Sygn. akt KIO/W 60/26

POSTANOWIENIE
z 16 marca 2026 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Agnieszka Trojanowska

Po rozpoznaniu na posiedzeniu niejawnym 16 marca 2026 r. w Warszawie wniosku z 13 marca 2026 r. o uchylenie zakazu zawarcia umowy do czasu ogłoszenia przez Krajową Izbę Odwoławczą wyroku lub postanowienia kończącego postępowanie odwoławcze, wniesionego przez Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mławie, ul. A.D. 1 w postępowaniu prowadzonym w trybie przetargu nieograniczonego na podstawie art. 138 ust. 2 pkt 2 ustawy PZP pn. „Rozbudowa systemów IT SPZOZ w Mławie" Numer postępowania: SPZOZ ZP-5/2026 ogłoszonego w Dzienniku Urzędowym Unii Europejskiej pod numerem Dz.U. S 30/2026 102987-2026 12 lutego 2026 r.

postanawia:

uchylić zakaz zawarcia umowy.

Przewodnicząca: ……..

Uzasadnienie

13 marca 2026 r. zamawiający Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mławie, ul. A.D. 1 wniósł o uchylenie zakazu zawarcia umowy w ww. postępowaniu o udzielenie zamówienia publicznego, o którym mowa w art. 577 ustawy

W uzasadnieniu wniosku podał, że postępowanie dotyczy realizacji projektu współfinansowanego ze środków UE w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia", Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia" finansowych przez Ministerstwo Zdrowia z Krajowego Planu Odbudowy (KPO), którego termin realizacji upływa w dniu 31 maja 2026 r. Umowa o dofinansowanie nakłada na zamawiającego obowiązek zakończenia rzeczowej realizacji projektu w określonym terminie, pod rygorem utraty dofinansowania.

Wniesione odwołanie powoduje, że zamawiający nie może zawrzeć umowy z wykonawcami do momentu rozpoznania odwołania wniesionego przez firmę SUNTAR Sp. z o.o. Zamawiający zwrócił uwagę, że w powyższej sprawie dopiero dzisiaj została nadana sygnatura odwołania, a zatem nie jest nawet wiadomy przybliżony termin jego rozpatrzenia. Uzasadnia to przekonanie, że wstrzymanie się z zawarciem umów z wykonawcami do momentu rozpoznania odwołania spowoduje niemożliwość realizacji inwestycji ze środków z KPO.

W przypadku wstrzymania zawarcia umowy wykonawca nie będzie mógł rozpocząć realizacji projektu, zagrożony zostanie harmonogram rzeczowo-finansowy przez co istnieje realne ryzyko utraty finansowania. Utrata dofinansowania oznaczałaby konieczność pokrycia całości kosztów inwestycji z budżetu szpitala, co bezpośrednio wpłynie na możliwość realizacji świadczeń zdrowotnych. Szacunkowy koszt wymaganych modernizacji i zakupów nowych rozwiązań przekracza znacznie możliwości finansowe Szpitala, dlatego jedyną możliwością realizacji zadania było skorzystanie z dofinansowania w ramach projektu. Nie ulega zatem wątpliwości, że utrata dofinansowania spowoduje, że zamawiający nie będzie w stanie kontynuować projektu.

Jednocześnie wskazał, że umowa ze Skarbem Państwa – Ministrem Zdrowia dotycząca objęcia zamawiającego wsparciem została zawarta w dniu 15 stycznia 2026 r., a termin realizacji przedmiotowego zamówienia upływa w dniu 31 maja 2026 r. Po zawarciu wskazanej umowy zamawiający niezwłocznie przystąpił do opracowania dokumentacji przetargowej, w tym opisu przedmiotu zamówienia, którego przygotowanie – z uwagi na złożony charakter zamówienia – wymagało odpowiedniego nakładu czasu.

Nie zawarcie umowy w przedmiotowym postępowaniu może spowodować poważne negatywne skutki dla interesu publicznego, polegające w szczególności na:

- zagrożeniu ciągłości działania systemów informatycznych obsługujących dokumentację medyczną (EDM), rejestrację pacjentów oraz systemy laboratoryjne i diagnostyczne,
- ryzyku utraty lub ograniczenia dostępu do danych medycznych pacjentów, co może bezpośrednio wpływać na bezpieczeństwo zdrowotne i życie pacjentów,
- braku możliwości integracji systemów z platformą e-Zdrowie (P1), co może skutkować naruszeniem obowiązków ustawowych szpitala,
- ryzyku utraty dofinansowania (jeżeli dotyczy – np. środki UE / KPO), w przypadku niedotrzymania harmonogramu realizacji projektu.

Systemy IT w podmiocie leczniczym stanowią infrastrukturę krytyczną dla zapewnienia ciągłości świadczeń zdrowotnych. Opóźnienie realizacji zamówienia może skutkować dezorganizacją pracy oddziałów szpitalnych, wydłużeniem czasu obsługi pacjentów oraz zwiększeniem ryzyka błędów medycznych.

SPZOZ w Mławie dokonał analizy potrzeb w celu przygotowania Dokumentacji Technicznej dla projektu „Rozbudowa systemów IT SPZOZ w Mławie". W dokumentacji zostały określone potrzeby w zakresie wymiany i wdrożenia systemów oraz modernizacji sprzętu komputerowego. Ponadto wykazano, że realizacja projektu jest niezbędna dla dalszej realizacji działań statutowych Szpitala. Realizacja projektu, pozwoli na kontynuację udzielania usług medycznych zgodnie z wymogami prawa. Procesy związane z realizacją usług będą wspierane przez funkcjonalności związane z realizacją zadań statutowych – tj. świadczenia medyczne.

Projekt ma na celu gruntowną transformację cyfrową placówki, zwiększenie dostępności, jakości i efektywności świadczeń medycznych na wysokim poziomie bezpieczeństwa. W odpowiedzi na rosnące potrzeby pacjentów i wyzwania współczesnej medycyny, projekt koncentruje się na cyfryzacji procesów wewnętrznych oraz rozszerzeniu katalogu e-usług medycznych. Głównym celem jest stworzenie nowoczesnego ekosystemu cyfrowego, który usprawni codzienne funkcjonowanie szpitala i poprawi doświadczenia pacjentów.

Ostatnie znaczące dofinansowanie infrastruktury informatycznej szpitala zostało pozyskane w 2017 roku. Od tego czasu znaczna część zakupionego wówczas sprzętu oraz oprogramowania uległa istotnemu zużyciu technologicznemu i nie spełnia już aktualnych standardów wydajności, bezpieczeństwa oraz interoperacyjności systemów ochrony zdrowia. Brak realizacji obecnego projektu oznaczałby konieczność dalszej pracy na przestarzałej infrastrukturze, co niesie ze sobą ryzyko: spadku wydajności systemów obsługujących procesy medyczne i administracyjne, zwiększonej awaryjności sprzętu, ograniczonej możliwości integracji z nowymi systemami krajowymi oraz usługami cyfrowymi w ochronie zdrowia, wzrostu zagrożeń w obszarze cyberbezpieczeństwa.

Jednym z kluczowych elementów planowanej inwestycji jest wdrożenie nowego systemu laboratoryjnego, który zastąpi obecnie funkcjonujące rozwiązanie informatyczne. Aktualny

system laboratoryjny wykorzystywany w szpitalu będzie objęty wsparciem producenta jedynie do końca bieżącego roku, co oznacza, że w niedługim czasie szpital utraci możliwość korzystania z aktualizacji, poprawek bezpieczeństwa oraz wsparcia technicznego. Dalsze funkcjonowanie systemu bez wsparcia producenta stwarza istotne ryzyko dla ciągłości pracy laboratorium oraz bezpieczeństwa przetwarzanych danych medycznych. Nowy system laboratoryjny planowany w ramach projektu umożliwi między innymi: integrację z systemem szpitalnym, usprawnienie procesu obsługi badań diagnostycznych, udostępnienie wyników badań laboratoryjnych on-line dla pacjentów, co znacząco poprawi dostępność informacji medycznej i komfort pacjentów. Rozwiązanie to wpisuje się w kierunek rozwoju cyfrowych usług w ochronie zdrowia oraz oczekiwania społeczne dotyczące dostępu do dokumentacji medycznej w formie elektronicznej.

