IGP.272.2.2025 Prochowice dn.03-02-2025 r.

ZAPYTANIE OFERTOWE

na zadanie pn. **Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Miasta i Gminy Prochowice oraz 4 jednostek podległych** realizowane w ramach projektu „Cyberbezpieczny Samorząd" dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe,
Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa

Dane dotyczące Zamawiającego
Nazwa: Gmina Prochowice
Adres: ul. Rynek 1, 59-230 Prochowice
Tel.: +48 076 85 84 342
Strona www: https://prochowice.com/

Tryb udzielenia zamówienia
1. Postępowanie prowadzone jest zgodnie z zasadą konkurencyjności, w oparciu o przepisy określone w Wytycznych dotyczących kwalifikowalności wydatków na lata 2021-2027 z dnia 18 listopada 2022 r.
2. Postępowanie prowadzone jest w języku polskim.

W związku z prowadzonym postępowaniem o udzielenie zamówienia publicznego, do którego nie stosuje się przepisów o zamówieniach publicznych, zwracam się z prośbą o przedstawienie oferty cenowej wykonania zamówienia na
Opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Miasta i Gminy Prochowice oraz 4 jednostek podległych dofinansowanego w formie grantu z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe,
Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa

I. Opis przedmiotu zamówienia:
1. Przedmiotem zamówienia jest usługa opracowania, wdrożenia, przeglądu, aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji dla Urzędu Miasta i Gminy Prochowice i dla 4 jednostek organizacyjnych.
2. Jednostki organizacyjne objęte przedmiotem zamówienia
   1) Urząd Miasta i Gminy Prochowice,
      adres: ul. Rynek 1, 59-230 Prochowice
   2) Szkoła Podstawowa nr 1 im. Mikołaja Kopernika w Prochowicach,
      adres: ul. Młyńska 3, 59-230 Prochowice
   3) Szkoła Podstawowa nr 2 im. Tadeusza Kościuszki w Prochowicach,
      adres: ul. Kościuszki 2, 59-230 Prochowice
   4) Szkoła Podstawowa im. ks. Jana Twardowskiego w Dąbiu,
      adres: Dąbie 5A, 59-230 Prochowice
   5) Przedszkole Miejskie w Prochowicach
      adres: ul. Kościuszki 1, 59-230 Prochowice

   Zamawiający wraz z jednostkami podległymi, o których mowa powyżej, zatrudnia 155 pracowników.
2. Zadanie objęte jest dofinansowaniem w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd".

3. Zakres realizacji usługi obejmuje opracowanie i wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301. Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:
   1) 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),
   2) ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.),
   3) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773).
4. Wykonawca zobowiązany jest do wytworzenia dokumentacji, formularzy, opracowania zasad postepowania, procedur, itd., które będą zgodne z zapisami Regulaminu Konkursu Grantowego oraz Wzorem Umowy o powierzeniu Grantu dostępnych na stronie: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad
5. Nazwy i kody dotyczące przedmiotu zamówienia określone we Wspólnym Słowniku Zamówień:
   79212000-3 Usługi audytu
   79417000-0 Usługi doradcze w zakresie bezpieczeństwa
   80500000-9 Usługi szkoleniowe
6. Ogólny zakres przedmiotu zamówienia obejmuje następujące części (etapy):

ETAP I

1) Wykonanie audytu wstępnego obejmującego min.:
   a) inwentaryzację uprawnień w programach i systemach informatycznych,
   b) inwentaryzację aktywów,
   c) rozpoznanie struktury organizacyjnej i realizowanych procesów oraz wymagań prawnych funkcjonowania jednostki.
2) Stworzenie/aktualizacja dokumentacji SZBI z uwzględnieniem istniejących procedur.
3) Opracowanie zasad i formularzy dotyczących nadawania i odbierania uprawnień w programach informatycznych.

ETAP II

1) Aktywny udział w inwentaryzacji aktywów oraz przypisaniu własności aktywów.
2) Analiza ryzyka i opracowanie planu postępowania z ryzykiem.
3) Dostosowanie procedur do istniejącego ryzyka.
4) Opracowanie planu ciągłości działania.

ETAP III

1) Przeprowadzenie w każdej jednostce stacjonarnego szkolenia dla kadry kierowniczej i pracowników z zakresu funkcjonowania i stosowania SZBI.
2) Opracowanie działań korygujących i zapobiegawczych.
3) Przygotowanie harmonogramu przeglądów funkcjonowania SZBI.

