
c) Wykonawca musi przedstawić opis modelu izolacji wielodzierżawnej.
d) 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.
e) Wykonawca musi wykonywać testy kontroli separacji danych po zmianach architektury i aplikacji. Informacja o tych zmianach powinna zostać przekazana do Zamawiającego.

6. Wymagania bezpieczeństwa, logi i monitoring:

6.1 Zakres rejestrowanych zdarzeń:

a) 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 kandydata;
- pobranie CV lub załącznika;
- eksport danych;
- masowe wyszukiwanie i pobieranie danych;
- zmianę statusu, danych i zgód kandydata;
- zmiany konfiguracji systemu;
- działania administratorów Wykonawcy;
- użycie API i tokenów technicznych;
- zmiany konfiguracji integracji;
- zdarzenia bezpieczeństwa i blokady kont.

b) System powinien rejestrować:
- usunięcie lub anonimizację danych;

c) 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.

6.2 Integralność i retencja:

a) Zwykły 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

b) Administrator systemu nie może usuwać śladów własnych działań bez wygenerowania nieusuwalnego zdarzenia audytowego.
c) Logi muszą być chronione przed nieautoryzowaną modyfikacją i przedwczesnym usunięciem.
d) Logi muszą być przechowywane przez minimum 12 miesięcy, chyba że zamawiający określi dłuższy okres.
e) Wykonawca musi zapewnić eksport logów w formacie umożliwiającym dalszą analizę.
f) Wykonawca musi udostępnić dokumentację formatów i pól logów.
g) System powinien umożliwiać Integrację z systemem SIEM po stronie zamawiającego, pod kątem wysyłania logów zdarzeń na potrzeby wykrywania incydentów bezpieczeństwa (opcjonalnie).
h) System musi umożliwiać przekazywanie logów do SIEM zamawiającego (opcjonalnie)..
i) Integracja musi obsługiwać co najmniej API, syslog over TLS, webhook albo mechanizm równoważny.
   - Wykonawca musi zapewnić:
   - uwierzytelnianie połączenia;
   - szyfrowanie transmisji;
   - kontrolę integralności komunikatów;
   - możliwość filtrowania kategorii zdarzeń;
   - możliwość określenia zakresu czasu i dzierżawy.
j) Wykonawca musi przekazać dokumentację integracji, przykładowe komunikaty oraz mapowanie pól.
k) Koszt udostępniania logów i API nie może być uzależniony od każdorazowego uzyskania zgody Wykonawcy.

6.3 Alerty:

a) System musi umożliwiać generowanie lub przekazywanie alertów dotyczących:
   - wielokrotnych nieudanych logowań;
   - nietypowej lokalizacji lub urządzenia logowania;
   - masowego pobrania CV;
   - masowego eksportu danych;
   - nadania uprawnień administracyjnych;
   - użycia konta po jego dezaktywacji;
   - dostępu administratora Wykonawcy;
   - zmiany konfiguracji bezpieczeństwa;
   - nietypowej aktywności API.

7. Wymagania bezpieczeństwa, bezpieczeństwo aplikacji:

7.1 Bezpieczne wytwarzanie:

a) Wykonawca musi utrzymywać udokumentowany proces bezpiecznego wytwarzania i utrzymania oprogramowania.
b) Proces musi obejmować analizę wymagań bezpieczeństwa, przeglądy kodu, testy, zarządzanie podatnościami i kontrolę zmian.
c) Wykonawca musi stosować OWASP ASVS albo równoważny, udokumentowany standard weryfikacji bezpieczeństwa aplikacji. OWASP ASVS służy właśnie

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

do definiowania i testowania technicznych kontroli bezpieczeństwa aplikacji internetowych.

d) Wykonawca musi wykorzystywać n/w metody testowania bezpieczeństwa oprogramowania, odpowiednio do architektury systemu:
   - SAST;
   - DAST;
   - SCA;

e) skanowanie obrazów kontenerów;

f) skanowanie infrastruktury jako kodu;

g) testy konfiguracji chmurowej.

h) Wyniki testów muszą być analizowane przed wdrożeniem zmiany do produkcji.

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

7.2 Testy penetracyjne:

a) Wykonawca musi przeprowadzać niezależny test penetracyjny systemu co najmniej raz na 12 miesięcy.

b) Test musi obejmować co najmniej:
   - aplikację webową;
   - API;
   - mechanizmy uwierzytelniania;
   - autoryzację i separację dzierżaw;
   - mechanizmy eksportu;
   - upload i przetwarzanie załączników;
   - integracje;
   - mechanizmy administracyjne.

c) Test musi być wykonany przez niezależny, kompetentny zespół.

d) Na żądanie zamawiającego Wykonawca musi przekazać raport lub jego część dotyczącą usługi zamawiającego.

e) Raport musi zawierać zakres, datę, metodologię, ograniczenia, klasyfikację podatności oraz status działań korygujących.

f) Zamawiający preferuje by Wykonawca usuwał:
   - podatności krytyczne w terminie do 7 dni;
   - podatności wysokie w terminie do 30 dni;
   - podatności średnie w terminie do 90 dni.