Projekt przewiduje również wdrożenie rozwiązań opartych na sztucznej inteligencji wspierających diagnostykę obrazową, które umożliwią szybszą analizę badań oraz przyspieszą proces ich opisu przez lekarzy. Dzięki temu pacjenci mogliby otrzymywać wyniki badań diagnostycznych w krótszym czasie. Brak realizacji projektu oznacza utratę tej możliwości i dalsze funkcjonowanie w oparciu o mniej wydajne procesy diagnostyczne.

Projekt zakłada również rozszerzenie zakresu Elektronicznej Dokumentacji Medycznej (EDM) poprzez wdrożenie nowych typów dokumentów medycznych w formie elektronicznej. Rozwiązanie to ułatwi pacjentom dostęp do własnej dokumentacji medycznej (dostęp on-line, którego aktualne systemy szpitalne nie przewidują), usprawni jej wymianę pomiędzy placówkami medycznymi oraz ograniczy konieczność dostarczania dokumentacji w formie papierowej.

Istotnym elementem projektu jest znaczące podniesienie poziomu cyberbezpieczeństwa infrastruktury informatycznej szpitala. W ramach inwestycji planowany jest zakup i wdrożenie nowoczesnych systemów bezpieczeństwa, w tym rozwiązań klasy SIEM, PAM, XDR, a także nowych urządzeń UTM wraz z zakupionym kilkuletnim wsparciem producenta. Rozwiązania te umożliwią skuteczne monitorowanie zdarzeń bezpieczeństwa, kontrolę dostępu uprzywilejowanego oraz szybsze wykrywanie i reagowanie na incydenty cyberbezpieczeństwa. Projekt obejmuje również aktualizację systemów wszystkich serwerów funkcjonujących w infrastrukturze szpitala, co pozwoli na usunięcie znanych podatności oraz zwiększenie stabilności działania systemów medycznych i administracyjnych. Dodatkowo przewidziano szkolenia z zakresu cyberbezpieczeństwa dla administratorów oraz pracowników szpitala, których celem jest podniesienie świadomości zagrożeń oraz poprawa zdolności reagowania na incydenty bezpieczeństwa. Brak realizacji projektu oznaczałby pozostawienie szpitala z przestarzałą infrastrukturą bezpieczeństwa, nieadekwatną do obecnych zagrożeń w cyberprzestrzeni.

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Mławie jest kluczową placówką medyczną zapewniającą opiekę zdrowotną mieszkańcom powiatu mławskiego i okolicznych powiatów. Realizacja przedmiotowej inwestycji ma bezpośredni wpływ na poprawę jakości i dostępności świadczeń zdrowotnych, bezpieczeństwo przetwarzania danych medycznych oraz rozwój nowoczesnych usług cyfrowych dla pacjentów.

Jeżeli projekt nie zostanie zrealizowany z powodu utraty dofinansowania, konsekwencje odczują przede wszystkim pacjenci korzystający ze świadczeń zdrowotnych, którzy utracą możliwość korzystania z nowoczesnych usług cyfrowych, które miały zostać wdrożone w ramach projektu.

W szczególności nie będzie możliwe uruchomienie funkcjonalności udostępniania wyników badań laboratoryjnych on-line, co oznacza konieczność osobistego odbierania wyników w placówce lub dłuższe oczekiwanie na ich przekazanie. Brak realizacji inwestycji oznacza również wolniejszą obsługę pacjentów, wynikającą z dalszego korzystania z przestarzałych systemów informatycznych. Nowa infrastruktura informatyczna miała usprawnić wymianę informacji pomiędzy oddziałami, laboratorium oraz personelem medycznym, co przekłada się na szybszy dostęp lekarzy do wyników badań oraz dokumentacji medycznej pacjentów. Pacjenci stracą także wyższy poziom bezpieczeństwa swoich danych medycznych, który miał zostać osiągnięty dzięki wdrożeniu nowoczesnych systemów cyberbezpieczeństwa oraz modernizacji infrastruktury serwerowej. Dane medyczne należą do informacji szczególnie wrażliwych, dlatego zapewnienie ich odpowiedniej ochrony ma kluczowe znaczenie dla bezpieczeństwa pacjentów. W praktyce oznacza to, że utrata dofinansowania doprowadzi do sytuacji, w której pacjenci będą nadal korzystać z usług świadczonych w oparciu o przestarzałą infrastrukturę informatyczną, a planowane usprawnienia w zakresie dostępności informacji medycznej, szybkości obsługi oraz bezpieczeństwa danych nie zostaną wdrożone.

Dodatkowym istotnym ryzykiem związanym z przedłużaniem procedury zawarcia umowy są zmiany cen na rynku sprzętu informatycznego. Opóźnienia wynikające z wniesienia odwołania powodują przesunięcie w czasie rozpoczęcia realizacji zamówienia, co w praktyce może prowadzić do wzrostu cen urządzeń komputerowych, serwerów oraz infrastruktury sieciowej, które stanowią kluczowy element planowanej inwestycji.

Rynek sprzętu IT charakteryzuje się dużą dynamiką cen, wynikającą m.in. ze zmian kursów walut, kosztów komponentów elektronicznych oraz globalnych łańcuchów dostaw. Wydłużenie procedur formalnych może spowodować sytuację, w której ceny urządzeń niezbędnych do realizacji projektu wzrosną w stosunku do poziomu przyjętego w ofercie wykonawcy.

W konsekwencji może to doprowadzić do sytuacji, w której realizacja projektu w pierwotnie założonym zakresie nie będzie możliwa w ramach dostępnego budżetu, co w skrajnym przypadku może zagrozić prawidłowemu wykonaniu inwestycji finansowanej ze środków Krajowy Plan Odbudowy i Zwiększania Odporności. Z tego względu niezwłoczne umożliwienie

zawarcia umowy z wykonawcą ma istotne znaczenie również z punktu widzenia stabilności finansowej i możliwości utrzymania założonego budżetu projektu.
Porównanie interesu publicznego z interesem odwołującego.
Jednocześnie zamawiający wskazał, że interes odwołującego ma charakter majątkowy i potencjalny. Natomiast interes publiczny w niniejszej sprawie obejmuje bezpieczeństwo zdrowotne pacjentów, ich danych osobowych, w tym w szczególności jakże wrażliwych danych w postaci dokumentacji medycznej, ciągłość świadczeń opieki zdrowotnej, a także ochronę środków publicznych.
Skutki nie zawarcia umowy mają charakter realny, bezpośredni i nieodwracalny (utrata finansowania, dezorganizacja pracy szpitala), podczas gdy ewentualne uwzględnienie odwołania może zostać skompensowane środkami przewidzianymi w ustawie.
W ocenie zamawiającego w sprawie zachodzą szczególne okoliczności uzasadniające uwzględnienie wniosku zamawiającego, a dalsze wstrzymywanie zawarcia umowy mogłoby prowadzić do poważnych i trudnych do odwrócenia skutków, sprzecznych z interesem publicznym.
Szpital podejmuje działania mające na celu przeciwdziałanie incydentom związanym z cyberbezpieczeństwem poprzez wdrożenie nowoczesnych systemów zabezpieczających infrastrukturę informatyczną. W ramach projektu planowany jest zakup specjalistycznych rozwiązań bezpieczeństwa, które umożliwią skuteczniejsze wykrywanie zagrożeń, monitorowanie zdarzeń oraz szybsze reagowanie na potencjalne ataki cybernetyczne. Celem tych działań jest zapewnienie ciągłości działania systemów medycznych oraz ochrona wrażliwych danych pacjentów.
Potrzeba realizacji takich działań wynika również z realnych zagrożeń, jakie w ostatnim czasie dotknęły placówki ochrony zdrowia. Przykładem jest niedawny incydent cyberbezpieczeństwa w Szpitalu Wojewódzkim w Szczecinie, gdzie w nocy z 7 na 8 marca 2026 roku doszło do ataku z wykorzystaniem oprogramowania typu ransomware. W wyniku ataku część systemów informatycznych została sparaliżowana, co znacząco utrudniło funkcjonowanie placówki oraz dostęp pacjentów do świadczeń medycznych.
Opisane zdarzenie pokazuje, że placówki ochrony zdrowia stanowią obecnie jeden z głównych celów cyberataków, a brak odpowiednich zabezpieczeń może prowadzić do poważnych zakłóceń w udzielaniu świadczeń zdrowotnych. Dlatego planowana inwestycja w systemy cyberbezpieczeństwa ma na celu ograniczenie ryzyka wystąpienia podobnych incydentów oraz zapewnienie pacjentom stabilnego i bezpiecznego dostępu do usług medycznych.
Nadużycie prawa do odwołania.
W ocenie zamawiającego całokształt okoliczności niniejszej sprawy wskazuje, że wniesione odwołanie stanowi przejaw instrumentalnego korzystania ze środków ochrony prawnej i zostało złożone przede wszystkim w celu uniemożliwienia zawarcia umowy przez