II. Wymagania stawiane Wykonawcom

1. Zamawiający wymaga aby wdrożenie SZBI polegało na analizie oraz aktualizacji i wdrożeniu istniejącej u Zamawiającego dokumentacji w sposób gwarantujący spełnienie wymagań norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005) i ISO 31000 w zakresie zarządzania ryzykiem oraz Systemu Zarządzania Ciągłością Działania – w zakresie systemów teleinformatycznych zgodnego z normą PN-EN ISO 22301.

2. Na bazie istniejącej w UMiG Prochowice dokumentacji Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm w celu spełnienia wymagań wynikających z:
   1) 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),
   2) ustawy z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.),
   3) rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773).
4. **Zamawiający wymaga aby Polityka Bezpieczeństwa Informacji wdrażana przez Wykonawcę w jednostkach organizacyjnych oparta została na dokumentacji wprowadzonej w UMiG Prochowice oraz (jeżeli będzie istniała taka możliwość) aby załączniki i procedury miały taką samą numerację.**
5. Kompletną dokumentację SZBI wraz formularzami, opracowaniami zasad postępowania, procedur oraz nową Politykę Ochrony Danych Osobowych **należy sporządzić w 2 egzemplarzach w wersji papierowej oraz 1 egz. w wersji elektronicznej, edytowalnej**.

III. Sposób realizacji zadania:

1. **Zamawiający wymaga aby wszystkie prace związane z przeprowadzaniem wywiadów, ankiet i analiz wśród pracowników Zamawiającego realizowane były przez przedstawiciela Wykonawcy w siedzibie Zamawiającego; Zamawiający wyklucza możliwość stosowania ankiet do samodzielnego wypełnienia przez pracowników Zamawiającego.**
2. **Wykonawca zobowiązany jest do stawiennictwa w siedzibie Zamawiającego na każde jego żądanie związane z realizacją przedmiotu zamówienia.**

IV. Wymagania dotyczące Polityki Bezpieczeństwa Informacji:

Zamawiający wymaga aby wdrożona Polityka Bezpieczeństwa Informacji w sposób usystematyzowany oraz jednoznaczny opisywała i regulowała wymienione niżej zagadnienia oraz obszary funkcjonowania wynikające bezpośrednio z celów stosowania zabezpieczeń stanowiących załącznik A do normy ISO/IEC 27001.

1. Polityka Bezpieczeństwa Informacji (zagadnienia ogólne):
   1) znaczenie bezpieczeństwa informacji dla organizacji,
   2) cele jakie organizacja zamierza osiągnąć w zakresie bezpieczeństwa informacji,
   3) obszar stosowania polityki,
   4) zgodność z obowiązującymi przepisami i normami.
2. Organizacja bezpieczeństwa informacji:
   1) role i odpowiedzialność za bezpieczeństwo informacji,
   2) rozdzielanie obowiązków,
   3) bezpieczeństwo informacji w zarządzaniu projektami,
   4) polityka stosowania urządzeń mobilnych,
   5) telepraca.
3. Bezpieczeństwo zasobów ludzkich:
   1) postępowanie sprawdzające przed zatrudnieniem,
   2) warunki zatrudnienia,
   3) odpowiedzialność kierownictwa, uświadamianie i szkolenia z zakresu bezpieczeństwa informacji,
   4) zakończenie zatrudnienia i zmiana zakresu obowiązków.
4. Zarządzanie aktywami:
   1) inwentaryzacja aktywów,
   2) własność aktywów,

3) akceptowalne użycie aktywów,
4) zwrot aktywów,
5) klasyfikowanie informacji,
6) oznaczanie informacji,
7) postępowanie z aktywami,
8) zarządzanie nośnikami wymiennymi,
9) wycofywanie nośników,
10) przekazywanie nośników.

