Znak postępowania: FDI.261.3.2026

ZAPYTANIE OFERTOWE

(zaproszenie do złożenia oferty)

Przedmiot zamówienia:

Audyt bezpieczeństwa IT, wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz opracowanie kompletnej dokumentacji zgodnej z ustawą o Krajowym Systemie Cyberbezpieczeństwa i dyrektywą NIS 2, wraz z testami penetracyjnymi, testami socjotechnicznymi i ćwiczeniem zarządzania kryzysowego

Zamówienie realizowane w ramach projektu pn. „Poprawa poziomu Cyberbezpieczeństwa w Sanockim Przedsiębiorstwie Gospodarki Komunalnej Sp. z o.o. w Sanoku", współfinansowanego ze środków Unii Europejskiej w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, Inwestycja C3.1.1 Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi, konkurs grantowy „Cyberbezpieczne Wodociągi" nr KPOD.05.10-CW.01-001/25.

I. Zamawiający

Sanockie Przedsiębiorstwo Gospodarki Komunalnej Sp. z o.o., ul. Jana Pawła II 59, 38-500 Sanok; NIP: 687-00-05-556; REGON: 370301150; KRS: 0000118475 (Sąd Rejonowy w Rzeszowie, XII Wydział Gospodarczy); kapitał zakładowy: 29 485 500,00 zł; tel.: 13 464 78 00; e-mail: sekretariat@spgk.com.pl; www.spgk.com.pl; spgk.nowybip.pl

II. Tryb postępowania

1) Postępowanie prowadzone jest w celu udzielenia zamówienia, którego wartość szacunkowa nie przekracza progu obligującego Zamawiającego do stosowania ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2026 r. poz. 793) i podlega wyłączeniu z obowiązku jej stosowania.

2) Postępowanie prowadzone jest na podstawie obowiązującego u Zamawiającego „Regulaminu przeprowadzania postępowań o udzielenie podprogowych zamówień publicznych", dokumentu „Zasady kwalifikowania wydatków w Przedsięwzięciach realizowanych w ramach Inwestycji C3.1.1 Krajowego Planu Odbudowy i Zwiększania Odporności – Załącznik nr 1: Zamówienia

udzielane w Przedsięwzięciach realizowanych w ramach inwestycji C3.1.1" oraz przepisów Kodeksu cywilnego.

3) Zgodnie z art. 70^1 § 3 KC Zamawiający zastrzega sobie prawo do zmiany lub odwołania warunków postępowania, a także do zamknięcia postępowania bez wyboru oferty i do jego unieważnienia na każdym etapie bez podania przyczyny. Niniejsze zapytanie nie stanowi zobowiązania Zamawiającego do zawarcia umowy.

4) Zamawiającemu przysługuje prawo do przeprowadzenia dodatkowych negocjacji z Wykonawcami, którzy złożyli oferty, oraz do wezwania Wykonawców do złożenia wyjaśnień, uzupełnień i ofert dodatkowych.

5) Zapytanie zostaje upublicznione na stronie podmiotowej Biuletynu Informacji Publicznej Zamawiającego (spgk.nowybip.pl). Postępowanie ma charakter otwarty – ofertę może złożyć każdy Wykonawca spełniający warunki określone w niniejszym zapytaniu. Postępowanie rozpoczyna się z dniem publikacji zapytania, a upublicznienie zapewnia zachowanie zasad przejrzystości, uczciwej konkurencji i równego traktowania Wykonawców, zgodnie z zasadami wskazanymi w pkt 2.

