Poland-Starogard Gdański: Portable computers
OJ S 102/2022 27/05/2022
Contract notice
Supplies

Legal Basis:
Directive 2014/24/EU

Section I: Contracting authority

I.1. Name and addresses

Official name: Gmina Miejska Starogard Gdański
National registration number: 191675652
Postal address: ul. Gdańska 6
Town: Starogard Gdański
NUTS code: PL638 Starogardzki
Postal code: 83-200
Country: Poland
Contact person: Jarosław Mikołajski
E-mail: zamowienia.publiczne@um.starogard.pl
Telephone: +48 585306057
Fax: +48 585306111
Internet address(es):
Main address: www.starogard.pl

I.3. Communication

The procurement documents are available for unrestricted and full direct access, free of charge, at: www.platformazakupowa.pl/starogard_gdanski
Additional information can be obtained from the abovementioned address
Tenders or requests to participate must be submitted electronically via: www.platformazakupowa.pl/starogard_gdanski
Tenders or requests to participate must be submitted to the abovementioned address

I.4. Type of the contracting authority

Regional or local authority

I.5. Main activity

General public services

Section II: Object

II.1. Scope of the procurement

II.1.1. Title

Zakup sprzętu komputerowego wraz z oprogramowaniem antywirusowym

II.1.2. Main CPV code

30213100 Portable computers

II.1.3. Type of contract

Supplies

II.1.4. Short description

1. Przedmiotem zamówienia jest zakup wraz z dostawą do siedziby Urzędu Miasta Starogard Gdański 257 laptopów wraz z oprogramowaniem antywirusowym. 2. Wykonawca zobowiązany jest wnieść przedmiot zamówienia do pomieszczenia wskazanego przez Zamawiającego.

II.1.5. Estimated total value

II.1.6. Information about lots

This contract is divided into lots: no

II.2. Description

II.2.3. Place of performance

NUTS code: PL638 Starogardzki
Main site or place of performance: ul. Gdańska 6, 83-200 Starogard Gdański

II.2.4. Description of the procurement

Typ:
Komputer typu notebook z ekranem o przekątnej 15-16” i rozdzielczości nie mniejszej niż 1920 x 1080 pikseli (FullHD). Podświetlenie LED, matryca wykonana w technologii IPS lub EWV /VA. Jasność matrycy nie mniejsza niż 220 nitów. Kontrast nie mniejszy niż 500:1. Matryca z fabryczną powłoką przeciwodblaskową. Pokrywa matrycy wykonana z aluminium lub innego metalu w celu dodatkowego zabezpieczenia panelu LCD.
Procesor:
Procesor klasy x86, zaprojektowany do pracy w komputerach przenośnych, osiągający w teście PassMark Performance Test, co najmniej 3900 punktów w kategorii Average CPU Mark (wynik na dzień 17.05.2022 r.) i po raz pierwszy będący na wykresach PassMark „CPU First Seen on Charts” w latach 2020-2022.
Pamięć RAM:
DDR4 8 GB z możliwością rozbudowy do min. 32 GB
Pamięć operacyjna/magazyn danych
M.2 PCIe 256GB o parametrach odczyt/zapis 1200/1200MB/s. Możliwość dołożenia drugiego dysku pracującego w standardzie SATA lub NVMe bez utraty gwarancji.
Karta graficzna:
Grafika zintegrowana z procesorem ze sprzętowym wsparciem dla DirectX 12, OpenGL 4.6.
Multimedia:
Karta dźwiękowa zgodna z HD Audio. Wbudowane głośniki. Kamera HD.
Łączność
Karta WLAN 802.11ac + BlueTooth 4.2. Zintegrowana gigabitowa karta LAN – zamawiający nie dopuszcza możliwości zastosowania karty USB-LAN.
Bateria i zasilacz:
Minimum 3 komorowa o pojemności 42Wh. Zasilacz dedykowany do notebooka.
Funkcje BIOS:
BIOS zgodny ze specyfikacją UEFI.
Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS bieżących informacji o:
- numerze seryjnym komputera.
- wersji BIOS.
- ilości zainstalowanej pamięci RAM.
- zastosowanym procesorze wraz z taktowaniem.
- zamontowanym dysku twardym wraz z jego pojemnością i modelem..

