OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Przedmiot zamówienia:**

   - Przedmiotem zamówienia jest usługa zapewnienia dostępu do infrastruktury obliczeniowej dla CEZ jako Usługa (IaaS). W ramach umowy wykonawca zobowiązuje się do oferowania dostępu do wszystkich usług dostępnych w ramach danej platformy. Poszczególne usługi będą zamawiane i rozliczane sukcesywnie w trakcie trwania umowy maksymalnie do 30.06.2026 r. lub do wyczerpania maksymalnej kwoty wynagrodzenia przewidzianej w umowie, w zależności które ze zdarzeń nastąpi wcześniej.

2. **Termin realizacji:** Wykonawca rozpocznie świadczenie Usługi w terminie 2 dni roboczych od dnia zawarcia Umowy.

3. **Ogólne wymagania:**

3.1. Przedmiotem zamówienia jest zapewnienie dostępu kompletnego pakietu usługi IaaS - dostępu do infrastruktury obliczeniowej obejmującego w szczególności:

- Dostęp do infrastruktury obliczeniowej, umożliwiającej tworzenie i utrzymanie środowisk teleinformatycznych.
- W ramach Usługi IaaS (Infrastructure as a Service) Wykonawca zapewni dostarczanie maszyn wirtualnych, zasobów obliczeniowych, pamięci masowej i sieci w modelu chmurowym; możliwość samodzielnego zarządzania instalacjami i sieciami wirtualnymi.
- Wszystkie usługi muszą być dostępne w ramach jednej dzierżawy, dostarczanej i obsługiwanej przez jednego operatora i zarządzane za pośrednictwem tego samego interfejsu.

3.2. Mechanizmy bezpieczeństwa i zgodności (szyfrowanie, ochrona przed atakami, kontrola dostępu, monitorowanie, zgodność z regulacjami):

- Wykonawca zapewni udostępnienie scentralizowanego kanału zgłoszeń umożliwiającego Administratorom Zamawiającego rejestrowanie, obsługę i monitorowanie zgłoszeń dotyczących usług, systemów lub zasobów objętych przedmiotem zamówienia, wraz z interfejsem umożliwiającym samodzielne korzystanie z kanału zgłoszeń przez użytkowników uprawnionych.
- W ramach usługi gwarancyjnej Wykonawca zapewni Zamawiającemu wsparcie techniczne dostawcy chmury obliczeniowej, wsparcie produktu oraz wsparcie Wykonawcy w zakresie serwisu przyjmującego i obsługującego zgłoszenia awarii i błędów, w trybie co najmniej 8 godzin dziennie, 5 dni w tygodniu (dni robocze). Wsparcie będzie odbywało się w języku polskim lub angielskim.
- W ramach Usługi bezpieczeństwa i zgodności mechanizmy ochrony i zgodność z regulacjami prawnymi i branżowymi zgodnie z wytycznymi opisanymi w niniejszym OPZ.

3.3. Usługi muszą być dostępne w formie ciągłej 24 godziny, 7 dni w tygodniu, 365 dni w roku.

3.4. Minimalna dostępność do środowisk obliczeniowych (SLA) w ujęciu miesięcznym musi wynosić co najmniej 99,95%.

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

3.5. Dostęp (autentykacja) do środowiska obliczeniowego musi opierać się o mechanizm Federated Identity i umożliwiać integrację z Identity Provider'em CEZ w standardzie Entra ID z włączoną autentykacją wieloetapową (MFA).

3.6. Dostarczona usługa musi umożliwiać przetwarzanie danych przy spełnieniu wszystkich wymagań wynikających z przepisów o ochronie danych i cyberbezpieczeństwie, w tym:

3.6.1. RODO (ogólne rozporządzenie o ochronie danych),

3.6.2. wymogów KRI (Krajowe Ramy Interoperacyjności),

3.6.3. ustawy o KSC (Krajowy System Cyberbezpieczeństwa),

3.6.4. dyrektywy NIS2

3.7. Wymagania bezpieczeństwa dla usługi chmurowej:

- Usługa IaaS musi być zgodna ze Standardami Cyberbezpieczeństwa Chmur Obliczeniowych minimalnie na poziomie 2. Platforma chmurowa musi spełniać wymagania SCCO 2 (zgodnie z dokumentem „Standardy Cyberbezpieczeństwa Chmur Obliczeniowych, wersja 2025" https://chmura.gov.pl/informacje/scco).

3.8. Dostarczony zestaw usług musi zapewniać przetwarzanie danych w izolowanych enklawach bez możliwości dostępu przez dostawcę chmury.

3.9. Dostarczony zestaw usług musi zapewniać szyfrowanie danych w pamięci podczas przetwarzania uniemożliwiając dostęp dostawcy chmury.