III. Osoby uprawnione do kontaktu

1) Osoba uprawniona do kontaktu: Michał Hassinger tel.: 798876391, e-mail: michal.hassinger@spgk.com.pl
2) Wykonawca może zwrócić się o wyjaśnienie treści zapytania na wskazany wyżej adres e-mail. Treść pytań (bez ujawniania źródła) wraz z odpowiedziami Zamawiający publikuje niezwłocznie na stronie BIP, w miejscu publikacji zapytania – w sposób i terminie gwarantującym równy dostęp do informacji o zamówieniu. Wiążąca jest wyłącznie treść opublikowana na stronie BIP.
3) Zamawiający może przed upływem terminu składania ofert zmienić treść zapytania; zmianę publikuje na stronie BIP, a jeżeli jest to konieczne dla uwzględnienia zmiany w ofertach – odpowiednio przedłuża termin składania ofert.
4) Informacja o wyniku postępowania (albo o jego zamknięciu bez wyboru oferty) zostanie opublikowana na stronie BIP oraz przekazana Wykonawcom, którzy złożyli oferty.

IV. Opis przedmiotu zamówienia

1) Zadanie 1 – Audyt zgodności z ustawą o KSC z uwzględnieniem dyrektywy NIS 2

Wykonawca przeprowadzi audyt obejmujący weryfikację realizacji przez Zamawiającego obowiązków wymaganych od podmiotów kluczowych i ważnych, w zakresie: zarządzania ryzykiem cyberbezpieczeństwa; ustanowienia i stosowania regulacji wewnętrznych dotyczących polityki zarządzania ryzykiem i oceny skuteczności środków, polityk bezpieczeństwa systemów

informatycznych, bezpieczeństwa łańcucha dostaw, cyberbezpieczeństwa, obsługi incydentów, bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów, postępowania z podatnościami, stosowania kryptografii, uwierzytelniania, ciągłości działania i przywracania działalności, kopii zapasowych, bezpieczeństwa zasobów ludzkich, bezpieczeństwa fizycznego, kontroli dostępu, zarządzania aktywami, prowadzenia audytów bezpieczeństwa oraz ochrony danych osobowych; szkoleń kadry i pracowników; stosowania certyfikowanych produktów, usług i procesów ICT; korzystania z kwalifikowanych usług zaufania; gotowości do zgłaszania incydentów poważnych do właściwego CSIRT, powiadamiania odbiorców usług oraz uczestnictwa w mechanizmach wymiany informacji.

Zamawiający dysponuje jedynie szczątkową dokumentacją z obszaru cyberbezpieczeństwa. Audyt będzie miał charakter analizy luk (gap analysis): Wykonawca samodzielnie zidentyfikuje wszystkie obszary wymagające uregulowania, a stan faktyczny ustali przede wszystkim na podstawie wywiadów z personelem, oględzin oraz weryfikacji technicznej konfiguracji systemów – nie zaś wyłącznie na podstawie analizy dokumentów; brak dokumentacji w danym obszarze zostanie odnotowany jako niezgodność ze wskazaniem dokumentów wymagających opracowania. Kryteriami audytu są (wg stanu prawnego na dzień realizacji, z obowiązkiem uwzględnienia znowelizowanej ustawy o KSC i aktów wykonawczych): dyrektywa NIS 2; ustawa o KSC z aktami wykonawczymi; rozporządzenia wykonawcze dotyczące usług kluczowych, progów incydentów, rodzajów dokumentacji oraz warunków organizacyjnych i technicznych; RODO w zakresie bezpieczeństwa przetwarzania; normy ISO/IEC 27001:2022 i PN-EN ISO/IEC 27001:2017-06, a pomocniczo – w zakresie ciągłości działania – PN-EN ISO 22301:2020-04 oraz normy bezpieczeństwa fizycznego (PN-EN 1627, PN-EN 12209, PN-EN 50131-1).

Audyt zostanie przeprowadzony w sposób spełniający wymagania audytu bezpieczeństwa systemu informacyjnego z art. 15 ustawy o KSC, przez audytorów spełniających wymagania określone przepisami (wymagane certyfikaty lub równoważne uprawnienia albo co najmniej dwóch audytorów z wymaganym doświadczeniem); dokumenty potwierdzające te wymagania Wykonawca przedłoży przed rozpoczęciem audytu. Wynikiem Zadania 1 jest raport wskazujący audytowane obszary, ocenę stanu, niezgodności i luki oraz rekomendacje z priorytetyzacją, w tym kompletny wykaz obszarów do uregulowania i dokumentów do opracowania – stanowiący podstawę zakresu prac Zadań 2 i 3, a także zawierający elementy wymagane przepisami dla sprawozdania z audytu.