zamawiającego, a nie w celu rzeczywistej ochrony interesu odwołującego w uzyskaniu zamówienia.

Zamawiający podkreślił, że instytucja odwołania przewidziana w przepisach ustawy – Prawo zamówień publicznych służy zapewnieniu wykonawcom realnej ochrony ich interesu w uzyskaniu zamówienia w sytuacji naruszenia przepisów ustawy przez zamawiającego. Środki ochrony prawnej nie mogą jednak być wykorzystywane w sposób sprzeczny z ich celem, w szczególności jako instrument o charakterze obstrukcyjnym, zmierzający wyłącznie do blokowania możliwości zawarcia umowy przez zamawiającego i realizacji zamówienia publicznego. W orzecznictwie Krajowej Izby Odwoławczej wielokrotnie podkreślano, że korzystanie ze środków ochrony prawnej powinno pozostawać w związku z rzeczywistym interesem wykonawcy w uzyskaniu zamówienia oraz nie może stanowić przejawu nadużycia prawa podmiotowego.

W tej sprawie na instrumentalny charakter odwołania wskazuje szereg okoliczności. Po pierwsze, odwołujący nie wykazywał żadnej aktywności w toku postępowania poprzedzającego wniesienie odwołania. W szczególności nie kierował do zamawiającego pytań dotyczących treści dokumentacji postępowania ani nie zgłaszał wniosków o jej wyjaśnienie lub zmianę. W praktyce postępowań o udzielenie zamówienia publicznego wykonawcy, którzy rzeczywiście dostrzegają w dokumentacji postępowania nieprawidłowości lub postanowienia utrudniające im ubieganie się o zamówienie, w pierwszej kolejności korzystają z instytucji pytań do specyfikacji warunków zamówienia. Brak jakiejkolwiek aktywności odwołującego na tym etapie postępowania wskazuje, że podnoszone w odwołaniu zarzuty nie stanowią konsekwencji rzeczywistej analizy dokumentacji postępowania ani reakcji na dostrzeżone naruszenia.

Po drugie, treść odwołania zawiera fragmenty argumentacji oraz sformułowania, które nie odnoszą się do przedmiotowego postępowania. Analiza uzasadnienia odwołania wskazuje, że część zawartych w nim twierdzeń dotyczy okoliczności, które nie występują w tym postępowaniu, co prowadzi do wniosku, że odwołanie zostało sporządzone w sposób schematyczny, z wykorzystaniem treści odnoszących się do innych postępowań. Okoliczność ta podważa wiarygodność zarzutów oraz wskazuje, że odwołanie nie zostało przygotowane w oparciu o rzeczywistą analizę dokumentacji niniejszego postępowania. Jako przykład można tu przytoczyć chociażby zarzuty dotyczące modelu komputera Dell Optiplex 7420, którego zamawiający nie opisuje w swojej dokumentacji. Specyfikacja przetargowa nie pasowała do modelu Optiplex 7420, a zostało to wykorzystane jako argument przeciwko Szpitalowi w odwołaniu.

Po trzecie, postępowanie o udzielenie zamówienia zostało podzielone na cztery odrębne części:

1. Część 1 – Rozbudowa HIS i PACS;

2. Część 2 – Wdrożenie systemu laboratoryjnego;
3. Część 3 – Szkolenie pracowników;
4. Część 4 – Sprzęt i oprogramowanie systemowe.

Odwołujący w treści odwołania formułuje zastrzeżenia wyłącznie w odniesieniu do części 4 postępowania, obejmującej dostawę sprzętu oraz oprogramowania systemowego. Pomimo tego odwołanie zostało wniesione w odniesieniu do całego postępowania – w petitum odwołania brak jest wskazania, aby dotyczyło ono wyłącznie określonej części zamówienia. W konsekwencji formalny zakres odwołania obejmuje wszystkie cztery części postępowania.

Takie ukształtowanie zakresu odwołania prowadzi do wniosku, że rzeczywistym jego skutkiem jest wstrzymanie możliwości zawarcia umów w całym postępowaniu, pomimo że zarzuty odnoszą się jedynie do jednej jego części. W ocenie zamawiającego okoliczność ta wskazuje, że celem działania odwołującego nie jest wyłącznie zakwestionowanie określonych postanowień dotyczących części 4 zamówienia, lecz doprowadzenie do zablokowania realizacji całego postępowania.

Zamawiający podkreślił, że poszczególne części zamówienia – choć formalnie wyodrębnione – pozostają ze sobą w ścisłym związku funkcjonalnym i technologicznym. W szczególności realizacja części 4 obejmującej dostawę sprzętu oraz oprogramowania systemowego stanowi warunek konieczny dla uruchomienia i prawidłowego funkcjonowania systemów informatycznych będących przedmiotem części 1 i 2 zamówienia. Systemy te wymagają odpowiedniej infrastruktury sprzętowej i systemowej umożliwiającej ich instalację, konfigurację, integrację oraz przeprowadzenie testów funkcjonalnych. Brak dostawy tej infrastruktury uniemożliwiłby wykonawcom realizującym części 1 i 2 dokonanie wdrożenia systemów w środowisku docelowym.

Brak realizacji części 4 uniemożliwiłby również przeprowadzenie w sposób rzeczywisty szkoleń przewidzianych w części 3 zamówienia, które powinny odbywać się w docelowym środowisku systemowym, na wdrożonych rozwiązaniach informatycznych. W konsekwencji brak zawarcia umowy w zakresie części 4 prowadziłby do sytuacji, w której wykonanie pozostałych części zamówienia byłoby w praktyce niemożliwe lub pozbawione gospodarczego sensu.

Uwzględniając wszystkie wskazane powyżej okoliczności należy uznać, że wniesione odwołanie ma charakter instrumentalny i zmierza przede wszystkim do uniemożliwienia Zamawiającemu zawarcia umowy i realizacji zamówienia. Takie korzystanie ze środków ochrony prawnej pozostaje sprzeczne z ich celem oraz stanowi przejaw nadużycia prawa podmiotowego.

Kwestie merytoryczne związane z odwołaniem.