5. Kontrola dostępu:
   1) polityka kontroli dostępu,
   2) dostęp do sieci i usług sieciowych,
   3) rejestrowanie i wyrejestrowanie użytkowników,
   4) przydzielanie dostępu użytkownikom,
   5) zarządzanie prawami uprzywilejowanego dostępu (w tym zasady funkcjonowania administratorów podstawowych, takich jak np.: admin, administrator, root),
   6) przegląd praw dostępu użytkowników,
   7) odbieranie lub dostosowanie praw dostępu,
   8) stosowanie poufnych informacji uwierzytelniających,
   9) ograniczanie dostępu do informacji,
   10) procedury bezpiecznego logowania,
   11) system zarządzania hasłami,
   12) użycie uprzywilejowanych programów narzędziowych,
   13) kontrola dostępu do kodów źródłowych programów.
6. Kryptografia:
   1) polityka stosowania zabezpieczeń kryptograficznych,
   2) zarządzanie kluczami.
7. Bezpieczeństwo fizyczne i środowiskowe.
   1) fizyczna granica obszaru bezpiecznego,
   2) fizyczne zabezpieczenie wejść,
   3) zabezpieczenie biur, pomieszczeń i obiektów,
   4) ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
   5) praca w obszarach bezpiecznych,
   6) obszary dostaw i załadunku,
   7) lokalizacja i ochrona sprzętu,
   8) systemy wspomagające,
   9) bezpieczeństwo okablowania,
   10) konserwacja sprzętu,
   11) wynoszenie aktywów,
   12) bezpieczeństwo sprzętu i aktywów poza siedzibą,
   13) bezpieczne zbywanie lub przekazywanie do ponownego użycia,
   14) pozostawienie sprzętu użytkownika bez opieki,
   15) polityka czystego biurka i czystego ekranu.
8. Bezpieczna eksploatacja:
   1) dokumentowanie procedur eksploatacyjnych,
   2) zarządzanie zmianami,
   3) zarządzanie pojemnością,
   4) zabezpieczenia przed szkodliwym oprogramowaniem,
   5) kopie zapasowe,
   6) rejestrowanie zdarzeń,
   7) ochrona informacji w dziennikach zdarzeń,
   8) rejestrowanie działań administratorów i operatorów,
   9) synchronizacja zegarów,
   10) instalacja oprogramowania w systemach produkcyjnych,
   11) zarządzanie podatnościami technicznymi,
   12) ograniczenia w instalowaniu oprogramowania.
9. Bezpieczeństwo komunikacji:

1) zabezpieczenia sieci,
2) bezpieczeństwo usług sieciowych,
3) rozdzielanie sieci,
4) polityki i procedury przesyłania informacji,
5) wiadomości elektroniczne.

10. Pozyskiwanie, rozwój i utrzymanie systemów:
    1) analiza i specyfikacja wymagań bezpieczeństwa informacji,
    2) zabezpieczanie usług aplikacyjnych w sieciach publicznych,
    3) procedury kontroli zmian w systemach.
11. Analiza ryzyka:
    1) strategia zarządzania ryzykiem - opis konkretnych działań odnoszących się do zarządzania ryzykiem, w tym: opis procesu, narzędzia i techniki, role i zakresy odpowiedzialności, skala oceny prawdopodobieństwa i wpływu ryzyka, progi tolerancji na ryzyko, kategorie ryzyka,
    2) szablony (wzory dokumentów) niezbędne w zarządzaniu ryzykiem, kluczowe wskaźniki efektywności i wskaźniki wczesnego ostrzegania, harmonogram działań, raportowanie,
    3) diagnoza ryzyka - identyfikacja ryzyk pozwalająca ocenić sytuację i zdarzenia pod kątem ich możliwego wpływu na bezpieczeństwo informacji,
    4) analiza i ocena - analiza ryzyka (ocena) z wykorzystaniem metody oceny jakościowej/ilościowej,
    5) monitorowanie ryzyka,
    6) rejestr ryzyk.
12. Plan ciągłości działania:
    1) identyfikacja kluczowych zasobów, procesów, usług i dostawców,
    2) scenariusze utraty ciągłości działania,
    3) zasady komunikacji w sytuacjach kryzysowych,
    4) plany przywracania ciągłości działania,
    5) redundancja zasobów i usług kluczowych,
    6) zasady testowania planu.