2)Zadanie 2 – Wdrożenie SZBI (ISO/IEC 27001:2022)

Zakres SZBI obejmie całą organizację Zamawiającego – wszystkie jednostki, lokalizacje oraz systemy IT i przemysłowe (OT/SCADA), w tym systemy wspierające świadczenie usług kluczowych; nie dopuszcza się zawężenia zakresu. Audyt z Zadania 1 zastępuje wstępny audyt bezpieczeństwa informacji. Wdrożenie nastąpi w trzech etapach:

– Etap 1: propozycja składu i regulaminu zespołu ds. cyberbezpieczeństwa i ciągłości działania wraz z projektem aktu powołującego; identyfikacja i udokumentowanie procesów wpływających

na usługi kluczowe; szkolenie zespołu wdrożeniowego z ISO/IEC 27001:2022; pełna identyfikacja aktywów informacyjnych z rejestrem aktywów (właściciele, lokalizacja, wymagania ochrony); zasady klasyfikacji informacji wraz z przeprowadzeniem klasyfikacji; analiza kontekstu organizacji; ocena ryzyka i szans (identyfikacja, analiza, ewaluacja, postępowanie z ryzykiem, monitorowanie) wraz z „Planem postępowania z ryzykiem".

– Etap 2: kompletna dokumentacja systemowa (nadzór nad udokumentowanymi informacjami, audyty wewnętrzne, działania korygujące, przeglądy zarządzania i pozostała dokumentacja wymagana normą i KSC); polityka bezpieczeństwa informacji; cele bezpieczeństwa; dokumentacja SZBI obejmująca zabezpieczenia załącznika A do ISO/IEC 27001:2022 w pełnym zakresie (organizacyjne, ludzkie, fizyczne, technologiczne) z mapowaniem na wymagania ustawy o KSC i NIS 2; „Deklaracja stosowania zabezpieczeń".

– Etap 3: szkolenie kadry zarządzającej z obowiązków i odpowiedzialności kierownictwa podmiotu kluczowego (KSC/NIS 2); szkolenia pracowników z dokumentacji SZBI; szkolenia audytorów wewnętrznych; plan (program) audytów wewnętrznych; przeprowadzenie pełnego audytu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (audyt SZBI), obejmującego wszystkie wymagania normy ISO/IEC 27001:2022 oraz zabezpieczenia ujęte w Deklaracji stosowania, zakończonego Raportem z audytu SZBI zawierającym: zakres i kryteria audytu, wykaz ustaleń i niezgodności wraz z ich klasyfikacją, ocenę skuteczności wdrożonych zabezpieczeń oraz rekomendacje doskonalące; przegląd zarządzania z raportem; działania korygujące z planem wdrożenia. Audyt SZBI zostanie przeprowadzony zgodnie z wytycznymi PN-EN ISO 19011, przez członka zespołu Wykonawcy posiadającego certyfikat audytora wiodącego SZBI, który nie brał udziału w opracowywaniu audytowanej dokumentacji – w celu zachowania zasady, że audytor nie ocenia wyników własnej pracy. Wykonawca wskaże tę osobę w wykazie osób z podaniem pełnionej roli.

Szkolenia: w języku polskim, stacjonarnie w siedzibie Zamawiającego lub zdalnie (forma i liczba grup do uzgodnienia); materiały szkoleniowe w wersji elektronicznej z prawem dalszego wykorzystywania wewnętrznego; listy obecności i zaświadczenia dla uczestników; organizacja umożliwiająca udział wszystkich pracowników bez zakłócenia ciągłości pracy przedsiębiorstwa.

