

269371-2026 - Wyniki

Polska – Pakiety oprogramowania do ochrony antywirusowej – Dostawa oprogramowania antywirusowego z modułem EDR/XDR, świadczenie zintegrowanej usługi typu Centrum Operacji Bezpieczeństwa oraz szkolenie personelu IT

OJ S 76/2026 20/04/2026

Ogłoszenie o udzieleniu zamówienia lub ogłoszenie o udzieleniu koncesji – tryb standardowy Dostawy

1. Nabywca

1.1. Nabywca

Oficjalna nazwa: Szpital Dziecięcy Polanki im. Macieja Płazyńskiego w Gdańsku sp. z o.o.

E-mail: zamowienia@szpitalpolanki.pl

Status prawny nabywcy: Podmiot prawa publicznego

Sektor działalności instytucji zamawiającej: Zdrowie

2. Procedura

2.1. Procedura

Tytuł: Dostawa oprogramowania antywirusowego z modułem EDR/XDR, świadczenie zintegrowanej usługi typu Centrum Operacji Bezpieczeństwa oraz szkolenie personelu IT

Opis: 1. Przedmiotem niniejszego zamówienia jest dostawa i aktualizacja oprogramowania służącego do informatyzacji i cyfryzacji Szpitala wraz usługami utrzymaniowa ochrony poczty, wsparcia EDR/XDR, utrzymania posiadanego systemu zarządzania podatnościami (SIEM) oraz systemu ochrony stacji roboczych i serwerów, a także szkolenie personelu IT w ramach realizacji przedsięwzięcia finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO). 2. Szczegółowy opis przedmiotu zamówienia został określony w OPZ (załącznik nr 1 do SWZ) oraz we wzorze umowy (załącznik nr 2 do SWZ). **WARUNKI UDZIAŁU W POSTĘPOWANIU:** 1.2.1. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej: 1) jedną dostawę oraz wdrożenie i uruchomienie oprogramowania ESET PROTECT Enterprise (EDR oraz XDR) lub rozwiązania równoważnego; Poprzez rozwiązanie równoważne do oprogramowania ESET PROTECT Enterprise (EDR oraz XDR) Zamawiający rozumie oprogramowanie spełniające łącznie poniższe minimalne wymagania funkcjonalne: a. Przypisanie licencji do konta Zamawiającego i dostarczenie certyfikatu wystawionego przez producenta. b. Możliwość sprawdzenia długości przypisanych licencji z poziomu konsoli zarządzającej. c. Liczba licencji: 316 szt.. d. Konsola zarządzająca. e. Wielowarstwowa ochrona stacji roboczych i serwerów. f. Ochrona systemu operacyjnego, przeglądarek WWW, poczty, pamięci operacyjnej. g. Możliwość szyfrowania dysków. h. Wykrywanie zagrożeń w oparciu o analizę ich zachowania i reputacji. i. Ochrona przed złośliwym oprogramowaniem typu ransomware i atakami zero-day. j. Zapobieganie atakom bezplikowym. k. Możliwość instalowania na stacjach roboczych z systemami Windows 10, Windows 11, Windows Server 2012R2 i późniejszych, macOS, Linux. l. Centralna konsola zarządzania licencjami, wykrytymi zagrożeniami, stacjami, użytkownikami, plikami skierowanymi do kwarantanny. m. Ochrona plików w czasie rzeczywistym. n. Ochrona sektorów startowych, UEFI. o. Skanowanie spakowanych plików. p. Wykrywanie zagrożeń algorytmami heurystycznymi. q. Wykrywanie zagrożeń na podstawie reputacji aplikacji. r. Wykrywanie zagrożeń na podstawie reputacji

