

**Ogłoszenie o wyniku postępowania
Dostawy**

Działania zwiększające poziom cyberbezpieczeństwa szpitala: Ochrona stacji roboczych i serwerów poprzez zakup licencji, wdrożenie systemu oraz zakup usługi Usługa Centrum Operacji Bezpieczeństwa SOC .

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: KLINICZNE CENTRUM GINEKOLOGII, POŁOŻNICTWA I NEONATOLOGII W OPOLU

1.3.) Oddział zamawiającego: Zamówienia Publiczne

1.4) Krajowy Numer Identyfikacyjny: REGON 000640136

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Władysława Reymonta 8

1.5.2.) Miejscowość: Opole

1.5.3.) Kod pocztowy: 45-066

1.5.4.) Województwo: opolskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL524 - Opolski

1.5.7.) Numer telefonu: 77 441 77 63

1.5.9.) Adres poczty elektronicznej: zam-publ@ginekologia.opole.pl

1.5.10.) Adres strony internetowej zamawiającego: www.ginekologia.opole.pl

1.6.) Adres strony internetowej prowadzonego postępowania:

<https://platformazakupowa.pl/transakcja/1290754>

1.7.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - samodzielny publiczny zakład opieki zdrowotnej

1.8.) Przedmiot działalności zamawiającego: Zdrowie

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

Działania zwiększające poziom cyberbezpieczeństwa szpitala: Ochrona stacji roboczych i serwerów poprzez zakup licencji, wdrożenie systemu oraz zakup usługi Usługa Centrum Operacji Bezpieczeństwa SOC .

2.4.) Identyfikator postępowania: ocds-148610-aeb06718-cdde-4f00-bd56-859e8d8b0394

2.5.) Numer ogłoszenia: 2026/BZP 00302854

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-06-23

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2026/BZP 00037152/06/P

2.10.) Identyfikator pozycji planu postępowań:

1.2.5 Działania zwiększające poziom cyberbezpieczeństwa szpitala: Ochrona stacji roboczych i serwerów poprzez zakup licencji, wdrożenie systemu oraz zakup usługi Usługa Centrum Operacji Bezpieczeństwa SOC

2.11.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii

Europejskiej: Tak

2.12.) Nazwa projektu lub programu:

Rozwój usług cyfrowych w Klinicznym Centrum Ginekologii, Położnictwa i Neonatologii w Opolu w ramach programu Krajowy Plan Odbudowy i Zwiększania Odporności

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy:

Tak

2.14.) Numer ogłoszenia: 2026/BZP 00208256

SEKCJA III – TRYB UDZIELENIA ZAMÓWIENIA LUB ZAWARCIA UMOWY RAMOWEJ

3.1.) Tryb udzielenia zamówienia wraz z podstawą prawną Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Numer referencyjny: ZP.263.18.2026

4.2.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.4.) Rodzaj zamówienia: Dostawy

4.5.1.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia są działania zwiększające poziom cyberbezpieczeństwa szpitala: Ochrona stacji roboczych i serwerów poprzez zakup licencji, wdrożenie systemu oraz zakup usługi Usługa Centrum Operacji Bezpieczeństwa SOC. Szczegółowy opis i zakres przedmiotu zamówienia określony został w załączniku nr 1 do umowy oraz wzorze umowy. Zadanie realizowane w ramach projektu pt. „Rozwój usług cyfrowych w Klinicznym Centrum Ginekologii, Położnictwa i Neonatologii w Opolu” – Zadanie nr 9, 11 dofinansowane w ramach programu „Krajowy Plan Odbudowy i Zwiększania Odporności”, działanie „D1.1.2. Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”.

Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą DNSH.

Jeżeli przedmiot zamówienia obejmuje albo może obejmować produkt ICT, usługę ICT lub proces ICT, Wykonawca jest zobowiązany zaoferować wyłącznie takie produkty ICT, usługi ICT i procesy ICT, które na dzień składania ofert:

- 1) nie są wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;
- 2) nie obejmują produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usługi ICT lub procesu ICT określonych w tej decyzji.

4.5.3.) Główny kod CPV: 48000000-8 - Pakiety oprogramowania i systemy informatyczne

4.5.4.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72262000-9 - Usługi rozbudowy oprogramowania

48810000-9 - Systemy informacyjne

72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się unieważnieniem

5.2.) Podstawa prawna unieważnienia postępowania: art. 255 pkt 5 ustawy

5.2.1.) Przyczyna unieważnienia postępowania:

Wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć.

Uzasadnienie faktyczne:

Zamówienie jest współfinansowane ze środków programu „Krajowy Plan Odbudowy i Zwiększania Odporności”, działanie „D1.1.2. Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia” w ramach realizacji projektu pt. „Rozwój usług cyfrowych w Klinicznym Centrum Ginekologii, Położnictwa i Neonatologii w Opolu” – Zadanie nr 9, 11, dla którego ostatecznym, sztywnym terminem zakończenia całego projektu jest dzień 15.07.2026 r. Dodatkowo powyższe zamówienie - Ochrona stacji roboczych i serwerów poprzez zakup licencji, wdrożenie systemu oraz zakup usługi Usługa Centrum Operacji Bezpieczeństwa SOC, powiązane jest ściśle z wykonaniem

Audytu końcowego w obszarze cyberbezpieczeństwa, weryfikującego prawidłowość wdrożeń rozwiązań w zakresie ochrony danych i systemów informatycznych. W celu terminowego wykonania czynności audytowych tj. do dnia 15 lipca 2026 r., ww. wdrożenie powinno się zakończyć najpóźniej do dnia 10 lipca 2026 r. Zamawiający oparł harmonogram o realne ramy czasowe, które pozwalały na terminowe wykonanie zamówienia i bezpieczne rozliczenie środków publicznych.