3) Zadanie 3 – Kompletna dokumentacja (KSC / NIS 2 / RODO) oraz procedury utrzymania oprogramowania

Wykonawca opracuje kompletną, gotową do zatwierdzenia i stosowania dokumentację (polityki i procedury) wymaganą od podmiotów kluczowych i ważnych, obejmującą co najmniej: zarządzanie aktywami; szacowanie ryzyka; bezpieczeństwo systemu informacyjnego; bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu (w tym testowania); bezpieczeństwo fizyczne i środowiskowe; bezpieczeństwo zasobów ludzkich; bezpieczeństwo i ciągłość łańcucha dostaw ICT; ciągłość działania i plany odtworzeniowe; monitorowanie w trybie ciągłym systemów usług kluczowych; kryptografię; bezpieczeństwo komunikacji; kontrolę dostępu; uwierzytelnianie; zarządzanie incydentami (w tym procedury

zgłaszania incydentów poważnych do CSIRT i powiadamiania odbiorców usług); zarządzanie zagrożeniami i podatnościami; kopie zapasowe i odtwarzanie danych; prowadzenie audytów bezpieczeństwa.

W zakresie przetwarzania danych osobowych – dokumentacja zapewniająca zgodność z RODO i spójność z SZBI: polityka ochrony danych; procedura naruszeń zintegrowana z zarządzaniem incydentami; metodyka i wzory analizy ryzyka dla praw i wolności oraz DPIA ze wskazaniem procesów jej wymagających; zasady relacji z dostawcami (umowy powierzenia, weryfikacja procesorów) w powiązaniu z łańcuchem dostaw; retencja i usuwanie danych; aktualizacja rejestru czynności przetwarzania – o ile audyt wykaże potrzebę.

Procedury utrzymania oprogramowania komercyjnego i open source obejmą co najmniej: inwentaryzację oprogramowania i komponentów open source (właściciele, wersje, środowiska, krytyczność); zarządzanie licencjami komercyjnymi (ewidencja, terminy wsparcia, odnowienia, zgodność); patch management (klasyfikacja poprawek, terminy wdrożeń wg krytyczności, testowanie, okna serwisowe, rollback); monitorowanie podatności (biuletyny producentów, CVE/NVD, komunikaty CSIRT); zasady postępowania z open source (ocena projektu, śledzenie wydań, aktualizacja komponentów, postępowanie przy porzuceniu projektu lub zmianie licencji); zarządzanie końcem wsparcia EOL/EOS z planem migracji lub środkami kompensacyjnymi; zasady instalacji i zarządzania konfiguracją; utrzymanie oprogramowania w środowiskach OT/SCADA z uwzględnieniem ograniczeń aktualizacji systemów przemysłowych. Cała dokumentacja: w języku polskim, dostosowana do struktury i środowiska Zamawiającego (nie dopuszcza się wzorców ogólnych), przekazana w wersji edytowalnej (DOCX) i PDF.

4) Zadanie 4 – Testy penetracyjne infrastruktury sieciowej

Testy zostaną przeprowadzone manualnie i automatycznie, z wykorzystaniem specjalistycznych narzędzi i własnych skryptów, w oparciu o metodykę OSSTMM. Zakres: weryfikacja dokumentacji i topologii sieci; rekonesans (identyfikacja hostów, usług i systemów, dostępność podsieci, wykrycie podatności) powtórzony dla każdej wskazanej sieci; skanowanie najistotniejszych hostów wybranych z Zamawiającym (serwery, kluczowe stacje, kamery, rejestratory) – luki usług, systemów i oprogramowania firm trzecich, weryfikacja haseł i dostępu; sprawdzenie haseł domyślnych (serwery, bramy, przełączniki); możliwość wylistowania użytkowników i zdobycia haseł; dostęp do zasobów współdzielonych; zabezpieczenia urządzeń sieciowych; zdalne testy adresów publicznych. Testy nie mogą zakłócić ciągłości usług kluczowych; testy w segmentach OT/SCADA i testy wpływające na dostępność – każdorazowo uzgadniane co do zakresu, metody i terminu. W ramach wynagrodzenia: jednokrotny retest podatności o ryzyku wysokim i krytycznym (po zgłoszeniu ich usunięcia, nie później niż 3 miesiące od przekazania raportu) z raportem z retestu oraz aktualizacja analizy ryzyka i „Planu postępowania z ryzykiem” o wyniki testów.

