

515394-2026 - Competition

Poland – Computer equipment and supplies – Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach. Część II - Obszar kompetencyjny oraz obszar techniczny IT.

OJ S 141/2026 24/07/2026

Contract or concession notice – standard regime - Change notice

Supplies - Services

1. Buyer

1.1. Buyer

Official name: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Email: sekretariat@pksiemiaticze.pl

Legal type of the buyer: Body governed by public law, controlled by a local authority

Activity of the contracting authority: General public services

2. Procedure

2.1. Procedure

Title: Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach. Część II - Obszar kompetencyjny oraz obszar techniczny IT.

Description: 1. Przedmiot zamówienia jest finansowany ze środków Programu Krajowy Plan Odbudowy i Zwiększania Odporności, Priorytet: C3 Cyberbezpieczeństwo. Działanie: C3.1.1. Cyberbezpieczeństwo – CyberPL. 2. Projekt ma na celu wzmocnienie cyberodporności poprzez modernizację infrastruktury oraz rozwój kompetencji zespołów. W ramach projektu zrealizowane zostaną działania: 1) Modernizacja infrastruktury sieciowej: Wdrożenie segmentacji i mikrosegmentacji sieci IT/OT, co umożliwi izolację newralgicznych systemów i minimalizację potencjalnych szkód w przypadku ataku. Zostanie również wdrożony system monitorowania ruchu sieciowego (IDS/IPS). Umożliwi on gromadzenie logów systemowych i dowodów cyfrowych niezbędnych do analizy incydentów. 2) Wdrożenie bezpiecznych zdalnych dostępów: Wprowadzenie scentralizowanego i bezpiecznego systemu zdalnego dostępu, który pozwoli na kontrolę i audytowanie połączeń z sieciami OT/IT. 3) Zapewnienie ciągłości działania: Zostanie wdrożony system do tworzenia i zarządzania kopiami zapasowymi, w tym również dla systemów sterowania, co zapewni szybki powrót do sprawności w przypadku incydentu. 3. Projekt jest zgodny z priorytetami KPO i Zwiększania Odporności, a w szczególności z celem Transformacji Cyfrowej. Inwestycja w nowoczesne technologie cyberbezpieczeństwa jest kluczowym elementem w dążeniu do stworzenia bezpiecznej infrastruktury krytycznej, zapewniającej ciągłość świadczenia usług publicznych. 4. Wdrożenie Części II projektu (Obszar kompetencyjny oraz obszar techniczny IT) polega na realizacji zadań: 1) Zadanie 1. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT /OT/ICS. 2) Zadanie 2. Oprogramowanie do badania podatności. 3) Zadanie 3. Oprogramowanie do ochrony przed ransomware. 4) Zadanie 4. Oprogramowanie typu EDR (Endpoint Detection and Response). 5) Zadanie 5. Urządzenie i oprogramowanie typu NDR z HoneyPot i monitorem sytuacyjnym (Network Detection & Response). 6) Zadanie 6. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to

