

## 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	3
II. Definicje	4
III. Zamówienie podstawowe i opcje	6
IV. Pakiet – uruchomienie i minimalne wymagania	10
V. Chmura Publiczna - minimalne wymagania:	11
VI. Usługi, w ramach pakietów - minimalne wymagania	13
VII. Usługi doradztwa/wsparcia Wykonawcy - minimalne wymagania	22
VIII. Bezpieczeństwo	23
IX. Warunki równoważności dot. pakietu, umowy licencyjnej, usług wsparcia, normy	24
X. Wizja lokalna	28

## **I. Przedmiot i termin realizacji zamówienia**

- 1) Wyrażenia pisane wielką 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 dnia podpisania umowy z Dostawcą, z zastrzeżeniem, że umowa z Wykonawcą zostanie zawarta na okres **38 miesięcy** od daty jej podpisania.
- 3) Zamawiający zastrzega, że podpisanie Umowy Server and Cloud Enrollment (SCE) lub równoważnej nastąpi nie później niż 2 miesiące od podpisania Umowy z Wykonawcą.
- 4) Szczegółowe informacje dotyczące zakresu zamówienia podstawowego i opcji zostały opisane w rozdziale III-VI OPZ.
- 5) Zamawiający dopuszcza dostawę pakietu równoważnego do Pakietu nabywanego w ramach umowy Server and Cloud Enrollment (SCE) lub równoważnej. Warunki uznania Pakietu/umowy za równoważny(ą) określają kryteria oceny równoważności, określone w rozdziale IX OPZ.
- 6) Opis przedmiotu zamówienia jest określony we Wspólnym Słowniku Zamówień jako:  
48900000-7 Różne pakiety oprogramowania i systemy komputerowe.

## 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 bezpośrednio dostarcza zasoby chmurowe Zamawiającemu, faktycznie odpowiedzialny za dostępność (SLA) usług wskazanych w tabeli w rozdziale VI opisu przedmiotu zamówienia

**Dysk tymczasowy** – zasób dyskowy, który zapewnia krótkotrwale przechowywanie aplikacji i procesów i jest przeznaczony wyłącznie do przechowywania danych, takich jak pliki stronicowania lub pliki wymiany. Dane na dysku tymczasowym mogą zostać utracone podczas konserwacji, ponownego wdrożenia maszyny wirtualnej lub zatrzymania maszyny wirtualnej.

**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 III-VII OPZ.

**PAYG** (ang Pay As You Go) – model rozliczeń kosztów za faktyczne użytkowanie, płatność za rzeczywiste wykorzystanie usługi po jej wykorzystaniu.

**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) – poziom i warunki świadczonych usług, określające 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.

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

### III. Zamówienie podstawowe i opcje

- 1) W ramach realizacji przedmiotu zamówienia Zamawiający jest uprawniony do zakupu:
  - a. Liczby Pakietów (Tabela 1).
  - b. Usług chmurowych, rozliczanych miesięcznie z dołu w systemie PAYG (Tabela 2).
  - c. Usług doradztwa/wsparcia (Tabela 3).

Tabela 1 – Zamówienie podstawowe i Opcja I - Liczba pakietów

Lp.	Nazwa Pakietu	Minimalna Liczba Pakietów	Maksymalna Liczba Pakietów	Maksymalna Liczba Pakietów	Maksymalna Liczba Pakietów - Zamówienie podstawowe + Opcja I
		Zamówienie podstawowe		Opcja I	
1	Pakiet (Azure prepayment 6QK-00001 lub równoważny)	360 szt.	1000 szt.	10400 szt.	11400 szt.

Tabela 2 – Zamówienie podstawowe i Opcja II - Usługi chmurowe – PAYG

Lp	Nazwa	Minimalna kwota na wykorzystanie usług chmurowych	Maksymalna kwota na wykorzystanie usług chmurowych	Maksymalna kwota na wykorzystanie usług chmurowych	Maksymalna kwota na wykorzystanie usług chmurowych - Zamówienie podstawowe + Opcja II
		Zamówienie podstawowe		Opcja II	
1	Usługi chmurowe (Azure lub równoważny)	0,00 zł brutto	50 000,00 zł brutto	50 000,00 zł brutto	100 000,00 zł brutto

Tabela 3 – Zamówienie podstawowe i Opcja III - Usługi doradztwa/wsparcia

Lp	Nazwa	Minimalna liczba roboczogodzin usług doradztwa / wsparcia	Maksymalna liczba roboczogodzin usług doradztwa / wsparcia	Maksymalna liczba roboczogodzin usług doradztwa / wsparcia	Maksymalna liczba roboczogodzin usług doradztwa / wsparcia - Zamówienie podstawowe + Opcja III
		Zamówienie podstawowe		Opcja III	
1	Usługi doradztwa/wsparcia	10	50	250	300

- 2) Pierwsze 360 szt. Pakietów zostanie jednorazowo zamówione przez Zamawiającego bezpośrednio po zawarciu umowy z Dostawcą.
- 3) W okresie trwania umowy Zamawiający, w ramach zamówienia podstawowego jest uprawniony zakupić maksymalnie 1000 szt. Pakietów, z zastrzeżeniem, że minimalna liczba Pakietów, którą Zamawiający zobowiązuje się nabyć w okresie trwania umowy to 360 szt. Oznacza to, że w przypadku gdy Zamawiający zakupi w trakcie trwania umowy 360 szt. Pakietów i więcej, Wykonawcy nie przysługuje żadne roszczenie w zakresie dot. zakupu pozostałych sztuk Pakietów przewidzianych do nabycia w ramach zamówienia podstawowego, w tym za utracone korzyści.
- 4) W okresie trwania umowy Zamawiający, w ramach zamówienia podstawowego jest uprawniony zakupić usługi chmurowe w systemie PAYG rozliczane wg cen Dostawcy do maksymalnej kwoty 50 000,00 zł brutto.,

przy czym minimalna kwota zamówienia w tym zakresie wynosi 0,00 zł a Wykonawcy nie przysługuje roszczenie zamówienia tych usług przez Zamawiającego. Zamawiający jest uprawniony do nabywania usług wg własnych potrzeb. Rozliczenie z Wykonawcą za wykorzystane usługi nastąpi w okresach miesięcznych z dołu. Uruchomienie usług w ramach zamówienia podstawowego może być wielokrotne aż do wykorzystania 50 000,00 zł brutto. Usługi chmurowe są rozliczane w systemie PAYG wyłącznie wtedy, kiedy nie jest możliwe ich rozliczenie w oparciu o zamówione przez Zamawiającego Pakiety.