Odnosząc się do zarzutów odwołującego zawartych w odwołaniu, a dotyczących treści opisu przedmiotu zamówienia, zamawiający wskazał, że stanowią one jedynie polemikę z przyjętym

przez zamawiającego sposobem określenia jego potrzeb, wyrażonych w Specyfikacji Warunków Zamówienia. Zarzuty te nie wskazują na rzeczywiste naruszenie przepisów ustawy – Prawo zamówień publicznych, lecz zmierzają do zakwestionowania przyjętych przez zamawiającego rozwiązań technicznych oraz organizacyjnych, które wynikają z obiektywnie uzasadnionych potrzeb zamawiającego związanych z realizacją planowanej inwestycji.

Zamawiający ma prawo określić przedmiot zamówienia w sposób odpowiadający jego rzeczywistym potrzebom oraz celom, jakie zamierza osiągnąć przez realizację zamówienia. Uprawnienie to znajduje potwierdzenie w utrwalonym orzecznictwie Krajowej Izby Odwoławczej. Można przytoczyć m.in.:

„Zamawiający ma prawo tak określić przedmiot zamówienia, aby opisać go adekwatnie do wyznaczonego celu, zachowując jednocześnie obiektywizm i precyzję w formułowaniu swoich potrzeb. Nie narusza przepisów p.z.p. sporządzenie opisu przedmiotu zamówienia, który uwzględnia potrzeby zamawiającego, nawet jeżeli utrudnia lub uniemożliwia niektórym podmiotom dostęp do zamówienia. Obowiązek zachowania zasady uczciwej konkurencji nie oznacza, iż zamawiający nie może opisać przedmiotu zamówienia w sposób odzwierciedlający jego potrzeby" – Wyrok Krajowej Izby Odwoławczej z dnia 19 stycznia 2023 r., sygn. Akt: KIO 3536/22,

„Izba podziela pogląd wielokrotnie prezentowany w orzecznictwie Krajowej Izby Odwoławczej, iż nie narusza przepisów ustawy Pzp sporządzenie opisu przedmiotu zamówienia, który uwzględnia potrzeby zamawiającego, nawet jeżeli utrudnia lub uniemożliwia niektórym podmiotom dostęp do zamówienia" - Wyrok Krajowej Izby Odwoławczej z dnia 7 września 2020 r, sygn. Akt: KIO 1592/20.

Wymagania określone w SWZ zostały sformułowane w celu zapewnienia kompatybilności zamawianego sprzętu i oprogramowania z infrastrukturą informatyczną, która jest już eksploatowana przez zamawiającego. Zamawiający dysponuje określonym środowiskiem technicznym obejmującym zarówno sprzęt, jak i oprogramowanie systemowe oraz aplikacyjne, które stanowią podstawę funkcjonowania systemów informatycznych wykorzystywanych w bieżącej działalności jednostki. W związku z powyższym opis przedmiotu zamówienia musiał uwzględniać konieczność zapewnienia prawidłowej współpracy nowo dostarczanych elementów infrastruktury z rozwiązaniami już funkcjonującymi u zamawiającego.

Ponadto rozwiązania przewidziane w SWZ zostały określone w sposób obiektywny i wynikają z potrzeby zapewnienia odpowiedniego standardu infrastruktury technicznej oraz bezpieczeństwa i stabilności funkcjonowania systemów informatycznych wdrażanych w ramach realizowanego przedsięwzięcia. Zamawiający jest zobowiązany do takiego ukształtowania wymagań technicznych, aby zagwarantować prawidłową realizację projektu oraz jego trwałość w perspektywie wieloletniej eksploatacji.

Jednocześnie zamawiający wskazał, że wymagania określone w SWZ nie mają charakteru dyskryminującego ani nie prowadzą do ograniczenia konkurencji w sposób nieuzasadniony. Rozwiązania przewidziane przez zamawiającego mogą zostać spełnione przez wielu producentów i dostawców obecnych na rynku. Potwierdzeniem powyższego jest fakt, że w tym postępowaniu wpłynęło wiele ofert, co jednoznacznie świadczy o realnym poziomie konkurencji oraz o tym, że wymagania zamawiającego nie stanowią bariery uniemożliwiającej udział w postępowaniu.

Odwołujący nie zgłosił w toku postępowania żadnych pytań ani wniosków o wyjaśnienie lub zmianę treści SWZ. Brak jakiejkolwiek aktywności odwołującego na etapie wyjaśniania dokumentacji postępowania wskazuje, że podnoszone obecnie zarzuty nie stanowią reakcji na rzeczywiście istniejące wątpliwości dotyczące treści dokumentacji, lecz zostały sformułowane dopiero na etapie wniesienia odwołania. Okoliczność ta dodatkowo potwierdza, że zarzuty odwołującego mają charakter polemiczny wobec przyjętego przez zamawiającego sposobu opisania jego potrzeb, które zamawiający uznaje za obiektywnie uzasadnione i pozostające w zgodzie z przepisami ustawy.

Zamawiający podkreślił przy tym, że jest w stanie szczegółowo wykazać zasadność przyjętych rozwiązań oraz ich związek z rzeczywistymi potrzebami zamawiającego na dalszym etapie postępowania odwoławczego.

W ocenie zamawiającego utrzymanie zakazu zawarcia umowy w niniejszej sprawie prowadziłoby do poważnego zagrożenia dla interesu publicznego, polegającego na utracie znacznych środków finansowych przeznaczonych na rozwój infrastruktury ochrony zdrowia oraz na zahamowaniu procesu modernizacji systemów informatycznych szpitala. W związku z tym, zasadne jest uchylenie zakazu zawarcia umowy, co umożliwi niezwłoczne rozpoczęcie realizacji projektu oraz zwiększy prawdopodobieństwo jego terminowego zakończenia i rozliczenia

Ustalenia KIO:

UMOWA NR KPOD.07.03-IP.10-0474/25/KPO/1084/2025/747 o objęcie wsparciem z planu rozwojowego przedsięwzięcia

§ 2.

1. Instytucja odpowiedzialna za realizację inwestycji obejmuje wsparciem bezzwrotnym z planu rozwojowego przedsięwzięcie pn. „Rozbudowa systemów IT SPZOZ w Mławie” w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”, a Ostateczny odbiorca wsparcia zobowiązuje się to przedsięwzięcie zrealizować.

2. Przedsięwzięcie, o którym mowa w ust. 1, realizowane jest zgodnie z: wnioskiem stanowiącym załącznik nr 3 do Umowy oraz harmonogramem stanowiącym załącznik nr 4 do Umowy i obejmuje następujące zadania:

1) integracja i rozbudowa systemów informatycznych świadczeniodawcy (wskaźnik D21G) w tym integracja systemów szpitalnych z systemem P1 (wskaźnik D21G.R1);
2) digitalizacja dokumentacji medycznej istotnej z punktu widzenia leczenia i profilaktyki (wskaźnik D18G) w tym karty informacyjne z leczenia szpitalnego w postaci elektronicznej dokumentacji medycznej od 1 stycznia 2023 r. do 31 grudnia 2025 r. zaindeksowane w systemie P1 lub umieszczone w centralnym repozytorium danych medycznych w Centrum e-Zdrowia (wskaźnik D18G.R1);
3) działania zwiększające poziom cyberbezpieczeństwa szpitala (wskaźnik D21 G) w tym zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej potwierdzone audytem bezpieczeństwa (wskaźnik D21G.R2);
4) wdrożenie rozwiązań AI i podłączenie do centralnego repozytorium danych medycznych (wskaźnik D 21G) w tym podłączenie do Platformy Usług Inteligentnych (PUI) w Centrum e-Zdrowia (wskaźnik D21G.R3).
4. Realizacja przedsięwzięcia, o którym mowa w ust. 1, zakończy się do 31 maja 2026 r., przy czym termin ten może zostać wydłużony w przypadku wydłużenia terminów realizacji poszczególnych kamieni milowych i/lub wskaźników w ramach rewizji Krajowego Planu Odbudowy i Zwiększania Odporności.
5. W przypadku wydłużenia terminu realizacji przedsięwzięcia, zastosowanie znajduje treść § 20 ust. 3 niniejszej Umowy.
6. Trwałość przedsięwzięcia finansowanego ze środków planu rozwojowego w ramach inwestycji D1.1.2 musi być zachowana przez okres 3 lat od daty zatwierdzenia przez Instytucję odpowiedzialną za realizację Inwestycji wniosku końcowego o płatność, składanego przez Ostatecznego Odbiorcę Wsparcia za pośrednictwem systemu CST2021.
11. W przypadku stwierdzenia naruszenia przez Ostatecznego odbiorcę wsparcia przepisów PZP albo zasady konkurencyjności, o których mowa w ust.10, Instytucja odpowiedzialna za realizację inwestycji dokonuje korekt finansowych zgodnie z treścią załącznika nr 2 do Wytycznych dotyczących kwalifikowalności wydatków finansowanych ze środków Instrumentu na rzecz Odbudowy i Zwiększania Odporności dla przedsięwzięć realizowanych w ramach inwestycji D1.1.2 „Zasady sposobu korygowania nieprawidłowości dotyczących udzielania i realizacji zamówień publicznych w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”.
Wysokość środków przeznaczonych na realizację przedsięwzięcia § 3.
1. Całkowita wartość przedsięwzięcia wynosi 6 498 195,13 zł (słownie: sześć milionów czterysta dziewięćdziesiąt osiem tysięcy sto dziewięćdziesiąt pięć złotych 13/100) brutto.

