Sygn. akt: KIO 1077/26

WYROK

z dnia 16 kwietnia 2026 roku

Krajowa Izba Odwoławcza - w składzie:

Przewodnicząca:Justyna Tomkowska

Protokolant: Krzysztof Chmielewski

po rozpoznaniu na rozprawie w dniu **13 kwietnia 2026 roku w Warszawie** odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu **9 marca 2026 roku** przez wykonawcę **Computex Spółka z ograniczoną odpowiedzialnością Spółka komandytowa z siedzibą w Warszawie** (Odwołujący)

w postępowaniu prowadzonym przez Zamawiającego – **Skarb Państwa, w imieniu którego postępowanie prowadzi Centrum e- Zdrowia z siedzibą w Warszawie**

przy udziale **Przystępującego** zgłaszającego przystąpienie **po stronie Zamawiającego: HUB4 Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie**

orzeka:

1.umarza postępowanie w zakresie zarzutów naruszenia art. 128 ust. 1 i ust. 4 ustawy Pzp oraz art. 128 ust 1 Pzp w zw. z § 6 ust 1 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej

w postępowaniu o udzielenie zamówienia publicznego lub konkursie;

2.Oddala odwołanie w pozostałym zakresie,

3.kosztami postępowania obciąża **Odwołującego - Computex Spółka z ograniczoną odpowiedzialnością Spółka komandytowa z siedzibą w Warszawie** w następujący sposób**:**

3.1.zalicza w poczet kosztów postępowania kwotę **15 000 zł 00 gr** (słownie: piętnastu tysięcy złotych zero groszy) uiszczoną przez **Odwołującego** tytułem wpisu od odwołania, kwotę **3 600 zł 00 gr** (słownie: trzech tysięcy sześciuset złotych zero groszy) poniesioną przez **Odwołującego** tytułem wynagrodzenia pełnomocnika, oraz kwotę **3 600 zł 00 gr** (słownie: trzech tysięcy sześciuset złotych zero groszy) poniesioną przez **Zamawiającego** tytułem wynagrodzenia pełnomocnika;

2.2.zasądza od **Odwołującego - Computex Spółka z ograniczoną odpowiedzialnością Spółka komandytowa z siedzibą w Warszawie** na rzecz **Zamawiającego – Skarbu Państwa, w imieniu którego postępowanie prowadzi Centrum e- Zdrowia z siedzibą w Warszawie** kwotę **3 600 zł 00 gr** (słownie: trzech tysięcy sześciuset złotych 00/100 groszy) stanowiącą uzasadnione koszty Strony poniesione tytułem wynagrodzenia pełnomocnika.

Na orzeczenie - w terminie 14 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do **Sądu Okręgowego w Warszawie - Sądu Zamówień Publicznych**.

Przewodnicząca:

……

sygn. akt KIO 1007/26

UZASADNIENIE

Zamawiający: Skarb Państwa, w imieniu którego postępowanie prowadzi Centrum e- Zdrowia z siedzibą w Warszawie, prowadzi postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2024 r. poz. 1320 ze zm., dalej: „ustawa Pzp") pn. pn. *„Dostawa deduplikatorów wraz z licencjami do oprogramowania do deduplikacji danych".* Ogłoszenie o zamówieniu opublikowane zostało w DzUUE: Dz.U. S: 190/2025 647783-2025 z dnia 03/10/2025r.

Dnia 9 marca 2026 roku do Prezesa Krajowej Izby Odwoławczej w Warszawie, na podstawie art. 513 pkt 1 ustawy Pzp odwołanie złożył wykonawca Computex Spółka z ograniczoną odpowiedzialnością Spółka komandytowa z siedzibą w Warszawie, dalej jako „Odwołujący".

Powiadomienie o czynności stanowiącej podstawę do złożenia odwołania zostało opublikowane w dniu 27 lutego 2026 roku (informacja o wyborze oferty najkorzystniejszej), zatem odwołanie złożono z zachowaniem ustawowego terminu. Kopia odwołania została przekazana Zamawiającemu. Odwołujący uiścił wpis w wymaganej wysokości.

Odwołanie złożono wobec czynności i zaniechań Zamawiającego polegających na:

1.Wyborze oferty najkorzystniejszej w postępowaniu i uznaniu za taką oferty wykonawcy HUB4 Spółka z

ograniczoną odpowiedzialnością z siedzibą w Warszawie (dalej jako „HUB4") – naruszenie art. 239 Pzp,

2.Zaniechaniu odrzucenia oferty wykonawcy HUB4:

- w sytuacji kiedy treść oferty tego wykonawcy pozostaje niezgodna z warunkami zamówienia - naruszenie art. 226 ust 1 pkt 5 Pzp

w przypadku nieuwzględnienia zarzutu zaniechania odrzucenia oferty HUB4:

4.Zaniechanie wezwania wykonawcy HUB4 do uzupełnienia podmiotowego środka dowodowego w zakresie potwierdzenia spełnienia warunku udziału w postępowaniu bowiem złożone na wezwanie dokumenty nie potwierdzają spełnienia warunku udziału (naruszenie art. 128 ust 1 Pzp lub co najmniej art. 128 ust. 4 Pzp)

5.złożone referencje są w nieprawidłowej formie – naruszenie art. 128 ust 1 Pzp w zw.

z § 6 ust 1 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu

o udzielenie zamówienia publicznego lub konkursie.