5) Zadanie 5 obejmuje:

(a) przeprowadzenie kontrolowanej kampanii socjotechnicznej – co najmniej dwie fale wiadomości phishingowych skierowane do wszystkich użytkowników poczty elektronicznej Zamawiającego, w tym co najmniej jeden scenariusz ukierunkowany na specjalistów pełniących obowiązki w ramach SZBI, oraz co najmniej jedną próbę socjotechniczną kanałem telefonicznym (vishing) – z weryfikacją zgodności reakcji personelu z procedurami wdrożonymi w ramach Zadań 2 i 3; (b) symulowany atak o charakterze edukacyjnym z natychmiastową informacją zwrotną dla użytkowników (moduł budowania świadomości); (c) przygotowanie i przeprowadzenie ćwiczenia symulacyjnego typu table-top (minimum 4 godziny) z zakresu reagowania na incydent i zarządzania kryzysowego, opartego na planach ciągłości działania wdrożonych w ramach Zadania 2, z udziałem kadry zarządzającej i zespołu SZBI. Produkty Zadania 5: raport z kampanii socjotechnicznej (statystyki, ocena reakcji, rekomendacje) oraz raport z ćwiczenia (wnioski i rekomendacje doskonalące).

6) Zadanie 6 (prawo opcji) obejmuje:

wsparcie w pełnieniu funkcji Pełnomocnika ds. SZBI od dnia aktywowania opcji do dnia [30.12.2026 r.], w łącznym wymiarze do 40 godzin, w tym: konsultacje w utrzymaniu i doskonaleniu SZBI, asystę przy przeglądzie zarządczym, aktualizację analizy ryzyka i dokumentacji w związku ze zmianami w infrastrukturze, wsparcie przy obsłudze incydentów i raportowaniu do właściwego CSIRT. Zamawiający może skorzystać z prawa opcji w terminie do 1 miesiąca od odbioru Zadań 2 i 3, nie później jednak niż do dnia [31.10.2026 r.], składając Wykonawcy pisemne oświadczenie; nieskorzystanie z opcji w całości lub części nie rodzi po stronie Wykonawcy żadnych roszczeń.

7) Dokumentacja

Wykonawca przekaże: raport z audytu zgodności (Zadanie 1); komplet dokumentacji SZBI z Deklaracją stosowania i Planem postępowania z ryzykiem, Raport z audytu SZBI oraz raport z przeglądu zarządzania wraz z planem działań korygujących (Zadanie 2); komplet dokumentacji Zadania 3 wraz z procedurami utrzymania oprogramowania; raport z testów penetracyjnych (elementy z podatnościami, klasyfikacja ryzyka wysokie/średnie/niskie, zalecenia dla każdej podatności, zestawienie zbiorcze, ocena poziomu bezpieczeństwa) oraz raport z retestu i zaktualizowaną analizę ryzyka; materiały szkoleniowe, listy obecności i zaświadczenia; wsparcie poaudytowe (odpowiedzi i wyjaśnienia do raportów) przez co najmniej 1 miesiąc od przekazania danego raportu.

V. Termin realizacji zamówienia

Harmonogram prac z uwzględnieniem harmonogramu etapowego określa wykonawca, przy czym pierwszy etap prac musi rozpocząć się nie później niż 14 dni od momentu podpisania umowy. Harmonogram realizacji wszystkich Zadań musi umożliwiać wystawienie faktur i dokonanie płatności w terminie pozwalającym na rozliczenie Projektu grantowego do dnia 15 grudnia 2026 r.

