Bydgoszcz, 07.12.2023 r.

ZAPYTANIE OFERTOWE

W związku z ubieganiem się o dofinansowanie projektu pn. „Zielona PESA – zwiększenie poziomu konkurencyjności i innowacyjności przedsiębiorstwa dzięki opracowaniu nowego typu hybrydowego pojazdu pasażerskiego zasilanego wodorem i energią z sieci trakcyjnej oraz wdrożenie innowacyjnej zrobotyzowanej technologii spawania laserowego i autorskich rozwiązań w obszarze cyberbezpieczeństwa" w ramach Działania 1.1 Ścieżka SMART programu Fundusze Europejskie dla Nowoczesnej Gospodarki 2021-2027 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego zwracamy się z prośbą o przedstawienie oferty na dostawę i konfigurację **systemu Firewall (2 szt.)**, zgodnie ze specyfikacją zamieszczoną poniżej.

1. Nazwa i adres Zamawiającego

Pojazdy Szynowe PESA Bydgoszcz S.A.

ul. Zygmunta Augusta 11

85-082 Bydgoszcz

NIP: 5540311775

kontakt: Maciej Koszur (tel.: +48 604 940 233, e-mail: maciej.koszur@pesa.pl)

adres strony internetowej: www.pesa.pl

2. Termin i sposób składania ofert

1) Oferta powinna zostać złożona na formularzu oferty stanowiącym Załącznik nr 1 do zapytania ofertowego oraz powinna zawierać:
   a) datę i miejsce sporządzenia,
   b) pieczęć firmy,
   c) nazwę i adres siedziby Oferenta, nr NIP Oferenta (lub równoważny nr obowiązujący w kraju, w którym podmiot jest zarejestrowany),
   d) imię i nazwisko oraz dane kontaktowe (telefon oraz adres e-mail) osoby wyznaczonej do kontaktów z Zamawiającym,
   e) adres do korespondencji (jeżeli inny niż adres siedziby),
   f) oferowaną cenę netto oraz brutto, która uwzględnia wszelkie koszty niezbędne do realizacji zamówienia (w przypadku ofert podanych w walucie innej niż PLN, wartość oferty zostanie przeliczona przy zastosowaniu średniego kursu sprzedaży ogłaszanego przez NBP, obowiązującego w dniu sporządzania protokołu wyboru oferty),
   g) okres gwarancji przedmiotu zamówienia (określony w miesiącach),
   h) termin realizacji zamówienia (określony w tygodniach),
   i) inne dodatkowe informacje (jeśli dotyczy),
   j) wyjaśnienie zakresu równoważności zaproponowanych parametrów w stosunku do opisu przedmiotu zamówienia określonego w pkt. 3 (jeśli dotyczy).
2) Każdy Oferent powinien dostarczyć również:
   a) pełnomocnictwo do podpisania oferty (jeśli nie wynika z dokumentów rejestrowych),

b) oświadczenie potwierdzające spełnienie warunków uczestnictwa w postępowaniu ofertowym stanowiące Załącznik nr 2 do zapytania ofertowego,

c) specyfikację techniczną potwierdzającą spełnienie parametrów technicznych zawartych w pkt. 3 (opcjonalnie).

3) Wymienione wyżej załączniki do oferty stanowią jej integralną część.

4) Formularz oferty oraz wszystkie załączniki do oferty powinny być opatrzone podpisem osoby upoważnionej lub umocowanej do reprezentowania Oferenta. Możliwe jest podpisanie oferty kwalifikowanym podpisem elektronicznym.

5) Ofertę wraz z kompletem załączników należy złożyć za pośrednictwem Bazy Konkurencyjności (https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/, dalej: **BK2021**) w wyznaczonym *Terminie składania ofert* w BK2021. Oferty złożone po upływie wskazanego terminu nie będą rozpatrywane.

6) Oferenci mogą przed terminem składania ofert zmienić, uzupełnić lub wycofać swoją ofertę.

7) W toku oceny ofert Zamawiający może żądać od Oferentów wyjaśnień formalnych dotyczących treści złożonych ofert.

