



Przedsiębiorstwo Energetyki Ciepłej – Gliwice
Spółka z ograniczoną odpowiedzialnością
ul. Królewskiej Tamy 135; 44 – 100 Gliwice
tel.: 32/3350105, 3350106
www.pec.gliwice.pl, office@pec.gliwice.pl

Numer postępowania DZ/2/70/2025

Numer sprawy 000505/25

PRZETARG

w trybie negocjacji z publikacją ogłoszenia

na zadanie

Świadczenie usług nadzoru bezpieczeństwa informatycznego

WARUNKI ZAMÓWIENIA

*Postępowanie prowadzone zgodnie z Regulaminem PEC - Gliwice Sp. z o. o.
udzielania zamówień nie objętych ustawą o zamówieniach publicznych.*

MAJ 2025 r.

KLUZULA INFORMACYJNA (KONTRAHENCI OSOBY, KTÓRYMI KONTRAHENT SIĘ POSŁUGUJE)

Na podstawie 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 (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1.), zwanego dalej Rodo informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest PEC – Gliwice Sp. z o.o. z siedzibą w Gliwicach przy ul. Królewskiej Tamy 135, nr KRS 0000061254, Nr NIP 631-01-00-822, Nr Regon 272857793, e-mail: office@pec.gliwice.pl, tel. 32 3350 105 (zwany dalej Administratorem lub Spółką).
2. Może się Pan/Pani skontaktować z Inspektorem ochrony danych osobowych za pośrednictwem poczty elektronicznej: iodo@pec.gliwice.pl
3. Podanie przez Panią/Pana danych osobowych jest dobrowolne. Jednak podanie danych jest niezbędne do zrealizowania celów określonych poniżej w pkt 6.
4. Pana/Pani dane zostały udostępnione spółce przez naszego kontrahenta, którego reprezentujesz/ jesteś pracownikiem/współpracownikiem lub pozyskane z rejestrów publicznych (np. rejestry przedsiębiorców, sądowe KRS/CEIDG) w związku ze złożeniem przez kontrahenta oferty w ramach prowadzonej przez niego działalności.
5. Będziemy przetwarzali następujące kategorie Pana/Pani danych osobowych:
 - a) w przypadku osób reprezentujących: imię/imiiona i nazwisko, numer PESEL, funkcja w organie reprezentującym, stanowisko, adres poczty elektronicznej, numer telefonu,
 - b) w przypadku pozostałych osób: imię/imiiona i nazwisko, adres poczty elektronicznej, numer telefonu, stanowisko,
 - c) inne dane zawarte w udostępnionych nam przez kontrahenta dokumentach (np. świadectwach posiadania określonych uprawnień).
6. Spółka będzie przetwarzać Pana/Pani dane osobowe, gdyż jest to niezbędne do celów wynikających z:
 - 1) prawnie uzasadnionych interesów realizowanych przez spółkę lub stronę trzecią (art. 6 ust. 1 lit. f RODO),
 - 2) wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO);– za które Administrator uznaje rozpatrzenie i przetworzenie oferty złożonej przez kontrahenta, zapobieganie oszustwom, stosowanie procesów nadzoru zgodności z prawem, a ponadto ustalanie, dochodzenie i obronę przed roszczeniami.
7. Odbiorcami Pana/Pani danych osobowych mogą być podmioty, które świadczą na rzecz spółki usługi, w tym m.in. usługi IT, doradcze, księgowe, audytowe, informatyczne, wysyłkowe, platnicze, archiwizacyjne i niszczenia dokumentów oraz biegli rewidenci i notariusze, a także właściwe organy uprawnione do otrzymania Twoich danych na podstawie przepisów prawa.
8. Pana/Pani dane osobowe przechowywane do upływu przedawnienia roszczeń. Po tych okresach dane będą przechowywane jedynie przez czas wymagany przepisami prawa.
9. Ma Pan/Pani prawo do żądania od spółkę dostępu do Twoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także przenoszenia danych.
10. Nie przysługuje Pani/Panu:
 - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.
11. Ma Pan/Pani prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Wzór oświadczenia wymaganego od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO

Oświadczam, że wypełniłem określone w art. 13 lub art. 14 rozp. RODO obowiązki informacyjne wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu złożenia oferty (uwaga: sprecyzować, o jaką ofertę chodzi ; podać nr i nazwę postępowania)

1. PRZEDMIOT ZAMÓWIENIA – PROCEDURA WYBORU NAJKORZYSTNIEJSZEJ OFERTY

Przedsiębiorstwo Energetyki Ciepłej - Gliwice Sp. z o.o. ogłasza postępowanie przetargowe na świadczenie usług nadzoru bezpieczeństwa informatycznego.