Odwołujący wnosił o uwzględnienie odwołania i:

1.unieważnienie czynności wyboru oferty najkorzystniejszej jako obarczonej wadą,

2.powtórzenie czynności badania oraz oceny ofert i odrzucenie oferty wykonawcy HUB4

ewentualnie w przypadku nieuwzględnienia zarzutu zaniechania odrzucenia oferty HUB4

3.wezwanie wykonawcy HUB4 do uzupełnienia podmiotowych środków dowodowych w celu potwierdzenia spełniania warunku udziału w zakresie doświadczenia.

Odwołujący wskazał, że osiada interes w uzyskaniu zamówienia oraz może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp bowiem zgodnie

z rankingiem oferty z zawiadomienia o wyborze oferty najkorzystniejszej jego oferta znalazła się na drugiej pozycji. W tej sytuacji odrzucenie oferty poprzedzającej spowoduje bezpośrednią możliwość uzyskania zamówienia przez Odwołującego i osiągnięcia zysku

z tytułu realizacji zamówienia na rzecz Zamawiającego.

W uzasadnieniu zarzutów wskazano, że przedmiotem zamówienia jest dostawa deduplikatorów wraz z licencjami do oprogramowania do deduplikacji danych, szczegółowo opisanych w Załączniku nr 1 do SWZ. Szczegółowy przedmiot zamówienia stanowi Załącznik nr 1 do SWZ - Opis przedmiotu zamówienia oraz Załącznik nr 2 do SWZ - Projektowane postanowienia umowy.

W ramach postępowania Zamawiający nie dopuszczał możliwości składania ofert częściowych ze względów organizacyjnych i technicznych, gdyż dotyczy dostawy

4 jednakowych urządzeń wraz z instalacją i konfiguracją tj. wdrożeniem.

Zamówienie obejmuje w szczególności: dostawę 4 nowych Urządzeń do backupu dyskowego z deduplikacją danych wraz z licencjami do oprogramowania do deduplikacji danych, montażem oraz min. 60 miesięczną gwarancją, zgodnie z pkt 4.14.

Jednym z najistotniejszych elementów urządzeń dedykowanych do przechowywania danych backupowych jest przede wszystkim zapewnienie bezpieczeństwa tych danych, gdyż ich potencjalna: utrata, przekłamanie, usunięcie bądź zaszyfrowanie (w efekcie ataków typu „ransomware") uniemożliwiałyby odtworzenie na ich podstawie chronionych systemów.

OPZ postępowania zawiera szereg elementów związanych z zapewnieniem bezpieczeństwa przechowywanych danych, w tym w szczególności tak newralgiczne jak:

Na treść oferty w przedmiotowym postępowaniu składał się formularz ofertowy oraz wszystkie dokumenty dookreślające i precyzujące zobowiązanie wykonawcy dotyczące przedmiotu oraz zakresu lub wielkości zamówienia, składane wraz z ofertą – w tym

w szczególności Załącznik nr 3 - Formularz ofertowy i dane w nim zawarte.

Integralnym elementem Formularza ofertowego jest tabela zawierająca identyfikację

i opis oferowanego rozwiązania:

Wykonawca HUB4 w treści złożonej oferty w Formularzu ofertowym dokonał identyfikacji oferowanych urządzeń wskazując, że jest to:

Zaoferowane deduplikatory to urządzenia identyfikowalne o publicznie dostępnej dokumentacji produktowej.

Ponadto oferta HUB4 zawiera wprost bezpośrednie odesłanie do publicznie dostępnej i jawnej oraz oficjalnej dokumentacji technicznej zaoferowanego w przetargu produktu

Odwołujący dokonał weryfikacji zawartości linków a także danych zawartych na stronie internetowej producenta.

Rozwiązanie zaoferowane przez HUB4 oparte na architekturze ExaGrid (Landing Zone + Repository Tier), nie spełnia krytycznych wymagań bezpieczeństwa zdefiniowanych w OPZ, w szczególnościw punktach 4.4.4, 4.4.5 oraz

4.4.6.

Architektura ta wprowadza systemowe „okno podatności” (vulnerability window), które w przypadku skompromitowania aplikacji backupowej lub ataku ransomware naraża Zamawiającego na nieodwracalną utratę danych.

Zaoferowane urządzenie nie chroni danych w sposób ciągły i pełny, a jedynie wybiórczy (tylko w jednej z warstw), co stoi w sprzeczności z definicją bezpiecznego przechowywania danych w systemach klasy Enterprise.

Wymagania OPZ (pkt 4.4.6) precyzują, że mechanizm ochrony musi być skuteczny*„niezależnie od prób obejścia zabezpieczeń przez oprogramowanie zewnętrzne”.*

Architektura ExaGrid jest dwuwarstwowa:

1.Landing Zone (LZ): Dyskowa strefa zrzutu (cache), gdzie dane trafiają

w pierwszej kolejności.

2.Retention Tier (RT): Strefa repozytorium (deduplikowana).