3.10. Dostarczony zestaw usług musi zawierać natywną usługę bezpieczeństwa, która w sposób ciągły zbiera, agreguje, normalizuje i ocenia stan bezpieczeństwa wszystkich zasobów na podstawie reguł zgodności, benchmarków (co najmniej CIS, ISO27001) oraz sygnałów z innych usług bezpieczeństwa oraz zapewnia pojedynczy ekran widoku do identyfikacji luk konfiguracyjnych, priorytetyzacji ryzyka oraz integracji z procesami reagowania na incydenty i audytu.

3.11. Sieć Internetowa Operatora Chmury musi być połączona do co najmniej jednego polskiego punktu wymiany ruchu internetowego (np. Equinix Warsaw-PLIX/THINX/TPIX).

3.12. Wszystkie zasoby/usługi infrastruktury obliczeniowej muszą:

3.12.1. automatycznie skalować się do zadanych przez Zamawiającego parametrów,

3.12.2. wspierać skalowalność pionową poprzez zmianę parametrów wydajnościowych usługi infrastruktury obliczeniowej, na której uruchomiony jest dany komponent,

3.12.3. wspierać skalowalność poziomą poprzez uruchomienie lub wyłączenie instancji usługi infrastruktury obliczeniowej, na której uruchomiony jest dany komponent, funkcjonalność skalowania poziomego instancji usług infrastruktury obliczeniowej, na których działają moduły musi być przezroczysta dla użytkownika.

4. Wymagania szczegółowe

4.1. Wymagania techniczne – IaaS:

4.1.1. Zasoby obliczeniowe (Compute) - Wykonawca zapewni szeroką gamę maszyn wirtualnych i zasobów obliczeniowych, spełniając następujące minima:

4.1.1.1. dostępne muszą być instancje VM różnych typów ogólnego przeznaczenia, zoptymalizowane pod wysoką moc obliczeniową CPU, zoptymalizowane pod dużą pamięć RAM, zoptymalizowane pod przepustowość dysków / operacje we/wy, a także wyspecjalizowane instancje z akceleracją GPU (do obliczeń grafiki/AI). Powinny być dostępne również ekonomiczne instancje z akceleracją grafiki o niskim koszcie oraz opcje HPC (wysokowydajne obliczenia).

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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4.1.2. Platforma musi umożliwiać utrzymanie maszyn z wysoką dostępnością. Powinna istnieć możliwość grupowania maszyn w strefach lub grupach dostępności celem zapewnienia HA (High Availability).

4.2. Usługa chmurowa musi umożliwiać Zamawiającemu tworzenie i zarządzanie wirtualną infrastrukturą sieciową w odseparowanym, bezpiecznym zakresie. Wymagania minimalne:

4.2.1. Możliwość definiowania wirtualnych sieci prywatnych (VPC/VNet) izolowanych od innych klientów, z adresacją prywatną i kontrolą routingu. W ramach VPC Zamawiający musi móc tworzyć dowolnie podsieć (subnets), także całkowicie prywatne (bez dostępu do Internetu). Wykonawca zapewni obsługę własnych przestrzeni adresowych (co najmniej IPv4; wsparcie IPv6 również wymagane na poziomie instancji lub bram).

4.2.2. Wykonawca musi umożliwić bezpieczne połączenie sieci Cez (on-premises) z siecią wirtualną w chmurze. Wymaga się obsługi VPN site-to-site (IPsec) - możliwość zestawienia wielu tuneli VPN między lokalizacją Zamawiającego a chmurą. Połączenia VPN powinny wspierać protokół BGP dla automatycznego przełączania awaryjnego (failover) między wieloma tunelami. Wykonawca musi także oferować opcję dedykowanego łącza prywatnego do chmury w celu uzyskania wyższej przepustowości i niezawodności połączenia z pominięciem Internetu.

4.2.3. Musi istnieć możliwość łączenia sieci wirtualnych w tym samym regionie (peering lokalny) jak i między regionami (peering globalny) z użyciem prywatnych adresów. Routing między sieciami i do Internetu powinien być konfigurowalny (tablice routingu, bramy internetowe/NAT).

4.2.4. Wykonawca zapewni pulę adresów publicznych do wykorzystania przez Zamawiającego. Wymagane jest automatyczne przydzielanie publicznego IP dla instancji (jeśli w podsieci publicznej) oraz możliwość rezerwacji statycznych publicznych adresów IP niezależnych od konkretnej maszyny (tzw. adresy elastyczne). Możliwość przypisania wielu adresów IP do jednej karty sieciowej oraz wielu kart sieciowych do jednej instancji również jest wymagana.