8) W toku oceny ofert ważnych odbywającej się zgodnie z przyjętymi kryteriami oceny określonymi w pkt. 7 Zamawiający może podjąć negocjacje cenowe ze wszystkimi Oferentami na równych warunkach. Przebieg negocjacji będzie potwierdzony protokołem z negocjacji.

9) Zamawiający może przed upływem terminu składania ofert zmodyfikować treść zapytania ofertowego wyznaczając nowy termin składania ofert. Zamawiający poinformuje o zakresie wprowadzonych zmian w treści zapytania ofertowego w BK2021. Wszelkie modyfikacje, uzupełnienia i ustalenia oraz zmiany, w tym zmiany terminów stają się integralną częścią zapytania ofertowego i będą wiążące przy składaniu ofert. Wszelkie prawa i zobowiązania Zamawiającego oraz Dostawcy odnośnie wcześniej ustalonych terminów będą podlegały nowemu terminowi. W takim przypadku każdy z Oferentów będzie miał prawo do nowelizacji już złożonej oferty. Nie dotyczy to nieistotnych korekt w treści zapytania ofertowego.

10) W przypadku aktualizacji oferty, Dostawca powinien wyraźnie określić, która ze złożonych ofert jest ofertą ostateczną.

3. Opis przedmiotu zamówienia

1) Przedmiot zamówienia obejmuje zakup, dostawę oraz konfigurację 2 szt. systemu Firewall o następujących elementach, parametrach i funkcjonalnościach:

3.1 Wymagania ogólne:

a) System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
b) Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.
c) W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
d) Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

e) System realizujący funkcję Firewall powinien zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
f) System powinien umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
g) System wspiera protokoły IPv4 oraz IPv6 w zakresie:
   - Firewall
   - Ochrony w warstwie aplikacji
   - Protokołów routingu dynamicznego
h) Dostarczany przedmiot zamówienia pochodzi bezpośrednio od producenta lub autoryzowanych kanałów dystrybucyjnych,
i) Dokument potwierdzający, iż importer przy wprowadzeniu rozwiązania na terytorium Polski, zachował wymogi zarządzania jakością wdrażając tzw. wewnętrzny system kontroli (WSK).

3.2 Redundancja, monitoring i wykrywanie awarii:

a) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system Firewall powinien zapewnić funkcję synchronizacji sesji.
b) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
c) Monitoring stanu realizowanych połączeń VPN.
d) System powinien umożliwić agregację statyczną linków oraz w oparciu o protokół LACP, a także dać możliwość tworzenia interfejsów redundantnych.
e) Praca w postaci redundantnego klastra.

3.3 Interfejsy, dysk, zasilanie:

a) System realizujący funkcję Firewall powinien dysponować co najmniej poniższą liczbą i rodzajem interfejsów:
   - 18 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP+ 10 Gbps.
   - 4 gniazdami SFP28 10/25 GE.
b) Wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
c) Możliwość skonfigurowania co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
d) Wyposażony w zasilanie 2 x AC.

3.4 Parametry wydajnościowe:

a) W zakresie Firewall'a obsługa nie mniej niż 7.5 mln jednoczesnych połączeń oraz 500 tys. nowych połączeń na sekundę.
b) Przepustowość Stateful Firewall: nie mniej niż 135 Gbps dla pakietów 512 B.
c) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji – nie mniej niż 30 Gbps.
d) Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 50 Gbps.
e) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 14 Gbps.

f) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 10 Gbps.
g) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8.6 Gbps.

3.5 Funkcje systemu bezpieczeństwa:

System ochrony powinien posiadać wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
b) Kontrola Aplikacji.
c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
d) Ochrona przed malware.
e) Ochrona przed atakami - Intrusion Prevention System.
f) Kontrola stron WWW.
g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
h) Zarządzanie pasmem (QoS, Traffic shaping).
i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
j) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu Client-to-Site.
k) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
l) Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
m) Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

3.6 Polityki, Firewall:

a) Polityka Firewall powinna uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
b) Realizacja translacji adresów NAT:
   - Źródłowego i docelowego.
   - Translacja PAT.
   - Translacja jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.
c) Możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
d) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
e) Możliwość filtrowania ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
f) Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach Firewall jest aktywna.
g) Element systemu realizujący funkcję Firewall powinien integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:
   - Amazon Web Services (AWS).

- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

3.7 Połączenia VPN:

a) System powinien umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji powinien zapewnić:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode (GCM).
   - Obsługę protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec Site-to-Site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, Dead Peer Detection (DPD), Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
b) Możliwość konfiguracji połączeń typu SSL VPN. W zakresie tej funkcji powinien zapewnić:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

3.8 Routing i obsługa łączy WAN:

W zakresie routingu rozwiązanie powinno zapewniać obsługę:
a) Routingu statycznego.
b) Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
d) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
e) ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
f) BFD (Bidirectional Forwarding Detection).
g) Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

3.9 Funkcje SD-WAN:

a) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
b) Wsparcie dla interfejsów fizycznych i wirtualnych (w tym VLAN, IPSec).

3.10 Zarządzanie pasmem:

a) Możliwość zarządzania pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
b) Możliwość określania pasma dla poszczególnych aplikacji.
c) Możliwość zdefiniowania pasma dla wybranych użytkowników niezależnie od ich adresu IP.
d) Możliwość zarządzania pasmem dla wybranych kategorii URL.

3.11 Ochrona przed malware:

a) Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
b) Silnik antywirusowy powinien zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
c) Możliwość skanowania archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
d) Możliwość blokowania i logowania archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
e) Sygnatury do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
f) Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
g) Współpraca z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
h) Możliwość usuwania aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
i) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
j) Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

3.12 Ochrona przed atakami:

a) Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
b) System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
c) Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
d) Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
e) Zapewnienie wykrywania anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

f) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: cross-site scripting (CSS), SQL Injecton, Trojany, Exploity, Roboty).
g) Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu HTTP.
h) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
i) Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

3.13 Kontrola aplikacji:

a) Funkcja Kontroli Aplikacji umożliwiająca kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
b) Baza Kontroli Aplikacji zawierająca minimum 2000 sygnatur z automatyczną aktualizacją, zgodnie z harmonogramem definiowanym przez administratora.
c) Kontrola aplikacji chmurowych (co najmniej: Facebook, Google Docs, Dropbox) pod względem wykonywanych czynności, np. pobieranie, wysyłanie plików.
d) Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
e) Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur.
f) Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
g) Możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

3.14 Kontrola WWW:

a) Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
b) W ramach filtra WWW dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
c) Filtr WWW powinien dostarczać kategorie stron zabronionych prawem np. Hazard.
d) Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
e) Filtr WWW powinien umożliwić statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwolić definiować strony z zastosowaniem wyrażeń regularnych (Regex).
f) Możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
g) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
h) Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
i) Możliwość określenia, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

3.15 Uwierzytelnianie użytkowników w ramach sesji:

a) Możliwość weryfikacji tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

b) Możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
c) Możliwość budowy architektury uwierzytelniania typu Single Sign-On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
d) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

3.16 Zarządzanie:

a) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
b) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania realizowana z wykorzystaniem szyfrowanych protokołów.
c) Możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
d) Współpraca z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz możliwość przekazywania statystyk ruchu za pomocą protokołów Netflow lub sFlow.
e) Możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
f) Element systemu pełniący funkcję Firewall powinien posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowania procesowania sesji oraz stanu sesji Firewall.
g) Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w Command Line Interpreter (CLI) lub Graphic User Interface (GUI), które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
h) Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (Role-based monitoring – RBM).
i) Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

3.17 Logowanie:

a) Elementy systemu bezpieczeństwa powinny realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
b) W ramach logowania element systemu pełniący funkcję Firewall powinien zapewnić przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
c) Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
d) Możliwość włączenia logowania per reguła w polityce Firewall.
e) Możliwość logowania do serwera SYSLOG.
f) Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

3.18 Testy wydajnościowe oraz funkcjonalne:

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

3.19 Serwisy i licencje:

Oferta powinna obejmować co najmniej następujące licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

3.20 Gwarancja oraz wsparcie:

System powinien być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Dostawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych Dostawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".