Celem Zamawiającego jest wybranie oferty najkorzystniejszej pod względem funkcjonalnym i kosztowym.

ETAP nr I

Składanie wniosków o dopuszczenie do udziału w postępowaniu w formie oferty wstępnej. Zamawiający zaprosi do udziału w kolejnym etapie (negocjacjach) wszystkich oferentów spełniających wymogi niniejszych Warunków Zamówienia.

ETAP nr II

Doprecyzowanie warunków realizacji usługi oraz negocjacje cenowe z zaproszonymi oferentami i złożenie ostatecznej oferty.

2. OPIS PRZEDMIOTU ZAMÓWIENIA.

Przedmiotem Zamówienia jest świadczenie usługi nadzoru bezpieczeństwa informatycznego (ang. MSS – Managed Security Services) w formule zdalnego dyżuru Centrum Nadzoru Bezpieczeństwa, zwanego dalej SOC (ang. Security Operations Center) wraz z usługą audytu cyberbezpieczeństwa zgodnie z wymaganiami ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 z późn. zm.) oraz z uwzględnieniem wymagań norm ISO/IEC 27001:2022 i ISO 22301:2019.

Zamawiający oczekuje realizacji SOC jako usługi obejmującej całość instytucji w sposób kompleksowy, zgodnie z wytycznymi aktów prawnych obowiązujących w dniu zawarcia umowy, w szczególności Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 1560), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 2016 Nr 119, str. 1., ze zm.). Zamawiający informuje jednocześnie, iż w chwili złożenia zamówienia nie posiada kompletnej dokumentacji związanej z analizą ryzyka teleinformatycznego, ani kompletu wytycznych Polityki Bezpieczeństwa, a co za tym idzie oczekuje od Wykonawcy, w początkowej fazie realizacji zadania, usług związanych z doradztwem i konsultacją pod kątem ogólnie przyjętych dobrych praktyk sztuk telekomunikacyjnej z zakresu bezpieczeństwa informacji, w celu zaprojektowania i wdrożenia rozwiązań technicznych pozwalających na skuteczny nadzór i zarządzanie bezpieczeństwem informatycznym, ze szczególnym naciskiem związanym z wymaganiami specyficznymi dla branży energetyki ciepłej.

Celem niniejszego zamówienia jest uruchomienie, wdrożenie, a następnie utrzymanie stałego monitoringu infrastruktury IT oraz OT Zamawiającego, identyfikacja i raportowanie występujących w jej obszarze zagrożeń, detekcja obsługa incydentów, a także ciągłe, cykliczne dostarczanie rekomendacji dotyczących poprawy stanu bezpieczeństwa, w tym również w związku z usługą audytu cyberbezpieczeństwa, którego szczegółowy zakres zostanie doprecyzowany na etapie negocjacji. Usługa świadczona przez Wykonawcę powinna pozwolić Zamawiającemu na zachowanie wysokiego poziomu odporności użytkowanych systemów cyfrowych na obecne w przestrzeni technicznej zagrożenia, przy uniknięciu konieczności tworzenia i utrzymywania własnego, wewnętrznego zespołu odpowiedzialnego za bezpieczeństwo IT oraz OT.

Przeprowadzenie audytu cyberbezpieczeństwa ma na celu ocenę stanu zabezpieczeń, identyfikację zagrożeń i luk oraz rekomendację działań mogących poprawić poziom bezpieczeństwa.

Szczegółowy opis usługi zawarto w dokumencie *Szczegółowy opis przedmiotu zamówienia* będący załącznikiem do niniejszych Warunków Zamówienia.

3. TERMINY REALIZACJI ZAMÓWIENIA

Uruchomienie usługi – w czasie zadeklarowanym przez usługodawcę, maksymalnie do 90 dni od zawarcia umowy.