VI. Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają łącznie następujące warunki:

1) w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonali należycie co najmniej dwie usługi o zakresie porównywalnym z przedmiotem zamówienia (audyt bezpieczeństwa lub wdrożenie SZBI wraz z dokumentacją), w tym co najmniej jedną na rzecz podmiotu objętego ustawą o KSC lub operatora infrastruktury wodociągowej/komunalnej;

2) dysponują zespołem łączącym kompetencje audytowe, wdrożeniowe i ofensywne, którego członkowie posiadają certyfikaty co najmniej: Audytor Wiodący SZBI wg ISO/IEC 27001, CISA, CISSP lub CISM (obszar audytu i zarządzania bezpieczeństwem) oraz CEH, OSCP, eWPT lub eWPTX (obszar testów penetracyjnych) – lub certyfikaty równoważne, tj. wydane przez niezależną jednostkę certyfikującą, potwierdzające wiedzę i umiejętności w tym samym obszarze merytorycznym, uzyskiwane po zdaniu egzaminu i aktualne na dzień składania ofert – przy czym ciężar wykazania równoważności spoczywa na Wykonawcy;

3) posiadają wdrożony i certyfikowany system zarządzania bezpieczeństwem informacji (ISO/IEC 27001) oraz system zarządzania jakością (ISO 9001) lub równoważne;

4) posiadają ubezpieczenie odpowiedzialności cywilnej z tytułu prowadzonej działalności, obejmujące usługi stanowiące przedmiot zamówienia (w tym testy penetracyjne), z sumą gwarancyjną nie niższą niż 1 000 000 zł.

Ocena spełniania warunków nastąpi na podstawie dokumentów wskazanych w pkt VIII, na zasadzie spełnia / nie spełnia.

VII. Podstawy wykluczenia

1) Z postępowania wyklucza się Wykonawcę, wobec którego zachodzą okoliczności wskazane 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 2025 r. poz. 514).

2) Z postępowania wyklucza się Wykonawcę powiązanego z Zamawiającym osobowo lub kapitałowo. Przez powiązania osobowe lub kapitałowe 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 przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na: uczestniczeniu w spółce jako wspólnik spółki cywilnej lub osobowej;

posiadaniu co najmniej 10% udziałów lub akcji; 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.

3) Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

VIII. Wymagane dokumenty i oświadczenia

1) Formularz ofertowy – Załącznik nr 1 (oryginał);

2) Oświadczenie o braku podstaw wykluczenia oraz o braku powiązań osobowych i kapitałowych z Zamawiającym – Załącznik nr 2;

3) Wykaz wykonanych usług wraz z dowodami należytego wykonania (referencje lub inne dokumenty) – Załącznik nr 3;

4) Wykaz osób skierowanych do realizacji zamówienia wraz ze wskazaniem posiadanych certyfikatów – Załącznik nr 4; na żądanie Zamawiającego Wykonawca przedłoży kopie certyfikatów;

5) Kopie certyfikatów ISO/IEC 27001 i ISO 9001 Wykonawcy (lub równoważnych);

6) Oświadczenie o posiadaniu ubezpieczenia OC zgodnie z pkt VI ppkt 4; kopię polisy Wykonawca przedłoży najpóźniej przed rozpoczęciem prac;

7) Pełnomocnictwo – jeżeli ofertę podpisuje pełnomocnik; w przypadku Wykonawców wspólnie ubiegających się o zamówienie – dokument ustanawiający pełnomocnika.

IX. Kryteria oceny ofert

Jedynym kryterium oceny ofert jest cena – waga 100%. Punktacja: C = (cena brutto oferty najtańszej / cena brutto oferty badanej) × 100 pkt. Za najkorzystniejszą zostanie uznana oferta z najwyższą liczbą punktów, spełniająca wszystkie wymagania zapytania.

X. Sposób przygotowania i złożenia oferty. Termin składania ofert

1) Ofertę należy złożyć w terminie do dnia [24.08.2026 r.], do godz. [14:00]: elektronicznie (skan podpisanych dokumentów albo dokumenty opatrzone podpisem kwalifikowanym/zaufanym/osobistym) na adres e-mail: cw@spgk.com.pl, w tytule wiadomości

podając znak postępowania; albo pisemnie w sekretariacie Zamawiającego. Oferty złożone po terminie nie będą rozpatrywane.