adresów IP. s. Ochrona przed atakami z sieci (IDS). t. Ochrona przed atakami typu brute force. u. Ochrona przed botnetami. v. Możliwość definiowania tzw. czarnej listy adresów IP. w. Wykrywanie włamań min. dla protokołów: SMB, RCP, RDP. x. Blokowanie niebezpiecznych adresów po wykryciu ataku. y. Możliwość definiowania wyłączeń dla w/w ustawień. z. Współpraca z domeną Windows AD. aa. Zdalna konfiguracja stacji roboczych możliwość definiowania różnych polityk dla różnych grup komputerów, serwerów, itp.. bb. Możliwość zdalnej instalacji systemu antywirusowego za pomocą WMI. cc. Możliwość zdalnej instalacji systemu antywirusowego za pomocą GPO. dd. Możliwość skanowania na żądanie wskazanej stacji roboczej lub serwera. ee. Możliwość skanowania w trakcie bezczynności komputera. ff. Możliwość skanowania przy uruchamianiu komputera / serwera. gg. Możliwość pobierania aktualizacji systemu antywirusowego bez konieczności stałego połączenia z Internetem na stacjach roboczych (np. przez serwer proxy, lokalne repozytorium aktualizacji lub podobne rozwiązanie). hh. Monitorowanie wersji oprogramowania antywirusowego i jego modułów, raportowanie w konsoli zarządzającej. ii. Monitorowanie aktualizacji systemu operacyjnego, raportowanie w konsoli zarządzającej. jj. Monitorowanie zdarzeń systemowych. kk. Możliwość wycofania aktualizacji modułu systemu antywirusowego w przypadku pojawienia się błędów lub fałszywych alertów. ll. Możliwość aktywnego filtrowania stron internetowych i poczty elektronicznej. mm. Możliwość zdefiniowania wyjątków dla aplikacji, wybranych stron i adresów IP. nn. Ochrona przed atakami typu "phishing". oo. Możliwość konfigurowania systemu i interfejsu użytkownika na stacjach roboczych i serwerach z poziomu centralnej konsoli zarządzającej. pp. Wysyłanie alertów przez pocztę elektroniczną na wskazane adresy. qq. Możliwość przygotowania pakietu instalacyjnego dla wybranej grupy urządzeń z uwzględnieniem wymaganych modułów, konfiguracji i polityk. rr. Moduł analizy danych zbieranych ze stacji roboczych i serwerów w celu korelacji zdarzeń i typowania zagrożeń. ss. Raportowanie, w formie drzewa, szczegółowych informacji dotyczących wykrytego zagrożenia, w tym: rodzaj zagrożenia, uruchomione procesy, rozpoznane zagrożenia, rozpoznane niepożądane interakcje, odniesienie do MITRE ATT&CK, data wystąpienia zdarzenia, data wykrycia zdarzenia, zalecane rozwiązania i działania, które zminimalizują lub rozwiążą problem. tt. Możliwość przypisania automatycznej akcji podejmowanej przez system dla podobnych wystąpień (playbook). uu. Możliwość wygenerowania listy zainstalowanych aplikacji na stacjach roboczych i serwerze wraz z analizą zagrożeń. vv. Możliwość przeglądania i filtrowania skryptów wykonywanych na stacjach lub serwerach. ww. Możliwość blokowania nieautoryzowanych skryptów i aplikacji przed uruchomieniem. xx. Automatyczne usuwanie niepożądanych aplikacji w ramach stosowanych rozwiązań usuwających wykryte zagrożenie. yy. Możliwość blokowania aplikacji lub skryptów na podstawie grupy użytkowników lub komputerów. zz. Możliwość grupowania komputerów na podstawie domeny AD lub ustawień ręcznych. aaa. Możliwość włączenia kwarantanny dla zainfekowanego komputera. bbb. Możliwość połączenia z konsolą zarządzającą za pomocą przeglądarki WWW. ccc. Możliwość wgrania komercyjnych certyfikatów SSL do serwerów odpowiadających za stronę WWW konsoli zarządzającej. ddd. Wykrywanie anomalii w zachowaniach stacji roboczych, programów i skryptów. eee. Wykrywanie działań naruszających ustanowione polityki. fff. Określanie stopnia zagrożenia na podstawie punktów ratingowych i progów alarmowych, po przekroczeniu, których będzie (...)

Identyfikator procedury: 2f6b55c0-9e32-4d54-b11b-5002ea870b35

Poprzednie ogłoszenie: 162032-2026

Wewnętrzny identyfikator: SZP/ZPZ/68/2026/KP

Rodzaj procedury: Otwarta

Procedura jest przyspieszona: nie

Główne aspekty procedury: WARUNKI UDZIAŁU CD: potwierdzony jest egzaminem.

Certyfikat równoważny nie może być wystawiony przez Wykonawcę lub podmiot zależny od

Wykonawcy. UWAGA: 1) Dopuszcza się wykazanie tej samej usługi w odniesieniu do różnych osób skierowanych do realizacji zamówienia. 1.2.3. Zamawiający uzna, że Wykonawca znajduje się w sytuacji ekonomicznej lub finansowej niezbędnej do realizacji zamówienia, jeżeli Wykonawca wykaże, że posiada ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną nie mniejszą niż 100.000,00 zł. Podstawy wykluczenia o charakterze wyłącznie krajowym. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy: nie podlegają wykluczeniu: na podstawie art. 108 ust. 1 ustawy Pzp, 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, 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. CIĄG DALSZY PODMIOTOWYCH ŚRODKÓW DOWODOWYCH: 2. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast informacji z Krajowego Rejestru Karnego, o której mowa w ust. 1 pkt 1 – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie, o którym mowa w ust. 1 pkt 1. Dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem. 3. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w ust. 2, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4 ustawy Pzp, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania osoby, której dokument miał dotyczyć. Dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem. 4. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia podmiotowe środki dowodowe na potwierdzenie braku podstaw wykluczenia, składa każdy z wykonawców występujących wspólnie. 5. W przypadku podmiotu, na którego zdolnościach lub sytuacji wykonawca polega na zasadach art. 118 Pzp, wykonawca składa podmiotowe środki dowodowe na potwierdzenie braku podstaw wykluczenia w odniesieniu do każdego z tych podmiotów. Informacja o przedmiotowych środkach dowodowych 1. Wykonawcy muszą złożyć wraz z ofertą następujące oświadczenia i dokumenty: • Oświadczenia Wykonawcy o spełnieniu zasady „Nie czyń poważnych szkód” (DNSH) – Załącznik nr 12 do SWZ. 2. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych wskazanych w ust. 1 lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wezwie do ich złożenia lub uzupełnienia w terminie wyznaczonym w wezwaniu, chyba że pomimo złożenia przedmiotowego środka dowodowego, oferta będzie podlegała odrzuceniu albo będą zachodziły przesłanki unieważnienia postępowania.