4. WARUNKI UCZESTNICTWA W PRZETARGU.

1. O zamówienie mogą ubiegać się oferenci, którzy:

- a) posiadają uprawnienia niezbędne do wykonywania określonej działalności lub czynności,
- b) posiadają niezbędną wiedzę i doświadczenie, a także dysponują potencjałem technicznym oraz pracownikami zdolnymi do wykonania danego zamówienia lub przedstawia pisemne zobowiązanie innych podmiotów do udostępniania potencjału technicznego i osób zdolnych do wykonania zamówieniu,
- c) znajdują się w sytuacji finansowej zapewniającej wykonanie zamówienia,
- d) nie otwarto wobec nich likwidacji ani nie ogłoszono upadłości,
- e) nie wyrządzili szkody w ostatnich 3 latach przed wszczęciem postępowania poprzez niewykonanie lub nienależyte wykonanie zamówienia,
- f) nie zostali prawomocnie skazani za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przeciwko środowisku, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo

- związku mających na celu popełnienie przestępstwa,
- g) nie zalegają z uiszczeniem podatków, opłat oraz składek na ubezpieczenie społeczne i zdrowotne.

2. W ramach powyższych wymogów zamawiający ustala następujące szczegółowe warunki udziału w postępowaniu:

- w zakresie warunku wskazanego w punkcie 4.1) b) wymagane jest:
- udokumentowana realizacja projektów cyberbezpieczeństwa dla instytucji publicznych,
- udokumentowane kompetencje w zakresie SOC, SIEM, analizy zagrożeń,
- doświadczenie w prowadzeniu audytów bezpieczeństwa informacji,
- udokumentowane kompetencje twarde związane z obsługą infrastruktury sieciowej, telefonii VoIP oraz infrastruktury serwerowej,
- potwierdzone minimum 3 letnie doświadczenie w zakresie monitorowania i zarządzania infrastrukturą teleinformatyczną Jednostek z obszaru Administracji Publicznej,
- oferent powinien wykazać ważną certyfikację usług cyberbezpieczeństwa w zakresie ISO/IEC 27001:2022 i ISO/IEC 22301:2019 wykonaną przez jednostkę certyfikującą akredytowaną w Polskim Centrum Akredytacji lub równoważną jednostkę na terenie UE;

Szczegółowe wymagania dotyczące oferenta oraz personelu sprawującego usługę SOC zawarto w dokumencie *Szczegółowy opis przedmiotu zamówienia*.

5. SPOSÓB PRZYGOTOWANIA OFERT

Każdy oferent składa w przetargu tylko jedną ofertę, przygotowaną zgodnie z niniejszymi warunkami, za pośrednictwem platformy zakupowej www.platformazakupowa.pl.

Kilka podmiotów może złożyć ofertę wspólną, w tym przypadku podmioty te ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania.

Ofertę składa się w jednym egzemplarzu. Oferta musi być sporządzona w języku polskim.

W przypadku, kiedy ofertę składa kilka podmiotów wspólnie, do oferty powinno zostać dołączone pełnomocnictwo dla osoby uprawnionej do reprezentowania członków konsorcjum w trakcie postępowania.

Oferowana cena jest ceną do porównania ofert. Zakłada się zawarcie umowy na okres trzech lat z możliwością przedłużenia.

Oferent podaje cenę netto świadczenia usług:

- nadzoru bezpieczeństwa informatycznego (usługa SOC) w skali jednego miesiąca,
- audytu cyberbezpieczeństwa w skali jednej roboczogodziny.

Przy fakturowaniu do ceny netto doliczony zostanie podatek od towarów i usług, zgodnie z obowiązującymi przepisami w dniu wystawienia faktury VAT.

Wykonawca, który złoży najkorzystniejszą ofertę, poprzez platformę zakupową, jest zobowiązany do dostarczenia Zamawiającemu pisemną formę oferty opatrzoną podpisem upoważnionej/upoważnionych osoby/osób. Niedostarczenie oryginalnych dokumentów skutkować będzie uznaniem, przez Zamawiającego, iż Wykonawca odmówił podpisania umowy. Wyjątek stanowią dokumenty opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub osobistym, które są dokumentami oryginalnymi, w związku z czym Zamawiający nie wymaga dostarczenia formy papierowej dokumentów.

Zaleca się aby Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia posiadał konto na platformie zakupowej. W celu założenia konta należy postępować zgodnie z instrukcją jak niżej https://platformazakupowa.pl/pn/pec_gliwice/supplier

Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych opisane są w **Instrukcji dla Wykonawców**.