2) Termin związania ofertą wynosi 30 dni od upływu terminu składania ofert.

3) Oferta niezgodna z postanowieniami niniejszego zapytania podlega odrzuceniu.

4) W przypadku powierzenia części zamówienia podwykonawcy, Wykonawca odpowiada za jego działania i zaniechania jak za własne. Wykonawcy wspólnie ubiegający się o zamówienie ponoszą solidarną odpowiedzialność za wykonanie umowy.

XI. Istotne postanowienia umowy

1) Z wybranym Wykonawcą zostanie zawarta umowa, której wzór stanowi Załącznik nr 5. Umowa obejmie w szczególności: odbiory etapowe poszczególnych Zadań na podstawie protokołów, wynagrodzenie płatne po odbiorze poszczególnych Zadań, kary umowne, przeniesienie majątkowych praw autorskich do dokumentacji (lub licencję w zakresie elementów standardowych) oraz obowiązki wynikające z finansowania zamówienia ze środków KPO – w tym poddanie się kontroli instytucji uprawnionych (CPPC, NASK-PIB i inne podmioty uprawnione), obowiązek przechowywania dokumentacji przez okres wymagany umową o powierzenie grantu oraz obowiązki informacyjno-promocyjne.

2) Przed rozpoczęciem prac Wykonawca zawrze z Zamawiającym umowę o zachowaniu poufności (NDA) oraz – w zakresie dostępu do danych osobowych – umowę powierzenia przetwarzania danych zgodną z art. 28 RODO, według wzorów stanowiących Załączniki nr 7 i 8 do zapytania. 3) Zadanie 6 objęte jest prawem opcji w rozumieniu opisanym w pkt IV ppkt 7; wynagrodzenie za Zadanie 6 przysługuje wyłącznie w przypadku i w zakresie skorzystania z opcji przez Zamawiającego.

XII. Ochrona danych osobowych (RODO)

Administratorem danych osobowych Wykonawców i osób wskazanych w ofertach jest Sanockie Przedsiębiorstwo Gospodarki Komunalnej Sp. z o.o., ul. Jana Pawła II 59, 38-500 Sanok. Kontakt do Inspektora Ochrony Danych: Michał Hassinger, e-mail: cd@spgk.com.pl. Dane przetwarzane są na podstawie art. 6 ust. 1 lit. b i c RODO w celu przeprowadzenia niniejszego postępowania, zawarcia i realizacji umowy oraz rozliczenia i udokumentowania wydatków projektu grantowego współfinansowanego ze środków KPO, a także na podstawie art. 6 ust. 1 lit. f RODO (dochodzenie i obrona roszczeń). Dane będą przechowywane przez okres wynikający z przepisów archiwizacyjnych i podatkowych, nie krócej niż przez okres przechowywania dokumentacji Projektu grantowego wymagany umową o powierzenie grantu. Odbiorcami danych mogą być podmioty uprawnione do kontroli i audytu Projektu (w tym CPPC i NASK-PIB) oraz dostawcy usług działający na zlecenie administratora. Osobom, których dane dotyczą,

przysługuje prawo dostępu do danych, ich sprostowania, ograniczenia przetwarzania oraz wniesienia skargi do Prezesa UODO. Klauzula informacyjna CPPC (jako odrębnego administratora w związku z realizacją Projektów grantowych KPO) stanowi Załącznik nr 6 do zapytania.

