

165012-2026 - Competition

Poland – Computer training services – Postępowanie w trybie przetargu nieograniczonego na uaktualnienie i uzupełnienie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), szkolenia dla personelu medycznego i administracyjnego z zakresu cyberhigieny oraz audyt końcowy w zakresie cyberbezpieczeństwa

OJ S 48/2026 10/03/2026

**Contract or concession notice – standard regime
Services**

1. Buyer

1.1. Buyer

Official name: Szpital Miejski św. Jana Pawła II w Elblągu

Email: a.zuk@szpitalmiejski.elblag.pl

Legal type of the buyer: Body governed by public law

Activity of the contracting authority: Health

2. Procedure

2.1. Procedure

Title: Postępowanie w trybie przetargu nieograniczonego na uaktualnienie i uzupełnienie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), szkolenia dla personelu medycznego i administracyjnego z zakresu cyberhigieny oraz audyt końcowy w zakresie cyberbezpieczeństwa

Description: Przedmiotem zamówienia jest: Zadanie/Etap nr 1: Obejmuje wsparcie w opracowaniu, uzupełnieniu i aktualizacji dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) z elementami ciągłości działania (CD) w bezpieczeństwie informacji, uwzględniający kontekst organizacyjny Zamawiającego, w celu osiągnięcia zgodności z polskimi normami PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 27002, Rozporządzeniem KRI oraz UKSC2. Wsparcie dotyczy w szczególności opracowania, uzupełnienia, aktualizacji lub integracji dokumentacji w zakresie bezpieczeństwa informacji – szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1.1 do SWZ, Rozdział I Zadanie/Etap nr 2: Obejmuje przeprowadzenie szkoleń stacjonarnych dla personelu szpitala w temacie „CYBERHIGIENA W PRAKTYCE” (łącznie 886 osób) – szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1.1 do SWZ, Rozdział II Zadanie/Etap nr 3: Obejmuje przeprowadzenie audytu końcowego cyberbezpieczeństwa. Celem audytu jest weryfikacja, czy w wyniku realizacji zadań w ramach Krajowego Planu Odbudowy i Zwiększania Odporności - Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” (Nabór nr KPOD.07.03-IP.10-001/25) nastąpiło podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z inicjalnej ankiety dojrzałości cyberbezpieczeństwa, będącej załącznikiem do umowy o dofinansowanie – szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1.1 do SWZ, Rozdział III

Procedure identifier: e93cea79-d224-4bc1-b04f-c93cc7f3f959

Type of procedure: Open

The procedure is accelerated: no

2.1.1. Purpose

Main nature of the contract: Services

Main classification (cpv): 80533100 Computer training services

2.1.2. Place of performance

Country subdivision (NUTS): Elbląski (PL621)

Country: Poland

2.1.4. General information

Additional information: Z postępowania o udzielenie zamówienia wykluczony zostanie Wykonawca, w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 108 ust. 1 ustawy Prawo zamówień publicznych, tj. wykonawcę: 1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo: a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego, b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego, c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego, w art. 46–48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054), d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego, e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa, f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769 oraz z 2020 r. poz. 2023), g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe, h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego; 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1; 3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności; 4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne; 5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub

wnioski niezależnie od siebie; 6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia. 7) Ponadto o udzielenie przedmiotowego zamówienia nie mogą ubiegać się wykonawcy, którzy podlegają wykluczeniu na podstawie art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), dalej: rozporządzenie 833/2014, w brzmieniu nadanym rozporządzeniem Rady (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1), dalej: rozporządzenie 2022/5762 oraz 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. poz. 835).3 Powyższe wykluczenie następować będzie na okres trwania ww. okoliczności. Zamawiający nie przewiduje fakultatywnych przesłanek wykluczenia z udziału w postępowaniu na podstawie art. 109 ust. 1 ustawy Pzp

Legal basis:

Directive 2014/24/EU

2.1.6. Grounds for exclusion

Sources of grounds for exclusion: Procurement Document

5. Lot

5.1. Lot: LOT-0001

Title: Postępowanie w trybie przetargu nieograniczonego na uaktualnienie i uzupełnienie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), szkolenia dla personelu medycznego i administracyjnego z zakresu cyberhigieny oraz audyt końcowy w zakresie cyberbezpieczeństwa