Sposób zapisu danych na urządzenia ExaGrid, zgodnie

z: https://www.exagrid.com/wp-content/uploads/ExaGridDetailed-Product-Description_DS-10.pdf

„As shown in the diagram to the right, backup data is written directly from the backup server to ExaGrid’s disk-cache Landing Zone at the highest possible rate with no inline processing to interfere”

w tłumaczeniu:

jak pokazano na schemacie po prawej stronie, dane kopii zapasowej są zapisywane bezpośrednio z serwera kopii zapasowych do „ExaGrid’s disk-cache Landing Zone”

z najwyższą możliwą szybkością, bez zakłócającego przetwarzania inline

Przedstawiony schemat zapisu danych na urządzenia ExaGrid pochodzi bezpośrednio z oficjalnej i publicznie udostępnianej dokumentacji producenta na stronie internetowej, do której odesłania znajdują się w ofercie HUB4.

Sposób zapisu danych na urządzeniach ExaGrid – dotyczy wszystkich zapisywanych na tym urządzeniu danych. Istotny jest fakt, że wszystkie zapisywane dane w pierwszym kroku lądują w tzw.: „Landing Zone”.

Zaoferowane przez HUB4 rozwiązanie jest niezgodne z OPZ w następujących aspektach:

•Brak ochrony "Urządzenia" jako całości:

Landing Zone („LZ”) jest integralną częścią fizyczną i logiczną oferowanego Urządzenia. Dane znajdujące się w tej strefie są danymi „przechowywanymi na Urządzeniu". Skoro Landing Zone nie posiada mechanizmu blokady przed modyfikacją/usunięciem

(co potwierdza dokumentacja producenta, wskazując na LZ jako strefę „szybkiego zapisu

i odczytu", nie objętą działaniem blokady Retention Time-Lock), to Urządzenie jako całość nie spełnia wymogu 4.4.6.

•Otwarty standard zapisu: Landing Zone jest udostępniana jako standardowy zasób sieciowy (CIFS/SMB/NFS) z pełnymi prawami zapisu i modyfikacji (Read/Write). Jest to konieczne dla działania technologii ExaGrid, by zapewnić szybkość ingestu.

Oznacza to jednak, że z poziomu sieci nie ma żadnej bariery (Immutability/WORM) chroniącej pliki po ich zapisaniu w Landing Zone.

•Niezgodność z pkt 4.4.4 , pkt 4.4.5, pkt 4.4.6 c.d.

Wymaganie OPZ stanowi, że dane mogą być usuwane*„jedynie w procesie czyszczenia”* (wewnętrzny proces retencji urządzenia).

W architekturze ExaGrid, dane w Landing Zone mogą zostać usunięte poleceniem zewnętrznym (np. komenda rm / del, polecenie usuwania z konsoli backupu, działanie skryptu szyfrującego).

Jest to bezpośrednie złamanie wymogu OPZ, gdyż usuwanie następuje na żądanie zewnętrzne, a nie w wyniku wewnętrznego procesu polityki retencji.

Zgodnie z zamieszczonym w ofercie HUB4linkiem: https://www.exagrid.com/wpcontent/uploads/ExaGrid-AI-Powered_Retention_Time-Lock_for_Ransomware_Recovery_DS-1.pdf

można odnaleźć jeden ze scenariuszy usunięcia czy skompromitowania danych np.: nadpisania czy zaszyfrowania:

w tłumaczeniu:

Dane są usuwane w strefie „ExaGrid disk-cache Landing Zone” poprzez aplikację backupową lub poprzez złamanie protokołu komunikacyjnego.

Powyższe oznacza, że aplikacja backupowa może usunąć dane z Landing Zone, dane te również mogą zostać skompromitowane (zmienione, zaszyfrowane, nadpisane)

w przypadku złamania protokołu komunikacyjnego – należy zauważyć, że sytuacja taka jak najbardziej może mieć miejsce przed zmigrowaniem danych z Landing Zone do Retention Tier (obszaru do długoterminowego przechowywania danych na urządzeniu ExaGrid –

w przypadku, którego urządzenie oferuje blokadę „ExaGrid Retention Time-Lock for Ransomware Recovery”, niedostępną w obszarze Landig Zone – sposób działania opisany w:

https://www.exagrid.com/wp-content/uploads/ExaGrid-Detailed-Product-Description_DS-10.pdf).

Oznacza to, że:

•dane (w tym przeterminowane – dane o krótkiej retencji przechowywania, nie zmigrowane do obszaru Retention Tier) mogą zostać usunięte przez aplikację backup'ową - co jest w sprzeczności z wymaganiem dot. możliwości usuwania danych jedynie w procesie czyszczenia - ppkt 4.4.4 (aplikacja backupowa nie ma nic wspólnego z procesem czyszczenia, który jest wewnętrznym procesem oferowanego urządzenia),

•dane znajdujące się w Landing Zone - nie zmigrowane do Retention Tier są danymi „przechowywanymi" na urządzeniu (zgodnie z nomenklaturę użytą w OPZ – ppkt 4.4.5) – nie są objęte mechanizmem uniemożliwiającym modyfikację bądź usunięcie.

W związku z powyższym zaoferowany mechanizm zabezpieczenia danych nie spełnia wymagania ppkt 4.4.6 zgodnie z którym: *„Mechanizm ten musi być konfigurowalny*
i kontrolowany w taki sposób, aby zapewnić skuteczną ochronę przed modyfikacją/usunięciem danych bezpośrednio na Urządzeniu, niezależnie od prób obejścia zabezpieczeń przez oprogramowanie zewnętrzne (w tym potencjalnie skompromitowaną aplikację backupową)."