również rozwiązań typu open source IT/ICS/IloT. 7) Zadanie 7. System typu UTM dla sieci IT HA Przedmiot zamówienia. 8) Zadanie 8. Usługi konfiguracji i hardeningu systemów/urządzeń IT. 9) Zadanie 9. Stacja robocza fizyczna z rolą stacji przesiadkowej (broker sesji) + dwa monitory 27 cali - 1 komplet. 10) Zadanie 10. Usługa segmentacji sieci. 11) Zadanie 11. Serwer do wykonywania kopii zapasowych (NAS). 12) Zadanie 12. Zarządzalny switch L2, 48p GE PoE + 4x SFP+ (2 szt.). 13) Zadanie 13. Zarządzalny switch L2, 16p GE + 2x SFP (6 szt.). 14) Zadanie 14. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise. 15) Zadanie 15. Oprogramowanie typu ITSM (Information Technology Service Management). 16) Zadanie 16. Oprogramowanie typu MDM (Mobile Device Management) Przedmiot zamówienia. 17) Zadanie 17. Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention). 18) Zadanie 18. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IloT. 19) Zadanie 19. Oprogramowanie do zarządzania tożsamością i dostępem. 20) Zadanie 20. Oprogramowanie lub urządzenie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie). 21) Zadanie 21. Klucze sprzętowe U2F. 22) Zadanie 22. Usługa inwentaryzacji aktywów teleinformatycznych OT/ICS/IloT. 23) Zadanie 23. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 24) Zadanie 24. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 25) Zadanie 25. Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT. Oprogramowanie zintegrowany System bezpieczeństwa-Industrial Central Management dla OT, Anomaly Detection, Threat Detection, Data Traceability Control, Anti DDOS, APT (Advanced Persistent Threat), SIEM, SOAR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT. 26) Zadanie 26. UTM (Unified Threat Management) Platforma sprzętowa DIN35 lub desktop - System bezpieczeństwa IPS/IDS, IT/OTAnomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat), AI MGMT, ZBFW. 27) Zadanie 27. Usługa Private APN. 28) Zadanie 28. Usługa inwentaryzacji aktywów teleinformatycznych IT. 29) Zadanie 29. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doбором urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT/ICS/IloT. 30) Zadanie 30. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IloT. 31) Zadanie 31. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IloT. 32) Zadanie 32. Usługi konfiguracji i hardeningu systemów/urządzeń OT/ICS/IloT. 5. Opis przedmiotu zamówienia wraz z określeniem minimalnych wymagań został przedstawiony w Załączniku nr 2 do SWZ – Szczegółowy Opis Przedmiotu Zamówienia (SOPZ).

Procedure identifier: 1ed3396f-1a0a-46ea-a0c4-ff893173fa76

Internal identifier: ZWiK.4500.2.5.2025

Type of procedure: Open

The procedure is accelerated: no

2.1.1. Purpose

Main nature of the contract: Supplies

Additional nature of the contract: Services

Main classification (cpv): 30200000 Computer equipment and supplies

Additional classification (cpv): 32420000 Network equipment, 32422000 Network components, 35100000 Emergency and security equipment, 35121000 Security equipment, 48000000 Software package and information systems, 48210000 Networking software package, 48600000 Database and operating software package, 48730000 Security software package, 48732000 Data security software package, 48820000 Servers, 48821000 Network servers, 48900000 Miscellaneous software package and computer systems, 51611100 Hardware installation services, 72222000 Information systems or technology strategic review and

planning services, 72263000 Software implementation services, 72265000 Software configuration services, 72315000 Data network management and support services, 72600000 Computer support and consultancy services, 73431000 Test and evaluation of security equipment, 79212000 Auditing services, 79417000 Safety consultancy services, 80510000 Specialist training services, 80533100 Computer training services, 80550000 Safety training services

2.1.2. Place of performance

Town: Siemiatycze
Postcode: 17-300
Country subdivision (NUTS): Łomżyński (PL842)
Country: Poland

2.1.4. General information

Legal basis:

Directive 2014/24/EU

2.1.6. Grounds for exclusion

Sources of grounds for exclusion: Notice

Direct or indirect involvement in the preparation of this procurement procedure: Dotyczy art. 108 ust. 1 pkt 6 ustawy Pzp.

Corruption: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

Fraud: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

Breaching of obligations in the fields of labour law: Dotyczy art. 108 ust. 1 pkt 1 lit. h i pkt 2 ustawy Pzp.

Breaching obligation relating to payment of social security contributions: Dotyczy art. 108 ust. 1 pkt 3 ustawy Pzp.

Breaching obligation relating to payment of taxes: Dotyczy art. 108 ust. 1 pkt 3 ustawy Pzp.

Purely national exclusion grounds: Dotyczy art. 108 ust. 1 pkt 1 ustawy Pzp. Dotyczy art. 108 ust. 1 pkt 4 ustawy Pzp. Dotyczy art. 108 ust. 2 ustawy Pzp.