Description: Przedmiotem zamówienia jest: Zadanie/Etap nr 1: Obejmuje wsparcie w opracowaniu, uzupełnieniu i aktualizacji dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI) z elementami ciągłości działania (CD) w bezpieczeństwie informacji, uwzględniający kontekst organizacyjny Zamawiającego, w celu osiągnięcia zgodności z polskimi normami PN-EN ISO/IEC 27001 i PN-EN ISO/IEC 27002, Rozporządzeniem KRI oraz UKSC2. Wsparcie dotyczy w szczególności opracowania, uzupełnienia, aktualizacji lub integracji dokumentacji w zakresie bezpieczeństwa informacji – szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1.1 do SWZ, Rozdział I Zadanie/Etap nr 2: Obejmuje przeprowadzenie szkoleń stacjonarnych dla personelu szpitala w temacie „CYBERHIGIENA W PRAKTYCE” (łącznie 886 osób) – szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1.1 do SWZ, Rozdział II Zadanie/Etap nr 3: Obejmuje przeprowadzenie audytu końcowego cyberbezpieczeństwa. Celem audytu jest weryfikacja, czy w wyniku realizacji zadań w ramach Krajowego Planu Odbudowy i Zwiększania Odporności - Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” będąca elementem komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” (Nabór nr KPOD.07.03-IP.10-001/25) nastąpiło podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z inicjalnej ankiety dojrzałości cyberbezpieczeństwa, będącej załącznikiem do

umowy o dofinansowanie – szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1.1 do SWZ, Rozdział III

5.1.1. Purpose

Main nature of the contract: Services

Main classification (cpv): 80533100 Computer training services

Options:

Description of the options: NIE DOTYCZY

5.1.2. Place of performance

Country subdivision (NUTS): Elbląski (PL621)

Country: Poland

5.1.3. Estimated duration

Start date: 10/04/2026

Duration end date: 31/05/2026

5.1.4. Renewal

Maximum renewals: 0

5.1.5. Value

Estimated value excluding VAT: 0,00 PLN

5.1.6. General information

Reserved participation:

Participation is not reserved.

Procurement Project fully or partially financed with EU Funds.

Information about European Union funds:

Identifier of EU funds: Projekt realizowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia” Inwestycja - D1.1.2 Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia. Tytuł Projektu: „Rozbudowa systemu informatycznego poprzez rozwój usług cyfrowych w Szpitalu Miejskim św. Jana Pawła II w Elblągu”, Umowa Nr KPOD.07.03-IP.10-0296/25/KPO/2304/2025/400

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

Additional information: 1) zdolności do występowania w obrocie gospodarczym: Zamawiający nie precyzuje w tym zakresie żadnych wymagań, 2) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów: Zamawiający nie precyzuje w tym zakresie żadnych wymagań, 3) sytuacji ekonomicznej lub finansowej: Zamawiający nie precyzuje w tym zakresie żadnych wymagań, 4) zdolności technicznej lub zawodowej: Dotyczy zadania nr 1: 4.1) Warunkiem udziału w postępowaniu jest wykonanie należycie i prawidłowe ukończenie w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie co najmniej 2 wdrożenia SZBI, których przedmiotem było opracowanie dokumentacji SZBI zgodnie z normami ISO/IEC 27001, każde dla innego zamawiającego; 4.2) Warunkiem udziału w postępowaniu jest dysponowanie wykwalifikowaną kadrą, niezbędną do realizacji zamówienia. Do realizacji zamówienia skieruje personel zdolny do należytego wykonania Zamówienia, składający się z co najmniej 3 osób, w tym: 1) co najmniej 2 osoby posiadające certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, lub

