WSTĘPNY OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa pakietów umożliwiających wykorzystanie zasobów chmury obliczeniowej na potrzeby rozwiązań informatycznych Centralnej Komisji Egzaminacyjnej

Spis treści:

I. Przedmiot i termin realizacji zamówienia

1. Wyrażenia pisane wielka literą w niniejszym Opisie przedmiotu zamówienia mają znaczenie nadane im w rozdziale II „Definicje".
2. Przedmiotem zamówienia jest sukcesywna dostawa, wg potrzeb Zamawiającego, Pakietów w ramach i na zasadach określonych w umowie Server and Cloud Enrollment (SCE) lub równoważnej, w okresie kolejnych 36-ciu miesięcy od aktywacji pierwszego Pakietu, z zastrzeżeniem, że umowa o udzielenie zamówienia zostanie zawarta na okres 42 miesięcy od daty jej podpisania.
3. Szczegółowe informacje dotyczące zakresu zamówienia podstawowego i opcji zostały opisane w rozdziale III OPZ.
4. Zamawiający gwarantuje że, w okresie 36 miesięcy, o których mowa w ust. 2, zakupi co najmniej 720 Pakietów (minimalny poziom realizacji zamówienia/wykorzystania umowy).
5. Zamawiający dopuszcza dostawę pakietu równoważnego do Pakietu nabywanego w ramach umowy Server and Cloud Enrollment (SCE) lub równoważnej. Warunki uznania Pakietu/umowy za równoważne określają kryteria oceny równoważności, określone w rozdziale VIII OPZ.
6. Opis przedmiotu zamówienia jest określony we Wspólnym Słowniku Zamówień jako: 48900000-7 Różne pakiety oprogramowania i systemy komputerowe.
7. Wykonawca zrealizuje przedmiot zamówienia w zakresie usług osadzonych na chmurze obliczeniowej zgodnie z normami ISO 27017:2015, ISO 27018:2019 (dopuszczalne są nowsze) lub równoważnymi i przedstawi certyfikaty (wystawione na Dostawcę) potwierdzające spełnienie wymagań tych norm lub norm równoważnych najpóźniej w dniu podpisania Umowy (przed podpisaniem Umowy). Za równoważne uważa się normy, która spełniają następujące warunki:
   1) normy dotyczą co najmniej usług osadzonych na chmurze obliczeniowej,
   2) normy są wydane przez niezależną jednostkę uprawnioną do certyfikowania,
   3) zakres przedmiotowej normy uznawanej za równoważną musi spełniać co najmniej wymagania wskazanej normy lub nowszej, co Wykonawca jest zobowiązany wykazać poprzez odniesienie się do każdego wymagania wskazanej normy.

II. Definicje

API - (ang. Application Programming Interface) - Interfejs programistyczny aplikacji, rozumiany, jako ściśle określony zestaw reguł, schematów, opisów, w jakich system może komunikować się z systemami zewnętrznymi.

Aktywacja Pakietu – uruchomienie Pakietu oferowanego przez Dostawcę

Botnet – Grupa komputerów zainfekowanych szkodliwym oprogramowaniem, pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach grupy.

Chmura publiczna – platforma udostępniająca usługi obliczeniowe oferowane przez Dostawcę za pośrednictwem publicznego Internetu.

CKE – Zamawiający, Centralna Komisja Egzaminacyjna.

DDoS (ang. Distributed Denial of Service) - rozproszona odmowa usługi, atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania usługi/systemu poprzez zajęcie wszystkich wolnych zasobów.

Dostawca - podmiot, który dostarcza zasoby chmurowe, spełniający definicję Dostawcy Usług Cyfrowych zgodnie z rozporządzeniem Wykonawczym Komisji UE 2018/151 z dnia 30 stycznia 2018 r.

IaC (ang. Infrastructure as Code) - to proces zarządzania i udostępniania komputerowych centrów danych za pomocą plików definicji do odczytu maszynowego, a nie fizycznej konfiguracji sprzętu lub interaktywnych narzędzi konfiguracyjnych. Definicje mogą znajdować się w systemie kontroli wersji. Kod w plikach definicji może wykorzystywać albo skrypty, albo definicje deklaratywne, zamiast utrzymywania kodu za pomocą procesów ręcznych.

IaaS (ang. Infrastructure as a Service) – model usługi chmury obliczeniowej zapewniający infrastrukturę chmury, na której odbiorca usług jest w stanie wdrożyć i uruchomić dowolne oprogramowanie (systemy operacyjne i aplikacje), jednak nie zarządza ani nie kontroluje infrastruktury chmury, z wyjątkiem kontroli nad systemami operacyjnymi, pamięcią masową i wdrożonymi aplikacjami oraz, ograniczoną kontrolą nad wybranymi komponentami sieciowymi.

OPZ – Opis przedmiotu zamówienia.

PaaS (ang. Platform as a Service) – model usługi chmurowej umożliwiający odbiorcy usług wdrożenie na infrastrukturze chmury aplikacji stworzonych przez siebie lub nabytych, które zostały przygotowane przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych przez dostawcę, w przypadku której odbiorca usług nie zarządza ani nie kontroluje infrastruktury chmury,

w tym sieci, serwerów, systemów operacyjnych oraz pamięci masowych, ale ma kontrolę nad wdrożonymi aplikacjami oraz nad ustawieniami konfiguracji środowiska dla aplikacji.

Pakiet – (Azure prepayment 6QK-00001 lub równoważny) to subskrypcja standardowa, powszechnie dostępna przez Internet, o określonej wartości, typu COTS (Commercial Of-The-Shelf), pozwalająca na dowolne korzystanie z usług lub aplikacji Chmury Publicznej oferowanych przez Dostawcę, w tym co najmniej w zakresie określonym w rozdziale VI OPZ.

RBAC (ang. Role Based Access Control) - kontrola dostępu oparta na rolach, mechanizm kontroli dostępu w systemach komputerowych.

SCE (ang. Server and Cloud Enrollment) - 3-letnie zobowiązanie podejmowane w ramach umowy Microsoft Enterprise Agreement (EA) umożliwiające zakup oprogramowania dla klientów dużych przedsiębiorstw gotowych do podjęcia całościowego zobowiązania tzn. standaryzacji infrastruktury IT w oparciu o wybrane technologie oferowane przez Microsoft dotyczące chmury obliczeniowej.