Agreements with other economic operators aimed at distorting competition: Dotyczy art. 108 ust. 1 pkt 5 ustawy Pzp.

Child labour and including other forms of trafficking in human beings: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

Money laundering or terrorist financing: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

Terrorist offences or offences linked to terrorist activities: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

Participation in a criminal organisation: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

5. Lot

5.1. Lot: LOT-0001

Title: Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu. Część II - Obszar kompetencyjny oraz obszar techniczny IT

Description: 1. Przedmiot zamówienia jest finansowany ze środków Programu Krajowy Plan Odbudowy i Zwiększania Odporności, Priorytet: C3 Cyberbezpieczeństwo. Działanie: C3.1.1. Cyberbezpieczeństwo – CyberPL. 2. Projekt ma na celu wzmocnienie cyberodporności poprzez modernizację infrastruktury oraz rozwój kompetencji zespołów. W ramach projektu zrealizowane zostaną działania: 1) Modernizacja infrastruktury sieciowej: Wdrożenie

segmentacji i mikrosegmentacji sieci IT/OT, co umożliwi izolację newralgicznych systemów i minimalizację potencjalnych szkód w przypadku ataku. Zostanie również wdrożony system monitorowania ruchu sieciowego (IDS/IPS). Umożliwi on gromadzenie logów systemowych i dowodów cyfrowych niezbędnych do analizy incydentów. 2) Wdrożenie bezpiecznych zdalnych dostępu: Wprowadzenie scentralizowanego i bezpiecznego systemu zdalnego dostępu, który pozwoli na kontrolę i audytowanie połączeń z sieciami OT/IT. 3) Zapewnienie ciągłości działania: Zostanie wdrożony system do tworzenia i zarządzania kopiami zapasowymi, w tym również dla systemów sterowania, co zapewni szybki powrót do sprawności w przypadku incydentu. 3. Projekt jest zgodny z priorytetami KPO i Zwiększania Odporności, a w szczególności z celem Transformacji Cyfrowej. Inwestycja w nowoczesne technologie cyberbezpieczeństwa jest kluczowym elementem w dążeniu do stworzenia bezpiecznej infrastruktury krytycznej, zapewniającej ciągłość świadczenia usług publicznych. 4. Wdrożenie Części II projektu (Obszar kompetencyjny oraz obszar techniczny IT)polega na realizacji zadań: 1) Zadanie 1. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT /OT/ICS. 2) Zadanie 2. Oprogramowanie do badania podatności. 3) Zadanie 3. Oprogramowanie do ochrony przed ransomware. 4) Zadanie 4. Oprogramowanie typu EDR (Endpoint Detection and Response). 5) Zadanie 5. Urządzenie i oprogramowanie typu NDR z HoneyPot i monitorem sytuacyjnym (Network Detection & Response). 6) Zadanie 6. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/ICS/IloT. 7) Zadanie 7. System typu UTM dla sieci IT HA Przedmiot zamówienia. 8) Zadanie 8. Usługi konfiguracji i hardeningu systemów/urządzeń IT. 9) Zadanie 9. Stacja robocza fizyczna z rolą stacji przesiadkowej (broker sesji) + dwa monitory 27 cali - 1 komplet. 10) Zadanie 10. Usługa segmentacji sieci . 11) Zadanie 11. Serwer do wykonywania kopii zapasowych (NAS). 12) Zadanie 12. Zarządzalny switch L2, 48p GE PoE + 4× SFP+ (2 szt.). 13) Zadanie 13. Zarządzalny switch L2, 16p GE + 2× SFP (6 szt.). 14) Zadanie 14. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise. 15) Zadanie 15. Oprogramowanie typu ITSM (Information Technology Service Management). 16) Zadanie 16. Oprogramowanie typu MDM (Mobile Device Management) Przedmiot zamówienia. 17) Zadanie 17. Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention). 18) Zadanie 18. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IloT. 19) Zadanie 19. Oprogramowanie do zarządzania tożsamością i dostępem. 20) Zadanie 20. Oprogramowanie lub urządzenie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie). 21) Zadanie 21. Klucze sprzętowe U2F. 22) Zadanie 22. Usługa inwentaryzacji aktywów teleinformatycznych OT/ICS/IloT. 23) Zadanie 23. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 24) Zadanie 24. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 25) Zadanie 25. Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT. Oprogramowanie zintegrowany System bezpieczeństwa-Industrial Central Management dla OT, Anomaly Detection, Threat Detection, Data Traceability Control, Anti DDOS, APT (Advanced Persistent Threat), SIEM, SOAR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT. 26) Zadanie 26. UTM (Unified Threat Management) Platforma sprzętowa DIN35 lub desktop - System bezpieczeństwa IPS/IDS, IT/OTAnomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat), AI MGMT, ZBFW. 27) Zadanie 27. Usługa Private APN. 28) Zadanie 28. Usługa inwentaryzacji aktywów teleinformatycznych IT. 29) Zadanie 29. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doбором urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT /ICS/IloT. 30) Zadanie 30. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu

bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/Ilo. 31) Zadanie 31. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IloT. 32) Zadanie 32. Usługi konfiguracji i hardeningu systemów/urządzeń OT/ICS/IloT. 5. Opis przedmiotu zamówienia wraz z określeniem minimalnych wymagań został przedstawiony w Załączniku nr 2 do SWZ – Szczegółowy Opis Przedmiotu Zamówienia (SOPZ).

Internal identifier: ZWiK.4500.2.5.2025

5.1.1. Purpose

Main nature of the contract: Supplies

Additional nature of the contract: Services

Main classification (cpv): 30200000 Computer equipment and supplies

Additional classification (cpv): 32420000 Network equipment, 32422000 Network components, 35100000 Emergency and security equipment, 35121000 Security equipment, 48000000 Software package and information systems, 48210000 Networking software package, 48600000 Database and operating software package, 48730000 Security software package, 48732000 Data security software package, 48820000 Servers, 48821000 Network servers, 48900000 Miscellaneous software package and computer systems, 51611100 Hardware installation services, 72222000 Information systems or technology strategic review and planning services, 72263000 Software implementation services, 72265000 Software configuration services, 72315000 Data network management and support services, 72600000 Computer support and consultancy services, 73431000 Test and evaluation of security equipment, 79212000 Auditing services, 79417000 Safety consultancy services, 80533100 Computer training services, 80510000 Specialist training services, 80550000 Safety training services

5.1.2. Place of performance

Town: Siemiatycze

Postcode: 17-300

Country subdivision (NUTS): Łomżyński (PL842)

Country: Poland

5.1.3. Estimated duration

Start date: 14/09/2026

Duration end date: 10/12/2026

5.1.6. General information

Reserved participation:

Participation is not reserved.

The names and professional qualifications of the staff assigned to perform the contract must be given: Not required

Procurement Project fully or partially financed with EU Funds.

Information about European Union funds:

Identifier of EU funds: Program Krajowy Plan Odbudowy i Zwiększania Odporności.

Further details of EU funds: Priorytet: C3 Cyberbezpieczeństwo. Działanie: C3.1.1.

Cyberbezpieczeństwo – CyberPL Konkurs grantowy pn. „Cyberbezpieczne Wodociągi” o numerze KPOD.05.10-CW.01-001/25 Tytuł projektu: Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu.

The procurement is covered by the Government Procurement Agreement (GPA): no

This procurement is also suitable for small and medium-sized enterprises (SMEs): yes

5.1.9. Selection criteria

Sources of selection criteria: Notice

Criterion: Professional risk indemnity insurance

Description of selection criterion: Wykonawca powinien wykazać, że posiada ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia (w szczególności ryzyk cybernetycznych) na sumę gwarancyjną nie mniejszą niż 300 000 zł (słownie: trzysta tysięcy złotych). Wykonawca obowiązany jest utrzymać ważność ubezpieczenia przez cały okres realizacji Umowy.