4.2.5. Platforma musi umożliwiać definiowanie reguł filtrowania ruchu przychodzącego i wychodzącego na poziomie maszyn lub podsieci (odpowiednik security groups, network ACL). Administrator powinien móc tworzyć własne reguły zezwalające/blokujące ruch na określonych portach/protokołach (TCP, UDP, ICMP itd.). Wykonawca powinien zapewnić także możliwość wyłączenia tzw. Source/Destination Check na interfejsach.

4.2.6. Wymagane jest udostępnienie usług równoważenia obciążenia (Load Balancer) na poziomie sieciowym i aplikacyjnym w warstwach 3 do 7.

4.2.7. Wykonawca dostarczy usługę DNS do obsługi rekordów domenowych związanych z infrastrukturą. Oczekiwane funkcje to zarządzanie strefami DNS prywatnymi i publicznymi, obsługa różnorodnych rekordów, wysoka dostępność serwerów DNS. Usługa DNS powinna integrować się z load balancerami (np. w kontekście globalnego load balancing) oraz umożliwiać definicję monitorowanych rekordów.

4.2.7.1. Całościowe zarządzanie usługą musi być możliwa poprzez wykorzystanie udostępnionego API.

4.2.7.2. Usługa powinna umożliwiać łatwą integrację z procesami DevOps Zamawiającego.

4.2.7.3. W ramach platformy musi być dostępny centralny system monitoringu pozwalający śledzić wykorzystanie zasobów i stan usług.

4.2.7.4. Platforma musi udostępniać narzędzia do monitorowania kosztów i optymalizacji wydatków. Zamawiający oczekuje możliwości ustawiania budżetów i progów kosztowych z alertami (np. powiadomienie, jeśli miesięczne koszty zbliżają się do określonego progu). Powinna być dostępna szczegółowa analiza kosztów per usługa/projekt oraz rekomendacje optymalizacyjne (np. niewykorzystane zasoby, propozycje rezerwacji).

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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4.3. Wymagania dotyczące backupu i Disaster Recovery (DR):

4.3.1. Wykonawca dostarczy usługę backupu danych, która zapewni tworzenie i odtwarzanie kopii zapasowych, konfigurowanie harmonogramów zgodnie z wymaganymi parametrami RPO/RTO. Środowisko obliczeniowe powinno zapewniać tworzenie mechanizmów Disaster Recovery w ramach pojedynczego i wielu regionów.

4.4. Mechanizmy wyjścia z usługi (off-boarding):

4.4.1. Zamawiający w ramach wynagrodzenia za realizację usługi (IaaS) musi mieć zagwarantowaną możliwości bezpiecznego zakończenia korzystania z usług po wygaśnięciu lub rozwiązaniu umowy, bez utraty swoich danych i z minimalnym zakłóceniem ciągłości działania. W związku z tym dane powinny być dostępne do bezpiecznego i integralnego wyniesienia w ciągu min. 30 dni od zakończenia świadczenia usługi.

4.4.1.1. Wykonawca zagwarantuje trwałe nieodwracalne, spełniające normy bezpiecznego usuniecie wszelkich danych Zamawiającego ze swoich systemów i nośników.

5. Dodatkowe wymagania:

5.1. Zamawiający oczekuje możliwości skorzystania z elastycznego modelu licencjonowania dla maszyn i usług. Jeżeli Zamawiający posiada własne licencje i platforma Wykonawcy to wspiera – powinien istnieć mechanizm BYOL (Bring Your Own License), tak aby można było użyć własnych licencji i obniżyć koszty.

5.2. Wykonawca musi posiadać co najmniej dwa regiony chmurowe zlokalizowane na obszarze Europejskiego Obszaru Gospodarczego (EOG), z czego co najmniej jedna strefa lokalna musi znajdować się na terytorium Rzeczypospolitej Polskiej, która umożliwi wykorzystanie usługi IaaS.

5.3. Interfejs do zarządzania usługami musi zostać udostępniony za pomocą strony www w języku polskim lub angielskim.

5.4. Musi istnieć możliwość utworzenia wielu użytkowników z różnym poziomem uprawnień.

6. Wymagania fakultatywne:

6.1. Wymagania fakultatywne stanowią kryterium oceny ofert.

6.2. Niespełnienie wymagań fakultatywnych nie stanowi podstawy do odrzucenia oferty.

6.3. Lista wymagań fakultatywnych:

6.3.1. Natywne usługi wspierające:

6.3.1.1. Centralnie Zarządzaną przez dedykowany zespół Sieć, która spełnia następujące wymagania:

- Pozwala wielu projektom lub zespołom w organizacji korzystać ze wspólnej sieci wirtualnej
- Projekty mogą uruchamiać swoje zasoby (maszyny wirtualne, kontenery, bazy danych itp.) w tej wspólnej sieci, ale nie mają kontroli nad jej konfiguracją
- Projekty korzystają z przydzielonych im podsieci w ramach centralnej sieci. Dostęp odbywa się na podstawie polityk RBAC.
- Zasoby podłączane do wydzielonej podsieci nie należą do projektu sieciowego co zapewnia zwiększoną separację zarządzania zasobami i siecią
- Centralne zarządzanie powinno obejmować:

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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- reguły zapory, trasy i podsieci
- Zespół bezpieczeństwa może wymuszać spójne polityki w całej organizacji
- Zespoły deweloperskie mogą korzystać z zasobów w sieci, ale nie mogą zmieniać ustawień sieci
- Kontrola dostępu na poziomie RBAC ma umożliwiać realizację zasady minimalnych uprawnień (least privilege).