SIEM (ang. Security Information and Event Management) – system do zarządzania informacją i zdarzeniami bezpieczeństwa. Systemy SIEM pozwalają wykryć wszelkiego rodzaju anomalie, zagrożenia lub próby ataku, zbierając dane w jednym miejscu. Po przeprowadzeniu analizy generują spójny raport z wnioskami i rekomendacjami „na jednym ekranie”.

SLA (ang. Service Level Agreement) - umowa dotycząca poziomu oraz warunków świadczonych usług z zakresu IT, określająca na jakim minimalnym poziomie Wykonawca lub Dostawca będzie świadczyć określone usługi.

Scenariusz B2B (ang. Business-to-Business) - możliwość zapraszania użytkowników-gości do współpracy z organizacją. Dzięki współpracy B2B można bezpiecznie udostępniać aplikacje i usługi firmy użytkownikom zewnętrznym przy zachowaniu kontroli nad własnymi danymi organizacji.

Scenariusz B2C (ang. Business-to-Business) - dostarczenie tożsamości firma-klient jako usługę. Klienci korzystają z preferowanych tożsamości społecznościowych, firmowych lub lokalnych kont, aby uzyskać dostęp do logowania jednokrotnego do aplikacji i interfejsów API organizacji.

Standardowe Klauzule Umowne - oznaczają (i) standardowe klauzule ochrony danych dotyczące przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w państwach trzecich, które nie zapewniają odpowiedniego poziomu ochrony danych, jak opisano w art. 46 RODO i zatwierdzono decyzją Komisji Europejskiej (UE) nr 2021/914/WE z dnia 4 czerwca 2021 r.; (ii) wszelkie klauzule zastępujące obecne, przyjęte przez (a) Komisję Europejską (b) Europejskiego Inspektora Ochrony Danych i zatwierdzone przez Komisję Europejską (c) Wielką Brytanię zgodnie z brytyjską ogólną federalną ustawą o ochronie danych, (d) Szwajcarię zgodnie ze szwajcarską federalną ustawą o ochronie danych lub (e) przez rząd w jurysdykcji innej niż Szwajcaria, Wielka Brytania oraz jurysdykcje obejmujące Unię Europejską / Europejski Obszar

Gospodarczy, w których klauzule regulujące międzynarodowe przekazywanie danych osobowych, zostają włączone i obowiązują dostawcę z dniem ich przyjęcia.

Tenant – (dzierżawa) jest cyfrową reprezentacją organizacji i jest skojarzona z domeną, na przykład z .onmicrosoft.com.

Usługi COTS (ang. Commercial Off The Shelf) – usługi dostarczane w formie gotowego, zamkniętego produktu.

Wykonawca – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej składająca ofertę

VPN (ang. Virtual Private Network) - tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy nadawcą i odbiorcą za pośrednictwem sieci publicznej.

Zamawiający – Centralna Komisja Egzaminacyjna

III. Zamówienie podstawowe i opcje

1. W ramach realizacji przedmiotu zamówienia Zamawiający jest uprawniony do zakupu następującej liczby Pakietów:
   Tabela 1 – Liczba pakietów

Lp	Nazwa Pakietu	Liczba Pakietów - minimalna	Liczba Pakietów - maksymalna	Liczba Pakietów - maksymalna w opcji	Łączna maksymalna liczba Pakietów w okresie trwania umowy
		Zamówienie podstawowe		opcja	
1	Pakiet (Azure prepayment 6QK-00001 lub równoważny)	720	1000	10400	11400

2. Pierwszych 720 Pakietów zostanie jednorazowo zakupione przez Zamawiającego i Aktywowane w okresie do 6 miesięcy od dnia zawarcia umowy z Wykonawcą.
3. W okresie trwania umowy Zamawiający, w ramach zamówienia podstawowego jest uprawniony zakupić maksymalnie 1000 Pakietów, z zastrzeżeniem, że minimalna liczba Pakietów którą Zamawiający zobowiązuje się nabyć w okresie trwania umowy to 720. Oznacza to, że w przypadku gdy Zamawiający zakupi w trakcie trwania umowy 720 Pakietów i więcej, Wykonawcy nie przysługuje żadne roszczenie w zakresie dot. zakupu pozostałych pakietów przewidzianych do nabycia w ramach zamówienia podstawowego, w tym za utracone korzyści.
4. Zamawiający zastrzega sobie prawo do rozszerzenia zakresu zamówienia o opcję, tj. 10400 Pakietów ponad liczbę Pakietów przewidzianych w zamówieniu podstawowym. Zamówienie w ramach opcji będzie uruchamiane w okresie trwania umowy poprzez przekazanie Wykonawcy oświadczenia woli o jej uruchomieniu zawierającego liczbę uruchomianych Pakietów w ramach opcji. Pakiety w ramach opcji mogą być uruchomione w dowolnej liczbie od 1-10400, po wykorzystaniu Pakietów przewidzianych w zamówieniu podstawowym. Opcja może być uruchamiana wielokrotnie aż do wykorzystania maksymalnej liczby Pakietów przewidzianych w ramach opcji.
5. W przypadku nie wykorzystania przez Zamawiającego opcji w całości lub części (liczba Pakietów w ramach opcji) Wykonawcy nie przysługuje jakiekolwiek roszczenie za jej niewykorzystanie, w tym za utracone korzyści.