V. Ochrona danych osobowych

Zamawiający wymaga aby zagadnienia związane z ochroną danych osobowych opracowane były w wydzielonym dokumencie (Polityka Ochrony Danych Osobowych). Zamawiający wymaga aby dokument ten zawierał w szczególności:

1. struktura organizacji ochrony danych osobowych,
2. zasady przekazywania danych odbiorcom (zasady powierzenia i udostępnienia danych),
3. zasady privacy by design oraz privacy by defalut,
4. zasady retencji danych osobowych,
5. procedura szkoleń oraz nadawania upoważnień do przetwarzania danych,
6. procedura postępowania z incydentami związanymi z ochroną danych osobowych,
7. procedura oceny skutków dla ochrony danych osobowych (DPIA),
8. procedura realizacji praw osób, których dane dotyczą,
9. procedura audytu zgodności przetwarzania danych osobowych,
10. opis organizacyjnych środków bezpieczeństwa,
11. opis fizycznych środków bezpieczeństwa,
12. opis technicznych środków bezpieczeństwa,
13. wzory ewentualnych formularzy do powyższych zasad i procedur.

VI. Wymagania dotyczące polityki bezpieczeństwa systemu informatycznego

Zamawiający wymaga aby wszystkie zagadnienia odnoszące się bezpośrednio do systemu informatycznego opracowane były w wydzielonym dokumencie do zapisów którego odnosić się będą zarówno Polityka Bezpieczeństwa Informacji oraz Polityka Ochrony Danych Osobowych. Zamawiający wymaga aby dokument ten regulował następujący (minimalny) zakres działań/zagadnień:

1. nadawanie uprawnień użytkownikom systemów informatycznych należących do Zamawiającego w sposób precyzyjny i jednoznaczny, umożliwiający wykonywanie okresowej kontroli uprawnień w programach i systemach informatycznych,

2. zasady nadawania uprawnień uprzywilejowanych (ASI),
3. nadawanie uprawnień w systemach informatycznych niepodlegających nadzorowi ze strony administratora lokalnego (np. ZUS PUE, GUS, ePUAP),
4. organizacja certyfikatów SSL,
5. organizacja kluczy szyfrujących,
6. zasady użytkowania zewnętrznych nośników informacji,
7. zasady użytkowania komputerów mobilnych,
8. zasady wykonywania pracy zdalnej przez pracowników Zamawiającego,
9. zasady nawiązywania połączeń zdalnych przez wsparcie techniczne producentów programów (w trybie nadzorowanym i nienadzorowanym),
10. zasady nawiązywania połączeń zdalnych przez Administratorów Systemu Informatycznego,
11. archiwizacja danych i testowanie kopii bezpieczeństwa,
12. kontrola dostępu do sieci, systemu i aplikacji,
13. użytkowanie i zabezpieczenia stanowiska użytkownika,
14. bezpieczeństwo fizyczne i środowiskowe,
15. kontrola połączeń z siecią publiczną,
16. zasady wykorzystania zabezpieczeń kryptograficznych,
17. aktualizacja i testowanie oprogramowania.

Dokumentacja opisująca zasady funkcjonowania i kontroli systemu informatycznego powinna zawierać szablony wszystkich wykazów i rejestrów które powinny być prowadzone przez użytkowników lub administratorów systemu informatycznego.

VII. Wymagania dotyczące zakresu szkoleń dla kadry kierowniczej i pracowników z zakresu funkcjonowania i stosowania SZBI

Szkolenie prowadzone dla pracowników Urzędu oraz jednostek podległych powinno obejmować m.in.:

1. Wymogi wynikające z Krajowych Ram Interoperacyjności (KRI), Ustawa o krajowym systemie cyberbezpieczeństwa (UoKSC) i Ogólne rozporządzenie o ochronie danych (RODO),
2. zarządzanie ryzykiem w bezpieczeństwie informacji,
3. System Zarzadzania Bezpieczeństwem informacji – jak skutecznie przestrzegać procedur wdrożonej Polityki Bezpieczeństwa Informacji,
4. ciągłość działania – dlaczego jest istotna i jak ją wdrożyć,
5. identyfikowanie zagrożeń – jak wdrożyć odpowiednie rozwiązania na przestrzeganie zasad bezpieczeństwa,
6. przegląd znanych typów ataków na JST - najnowsze zagrożenia,
7. podstawy prawne i główne zasady cyberbezpieczeństwa,
8. bezpieczeństwo informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI:
   1) wewnętrzne procedury w obszarze bezpieczeństwa informacji cyberbezpieczeństwa,
   2) wymagania dla pracowników wynikające z KRI, UoKSC oraz RODO,
   3) System Zarządzania Bezpieczeństwem Informacji w praktyce.
9. Przegląd najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu:
   1) ochrona informacji i prywatność w internecie,
   2) Ransomware jako poważne zagrożenie dla JST,
   3) Phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise),
   4) Cyberhigiena, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne,
   5) bezpieczne hasła i uwierzytelnienie dwuskładnikowe,
   6) wewnętrzne zalecenia i rekomendacje, w tym sposoby reakcji na incydenty bezpieczeństwa.