Criterion: Relevant educational and professional qualifications

Description of selection criterion: Wykonawca powinien wskazać co najmniej dwie osoby zatrudnione przez Wykonawcę – specjalistów odpowiedzialnych za wdrożenia rozwiązań objętych niniejszym przedmiotem zamówienia, posiadających niezbędną wiedzę i doświadczenie potwierdzone co najmniej 4-letnim stażem pracy związanym z wdrożeniami systemów cyberbezpieczeństwa oraz wykształceniem wyższym na kierunku informatycznym, oraz z ważnymi certyfikatami oferowanych rozwiązań z cyberbezpieczeństwa IT oraz OT na poziomie Professional.

Criterion: References on specified deliveries

Description of selection criterion: Wykonawca powinien wykazać, że w okresie ostatnich trzech lat przed dniem, w którym upływa termin składania ofert, a jeżeli okres prowadzenia działalności jest krótszy to w tym okresie, zrealizował co najmniej sześć dostaw lub usług, związanych z wdrażaniem systemów bezpieczeństwa, w ramach której zrealizowano co najmniej: - jedno (1) zamówienie na dostawę rozwiązań z zakresu cyberbezpieczeństwa, przy czym w skład rozwiązania wchodził minimum serwer, macierz dyskowa, systemy do backupu, o wartości zamówienia nie mniejszej niż 200 000,00 złotych brutto; - jedno (1) zamówienie na dostawę systemów bezpieczeństwa sieci, zapory sieciowe NGFW, IPS, NDR, o wartości zamówienia nie mniejszej niż 400 000,00 złotych brutto; - jedno (1) zamówienie na dostawę systemów bezpieczeństwa klasy SIEM, o wartości zamówienia nie mniejszej niż 500 000,00 złotych brutto;

Criterion: Measures for ensuring quality

Description of selection criterion: Wykonawca musi posiadać aktualną autoryzację lub partnerstwo techniczne wystawione przez producenta rozwiązania oferowanego w niniejszym postępowaniu, potwierdzające prawo do jego sprzedaży, wdrażania i świadczenia wsparcia technicznego na terytorium Rzeczypospolitej Polskiej. Wymóg ten stosuje się odpowiednio do każdego producenta; w przypadku oferty wieloproducentowej dopuszczany jest dowód równoważny (Multivendor).

5.1.10. Award criteria

Criterion:

Type: Price

Name: Cena

Description: 1. Ocena ofert będzie dokonywana według skali punktowej, przy założeniu, że maksymalna punktacja wynosi 100 punktów. 2. Zamawiający dokona oceny ofert przyznając punkty w ramach poszczególnych kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt. 3. Przy wyborze oferty Zamawiający będzie się kierował kryterium najniższej ceny. 4. Punkty w kryterium „Cena” zostaną obliczone na podstawie poniższego wzoru: Cena oferty najtańszej
Liczba punktów = ----- x 100 Cena oferty badanej 5.

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku zgodnie z zasadami arytmetyki. 6. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą liczbę punktów. 7. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie, wezwie on Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach. 8. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego. 9. Zamawiający wybiera najkorzystniejszą ofertą w terminie związania ofertą określonym w SWZ. 10. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższą oceną, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty. 11. W przypadku braku zgody, o której mowa w ust. 9, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.

5.1.11. Procurement documents

Address of the procurement documents: <https://ezamowienia.gov.pl>

Ad hoc communication channel:

Name: Portal e-Zamówienia

URL: <https://ezamowienia.gov.pl>

5.1.12. Terms of procurement

Terms of submission:

Electronic submission: Required

Address for submission: <https://ezamowienia.gov.pl>

Languages in which tenders or requests to participate may be submitted: Polish

Electronic catalogue: Not allowed

Advanced or qualified electronic signature or seal (as defined in Regulation (EU) No 910/2014) is required

Variants: Not allowed

Deadline for receipt of tenders: 18/08/2026 10:00:00 (UTC+02:00) Eastern European Time, Central European Summer Time