3) Przedmiot zamówienia będzie zgodny z warunkami niniejszego zapytania ofertowego, jeśli będzie spełniał warunki przedstawione w powyższej specyfikacji technicznej w sposób zgodny lub równoważny (zakres równoważności dotyczy modelu lub poszczególnych elementów). Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki element, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w powyższej specyfikacji. Przedmiot zamówienia nie może mieć parametrów gorszych niż przedstawione w zapytaniu ofertowym. Odpowiedzialność za wyjaśnienie zakresu równoważności zaproponowanych parametrów spoczywa na składającym ofertę. W przypadku zaproponowania przez Oferenta równoważnego systemu, należy zagwarantować bezpłatne szkolenie przez producenta zaproponowanego systemu (w tym szkolenie certyfikowane, jeżeli jest wymagane do obsługi zaproponowanego rozwiązania).

4) Kod numeryczny Wspólnego Słownika Zamówień (CPV) dla przedmiotowego zadania:

32420000-3 Urządzenia sieciowe

32424000-1 Infrastruktura sieciowa

32425000-8 Sieciowy system operacyjny

32427000-2 System sieciowy

48730000-4 Pakiety oprogramowania zabezpieczającego

48761000-0 Pakiety oprogramowania antywirusowego

4. Harmonogram realizacji zamówienia

1) Termin wykonania zamówienia: do **12 tygodni** od daty podpisania umowy.

2) Termin związania z ofertą: 60 dni od daty złożenia oferty.

5. Warunki udziału w postępowaniu

5.1 Uprawnienia do wykonywania określonej działalności lub czynności

O udzielenie zamówienia może ubiegać się wyłącznie podmiot spełniający łącznie wszystkie następujące warunki:

1) Czynne prowadzenie działalności gospodarczej (w przypadku dostawców krajowych - aktywny wpis w CEIDG lub KRS) oraz posiadanie uprawnień do wykonywania działalności polegającej na sprzedaży przedmiotu zapytania ofertowego – weryfikacja na podstawie oświadczenia stanowiącego integralną część oferty.

2) Wobec Oferenta nie otwarto likwidacji ani nie ogłoszono upadłości – weryfikacja na podstawie oświadczenia stanowiącego integralną część oferty.

3) Brak powiązań osobowych lub kapitałowych z Zamawiającym – weryfikacja na podstawie oświadczenia stanowiącego integralną część oferty.

5.2 Wiedza i doświadczenie

O udzielenie zamówienia może ubiegać się wyłącznie podmiot, który posiada wiedzę i doświadczenie umożliwiające poprawną realizację zamówienia. Ocena spełnienia warunku dokonana zostanie na zasadzie *spełnia/nie spełnia* na podstawie złożonego przez Oferenta oświadczenia (Załącznik nr 2 do zapytania ofertowego).

5.3 Potencjał techniczny

O udzielenie zamówienia może ubiegać się wyłącznie podmiot, który posiada potencjał techniczny umożliwiający poprawną realizację zamówienia, tj. będzie w stanie zapewnić serwis gwarancyjny przez producenta lub autoryzowanego partnera.

Ocena spełnienia warunku dysponowania odpowiednim potencjałem technicznym zdolnym do wykonania Zamówienia będzie dokonana na zasadzie *spełnia/nie spełnia* na podstawie złożonego przez Oferenta oświadczenia (Załącznik nr 2 do zapytania ofertowego). Zamawiający może żądać od Oferenta dodatkowych dokumentów potwierdzających spełnienie powyższego warunku.

5.4 Osoby zdolne do wykonania zamówienia

O udzielenie zamówienia może ubiegać się wyłącznie podmiot, który posiada zasoby kadrowe umożliwiające poprawną realizację zamówienia oraz jest w stanie dostarczyć przedmiot zamówienia od importera, który posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli (WSK) regulujący zasady obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, potwierdzony certyfikatem.

Ocena spełnienia warunku dokonana zostanie na zasadzie *spełnia/nie spełnia* na podstawie złożonego przez Oferenta oświadczenia (Załącznik nr 2 do zapytania ofertowego).