2. Całkowita kwota wydatków kwalifikowalnych przedsięwzięcia wynosi: 5 288 695,22 zł (słownie: pięć milionów dwieście osiemdziesiąt osiem tysięcy sześćset dziewięćdziesiąt pięć złotych 22/100).
3. Kwota wsparcia wynosi 5 288 695,22 zł (słownie: pięć milionów dwieście osiemdziesiąt osiem tysięcy sześćset dziewięćdziesiąt pięć złotych 22/100) i stanowi nie więcej niż 100 % kwoty całkowitych wydatków kwalifikowalnych.
Zmiany w przedsięwzięciu § 20.
1. W trakcie realizacji przedsięwzięcia Ostateczny odbiorca wsparcia może składać wnioski o zmianę w CST2021 pod warunkiem zachowania zgodności przedsięwzięcia z dokumentami wymienionymi w pkt. 1 i 8 preambuły. W przypadku akceptacji wniosku o zmianę, zmianie ulegają także wszystkie dokumenty określone w treści § 2 ust.2 niniejszej Umowy tj. wniosek i harmonogram stanowiące odpowiednio załączniki nr 3 i 4 do Umowy.
2. Instytucja odpowiedzialna za realizację inwestycji weryfikuje wniosek o zmianę w terminie 14 dni od dnia jego otrzymania w CST2021. W przypadku złożenia wniosku o zmianę zawierającego błędy lub niekompletnego, Ostateczny odbiorca wsparcia zobowiązuje się, na wezwanie Instytucji odpowiedzialnej za realizację inwestycji, do złożenia poprawionego dokumentu lub uzupełnienia wskazanych braków w terminie 3 dni od dnia otrzymania wezwania. W takim przypadku termin weryfikacji wniosku o zmianę ulega zawieszeniu do dnia złożenia poprawionego lub uzupełnionego dokumentu. W przypadku akceptacji wniosku o zmianę Strony zawierają aneks do Umowy.
3. Wydłużenie terminu realizacji przedsięwzięcia, o którym mowa w treści § 2 ust.4 niniejszej Umowy, wymaga zawarcia między Stronami aneksu do Umowy.
4. Przedsięwzięcie może być zmienione zgodnie z niniejszym paragrafem pod warunkiem, że:
1) zmiany nie wpłynęłyby na wynik oceny przedsięwzięcia w sposób, który skutkowałby negatywną oceną przedsięwzięcia, albo
2) zmiany wynikają z wystąpienia okoliczności niezależnych od Ostatecznego odbiorcy wsparcia, których nie mógł przewidzieć, działając z należytą starannością, oraz zmienione przedsięwzięcie w wystarczającym stopniu będzie przyczyniało się do realizacji celów inwestycji.

23 lutego 2026 r. wykonawca Suntar spółka z ograniczoną odpowiedzialnością wniósł odwołania wobec treści SWZ zarzucając zamawiającemu naruszenie art. 16 pkt 1 ustawy w zw. z art. 99 ust. 1 ustawy w zw. z art. 99 ust. 2 zw. z art. 99 ust. 4 ustawy przez sporządzenie opisu przedmiotu zamówienia w sposób ograniczający uczciwą konkurencję, niewynikający z uzasadnionych potrzeb zamawiającego oraz nie proporcjonalny do wartości i celów jakie chciałby osiągnąć zamawiający.

Wniósł o uwzględnienie odwołania i nakazanie zamawiającemu, aby dokonał modyfikacji treści SWZ (opisu przedmiotu zamówienia) w sposób wskazany w treści uzasadnienia odwołania oraz przesunięcie terminu składania ofert o okres co najmniej 14 dni.

W ocenie odwołującego zamawiający skonstruował opis przedmiotu zamówienia w sposób:

- kumulatywnie zawężający konkurencję,
- oparty na funkcjonalnościach występujących łącznie jedynie w rozwiązaniach Dell,
- nieuwzględniający realnej równoważności technologicznej,
- nieproporcjonalny do celu zamówienia.

co stanowi to naruszenie art. 16, art. 99 ust. 4 ustawy. Odwołujący w powyższym zakresie kwestionuje następujące wymagania OPZ i wnosi o ich nakazanie zamawiającemu ich zmiany jako naruszających przepisy ustawy Prawo zamówień publicznych:

Odwołujący przytoczył treść przepisów powołanych w zarzutach oraz powołał orzecznictwo KIO. W aspekcie szczegółowym podniósł

W odniesieniu do serwerów:

1. Mechanizm weryfikacji integralności sprzętu od produkcji do dostawy

Wymóg SWZ:

Mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej od momentu produkcji oraz kontrolę otwarcia w trakcie transportu (niezależnie od zasilania).

Wskazane wymaganie to odpowiednik funkcjonalności „Secured Component Verification" / „Supply Chain Security" stosowanej przez Dell.

Wniosek:

To wymaganie wykracza poza standardowe zabezpieczenia firmware (Secure Boot, TPM, podpis cyfrowy BIOS) i ma charakter marketingowy, a nie funkcjonalny. Wniósł o nakazanie zamawiającemu wykreślenia wskazanego zapisu.

2. Wbudowany „Lifecycle Log" powiązany z tożsamością użytkownika Wymóg SWZ:

Dziennik cyklu życia sprzętu rejestrujący szczegółowe zdarzenia konfiguracyjne powiązane z tożsamością użytkownika.

Terminologia oraz zakres wymagania odpowiadają rozwiązaniu Lifecycle Log w iDRAC.

Wniosek:

Wymóg ma charakter specyficzny dla jednej platformy zarządzania. W ocenie odwołującego wskazane wymaganie nie wynika z uzasadnionych potrzeb zamawiającego i może być realizowane w zakresie odpowiadającym jego potrzebom w inny sposób. Wniósł o usunięcie wymogu.

3. Integracja z RSA SecurID na poziomie BMC Wymóg SWZ:

Możliwość wykorzystania tokenu lub aplikacji SecurID do MFA przy logowaniu do karty zarządzającej.

W ocenie odwołującego standardem rynkowym jest:

- TOTP,
- LDAP + MFA,
- SAML,
- integracja z IdP.

Wskazanie RSA SecurID jako mechanizmu natywnego ogranicza konkurencję. Wymóg ma charakter specyficzny dla jednej platformy zarządzania. Wniósł o usunięcie wymogu.