Dodatkowo opisywany powyżej scenariusz usunięcia/skompromitowania danych przedstawiony w dokumentacji ExaGrid – w swej dalszej części:

„Since the Repository Tier data has a delayed delete time lock, the objects are still intact and available to restore. With Auto Detect & Guard the system automatically identifies
a unique delete pattern and automatically indefinitely extends the delayed delete policy, as well as alerts IT to the potential attack."

w tłumaczeniu:

„Ponieważ dane w warstwie repozytorium mają opóźnioną blokadę czasową usuwania, obiekty pozostają nienaruszone i dostępne do przywrócenia. Dzięki funkcji Auto Detect & Guard system automatycznie identyfikuje unikalny wzorzec usuwania i automatycznie rozszerza zasady opóźnionego usuwania na czas nieokreślony, a także powiadamia dział IT o potencjalnym ataku."

nie polepsza sytuacji w przypadku, gdy na urządzeniu ExaGrid zapisywane są nowe bądź zmienione w stosunku do poprzednich kopii dane – dotychczas nie przechowywane na urządzeniu – gdyż w takim wypadku nie można ich odtworzyć z obszaru „Retention Tier" (repozytorium danych) mimo zastosowania „opóźnionej blokady", gdyż tych danych tam nie ma.

•Ryzyko operacyjne i utrata RPO:

Z perspektywy Centrum e-Zdrowia wartość systemu backupu mierzy się zdolnością do odtworzenia stanu z momentu awarii (RPO - Recovery Point Objective).

•Okno podatności (Time-to-Protect): W architekturze ExaGrid dane są przenoszone z Landing Zone do bezpiecznego Retention Tier dopiero w procesie *„Adaptive Deduplication".* W przypadku dużych kopii zapasowych (np. weekendowych Full Backup), dane mogą przebywać w niechronionej strefie Landing Zone przez wiele godzin, zanim trafią do bezpiecznego repozytorium.

W scenariuszu ataku: Atak ransomware zazwyczaj następuje w nocy, równolegle
z oknem backupowym. Atakujący, posiadając uprawnienia do sieci backupowej, może usunąć lub zaszyfrować pliki w Landing Zone w trakcie ich zapisywania lub tuż po zapisaniu. Następuje wówczas skutek krytyczny: Ponieważ dane te nie zdążyły zostać zmigrowane do Retention Tier (lub zostały usunięte przed migracją), mechanizm "Retention Time-Lock" (działający tylko w RT) jest bezużyteczny.

Zamawiający traci najświeższą, najbardziej krytyczną kopię danych. W przypadku zaszyfrowania infrastruktury produkcyjnej, brak kopii z ostatniej doby oznacza nieodwracalną utratę np. tysięcy rekordów medycznych lub transakcji.

Rozwiązanie chroniące *tylko „dane historyczne"* (wczorajsze i starsze), a wystawiające na ryzyko „dane bieżące", nie realizuje celu zamówienia jakim jest zapewnienie bezpieczeństwa ciągłości działania.

Standardem rynkowym wymaganym w OPZ (zabezpieczenie przed modyfikacją/usunięciem) są rozwiązania typu Inline Immutability (dostępne np. w Dell Data Domain, HPE StoreOnce, rozwiązaniach Object Storage z funkcją Objec Lock). W tych technologiach blokada zakładana jest natychmiast po zapisaniu bloku danych. Nawet administrator z najwyższymi uprawnieniami ("root") nie może usunąć tych danych przed upływem czasu retencji.

ExaGrid z otwartą strefą Landing Zone nie oferuje tego poziomu bezpieczeństwa ("Zero Trust"), polegając jedynie na politykach, a nie fizycznej niezmienności danych w punkcie styku z siecią.

Reasumując Odwołujący wywodził, że:

•dane (w tym przeterminowane – dane o krótkiej retencji przechowywania, nie zmigrowane do obszaru Retention Tier) mogą zostać usunięte przez aplikację backup'ową - co jest w sprzeczności z wymaganiem dot. możliwości usuwania danych jedynie w procesie czyszczenia - ppkt 4.4.4 (aplikacja backupowa nie ma nic wspólnego z procesem

czyszczenia, który jest wewnętrznym procesem oferowanego urządzenia),

•dane znajdujące się w Landing Zone - nie zmigrowane do Retention Tier są danymi „przechowywanymi" na urządzeniu (zgodnie z nomenklaturę użytą w OPZ – ppkt 4.4.5) – nie są objęte mechanizmem uniemożliwiającym modyfikację bądź usunięcie. WSZYTKIE DANE PRZECHOWYWANE na urządzeniu w pewnym okresie znajdują się Landing Zone przez co są podatne na atak, w związku z powyższym oferowany mechanizm zabezpieczenia danych nie spełnia wymagania ppkt 4.4.6.