5.5 Sytuacja ekonomiczna i finansowa

O udzielenie zamówienia może ubiegać się wyłącznie podmiot, który znajduje się w sytuacji ekonomicznej i finansowanej zapewniającej prawidłową realizację pełnego zakresu przedmiotu zamówienia, w tym jego terminową realizację oraz nie znajduje się w stanie upadłości ani likwidacji, nie wszczęto wobec Oferenta postępowania upadłościowego czy likwidacyjnego. Ocena spełnienia warunku będzie dokonana zostanie na zasadzie *spełnia/nie spełnia* na podstawie złożonego przez Oferenta oświadczenia (Załącznik nr 2 do zapytania ofertowego).

6. Inne postanowienia zapytania ofertowego

1) W ramach postępowania Zamawiający nie dopuszcza ofert wariantowych oraz wariantowości cen.

2) W ramach postępowania Zamawiający nie dopuszcza możliwości składania ofert częściowych.

3) Zamawiający ma prawo wglądu do dokumentów potwierdzających prawdziwość danych zawartych w ofercie oraz załącznikach do oferty.

4) W przypadku niewpłynięcia żadnej oferty na przedmiot zamówienia lub wpłynięcia tylko ofert podlegających odrzuceniu, lub w sytuacji, gdy wszyscy potencjalni Dostawcy zostaną wykluczeni z postępowania, lub nie spełnią warunków udziału w postępowaniu, Zamawiający dokona wyboru dowolnego Dostawcy przedmiotu zamówienia (z wolnej ręki), który spełni wszystkie kryteria i warunki określone w niniejszym zapytaniu ofertowym.

5) Jeżeli zaoferowana cena lub koszt wydadzą się rażąco niskie w stosunku do przedmiotu zamówienia, tj. różnią się o więcej niż 30% od średniej arytmetycznej cen wszystkich ważnych ofert niepodlegających odrzuceniu, lub wzbudzą wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w zapytaniu ofertowym lub wynikającymi z odrębnych przepisów, Zamawiający żąda od Oferenta złożenia w wyznaczonym terminie wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu. Zamawiający oceni te wyjaśnienia w konsultacji z Oferentem i będzie mógł odrzucić tę ofertę wyłącznie w przypadku, gdy złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej ceny lub kosztu w tej ofercie.

6) W przypadku, gdy wybrany Dostawca odstąpi od zawarcia umowy w sprawie zamówienia, Zamawiający może zawrzeć umowę z Oferentem, który w prawidłowo przeprowadzonym postępowaniu o udzielenie zamówienia uzyskał kolejną najwyższą liczbę punktów.

7) Zamawiający jest uprawniony do odstąpienia od zastosowania zasady konkurencyjności w sytuacji, w której ze względu na wyjątkową sytuację niewynikającą z przyczyn leżących po stronie Zamawiającego, której wcześniej nie można było przewidzieć (np. klęski żywiołowe, katastrofy, awarie), wymagane jest natychmiastowe wykonanie zamówienia i nie można zachować określonego terminu składania ofert. W przypadku wystąpienia wymienionej sytuacji Zamawiający jest zobowiązany do pisemnego uzasadnienia spełnienia wskazanych przesłanek.

8) Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyn na każdym etapie postępowania, w tym na etapie zakończenia postępowania bez dokonania wyboru Dostawcy oraz do unieważnienia postępowania także po dokonaniu wyboru najkorzystniejszej oferty.

7. Kryteria oceny ofert

Zamawiający dokona oceny ważnych ofert na podstawie następujących kryteriów:

7.1 Kryteria dopuszczające:

1) Spełnienie warunków udziału w postępowaniu określonych w pkt. 5.

2) Złożenie oferty w terminie.

3) Przygotowanie oferty zgodnie z wymaganiami określonymi w pkt. 2.

4) Przedstawienie wszystkich wymaganych załączników do zapytania ofertowego.

5) Zakres oferowanego zamówienia jest zgodny z określonymi wymogami.