4. Automatyczne zgłaszanie alertów do centrum serwisowego producenta

Wymóg SWZ:

Automatyczne generowanie i zgłaszanie incydentów bezpośrednio do producenta.

Kwestionowane postanowienie odpowiada modelowi ProSupport/SupportAssist.

Kumulacja tego wymogu z pozostałymi powoduje de facto wskazanie producenta DELL.

W ocenie odwołującego wskazane wymaganie nie wynika z uzasadnionych potrzeb zamawiającego i może być realizowane w zakresie odpowiadającym jego potrzebom w inny sposób. Wniósł o usunięcie wymogu

5. Eksport/import konfiguracji w XML/JSON obejmujący BIOS, HBA, RAID

Kwstionowane wymaganie to precyzyjne odwzorowanie funkcjonalności OpenManage Enterprise. Brak analogicznej, identycznej funkcji u konkurencji w wymaganym zakresie.

Wniósł o usunięcie wymogu

6. Aplikacja mobilna przez BLE

Wymóg:

- aplikacja Android/iOS,
- komunikacja BLE bez sieci.

Wskazane wymaganie jest charakterystyczne dla Dell Quick Sync 2. Nie jest to wymóg standardowy w środowiskach data center. Wniósł o usunięcie wymogu.

7. Wymóg określonego wyniku SPEC CPU 2017 (197 / 200 / 370 pkt)

Wymóg:

Minimalny wynik w teście SPECrate2017_int_base dla konfiguracji jednoprocesorowej, dla oferowanego serwera lub innego serwera tego samego producenta.

1. Wymóg uzależnia możliwość złożenia oferty od:

o przeprowadzenia przez producenta testu SPEC,

o opublikowania wyniku dla konkretnej konfiguracji, o przeprowadzenia testu w trybie jednoprocesorowym.

Zamawiający nie dopuścił: o równoważnego benchmarku, o oświadczenia producenta, o testu własnego wykonanego przez wykonawcę. Wniósł o wskazanie równoważności wyniku dla procesorów w teście z www.cpubenchmark.net

8. Permanent Fault Detection

Wymóg wskazuje na konkretną implementację producenta.

Brak dopuszczenia równoważnych mechanizmów RAS powoduje ograniczenie konkurencji
Wniósł o dopuszczenie równoważności np. ECC + monitoring progowy (Patrol Scrubbing) + BIOS rank/channel disable + logowanie zdarzeń przez HDM.

9. Czteroportowa karta 25Gb SFP28 nie zajmująca slotu PCIe Wymóg:

- karta 4×25Gb
- w standardzie SFP28
- nie zajmująca slotu PCIe

Jest to wymóg konstrukcyjny, nie funkcjonalny.
Wniósł o dopuszczenie równoważności w postaci dwóch kart dwuportowych, z czego jedna z nich w slocie PCIe.

10. Dwa dyski M.2 NVMe FIPS RAID1 Wymóg FIPS na poziomie M.2 NVMe:

- nie jest wymagany przez przepisy prawa,
- wyklucza producentów, którzy oferują FIPS wyłącznie w dyskach 2.5".

Wniósł o usunięcie wymogu FIPS

11. Wyłączenie przycisku zasilania w BIOS

Nie jest to:

- wymóg bezpieczeństwa wynikający z norm,
- standard branżowy.

Wniósł o równoważność np. z poziomu oprogramowania do zarządzania serwerami.

12. Mechanizm weryfikacji niezmienności konfiguracji od produkcji

Wymóg wykracza poza standard Root of Trust.
Nie każdy producent oferuje mechanizm „transport chain verification".
Wniósł o usunięcie wymogu lub dopuszczenie równoważności w postaci np. TPM

13. Automatyczne firmware update + automatyczny backup konfiguracji

Wniósł o usunięcie wymogu

14. BIOS integrity monitoring, SSL auto-renew, SecurID, custom cooling rules, temperature thresholds, telemetry

To zestaw bardzo szczegółowych funkcji implementacyjnych.
Wniósł o usunięcie wymogu.

15. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych Wymóg zarządzania urządzeniami sieciowymi i storage.

Wniósł o usunięcie wymogu dla urządzeń sieciowych oraz pamięci masowych.

16. Raporty CSV, HTML, XLS, PDF

Brak dopuszczenia tylko jednego z formatów.
Wniósł o zmianę na „Raporty CSV lub HTML lub XLS lub PDF".

17. Automatyczne grupowanie wg dowolnego elementu konfiguracji Zbyt szeroki, nieprecyzyjny i nieproporcjonalny wymóg.

Może być interpretowany dowolnie i prowadzi do eliminacji konkurencji. Wniósł o usunięcie wymogu

18. Import plików MIB

Nie jest wymagany do prawidłowej pracy środowiska. Wniósł o usunięcie wymogu

19. Rozbudowany moduł raportujący

Zakres raportu wykracza poza niezbędne potrzeby zarządzania serwerem.

Wniósł o usunięcie wymogu.

20. Appliance dla KVM, ESXi i Hyper-V

Wymóg jednoczesnej obsługi trzech hypervisorów eliminuje producentów, którzy wspierają tylko jeden lub dwa.

Wniósł o zmianę na „Appliance dla KVM lub ESXi lub Hyper-V".

21. Dyrektywa 67/548/EEC

Dyrektywa uchylona i zastąpiona przez rozporządzenie CLP (1272/2008).

Wniósł o usunięcie wymogu.

22. EPEAT Silver

Wymóg wydruku z konkretnej strony (epeat.net).

Brak dopuszczenia:

- równoważnych certyfikatów środowiskowych

Wniósł o usunięcie wymogu lub dopuszczenie równoważnych certyfikatów środowiskowych lub oświadczenia producenta

23. Jeden punkt kontaktu dla całego rozwiązania Wśród rozwiązania znajduje się:

Microsoft Windows Server 202x

Producent sprzętu nie jest producentem systemu operacyjnego.

Wniósł o usunięcie wymogu.

24. Samodzielna kwalifikacja ważności naprawy Brak mechanizmu weryfikacji. Wniósł o usunięcie wymogu.

25. Zasilacze maks. 1100W Titanium

Wymóg „maksymalnej mocy" zamiast minimalnej:

- nieuzasadniony technicznie,
- ogranicza możliwość zastosowania mocniejszych jednostek,
- nie ma związku z efektywnością.

Wniósł o zmianę zapisu na „Zasilacze min. 1100W Titanium".

Podsumowując wymagania w pkt. 1-25 wskazał, że zamawiający stworzył:

- opis parametryczny, zawierający implementacyjne cechy produktu, o wysokim stopniu szczegółowości,
- bez realnego dopuszczenia równoważności,
- eliminujący znaczną część rynku.

Opis ma charakter modelu referencyjnego konkretnego producenta, co stanowi obejście zakazu wskazywania znaków towarowych.

Pojedyncze wymagania mogłyby zostać uznane za dopuszczalne.

Zamawiający nie wykazał:

- związku wymagań z bezpieczeństwem oraz z wymogami prawa,
- konieczności natywnej integracji z RSA SecurID.

Funkcjonalności te nie wynikają z:

- KRI,
- NIS2,
- ustawy o KSC,
- ISO 27001,
- ISO 22301.

Opis przedmiotu zamówienia:

- nie jest neutralny technologicznie,
- prowadzi do uprzywilejowania jednego producenta,
- eliminuje konkurencję,
- powinien skutkować unieważnieniem postępowania

W odniesieniu do komputerów All-in-One:

Opis parametrów technicznych stanowi zestaw cech odpowiadających konfiguracji komputera Dell OptiPlex 7420 All-in-One, w szczególności w zakresie:

- matrycy 23.8” IPS FHD 90Hz 99% sRGB 1500:1,
- pełnej regulacji podstawy (pivot 90°, 130 mm wysokości, swivel 45°),
- portów w dokładnym układzie: 1x USB-C z ładowaniem + 5x USB-A + HDMI + DP.