IV. Pakiet – uruchomienie i minimalne wymagania

1. Oferowane przez Wykonawcę Pakiety mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
2. Zamawiający wymaga dostawy i realizacji Pakietów na warunkach przewidzianych w umowie licencyjnej z Dostawcą.
3. Wykonawca przed podpisaniem umowy udostępni Zamawiającemu link do stron/y internetowych/ej Dostawcy zawierającej/ych opis oferowanych Pakietów oraz zasad ich używania wraz ze zobowiązaniami Dostawcy w zakresie ochrony danych.
4. Wykonawca, po zawarciu Umowy, a przed rozpoczęciem korzystania z Pakietów, udostępni mechanizmy podpisania przez Zamawiającego umowy licencyjnej z Dostawcą.
5. Wykonawca, w terminie do 10 dni roboczych od podpisania Umowy, udzieli uprawnień Zamawiającemu – osobom upoważnionym przez Zamawiającego do wykorzystania Pakietów na stronie Dostawcy.
6. Pakiety wyrażają swoją wartość w walucie EUR, wskazaną przez Wykonawcę w treści oferty, celem rozliczenia zużycia przez Zamawiającego usług/aplikacji oferowanych przez Dostawcę. Wartość Pakietu nie ulega zmianie w okresie trwania Umowy.
7. W ramach Pakietów Zamawiający może zamawiać dowolne aplikacje/usługi oferowane przez Dostawcę w zakresie minimalnym określonym w rozdziale VI i zużywane zgodnie z ogólnodostępnym cennikiem Dostawcy usług chmurowych.
8. Minimalny zakres Pakietu – w ramach jednego Pakietu musi być możliwe łączne uruchomienie i nieprzerwane korzystanie w ciągu jednego miesiąca (730 godzin) z usług o parametrach opisanych poniżej lub wyższych:
    a) 1 maszyna wirtualna o parametrach - 1 rdzeń procesora, 3,5 GB RAM, 7 GB dysku tymczasowego. System operacyjny z rodziny Linux (Open Source).
    b) 7 GB dostępnej lokalnie redundantnej przestrzeni dyskowej na dyskach SSD, 500 IOPS, 100 MB/sec.
    c) 650 GB transferu danych do, i 650 GB transferu danych z aplikacji/usługi miesięcznie.

V. Chmura Publiczna - minimalne wymagania:

1. Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług.
2. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów, z możliwością zdalnego dostępu.
3. Komunikacja z mechanizmami zarządzania usługi poprzez REST API.
4. Dostępność mechanizmów integracji danych zawierających:
   1) Mechanizmy zarządzania integracji danych wraz z konektorami do źródeł danych:
      a) Dane strukturalne i niestrukturalne,
      b) Data Lake,
      c) Relacyjne bazy danych,
      d) Strumienie danych;
   2) Zarządzanie API w postaci hybrydowej, wielochmurowej platformy zarządzania interfejsami API w wybranych środowiskach.
      b) Usługi umożliwiające tworzenie aplikacji z architekturą opartą na zdarzeniach, z wbudowaną obsługą zdarzeń pochodzących z usług platformy, takich jak obiekty blob magazynu i grupy zasobów,
      c) Usługi tworzenia i uruchamiania zautomatyzowanych przepływów pracy, które integrują aplikacje, dane, usługi i systemy, pozwalające na tworzenie skalowalnych rozwiązań integracyjnych dla Scenariuszy B2C i B2B pozwalając łączyć systemy w środowiskach chmurowych, lokalnych i hybrydowych,
      d) Zarządzany broker komunikatów z kolejkami komunikatów oraz tematami publikowania i subskrybowania (w przestrzeni nazw), umożliwiający oddzielanie aplikacji i usług od siebie i zapewniający:
         i. Równoważenie obciążenia między zadaniami,
         ii. Bezpieczne kierowanie i przesyłanie danych oraz kontrolę między granicami usług i aplikacji,
         iii. Koordynowanie prac transakcyjnych, które wymagają wysokiego stopnia niezawodności;
5. Dostępność narzędzi kompleksowego zarządzania danymi w środowiskach hybrydowych wraz z mechanizmami klasyfikacji danych.
6. Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a Dostawcą usług chmurowych w technologii opartej o światłowody.
7. Posiadanie przez Dostawcę centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.

8. Możliwość budowania potoków automatyzacji wdrażania i uruchamiania aplikacji zarówno w postaci infrastruktury pod aplikację, jak i budowania kontenerów oraz wdrażania i uruchamiania aplikacji, testowania aplikacji i generowania raportów z procesu.
9. Włączenie reguł wymuszających stosowanie się do odpowiedniej nomenklatury nazewnictwa zasobów w obrębie środowiska, wymuszając wykorzystanie ustalonego modelu nazw, prefiksów dla określonych typów zasobów.
10. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci, systemy operacyjne).
11. Możliwość zdefiniowania szablonu maszyny wirtualnej włącznie z konfiguracją aplikacji, uruchamiania serwisów poprzez zdefiniowanie stanu oczekiwanego w postaci plików konfiguracyjnych.
12. Możliwość wyboru różnych rodzajów dysków i ich pojemności.
13. Możliwość przechowywania danych spełniająca następujące wymagania:
    1) Skalowalność, auto-partycjonowanie, równoważenie obciążenia.
    2) Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka.
    3) Wsparcie dla systemów klienckich Windows i Linux.
    4) Replikacja danych - minimum 3 kopie w ramach pojedynczej lokalizacji.
    5) Replikacja do innej lokalizacji oddalonej o min. 400 km od lokalizacji podstawowej.
    6) Udostępnienie zasobów pamięci poprzez REST API.
14. Muszą posiadać możliwość replikacji danych w przynajmniej dwóch równorzędnych ośrodkach przetwarzania danych, których odległość od siebie gwarantuje bezpieczeństwo, niezależność oraz możliwość odtworzenia kopii danych w przypadku dużych zdarzeń losowych skutkujących zniszczeniem jednego z miejsc replikacji danych (m.in. w wyniku utraty zasilania, wybuchu, awarii sprzętu itp.). Zamawiający wymaga ośrodków odległych od siebie o co najmniej 400 km.
15. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów członkowskich Unii Europejskiej.
16. Możliwość automatycznej dystrybucji danych pomiędzy różne regiony oraz ulokowane w nich centra obliczeniowe wraz z możliwością ręcznego, jak i automatycznego przełączania replik.
17. Wykonawca zapewni dostęp do spersonalizowanej strony Dostawcy pozwalającej upoważnionym osobom ze strony Zamawiającego na:
    1) Pobieranie zakupionego oprogramowania.
    2) Aktywację zakupionego oprogramowania i usług.
    3) Sprawdzanie liczby zakupionych usług w wykazie zakupionych usług.
18. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
19. Konfigurowalne usługi wyszukiwania treści w zasobach własnych i Internet.
20. Konfigurowalne usługi analizy wyszukanych treści.