- 5) W okresie trwania umowy Zamawiający, w ramach zamówienia podstawowego jest uprawniony zakupić maksymalnie 50 roboczogodzin usług doradztwa/wsparcia, z zastrzeżeniem, że minimalna liczba roboczogodzin, którą Zamawiający zobowiązuje się nabyć w okresie trwania umowy to 10. Oznacza to, że w przypadku gdy Zamawiający zakupi w trakcie trwania umowy 10 roboczogodzin i więcej, Wykonawcy nie przysługuje żadne roszczenie w zakresie zakupu pozostałych roboczogodzin przewidzianych do nabycia w ramach zamówienia podstawowego, w tym za utracone korzyści.
- 6) Strony określają Harmonogram Zobowiązań w Zakresie Pakietów, jako zakres pozostających w dyspozycji Zamawiającego Pakietów w poszczególnych miesiącach świadczenia odsprzedaży usług przez Wykonawcę. Na moment uruchomienia procesu odsprzedaży usług przyjmuje się następujący Harmonogram Zobowiązań w Zakresie Pakietów:

Tabela 4 – Harmonogram Zobowiązań w Zakresie Pakietów

Miesiąc realizacji umowy z Dostawcą	Liczba nowych pakietów do dyspozycji Zamawiającego
1	360 szt.
2-36	zgodnie z zapotrzebowaniem Zamawiającego minimum 0 szt.

- 7) Określa się następujące zasady kształtowania Harmonogramu Zobowiązań w Zakresie Pakietów:
- a) Zamawiający ma prawo do aktualizacji Harmonogramu Zobowiązań w Zakresie Pakietów nie później niż na 7 dni przed rozpoczęciem miesiąca, którego dotyczy aktualizacja.
- b) W przypadku, gdy skumulowana liczba Pakietów zrealizowanych w ramach umowy oraz koniecznych do udostępnienia Zamawiającemu w kolejnym miesięcznym okresie rozliczeniowym przekroczy zakres zamówienia podstawowego, Zamawiający zobowiązany jest do złożenia w terminie, o którym mowa w punkcie a), oświadczenia o skorzystaniu z Prawa Opcji w zakresie wynikającym z liczby Pakietów udostępnianych w kolejnym miesiącu. Brak takiego oświadczenia oznacza, że liczba Pakietów udostępnianych w kolejnym miesiącu wynosi 0.
- c) Zamawiający ma prawo do aktualizacji Harmonogramu Zobowiązań w Zakresie Pakietów w większym zakresie, niż jeden miesiąc oraz do objęcia oświadczeniem o skorzystaniu z Prawa Opcji dłuższego okresu czasu.



- d) W przypadku braku informacji ze strony Zamawiającego w terminie, o którym mowa w punkcie a), przyjmuje się, że Harmonogram Zobowiązań w Zakresie Pakietów nie uległ zmianie.
- e) Wykonawca zobowiązany jest do dostosowania zamówień kierowanych do Dostawcy chmury w sposób odzwierciedlający Harmonogram Zobowiązań w Zakresie Pakietów.
- f) Wykonawca ma prawo do wydawania rekomendacji w zakresie zmian w Harmonogramie Zobowiązań w Zakresie Pakietów, jednak ostateczna decyzja należy do Zamawiającego.
- g) Zamówienia Pakietów odbywają się zgodnie z Harmonogramem Zobowiązań w Zakresie Pakietów, o którym mowa w Tabeli 4) powyżej.

Dodatkowo, Zamawiającemu przysługuje prawo do zamówienia dodatkowych Pakietów ponad Harmonogram Zobowiązań w Zakresie Pakietów w trakcie miesiąca rozliczeniowego w sytuacjach wynikających np. z przekroczeń wykorzystania usług chmurowych w stosunku do planów Zamawiającego – w takiej sytuacji Zamawiający wystąpi do Wykonawcy z wnioskiem o dostawę Pakietów. Wykonawca jest zobowiązany zrealizować potrzebę Zamawiającego w terminie nie dłuższym, niż 4 dni robocze. Zamówione dodatkowo Pakiety są rozliczane na zasadach analogicznych do wskazanych w punktach a) do g).

8) Zamawiającemu przysługuje prawo opcji:

- a) Opcja I, tj. do 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 zamówionych Pakietów w ramach opcji. Pakiety w ramach opcji mogą być zamówione 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 I. W przypadku niewykorzystania przez Zamawiającego opcji w całości lub w części Wykonawcy nie przysługuje jakiegokolwiek roszczenie za jej niewykorzystanie, w tym za utracone korzyści.
- b) Opcja II, tj. zamówienie usług chmurowych wg cen Dostawcy do maksymalnej kwoty 50 000,00 zł brutto. Zamawiający jest uprawniony do nabywania usług wg własnych potrzeb. Rozliczenie z Wykonawcą za wykorzystane usługi nastąpi w okresach miesięcznych z dołu. Uruchomienie usług w ramach Opcji II może być wielokrotne aż do wykorzystania 50 000,00 zł brutto. W przypadku niewykorzystania przez Zamawiającego opcji w całości lub w części Wykonawcy nie przysługuje jakiegokolwiek roszczenie za jej niewykorzystanie, w tym za utracone korzyści.
- c) Opcja III, tj. zamówienie usług doradztwa/wsparcia. W ramach prawa opcji Zamawiający jest uprawniony do nabycia 250 roboczogodzin konsultacji/wsparcia. Zamawiający poinformuje Wykonawcę o zamiarze skorzystania z opcji określając zakres potrzeby Zamawiającego. Proces ustalenia liczby roboczogodzin uruchamianych w ramach prawa opcji jest ustalany w sposób tożsamy jak dla zamówienia podstawowego, z zastrzeżeniem, że uruchomienie opcji następuje po

zaakceptowaniu przez Zamawiającego liczby roboczogodzin, na podstawie oświadczenia Zamawiającego o uruchomieniu prawa opcji. Zamawiający jest uprawniony wielokrotnie korzystać z prawa opcji do momentu wyczerpania limitu 250 roboczogodzin. W przypadku niewykorzystania przez Zamawiającego opcji w całości lub w części Wykonawcy nie przysługuje jakiegokolwiek roszczenie za jej niewykorzystanie, w tym za utracone korzyści.

#### IV. Pakiet – uruchomienie i minimalne wymagania

Zaoferowane przez Wykonawcę Pakiety muszą spełniać następujące wymagania:

Tabela 5 – uruchomienie i minimalne wymagania dla Pakietów		
Lp.	Wymaganie	Opis
1	Rodzaj produktu	Oferowane przez Wykonawcę Pakiety/Usługi chmurowe mają być produktami standardowymi Dostawcy – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
2	Warunki dostawy	Zamawiający wymaga dostawy i realizacji Pakietów/Usług chmurowych na warunkach przewidzianych w umowie licencyjnej z Dostawcą.
3	Informacje o produktach	Wykonawca przed podpisaniem umowy udostępni Zamawiającemu link do stron/y internetowych/ej Dostawcy zawierającej/yh opis oferowanych Pakietów/Usług chmurowych oraz zasad ich używania wraz ze zobowiązaniami Dostawcy w zakresie ochrony danych.
4	Podpisanie umowy licencyjnej	Wykonawca, po zawarciu Umowy, a przed rozpoczęciem korzystania z Pakietów/Usług chmurowych, udostępni mechanizmy podpisania przez Zamawiającego umowy licencyjnej z Dostawcą.
5	Udzielanie uprawnień	Wykonawca, w terminie do 10 dni roboczych od podpisania Umowy, udzieli uprawnień Zamawiającemu – osobom upoważnionym przez Zamawiającego do wykorzystania Pakietów/Usług chmurowych na stronie Dostawcy.
6	Wymagania bezpieczeństwa	Usługi osadzone na chmurze obliczeniowej będą świadczone zgodnie z normami ISO 27017:2015 i ISO 27018:2019 (lub nowszymi) lub równoważnymi w rozumieniu zapisów rozdziału IX pkt. 5 OPZ.
7	Wartość Pakietu	Pakiet wyraża swoją wartość w walucie EUR, wskazaną przez Wykonawcę w treści oferty, celem rozliczenia zużycia przez Zamawiającego usług oferowanych przez Dostawcę. Wartość Pakietu nie ulega zmianie w okresie trwania Umowy. Usługi rozliczane są zgodnie z cennikiem Dostawcy.
8	Zakres usług	W ramach Pakietów Zamawiający może zamawiać dowolne aplikacje/usługi oferowane przez Dostawcę, w tym usługi w zakresie określonym w rozdziale VI OPZ. Rozliczenie wykorzystane usług nastąpi na podstawie ogólnodostępnego cennika Dostawcy usług chmurowych obowiązującego w dniu zawarcia umowy z Dostawcą – cennik nie ulegnie zmianie przez 36 miesięcy od dnia podpisania ww. umowy. W przypadku nabycia usług w ramach Pakietów, które nie istniały w dniu zawarcia umowy z Dostawcą, rozliczenie ich nastąpi na podstawie ogólnodostępnego cennika Dostawcy obowiązującego w dniu uruchomienia usług.
9	Minimalny zakres Pakietu	Wartość jednego Pakietu musi zapewniać, w oparciu o standardowy cennik Dostawcy, łączne uruchomienie i nieprzerwane korzystanie w ciągu jednego miesiąca (730 godzin), łącznie z usług o parametrach opisanych poniżej lub wyższych: <ul style="list-style-type: none"> <li>• 1 maszyna wirtualna o parametrach - 1 rdzeń procesora, 3,5 GB RAM, 7 GB dysku tymczasowego. System operacyjny z rodziny Linux (Open Source) oraz</li> </ul>

	<ul style="list-style-type: none"> <li>• 7 GB dostępnej lokalnie redundantnej przestrzeni dyskowej na dyskach SSD, 500 IOPS, 100 MB/sec. oraz</li> <li>• 650 GB transferu danych do, i 650 GB transferu danych z usługi miesięcznie.</li> </ul>
--	---

## V. Chmura Publiczna - minimalne wymagania:

Wykonawca jest zobowiązany zapewnić dostęp do usług chmury publicznej, która posiada/umożliwia:

Tabela 6 – Minimalne wymagania w zakresie Chmury Publicznej

Lp.	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	Komunikację z mechanizmami zarządzania usługi poprzez REST API.
4	<p>Mechanizmy integracji danych zawierające:</p> <ul style="list-style-type: none"> <li>• Mechanizmy zarządzania integracji danych wraz z konektorami do źródeł danych <ul style="list-style-type: none"> <li>○ Dane strukturalne i niestructuralne.</li> <li>○ Data Lake.</li> <li>○ Relacyjne bazy danych.</li> <li>○ Strumienie danych.</li> </ul> </li> <li>• Zarządzanie API w postaci hybrydowej, wielochmurowej platformy zarządzania interfejsami API w wybranych środowiskach <ul style="list-style-type: none"> <li>○ 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.</li> <li>○ 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.</li> <li>○ Zarządzany broker komunikatów z kolejkami komunikatów oraz tematami publikowania i subskrybowania (w przestrzeni nazw), umożliwiający oddzielanie aplikacji i usług od siebie i zapewniający: <ul style="list-style-type: none"> <li>▪ Równoważenie obciążenia między zadaniami.</li> <li>▪ Bezpieczne kierowanie i przesyłanie danych oraz kontrolę między granicami usług i aplikacji.</li> <li>▪ Koordynowanie prac transakcyjnych, które wymagają wysokiego stopnia niezawodności.</li> </ul> </li> </ul> </li> </ul>
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: <ul style="list-style-type: none"> <li>• Skalowalność, auto-partycjonowanie, równoważenie obciążenia.</li> <li>• Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka.</li> <li>• Wsparcie dla systemów klienckich Windows i Linux.</li> <li>• Replikacja danych - minimum 3 kopie w ramach pojedynczej lokalizacji.</li> <li>• Udostępnienie zasobów pamięci poprzez REST API,</li> </ul>
14	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	Dostęp do spersonalizowanej strony Dostawcy pozwalającej upoważnionym osobom ze strony Zamawiającego na: <ul style="list-style-type: none"> <li>• Pobieranie zakupionego oprogramowania.</li> <li>• Aktywację zakupionego oprogramowania i usług.</li> <li>• Sprawdzanie liczby zakupionych usług w wykazie zakupionych usług.</li> </ul>
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 usługi.
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, 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	Gwarancję przetwarzania danych osobowych zgodnie z wymaganiami przepisów prawa, a w szczególności w zakresie ochrony danych osobowych w tym 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”).
33	Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
34	Możliwość uwierzytelnienia na bazie usługi zarządzania tożsamością będącej składową usług oferowanych przez Dostawcę.
35	Mechanizmy uwierzytelniania/autoryzacji, aby dostarczone usługi korzystały z mechanizmów zarządzania tożsamością użytkowników implementowanej u Zamawiającego usługi Entra Identity Premium Plan 2 w ramach posiadanych Tenantów i umożliwiały wsparcie techniczne Dostawcy dla tych mechanizmów, a w szczególności wymaganych funkcjonalności: <ul style="list-style-type: none"> <li>• Dostęp warunkowy oparty na ryzyku (ryzyko logowania, ryzyko użytkownika).</li> <li>• Filtry urządzenia i aplikacji na potrzeby dostępu warunkowego.</li> <li>• Ochrona tokena.</li> <li>• Wykrywanie luk w zabezpieczeniach i ryzykownych kont.</li> <li>• Badanie zdarzeń o podwyższonym ryzyku.</li> <li>• Serwer proxy aplikacji dla lokalnego, opartego na nagłówkach i zintegrowanego uwierzytelniania systemu Windows.</li> <li>• Współpraca w ramach bezpiecznego dostępu hybrydowego (Kerberos, NTLM, LDAP, RDP i uwierzytelnianie SSH).</li> <li>• Samoobsługowe resetowanie haseł/zmienianie/odblokowywanie.</li> <li>• Samoobsługowe wyszukiwanie i raportowanie aktywności dotyczącej logowania.</li> <li>• Samoobsługowe zarządzanie grupą (Moje grupy).</li> <li>• Samoobsługowe zarządzanie upoważnieniami (Mój dostęp).</li> <li>• Uwierzytelnianie bezhasłowe (Microsoft Authenticator, FIDO2, integracje klucza zabezpieczeń).</li> <li>• Zarządzanie okresem istnienia sesji.</li> <li>• Globalna ochrona hasłami i zarządzanie (w tym niestandardowe zabronione hasła)</li> <li>• Integracja z posiadany systemem zarządzania informacjami i zdarzeniami zabezpieczeń (SIEM) Microsoft Sentinel.</li> </ul>