W trakcie oceny ofert Zamawiający działając w trybie art. 223 ust 1 Pzp w dniu 29.12.2025r. skierował do wykonawcy HUB4 wezwanie do udzielenia wyjaśnień
w przedmiocie spełniania wymagań:

Wykonawca HUB4 pismem z dnia 05.01.2026 r. udzielił wyjaśnień w odniesieniu do poszczególnych wymagań:

Ad 4.4.4. Wykonawca HUB4 wyjaśnił:

Zgodnie z wyjaśnieniem HUB4 dane trafiają najpierw na Landing Zone, a następnie są deduplikowane i umieszczane w Repository Tier. Oznacza to, że na Landing Zone nie jest zakładany Retention Time Lock i dane tam umieszczone mogą podlegać modyfikacji, poprzez umieszczenie szkodliwego oprogramowania, skasowania itd. - stanowi to niespełnienie punktu 4.4.4.

Ad 4.4.5. Wykonawca HUB4 wyjaśnił:

Zgodnie z wyjaśnieniem HUB4 dane trafiają najpierw na Landing Zone, a następnie są deduplikowane i umieszczane w Repository Tier. Oznacza to, że na Landing Zone nie jest zakładany Retention Time Lock i dane tam umieszczone mogą podlegać modyfikacji, poprzez umieszczenie szkodliwego oprogramowania lub usunięciu. W przypadku protokołów CIFS
i NFS, które są udostępniane między serwerami jako udziały sieciowe dane, które tam trafią mogą być zmodyfikowane, zainfekowane groźnym oprogramowaniem z hosta, którego zabezpieczenia pokonał atakujący. Następnie rozprzestrzenione na pozostałe hosty, które współdzielą zasób, ponieważ Retention Time Lock nie zostanie nałożony po utworzeniu dokumentu w Landing Zone, a te dane są serwowane jako pierwsze dla pozostałych hostów - stanowi to niespełnienie punktu 4.4.5. dla protokołów CIFS/NFS.

Ad 4.4.6. Wykonawca HUB4 wyjaśnił:

Zgodnie z wyjaśnieniem HUB4 dane trafiają najpierw na Landing Zone, a następnie są deduplikowane i umieszczane w Repository Tier. Oznacza to, że na Landing Zone nie jest zakładany Retention Time Lock i dane tam umieszczone mogą podlegać modyfikacji, poprzez umieszczenie szkodliwego oprogramowania (np.:Ransomware). Dane z Landing Zone są wykorzystywane w procesie odtwarzania dla najświeższych kopii. Czyli modyfikując dane
w Landing Zone zainfekujemy docelowy serwer, na który te dane będą odtwarzane. Co stanowi obejście zabezpieczeń i bezpośrednie niespełnienie punktu 4.4.6.

W ocenie Odwołującego z opisanych powodów zaoferowane przez wykonawcę HUB4 rozwiązanie jest niezgodne z warunkami zamówienia a oferta winna być odrzucona na podstawie art. 226 ust 1 pkt 5 Pzp.

<u>Zarzuty dotyczące niewykazania spełniania warunku udziału w zakresie doświadczenia zawodowego przez wykonawcę HUB4.</u>

Zgodnie z SWZ Zamawiający określił następujący warunek podmiotowy udziału
w postępowaniu dotyczący doświadczenia zawodowego:

Rozdział V SWZ pkt 1.4.

Wykonawca spełni warunek jeżeli wykaże w wykazie wykonanych dostaw,
a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, że w okresie ostatnich 5 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej dwa zamówienia o wartości co najmniej 9 000 000,00 zł brutto każde, obejmujące swoim zakresem dostawę i/lub rozbudowę deduplikatorów.*

W trakcie postępowania wykonawcy wnosili do Zamawiającego o dokonanie modyfikacji warunku

Zamawiający podtrzymał jednak wymóg aby wykonawca legitymował się min 2 zamówieniami referencyjnymi, z których każde miało posiadać wartość min 9 mln zł brutto oraz obejmowało będzie swoim zakresem dostawę i/lub rozbudowę deduplikatorów.

Wykonawca HUB4 w celu potwierdzenia spełnienia warunku udziału w zakresie doświadczenia zawodowego powołał się na następujące zamówienia referencyjne:

Jednocześnie złożono w charakterze poświadczeń należytego wykonania wykazanych zamówień następujący dokument referencyjny:

1.Reference letter.pdf

2.Reference letter-tlumaczenie.pdf

W złożonym Wykazie dostaw Wykonawca wykazał 2 pozycje realizowane na rzecz ITDZ Berlin (na kwoty 9 367 550 zł oraz 10 975 000 zł). Na potwierdzenie ich należytego wykonania załączono dwa dokumenty referencyjne wystawione przez ITDZ Berlin dla podmiotu udostępniającego zasoby (PDV-Systemhaus GmbH), opatrzone datami 15.11.2023 r. oraz 12.11.2024 r.

Zdaniem Odwołującego z dokumentów tych nie wynika, czy faktycznie wykazane doświadczenie spełnia wymóg ilościowy postawiony w SWZ (tj. realizacja co najmniej dwóch zamówień). Z treści ogólnych dokumentów referencyjnych oraz Wykazu dostaw nie wynika jednoznacznie, czy wskazane dostawy stanowią dwa odrębne, niezależne od siebie stosunki zobowiązaniowe (dwie odrębne umowy), czy też są to referencje częściowe wystawione
z tytułu realizacji poszczególnych etapów (transz) w ramach jednej, zawartej na wyższą kwotę umowy. W świetle powyższego Odwołujący uważa, że konieczne jest wezwanie wykonawcy do uzupełnienia podmiotowych środków dowodowych w trybie art. 128 ust 1 Pzp względnie udzielenia wyjaśnień na podstawie art. 128 ust 4 Pzp.