Przy składaniu ofert elektronicznych zastosowanie ma **Regulamin Internetowej Platformy zakupowej Open Nexus Sp. z o.o**

6. ZAWARTOŚĆ OFERTY WSTĘPNEJ

- 1) wypełniony i podpisany wniosek – Zał. nr 1,
- 2) oferta cenowa (cena netto świadczenia usług nadzoru bezpieczeństwa informatycznego w skali jednego miesiąca),
- 3) pełnomocnictwa osób podpisujących ofertę do podejmowania zobowiązań w imieniu firmy (w przypadku podpisania oferty przez osoby nieumocowane do składania oświadczeń woli),
- 4) propozycja wzoru umowy Wykonawcy zawierająca wstępny harmonogram prac oraz ich zakres.
- 5) dokumenty potwierdzające doświadczenie zawodowe zgodnie z wymogami pkt 4 oraz *Szczegółowego opisu przedmiotu zamówienia*

7. MIEJSCE I TERMIN SKŁADANIA OFERT WSTĘPNYCH

Oferty należy składać do dnia **13 czerwca 2025 r. do godz. 11:00** za pośrednictwem platformy zakupowej www.platformazakupowa.pl Otwarcie ofert niejawne.

8. OKRES WAŻNOŚCI OFERTY.

Okres ważności oferty - 30 dni od daty złożenia oferty ostatecznej.

9. UDZIELANIE WYJAŚNIEŃ.

W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Oferentem odbywa się przy użyciu platformy zakupowej. Zamawiający odpowie na pytania które wpłyną nie później niż 4 dni przed terminem składania ofert.

Osobami ze strony zamawiającego upoważnionymi do kontaktowania się z oferentami są:

- Mariusz Migda - tel. 32 335 0230 (w zakresie merytorycznym),
- Przemysła Galicki - tel. 32 335 0149 (w zakresie merytorycznym),
- Renata Uramowska-Słusznik - tel. 32 33 50 104 w zakresie formalnym).

10. KRYTERIA I SPOSÓB OCENY OFERT.

Ocena ofert zostanie dokonana w oparciu o następujące kryterium:

Cena (netto) - 100 %

przeliczana wg wzoru:
$$C = \frac{\text{cena oferty najkorzystniejszej / najtańszej}}{\text{cena kolejnej oferty}} \times 100 \text{ pkt.}$$

Zamawiający odrzuci ofertę, jeżeli:

- 1) jest sprzeczna z istotnymi warunkami zamówienia,
- 2) jej złożenie stanowi czyn nieuczciwej konkurencji,
- 3) jest nieważna na podstawie odrębnych przepisów.

Z tytułu odrzucenia ofert oferentom nie przysługują żadne roszczenia przeciwko zamawiającemu.

11. INFORMACJA O WSZELKICH FORMALNOŚCIACH JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO ZAKOŃCZENIU PRZETARGU W CELU ZAWARCIA UMOWY.

1. Niezwłocznie po wyborze oferty Zamawiający powiadomi Oferentów o wyniku postępowania oraz zamieści informację na stronie prowadzonego postępowania.
2. Zamawiający zawiera umowę z Oferentem, który przedstawił ofertę najkorzystniejszą w świetle niniejszych warunków zamówienia i przeprowadzonych negocjacji.
3. Zawarcie umowy nastąpi po uzyskaniu informacji o wyniku postępowania, w terminie ważności oferty.

12. POZOSTAŁE INFORMACJE.

Do niniejszego postępowania nie mają zastosowania przepisy ustawy „prawo zamówień publicznych”, w tym nie przysługuje prawo do protestów i odwołań w jej rozumieniu.

Zamawiający zastrzega sobie prawo zakończenia negocjacji w każdym momencie, bez podawania przyczyny.

Zamawiający zastrzega sobie prawo do swobodnej modyfikacji warunków zamówienia na każdym etapie procedury prowadzącej do wyboru zleceniobiorcy oraz do swobodnej modyfikacji procedury negocjacji na każdym etapie.

Załączniki:

1. Wniosek o dopuszczenie do udziału w postępowaniu.

Zatwierdzam:

Uzgodnienia branżowe :

Budowlano-architektoniczne	Technologiczne	Elektryczne	AKPiA	Informatyczne	Ochrona Środowiska	BHP
Nie dotyczy	Nie dotyczy	Nie dotyczy		Nie dotyczy	Nie dotyczy	Nie dotyczy