## VI. Usługi, w ramach pakietów - minimalne wymagania

- 1) Zamawiający dopuszcza oferowanie usług o szerszej niż opisana w OPZ funkcjonalności. Zamawiający wymaga dostawy usług na warunkach przewidzianych przez Dostawcę.
- 2) Wszystkie usługi muszą być oferowane przez jednego Dostawcę.
- 3) Zamawiający wymaga dostępności w ramach pakietów co najmniej usług o następujących parametrach:

Tabela 7 – Minimalne wymagania w zakresie usług

L.p.	Usługa	Opis
------	--------	------

1.	<b>Zapora typu Firewall</b>	<p>1.1. Zarządzana usługa zapory sieciowej, zapewniająca filtrowanie w warstwach L3-L7 modelu ISO OSI lub równoważny 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.</p> <p>1.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Obsługa skalowalności w chmurze</li> <li>• Obsługa przepustowości do 30 Gbps</li> <li>• Obsługa reguł filtrowania w pełni kwalifikowanych nazw domen aplikacji</li> <li>• Obsługa reguł filtrowania ruchu sieciowego</li> <li>• Obsługa etykiet dla w pełni kwalifikowanych nazw domen (FQDN)</li> <li>• Obsługa etykiet dla usług</li> <li>• Wsparcie dla serwera proxy DNS</li> <li>• Obsługa nazw FQDN w regułach sieci</li> <li>• Obsługa translacji adresów sieciowych źródła (SNAT) dla ruchu wychodzącego</li> <li>• Obsługa technologii DNAT dla ruchu przychodzącego</li> <li>• Obsługa wymuszonego tunelowania</li> <li>• Obsługa kategorii witryn Web</li> <li>• Obsługa odporności na awarię pojedynczego centrum danych</li> </ul> <p>1.3 SLA, minimalna dostępność: 99,95%</p>
2.	<b>Zapora dla aplikacji internetowej</b>	<p>2.1. Zarządzana usługa służąca do równoważenia obciążenia, działająca w warstwie L7 modelu ISO OSI lub równoważny 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.</p> <p>2.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Obsługa routingu opartego na adresach URL</li> <li>• Obsługa Transport Layer Security (TLS) / SECURE Sockets Layer (SSL)</li> <li>• Obsługa protokołu WebSocket</li> <li>• Obsługa protokołu HTTP/2</li> </ul>

		<ul style="list-style-type: none"> <li>• Automatyczne skalowanie</li> <li>• Obsługa statycznych adresów VIP</li> <li>• Integracja z usługą bezpiecznego miejsca przechowywania wpisów tajnych</li> <li>• Obsługa uwierzytelniania mTLS (mutual SSL)</li> <li>• Integracja dla środowisk zarządzania klastrami Kubernetes do kontrolowania ruchu przychodzącego</li> <li>• Skalowalność zapory oparta o liczbę utrzymywanych połączeń i/lub przepustowość</li> <li>• Obsługa odporności na awarię pojedynczego centrum danych</li> <li>• Ilość połączeń trwałych: minimum 1000</li> <li>• Przepływność: minimum 100 Mb/s</li> <li>• Liczba jednostek obliczeniowych: minimum 45</li> <li>• Transfer wychodzący: minimum 100 GB</li> </ul> <p>2.3. SLA, minimalna dostępność: 99,95%</p>
<b>3.</b>	<b>Zarządzana usługa klastra Kubernetes</b>	<p>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.</p> <p>3.2 Wymagane funkcjonalności dla węzłów Klaster System Pool:</p> <ul style="list-style-type: none"> <li>• Procesor: 2vCpu, 3.5 GHz</li> <li>• Pamięć RAM minimum: 8GB</li> <li>• Dyski minimum: 75 GB przestrzeni dyskowej SSD</li> </ul> <p>Ilość węzłów minimum: 2</p> <p>3.3 SLA, dostępność minimum: 99,95%</p>
<b>4.</b>	<b>Zarządzana usługa klastra Kubernetes</b>	<p>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.</p> <p>4.2 Wymagane funkcjonalności dla węzłów Klaster User Pool:</p> <ul style="list-style-type: none"> <li>• Procesor: 4vCpu, 3.5 GHz</li> <li>• Pamięć RAM minimum: 16GB</li> <li>• Dyski minimum: 150 GB przestrzeni dyskowej SSD</li> <li>• Ilość węzłów minimum: 2</li> </ul>

		4.3 SLA, dostępność minimum: 99,95%
5.	<b>Zarządzana usługa bazy danych Microsoft SQL</b>	<p>5.1. Zarządzana usługa pojedynczej, odizolowanej bazy danych zbudowana na silniku Microsoft SQL. Usługa realizowana w ramach modelu zakupowego opartego na rzeczywistej użyciu rdzeni CPU, pamięci RAM, oraz operacji odczytu i zapisu.</p> <p>Struktura/Typ bazy danych wynika z budowy istniejącego systemu, który będzie wykorzystywał Infrastrukturę.</p> <p>5.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Liczba baz: minimum 1 szt.</li> <li>• Wydajność: minimum: 2vCpu</li> <li>• Pojemność minimum: 250GB</li> <li>• Pojemność na kopie zapasowe minimum: 500GB</li> </ul> <p>5.3. SLA, minimalna dostępność: 99,99%</p>
6.	<b>Zarządzana usługa rejestru oparta na standardzie open-source Docker Registry</b>	<p>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 powiązаныmi 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.</p> <p>Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Liczba repozytoriów: minimum 1 szt.</li> <li>• Pojemność minimum: 100 GB</li> </ul> <p>6.2 SLA, minimalna dostępność: 99,9%</p>
7.	<b>Usługa zarządzania wpisami tajnymi</b>	<p>7.1 Zarządzana usługa do zarządzania kluczami, sekretami oraz certyfikatami.</p> <p>7.2 Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Centralne miejsce przechowywania haseł i kluczy aplikacji umożliwiające kontrolę ich dystrybucji</li> <li>• Bezpieczne przechowywanie haseł i kluczy, za pośrednictwem odpowiednich mechanizmów uwierzytelniania oraz autoryzacji chroniące przed dostępem do nich użytkownika lub aplikacji.</li> <li>• Monitorowanie dostępu do haseł i kluczy, zintegrowane z pozostałymi elementami środowiska.</li> <li>• Administrację całym cyklem życia hasła lub klucza.</li> <li>• Obsługa min. kluczy RSA 2048-bit, RSA 3072-bit, RSA 4096-bit, Elliptic-Curve Cryptography (ECC)</li> <li>• Liczba operacji dla kluczy RSA 2048-bit: minimum 100 000</li> </ul>