Potwierdzeniem udziału kadry kierowniczej i pracowników w szkoleniu będzie imienna lista obecności.

Uwaga!.
W przypadku gdy przywoływane przez Zamawiającego „aktualne normy" nie posiadają oficjalnej, polskiej wersji językowej osiągalnej za pośrednictwem Polskiego Komitetu

Normalizacyjnego Zamawiający dopuszcza zastosowanie ich wersji poprzedniej (wycofanej) opublikowanej w polskiej wersji językowej.

VIII. Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny ich spełniania

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu, dotyczące **zdolności technicznej i zawodowej:**

1. **w zakresie doświadczenia Wykonawcy**:
   Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat, a jeśli okres jego działalności jest krótszy, to w tym okresie wykonał **co najmniej 4 usługi** w zakresie audytowania systemów zarządzania bezpieczeństwem informacji (SZBI).
   Na potwierdzenie spełnienia ww. warunku udziału w postępowaniu w zakresie doświadczenia Wykonawcy, Wykonawca zobowiązany jest przedstawić **wraz z ofertą** wykaz wykonanych usług w okresie ostatnich 3 lat licząc wstecz od dnia upływu terminu składania ofert, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane oraz załączeniem dokumentów potwierdzających należyte wykonanie usług (np. referencje, protokoły odbioru usług lub inne, z których będzie jednoznacznie wynikać należyte wykonanie usługi) - **wzór wykazu stanowi Załącznik nr 3 do Zapytania cenowego.**
2. **w zakresie osób skierowanych przez Wykonawcę do realizacji zamówienia:**
   Zamawiający uzna warunek za spełniony, jeżeli Wykonawca skieruje do realizacji zamówienia **co najmniej jedną osobę** będącą audytorem posiadającym przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999).
   Na potwierdzenie spełnienia ww. warunków Wykonawca zobowiązany jest przedstawić wykaz osób skierowanych do realizacji zamówienia wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności a także kopiami dokumentów potwierdzającymi posiadane doświadczenie i certyfikaty - **wzór wykazu stanowi Załącznik nr 4 do Zapytania cenowego.**

IX. Podstawy wykluczenia wykonawcy z postępowania oraz ocena braku podstaw wykluczenia wykonawcy z postępowania

1. O udzielenie zamówienia **nie może ubiegać się** Wykonawca jeżeli w stosunku do niego zachodzi którakolwiek z okoliczności, o których mowa w 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. z 2023 r. poz. 1497 z późn. zm.);
2. O udzielenie zamówienia **nie może ubiegać się** Wykonawca jeżeli w stosunku do niego zachodzi jakikolwiek konflikt interesów lub powiązania osobowe lub kapitałowe z Zamawiającym.
3. W celu potwierdzenia braku podstaw do wykluczenia Wykonawcy wskazanych w ust. 1, Wykonawca zobowiązany jest złożyć **wraz z ofertą** oświadczenie, zgodne ze wzorami oświadczeń, stanowiących **Załącznik nr 5 i 6 do Zapytania cenowego**.
4. Zamawiający wykluczy Wykonawcę z postępowania o udzielenie zamówienia, w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w pkt 1 lub pkt 2.

X. Termin wykonania zamówienia

Termin realizacji całego przedmiotu zamówienia ustala od dnia zawarcia umowy **do dnia 31 sierpnia 2025r.**

XI. Kryteria oceny ofert.

1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami:

Nazwa kryterium	Waga
Cena (C)	100%

Najniższa cena – 100 pkt.

Badana oferta – C

$$C = (C_{min} / C_b) \times 100$$

C_{min}- najniższa cena spośród wszystkich ofert niepodlegających odrzuceniu;
C_b- cena oferty badanej niepodlegającej odrzuceniu.