6.3.1.2. Definiowanie stref bezpieczeństwa

- możliwość zdefiniowania na poziomie Polityk bezpieczeństwa strefy ochronnej wokół wrażliwych zasobów, kontrolując, które projekty lub sieci mogą je osiągnąć
- ochrona zasobów nawet przed uprawnionymi użytkownikami, jeśli próbują je użyć spoza wyznaczonej strefy
- zasoby wewnątrz strefy nie są dostępne z sieci zewnętrznych ani nieautoryzowanych projektów
- blokowanie przypadkowego lub złośliwego przesyłania danych
- Umożliwia ograniczanie dostępy według projektów, sieci oraz typów zasobów
- Działa we współpracy z bazą polityk uprawnień użytkowników

wspiera prywatną komunikację.

7. Model rozliczeniowy i warunki finansowe:

7.1. Model rozliczeń za usługi będzie oparty na faktycznym zużyciu zasobów („pay as you go"), bez stosowania mechanizmu przedpłat (prepaid). Wykonawca jest zobowiązany do bieżącej kontroli budżetu określonego w umowie oraz do informowania Zamawiającego o możliwości jego przekroczenia.

7.2. Rozliczenia będą prowadzone w PLN, a ceny jednostkowe poszczególnych usług będą wynikały z gwarantowanego w ofercie Wykonawcy rabatu % od cen zawartych w oficjalnym, aktualnie obowiązującym cenniku producenta platformy obliczeniowej. W przypadku konieczności przewalutowania z USD lub EUR, stosowany będzie kurs średni NBP z miesiąca poprzedzającego okres rozliczeniowy.

7.3. Zamawiający nie zobowiązuje się do zrealizowania zamówienia w określonej wartości a niewykorzystanie pełnej kwoty wynagrodzenia nie rodzi po stronie Zamawiającego żadnych roszczeń Wykonawcy.

7.4. Co miesiąc Wykonawca dostarczy Zamawiającemu szczegółowy raport zużycia zasobów (w formacie CSV/Excel oraz w podsumowaniu PDF), oraz odpowiadające im koszty. Po zaakceptowaniu raportu przez Zamawiającego Wykonawca wystawi fakturę VAT.

7.5. Przykładowy profil wykorzystania zasobów zawarty jest w załączniku nr 1 do niniejszego OPZ- „formularz cenowy", który posłuży do porównania ofert cenowych i jednocześnie stanowi minimalne wymagania funkcjonalne.

8. Kryteria oceny ofert:

8.1. Ocena ofert odbywać się będzie na podstawie **punktacji** przyznanej kryterium:

8.1.1. **Cena** – waga 80% (max 80 pkt).
W ramach kryterium ceny będzie oceniany łączny koszt w PLN brutto za przyjęty w celach

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

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

porównawczych profil wykorzystania. Najwyższą liczbę punktów w tym kryterium otrzyma oferta z **najniższą łączną** oferowaną ceną brutto. Pozostałe oferty otrzymają proporcjonalnie mniej punktów według formuły: *najniższa oferowana cena / cena oferty ocenianej *80 pkt*.

8.1.2. **Spełnienie wymagań fakultatywnych** – łączna waga 20% (max 20 pkt).

W ramach kryterium „Spełnienie wymagań fakultatywnych" będzie oceniane, czy oferta spełnia wymagania fakultatywne określone w OPZ. Kryterium ma charakter zero-jedynkowy i składa się z dwóch podkryteriów:

- **Spełnienie wymagania „Centralnie zarządzana sieć" – waga 10% (maksymalnie 10 pkt)**
  Jeżeli Wykonawca spełnia wszystkie wymaganie w tym zakresie– otrzymuje 10 pkt. Jeżeli nie spełnia choćby jednego – otrzymuje 0 pkt.
- **Spełnienie wymagania „Definiowanie stref bezpieczeństwa" – waga 10% (maksymalnie 10 pkt)**
  Jeżeli Wykonawca spełnia wszystkie wymaganie w tym zakresie– otrzymuje 10 pkt. Jeżeli nie spełnia choćby jednego – otrzymuje 0 pkt.

Punkty zostaną przeliczone zgodnie z wagą kryterium w ocenie końcowej.

8.2. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

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