		<ul style="list-style-type: none"> <li>Liczba operacji dla pozostałych kluczy: minimum 10 000</li> </ul> <p>7.3 SLA, dostępność: minimum 99,9%</p>
8.	<b>Zarządzana usługa brokera komunikatów</b>	<p>8.1 Zarządzana usługa brokera komunikatów, obsługująca kolejki komunikatów oraz zarządzanie tematami w schemacie publish-subscribe.</p> <p>8.2 Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>Obsługa rozdzielania aplikacji i usług od siebie, w celu równoważenia obciążenia pomiędzy konkurującymi usługami typu worker</li> <li>Obsługa bezpiecznego kierowania i przesyłania danych oraz kontroli na granicy usług oraz aplikacji</li> <li>Obsługa koordynacji pracy transakcyjnej</li> <li>Obsługa integracji z wirtualną siecią</li> <li>Liczba obsługiwanych komunikatów: minimum 500 000</li> </ul> <p>8.3 SLA, dostępność: minimum 99,9%</p>
9.	<b>Zarządzana usługa służąca do przechowywania danych obiektowych</b>	<p>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.</p> <p>9.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>Obsługa dostępu dla użytkowników lub usług za pośrednictwem HTTP/HTTPS</li> <li>Dane obiektowe w usłudze muszą być dostępne za pośrednictwem REST API, wiersza poleceń lub bibliotek programistycznych</li> <li>Obsługa bezpiecznego dostępu za pośrednictwem SSH File Transfer Protocol (SFTP) i monitorować za pomocą protokołu Network File System (NFS) min. 3.0</li> <li>Dane muszą być przechowywane w przynajmniej w trzech miejscach.</li> <li>Pojemność minimum: 4096 GB</li> </ul> <p>9.3. SLA, dostępność: minimum 99,9%</p>
10.	<b>Zarządzana usługa maszyny wirtualnej do celów administracyjnych</b>	<p>10.1 Usługa zarządzanej maszyny wirtualnej, dostępnej na żądanie.</p> <p>10.2 Wymagania/Typ systemu operacyjnego wynikają z budowy istniejącego systemu, który będzie wykorzystywał Infrastrukturę.</p> <p>10.3 Wymagane funkcjonalności dla każdej maszyny wirtualnej:</p> <ul style="list-style-type: none"> <li>Usługa musi zapewniać elastyczność wirtualizacji bez konieczności zakupu i utrzymywania fizycznego sprzętu, który ją obsługuje</li> <li>Specyfikacja techniczna maszyny wirtualnej musi wspierać możliwość wyboru rozmiaru, oferującego liczbę rdzeni, moc procesora, pamięci RAM oraz pojemności dysków</li> </ul>

		<ul style="list-style-type: none"> <li>• Usługa musi oferować model zakupowy oparty na rzeczywistej, godzinowej użyciu, z dokładnością do każdej minuty działania</li> <li>• Wymagany system operacyjny: Linux (Open Source)</li> <li>• Procesor: minimum 1 vCpu</li> <li>• Pamięć RAM: minimum 3.5 GB</li> <li>• Dysk tymczasowy: minimum 7 GB</li> <li>• Dysk: minimum 7 GB redundantnej lokalnie przestrzeni dyskowej, SSD (500 IOPS, 100 MB/sec.)</li> <li>• Transfer: 650 GB transferu danych do, i 650 GB transferu danych z usługi miesięcznie</li> </ul> <p>10.4 SLA, dostępność: minimum 99,9%</p>
11.	Zarządzana usługa maszyny wirtualnej dla usług raportowania	<p>11.1 Usługa zarządzanej maszyny wirtualnej, dostępnej na żądanie.</p> <p>11.2 Wymagania/Typ bazy danych i systemu operacyjnego wynikają z budowy istniejącego systemu, który będzie wykorzystywał Infrastrukturę.</p> <p>11.3 Zamawiający wymaga minimum 2 maszyn wirtualnych, dla każdej wymagane funkcjonalności to:</p> <ul style="list-style-type: none"> <li>• Usługa musi zapewniać elastyczność wirtualizacji bez konieczności zakupu i utrzymywania fizycznego sprzętu, który ją obsługuje</li> <li>• Specyfikacja techniczna maszyny wirtualnej musi wspierać możliwość wyboru rozmiaru, oferującego liczbę rdzeni, moc procesora, pamięci RAM oraz pojemności dysków</li> <li>• Usługa musi oferować model zakupowy oparty na rzeczywistej, godzinowej użyciu, z dokładnością do każdej minuty działania</li> <li>• System raportowania wymaga oprogramowania bazodanowego Microsoft SQL Server Standard oraz systemu operacyjnego Microsoft Windows Server</li> <li>• Wymagany system operacyjny: Windows</li> <li>• Procesor: minimum 4vCpu</li> <li>• Pamięć RAM: minimum 16GB</li> <li>• Dyski: minimum 512 GB przestrzeni dyskowej SSD na dane</li> </ul> <p>11.4 SLA, dostępność: minimum 99,9%</p>
12.	Zarządzana usługa publicznego adresu IP	<p>12.1. Usługa zarządzanego publicznego adresu IP, umożliwiającego komunikację przychodzącą zasobom internetowym.</p> <p>12.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• Adres IP musi być dedykowany dla danego zasobu z możliwością rezerwacji stałej</li> <li>• Usługa musi wspierać adresację według standardu IPv4</li> <li>• Obsługa odporności na awarię pojedynczego centrum danych</li> <li>• Liczba adresów: minimum 9</li> </ul> <p>12.3 SLA, dostępność: minimum 99,95%</p>

13.	<b>Zarządzana usługa wirtualnej sieci</b>	<p>13.1. Usługa sieci wirtualnej umożliwiająca bezpieczną komunikację usług chmurowych pomiędzy sobą, z Internetem oraz sieciami lokalnymi.</p> <p>13.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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.</li> <li>• Ilość danych (transfer pomiędzy sieciami): minimum 20480 GB</li> </ul>
14.	<b>Zarządzana usługa wirtualnej bramy sieciowej</b>	<p>14.1. Usługa zarządzanej wirtualnej bramy sieciowej służąca do wysyłania zaszyfrowanego ruchu pomiędzy siecią wirtualną a lokalizacjami lokalnymi przez publiczny Internet.</p> <p>14.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>• 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)</li> <li>• Usługa musi posiadać możliwość skalowania na żądanie</li> <li>• Ilość jednoczesnych połączeń (tunele S2S): minimum 16</li> <li>• Ilość danych (transfer pomiędzy sieciami): minimum 10240 GB</li> </ul> <p>14.3. SLA, dostępność: minimum 99,95%</p>
15.	<b>Zestaw narzędzi i procesów wspierających współpracę</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Narzędzia Agile wspierające planowanie i śledzenie pracy, defektów kodu i problemów przy użyciu metod min. Kanban i Scrum.</li> <li>• Usługi budowania i wdrażania, wspierające ciągłą integrację i dostarczanie aplikacji.</li> <li>• Narzędzia służące do testowania aplikacji, w tym testowanie ręczne/eksploracyjne i testowanie ciągłe.</li> <li>• Usługi umożliwiające udostępnianie pakietów, w szczególności takich jak Maven, npm, NuGet z publicznych i prywatnych źródeł oraz integrowanie udostępniania pakietów w tzw. pipeline'ach.</li> </ul>
16.	<b>Zarządzana usługa</b>	<p>16.1. Zarządzana usługa do monitorowania służąca do zbierania, analizowania i reagowania na dane telemetryczne z usług chmurowych.</p>