Możliwość włączenia/wyłączenia zintegrowanego z komputerem touchpada; bezprzewodowej karty sieciowej i modułu BlueTooth; zintegrowanej karty LAN; karty dźwiękowej; zintegrowanej kamery; portów USB; modułu TPM.
Możliwość ustawienia niezależnych haseł dla konta administratora, użytkownika i dysku twardego. Brak możliwości uruchomienia systemu operacyjnego bez podania hasła.
Funkcja ustawień zależności między hasłem administratora a użytkownika tak, aby nie było możliwe wprowadzenie zmian z poziomu użytkownika bez podania hasła do konta administratora.
Główne hasło zabezpieczające rozruch musi być zachowane nawet w przypadku odcięcia wszystkich źródeł zasilania (wliczając baterię RTC/CMOS).
Certyfikaty i standardy:
CE dla oferowanego komputera.
ISO 9001:2015 dla autoryzowanego serwisu Producenta notebooka.
Waga i wymiary:
Waga nieprzekraczająca 1,75kg, wymiary maksymalne 36x24x1,95cm
Bezpieczeństwo:
Dedykowana dioda LED zintegrowanej kamery sygnalizująca pracę komponentu.
Fizyczna przesłona na kamerze zintegrowana z obudową komputera.
Zintegrowany z płytą główną moduł TPM
Zintegrowane z obudową gniazdo Kensington
Wbudowany w obudowę czytnik linii papilarnych
Warunki gwarancji:
Minimum 36 miesięcy.
Gwarancja realizowana na miejscu u klienta.
Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych.
Wymagana gwarancja na baterię
Gwarancja na baterię nie może być krótsza niż gwarancja na całe urządzenie.
Wsparcie techniczne producenta:
Możliwość sprawdzenia telefonicznego bezpośrednio u producenta oraz na stronie internetowej producenta oferowanego notebooka, po podaniu numeru seryjnego - konfiguracji sprzętowej notebooka oraz warunków gwarancji.
Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu notebooka
Porty
- 2 porty USB typ A (3.2 Gen 2)
- 1 port USB typ C (3.2 Gen 2)
- 1 port HDMI
- 1 port VGA
- 1 port LAN RJ45
- 1 port Micro SD
- 1 port audio 3.5mm jack (combo lub osobne łącza)
Klawiatura
Z dedykowanym blokiem numerycznym po prawej stronie, podświetlona.
ciąg dalszy sekcja III.1.2)

II.2.5. Award criteria

Criteria below
Quality criterion - Name: Termin dostawy / Weighting: 15
Quality criterion - Name: Termin płatności / Weighting: 15

Quality criterion - Name: Wzmocniona konstrukcja / Weighting: 10
Price - Weighting: 60

II.2.6. Estimated value

II.2.7. Duration of the contract, framework agreement or dynamic purchasing system

Duration in days: 40
This contract is subject to renewal: no

II.2.10. Information about variants

Variants will be accepted: no

II.2.11. Information about options

Options: no

II.2.13. Information about European Union funds

The procurement is related to a project and/or programme financed by European Union funds: yes
Identification of the project: Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczące realizacji projektu grantowego "Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym - Granty PPGR"Program Operacyjny Polska Cyfrowa na lata 2014 – 2020Projekt: Cyfrowa Gmina POPC.05.01.00-00-0001/21-00

II.2.14. Additional information

Section III: Legal, economic, financial and technical information

III.1. Conditions for participation

III.1.1. Suitability to pursue the professional activity, including requirements relating to enrolment on professional or trade registers

List and brief description of conditions:
1. Do oferty wykonawca dołącza oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu, w zakresie wskazanym przez zamawiającego. Oświadczenie, o którym mowa powyżej, składa się na formularzu jednolitego europejskiego dokumentu zamówienia, sporządzonym zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16) oraz oświadczenia w zakresie szczególnych podstaw wykluczenia stanowiącym załącznik nr 3 do oferty. W celu potwierdzenia spełnienia warunków udziału w postępowaniu wykonawca ogranicza się do ogólnego oświadczenia dotyczącego wszystkich kryteriów kwalifikacji poprzez wypełnienie sekcji α i nie musi wypełniać żadnej z pozostałych sekcji w części IV Jednolitego dokumentu zamówienia (dalej JEDZ).
2. JEDZ, o którym mowa w ust. 1, stanowi dowód potwierdzający brak podstaw wykluczenia, spełnianie warunków udziału w postępowaniu na dzień składania ofert, tymczasowo zastępujący wymagane przez zamawiającego podmiotowe środki dowodowe. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, jednolite dokumenty zamówienia składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia.
3. Przedmiotowe środki dowodowe:

Zamawiający wymaga złożenia wraz z ofertą szczegółowej specyfikacji oferowanego sprzętu. Wzór szczegółowej specyfikacji oferowanego sprzętu stanowi załącznik nr 2 do SWZ. Złożona przez Wykonawcę szczegółowa specyfikacja oferowanego sprzętu powinna zawierać wszystkie informacje, które są wymagane w przygotowanym wzorze tzn.
◦ ogólne potwierdzenie, że oferowany sprzęt spełnia wymagania, dotyczy to komórek, gdzie Zamawiający wymaga wskazania odpowiedzi TAK lub NIE,
◦ szczegółowych informacji w zakresie komórek, w których znajdują się wykropkowane miejsca.
Szczegółowa specyfikacja powinna się odnosić do wszystkich elementów wskazanych w opisie przedmiotu zamówienia. Wykorzystanie wzoru przygotowanego przez Zamawiającego nie zwalnia Wykonawcy z obowiązku weryfikacji czy złożony przedmiotowy środek dowodowy odnosi się do wszystkich elementów wskazanych w opisie przedmiotu zamówienia
4. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
5. Zamawiający wzywa wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni od dnia wezwania, podmiotowych środków dowodowych, jeżeli wymagał ich złożenia w ogłoszeniu o zamówieniu lub dokumentach zamówienia, aktualnych na dzień złożenia podmiotowych środków dowodowych.
ciąg dalszy sekcja VI.3)

III.1.2. Economic and financial standing

List and brief description of selection criteria:
System operacyjny
Zainstalowany fabrycznie system operacyjny 64-bit w polskiej wersji językowej, klucz licencyjny zapisany trwale w BIOS umożliwiający instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Z racji na przeznaczenie komputera dopuszcza się możliwość zaoferowania systemu operacyjnego 64-bit w wersji Academic, spełniający co najmniej następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
1.Dostępne dwa rodzaje graficznego interfejsu użytkownika:
a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2.Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
3.Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4.Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5.Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7.Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8.Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9.Wbudowany system pomocy w języku polskim.
10.Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).

11.Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12.Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13.Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14.Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15.Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16.Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17.Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18.Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19.Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20.Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21.Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22.Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23.Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24.Wbudowany mechanizm wirtualizacji typu hypervisor.
25.Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26.Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
ciąg dalszy poniżej
Minimum level(s) of standards possibly required:
27.Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28.Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29.Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30.Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31.Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32.Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33.Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34.Możliwość tworzenia wirtualnych kart inteligentnych.

35.Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36.Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
37.Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38.Mechanizmy logowania w oparciu o:
a. Login i hasło,
b. Karty inteligentne i certyfikaty (smartcard),
c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
d. Certyfikat/Klucz i PIN
e. Certyfikat/Klucz i uwierzytelnienie biometryczne
39.Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej
Oprogramowanie antywirusowe
Ochrona antywirusowa i antyspyware
1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog3
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
13. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
14. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
15. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
16. Praca programu musi być niezauważalna dla użytkownika.
17.Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
18. Możliwość odblokowania ustawień programu po wpisaniu hasła
ciąg dalszy sekcja III.1.3)

III.1.3. Technical and professional ability

List and brief description of selection criteria:

19. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)
20. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
21. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
22. Wbudowany IDS
23. Możliwość tworzenia list sieci zaufanych.
24. Możliwość dezaktywacji funkcji zapory sieciowej.
25. Ochrona poczty(add-on1,2) – mechanizm pozwalający na ochronę poczty Office 365 lub Microsoft Exchange z wykorzystaniem serwera pośredniczącego.
26. Pełne Szyfrowanie dysków(add-on1)
27.Zarządzanie aktualizacjami oprogramowania firm trzecich(add-on1)
28.Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.
Ochrona stacji roboczych
1.Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2.Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3.Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4.Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5.Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6.Skanowanie plików spakowanych i skompresowanych.
7.Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8.Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9.Produkt i sygnatury są aktualizowane nie rzadziej niż raz na godzinę.
10.Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
11.Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12.Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13.Program musi mieć wbudowany skaner wyszukiwania rootkitów
14.Możliwość odblokowania ustawień programu po wpisaniu hasła
15.Możliwość uruchomienia zadania skanowania z niskim priorytetem
16.Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu)
17.Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
20.
Kolor obudowy
Dopuszcza się następujące kolory obudowy: szary, czarny, srebrny, granatowy.