2.1.1. Przeznaczenie

Charakter zamówienia: Dostawy

Główna klasyfikacja (cpv): 48760000 Pakiety oprogramowania do ochrony antywirusowej

Dodatkowa klasyfikacja (cpv): 72250000 Usługi w zakresie konserwacji i wsparcia systemów, 72510000 Usługi zarządzania wspierane komputerowo, 80533100 Usługi szkolenia komputerowego, 72253200 Usługi w zakresie wsparcia systemu

2.1.2. Miejsce realizacji

Adres pocztowy: Polanki 119

Miejscowość: Gdańsk

Kod pocztowy: 80-308

Podpodział krajowy (NUTS): Gdański (PL634)

Kraj: Polska

Informacje dodatkowe: WARUNKI UDZIAŁU CD: (....)będzie wyzwalana akcja lub powiadomienia dla administratora. ggg. Zaawansowane wykrywanie zagrożeń (EDR Endpoint Detection and Response) System analizuje zachowania procesów i użytkowników w czasie rzeczywistym, identyfikując anomalie, ataki typu zero-day, fileless malware oraz podejrzane działania w sieci organizacji. hhh. Reagowanie i neutralizacja incydentów bezpieczeństwa Umożliwia natychmiastowe działania zdalne izolację zainfekowanych urządzeń, zakończenie procesów, zbieranie logów oraz usuwanie zagrożeń bez potrzeby fizycznego dostępu do stacji roboczej. iii. Analiza, raportowanie i wizualizacja ataków Oferuje centralne zarządzanie zdarzeniami, korelację danych z wielu urządzeń, tworzenie szczegółowych raportów bezpieczeństwa oraz graficzną prezentację łańcucha ataku (attack chain visualization). jjj. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu. 2) jedną usługę administracji i utrzymania oprogramowania klasy SIEM zawierającego moduł EDR oraz XDR w podmiocie liczącym co najmniej 150 stacji roboczych i co najmniej 10 serwerów fizycznych; 3) jedną usługę administracji i utrzymania środowiska poczty elektronicznej, obejmującego środowisko co najmniej 300 użytkowników (lub skrzynek); 4) trzy usługi polegające na przeprowadzeniu szkolenia z zakresu cyberbezpieczeństwa lub bezpieczeństwa IT, przy czym szkolenie w ramach każdej usługi obejmowało co najmniej dwa z następujących zagadnień: a) systemy klasy EDR lub XDR, b) reagowanie na incydenty bezpieczeństwa (incident response), c) monitoring zdarzeń bezpieczeństwa, analiza alertów, d) zarządzanie podatnościami lub skanowanie podatności. Szkolenie w ramach każdej usługi spełniało łącznie poniższe warunki: a) zostało zrealizowane w formie warsztatowej z częścią praktyczną, przez co należy rozumieć zajęcia, w których uczestnicy aktywnie pracują nad zadaniami lub problemami, b) obejmowało minimum 8 godzin zegarowych, c) było skierowane do personelu IT. UWAGA: 1) Poprzez trzy usługi Zamawiający rozumie usługi wykonane na podstawie trzech różnych umów. 2) W przypadku gdy Wykonawca realizował zamówienie jako jeden z grupy Wykonawców (konsorcjum) może powoływać się jedynie na swoje własne, realne doświadczenie, które zdobył realizując daną część zamówienia, która została mu przypisana w ramach grupy, tzn. może wykazywać się doświadczeniem jedynie w zakresie, jaki rzeczywiście dany podmiot wykonywał. Doświadczenia nie uzyskuje się poprzez sam udział w konsorcjum, lecz poprzez konkretne czynności realizowane w jego ramach. 1.2.2. Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że skieruje do realizacji zamówienia (dysponuje lub będzie dysponował): 1) co najmniej jedną osobą skierowaną do realizacji zamówienia, pełniącą rolę członka zespołu wdrożeniowego zamówienia opisanego w pkt. 1 ppkt. 2 lit. a OPZ, spełniającą łącznie następujące wymagania: a. w okresie ostatnich 3 lat przed terminem składania ofert uczestniczyła w co najmniej dwóch wdrożeniach, konfiguracji i uruchomieniu rozwiązania klasy EDR oraz XDR dla stacji roboczych lub serwerów, b. ukończyła szkolenie producenta oprogramowania ESET PROTECT Enterprise (EDR/XDR) lub producenta rozwiązania równoważnego (opisanego w pkt 1.2.1. ppkt 1) w zakresie wdrożenia i administracji rozwiązania klasy EDR oraz XDR dla stacji roboczych lub

serwerów. 2) osobami skierowanymi do realizacji zamówienia, pełniącymi role członków zespołu świadczącego usługę stanowiącą przedmiot zamówienia opisanego w pkt. 1 ppkt. 2 lit. b-e, w tym co najmniej: a. jedną osobą posiadającą minimum 2-letnie doświadczenie zawodowe w zakresie administracji i utrzymania systemu klasy SIEM (w tym konfiguracji źródeł logów, reguł korelacji, obsługi alertów i raportowania), b. jedną osobą posiadającą minimum 2-letnie doświadczenie zawodowe w zakresie administracji i utrzymania rozwiązania ochrony stacji roboczych/serwerów z modulem EDR oraz XDR, c. jedną osobą posiadającą minimum 2-letnie doświadczenie zawodowe w zakresie administracji i utrzymania środowiska serwera którego funkcją jest obsługa poczty elektronicznej, w szczególności przyjmowanie, wysyłanie, przekazywanie, przechowywanie oraz udostępnianie użytkownikom wiadomości e-mail w sieci teleinformatycznej, d. jedną osobą posiadającą minimum 2-letnie doświadczenie zawodowe w zakresie realizacji proaktywnego monitorowania obejmującego ciągły, zautomatyzowany nadzór stanu, dostępności oraz parametrów wydajnościowych kluczowych komponentów infrastruktury IT (NOC/monitoring), przy czym Zamawiający dopuszcza łączenie ról przez jedną osobę, o ile spełnia ona wymagania dla każdej z ról. 3) co najmniej jedną osobą skierowaną do realizacji zamówienia, pełniącą rolę trenera zamówienia opisanego w pkt. 1 ppkt. 2 lit. f OPZ, która posiada kwalifikacje zawodowe i doświadczenie odpowiadające warunkom określonym poniżej: a. minimum 3-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa lub administracji systemami bezpieczeństwa IT; b. doświadczenie w przeprowadzeniu co najmniej trzech szkoleń lub warsztatów w obszarze cyberbezpieczeństwa dla personelu IT w ciągu ostatnich trzech lat przed terminem składania ofert; c. ważny 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 (tj. Dz. U. z 2025 r. poz. 568) lub certyfikat równoważny. Przez certyfikat równoważny Zamawiający rozumie certyfikat, który jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy dla danej roli, co jest rozumiane jako: analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat; analogiczny stopień poziomu kompetencji; analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu; (...)