równoważny, przy czym każda z osób spełnia dodatkowo następujące wymagania: posiada wykształcenie wyższe na kierunku informatyka (lub pokrewnym) lub wykształcenie wyższe na kierunku prawo (lub pokrewnym); co najmniej 2 zrealizowane audyty w obszarze bezpieczeństwa informacji w ostatnich 12 miesiącach; udział w co najmniej 2 wdrożeniach systemu zarządzania bezpieczeństwem informacji w ostatnich 12 miesiącach, polegających na opracowaniu dokumentacji systemu; minimum 5 letnie doświadczenie zawodowe; 2) co najmniej 1 osoba posiadająca certyfikat audytora wiodącego systemu zarządzania ciągłością działania według normy PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, lub równoważny; 3) co najmniej 1 osoba posiadająca certyfikat audytora wiodącego systemu zarządzania sztuczną inteligencją według normy PN-EN ISO /IEC 42001, lub równoważny; 4) co najmniej 1 osoba posiadająca udokumentowaną wiedzę w obszarze ochrony danych osobowych na poziomie inspektora ochrony danych osobowych w postaci certyfikatu lub potwierdzenia ukończenia szkolenia z zagadnień ochrony danych osobowych na poziomie inspektora danych osobowych; 5) co najmniej 1 osoba posiadająca posiada udokumentowaną wiedzę w obszarze cyberbezpieczeństwa w postaci certyfikatu lub potwierdzenia ukończenia szkolenia z zagadnień cyberbezpieczeństwa np. CISSP, CompTIA Security+ lub równoważne; 6) co najmniej 1 osoba posiadająca udokumentowaną wiedzę w pozyskiwaniu, analizie, dokumentowaniu i zarządzaniu wymaganiami systemów i oprogramowania w postaci certyfikatu CPRE, lub równoważnego, przy czym Zamawiający dopuszcza, aby każda z osób posiadała więcej niż jeden certyfikat. Informacje w zakresie równoważności certyfikatów: 2. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony w ust.2 warunek dotyczący zdolności zawodowej spełniał w całości jeden Wykonawca. Dotyczy Zadania nr 2: 4.3) Warunkiem udziału w postępowaniu jest dysponowanie wykwalifikowaną kadrą, niezbędną do realizacji zamówienia. Wykonawca spełni warunek udziału w postępowaniu dotyczący zdolności technicznej lub zawodowej, jeżeli wykaże, że do realizacji zamówienia skieruje personel zdolny do należytego wykonania Zamówienia, składający się z co najmniej 2 osób posiadających doświadczenie w prowadzeniu szkoleń z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa, w tym: 1) każda z osób w ostatnich 12 miesiącach przeprowadziła przynajmniej 1 szkolenie dla personelu lub kadry zarządzającej z zagadnień bezpieczeństwa informacji lub cyberbezpieczeństwa; 2) każda z osób posiada wykształcenie wyższe na kierunku informatyka (lub pokrewnym) lub wykształcenie wyższe na kierunku prawo (lub pokrewnym); 3) każda z osób posiada minimum 5 letnie doświadczenie zawodowe; 4) każda z osób posiada certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, lub równoważny; 5) co najmniej 1 osoba posiadająca posiada udokumentowaną wiedzę w obszarze cyberbezpieczeństwa w postaci certyfikatu lub potwierdzenia ukończenia szkolenia z zagadnień cyberbezpieczeństwa (np. CISSP, CompTIA Security+ lub równoważne); 6) co najmniej 1 osoba posiadająca certyfikat audytora wiodącego systemu zarządzania ciągłością działania według normy PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w

zakresie certyfikacji osób, lub równoważny; 7) co najmniej 1 osoba posiadająca udokumentowaną wiedzę w obszarze ochrony danych osobowych na poziomie inspektora ochrony danych osobowych w postaci certyfikatu lub potwierdzenia ukończenia szkolenia z zagadnień ochrony danych osobowych na poziomie inspektora danych osobowych; 8) co najmniej 1 osoba posiadająca certyfikat audytora wiodącego systemu zarządzania sztuczną inteligencją według normy PN-EN ISO/IEC 42001, lub równoważny. przy czym Zamawiający dopuszcza, aby każda z osób posiadała więcej niż jeden certyfikat 2. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych Dotyczy Zadania nr 3: 4.4) Warunkiem udziału w postępowaniu jest wykonanie należycie, w szczególności zgodnie z przepisami prawa budowlanego i prawidłowe ukończenie w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie zrealizował co najmniej: a) 2 audyty bezpieczeństwa informacji w obszarze zgodności z normami ISO/IEC 27001, każdy dla innego zamawiającego; b) 2 audyty bezpieczeństwa systemów informatycznych w postaci testów penetracyjnych, każdy dla innego zamawiającego 4.5) Warunkiem udziału w postępowaniu jest dysponowanie wykwalifikowaną kadrą, niezbędną do realizacji zamówienia. Wykonawca spełni warunek udziału w postępowaniu dotyczący zdolności technicznej lub zawodowej, jeżeli wykaże, że: 1) do realizacji zamówienia skieruje personel zdolny do należytego wykonania Zamówienia, składający się z co najmniej 3 osób, z których każda posiada przynajmniej 1 certyfikat uprawniający do przeprowadzania audytów wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999), w tym: a. co najmniej 2 osoby posiadające certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, lub równoważny, przy czym każda z osób spełnia dodatkowo następujące wymagania: posiada wykształcenie wyższe na kierunku informatyka (lub pokrewnym) lub wykształcenie wyższe na kierunku prawo (lub pokrewnym); co najmniej 2 zrealizowane audyty w obszarze bezpieczeństwa informacji w ostatnich 12 miesiącach; udział w co najmniej 2 wdrożeniach systemu zarządzania bezpieczeństwem informacji w ostatnich 12 miesiącach, polegających na opracowaniu dokumentacji systemu; minimum 5 letnie doświadczenie zawodowe; b. co najmniej 1 osoba posiadająca certyfikat audytora wiodącego systemu zarządzania ciągłością działania według normy PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób, lub równoważny; c. co najmniej 1 osoba posiadająca certyfikat audytora wiodącego systemu zarządzania sztuczną inteligencją według normy PN-EN ISO/IEC 42001, lub równoważny. d. co najmniej 1 osoba posiadająca udokumentowaną wiedzę w obszarze ochrony danych osobowych na poziomie inspektora ochrony danych osobowych w postaci certyfikatu lub potwierdzenia ukończenia szkolenia z zagadnień ochrony danych osobowych na poziomie inspektora danych osobowych; e. co najmniej 1 osoba posiadająca udokumentowaną wiedzę w obszarze cyberbezpieczeństwa w postaci certyfikatu lub potwierdzenia ukończenia szkolenia z zagadnień cyberbezpieczeństwa (np. CISSP, CompTIA Security+ lub równoważne); f. co najmniej 1 osoba posiadająca udokumentowaną wiedzę w pozyskiwaniu, analizie, dokumentowaniu i zarządzaniu wymaganiami systemów i oprogramowania w postaci certyfikatu CPRE, lub r