Taka konfiguracja do zastosowań biurowych jest nadmiarowa.

Do pracy biurowej standardem rynkowym w sektorze publicznym pozostaje:

- 2-4 x USB typu A oraz 1-2 x USB typu C
- HDMI
- kontrast 1000:1,
- 60–75 Hz,

Wniósł o taką zmianę.

Wymóg:

- 90 Hz
- kontrast 1500:1
- 99% sRGB w segmencie biurowym AiO praktycznie nie występuje łącznie poza jednostkowymi modelami.

Dla zastosowań biurowych standardem rynkowym jest:

- 60–75 Hz,

- kontrast 1000:1,
- 99% sRGB (opcjonalnie).

Wymóg:

„5x USB 3.2 typu A (na zewnątrz obudowy, bez stosowania konwerterów, przejściówek itp.)" należy uznać za nieproporcjonalny oraz sztucznie ograniczający konkurencję, w szczególności w segmencie komputerów All-in-One.

W segmencie biznesowych AiO standardem rynkowym jest:

2–4 porty USB-A

1–2 porty USB-C

Współczesny trend konstrukcyjny polega na:

- ograniczaniu liczby portów typu A,
- zastępowaniu ich USB-C (uniwersalność, zasilanie, DisplayPort Alt Mode).

Wymóg aż 5 portów USB 3.2 typu A, przy jednoczesnym braku dopuszczenia równoważności poprzez hub lub replikator, wykracza poza standard rynkowy.W praktyce 3–4 porty USB-A w zupełności wystarczają. Wniósł o taką zmianę.

W praktyce ogranicza to rynek do bardzo wąskiej grupy modeli, w tym m.in.: • Dell OptiPlex 7420 All-in-One

Każdy parametr oddzielnie może wydawać się dopuszczalny, jednak ich łączna konfiguracja powoduje, że:

- krąg realnych wykonawców zostaje ograniczony do 1–2 modeli, dochodzi do faktycznego wskazania produktu, rynek nie ma realnej możliwości konkurencji cenowej.

Dotyczy urządzenia do długoterminowego przechowywania kopi bezpieczeństwa - Deduplikator:

Opis przedmiotu zamówienia we wskazanym zakresie stanowi w istocie techniczny opis urządzenia Dell PowerProtect DD6410 produkcji Dell Technologies. 1. Wymóg deduplikacji zmiennym blokiem ≤ 12 kB (pkt 13)

Zamawiający wymaga:

- zmiennego, dynamicznego bloku, • o wielkości nie większej niż 12 kB,
- zakazu bloków stałej długości.

Jest to charakterystyczna cecha architektury Data Domain (Dell PowerProtect).

Wniósł o usunięcie wymogu.

2. Zakaz jakiegokolwiek bufora danych (pkt 12, 15, 16) Zamawiający wymaga:

- 100% deduplikacji in-line,
- całkowitego zakazu przechowywania danych w postaci niezdeduplikowanej w jakiejkolwiek fazie,
- zapisu wyłącznie unikalnych bloków.

Wniósł o usunięcie wymogu.

3. Deduplikacja na źródle przez LAN i FC (pkt 19, 20, 26) Wymóg:

source-side dedupe przez LAN, source-side dedupe przez FC (SAN),

- transmisja wyłącznie nowych bloków przez FC,
- wsparcie jednocześnie dla Commvault, Veeam i NetWorker, jest unikalny dla platformy Dell PowerProtect.

Wniósł o usunięcie wymogu.

4. Parametry VTL (pkt 9–11) Wymagania:

- emulacja StorageTek L180,
- emulacja IBM TS3500,
- min. 250 napędów,
- min. 60 000 slotów, odzwierciedlają maksymalne parametry Data Domain.

Zamawiający nie wykazał:

- że posiada fizyczne biblioteki wymagające dokładnie tych modeli,
- że inna emulacja nie zapewnia kompatybilności

Wniósł o usunięcie wymogu.

5. Wydajność podana marketingowo (pkt 7) Wymóg:

- 25 TB/h NFS,
- 50 TB/h przy deduplikacji na źródle,
- „zgodnie z danymi producenta”, jest bezpośrednim cytatem parametrów marketingowych Dell.

Wniósł o usunięcie wymogu.

Ponownie podkreślił kumulatywność wymogów wykluczającą konkurencję.

Opis OPZ:

- uniemożliwia złożenie oferty przez innych producentów niż Dell,
- ogranicza konkurencję tylko do jednego produktu,
- stwarza pozór konkurencyjności przy faktycznym braku konkurencji,
- prowadzi do ryzyka niegospodarności środków publicznych.

Dotyczy wymagań na macierze:

Wymóg:

„macierz musi zajmować maksymalnie 2U i pozwalać na instalację 24 dysków 2.5”” w połączeniu z pozostałymi parametrami (8x FC 32Gb, ADAPT, 24Gb SAS, 16GB cache na kontroler) powoduje, że wymagania spełnia wyłącznie seria Dell PowerVault ME5224 Skumulowanie wszystkich parametrów eliminuje innych producentów.

Wymóg:

„Możliwość konfiguracji RAID 1, 5, 6, 10, ADAPT”

RAID ADAPT jest nazwą handlową technologii charakterystycznej dla Dell PowerVault ME5.

Zarzut kluczowy: Użycie nazwy technologii handlowej bez dopuszczenia rozwiązania równoważnego narusza art. 99 ust. 4 Pzp.

Wniósł o zmianę na „Możliwość konfiguracji RAID 5, 6, 10”.

Wymóg:

„16 dysków SSD SAS 24Gb/s” Standard rynkowy:

- większość producentów w tej klasie oferuje SSD SAS 12Gb/s,
- SAS 24Gb/s jest rozwiązaniem nowej generacji, dostępnej w wąskiej grupie platform.

Cache min. 16GB na kontroler Parametr wydaje się dopasowany do konkretnej konfiguracji ME5224. Wniósł o zmianę na „16 dysków SSD SAS 12Gb/s”.

Wymóg auto-tiering + SSD cache do 8TB Jednoczesne wymaganie:

- auto-tieringu,
- SSD jako cache,
- rozbudowy cache do 8TB, jest charakterystyczne dla konkretnej architektury Dell ME5.

Wniósł o usunięcie wymogu.

Wymóg:

„Rozwiązanie musi wspierać obsługę samoszyfrujących się dysków” nie ma uzasadnienia funkcjonalnego. Wniósł o usunięcie wymogu lub dopuszczenie szyfrowania software'owego.

Ograniczenie konkurencji poprzez architekturę producenta Obsługa SED w praktyce wymaga:

- dedykowanego firmware kontrolerów,
- często dodatkowych licencji,
- niekiedy dedykowanego modułu zarządzania kluczami.

W efekcie wymóg zawęża katalog producentów do platform oferujących SED w tej konkretnej konfiguracji kontrolerów i firmware – co w praktyce ponownie wskazuje na serię Dell ME5. wskazanie konkretnej technologii sprzętowej (SED) bez określenia efektu bezpieczeństwa jest opisem rozwiązania technicznego, a nie potrzeby.

Po analizie rynku:

Zestaw wszystkich parametrów łącznie spełnia wyłącznie:

- Dell PowerVault ME5224. Inni producenci:
- nie oferują RAID ADAPT,
- nie łączą wszystkich wymaganych funkcjonalności w jednej platformie. Oznacza to faktyczne ograniczenie konkurencji do jednego producenta.

Do postępowania odwoławczego nikt nie przystąpił.

Z informacji wynikającej z wniosku o uchylenie zakazu wynika, że zamawiający mimo wniesienia odwołania podejmował dalsze czynności w postępowania, w tym dokonał otwarcia ofert. Odwołujący nie złożył oferty.

Rozważania KIO:

Wniosek zasługuje na uwzględnienie.