2.1.3. Wartość

Szacunkowa wartość bez VAT: 1 227 539,00 PLN

2.1.4. Informacje ogólne

Informacje dodatkowe: 1. Wykonawca składa tylko jedną ofertę za pośrednictwem Platformy Zakupowej pod adresem <https://szpitalpolanki.ezamawiajacy.pl> poprzez jej załączenie w zakładce Załączniki. 2. Oferta powinna zostać sporządzona poprzez wypełnienie elektronicznego formularza ofertowego i złożenie Formularza Ofertowego, stanowiącego załącznik nr 3 do SWZ. Uwaga: W razie sprzeczności pomiędzy treścią elektronicznego formularza ofertowego i Formularza Ofertowego, stanowiącego załącznik nr 3 do SWZ, przyjmuje się, że Wykonawca złożył ofertę o treści zawartej w Formularzu Ofertowym, stanowiącym załącznik nr 3 do SWZ, zaś elektroniczny formularz ofertowy będzie podlegał sprostowaniu. Formularz oferty nie podlega uzupełnieniu. 3. Wykonawcy muszą złożyć wraz z ofertą następujące oświadczenia i dokumenty: 1) aktualne na dzień składania ofert oświadczenie w zakresie wskazanym w SWZ. Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu z postępowania oraz spełnia warunki udziału w postępowaniu. Oświadczenie składa się na formularzu jednolitego europejskiego dokumentu zamówienia, sporządzonym zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji (UE) 2016/7

z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16), zwanego dalej "JEDZ" Instrukcja wypełniania JEDZ: Istnieje możliwość wypełnienia JEDZ bezpośrednio na Platformie zakupowej bądź złożenia go jako osobnego dokumentu. Informujemy, że pod adresem <https://espd.uzp.gov.pl> Urząd Zamówień Publicznych udostępnił narzędzie umożliwiające zamawiającym i wykonawcom utworzenie, wypełnienie i ponowne wykorzystanie standardowego formularza JEDZ/ESPD w wersji elektronicznej (eESPD). W celu wypełnienia JEDZ należy: 1. z Platformy zakupowej w zakładce „Załączniki” przedmiotowego postępowania pobrać plik JEDZ będący załącznikiem nr 4 do SWZ i rozpakować go, 2. uruchomić stronę <https://espd.uzp.gov.pl>, 3. po uruchomieniu strony i wyborze języka polskiego, należy wybrać opcję „Jestem wykonawcą”, 4. następnie należy wybrać opcję „zaimportować ESPD”, wczytać rozpakowany plik JEDZ będący załącznikiem nr 4 do SWZ, wybrać kraj „Polska” i postępować dalej zgodnie z instrukcjami (podpowiedziami) w narzędziu, 5. Formularz JEDZ należy wypełnić w polach, które nie zostały przez Zamawiającego zacieniowane; Uwaga: W części IV Kryteria klasyfikacji, Wykonawca ogranicza się jedynie do wypełnienia sekcji α i nie wypełnia żadnej z pozostałych sekcji w części IV; Oświadczenie zawarte w cz. III lit. D (Podstawy wykluczenia o charakterze wyłącznie krajowym) obejmuje również potwierdzenie, że Wykonawca nie podlega wykluczeniu na podstawie przesłanek wskazanych w rozdz. VI ust. 1 pkt 1.1. ppkt 1.1.2. 2) oświadczenia wykonawcy/podmiotu udostępniającego zasoby, którego wzór określono w Załączniku nr 8 do SWZ, że w stosunku do danego wykonawcy/podmiotu udostępniającego zasoby nie zachodzą przesłanki wykluczenia przewidziane w art. 5k rozporządzenia 833/2014; 3) W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenia, o których mowa w pkt 1 i 2, składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to ma potwierdzić brak podstaw wykluczenia oraz spełnienie warunków udziału w postępowaniu w zakresie, w którym każdy z wykonawców wykazuje spełnienie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia; 4) Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia oświadczenia, o których mowa w pkt 1 i 2, podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu w zakresie, w jakim wykonawca powołuje się na jego zasoby; 5) zobowiązanie podmiotu trzeciego, o którym mowa w rozdziale VI ust. 4 i 5 SWZ, jeżeli wykonawca polega na zasobach lub sytuacji podmiotu trzeciego (wzór zobowiązania do oddania do dyspozycji zasobów określa Załącznik nr 9); 6) pełnomocnictwa lub inne dokumenty, z których wynika prawo do złożenia oferty oraz innych dokumentów składanych wraz z ofertą; 7) pełnomocnictwa do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia, ewentualnie umowa o współdziałaniu z której będzie wynikać przedmiotowe pełnomocnictwo; 8) przedmiotowe środki dowodowe określone w rozdz. IV SWZ; 9) inne dokumenty określone w SWZ. 4. Oferta winna zostać złożona pod rygorem nieważności w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym za pośrednictwem Platformy dostępnej pod adresem <https://szpitalpolanki.ezamawiajacy.pl> 5. Korzystanie z Platformy jest bezpłatne. 6. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski. 7. Oferta jest jawna od chwili jej otwarcia. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp. **PODMIOTOWE ŚRODKI DOWODOWE:** 1. Zamawiający

przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni, aktualnych na dzień złożenia następujących oświadczeń lub dokumentów: 1) informacji z Krajowego Rejestru Karnego w zakresie: a) art. 108 ust. 1 pkt 1 i 2 ustawy Pzp, b) art. 108 ust. 1 pkt 4 ustawy Pzp, dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego, - sporządzonej nie wcześniej niż 6 miesięcy przed jej złożeniem; 2) oświadczenia wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2023 r. poz. 1689 z późn. zm.), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej (wzór oświadczenia stanowi załącznik nr 5 do SWZ); 3) oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy (JEDZ), w zakresie podstaw wykluczenia z postępowania wskazanych przez zamawiającego, o których mowa w: a) art. 108 ust. 1 pkt 3 ustawy, b) art. 108 ust. 1 pkt 4 ustawy, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego, c) art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji, d) art. 108 ust. 1 pkt 6 ustawy; 4) dokumentów dotyczących podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy, w celu wykazania braku istnienia wobec niego podstaw wykluczenia (pkt 1 – 3) oraz spełnienia, w zakresie, w jakim Wykonawca powołuje się na jego zasoby, warunków udziału w postępowaniu (pkt 5-7) – jeżeli wykonawca polega na zasobach podmiotu trzeciego; 5) dokumentów potwierdzających, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia ze wskazaniem sumy gwarancyjnej tego ubezpieczenia; 6) wykazu dostaw/usług (w zakresie wskazanym w rozdz. VI ust. 1 pkt 1.2. ppkt 1.2.1. SWZ) wykonanych w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy/usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy/usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy/usługi zostały wykonane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy (wg wzoru stanowiącego Załącznik nr 6 do SWZ); 7) wykazu osób (w zakresie wskazanym w rozdz. VI ust. 1 pkt 1.2. ppkt 1.2.2. SWZ), skierowanych przez Wykonawcę do realizacji zamówienia publicznego, wraz z informacjami na temat ich doświadczenia niezbędnego do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami (wg wzoru stanowiącego Załącznik nr 7 do SWZ).

Podstawa prawna:

Dyrektywa 2014/24/UE

Dyrektywa 2014/24/UE - art. 132 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320).

Właściwe prawo transgraniczne: Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia: 1) w przypadku spółki cywilnej Zamawiający przyjmuje, że Wykonawcami są wspólnicy spółki cywilnej, których udział w postępowaniu traktowany jest jako wspólne ubieganie się o udzielenie zamówienia w rozumieniu art. 58 ust. 1 ustawy Pzp; 2) Wykonawcy występujący wspólnie ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie

zamówienia publicznego; 3) Pełnomocnictwo do dokonywania czynności, o których mowa w pkt 2 powinno mieć postać dokumentu stwierdzającego ustanowienie pełnomocnika, podpisanego przez uprawnionych do ich reprezentacji przedstawicieli wszystkich pozostałych Wykonawców. Pełnomocnictwo należy dołączyć do oferty; 4) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ponoszą solidarną odpowiedzialność za wykonanie umowy i wniesienie zabezpieczenia należytego wykonania umowy;

5. Część zamówienia

5.1. Część zamówienia: LOT-0001

Tytuł: Dostawa oprogramowania antywirusowego z modułem EDR/XDR, świadczenie zintegrowanej usługi typu Centrum Operacji Bezpieczeństwa oraz szkolenie personelu IT

Opis: 1. Przedmiotem niniejszego zamówienia jest dostawa i aktualizacja oprogramowania służącego do informatyzacji i cyfryzacji Szpitala wraz usługami utrzymaniowymi ochrony poczty, wsparcia EDR/XDR, utrzymania posiadanego systemu zarządzania podatnościami (SIEM) oraz systemu ochrony stacji roboczych i serwerów, a także szkolenie personelu IT w ramach realizacji przedsięwzięcia finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO). 2. Szczegółowy opis przedmiotu zamówienia został określony w OPZ (załącznik nr 1 do SWZ) oraz we wzorze umowy (załącznik nr 2 do SWZ). Termin realizacji przedmiotu zamówienia wynosi 38 miesięcy od dnia zawarcia umowy. Postępowanie prowadzone jest w języku polskim. UZASADNIENIE BRAKU PODZIAŁU NA CZĘŚCI