	<p><b>monitorowania środowiska oraz pozyskiwania i przechowywania danych dziennika (logów)</b></p>	<p>16.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>● 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</li> <li>● Ilość zbieranych dzienników (logów) minimum: 3 GB dziennie</li> <li>● Czas działania (przechowywanie danych): minimum 18 miesięcy</li> </ul>
<p>17.</p>	<p><b>Zarządzana usługa punktów końcowych usługi wirtualnej sieci</b></p>	<p>17.1. Zarządzana usługa punktu końcowego (<b>endpoint</b>) usługi wirtualnej sieci.</p> <p>17.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>● Usługa zapewnia bezpieczną i bezpośrednią łączność z innymi usługami Infrastruktury za pośrednictwem zoptymalizowanej trasy przez sieć szkieletową Dostawcy chmury obliczeniowej.</li> <li>● Punkty końcowe muszą umożliwiać zabezpieczanie krytycznych zasobów Infrastruktury tylko do sieci wirtualnych.</li> <li>● 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.</li> <li>● Ilość punktów końcowych: minimum 3</li> <li>● Ilość danych wychodzących: minimum 20480 GB dla zarządzanej usługi wirtualnej sieci</li> <li>● Ilość danych wchodzących minimum 20480 GB dla zarządzanej usługi wirtualnej sieci</li> </ul>
<p>18.</p>	<p><b>Zarządzana usługa prywatnych stref DNS</b></p>	<p>18.1. Zarządzana usługa prywatnych stref DNS.</p> <p>18.2. Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● 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.</li> <li>● 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.</li> <li>● Ilość hostowanych stref DNS: minimum 6</li> </ul>

19.	Zarządzana usługa ochrony sieci przed atakami DDoS	<ul style="list-style-type: none"> <li>● Zapytania DNS (w milionach): minimum 1</li> </ul> <p>19,1 Zarządzana usługa ochrony sieci przed atakami DDoS</p> <p>19.2 Wymagane funkcjonalności:</p> <ul style="list-style-type: none"> <li>● Monitorowanie ruchu przez 24 godziny dziennie, 7 dni w tygodniu, w celu szukania wskaźników ataków DDoS.</li> <li>● Adaptacyjne dostrajanie w czasie rzeczywistym: profilowanie ruchu inteligentnego uczenie się ruchu aplikacji w czasie i wybieranie oraz aktualizuje profil, w zależności od potrzeb odpowiednich dla chronionych usługi.</li> <li>● Analiza, metryki i alerty usługi DDoS Protection: Użycie minimum trzech automatycznie dostrojonych zasad ograniczania ryzyka (TCP SYN, TCP i UDP) dla każdego publicznego adresu IP chronionego zasobu w usłudze zarządzanej wirtualnej sieci z włączoną funkcją DDoS. Progi zasad muszą być konfigurowane automatycznie za pośrednictwem profilowania ruchu sieciowego opartego na uczeniu maszynowym. Ograniczenie ryzyka ataków DDoS muszą być stosowane dla adresu IP objętego atakiem tylko wtedy, gdy próg zasad zostanie przekroczony.</li> <li>● Analiza ataków: uzyskiwanie szczegółowych raportów w pięciu minutach przyrostowych podczas ataku oraz pełne podsumowanie po zakończeniu ataku. Przesyłanie strumieniowe dzienników przepływu ograniczania ryzyka do systemu zarządzania informacjami i zdarzeniami w trybie offline (SIEM) na potrzeby monitorowania niemal w czasie rzeczywistym podczas ataku.</li> <li>● Metryki ataku: podsumowane metryki z każdego ataku muszą być dostępne za pośrednictwem zarządzanej usługi monitorowania środowiska oraz pozyskiwania i przechowywania danych dziennika (logów).</li> <li>● Alerty ataku: alerty muszą umożliwiać konfigurację na początku i zatrzymaniu ataku oraz w czasie trwania ataku przy użyciu wbudowanych metryk ataku. Alerty muszą integrować się z oprogramowaniem operacyjnym, takimi jak dzienniki zarządzanej usługi monitorowania środowiska oraz pozyskiwania i przechowywania danych dziennika, zarządzana usługa służąca do przechowywania danych obiektowych, poczta e-mail.</li> <li>● Natywna integracja platformy: natywnie zintegrowana z platformą chmury obliczeniowej. Obejmuje konfigurację za pośrednictwem witryny Dostawcy usług chmury obliczeniowej.</li> <li>● Ochrona wszystkich zasobów w usłudze zarządzanej wirtualnej sieci natychmiast po włączeniu ochrony sieci przed atakami DDoS. Nie jest wymagana żadna interwencja, ani definicja użytkownika. Podobnie natychmiast chroni zarządzaną usługę publicznego adresu IP po włączeniu ochrony adresów IP przed atakami DDoS.</li> </ul>
-----	--	---

		<ul style="list-style-type: none"><li>Ochrona wielowarstwowa: usługa zapory dla aplikacji internetowej musi być chroniona zarówno w warstwie sieciowej (warstwa 3 i 4) jak i w warstwie aplikacji (warstwa 7 chroniona przez zaporę aplikacji internetowej).</li></ul>
--	--	--

## VII. Usługi doradztwa/wsparcia Wykonawcy - minimalne wymagania

- Wykonawca zapewni usługi doradztwa/wsparcia dla Zamawiającego w zakresie optymalizacji kosztów i działania dla wykorzystywanych w ramach Pakietów usług chmurowych przez okres trwania Umowy, a w szczególności:
  - Wsparcie dla optymalizacji wykorzystania usług chmurowych w ramach Pakietów, tym doboru odpowiednich jednostek magazynowych (ang. SKU – Stock Keeping Unit) oraz planów rezerwacji lub innych możliwości oszczędności.
  - Doradztwo licencyjne dot. możliwości wykorzystania licencji w ramach środowisk hybrydowych.
  - Doradztwo dot. optymalizacji zakupów Pakietów w ramach prawa Opcji.
  - Przekazywanie informacji o aktualizacjach funkcjonalności produktów i usług chmurowych wykorzystywanych w ramach Pakietów oraz informacji o zmianach w prawie licencyjnym do używania tych produktów i usług, a także informowanie o dostępnych akcjach promocyjnych.
  - Wsparcie merytorycznego i okresowe szkolenia w zakresie efektywnego korzystania z usług chmurowych wykorzystywanych w ramach Pakietów.
  - Przeprowadzanie audytów bezpieczeństwa uruchomionych oraz wykorzystywanych przez Zamawiającego usług chmurowych wykorzystywanych w ramach Pakietów.
  - Weryfikację zgodności korzystania z usług chmurowych wykorzystywanych w ramach Pakietów z zasadami licencjonowania Dostawy usług chmurowych.
  - Testowanie poprawności działania procedur odtwarzania kopii archiwalnych systemów i procesów obecnie działających u Zamawiającego na chmurze Microsoft Azure lub zaoferowanej równoważnej, na zasobach udostępnionych przez Zamawiającego.
  - Testowanie poprawności działania procedur odtwarzania awaryjnego (ang. Disaster Recovery) systemów i procesów obecnie działających u Zamawiającego na chmurze Microsoft Azure lub zaoferowanej równoważnej, na zasobach udostępnionych przez Zamawiającego.
  - Inne potrzeby Zamawiającego związane z doradztwem/wsparciem w zakresie zamówienia.
- W celu realizowania usług doradztwa Zamawiający nada Wykonawcy niezbędne uprawnienia oraz dostępy umożliwiające świadczenie tych usług.