7.3 Opcjonalnie Wykonawca powinien przedstawić własny harmonogram usuwania podatności.Załączniki:

a) System musi ograniczać typy i rozmiary przesyłanych plików.

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

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

d) System musi chronić przed:
   - path traversal;
   - uploadem plików wykonywalnych;

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

- spoofingiem typu MIME;
- złośliwymi makrami;
- zip bomb;
- przejęciem ścieżki pliku;
- nieautoryzowanym dostępem do załącznika.

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

8. Wymagania bezpieczeństwa, Backup i ciągłość działania:

8.1 SLA:

a) Wykonawca musi zapewnić dostępność usługi na poziomie nie niższym niż 99,9% w każdym miesiącu kalendarzowym, z wyłączeniem uzgodnionych okien serwisowych.

b) Wykonawca musi określić:
- RTO;
- RPO;
- czas reakcji;
- czas usunięcia awarii;
- zasady eskalacji;
- rekompensaty za niedotrzymanie SLA.

c) Maksymalny RTO nie może przekroczyć 8 godzin.

d) Maksymalny RPO nie może przekroczyć 4 godzin.

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

8.2 Backup:

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

b) Kopie muszą być szyfrowane.

c) Co najmniej jedna kopia musi być przechowywana w lokalizacji geograficznie odseparowanej od środowiska podstawowego.

d) Kopie muszą być chronione przed nieautoryzowanym usunięciem i modyfikacją.

e) Wykonawca musi wykonywać test odtworzenia co najmniej raz na kwartał.

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

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

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

9. Wymagania bezpieczeństwa, Incydenty i podatności:

9.1. Zgłaszanie Incydentów:

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

b) Zgłoszenie musi nastąpić:

c) w ciągu 1 godziny — dla incydentu krytycznego lub podejrzenia naruszenia 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

d) w ciągu 4 godzin — dla pozostałego incydentu wpływającego na bezpieczeństwo lub dostępność;
e) w ciągu 24 godzin — dla podatności krytycznej dotyczącej usługi zamawiającego.
f) Zgłoszenie musi być przekazane przez wskazany kanał alarmowy oraz kanał pisemny.
g) 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.

h) Wykonawca nie może uznać zdarzenia za nieistotne bez przekazania zamawiającemu informacji umożliwiających niezależną ocenę.

9.2. Współpraca powłamaniowa:
a) Wykonawca musi współpracować z zamawiającym przy analizie incydentu.
b) Wykonawca musi zabezpieczyć i udostępnić logi, konfiguracje, dane sesyjne, informacje o kontach, adresach IP, tokenach i wykonanych czynnościach.
c) Wykonawca nie może usuwać ani modyfikować danych dowodowych bez uzgodnienia z zamawiającym.
d) 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.

10. **Wymagania bezpieczeństwa, RODO i podwykonawcy:**

10.1 Powierzenie:
a) Przed rozpoczęciem przetwarzania danych Wykonawca musi zawrzeć z zamawiającym umowę powierzenia zgodną z art. 28 RODO.
b) Wykonawca może przetwarzać dane wyłącznie na udokumentowane polecenie zamawiającego.
c) Wykonawca nie może wykorzystywać danych:
- do własnych celów marketingowych;
- do profilowania kandydatów na potrzeby Wykonawcy;
- do trenowania modeli AI;
- do tworzenia produktów lub usług dla innych klientów;
- do analityki niezwiązanej ze świadczeniem usługi.

d) Wykonawca musi zapewnić pomoc przy:

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

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

10.2 Retencja:

a) System musi umożliwiać konfigurację okresów przechowywania danych według procesu i kategorii kandydata.
b) System musi umożliwiać automatyczne usuwanie albo anonimizację danych po upływie retencji.
c) Usunięcie musi obejmować dane aktywne, załączniki, indeksy wyszukiwania, cache i środowiska testowe.
d) Dane w backupach muszą być usuwane zgodnie z cyklem nadpisywania określonym przez Wykonawcę.
e) Wykonawca musi wskazać maksymalny czas całkowitego usunięcia danych z systemów produkcyjnych i kopii pomocniczych.
f) System musi generować raport wykonania usunięcia lub anonimizacji.