Duration during which the tender must remain valid: 90 Days

Information about public opening:

Opening date: 18/08/2026 10:30:00 (UTC+02:00) Eastern European Time, Central European Summer Time

Place: <https://ezamowienia.gov.pl>

Terms of contract:

The execution of the contract must be performed within the framework of sheltered employment programmes: No

Electronic invoicing: Required

Electronic ordering will be used: no

Electronic payment will be used: yes

5.1.15. Techniques

Framework agreement:

No framework agreement

Information about the dynamic purchasing system:

No dynamic purchase system

5.1.16. Further information, mediation and review

Review organisation: Krajowa Izba Odwoławcza

Information about review deadlines: Informacje o terminach odwołania: 1. Odwołanie wnosi się: 1) w przypadku zamówień, których wartość jest równa albo przekracza progi unijne, w terminie: a) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej, b) 15 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a; 2) w przypadku zamówień, których wartość jest mniejsza niż progi unijne, w terminie: a) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej, b) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a. 2. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie: 1) 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest równa albo przekracza progi unijne; 2) 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest mniejsza niż progi unijne. 3. Odwołanie w przypadkach innych niż określone w ust. 1 i 2 wnosi się w terminie: 1) 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest równa albo przekracza progi unijne; 2) <https://ted.europa.eu/TED> Page 5/7 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne. 4. Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty lub nie zaprosił wykonawcy do złożenia oferty w ramach dynamicznego systemu zakupów lub umowy ramowej, odwołanie wnosi się nie później niż w terminie: 1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo 30 dni od dnia publikacji w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia, a w przypadku udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki ogłoszenia o wyniku postępowania albo ogłoszenia o udzieleniu zamówienia, zawierającego uzasadnienie udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki; 2) 6 miesięcy od dnia zawarcia umowy, jeżeli zamawiający: a) nie opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia albo b) opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenie o udzieleniu zamówienia, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki; 3) miesiąca od dnia zawarcia umowy, jeżeli zamawiający: a) nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.

Organisation providing more information on the review procedures: Krajowa Izba Odwoławcza

Organisation receiving requests to participate: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Organisation processing tenders: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

8. Organisations

8.1. ORG-0001

Official name: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Registration number: NIP: 5440004192

Registration number: REGON: 050243985

Postal address: ul. ul. Armii Krajowej 26

Town: Siemiatycze

Postcode: 17-300

Country subdivision (NUTS): Łomżyński (PL842)

Country: Poland

Email: sekretariat@pksiemiaticze.pl

Telephone: +4885 6552577

Internet address: www.pksiemiaticze.pl

Roles of this organisation:

Buyer

Organisation receiving requests to participate

Organisation processing tenders

8.1. ORG-0002

Official name: Krajowa Izba Odwoławcza

Registration number: NIP 5262239325

Postal address: ul. Postępu 17a

Town: Warszawa

Postcode: 02676

Country subdivision (NUTS): Miasto Warszawa (PL911)

Country: Poland

Email: odwolania@uzp.gov.pl

Telephone: +48 (22) 458 78 01

Fax: +48 458 78 00

Internet address: <https://www.gov.pl/web/uzp/kontakt2>

Roles of this organisation:

Review organisation

Organisation providing more information on the review procedures

10. Change

Version of the previous notice to be changed

:

ec2e6e82-aabf-48f7-8168-46261f4e1118-02

Main reason for change

:

Publisher correction

Notice information

Notice identifier/version: 87cfdb74-d23d-4d38-af7a-176e0bbd7d44 - 02

Form type: Competition

Notice type: Contract or concession notice – standard regime

Notice subtype: 16

Notice dispatch date: 23/07/2026 11:41:56 (UTC+02:00) Eastern European Time, Central European Summer Time

Languages in which this notice is officially available: Polish

Notice publication number: 515394-2026

OJ S issue number: 141/2026

Publication date: 24/07/2026