- 3) W ramach usług doradztwa/wsparcia, Wykonawca zapewnia specjalistów do realizacji tych usług.
- 4) Zamawiający będzie zlecać usługi, o których mowa w pkt. 1) z wyprzedzeniem minimalnym 15 dni kalendarzowych. Zamawiający i Wykonawca mogą uzgodnić wcześniejszą realizację ww usług.
- 5) Zamawiający poinformuje Wykonawcę o zleceniu roboczogodzin doradztwa/wsparcia określając jego zakres. Udzielenie odpowiedzi na zlecenie nastąpi do 2 dni roboczych od momentu przesłania zlecenia do Wykonawcy przez Zamawiającego. W przesłanej odpowiedzi Wykonawca określi termin i liczbę roboczogodzin\* niezbędną do realizacji zlecenia, z zastrzeżeniem, że termin realizacji zlecenia nie przekroczy 10 dni roboczych od momentu akceptacji liczby roboczogodzin przez Zamawiającego. Zamawiający jest uprawniony zakwestionować wskazaną liczbę roboczogodzin przez Wykonawcę, w szczególności gdy informacje pozyskane przez Zamawiającego z rynku wskażą, że liczba roboczogodzin niezbędnych do realizacji zlecenia znacząco odbiega (co najmniej o 40%) od wskazanej liczby roboczogodzin przez Wykonawcę. Wówczas Strony przystąpią do negocjacji w celu ustalenia ostatecznej liczby roboczogodzin. Po ustaleniu przez Strony ostatecznej liczby roboczogodzin – akceptacja przez Zamawiającego, Wykonawca przystąpi do realizacji zlecenia. Realizacja zlecenia w terminie dłuższym niż ww. (5 dni) może nastąpić wyłącznie za zgodą Zamawiającego. Zlecenie zostanie zrealizowane w sposób wskazany przez Zamawiającego – w sposób zdalny lub w siedzibie Zamawiającego.

## VIII. Bezpieczeństwo

Usługi oferowane w ramach pakietów muszą:

- 1) być zgodne ze Standardowymi Klauzulami Umownymi opublikowanymi przez Komisję Europejską w zakresie ochrony danych osobowych;
- 2) gwarantować pozostanie całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego;
- 3) zapewniać automatyczną, niewpływającą na ciągłość pracy systemów Zamawiającego działających na usługach chmury obliczeniowej instalacji poprawek przez Dostawcę chmury obliczeniowej dla wybranych składników usługi;
- 4) posiadać:
  - a) dostępne mechanizmy pełnej rozliczalności działań użytkowników w usługach,
  - b) mechanizmy monitorowania zachowania użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
  - c) możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania na bazie własnej usługi katalogowej,
  - d) 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”,
  - e) mechanizm uwierzytelnienia wieloskładnikowego,

- f) możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
  - g) wbudowane mechanizmy zabezpieczające przez atakami DDoS,
  - h) raporty odnośnie dzienników z urządzeń potencjalnie zainfekowanych, z sieci Botnet,
  - i) silnik rekomendacji zabezpieczeń infrastruktury oparty o algorytmy uczenia maszynowego,
  - j) 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),
  - k) 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.
- 5) udostępnić:
- a) 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,
  - b) zapisy umowne Dostawcy zawierających tzw. Standardowe Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych;
- 6) umożliwić:
- a) zastrzeżenie miejsca uruchomienia usług i składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego (EOG),
  - b) 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.

## **IX. Warunki równoważności dot. pakietu, umowy licencyjnej, usług wsparcia, normy**

### **1. Zasady ogólne**

- a) W przypadku gdy, Wykonawca zaoferował w treści oferty pakietu, program (umowę licencyjną), usługę wsparcia lub normy równoważne do wskazanych przez Zamawiającego w OPZ, Wykonawca zobowiązany jest wykazać, że spełniają one wymagania Zamawiającego w zakresie kryteriów oceny równoważności opisanych w niniejszym rozdziale;
  - b) Zamawiający dokona oceny i badania rozwiązań równoważnych określonych w pkt. a);
  - c) W przypadku gdy oferowane przez Wykonawcę rozwiązanie równoważne nie spełni wymagań Zamawiającego, Zamawiający odrzuci ofertę Wykonawcy na podstawie art. 226 ust. 1 pkt 5 ustawy PZP – z powodu jej niezgodności z warunkami zamówienia.
2. W przypadku zaoferowania rozwiązania równoważnego, które spowoduje konieczność migracji systemów i procesów obecnie działających u Zamawiającego na chmurze Microsoft Azure, Wykonawca jest zobowiązany w ramach wynagrodzenia za realizację przedmiotu zamówienia dokonać ww. migracji.



Wykonawca, podczas procesu migracji, musi zapewnić ciągłość działania systemów Zamawiającego. Zamawiający udostępni dokumentację infrastruktury na platformie Microsoft Azure oraz systemów działających na infrastrukturze i współdziałających z infrastrukturą podczas wizji lokalnej, o której mowa w rozdziale X.

Ewentualne świadczenia w zakresie migracji systemów i procesów muszą zostać wykonane w okresie do 15-stu dni roboczych od dnia podpisania umowy z Dostawcą.

Po dokonaniu migracji Wykonawca jest zobowiązany zaktualizować dokumentację systemów IT, które zostały zmigrowane na oferowaną przez Wykonawcę chmurę, uwzględniając jej specyfikę, a także przeszkolić maksymalnie 24 osoby wskazane przez Zamawiającego, w zakresie wszystkich funkcjonalności oferowanego przez Wykonawcę rozwiązania. Szkolenie odbędzie się w siedzibie Zamawiającego w ustalonym przez Strony terminie, z zastrzeżeniem, że szkolenie będzie trwało nie krócej niż 5 dni szkoleniowych (40 godzin). Za zgodą Zamawiającego szkolenie może odbyć się w formie zdalnej. Liczba uczestników pojedynczych szkoleń: maksymalnie 8 osób. Wykonawca jest zobowiązany przygotować i dostarczyć uczestnikom szkolenia materiały szkoleniowe w języku polskim, w formie pisemnej lub elektronicznej.

Ww. świadczenia muszą zostać wykonane w okresie do 30-stu dni roboczych od dnia podpisania umowy z Dostawcą.