Zamawiający odstąpił od podziału zamówienia na części, ponieważ specyfika przedmiotu zamówienia wymaga zapewnienia pełnej spójności technologicznej oraz organizacyjnej pomiędzy poszczególnymi elementami systemu cyberbezpieczeństwa. Przedmiot zamówienia obejmuje zarówno dostawę i wdrożenie oprogramowania antywirusowego z modułem EDR/XDR, jak również świadczenie usług utrzymania systemu ochrony stacji roboczych, administracji systemem poczty elektronicznej, administracji systemem SIEM oraz proaktywnego monitorowania infrastruktury IT. Zakres tych usług stanowi funkcjonalnie jeden spójny proces zapewnienia bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego. Poszczególne elementy systemu bezpieczeństwa – w szczególności system EDR/XDR, system SIEM, system poczty elektronicznej oraz monitoring infrastruktury – są ze sobą ściśle powiązane i współpracują w ramach jednego procesu detekcji, analizy oraz reagowania na incydenty bezpieczeństwa. Podział zamówienia na części mógłby prowadzić do powstania nadmiernych trudności technicznych oraz organizacyjnych związanych z integracją poszczególnych komponentów systemu oraz koordynacją działań wielu wykonawców. W szczególności mógłby powodować rozproszenie odpowiedzialności za obsługę incydentów bezpieczeństwa, wydłużenie czasu reakcji na zdarzenia oraz utrudnienia w zapewnieniu jednolitego modelu operacyjnego usług bezpieczeństwa. Zamawiający wskazuje, że realizacja usług objętych zamówieniem powinna odbywać się w modelu zapewniającym jeden punkt kontaktu dla zgłoszeń, jednolity system obsługi incydentów, wspólne procedury reagowania oraz jednolite raportowanie w zakresie realizacji usług. Zapewnienie takiego modelu operacyjnego w przypadku realizacji poszczególnych elementów zamówienia przez różnych wykonawców byłoby znacząco utrudnione. Dodatkowo przedmiot zamówienia realizowany jest w środowisku podmiotu leczniczego, w którym systemy informatyczne obsługują procesy krytyczne związane z udzielaniem świadczeń zdrowotnych. Wdrożenie i utrzymanie systemów bezpieczeństwa musi być prowadzone w sposób zapewniający ciągłość działania infrastruktury IT oraz minimalizujący ryzyko zakłóceń funkcjonowania systemów wykorzystywanych w działalności medycznej. Mając na uwadze powyższe względy techniczne i organizacyjne Zamawiający uznał, że realizacja zamówienia przez jednego wykonawcę zapewni właściwą koordynację prac, spójność technologiczną systemów oraz ograniczy

ryzyko operacyjne związane z utrzymaniem infrastruktury IT. W konsekwencji brak podziału zamówienia na części należy uznać za rozwiązanie uzasadnione i racjonalne.

Wewnętrzny identyfikator: SZP/ZPZ/68/2026/KP

5.1.1. Przeznaczenie

Charakter zamówienia: Dostawy

Główna klasyfikacja (cpv): 48760000 Pakiety oprogramowania do ochrony antywirusowej

Dodatkowa klasyfikacja (cpv): 72250000 Usługi w zakresie konserwacji i wsparcia systemów, 72510000 Usługi zarządzania wspierane komputerowo, 80533100 Usługi szkolenia

komputerowego, 72253200 Usługi w zakresie wsparcia systemu

5.1.2. Miejsce realizacji

Adres pocztowy: Polanki 119

Miejscowość: Gdańsk

Kod pocztowy: 80-308

Podpodział krajowy (NUTS): Gdański (PL634)

Kraj: Polska

Informacje dodatkowe: 1. Postępowanie prowadzone jest w formie elektronicznej za pośrednictwem Platformy Zakupowej pod adresem: <https://szpitalpolanki.ezamawiajacy.pl> 2. Pełną obsługę techniczną Platformy zakupowej świadczy firma Otwarty Rynek Elektroniczny S. A. z siedzibą w Warszawie (02-672), ul. Domaniewska 49. W przypadku ewentualnych problemów technicznych prosimy o kontakt z infolinią techniczną pod numerem +48 22 257 22 23 (infolinia dostępna w dni robocze, w godzinach 9.00-17.00), lub pod adresem e-mail: oneplace@marketplanet.pl 3. W przedmiotowym postępowaniu Zamawiający dopuszcza możliwość przekazywania sobie przez strony postępowania oświadczeń, wniosków, zawiadomień oraz informacji za pośrednictwem Platformy znajdującej się pod adresem: <https://szpitalpolanki.ezamawiajacy.pl> w sekcji „Korespondencja”. 4. Oświadczenia, wnioski, zawiadomienia lub informacje, które wpłyną do Zamawiającego, uważa się za dokumenty złożone w terminie, jeśli ich czytelna treść dotrze do Zamawiającego przed upływem tego terminu. Za datę wpływu oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich wysłania za pośrednictwem sekcji „Wiadomości”. 5. Ogólne zasady korzystania z Platformy określa SWZ. Zmiany umowy 1. Zamawiający dopuszcza możliwość dokonywania zmian umowy zgodnie z art. 455 ustawy pzp. 2. Zmiany postanowień umowy w stosunku do treści oferty mogą dotyczyć: 1) terminu realizacji zamówienia, 2) sposobu realizacji zamówienia, 3) osób wskazanych w ofercie. 3. Zmiany, o których mowa w ust. 2 następują: 1) w przypadku wystąpienia „siły wyższej”. Pod pojęciem siły wyższej Zamawiający rozumie okoliczności, które pomimo zachowania należytej staranności są nieprzewidywalne oraz, którym nie można zapobiec lub przeciwstawić się skutecznie. O braku możliwości dotrzymania terminu Wykonawca obowiązany jest niezwłocznie powiadomić Zamawiającego, określając jednocześnie nowy termin realizacji zamówienia, 2) w zakresie pkt 2, jeśli rozwiązania zaproponowane przez Zamawiającego lub Wykonawcę przyczynią się do uzyskania wyższej jakości końcowej zamówienia, przy czym zmiana ta nie będzie miała wpływu na wysokość wynagrodzenia Wykonawcy, 3) w zakresie pkt 3, w przypadku, gdy osoba wskazana w ofercie z przyczyn niezależnych od Wykonawcy, których nie można było przewidzieć w chwili upływu terminu składania ofert, nie może uczestniczyć w realizacji zamówienia, zaś osoba ją zastępująca spełnia warunki udziału w postępowaniu wskazane w SWZ w zakresie, w jakim spełniała je osoba zastępowana. 3. Wszelkie zmiany Umowy wymagają formy pisemnej, pod rygorem nieważności. 4. W trakcie trwania Umowy Wykonawca zobowiązuje się do

pisemnego powiadamiania Zamawiającego o zmianie siedziby lub nazwy firmy. 5. Żadna ze stron nie może bez zgody drugiej strony przenieść na osobę trzecią wierzytelności, wynikających z niniejszej umowy.