Odnośnie do formy listów referencyjnych, to dokumenty zawierają wyłącznie adnotację o złożeniu podpisu elektronicznego:

Na przekazanym przez HUB4 pliku PDF zawierającym referencje widnieje informacja graficzna (stempel/wizualizacja) o treści: „Digital unterschrieben von Schroer Torsten Datum: 2025.12.16”.

Po przeprowadzeniu weryfikacji struktury przekazanych plików elektronicznych, dokument nie zawiera takiego podpisu w dokumencie, który został dostarczony Zamawiającemu.

Przekazane pliki PDF nie zawierają rzeczywistej, kryptograficznej warstwy podpisu elektronicznego złożonego przez wystawcę dokumentu (Pana T.S.).

Złożone pliki stanowią jedynie graficzne odwzorowanie (tzw. faksymile lub "wydruk do PDF") dokumentu, pozbawione elektronicznej warstwy podpisu, co uniemożliwia Zamawiającemu weryfikację dokumentu oraz weryfikację ważności podpisu elektronicznego jego wystawcy a samo dodanie do takiego dokumentu podpisów kwalifikowanych wykonawcy jest nieprawidłowe w świetle przepisów wykonawczych do ustawy Pzp.

Zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r.
w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu
o udzielenie zamówienia publicznego lub konkursie w § 6 ust. 1 wskazuje się, że *w przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty, w tym dokumenty, o których mowa w art. 94 ust. 2 ustawy, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument.*

Wykonawca jest zatem zobowiązany był przekazać Zamawiającemu ten oryginalny plik zawierający nienaruszoną warstwę podpisu elektronicznego wystawcy. Z dokumentu wynika, że został podpisany podpisem elektronicznym – tymczasem dokument faktycznie takiego podpisu elektronicznego nie zawiera. W świetle powyższego konieczne jest wezwanie do uzupełnienia dokumentu w trybie art. 128 ust 1 Pzp.

Mając powyższe na względzie Odwołujący wnosił o uwzględnienie odwołania.

Po przeprowadzeniu rozprawy z udziałem Stron i Uczestnika postępowania odwoławczego, na podstawie zgromadzonego w sprawie materiału dowodowego oraz oświadczeń, a także stanowisk Stron i Uczestnika postępowania, Krajowa Izba Odwoławcza ustaliła i zważyła, co następuje:

Izba ustaliła, iż nie została wypełniona żadna z przesłanek skutkujących odrzuceniem odwołania, odwołanie nie zawierało braków formalnych i mogło zostać rozpoznane merytorycznie.

W ocenie Izby Odwołujący wykazał interes we wniesieniu odwołania i możliwość poniesienia szkody w postaci utraty zamówienia i osiągnięcia zysku. Odwołujący złożył
w postępowaniu ofertę, natomiast Zamawiający uznał ofertę Przystępującego za najkorzystniejszą. W ocenie Odwołującego Zamawiający dokonał badania i oceny ofert, a więc także wyboru oferty najkorzystniejszej z naruszeniem przepisów ustawy Pzp. Działania te oznaczają, że Odwołujący nie uzyska zamówienia i nie osiągnie zysku z jego realizacji.

Zgłoszenie przystąpienia do postępowania odwoławczego po stronie Zamawiającego złożył Wykonawca HUB4 Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie. Izba potwierdziła skuteczność zgłoszenia i dopuściła

Wykonawcę jako Przystępującego.

Zamawiający i Przystępujący w złożonych pisemnych stanowiskach procesowych wnosili o oddalenie odwołania. Przystępujący na posiedzeniu złożył materiał dowodowy
w postaci wyciągów z dokumentacji źródłowej urządzenia, do których odwoływał się
w stanowisku pisemnym oraz oświadczenie producenta, że oferowane urządzenie spełnia wszystkie wymogi opisu przedmiotu zamówienia.

Izba ustaliła, że Strony i Uczestnik postępowania wiernie przytoczyły postanowienia SWZ i OPZ, istotne dla rozstrzygnięcia sporu, nie zachodziła konieczność ich powtarzania.

Odwołujący na rozprawie złożył oświadczenie o wycofaniu zarzutów odnoszących się do potwierdzenia spełnienia warunku udziału w postępowaniu i nieprawidłowej formy złożonej referencji. W tym zakresie postępowanie odwoławcze podlegało umorzeni, co odzwierciedla punkt 1 sentencji.

Biorąc pod uwagę poczynione ustalenia i stanowiska Stron oraz Uczestnika postępowania odwoławczego, Izba uznała, że odwołanie w zakresie podtrzymywanym podlega oddaleniu, co uwidoczniono w punkcie 2 sentencji orzeczenia.