Niespełnienie któregokolwiek z powyższych kryteriów spowoduje odrzucenie oferty – nie będzie podlegała dalszej ocenie, przy czym istnieje możliwość uzupełnienia oferty, jeśli Zamawiający

uzna, że jej weryfikacja będzie wymagała wyjaśnienia informacji zawartych w ofercie. W takich przypadkach, odrzucenie oferty nastąpi, jeśli Oferent nie uzupełni złożonej oferty w ciągu maksymalnie 5 dni roboczych od otrzymania od Zamawiającego wezwania do uzupełnienia. W przypadku uzupełnienia oferty przez Oferenta, Zamawiający dokona ponownej oceny oferty biorąc pod uwagę dostarczone uzupełnienia. Ponowny brak spełnienia któregokolwiek z powyższych kryteriów spowoduje odrzucenie oferty bez możliwości jej ponownego uzupełnienia.

7.2 Kryteria punktowe:

1) Przy ocenie oferty będą brane pod uwagę następujące elementy:

   a) cena zamówienia netto (C) - waga: 90%,
   b) okres gwarancji (G) – waga: 10%.

2) Końcowa liczba punktów to sumaryczna ilość punktów za poszczególne kryteria. Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą końcową liczbę punktów.

3) Cena zamówienia (max 90 pkt):

   a) Wartość oferty powinna zawierać wszystkie koszty, jakie Zamawiający będzie musiał ponieść w związku z wykonaniem przedmiotu zamówienia. W cenie netto należy uwzględnić koszty dostawy, konfiguracji przedmiotu zamówienia oraz koszty zaproponowanego okresu gwarancji.

   b) Cena podlegająca ocenie będzie łączną ceną netto (bez VAT) za wykonanie zlecenia.

   c) Cena przedmiotu zamówienia może być tylko jedna - nie dopuszcza się wariantowości ofert. Wszelkie upusty, rabaty, winny być od razu ujęte w cenie, tak by podana cena za realizację przedmiotu zamówienia była ceną ostateczną, bez konieczności dokonywania przez Zamawiającego przeliczeń i innych działań w celu jej określenia.

Metodologia przyznania punktów:

Liczba punktów (C) dla badanej oferty zostanie obliczona wg następującego wzoru:

$$C = \frac{\textbf{cena oferty, na której wskazano najniższą cenę netto wśród ocenianych ofert}}{\textbf{cena wskazana na ofercie badanej}} * 90\%$$

4) Okres gwarancji (max 10 pkt):

   a) Okres gwarancji wyrażony w miesiącach, liczony jest od dnia podpisania protokołu końcowego po przeprowadzeniu konfiguracji przedmiotu zamówienia przez Dostawcę.
   b) Minimalny okres gwarancji wynosi 36 miesięcy. W przypadku gdy Dostawca wskaże w ofercie okres gwarancji krótszy niż 36 miesięcy, jego oferta zostanie odrzucona jako niespełniająca kryteriów udziału w postępowaniu.
   c) Oczekiwany maksymalny okres gwarancji wynosi 60 miesięcy. W przypadku gdy Dostawca zaoferuje okres gwarancji dłuższy niż 60 miesięcy, do obliczenia wartości punktowej Zamawiający przyjmie okres gwarancji o długości 60 miesięcy.

Metodologia przyznania punktów:

Liczba punktów (G) dla badanej oferty zostanie obliczona wg następującego wzoru:

$$G = \frac{\textbf{okres gwarancji wskazany na ofercie badanej}}{\textbf{60 miesięcy}} * 10\%$$

5) Oferta, która otrzyma największą liczbę punktów wyliczoną wg poniższego wzoru zostanie uznana za najkorzystniejszą. Wybór Zamawiającego jest ostateczny i nie podlega zaskarżeniu oraz zażaleniu.

OCENA KOŃCOWA = C + G

6) Wyniki działań matematycznych, dokonywanych przy ocenie badania ofert podlegają zaokrągleniu do drugiego miejsca po przecinku. W przypadku uzyskania w ten sposób równej punktacji dla co najmniej dwóch ofert, dokonuje się ponownych wyliczeń, zaokrąglając wyniki działań matematycznych do czwartego miejsca po przecinku.