5.1.9. Selection criteria

Sources of selection criteria: Procurement Document

5.1.10. Award criteria

Criterion:

Type: Price

Name: Cena

Description: 1) Kryterium – Cena [C] - oceniane będzie jak niżej: $C = C_{min} \times 100 : C_o$ gdzie: C - wartość punktowa w kryterium cena C_{min} - najniższa cena ze złożonych ofert C_o - cena ocenianej oferty 100 - maksymalna wartość punktowa możliwa do uzyskania w kryterium cena

Category of award weight criterion: Weight (percentage, exact)

Award criterion number: 100

5.1.11. Procurement documents

Languages in which the procurement documents are officially available: Polish

Address of the procurement documents: https://platformazakupowa.pl/pn/szpitalmiejski_elblag

5.1.12. Terms of procurement

Terms of submission:

Electronic submission: Required

Address for submission: https://platformazakupowa.pl/pn/szpitalmiejski_elblag

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

Electronic catalogue: Allowed

Deadline for receipt of tenders: 09/04/2026 09:00:00 (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: 09/04/2026 09:05:00 (UTC+02:00) Eastern European Time, Central European Summer Time

Additional information: Termin związania ofertą określony datą: 2026-07-07

Terms of contract:

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

Electronic invoicing: Allowed

Electronic ordering will be used: yes

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: 1. Odwołanie wnosi się w terminie 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej 2.

Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia, wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów

zamówienia na stronie internetowej. 3. Odwołanie w przypadkach innych niż określone w pkt. 6 i 7 wnosi się w terminie 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, 4. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” ustawy Pzp.

Organisation providing additional information about the procurement procedure: Szpital Miejski św. Jana Pawła II w Elblągu

Organisation providing offline access to the procurement documents: Szpital Miejski św. Jana Pawła II w Elblągu

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

Organisation receiving requests to participate: Szpital Miejski św. Jana Pawła II w Elblągu

Organisation processing tenders: Szpital Miejski św. Jana Pawła II w Elblągu

8. Organisations

8.1. ORG-0001

Official name: Krajowa Izba Odwoławcza

Registration number: 5262239325

Postal address: ul. Postępu 17a

Town: Warszawa

Postcode: 02-676

Country subdivision (NUTS): Miasto Warszawa (PL911)

Country: Poland

Email: odwolania@uzp.gov.pl

Telephone: 224587840

Internet address: <https://www.gov.pl/web/uzp/krajowa-izba-odwolawcza>

Roles of this organisation:

Review organisation

Organisation providing more information on the review procedures

8.1. ORG-0002

Official name: Szpital Miejski św. Jana Pawła II w Elblągu

Registration number: 5783104467

Postal address: Jana Amosa Komeńskiego 35

Town: Elbląg

Postcode: 82-300

Country subdivision (NUTS): Elbląski (PL621)

Country: Poland

Email: a.zuk@szpitalmiejski.elblag.pl

Telephone: +48552304184

Internet address: <https://www.szpitalmiejski.elblag.pl>

Information exchange endpoint (URL): https://platformazakupowa.pl/pn/szpitalmiejski_elblag

Buyer profile: https://platformazakupowa.pl/pn/szpitalmiejski_elblag

Roles of this organisation:

Buyer

Organisation providing additional information about the procurement procedure

Organisation providing offline access to the procurement documents

Organisation receiving requests to participate

Organisation processing tenders

Notice information

Notice identifier/version: 40e2c532-2287-414a-be81-b85d760f0ec0 - 01

Form type: Competition

Notice type: Contract or concession notice – standard regime

Notice subtype: 16

Notice dispatch date: 09/03/2026 10:00:57 (UTC+00:00) Western European Time, GMT

Languages in which this notice is officially available: Polish

Notice publication number: 165012-2026

OJ S issue number: 48/2026

Publication date: 10/03/2026