Zgodnie z zapisami SWZ Zamawiający wymagał:

4.4.4 *Ze względów bezpieczeństwa Urządzenie musi zabezpieczać dane przed możliwością nadpisania, a dane przeterminowane powinny być usuwane jedynie w procesie czyszczenia.*

4.4.5 Zintegrowana ochrona przed ransomware: Urządzenie musi posiadać zintegrowany mechanizm ochrony danych przed nieautoryzowanymi zmianami, usunięciem (np. ataki ransomware, błędy ludzkie). Mechanizm ten może opierać się na funkcji nieusuwalności (immutability/WORM - Write Once, Read Many lub innym rozwiązaniu) dla przechowywanych danych, co uniemożliwi ich modyfikację lub usunięcie przed upływem zdefiniowanego okresu retencji. Mechanizm musi być dostępny dla protokołów CIFS, NFS i dedykowanego protokołu, jeśli taki jest dostępny.

4.4.6 Integracja mechanizmu ransomware nieusuwalności danych musi być oficjalnie wspierany przez aplikację systemu kopii zapasowych używaną przez zamawiającego,
o którym mowa w punkcie 3 OPZ, używaną do zapisu danych na Urządzeniu. Wykonawca musi przedstawić potwierdzenie tej kompatybilności, np. w postaci linku do oficjalnej dokumentacji systemu kopii zapasowych używanego przez zamawiającego lub oficjalnej dokumentacji producenta urządzenia. Mechanizm ten musi być konfigurowalny i kontrolowany w taki sposób, aby zapewnić skuteczną ochronę przed modyfikacją/usunięciem danych bezpośrednio na Urządzeniu, niezależnie od prób obejścia zabezpieczeń przez oprogramowanie zewnętrzne (w tym potencjalnie skompromitowaną aplikację backupową).

Nie było sporne między stronami, że architektura rozwiązania oferowanego przez Przystępującego jest warstwowa, składa się z dwóch warstw (LZ i RT). Nie było także sporne, iż Zamawiający w OPZ obowiązującym w postępowaniu dopuścił takie rozwiązania.

W ocenie Izby, za Zamawiającym i Przystępującym, powtórzyć należy, iż interpretacja warunków opisu zamówienia przedstawiona przez Odwołującego ma charakter rozszerzający w stosunku do rzeczywistych zapisów SWZ i OPZ. Zamawiający postawił wymagania dla urządzenia. Jest to twierdzenie prawdziwe. Jednocześnie Zamawiający dopuszczając różne rozwiązania ochrony danych nie zaznaczył, że w przypadku rozwiązań opartych o architekturę warstwową momentem rozpoczęcia ochrony ma być moment wprowadzenia danych do strefy roboczej, w przypadku Przystępującego będzie to LZ. W tym zaznaczeniu interpretację zapisów OPZ przedstawioną w odwołaniu należy uznać za rozszerzającą.

Zamawiający, zdaniem Izby, właśnie jasno sprecyzował, że to „urządzenie" ma posiadać określone właściwości. Jednocześnie nie doprecyzowano w żaden sposób jaka ścieżka ma umożliwić osiągnięcie wymaganych funkcjonalności. Urządzenie oferowane przez Przystępującego co do zasady spełnia wszystkie wymagania OPZ, ponieważ mechanizm ExaGrid Retention Time-Lock jest zapewniony w warstwie Retention Tier, spełnione są także inne wymagania przywołane w odwołaniu z punktów 4.4.4 do 4.4.6. Tym samym „urządzenie" jako całość rozwiązania posiada wymaganą funkcjonalność. Zamawiający w OPZ nie dokonał rozróżnienia opisu posiłkując się nawiązaniem do architektury danego rozwiązania. Było wręcz odwrotnie. Zamawiający zaznaczył, że osiągnięcie danej funkcjonalności może być oparte
o rożne rozwiązania: immutability (stosowane w rozwiązaniu oferowanym przez Odwołującego), WORM - Write Once, Read Many lub innym rozwiązaniu. Takim innym rozwiązaniem jest to zaoferowane przez Przystępującego.

Izba podziela stanowisko, że Odwołujący błędnie utożsamia pojęcie „Urządzenia"
z każdą warstwą logiczną urządzenia. W przedmiotowym postępowaniu pojęcie „urządzenia" nie zostało w ten sposób zdefiniowane. Opis przedmiotu zamówienia referował do definicji funkcjonalnej, wymagał osiągnięcia danej funkcjonalności bez uszczegółowiania ścieżki prowadzącej do rezultatu końcowego. Zatem każda ścieżka, w wyniku której dana i wymagana funkcjonalność zostanie osiągnięta spełniała wymagania Zamawiającego, o ile finalnie oferowane urządzenie posiadało będzie opisane cechy. W żadnym z przywołanych zapisów

w punkach 4.4.4 do 4.4.6 Zamawiający nie oznaczył znacznika czasowego, powiązanego z momentem wprowadzenia danych do urządzenia, jak już wspomniano - nie dokonał także rozróżnienia dla rozwiązań warstwowych. Nie ma zaś wątpliwości, że Odwołujący niespełnienie wymagań rozwiązania oferowanego przez Przystępującego wywodzi z warstwowej budowy tego rozwiązania. Zdaniem Izby Zamawiający w przedmiotowym postępowaniu traktował „urządzenie" jako całość, a więc „całościowo" dane rozwiązanie techniczne miało spełniać opisane wymagania.