2. Punktacja przyznawana ofertom będzie liczona z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
3. Wykonanie zamówienia powierzone będzie temu Wykonawcy, który spełnia wszystkie wymagania wymienione w Zapytaniu cenowym oraz przedstawi najkorzystniejszą ofertę cenową.
4. Jeżeli nie będzie można dokonać wyboru najkorzystniejszej oferty z uwagi na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę.

XII. Opis sposobu obliczenia ceny i rozliczenia zamówienia:

1. Za usługę Wykonawca powinien przedstawić cenę w PLN wraz z należnym podatkiem VAT wyliczoną na podstawie formularza cenowego stanowiącego **Załącznik nr 1 do Zapytania cenowego.**
2. **Oferta musi obejmować całość zamówienia** – zgodnie z opisem zawartym w Zapytaniu cenowym.
3. Wykonawca poniesie wszelkie koszty związane z realizacją przedmiotu zamówienia.
4. Cena musi obejmować wszystkie wymagane przepisami prawa obciążenia fiskalne.
5. Szczegóły dotyczące rozliczenie i wypłaty wynagrodzenia zawarte zostały w projekcie umowy stanowiącym Zał. Nr 2 do Zapytania cenowego.
7. Rozliczenia prowadzone będą w walucie polskiej.
8. W przypadku stwierdzenia nieścisłości Wykonawca winien zwrócić się do Zamawiającego w celu ich wyjaśnienia.
9. Wszystkie ceny jednostkowe określone przez Wykonawcę zostaną ustalone na okres ważności umowy i nie będą podlegały zmianom za wyjątkiem zmiany stawki podatku VAT. Rozliczenie wg warunków jak w projekcie umowy stanowiącym **Załącznik nr 2 do Zapytania cenowego.**

XIII. Termin i sposób składania ofert

1. **Oferta musi obejmować całość zamówienia** zgodnie z opisem przedmiotu zamówienia w ramach niniejszego Zapytania cenowego.
2. Ofertę należy złożyć pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy.
3. Oferty stanowiące odpowiedź na niniejsze zaproszenie należy złożyć za pośrednictwem **Bazy konkurencyjności (BK2021)** dostępnej pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/ Zakładka „Oferty”
4. Oferta powinna być złożona na wzorze formularza ofertowego stanowiącego **Załącznik nr 1 do Zapytania cenowego.** Zasady składania ofert w Bazie Konkurencyjności zostały określone pod adresem:https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/pomoc/50-dodanie-oferty-doogloszenia
5. Zamawiający nie dopuszcza innej formy i sposobu składania ofert niż za pośrednictwem BK2021. Niespełnienie tego wymogu oznacza niezgodność oferty z zaproszeniem.
6. Oferty złożone poza BK2021 zostaną odrzucone przez Zamawiającego.
7. Oferty można składać do dnia **14 lutego 2025r. do godz. 12:00.**
8. O terminowym złożeniu oferty decyduje data złożenia oferty za pośrednictwem BK2021.
9. Otwarcie ofert nastąpi niezwłocznie po upływie terminu na ich złożenie
10. Wykonawca może złożyć tylko jedną ofertę.
11. Wykonawca przedstawi ofertę zgodnie z postanowieniami niniejszego Zapytania cenowego.
12. Wszelkie koszty związane z przygotowaniem oferty ponosi Wykonawca.

13. Upoważnienie do podpisania oferty winno być dołączone do oferty, o ile nie wynika ono z ustawy lub innych dokumentów załączonych do oferty.
14. Oferta oraz załączone dokumenty nie podlegają zwrotowi po jej otwarciu.
15. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
16. Oferta winna być sporządzona w języku polskim pod rygorem nieważności. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.

XIV. Informacja o oświadczeniach i dokumentach, jakie ma dostarczyć Wykonawca w ofercie.

Złożona oferta powinna zawierać co najmniej:

1. Ofertę cenową złożoną na formularzu stanowiącym **Załącznik nr 1** do niniejszego Zapytania cenowego. Upoważnienie do podpisania oferty winno być dołączone do oferty, o ile nie wynika ono z ustawy lub innych dokumentów załączonych do oferty.
2. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

***„Uwaga!** Zamawiający nie wymaga złożenia, jeżeli może je uzyskać dokument za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r, o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazał dane umożliwiające dostęp do tych środków.*