21. Dostępność mechanizmów zarządzania danymi z różnych środowisk wraz z ich klasyfikacją i określeniem uprawnień dostępu.
22. Dostępność usług umożliwiających uruchamianie aplikacji webowych w modelu gotowej do wykorzystania usługi, z utrzymywanymi przez dostawcę usług komponentami infrastruktury i możliwości w pełni automatycznego skalowania. Usługi te powinny zapewniać możliwość uruchamiania aplikacji działających w minimum następujących technologiach: ASP .NET, Python, Node js.
23. Dostępność gotowej usługi realizującej kopię i archiwizację serwerów oraz stacji roboczych – zarówno wirtualnych, jak i fizycznych. Usługa musi zapewniać całościowy scenariusz kopii i archiwizacji, bez konieczności instalacji komponentów spoza samej usługi, z możliwością definiowania polityk kopii i archiwizacji, wbudowanym szyfrowaniem i możliwością zdefiniowania rozporoszonej geograficznie przestrzeni magazynowej.
24. Dostępność relacyjnej bazy danych, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
25. Możliwość serializacji do określonego formatu tekstowego (np. opartego o XML lub JSON) rozwiązań opartych o maszyny wirtualne, wraz z ich konfiguracją, w sposób umożliwiający ich automatyczną deserializację i utworzenie na tej podstawie gotowego do pracy środowiska.
26. Możliwość wykorzystania usług SMB 3.0 do współdzielenia plików wykorzystując szyfrowanie podczas transmisji, jako usługa.
27. Dostępność usług umożliwiających utworzenie prywatnego repozytorium obrazów kontenerów w standardzie zgodnym z Docker.
28. Dostępność usług umożliwiających utworzenie gotowej do działania infrastruktury utrzymania aplikacji w formie kontenerów zgodnych z Docker – usługi działającej w formie PaaS, w szczególności bez konieczności ręcznego konfigurowania węzłów roboczych i zarządzających.
29. Możliwość analizy ruchu sieciowego.
30. Po 120-stu dniach od zakończenia okresu trwania Umowy, o ile strony nie postanowią inaczej, Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Dostawcy i usunięcie danych Zamawiającego z centrów przetwarzania Dostawcy.
31. Gwarancję braku dostępu do danych Zamawiającego przez Dostawcę, z wyłączeniem działań serwisowych i wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy.
32. Zapewnienie przetwarzania danych osobowych zgodnie z wymaganiami przepisów prawa, a w szczególności w zakresie ochrony danych osobowych w tym Ogólnym rozporządzeniem o ochronie danych.
33. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi zarządzania tożsamością będącej składową usług oferowanych przez Dostawcę.
34. Zamawiający wymaga, aby dostarczone usługi korzystały wprost z mechanizmów zarządzania tożsamością użytkowników posiadanej przez Zamawiającego usługi Entra Identity Premium Plan 2

w ramach posiadanych Tenantów i umożliwiały wsparcie techniczne Dostawcy dla tych mechanizmów, a w szczególności wymaganych funkcjonalności:

1) Dostęp warunkowy oparty na ryzyku (ryzyko logowania, ryzyko użytkownika).
2) Filtry urządzenia i aplikacji na potrzeby dostępu warunkowego.
3) Ochrona tokena.
4) Luki w zabezpieczeniach i ryzykowne konta.
5) Badanie zdarzeń o podwyższonym ryzyku.
6) Serwer proxy aplikacji dla lokalnego, opartego na nagłówkach i zintegrowanego uwierzytelniania systemu Windows.
7) Współpraca w ramach bezpiecznego dostępu hybrydowego (Kerberos, NTLM, LDAP, RDP i uwierzytelnianie SSH).
8) Samoobsługowe resetowanie haseł/zmienianie/odblokowywanie.
9) Samoobsługowe wyszukiwanie i raportowanie aktywności dotyczącej logowania.
10) Samoobsługowe zarządzanie grupą (Moje grupy).
11) Samoobsługowe zarządzanie upoważnieniami (Mój dostęp).
12) Uwierzytelnanie bezhasłowe (Microsoft Authenticator, FIDO2, integracje klucza zabezpieczeń).
13) Zarządzanie okresem istnienia sesji
14) Globalna ochrona hasłami i zarządzanie (w tym niestandardowe zabronione hasła)
15) Integracja z posiadanym systemem zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM) Microsoft Sentinel.

VI. Usługi, w ramach pakietów - minimalne wymagania

1. Usługi wykorzystywane w ramach Pakietów (łącznie z pojedynczym wystąpieniem maszyny wirtualnej) muszą zapewniać dostępność na poziomie minimum 99,9%.
2. Dostarczone usługi muszą mieć możliwość objęcia ich wsparciem technicznym Dostawcy – Premier Support, Unified Support lub równoważne.
3. Zamawiający dopuszcza oferowanie usług o szerszej niż opisana w OPZ funkcjonalności. Zamawiający wymaga dostawy usług na warunkach przewidzianych przez Dostawcę.
4. Usługi muszą pochodzić od jednego Dostawcy chmury obliczeniowej.
5. Zamawiający wymaga dostępności w ramach pakietów co najmniej usług o następujących parametrach:

Tabela 2 – minimalne wymagania w zakresie usług

L.p.	Usługa	Opis
1.	**Zapora typu Firewall**	1.1. Zarządzana usługa zapory sieciowej, zapewniająca filtrowanie w warstwach L3-L7 modelu ISO OSI oparte na informacjach o zagrożeniach, ostrzegające i blokujące ruch z/do znanych złośliwych adresów IP i domen, aktualizowane w czasie rzeczywistym w celu ochrony przed nowymi i pojawiającymi się atakami. Usługa musi posiadać wbudowaną wysoką dostępność oraz nieograniczoną skalowalność w chmurze. Usługa musi zapewniać inspekcję ruchu sieciowego zarówno wschód-zachód, jak i północ-południe. Usługa musi zapewniać możliwość wdrażania i rejestrowania polityk połączeń aplikacji oraz podsieci w ramach sieci wirtualnych. 1.2. Wymagane funkcjonalności: • Obsługa skalowalności w chmurze • Obsługa przepustowości do 30 Gbps • Obsługa reguł filtrowania w pełni kwalifikowanych nazw domen aplikacji • Obsługa reguł filtrowania ruchu sieciowego • Obsługa etykiet dla w pełni kwalifikowanych nazw domen (FQDN) • Obsługa etykiet dla usług • Wsparcie dla serwera proxy DNS • Obsługa nazw FQDN w regułach sieci • Obsługa translacji adresów sieciowych źródła (SNAT) dla ruchu wychodzącego • Obsługa technologii DNAT dla ruchu przychodzącego • Obsługa wymuszonego tunelowania • Obsługa kategorii witryn Web • Obsługa odporności na awarię pojedynczego centrum danych 1.3 SLA, minimalna dostępność: 99,95%