### **3. Równoważność do umowy licencyjnej Server and Cloud Enrollment (SCE)**

W przypadku zaoferowania umowy równoważnej Wykonawca musi wykazać, że:

- a) Wartość Pakietu wyrażona w walucie euro wskazana w treści oferty nie ulegnie zmianie przez cały okres umowy z Wykonawcą.
- b) Ceny usług chmurowych nabywanych w ramach Pakietów lub formuły PAYG przez Zamawiającego będą stałe i świadczone wg cennika Dostawcy. Jednocześnie w przypadku, gdy w ofercie Dostawcy pojawiają się nowe usługi nieistniejące w dniu zawarcia umowy z Dostawcą zapewniona będzie możliwość skorzystania z takich usług w ramach umowy licencyjnej/posiadanych przez Zamawiającego Pakietów/formuły PAYG (wybór należy do Zamawiającego), zaś rozliczenie za nie nastąpi wg cennika Dostawcy z dnia uruchomienia tych usług.
- c) Wykonawca musi posiadać autoryzację Dostawcy do bezpośredniej odsprzedaży Pakietów w ramach umowy Zamawiającego z Dostawcą.
- d) Pakiety będą dostarczane na warunkach przewidzianych przez Dostawcę lub jego spółki zależne (Dostawcy).

e) Po zawarciu Umowy, a przed rozpoczęciem korzystania z Pakietów, zostaną udostępnione przez Wykonawcę mechanizmy podpisania umowy licencyjnej z Dostawcą.

**4. Równoważność do Pakietu Azure prepayment 6QK-00001**

W przypadku zaferowania pakietów równoważnych Wykonawca musi wykazać, że:

- a) w ramach oferowanych pakietów w ramach programu (umowy) licencyjnego rozwiązanie równoważne musi pozwalać Zamawiającemu zamawiać, w okresie obowiązywania umowy z Dostawcą (min. 36 miesięcy), dowolne aplikacje/usługi chmurowe oferowane przez Dostawcę, które będą nabywane zgodnie z cennikiem Dostawcy usług chmurowych obowiązującym w dniu podpisania umowy z Dostawcą. Ceny zaferowanych usług Dostawcy są stałe przez cały okres trwania ww. umowy (nie ulegną zmianie przez okres 36 miesięcy od dnia podpisania umowy z Dostawcą);
- b) w ramach oferowanych przez Wykonawcę pakietów równoważnych możliwe jest uruchomienie odrębnie usług opisanych w rozdziale VI ust. 5 OPZ - co najmniej w rodzaju i o minimalnych parametrach technicznych dla danej usługi;
- c) pakiet równoważny spełnia wszystkie wymagania dotyczące pakietów określone w rozdziale IV OPZ
- d) pakiet równoważny jest równoważny do Pakietu w zakresie łącznego uruchomienia i nieprzerwanego korzystania w ciągu jednego miesiąca (730 godzin) z usług o parametrach opisanych poniżej lub wyższych:
  - i. 1 maszyna wirtualna o parametrach - 1 rdzeń procesora, 3,5 GB RAM, 7 GB dysku tymczasowego. System operacyjny z rodziny Linux (Open Source),
  - ii. 7 GB dostępnej lokalnie redundantnej przestrzeni dyskowej na dyskach SSD, 500 IOPS, 100 MB/sec.,
  - iii. 650 GB transferu danych do, i 650 GB transferu danych z usługi miesięcznie.

wg metodyki opisanej w tabeli poniżej:

Tabela nr 8 – Oferowane rozwiązanie równoważne			
	Wymagane parametry minimalne usług w ramach pakietu	Parametry usług równoważnych zaferowanych przez Wykonawcę w ramach pakietu	Liczba jednostek
	Dostawca chmury obliczeniowej: <i>(podać nazwę)</i> .....		
	Oferowana chmura obliczeniowa dla usług z punktu c: <i>(przykładowo: AWS / Inna – podać jaka)</i> .....		

	Model zakupu usług oferowanej chmury obliczeniowej dla usług z punktu c): (przykładowo: AWS EDP / 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 usługi miesięcznie.	..... GB transferu danych do usługi miesięcznie ..... GB transferu danych z usługi miesięcznie	730 godzin
Wartość pakietu równoważnego (Wartość pakietu obliczono na podstawie ogólnodostępnego cennika Dostawcy usług chmurowych w dniu ....., ale nie starszego niż 14 dni przed złożeniem oferty.) Link do cennika Dostawcy z kalkulacją:  .....  Wykonawca zobowiązany jest załączyć ww. kalkulację do oferty.			..... Euro

## 5. Normy równoważne

- a) Wskazany przez Wykonawcę Dostawca chmury obliczeniowej zrealizuje przedmiot zamówienia w zakresie usług osadzonych na chmurze obliczeniowej zgodnie z normami ISO 27017:2015, ISO 27018:2019 (lub nowszymi) lub równoważnymi. Za równoważne uważa się normy, które spełniają następujące warunki:
- i. normy dotyczą co najmniej usług osadzonych na chmurze obliczeniowej,
  - ii. normy są wydane przez niezależną jednostkę uprawnioną do certyfikowania,

- iii. 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.

## **X. Wizja lokalna**

Z uwagi na fakt, że dokumenty dotyczące infrastruktury Zamawiającego mają charakter poufny, Zamawiający udostępni je Wykonawcom podczas wizji lokalnej w siedzibie Zamawiającego zgodnie z poniższymi informacjami:

Zamawiający w toku postępowania przewiduje przeprowadzenie **wizji lokalnej**. Warunki odbycia wizji lokalnej:

- 1) udział w wizji lokalnej ma charakter fakultatywny tj. Wykonawca nie jest zobowiązany do uczestniczenia w wizji lokalnej; Zamawiający zaleca uczestnictwo w wizji lokalnej w celu prawidłowej wyceny oferowanych produktów/usług.
- 2) wnioski o uczestnictwo wizji należy składać do dnia ....2024, do godz. 11:00.
- 3) wizja lokalna odbędzie się najpóźniej 10 dni przed terminem składania ofert w siedzibie Zamawiającego,
- 4) warunkiem uczestnictwa w wizji lokalnej jest:
  - a) złożenie przez Wykonawcę wniosku o uczestnictwo w wizji lokalnej podpisanego przez osobę uprawnioną do reprezentacji Wykonawcy wraz ze wskazaniem osób, które będą uczestniczyć w wizji lokalnej,
  - b) podpisanie przez osobę uprawnioną do reprezentowania Wykonawcy oraz przez osoby wskazane w pkt a) oświadczenia o zachowaniu w poufności informacji uzyskanych w trakcie wizji lokalnej;

Zakres wizji lokalnej obejmuje:

- a) weryfikację dokumentów Wykonawców upoważniających do uczestnictwa,
- b) wgląd do dokumentacji powykonawczej infrastruktury na platformie Microsoft Azure oraz dokumentacji systemów działających na infrastrukturze,
- c) ewentualne udzielenie informacji dodatkowych,
- d) zakończenie wizji lokalnej.