3. Wykazu usług wykonanych – wzór wykazu stanowi **Załącznik nr 3**.
4. Wykaz osób skierowanych do realizacji zamówienia - – wzór wykazu stanowi **Załącznik nr 4.**
5. Oświadczenie Wykonawcy dotyczące niepodlegania wykluczeniu z postępowania lub realizacji umowy - **Załącznik nr 5**.
6. Oświadczenie Wykonawca o konflikcie interesów – **Załącznik nr 6.**

XV. Informacje dotyczące ofert częściowych, ofert wariantowych

1. Zamawiający nie dopuszcza składania ofert wariantowych. Wykonawca przedstawi ofertę zgodnie z postanowieniami niniejszej dokumentacji. Alternatywy nie będą brane pod uwagę.
2. Zamawiający **nie przewiduje** możliwości składania ofert częściowych w ramach niniejszego Zapytania ofertowego.
3. Przedmiot niniejszego Zapytania dotyczy jednej usługi stanowiącej zintegrowane ze sobą elementy, których nie można dzielić. Zamawiający działając racjonalnie, poprzez uzyskanie najlepszych efektów z poniesionych nakładów, nie może dopuścić do maksymalnego możliwego rozdrobnienia zamówienia, z uwagi na fakt, że nadmierne rozdrobnienie przedmiotowego zamówienia na części może pociągnąć za sobą negatywne skutki dla Zamawiającego. Wartością stanowiąca podstawę wyboru trybu jest łączna wartość innych podobnych zamówień uwzględnionych w określeniu wartości szacunkowej niniejszego Zapytania. Zamawiający dokonał więc już podziału wyodrębniając podobne zamówienia dla całego grantu. Dokonywanie dalszego podziału wiązałoby się z nadmiernym rozdrobnieniem zamówienia.
4. Zamawiający nie przewiduje udzielania zamówień uzupełniających.

XVI. Określenie warunków istotnych zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia

Warunki zmian umowy zostały określone w projekcie umowy stanowiącej **Załącznik nr 2** do Zapytania cenowego.

XVII. Pozostałe uwarunkowania

1. W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Wykonawcą w celu uzupełnienia lub doprecyzowania przesłanych dokumentów.
2. W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień oraz uzupełnień dotyczących treści złożonej oferty.
3. Zamawiający zastrzega sobie możliwość przeprowadzenia negocjacji dotyczących złożonej oferty.
4. Negocjacje mogą być prowadzone w celu doprecyzowania warunków umowy, formy realizacji

zamówienia.

5. Termin związania ofertą wynosi 30 dni kalendarzowych od dnia upływu terminu składania ofert.
6. Zamawiający odrzuci oferty Wykonawcy jeżeli :
    1) Wykonawca nie spełni wymagań stawianych przez Zamawiającego;
    2) Wykonawca nie odpowie na wezwanie do uzupełnień / wyjaśnień w terminie określonym przez Zamawiającego w wezwaniu;
    3) jej treść nie odpowiada treści Zapytania cenowego;
    4) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
    5) zawiera błędy w obliczeniu ceny lub kosztu;
    6) jest nieważna na podstawie odrębnych przepisów;
    7) została złożona po terminie wyznaczonym na złożenie.
7. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, bez podania przyczyny, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.
8. Jeżeli Wykonawca, którego oferta została wybrana, uchyli się od zawarcia umowy, Zamawiający wybierze ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownej oceny.
9. Zamawiający zawrze umowę niezwłocznie po przekazaniu zawiadomienia o wyborze oferty.
10. Wykonawca ponosi odpowiedzialność z tytułu **rękojmi** za wady fizyczne i prawne przedmiotu zamówienia.
11. Okres rękojmi i gwarancji ustalony jest na cały okres realizacji i trwałości projektu i wynosi 24 miesiące od daty odbioru przedmiotu zamówienia.
12. Zamawiający może wykonywać uprawnienia z tytułu **gwarancji** niezależnie od uprawnień z tytułu rękojmi, w szczególności w dochodzeniu usunięcia wad przedmiotu umowy. Zamawiający ma prawo wyboru między gwarancją i rękojmią. Wykonawca nie może odmówić usunięcia wad bez względu na wysokość związanych z tym kosztów. W przypadku nieusunięcia ujawnionych wad w terminie określonym przez Wykonawcę, Zamawiający ma prawo do zastępczego usunięcia wad w ramach rękojmi – na koszt Wykonawcy.
13. Wykonawca zobowiązany jest niezwłocznie udzielać informacji i wyjaśnień w przypadku wątpliwości i zastrzeżeń dotyczących udzielonego doradztwa lub przygotowanych dokumentów.
14. Do prowadzonego postępowania nie przysługują Wykonawcom środki ochrony prawnej określone w przepisach Ustawy Prawo zamówień publicznych tj. odwołanie, skarga.