5.1.3. Szacowany okres obowiązywania

Okres obowiązywania: 38 Miesiące

5.1.5. Wartość

Szacunkowa wartość bez VAT: 1 227 539,00 PLN

5.1.6. Informacje ogólne

Projekt zamówienia w pełni lub częściowo finansowany z funduszy UE

Zamówienie jest objęte zakresem Porozumienia w sprawie zamówień rządowych (GPA): nie

Informacje dodatkowe: Zgodnie z art. 13 ust. 1 i 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. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że: 1) administratorem danych osobowych jest Szpital Dziecięcy Polanki im. Macieja Płażyńskiego w Gdańsku sp. z o.o., ul. Polanki 119, 80-308 Gdańsk; tel. 58 520 93 00, fax 58 552 47 41, E-mail: zamowienia@szpitalpolanki.pl 2) inspektorem ochrony danych osobowych w Szpitalu Dziecięcym Polanki im. Macieja Płażyńskiego w Gdańsku sp. z o.o. jest Maciej Pabiś, kontakt: iod@szpitalpolanki.pl; 3) dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego prowadzonym także w celu wypełnienia obowiązków wynikających z finansowania ze środków KPO oraz warunkami umowy o dofinansowanie; 4) odbiorcami danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania zgodnie z ustawą z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2023 r. poz. 1605), dalej „ustawa Pzp” oraz Otwarty Rynek Elektroniczny Spółka akcyjna z siedzibą w Warszawie (adres: Al. Komisji Edukacji Narodowej 51 lok. U21, 02-797 Warszawa), wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000041441, REGON: 017282436, NIP: 526-25-35-153, właściciel Platformy zakupowej, na której Zamawiający prowadzi postępowania o udzielenie zamówienia publicznego, Minister Funduszy i Polityki Regionalnej, Minister Zdrowia; 5) dane osobowe będą przechowywane, zgodnie z warunkami umowy wskazanej w ust. 1 przez okres 5 lat od 31 grudnia następującego po zatwierdzeniu wniosku o płatność końcową. Podstawa prawna art. 133 Rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 z dnia 23 września 2024 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii (Dz. U. UE. L. z 2024 r. poz.2509); 6) obowiązek podania przez danych osobowych bezpośrednio dotyczących wykonawcy będącego osobą fizyczną jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp; 7) w odniesieniu do danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO; 8) osoba, której dane są przetwarzane, posiada: a) na podstawie art. 15 RODO prawo dostępu do danych osobowych jej dotyczących; b) na podstawie art. 16 RODO prawo do sprostowania jej danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników); c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do

przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego); d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych narusza przepisy RODO; 9) osoba, której dane są przetwarzane, nie posiada: a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawa do usunięcia danych osobowych; b) prawa do przenoszenia danych osobowych, o którym mowa w art. 20 RODO; c) na podstawie art. 21 RODO prawa sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.

5.1.10. Kryteria udzielenia zamówienia

Kryterium:

Rodzaj: Cena

Opis: 1. Sposób obliczenia dla kryterium „Cena brutto wykonania zamówienia” $P = [CN / CR \times 100 \%] \times 100$ P – ilość punktów dla kryterium CN – najniższa oferowana cena CR – cena oferty rozpatrywanej 2. Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów. 3. W celu obliczenia punktów wyniki poszczególnych działań matematycznych będą zaokrąglane do dwóch miejsc po przecinku lub z większą dokładnością, jeśli przy zastosowaniu wymienionego zaokrąglenia nie występuje różnica w ilości przyznanych punktów. 4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert. 5. Zamawiający nie przewiduje dogrywki w formie aukcji elektronicznej.

Kategoria kryterium udzielenia zamówienia waga: Waga (wartość procentowa, dokładna)

Kryterium udzielenia - Liczba: 100

5.1.15. Techniki

Umowa ramowa:

Brak umowy ramowej

Informacje o dynamicznym systemie zakupów:

Brak dynamicznego systemu zakupów

5.1.16. Dalsze informacje, mediacja i odwołanie

Organ odwoławczy: Prezes Krajowej Izby Odwoławczej

Informacje o terminach odwołania: 1. Środki ochrony prawnej przysługujące wykonawcy określa DZIAŁ IX ustawy Pzp. 2. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy. 3. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy Pzp, oraz Rzecznikowi Małych i Średnich Przedsiębiorców. 4. Pisma w postępowaniu odwoławczym wnoszą się w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej, z tym że odwołanie i przystąpienie do postępowania odwoławczego, wniesione w postaci elektronicznej, wymagają opatrzenia podpisem zaufanym. 5. Pisma w formie pisemnej wnoszą się za pośrednictwem operatora pocztowego, w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe, osobiście, za pośrednictwem posłańca, a pisma w postaci elektronicznej wnoszą się przy użyciu środków komunikacji elektronicznej. 6. Terminy oblicza się według przepisów prawa cywilnego. 7. Jeżeli koniec terminu do wykonania czynności przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następnego po dniu lub dniach wolnych od pracy. 8. Odwołanie przysługuje na: 1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy; 2) zaniechanie czynności w

postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy; 3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia, mimo że zamawiający był do tego obowiązany. 9. Odwołanie wnosi się do Prezesa Izby. 10. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. 11. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej. 12. Odwołanie wnosi się 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. 13. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs 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. 14. Odwołanie w przypadkach innych niż określone w ust. 12 i 13 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) 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. 15. Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty 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; 2) 6 miesięcy od dnia zawarcia umowy, jeżeli zamawiający nie opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia.