Zamawiający powołał się na istnienie interesu publicznego w realizacji przedmiotowej inwestycji szeroko opisując cel inwestycji, jej znaczenie społeczne i ekonomiczne oraz możliwość utraty dofinansowania w przypadku nie zawarcia umowy do 31 maja 2026 r.
Zgodnie z art. 578 ust. 2 pkt 1 ustawy KIO może uchylić zakaz zawarcia umowy, jeżeli nie zawarcie umowy mogłoby spowodować negatywne skutki dla interesu publicznego, przewyższające korzyści związane z koniecznością ochrony wszystkich interesów, w odniesieniu do których zachodzi prawdopodobieństwo doznania uszczerbku w wyniku czynności podjętych przez zamawiającego w postępowaniu o udzielenie zamówienia. Zamawiający wskazał na istnienie interesu publicznego polegającego na:
- utracie dofinansowania przeznaczonego na realizację przedmiotowego zadania a w konsekwencji brak możliwości realizacji zadania,
- niemożliwość realizacji inwestycji ze środków z KPO.
- zagrożeniu ciągłości działania systemów informatycznych obsługujących dokumentację medyczną (EDM), rejestrację pacjentów oraz systemy laboratoryjne i diagnostyczne,
- ryzyku utraty lub ograniczenia dostępu do danych medycznych pacjentów, co może bezpośrednio wpływać na bezpieczeństwo zdrowotne i życie pacjentów,
- braku możliwości integracji systemów z platformą e-Zdrowie (P1), co może skutkować naruszeniem obowiązków ustawowych szpitala,
- dezorganizacją pracy oddziałów szpitalnych, wydłużeniem czasu obsługi pacjentów oraz zwiększeniem ryzyka błędów medycznych,
- zużycie technologiczne sprzętu i oprogramowania, brak spełniania aktualnych standardów wydajności, bezpieczeństwa i interoperacyjności – tu wskazano, że ostatnie dofinansowanie Szpitala miało miejsce 9 lat temu.
- ryzyko: spadku wydajności systemów obsługujących procesy medyczne i administracyjne, zwiększonej awaryjności sprzętu, ograniczonej możliwości integracji z nowymi systemami krajowymi oraz usługami cyfrowymi w ochronie zdrowia, wzrostu zagrożeń w obszarze cyberbezpieczeństwa.
- ryzyko dla ciągłości pracy laboratorium oraz bezpieczeństwa przetwarzanych danych medycznych wobec utraty z końcem roku wsparcia producenta
- konsekwencje dla pacjentów korzystających ze świadczeń zdrowotnych, którzy utracą możliwość korzystania z nowoczesnych usług cyfrowych, które miały zostać wdrożone w ramach projektu.
- nie będzie możliwe uruchomienie funkcjonalności udostępniania wyników badań laboratoryjnych on-line, co oznacza konieczność osobistego odbierania wyników w placówce lub dłuższe oczekiwanie na ich przekazanie.
- wolniejszą obsługę pacjentów, wynikającą z dalszego korzystania z przestarzałych systemów informatycznych.

- ryzyko zmiany cen na rynku sprzętu informatycznego.

Zamawiający podkreślił znaczenie swojej placówki dla pacjentów i ich rodzin.

Opisał stan bieżący istniejącej infrastruktury technicznej. Podkreślił, że nie posiada własnych środków na sfinansowanie zamówienia i utrata dofinansowania spowoduje, że szpitala nie będzie stać na zrealizowanie przedsięwzięcia w przyszłości.

Zamawiający podkreślił brak przyczynienia się do przewlekłości postępowania, przeciwnie podkreślił, że podjął działania związane z prowadzeniem przedmiotowego postępowania niezwłocznie po zawarciu umowy o dofinansowanie, wskazał także na możliwość wydłużenia się postępowania odwoławczego.

Zamawiający zatem wskazał na konkretne realne negatywne skutki dla interesu publicznego zarówno w aspekcie lokalnym dla potrzeb mieszkańców jak i jako inwestycji oddziałującej na opiekę medyczną w regionie, wskazał także na negatywny aspekt ekonomiczny brak realizacji inwestycji. Podkreślił dochowanie należytej staranności w organizacji postępowania o udzielenie zamówienia, a tym wszystkim okolicznościom przeciwstawił indywidualny interes odwołującego i jego potencjalną szkodę w przypadku braku uzyskania przedmiotowego zamówienia. KIO wzięła także pod uwagę fakt, że zamawiający prowadzi postępowanie w 4 powiązanych ze sobą częściach, a odwołujący nie wskazał, do której części kieruje wniesione odwołania, co spowodowało, że zakazem zawarcia umowy objęte są wszystkie części zamówienia, nie tylko te w których przedmiotem jest dostawa sprzętu, ale także te, które wymagają rozbudowy istniejącego oprogramowania, wdrożenia systemu laboratoryjnego i przeprowadzenia szkoleń. Zwłaszcza w odniesieniu do części 1 i 2 czas umożliwiający zrealizowanie zadania jest według KIO bardziej kluczowy niż w przypadku dostawy sprzętu. Te dwa pierwsze zadania także niosą w sobie większe ryzyko potrzeby jego wydłużenia, a w konsekwencji w sytuacji utrzymywania się zakazu wobec wszystkich części ryzyko nie dotrzymania terminu z umowy o dofinansowanie ulega zwiększeniu. KIO oczywiście dostrzega, że umowa o dofinansowanie przewiduje możliwość zmiany terminu, jednak za zmiana wymaga akceptacji instytucji wdrażającej i nie musi być dopuszczona automatycznie na wniosek zamawiającego. W ocenie KIO wszystkie wskazane przez zamawiającego okoliczności przemawiają za uznaniem, że negatywne skutki dla interesu publicznego przewyższają korzyści związane z ochroną interesu odwołującego, a zatem zamawiający wykazał przesłankę dopuszczalności uchylenia zakazu z art. 578 ust. 2 pkt 1 ustawy, a w konsekwencji KIO orzekła o uchyleniu zakazu zawarcia umowy, zgodnie z żądaniem zamawiającego.

KIO nie podzieliła natomiast argumentacji zamawiającego opartej o przesłankę z art. 578 ust. 2 pkt 2 ustawy. W ocenie KIO odwołujący nie ma obowiązku wyczerpania przed wniesieniem odwołania wobec treści SWZ procedury zapytań do treści SWZ. Odwołujący mógłby narazić się na negatywne konsekwencje utraty możliwości skutecznego odwołania wobec treści SWZ,

gdyby zadał pytania, a zamawiający nie odpowiedział na nie w terminie umożliwiającym odwołującemu jeszcze skorzystanie z prawa do wniesienia odwołania. Tym samym argumentacja o braku aktywności odwołującego na etapie przed upływem składania ofert nie jest zasadna i nie świadczy o dążeniu odwołującego wyłącznie do uniemożliwienia zamawiającemu zawarcia umowy. Także sam fakt, że zamawiający nie opisał w OPZ specyfikacji technicznej pasującej dla komputerów all-in-one wyłącznie do jednego wskazanego przez odwołującego modelu nie zmienia faktu, że jest to jedynie jeden z wielu zarzutów sformułowanych przez odwołującego i nawet jego potencjalne oddalenie nie powodowałoby jeszcze konstatacji, że odwołujący nie mógłby wygrać postępowania odwoławczego i tym samym osiągnąć założonego przez siebie celu. W ramach wniosku o uchylenie zakazu zawarcia umowy KIO nie dokonuje oceny zasadności odwołania, stąd odnoszenie się przez zamawiającego w sposób merytoryczny do zarzutów, nie mogło mieć znaczenia dla oceny rozpoznawanego wniosku.

Z uwagi na powyższe Izba na podstawie art. 578 ust. 4 ustawy postanowiła jak w sentencji.

Przewodnicząca: ……