Przystępujący w żadnym momencie nie ukrywał w jaki sposób oferowane rozwiązanie spełnia wymagania funkcjonalne. W toku postępowania o udzielenie zamówienia publicznego Przystępujący złożył wyczerpujące wyjaśnienia związane z ExGrid. Treścią oferty są linki do oficjalnej dokumentacji technicznej oferowanego rozwiązania, z których sam Odwołujący czerpał wiedzę na temat szczegółowego sposobu działania danego rozwiązania. W ocenie Izby Odwołujący w odwołaniu przedstawił rozszerzającą interpretację zapisów SWZ i OPZ, wywodząc z nich wymagania dla zamawianego przedmiotu zamówienia, które z opisu przedstawionego przez Zamawiającego nie wynikały.

Hipotetycznie przyjmując, że intencje Zamawiającego były zbieżne z wyrażonymi w odwołaniu, to dostrzeżenia wymaga, iż zgodnie z ugruntowanym stanowiskiem orzecznictwa i doktryny wszelkie niejednoznaczności zapisów SWZ tłumaczy się na korzyść wykonawców. Zgodnie z wyrokiem Sądu Okręgowego w Warszawie z 31 maja 2022 r. sygn. akt: XXIII Zs 58/22 *„wszelkie niejasności, dwuznaczności, niezgodności należy rozpatrywać na korzyść wykonawcy, co ma na celu realizację zasady uczciwej konkurencji i równego traktowania".*

Sąd Okręgowy w Szczecinie w wyroku z dnia 7 marca 2018 r., sygn. akt VIII Ga 102/18 wskazał, że *„obowiązywanie reguły interpretacyjnej „na korzyść wykonawcy" uzasadnia także jej związek z wyrażoną w art. 7 ust. 1 Pzp* (obecnie art. 16 ustawy Pzp – dopisek Izby) *kwestią przejrzystości, która oznacza również zakaz wyciągania negatywnych konsekwencji wobec wykonawcy wskutek niedopełnienia przez niego obowiązku, który nie wynika wyraźnie z dokumentacji przetargowej lub obowiązujących przepisów prawa krajowego, lecz jedynie z wykładni tych przepisów lub dokumentacji, a także z uzupełniania przez krajowe organy lub sądownictwo występujących w tej dokumentacji luk*". Zatem Przystępującego nie mogą na danym etapie postępowania o udzielenie zamówienia publicznego, obciążać zapisy SWZ, które można by interpretować na różne sposoby.

Niezgodność treści oferty z warunkami zamówienia, która stanowi obligatoryjną przesłankę odrzucenia oferty, zachodzi, gdy zawartość merytoryczna złożonej w danym postępowaniu oferty nie odpowiada pod względem przedmiotu zamówienia albo sposobu wykonania przedmiotu zamówienia ukształtowanym przez Zamawiającego i zawartym w SWZ wymaganiom (wyrok KIO z dnia 19 lutego 2021 r., sygn. akt KIO 268/21).

Przewidziane w przepisie art. 226 ust. 1 pkt 5 ustawy Pzp odrzucenie oferty skutkuje tym, że oferta zostaje wyeliminowana z postępowania, co w konsekwencji przekreśla szanse wykonawcy, który ją złożył, na uzyskanie zamówienia. Zatem tak istotna i brzemienna w skutki czynność Zamawiającego, jaką jest odrzucenie oferty, może być podjęta wyłącznie wtedy, gdy zachodzi niewątpliwa i jednoznaczna niezgodność treści oferty z warunkami zamówienia określonymi przez Zamawiającego. Niezgodność ta musi wynikać wprost z postanowień SWZ i nie może być domniemywana albo też wyinterpretowana z jakichkolwiek treści.

Izba, podzielając stanowisko Zamawiającego i Przystępującego, uważa, że zapisy SWZ i opis przedmiotu zamówienia nie zamykały możliwości zaoferowania rozwiązania zbudowanego w oparciu o architekturę warstwową, jednocześnie wymagania bezpieczeństwa danych Zamawiający opisał w stosunku do urządzenia rozumianego jako całość rozwiązania, nie zaś jak przedstawiał to Odwołujący – w stosunku do warstw danego rozwiązania.

Nie ulegało wątpliwości, że rozwiązanie oferowane przez Przystępującego jako całość spełnia wymagania SWZ. Zatem twierdzenia odwołania, że rozwiązanie *„nie chroni w sposób ciągły i pełny, a jedynie wybiórczy (tylko w jednej z warstw), co stoi w sprzeczności z definicją bezpiecznego przechowywania danych w systemach klasy Enterprise*" nie mogły zostać uwzględnione.

Izba uznała, iż Zamawiający badając dokonując wyboru oferty najkorzystniejszej nie naruszył zasad prowadzenia postępowania wynikających z art. 16 i 17 ustawy Pzp oraz art. 239 ustawy Pzp. Wyboru oferty najkorzystniejszej dokonano na podstawie kryteriów oceny ofert ustalonych w postępowaniu.

W świetle powyższych ustaleń Izba uznała za niezasadne zarzuty odwołania i oddaliła odwołanie w całości.

O kosztach postępowania odwoławczego orzeczono na podstawie art. 574 oraz art. 575 ustawy Pzp, a także w oparciu o przepisy § 5 pkt 1 i 2 lit. b oraz § 8 ust. 2 pkt 1 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 roku w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. z 2020r., poz. 2437 ze zmianami), orzekając w tym zakresie o obciążeniu kosztami postępowania stronę przegrywającą, czyli Odwołującego.

Przewodnicząca:

……