Organizacja udzielająca dodatkowych informacji na temat postępowania o udzielenie zamówienia: Szpital Dziecięcy Polanki im. Macieja Płażyńskiego w Gdańsku sp. z o.o.

Organizacja zapewniająca dostęp offline do dokumentów zamówienia: Szpital Dziecięcy Polanki im. Macieja Płażyńskiego w Gdańsku sp. z o.o.

Organizacja udzielająca dodatkowych informacji na temat procedur odwoławczych: Prezes Krajowej Izby Odwoławczej

6. Wyniki

6.1. Wyniki – ID części zamówienia: LOT-0001

Status wyboru zwycięzcy: Nie wyłoniono zwycięzcy, a procedura konkurencyjna została zamknięta.

Powód, dla którego nie wyłoniono zwycięzcy: Decyzja nabywcy nie będąca następstwem wniosku oferenta o rewizję rozstrzygnięcia, z powodu błędów technicznych lub proceduralnych

6.1.4. Informacje statystyczne

Otrzymane oferty lub wnioski o dopuszczenie do udziału:

Rodzaj otrzymanych ofert lub wniosków: Oferty

Liczba otrzymanych ofert lub wniosków o dopuszczenie do udziału: 2
Rodzaj otrzymanych ofert lub wniosków: Oferty złożone drogą elektroniczną
Liczba otrzymanych ofert lub wniosków o dopuszczenie do udziału: 2
Rodzaj otrzymanych ofert lub wniosków: Oferty złożone przez mikro-, małych lub średnich oferentów
Liczba otrzymanych ofert lub wniosków o dopuszczenie do udziału: 2
Rodzaj otrzymanych ofert lub wniosków: Oferty złożone przez oferentów z siedzibą w państwach Europejskiego Obszaru Gospodarczego innych niż państwo nabywcy
Liczba otrzymanych ofert lub wniosków o dopuszczenie do udziału: 0
Rodzaj otrzymanych ofert lub wniosków: Oferty złożone przez oferentów z siedzibą w państwach spoza Europejskiego Obszaru Gospodarczego
Liczba otrzymanych ofert lub wniosków o dopuszczenie do udziału: 0

8. Organizacje

8.1. ORG-0001

Oficjalna nazwa: Szpital Dziecięcy Polanki im. Macieja Płazyńskiego w Gdańsku sp. z o.o.
Numer rejestracyjny: NIP:5842728762
Adres pocztowy: Polanki 119
Miejscowość: Gdańsk
Kod pocztowy: 80-308
Podpodział krajowy (NUTS): Gdański (PL634)
Kraj: Polska
E-mail: zamowienia@szpitalpolanki.pl
Telefon: 58 520 93 00
Faks: 58 552 47 41
Adres strony internetowej: <https://szpitalpolanki.ezamawiajacy.pl>
Adres na potrzeby wymiany informacji (URL): <https://szpitalpolanki.ezamawiajacy.pl>
Role tej organizacji:
Nabywca
Organizacja udzielająca dodatkowych informacji na temat postępowania o udzielenie zamówienia
Organizacja zapewniająca dostęp offline do dokumentów zamówienia

8.1. ORG-0002

Oficjalna nazwa: Prezes Krajowej Izby Odwoławczej
Numer rejestracyjny: NIP:5262239325
Adres pocztowy: Postępu 17A
Miejscowość: Warszawa
Kod pocztowy: 02-676
Podpodział krajowy (NUTS): Miasto Warszawa (PL911)
Kraj: Polska
E-mail: odwolania@uzp.gov.pl
Telefon: +48224587801
Adres strony internetowej: <https://www.uzp.gov.pl/kio/strona-glowna>
Adres na potrzeby wymiany informacji (URL): <https://www.uzp.gov.pl/kio/strona-glowna>
Role tej organizacji:
Organ odwoławczy
Organizacja udzielająca dodatkowych informacji na temat procedur odwoławczych

8.1. ORG-0000

Oficjalna nazwa: Publications Office of the European Union

Numer rejestracyjny: PUBL

Miejscowość: Luxembourg

Kod pocztowy: 2417

Podpodział krajowy (NUTS): Luxembourg (LU000)

Kraj: Luksemburg

E-mail: ted@publications.europa.eu

Telefon: +352 29291

Adres strony internetowej: <https://op.europa.eu>

Role tej organizacji:

TED eSender

Informacje o ogłoszeniu

Identyfikator/wersja ogłoszenia: 18804db5-cd72-414f-8522-815e0f00e764 - 01

Typ formularza: Wyniki

Rodzaj ogłoszenia: Ogłoszenie o udzieleniu zamówienia lub ogłoszenie o udzieleniu koncesji
– tryb standardowy

Podrodzaj ogłoszenia: 29

Ogłoszenie – data wysłania: 17/04/2026 07:54:34 (UTC+00:00) czas zachodnioeuropejski,
GMT

Języki, w których przedmiotowe ogłoszenie jest oficjalnie dostępne: polski

Numer publikacji ogłoszenia: 269371-2026

Numer wydania Dz.U. S: 76/2026

Data publikacji: 20/04/2026