III.2. Conditions related to the contract

III.2.2. Contract performance conditions

Projektowane postanowienia umowy są załączone do SWZ.
6. Przed podpisaniem umowy zamawiający może żądać przedstawienia:
1) certyfikatu CE dla oferowanego komputera;
2) ISO 9001:2015 dla autoryzowanego serwisu Producenta komputera;
3) dokumentu potwierdzającego, że oferowany sprzęt spełnia normę MIL-STD 810H minimum w zakresie metody 501.7, 502.7, 514.8, 516.8 lub normę równoważną.
- o ile powyższy dokument został wskazany w opisie przedmiotu zamówienia lub wykonawca wskazał go w ramach kryteriów oceny ofert

Section IV: Procedure

IV.1. Description

IV.1.1. Type of procedure
Open procedure

IV.1.3. Information about a framework agreement or a dynamic purchasing system

IV.1.8. Information about the Government Procurement Agreement (GPA)
The procurement is covered by the Government Procurement Agreement: no

IV.2. Administrative information

IV.2.2. Time limit for receipt of tenders or requests to participate
Date: 23/06/2022 Local time: 10:00

IV.2.3. Estimated date of dispatch of invitations to tender or to participate to selected candidates

IV.2.4. Languages in which tenders or requests to participate may be submitted
Polish

IV.2.6. Minimum time frame during which the tenderer must maintain the tender
Tender must be valid until: 20/09/2022

IV.2.7. Conditions for opening of tenders
Date: 23/06/2022 Local time: 10:05
Place:
www.platformazakupowa.pl/starogard_gdanski

Section VI: Complementary information

VI.1. Information about recurrence
This is a recurrent procurement: no

VI.3. Additional information
6. Podmiotowe środki dowodowe wymagane od wykonawcy obejmują:
1) informacji z Krajowego Rejestru Karnego w zakresie:
a) art. 108 ust. 1 pkt 1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych,
b) art. 108 ust. 1 pkt 4 ustawy, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego,
◦ sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem;

2) oświadczenia wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2020 r. poz. 1076 i 1086), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej;
3) oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w:
a) art. 108 ust. 1 pkt 3 ustawy,
b) art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
c) art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
d) art. 108 ust. 1 pkt 6 ustawy,
e) 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 (Dz.U. poz. 835) oraz w oświadczeniu o nie podleganiu zakazowi, o którym mowa w art. 5k ust. 1 pkt. a) - c) rozporządzenia Rady (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie.
7. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast dokumentu, o których mowa w ust. 6 pkt 1 składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania;
8. Dokumenty, o których mowa w ust. 7 powinien być wystawiony nie wcześniej niż 6 miesiące przed jego złożeniem;
9. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 7 lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa powyżej, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy. Zapisy ust. 8 stosuje się.
10. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.

VI.4. Procedures for review

VI.4.1. Review body

Official name: Krajowa Izba Odwoławcza
Postal address: ul. Postępu 17a
Town: Warszawa
Postal code: 02-676

Country: Poland
Internet address: https://www.uzp.gov.pl/kio

VI.4.3. Review procedure

Precise information on deadline(s) for review procedures:
1. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów Ustawy.
2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 p.z.p. oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
2) zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy.
4. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 10 dni od dnia zamieszczenia ogłoszenia w Dzienniku Urzędowym Unii Europejskij lub treści SWZ na stronie internetowej.
6. Odwołanie wnosi się w terminie:
1) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
2) 15 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).
7. Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
8. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 Ustawy, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
9. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17.11.1964 r. - Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.
10. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych, zwanego dalej "sądem zamówień publicznych".
11. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy p.z.p., przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23.11.2012 r. - Prawo pocztowe jest równoznaczne z jej wniesieniem.
12. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.

VI.4.4. Service from which information about the review procedure may be obtained

Official name: Krajowa Izba Odwoławcza

Postal address: ul. Postępu 17a
Town: Warszawa
Postal code: 02-676
Country: Poland
Internet address: https://www.uzp.gov.pl/kio

VI.5. Date of dispatch of this notice

23/05/2022