2.	**Zapora dla aplikacji internetowej**	2.1. Zarządzana usługa służąca do równoważenia obciążenia, działająca w warstwie L7 modelu ISO OSI lub równoważnych z wbudowaną zaporą internetową, zapewniającą scentralizowaną ochronę aplikacji internetowych przed popularnymi zagrożeniami typu exploit oraz podatnościami. Ochrona przed atakami typu: wstrzykiwanie kodu SQL i cross-site scripting. Usługa wbudowanej zapory internetowej opartej na Core Rule Set (CRS) z Open Web Application Security Project (OWASP). Możliwość wdrożenia wielu polityk, które mogą być skojarzone z bramą aplikacji, z poszczególnymi listenerami lub z regułami routingu opartymi na ścieżkach. 2.2. Wymagane funkcjonalności: • Obsługa routingu opartego na adresach URL • Obsługa Transport Layer Security (TLS) / SECURE Sockets Layer (SSL) • Obsługa protokołu WebSocket • Obsługa protokołu HTTP/2 • Automatyczne skalowanie • Obsługa statycznych adresów VIP • Integracja z usługą bezpiecznego miejsca przechowywania wpisów tajnych • Obsługa uwierzytelniania mTLS (mutual SSL) • Integracja dla środowisk zarządzania klastrami Kubernetes do kontrolowania ruchu przychodzącego • Skalowalność zapory oparta o liczbę utrzymywanych połączeń i/lub przepustowość • Obsługa odporności na awarię pojedynczego centrum danych • Ilość połączeń trwałych: minimum 1000 • Przepływność: minimum 100 Mb/s • Liczba jednostek obliczeniowych: minimum 45 • Transfer wychodzący: minimum 100 GB 2.3. SLA, minimalna dostępność**:** 99,95%
3.	**Zarządzana usługa klastra Kubernetes**	3.1 Zarządzana usługa klastra Kubernetes z funkcjonalnością automatycznej obsługi krytycznych zadań, takich jak monitorowania stanu, tworzenia i konfigurowania warstwy kontrolnej. Wsparcie dla tworzenia usługi za pomocą wiersza poleceń i graficznego interfejsu użytkownika, jak i za pośrednictwem szablonów typu IaC. Usługa musi umożliwiać konfigurację zaawansowanych funkcji sieciowych, integrację z usługami tożsamości chmurowej, monitorowanie. 3.2 Wymagane funkcjonalności dla węzłów Klaster System Pool: • Procesor: 2vCpu, 3.5 GHz • Pamięć RAM minimum: 8GB • Dyski minimum: 75 GB przestrzeni dyskowej SSD

		Ilość węzłów minimum: 2 3.3 SLA, dostępność minimum: 99,95%
4.	**Zarządzana usługa klastra Kubernetes**	4.1 Zarządzana usługa klastra Kubernetes z funkcjonalnością automatycznej obsługi krytycznych zadań, takich jak monitorowania stanu, tworzenia i konfigurowania warstwy kontrolnej. Wsparcie dla tworzenia usługi za pomocą wiersza poleceń i graficznego interfejsu użytkownika, jak i za pośrednictwem szablonów typu IaC. Usługa musi umożliwiać konfigurację zaawansowanych funkcji sieciowych, integrację z usługami tożsamości chmurowej, monitorowanie. 4.2 Wymagane funkcjonalności dla węzłów Klaster User Pool: • Procesor: 4vCpu, 3.5 GHz • Pamięć RAM minimum: 16GB • Dyski minimum: 150 GB przestrzeni dyskowej SSD • Ilość węzłów minimum: 2 4.3 SLA, dostępność minimum: 99,95%
5.	**Zarządzana usługa bazy danych Microsoft SQL**	5.1. Zarządzana usługa pojedynczej, odizolowanej bazy danych zbudowana na silniku Microsoft SQL. Usługa realizowana w ramach modelu zakupowego opartego na rzeczywistej utylizacji rdzeni CPU, pamięci RAM, oraz operacji odczytu i zapisu. Struktura/Typ bazy danych wynika z budowy istniejącego systemu, który będzie wykorzystywał Infrastrukturę. 5.2. Wymagane funkcjonalności: • Liczba baz: minimum 1 szt. • Wydajność: minimum: 2vCpu • Pojemność minimum: 250GB • Pojemność na kopie zapasowe minimum: 500GB 5.3. SLA, minimalna dostępność: 99,99%
6.	**Zarządzana usługa rejestru oparta na standardzie open-source Docker Registry**	6.1 Zarządzana usługa rejestru oparta na standardzie open-source Docker Registry 2.0. Usługa musi umożliwiać tworzenie i utrzymywanie repozytorium kontenerów, aby móc przechowywać i zarządzać obrazami kontenerów oraz powiązanymi artefaktami. Usługa musi wspierać integrację z potokami tworzenia i wdrażania kontenerów ze znanymi narzędziami DevOps, np. Jenkins, Azure DevOps, AWS Code Pipelines. Usługa musi umożliwiać budowanie obrazów na żądanie i w pełni zautomatyzowaną kompilację obrazów. Wymagane funkcjonalności: • Liczba repozytoriów: minimum 1 szt. • Pojemność minimum: 100 GB