XIII. Załączniki

1) Załącznik nr 1 – Formularz ofertowy;
2) Załącznik nr 2 – Oświadczenie o braku podstaw wykluczenia oraz o braku powiązań osobowych i kapitałowych;
3) Załącznik nr 3 – Wykaz wykonanych usług;
4) Załącznik nr 4 – Wykaz osób skierowanych do realizacji zamówienia;
5) Załącznik nr 5 – Wzór umowy;
6) Załącznik nr 6 – Klauzula informacyjna KPO (CPPC);
7) Załącznik nr 7 – Wzór umowy o zachowaniu poufności (NDA);
8) Załącznik nr 8 – Wzór umowy powierzenia przetwarzania danych osobowych;

Zatwierdzam: _____

Załącznik nr 1 do Zapytania ofertowego

FORMULARZ OFERTOWY

Wykonawca (nazwa, adres, NIP, REGON/KRS):
……

Tel.: …… E-mail:
……

W odpowiedzi na zapytanie ofertowe znak FDI.261.3.2026 oferujemy wykonanie przedmiotu zamówienia zgodnie z wymaganiami zapytania i OPZ, za łączną cenę:

Cena netto: …… zł, podatek VAT: …… zł, cena brutto: …… zł (słownie brutto: ……),

w tym: Zadanie 1-5 .....; Zadanie 6 (prawo opcji – wsparcie Pełnomocnika ds. SZBI, do [30.12.2026 r.], do 40 godzin): …… zł brutto.

1) Oświadczamy, że zapoznaliśmy się z treścią zapytania ofertowego wraz z załącznikami, w tym z opisem przedmiotu zamówienia i wzorem umowy, przyjmujemy je bez zastrzeżeń i zobowiązujemy się do zawarcia umowy w terminie i miejscu wskazanym przez Zamawiającego.
2) Oświadczamy, że cena oferty obejmuje wszystkie koszty prawidłowego wykonania zamówienia, w tym retest podatności i wsparcie poaudytowe.
3) Oświadczamy, że jesteśmy związani ofertą przez 30 dni od upływu terminu składania ofert.
4) Zamówienie zrealizujemy w terminach określonych w zapytaniu ofertowym.
5) Podwykonawcom zamierzamy powierzyć następujący zakres: …… (jeżeli dotyczy).
6) Oświadczamy, że wypełniliśmy obowiązki informacyjne z art. 13 lub 14 RODO wobec osób fizycznych, których dane przekazujemy w ofercie.

…… ……

(miejscowość, data) *(podpis osoby/osób uprawnionych)*

Załącznik nr 2 do Zapytania ofertowego

OŚWIADCZENIE WYKONAWCY

o braku podstaw wykluczenia oraz o braku powiązań osobowych i kapitałowych

Wykonawca (nazwa, adres, NIP):
……

Składając ofertę w postępowaniu znak FDI.261.3.2026 oświadczam/y, że:

1) nie podlegam/y wykluczeniu z postępowania na podstawie 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 2025 r. poz. 514);
2) nie jestem/eśmy powiązany/i z Zamawiającym osobowo ani kapitałowo w rozumieniu pkt VII ppkt 2 zapytania ofertowego;
3) wszystkie informacje podane w ofercie i załączonych dokumentach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd.

…… ……

(miejscowość, data) *(podpis osoby/osób uprawnionych)*

Załącznik nr 3 do Zapytania ofertowego

WYKAZ WYKONANYCH USŁUG

Lp.	Przedmiot usługi (zakres)	Odbiorca (w tym: podmiot KSC / operator wod.-kan.)	Termin realizacji	Wartość brutto
1				
2				
3				

Do wykazu załączamy dowody należytego wykonania usług (referencje lub inne dokumenty).

…… ……

(miejscowość, data) *(podpis osoby/osób uprawnionych)*

Załącznik nr 4 do Zapytania ofertowego

WYKAZ OSÓB SKIEROWANYCH DO REALIZACJI ZAMÓWIENIA

Lp.	Imię i nazwisko	Rola w zespole (audyt / wdrożenie / testy)	Posiadane certyfikaty (nazwa, nr, ważność)	Podstawa dysponowania
1				
2				
3				
4				

Oświadczamy, że wskazane osoby posiadają certyfikaty wymagane w pkt VI ppkt 2 zapytania (lub równoważne) i będą uczestniczyć w realizacji zamówienia; kopie certyfikatów przedłożymy na żądanie Zamawiającego.

…… ……

(miejscowość, data) *(podpis osoby/osób uprawnionych)*