Postępowanie

W toku postępowania zaistniały jednak niezależne od woli Zamawiającego okoliczności o charakterze proceduralnym, których czasu trwania nie sposób było obiektywnie przewidzieć na etapie przygotowywania postępowania.

Wobec czynności Zamawiającego polegającej na unieważnieniu postępowania w dniu 14.05.2026 r., z uwagi na zidentyfikowane kwestie związane z opisem przedmiotu zamówienia (OPZ), jeden z Wykonawców, tj. Cyber 360 Sp. z o.o., ul. Władysława IV 43/414-415, 81-308 Gdynia, wniósł odwołanie do Krajowej Izby Odwoławczej w dniu 19.05.2026 r. (sygn. akt KIO 2411/26), do którego następnie przystąpił drugi z Wykonawców, tj. IT Systems and Solutions Sp. z o.o., ul. Syta 68A; 02-993 Warszawa. Działając w celu poszanowania zasad

ekonomii procesowej oraz dążąc do jak najszybszego naprawienia sytuacji, Zamawiający w całości uwzględnił zarzuty przedstawione w odwołaniu. W konsekwencji powyższego, Krajowa Izba Odwoławcza postanowieniem z dnia 27.05.2026 r. miała umorzyć postępowanie odwoławcze, o czym Zamawiający powziął póki co jedynie nieformalną informację (opublikowaną na stronie Urzędu Zamówień Publicznych), oczekując w dalszym ciągu na doręczenie postanowienia zapadłego na posiedzeniu niejawnym.

Zgodnie z przepisami ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 z późn. zm.), w szczególności art. 577 ww. ustawy a contrario, Zamawiający niezwłocznie unieważnił swoją poprzednią czynność i przystąpił do ponownego badania i oceny ofert.

Niemniej jednak, opisany powyżej skomplikowany proces odwoławczo-proceduralny przed KIO doprowadził do znacznego i nieprzewidzianego upływu czasu. Od momentu wniesienia odwołania do dnia zakończenia ponownej oceny ofert minęło łącznie 28 dni. Ten dodatkowy okres sprawił, że pierwotny harmonogram inwestycji stał się całkowicie nierealny.

SEKCJA IX INFORMACJE DODATKOWE

Biorąc pod uwagę:

1. minimalny czas potrzebny na ewentualne dalsze czynności (np. upływ terminów na wniesienie kolejnych środków ochrony prawnej),
2. konieczność odczekania na doręczenie postanowienia KIO z dnia 27.05.2026 r.
3. czas niezbędny na podpisanie umowy,
4. czas na faktyczną realizację zamówienia wynoszący do 10 dni roboczych

najwcześniejszy możliwy termin zakończenia realizacji zadania przypadłby na dzień 20 lipca 2026 r. (przy uwzględnieniu minimalnego czasu wynikającego z ewentualnego skorzystania przez którykolwiek z uprawnionych podmiotów ze środków ochrony prawnej). Termin ten wykracza poza granice czasowe projektu finansowanego ze środków zewnętrznych, co oznacza, że zadanie zakończyłoby się po terminie jego realizacji. Opisany stan rzeczy stanowi istotną zmianę okoliczności, której Zamawiający – pomimo dołożenia należytej staranności – nie mógł wcześniej przewidzieć na etapie wszczynania postępowania. Zamawiający nie miał bowiem wpływu na czas trwania procedury przed KIO ani na moment, w którym sprawa formalnie powróci na etap oceny ofert.

Dalsze prowadzenie postępowania i podpisanie umowy w takich warunkach nie leży w interesie publicznym. Kontynuowanie procedury skutkowałoby realizacją zadania, którego koszty (wobec utraty dofinansowania zewnętrznego na skutek przekroczenia terminów) musiałyby zostać w 100% pokryte ze środków własnych Zamawiającego, który nie zaplanował przeznaczenia takich środków na taki cel. Doprowadziłoby to do rażącego naruszenia dyscypliny finansów publicznych oraz zasad celowości, gospodarności i oszczędności w dysponowaniu środkami publicznymi. Interes publiczny nakazuje w tym miejscu ochronę budżetu przed tak drastycznym i nieuzasadnionym obciążeniem.

Zgodnie z ugruntowanym orzecznictwem, interes publiczny należy rozumieć m.in. jako dbałość o celowe, oszczędne i racjonalne wydatkowanie środków publicznych. Realizacja zadania po terminie ważności projektu i utrata finansowania zewnętrznego drastycznie narusza te zasady i godzi w szeroko pojęty interes społeczny. W związku z tym, dalsze prowadzenie postępowania i doprowadzenie do podpisania umowy stało się nieuzasadnione, a wykonanie zamówienia w obecnych realiach uderza w interes publiczny. Unieważnienie postępowania jest w tej sytuacji konieczne i uzasadnione. Mając na uwadze łącznie spełnienie wszystkich przesłanek z art. 255 pkt 5 ustawy Pzp, unieważnienie przedmiotowego postępowania stało się w pełni uzasadnione i konieczne.