		6.2 SLA**,** minimalna dostępność**:** 99,9%
7.	**Usługa zarządzania wpisami tajnymi**	7.1 Zarządzana usługa do zarządzania kluczami, sekretami oraz certyfikatami. 7.2 Wymagane funkcjonalności: • Centralne miejsce przechowywania haseł i kluczy aplikacji umożliwiające kontrolę ich dystrybucji • Bezpieczne przechowywanie haseł i kluczy, za pośrednictwem odpowiednich mechanizmów uwierzytelniania oraz autoryzacji chroniące przed dostępem do nich użytkownika lub aplikacji. • Monitorowanie dostępu do haseł i kluczy, zintegrowane z pozostałymi elementami środowiska. • Administrację całym cyklem życia hasła lub klucza. • Obsługa min. kluczy RSA 2048-bit, RSA 3072-bit, RSA 4096-bit, Elliptic-Curve Cryptography (ECC) • Wsparcie dla FIPS 140-2 poziom 2 lub równoważnego • Liczba operacji dla kluczy RSA 2048-bit: minimum 100 000 • Liczba operacji dla pozostałych kluczy: minimum 10 000 7.3 SLA**,** dostępność**:** minimum 99,9%
8.	**Zarządzana usługa brokera komunikatów**	8.1 Zarządzana usługa brokera komunikatów, obsługująca kolejki komunikatów oraz zarządzanie tematami w schemacie publish-subscribe. 8.2 Wymagane funkcjonalności: • Obsługa rozdzielania aplikacji i usług od siebie, w celu równoważenia obciążenia pomiędzy konkurującymi usługami typu worker • Obsługa bezpiecznego kierowania i przesyłania danych oraz kontroli na granicy usług oraz aplikacji • Obsługa koordynacji pracy transakcyjnej • Obsługa integracji z wirtualną siecią • Liczba obsługiwanych komunikatów: minimum 500 000 8.3 SLA**,** dostępność**:** minimum 99,9%
9.	**Zarządzana usługa służąca do przechowywania danych obiektowych**	9.1. Zarządzana usługa służąca do przechowywania danych obiektowych, zoptymalizowana do przechowywania danych nieustrukturyzowanych (takich, które nie przynależą do określonego modelu danych lub definicji, np. tekst lub dane binarne) oraz danych podlegających częstym zmianom. 9.2. Wymagane funkcjonalności: • Obsługa dostępu dla użytkowników lub usług za pośrednictwem HTTP/HTTPS • Dane obiektowe w usłudze muszą być dostępne za pośrednictwem REST API, wiersza poleceń lub bibliotek programistycznych

		• Obsługa bezpiecznego dostępu za pośrednictwem SSH File Transfer Protocol (SFTP) i monitorować za pomocą protokołu Network File System (NFS) min. 3.0 • Dane muszą być przechowywane w przynajmniej w trzech miejscach. • Pojemność minimum: 4096 GB 9.3. SLA**,** dostępność**:** minimum 99,9%
10.	**Zarządzana usługa maszyny wirtualnej do celów administracyjnych**	10.1 Usługa zarządzanej maszyny wirtualnej, dostępnej na żądanie. 10.2 Wymagania/Typ systemu operacyjnego wynikają z budowy istniejącego systemu, który będzie wykorzystywał Infrastrukturę. 10.3 Wymagane funkcjonalności dla każdej maszyny wirtualnej: • Usługa musi zapewniać elastyczność wirtualizacji bez konieczności zakupu i utrzymywania fizycznego sprzętu, który ją obsługuje • Specyfikacja techniczna maszyny wirtualnej musi wspierać możliwość wyboru rozmiaru, oferującego liczbę rdzeni, moc procesora, pamięci RAM oraz pojemności dysków • Usługa musi oferować model zakupowy oparty na rzeczywistej, godzinowej utylizacji, z dokładnością do każdej minuty działania • Wymagany system operacyjny: Linux (Open Source) • Procesor: minimum 1 vCpu • Pamięć RAM: minimum 3.5 GB • Dysk tymczasowy: minimum 7 GB • Dysk: minimum 7 GB redundantnej lokalnie przestrzeni dyskowej, SSD (500 IOPS, 100 MB/sec.) • Transfer: 650 GB transferu danych do, i 650 GB transferu danych z aplikacji/usługi miesięcznie 10.4 SLA, dostępność: minimum 99,9%
11.	**Zarządzana usługa maszyny wirtualnej dla usług raportowania**	11.1 Usługa zarządzanej maszyny wirtualnej, dostępnej na żądanie. 11.2 Wymagania/Typ bazy danych i systemu operacyjnego wynikają z budowy istniejącego systemu, który będzie wykorzystywał Infrastrukturę. 11.3 Zamawiający wymaga minimum 2 maszyn wirtualnych, dla każdej wymagane funkcjonalności to: • Usługa musi zapewniać elastyczność wirtualizacji bez konieczności zakupu i utrzymywania fizycznego sprzętu, który ją obsługuje

		• Specyfikacja techniczna maszyny wirtualnej musi wspierać możliwość wyboru rozmiaru, oferującego liczbę rdzeni, moc procesora, pamięci RAM oraz pojemności dysków • Usługa musi oferować model zakupowy oparty na rzeczywistej, godzinowej utylizacji, z dokładnością do każdej minuty działania • System raportowania wymaga oprogramowania bazodanowego Microsoft SQL Server Standard oraz systemu operacyjnego Microsoft Windows Server • Wymagany system operacyjny: Windows • Procesor: minimum 4vCpu • Pamięć RAM: minimum 16GB • Dyski: minimum 512 GB przestrzeni dyskowej SSD na dane 11.4 SLA, dostępność**:** minimum 99,9%
12.	**Zarządzana usługa publicznego adresu IP**	12.1. Usługa zarządzanego publicznego adresu IP, umożliwiającego komunikację przychodzącą zasobom internetowym. 12.2. Wymagane funkcjonalności: • Adres IP musi być dedykowany dla danego zasobu z możliwością rezerwacji stałej • Usługa musi wspierać adresację według standardu IPv4 • Obsługa odporności na awarię pojedynczego centrum danych • Liczba adresów: minimum 9 12.3 SLA, dostępność: minimum 99,95%
13.	**Zarządzana usługa wirtualnej sieci**	13.1. Usługa sieci wirtualnej umożliwiająca bezpieczną komunikację usług chmurowych pomiędzy sobą, z Internetem oraz sieciami lokalnymi. 13.2. Wymagane funkcjonalności: • Usługa musi wspierać połączenia pomiędzy sieciami wirtualnymi w topologii sieciowej Hub and Spoke, za pomocą zabezpieczonego, prywatnego kanału, opartego na wewnętrznej sieci szkieletowej dostawcy chmurowego • W komunikacji między sieciami wirtualnymi nie może być wymagany publiczny Internet, bramy czy szyfrowanie, a opóźnienia w obrębie tego samego regionu nie mogą być większe niż podczas komunikacji wewnątrz sieci wirtualnej. • Ilość danych (transfer pomiędzy sieciami): minimum 20480 GB
14.	**Zarządzana usługa wirtualnej bramy sieciowej**	14.1. Usługa zarządzanej wirtualnej bramy sieciowej służąca do wysyłania zaszyfrowanego ruchu pomiędzy siecią wirtualną a lokalizacjami lokalnymi przez publiczny Internet. 14.2. Wymagane funkcjonalności: • Usługa musi wspierać utworzenie wielu zaszyfrowanych kanałów, w topologii Site-to-site (protokół IPsec) oraz Point-to-