7) Oferty spełniające wszystkie wymogi przedstawione w niniejszym zapytaniu ofertowym, zostaną uszeregowane od najmniej korzystnej do najbardziej korzystnej cenowo. Następnie ofertom zostaną przyznane punkty zgodnie z metodologią przyznawania punktów opisaną powyżej. W postępowaniu ofertowym zwycięży Oferent, który zdobędzie najwyższą liczbę punktów. W przypadku równej liczby punktów zwycięży Oferent, który zaproponował najbardziej korzystną cenę.

8. Wykluczenia

1) Wykluczeniu z postępowania podlegają Dostawcy, którzy są powiązani osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzaniem procedury wyboru Dostawcy a Dostawcą, polegające w szczególności na:

   - uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10 % udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa,
   - pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   - pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z Dostawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,
   - pozostawaniu z Dostawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

2) Wykluczeniu z postępowania podlegają Dostawcy, którzy znajdują się na liście podmiotów objętych sankcjami oraz wykluczonych w postępowania zgodnie z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

3) Wykluczeniu z postępowania podlegają Dostawcy, którzy podlegają wykluczeniu z postępowania na podstawie art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), w brzmieniu nadanym rozporządzeniem Rady (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1).

9. Maksymalne kary umowne

1) Dostawca zobowiąże się do zapłaty na rzecz Zamawiającego kary umownej w razie niedotrzymania terminu wykonania umowy Zamawiający naliczy karę umowną w wysokości 2% określonego wynagrodzenia netto za każdy dzień zwłoki w dostawie przedmiotu zapytania

w stosunku do terminu określonego w umowie lub aneksach do umowy, jednak nie więcej, niż 20% wartości całego zamówienia. Kara umowna nie zostanie naliczona w przypadku zaistnienia siły wyższej, o czym Dostawca bezzwłocznie powiadomi Zamawiającego.

2) W przypadku odstąpienia od umowy z przyczyn leżących po stronie Dostawcy Zamawiający ma prawo żądania odszkodowania w zakresie przekraczającym zastrzeżone powyżej kary umowne.

10. Warunki zmiany umowy

Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Dostawcy, w następującym zakresie:

1) Konieczność wprowadzenia zmian będzie następstwem zmian wprowadzonych w umowach pomiędzy Zamawiającym a inną niż Dostawca stroną, w tym innym dostawcą lub instytucją nadzorującą realizację projektu, w ramach którego realizowane jest zamówienie, przy czym zmiana może dotyczyć wyłącznie tych zapisów umowy, na które będą miały bezpośredni wpływ modyfikacje, a zmiany nie mogą prowadzić do zwiększenia wynagrodzenia Dostawcy.

2) Z uwagi na przedłużającą się procedurę wyboru Dostawcy w postępowaniu o udzieleniu niniejszego zamówienia lub w związku z innymi okolicznościami, których nie dało się wcześniej przewidzieć, uniemożliwiającymi prawidłową realizację dostaw objętych przedmiotem umowy, konieczna stanie się modyfikacja terminów określonych w zapytaniu bądź umowie.

3) Dopuszcza się zmianę terminu wykonania umowy w przypadkach, gdy:

   a) wystąpiły zjawiska związane z działaniem siły wyższej (klęska żywiołowa, niepokoje społeczne, działania militarne, pandemia, itp.) uniemożliwiające dostawę przedmiotu zamówienia,

   b) wystąpią okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności lub z przyczyn wystąpienia przeszkód formalnoprawnych niezależnych od stron umowy,

   c) powstały opóźnienia na wcześniejszych etapach realizacji projektu,

   d) powstały opóźnienia w wydaniu lub zmiany w decyzjach administracyjnych lub innych instytucji (decyzje władz publicznych, zmiany obowiązującego prawa, oczekiwanie na nieprzewidziane wcześniej a konieczne wyniki ekspertyz, wyroki sądowe, itp.),

   e) przedmiot umowy zostanie wykonany przed terminem umownym i pozyskania przez Zamawiającego środków na zapłatę wynagrodzenia Dostawcy we wcześniejszym terminie,

   f) wystąpi potrzeba przeprowadzenia dodatkowych dostaw, polegających na częściowej wymianie dostarczonych elementów zamówienia lub instalacji albo zwiększeniu zaplanowanej dostawy lub rozbudowie istniejących instalacji.