10.3 Dalsi podwykonawcy:

a) Wykonawca musi przedstawić pełną listę dalszych podmiotów przetwarzających.
b) Zmiana dalszego podmiotu przetwarzającego wymaga uprzedniego powiadomienia zamawiającego co najmniej 30 dni przed zmianą.
c) Zamawiający ma prawo zgłosić sprzeciw wobec zmiany z przyczyn związanych z bezpieczeństwem lub ochroną danych.
d) Wykonawca musi nałożyć na dalszych podwykonawców wymagania co najmniej równoważne wymaganiom niniejszego OPZ.
e) Wykonawca ponosi odpowiedzialność za działania dalszych podwykonawców jak za własne działania.

11. **Wymagania bezpieczeństwa, Lokalizacja i transfer danych:**

a) Wykonawca musi wskazać wszystkie lokalizacje:
   - środowisk produkcyjnych;
   - środowisk zapasowych;
   - kopii backupowych;
   - centrów operacji bezpieczeństwa;
   - wsparcia technicznego;
   - przetwarzania logów i telemetrii.
b) Podstawowa lokalizacja przetwarzania danych musi znajdować się na terytorium EOG.
c) Transfer danych poza EOG wymaga uprzedniej zgody zamawiającego i wskazania podstawy prawnej transferu.
d) Wykonawca musi wskazać mechanizm transferu, dodatkowe zabezpieczenia oraz państwa, do których dane mogą być przekazywane.

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

e) Wykonawca nie może zmienić lokalizacji przetwarzania bez uprzedniego powiadomienia zamawiającego.

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

13. **Wymagania bezpieczeństwa, zakończenie współpracy:**
    a) Wykonawca musi zapewnić eksport wszystkich danych zamawiającego bez dodatkowych ograniczeń technicznych.
    b) Eksport musi obejmować co najmniej:
        - profile kandydatów;
        - CV i załączniki;
        - historię zmian;
        - historię komunikacji;
        - zgody;
        - statusy procesów;
        - dane użytkowników i ról;
        - słowniki i konfigurację;
        - logi;
        - dane integracyjne.
    c) Eksport musi być wykonany w otwartym, udokumentowanym formacie.
    d) Załączniki muszą być eksportowane wraz z jednoznacznym powiązaniem z kandydatem i procesem.

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

e) Wykonawca musi zapewnić wsparcie migracji przez minimum 60 dni od zgłoszenia zamiaru zakończenia usługi.
f) Po zakończeniu migracji Wykonawca musi usunąć dane zamawiającego z systemów produkcyjnych i pomocniczych.
g) Wykonawca musi przekazać pisemne potwierdzenie usunięcia danych.
h) Wykonawca musi zapewnić, że po zakończeniu umowy pozostaną wyłączone wszystkie:
   - konta;
   - tokeny;
   - integracje;
   - klucze API;
   - webhooki;
   - mechanizmy dostępu serwisowego.
i) Wykonawca nie może uzależniać eksportu danych od zawarcia dodatkowej umowy ani od uiszczenia opłat innych niż wskazane w ofercie.

14. Odbiór przedmiotu Zamówienia

Odbiór przedmiotu zamówienia następuje po spełnieniu łącznie następujących warunków:

14.1 Aktywacji usługi SaaS dla wyznaczonej w pkt.2.1 ilości pracowników zamawiającego;
14.2 Potwierdzeniu zgodności ilościowej i funkcjonalnej z OPZ;
14.3 Przekazaniu Zamawiającemu wszystkich wymaganych dokumentów oraz danych dostępowych;
14.4 Uruchomieniu Wsparcia Technicznego – jeżeli dotyczy;
14.5 Warunkiem dokonania odbioru jest potwierdzenie zgodności przedmiotu zamówienia z OPZ oraz Umową;
14.6 Z czynności odbioru sporządza się protokół odbioru podpisany przez upoważnionych przedstawicieli Stron;
14.7 W przypadku stwierdzenia braków, wad lub niezgodności Zamawiający może odmówić podpisania protokołu odbioru albo podpisać go z uwagami, wyznaczając termin ich usunięcia;
14.8 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:
   a) nośniki lub pliki instalacyjne Oprogramowania – jeżeli dotyczy;
   b) wszystkie wymagane klucze licencyjne i aktywacyjne – jeżeli dotyczy;
   c) dokument potwierdzający dostawę przedmiotu zamówienia wraz ze wskazaniem okresu obowiązywania usługi;
   d) umowę licencyjną producenta rozwiązania;
   e) aktualne zestawienie w formacie edytowalnym (np. XLS) wszystkich dostarczonych pozycji, zawierające co najmniej: oznaczenie producenta (tzw. part numer), pełną nazwę produktu, wersję i edycje rozwiązania, 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