		site (protokoły Secure Sockets Tunneling Protocol (SSTP), OpenVPN, IPsec) • Usługa musi posiadać możliwość skalowania na żądanie • Ilość jednoczesnych połączeń (tunele S2S): minimum 16 • Ilość danych (transfer pomiędzy sieciami): minimum 10240 GB 14.3. SLA, dostępność: minimum 99,95%
15.	**Zestaw narzędzi i procesów wspierających współpracę**	15.1. Zestaw narzędzi i procesów wspierających współpracę programistów, kierowników projektów i współpracowników w celu tworzenia oprogramowania. Zestaw narzędzi musi zapewniać zintegrowane funkcjonalności, do których można uzyskać dostęp za pośrednictwem przeglądarki internetowej lub środowiska programistycznego (klienta IDE, Integrated Development Environment). Możliwość selektywnego wyboru narzędzi, w tym: • Narzędzia Agile wspierające planowanie i śledzenie pracy, defektów kodu i problemów przy użyciu metod min. Kanban i Scrum. • Usługi budowania i wdrażania, wspierające ciągłą integrację i dostarczanie aplikacji. • Narzędzia służące do testowania aplikacji, w tym testowanie ręczne/eksploracyjne i testowanie ciągłe. • Usługi umożliwiające udostępnianie pakietów, w szczególności takich jak Maven, npm, NuGet z publicznych i prywatnych źródeł oraz integrowanie udostępniania pakietów w tzw. pipeline'ach.
16.	**Zarządzana usługa monitorowania środowiska oraz pozyskiwania i przechowywania danych dziennika (logów)**	16.1. Zarządzana usługa do monitorowania służąca do zbierania, analizowania i reagowania na dane telemetryczne z usług chmurowych. 16.2. Wymagane funkcjonalności: • Usługa musi zbierać i agregować dane z każdej warstwy i składnika usług chmurowych do wspólnej platformy danych. Usługa musi posiadać narzędzia do analizy i wizualizacji, aby ułatwić zrozumienie sposobu działania usług i aplikacji chmurowych oraz automatycznego reagowania na zdarzenia systemowe • Ilość zbieranych dzienników (logów) minimum: 3 GB dziennie • Czas działania (przechowywanie danych): minimum 18 miesięcy
17.	**Zarządzana usługa punktów końcowych usługi wirtualnej sieci**	17.1. Zarządzana usługa punktu końcowego **(endpoint)** usługi wirtualnej sieci. 17.2. Wymagane funkcjonalności: • Usługa zapewnia bezpieczną i bezpośrednią łączność z innymi usługami Infrastruktury za pośrednictwem

		zoptymalizowanej trasy przez sieć szkieletową Dostawcy chmury obliczeniowej. ● Punkty końcowe muszą umożliwiać zabezpieczanie krytycznych zasobów Infrastruktury tylko do sieci wirtualnych. ● Punkty końcowe usługi muszą umożliwiać prywatnym adresom IP w sieci wirtualnej uzyskiwanie dostępu do punktu końcowego usług Infrastruktury bez konieczności korzystania z publicznego adresu IP w sieci wirtualnej. ● Ilość punktów końcowych: minimum 3 ● Ilość danych wychodzących: minimum 20480 GB dla zarządzanej usługi wirtualnej sieci ● Ilość danych wchodzących minimum 20480 GB dla zarządzanej usługi wirtualnej sieci
18.	**Zarządzana usługa prywatnych stref DNS**	18.1. Zarządzana usługa prywatnych stref DNS. 18.2. Wymagane funkcjonalności: ● Automatyczna rejestracja maszyn wirtualnych z sieci wirtualnej połączonej ze strefą prywatną z włączoną funkcją automatycznego rejestrowania. Maszyny wirtualne mieć możliwość rejestracji w strefie prywatnej jako rekordy A wskazujące ich prywatne adresy IP. Gdy maszyna wirtualna w połączeniu sieci wirtualnej z włączoną funkcją autorejestracji zostanie usunięta, usługa automatycznie usunie odpowiedni rekord DNS z połączonej strefy prywatnej. ● Przekazywanie rozpoznawania nazw DNS musi być obsługiwane w sieciach wirtualnych połączonych ze strefą prywatną. W przypadku rozpoznawania nazw DNS między sieciami wirtualnymi nie może być jawnej zależności, tak aby sieci wirtualne były ze sobą równorzędne. ● Wsteczne wyszukiwanie DNS musi być obsługiwane w zakresie sieci wirtualnej. Wsteczne wyszukiwanie DNS dla prywatnego adresu IP skojarzonego z strefą prywatną zwróci nazwę FQDN zawierającą nazwę hosta/rekordu i nazwę strefy jako sufiks. ● Ilość hostowanych stref DNS: minimum 6 ● Zapytania DNS (w milionach): minimum 1

VII. Bezpieczeństwo usług chmurowych - minimalne wymagania

1. Muszą spełniać zapisy umowne zawierające tzw. Standardowe Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych.
2. Muszą spełniać zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
3. Muszą spełniać zobowiązania umowne Dostawcy potwierdzające zgodność z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „Ogólne rozporządzenie o ochronie danych") oraz potwierdzające rolę Dostawcy jako przetwarzającego dane.
4. Muszą posiadać dostępne mechanizmy pełnej rozliczalności działań użytkowników w usługach.
5. Muszą zapewniać automatyczną, niewpływającą na ciągłość pracy systemów Zamawiającego działających na usługach chmury obliczeniowej instalacji poprawek przez Dostawcę chmury obliczeniowej dla wybranych składników usługi.
6. Muszą posiadać mechanizmy monitorowania zachowania użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego.
7. Muszą posiadać możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania na bazie własnej usługi katalogowej.
8. Muszą posiadać dzienniki informujące o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione".
9. Muszą posiadać mechanizm uwierzytelnienia wieloskładnikowego.
10. Muszą posiadać możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN).
11. Muszą posiadać wbudowane mechanizmy zabezpieczające przez atakami DDoS.
12. Muszą posiadać raporty odnośnie dzienników z urządzeń potencjalnie zainfekowanych, z sieci Botnet.
13. Muszą posiadać silnik rekomendacji zabezpieczeń infrastruktury oparty o algorytmy uczenia maszynowego.
14. Muszą posiadać usługi umożliwiające przechowywanie certyfikatów, haseł dostępu zgodnie ze standardem FIPS 140-2 poziomu 2 lub równoważnym. Zamawiający wskazuje następujące kryteria stosowane w celu oceny równoważności dla ww. Normy i uzna za równoważną opisywanej, normę która łącznie:
    1) definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
    2) została wydana przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,
    3) opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
    4) została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.