Burmistrz Miasta i Gminy Prochowice

Alicja Elżbieta Sielicka

Elektronicznie podpisany przez Alicja Elżbieta Sielicka
Data: 2025.02.03 13:33:43 +01'00'

Załączniki :

1. Formularz oferty.
2. Projekt umowy.
3. Wykaz usług.
4. Wykaz osób.
5. Oświadczenie Wykonawcy.
6. Oświadczenie Wykonawcy.

KLAUZULA INFORMACYJNA Z ART. 13 RODO

Zgodnie z art. 13 ust. 1 i ust. 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 (RODO), informujemy że:

1. Administratorem Pani/Pana danych osobowych jest: : Miasto i Gmina Prochowice reprezentowane przez Burmistrza, ul. Rynek 1, 59-230 Prochowice, tel. 76 85 84 342, e-mail: prochowice@prochowice.pl
2. W sprawach związanych z Pani/Pana danymi osobowymi proszę kontaktować się z Inspektorem Ochrony Danych (IOD): e-mail: iodo@amt24.biz
3. Pani/Pana dane osobowe przetwarzane będą w celu przeprowadzenia postępowania i udzieleniu zamówienia, prowadzeniu dokumentacji księgowo-podatkowej, archiwizacji danych, dochodzenia roszczeń lub obroną przed roszczeniami.
4. Podstawą przetwarzania danych osobowych jest:
    1) Ustawa z dnia 11 września 2020r. Prawo zamówień publicznych.
    2) Ustawa z dnia 27 sierpnia 2009r. o finansach publicznych.
    3) Ustawa z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach.
    4) art. 6 pkt.1 lit. c RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.
5. Odbiorca lub kategorie odbiorców: Podmioty upoważnione na podstawie zawartych umów powierzenia oraz uprawnione na mocy obowiązujących przepisów prawa. W szczególności osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania w oparciu o art. 18 oraz art. 421 ust.4 ustawy z dnia 11 września 2019r. Prawo zamówień Publicznych (Dz.U. z 2019r. Poz. 2019 ze zm.); Zasada jawności ma zastosowanie do wszystkich danych osobowych z wyjątkiem danych o których mowa w art. 9 ust. 1 RODO (szczególna kategoria danych),
6. Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji celu przetwarzania, oraz przez okres wynikający z przepisów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych. W szczególności zgodnie z ustawą PZP przez okres 4 lat od zakończenia roku kalendarzowego, w którym umowa została wykonana lub postępowanie o udzielenie Zamówienia zostało zakończone bez zawarcia umowy.
7. Posiada Pani/Pan prawo:
    1) Prawo żądania dostępu do danych (w przypadku gdy wykonanie tego obowiązku, wymagałoby niewspółmiernie dużego wysiłku, zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu zgodnie ustawą PZP).
    2) Prawo żądania sprostowania danych - wykonanie tego obowiązku nie może skutkować zmianą wyniku postępowania ani zmianą postanowień umowy w zakresie niezgodnym z ustawą oraz nie może naruszać integralności protokołu oraz jego załączników zgodnie z art. 18 ustawy PZP.
    3) Prawo usunięcia danych w przypadku gdy dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.
    4) Prawo żądania ograniczenia przetwarzania (zgodnie z ustawą PZP wykonanie tego obowiązku nie ogranicza przetwarzania danych osobowych do czasu zakończenie postępowania o udzielenie zamówienia publicznego).
8. Ma Pani/Pan prawo do wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych ul. Stawki 2, 00-913 Warszawa.
9. Pani/Pana dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu.
10. Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.
11. Podanie danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy PZP, związanych z udziałem w postępowaniu o udzielenie zamówienia publicznego.
12. Konsekwencją niepodania danych osobowych będzie brak możliwości udziału w postępowaniu o udzielenie zamówienia publicznego.