   Wszelkie zmiany postanowień umowy wymagają formy pisemnej pod rygorem nieważności. Wystąpienie którejkolwiek z wymienionych wyżej okoliczności w zakresie mającym wpływ na przebieg realizacji zamówienia skutkuje tym, iż termin wykonania umowy może ulec odpowiedniemu przedłużeniu/zmianie o czas niezbędny do zakończenia wykonania jej przedmiotu w sposób należyty. Wszelkie opóźnienia/zmiany muszą być udokumentowane stosownymi protokołami podpisanymi przez Dostawcę i Zamawiającego, na podstawie których strony ustalą nowe terminy.

11. Klauzula informacyjna RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej: RODO, Zamawiający informuję, że:

1) Administratorem Pani/Pana danych osobowych jest Pojazdy Szynowe PESA Bydgoszcz S.A., ul. Zygmunta Augusta 11, 85-082 Bydgoszcz, NIP: 5540311775.

2) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia oraz zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień wynikający z „Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027", określające ujednolicone warunki i procedury dotyczące kwalifikowalności wydatków dla EFS+, EFRR, FS i FST.

3) Dane osobowe będą przetwarzane przez okres prowadzenia postępowania o udzielenie przedmiotowego zamówienia oraz po jego zakończeniu zgodnie z przepisami dotyczącymi archiwizacji oraz trwałości projektu (jeżeli dotyczy).

4) Przetwarzane dane osobowe mogą być pozyskiwane od Dostawców, których dane dotyczą lub innych podmiotów, na których zasoby powołują się Dostawcy.

5) Przetwarzane dane osobowe obejmują w szczególności imię i nazwisko, adres, NIP, REGON, numer CEIDG, numer KRS oraz inne dane osobowe podane przez osobę składającą ofertę i inną korespondencję wpływającą do Zamawiającego w celu udziału w postępowaniu o udzielenie przedmiotowego zamówienia.

6) Dane osobowe mogą być przekazywane do organów publicznych i urzędów państwowych lub innych podmiotów upoważnionych na podstawie przepisów prawa lub wykonujących zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej, w szczególności do podmiotów prowadzących działalność kontrolną wobec Zamawiającego.

7) Dane osobowe są przekazywane do podmiotów przetwarzających dane w imieniu administratora danych osobowych.

8) Przysługuje Pani/Panu prawo do żądania od administratora danych osobowych:

   a) na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Pani / Pana,

   b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych,

   c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO,

   d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzania danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

9) Nie przysługuje Pani/Panu:

   a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,

   b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,

c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

12. Postanowienia końcowe

1) Wszelka komunikacja w postępowaniu o udzielenie zamówienia, w tym ogłoszenie zapytania ofertowego, składanie ofert, wymiana informacji między Zamawiającym a Oferentami, w tym zadawanie pytań dotyczących zapytania ofertowego oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą BK2021.

2) Oferenci mają prawo do zadawania pytań do treści zapytania ofertowego poprzez BK2021 nie później niż 6 dni przed terminem złożenia ofert.

3) Zamawiający będzie udzielał odpowiedzi na otrzymane pytania poprzez BK2021 w ciągu około 5 dni roboczych.

4) O wyborze najkorzystniejszej oferty Zamawiający poinformuje za pośrednictwem BK2021.

5) Złożenie oferty jest równoznaczne z wyrażeniem zgody na publikację danych Oferenta oraz oferowanych warunków realizacji zamówienia określonych w ofercie.

6) Oferenci ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty we własnym zakresie. Oferenci zobowiązują się nie rościć z tego tytułu żadnych żądań względem Zamawiającego.

13. Załączniki

1) Wzór formularza oferty.

2) Oświadczenie potwierdzające spełnienie warunków uczestnictwa w postępowaniu ofertowym.