15. Muszą posiadać gradację zakresu uprawnień i budowa konfigurowalnych zasad i ról dostępu do środowiska do poziomu pojedynczych kart sieciowych, dysków czy zarządzania uprawnieniami (tzw. RBAC, Role-Based Access Control).
16. Muszą udostępniać na żądanie Zamawiającego wyniki aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO posiadanymi przez Dostawcę.
17. Muszą umożliwiać zastrzeżenie miejsca uruchomienia usług i składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego (EOG).
18. Muszą umożliwiać korzystanie z przynajmniej dwóch równorzędnych centrów przetwarzania danych Dostawcy, składających się z przynajmniej trzech redundantnych ośrodków przetwarzania i położonych na obszarze EOG, w tym na terenie Polski.
19. Muszą udostępniać zapisy umowne Dostawcy zawierających tzw. Standardowe Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych.
20. Muszą posiadać, zarządzane przez Dostawcę centra przetwarzania, w których działają w trybie 24/7 zespoły monitorujące i zwalczające cyberataki oraz przedstawiające cykliczne raporty na temat aktualnych zagrożeń i opis sposobu ich zwalczania.

VIII. Warunki równoważności - specyfikacja techniczno-eksploatacyjna i cech użytkowych Pakietów.

W przypadku zaoferowania przez Wykonawcę Pakietów równoważnych lub oferowania ich w równoważnych do opisanych w OPZ umowach licencyjnych, Wykonawca poniesie całkowity koszt prac związanych z migracją systemów (m.in. system One), i procesów organizacyjnych obecnie działających u Zamawiającego, w tym niezbędne aktualizacje dokumentacji i szkolenia.

Ww. prace muszą zostać wykonane w okresie do 15-stu dni roboczych od dnia aktywacji Pakietów. O planowanym terminie aktywacji Pakietów Zamawiający poinformuje Wykonawcę nie później niż … dni roboczych przed planowanym terminem aktywowania pierwszego Pakietu.

W ramach Pakietów Zamawiający jest uprawniony do zamawiania dowolnej aplikacji/usługi oferowanej przez Dostawcę -zakres minimalny określono w rozdziale VI. Aplikacje/usługi będą uruchamiane i używane wg bieżących potrzeb Zamawiającego zaś rozliczenie za ich zużycie nastąpi wg zasad i ogólnodostępnych cenników Dostawcy usług chmurowych.

Procedura weryfikacji równoważności Pakietów/Wsparcia/Umowy Licencyjnej:

W przypadku zaoferowania Pakietów równoważnych do oceny przez Zamawiającego, Wykonawca musi wykazać (poza spełnieniem warunków, o których mowa w Tabeli 2) równoważność parametrów kosztowych zaoferowanych Pakietów poprzez następującą procedurę:

Wykonawca, celem wykazania równoważności Pakietów, posługuje się cenami ogólnodostępnego cennika Dostawcy usług chmurowych obowiązującego w dniu publikacji dokumentów zamówienia na Platformie ezamówienia.

Na potrzeby oceny równoważności rozwiązania Wykonawca zobowiązany jest wykazać, że warunki równoważności zostaną spełnione dla całkowitego kosztu uruchomienia usługi ciągle przez okres 730 godzin. Po tym okresie usługa będzie wyłączona i nie będzie włączana ponownie.

Zamawiający uzna, że zaoferowany Pakiet spełnia warunek równoważności w zakresie parametrów kosztowych do Pakietu opisanego w OPZ, jeżeli Wykonawca zaproponuje zestaw usług jednej i tej samej oferowanej chmury obliczeniowej spełniający minimalne parametry wskazane przez Zamawiającego oraz wyceni koszt ich funkcjonowania w standardowym okresie 730 godzin w walucie EUR. Zamawiający uzna, że zaoferowany Pakiet spełnia warunek równoważności w stosunku do Pakietu opisanego w OPZ, jeżeli zaoferowany Pakiet gwarantuje wykorzystanie usług w zakresie wskazanym w tabeli 3.

Tabela 1 – Warunki równoważności

	Opis usługi – parametry minimalne	Opis usługi – parametry zaproponowane przez Wykonawcę w oparciu o usługi oferowanej chmury	Liczba jednostek
	Oferowana chmura obliczeniowa dla usług z punktów a, b, c: *(przykładowo: AWS / GPC / Inna – podać jaka)* ……..……..……..……..…… Model zakupu aplikacji/usług oferowanej chmury obliczeniowej dla usług z punktów a, b, c: *(przykładowo: AWS EDP / GPC CUD / Inna – podać jaka)* ……..……..……..……		
a)	1 maszyna wirtualna o parametrach - 1 rdzeń procesora, 3,5 GB RAM, 7 GB dysku tymczasowego. System operacyjny z rodziny Linux (Open Source).	1 maszyna wirtualna (typ instancji) …… o parametrach: …… rdzeni procesora …… GB RAM …… GB dysku tymczasowego System operacyjny ……	730 godzin
b)	7 GB dostępnej lokalnie redundantnej przestrzeni dyskowej na dyskach SSD, 500 IOPS, 100 MB/sec.	…… GB dostępnej lokalnie redundantnej przestrzeni dyskowej Wydajność dysków SSD …… IOPS Transfer dysków SSD …… MB/s	730 godzin

c)	650 GB transferu danych do, i 650 GB transferu danych z aplikacji/usługi miesięcznie.	…… GB transferu danych do aplikacji/usługi miesięcznie …… GB transferu danych z aplikacji/usługi miesięcznie	1 miesiąc

Tabela 2 – minimalne wymagania w zakresie wsparcia		
L.p.	**Usługa**	**Opis**
1.	Premier Support	
2.	Unified Support	