Sygn. akt: KIO 2974/25

WYROK

Warszawa, dnia 28 lipca 2025 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodnicząca:Luiza Łamejko

Protokolant:Tomasz Skowroński

po rozpoznaniu na rozprawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 18 lipca 2025 r. przez wykonawcę GRUPA E Sp. z o.o. z siedzibą w Tychach

w postępowaniu prowadzonym przez Miasto Katowice

uczestnik po stronie zamawiającego – wykonawca COIG S.A. z siedzibą w Katowicach

orzeka:

1.Oddala odwołanie.
2.Kosztami postępowania obciąża wykonawcę GRUPA E Sp. z o.o. z siedzibą w Tychach i zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawcę GRUPA E Sp. z o.o.
z siedzibą w Tychach tytułem wpisu od odwołania oraz kwotę 3 749 zł 00 gr (słownie: trzy tysiące siedemset czterdzieści dziewięć złotych zero groszy) poniesioną przez GRUPA E
Sp. z o.o. z siedzibą w Tychach tytułem wynagrodzenia pełnomocnika i dojazdu na posiedzenie Izby.

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 2974/25

U z a s a d n i e n i e

Miasto Katowice (dalej: „Zamawiający") prowadzi w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia publicznego pod nazwą „Wdrożenie systemu klasy XDR w Urzędzie Miasta Katowice". Postępowanie to prowadzone jest na podstawie przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 ze zm.), zwanej dalej: „ustawy Pzp". Ogłoszenie o zamówieniu zostało opublikowane
w Dzienniku Urzędowym Unii Europejskiej w dniu 7 maja 2025 r. pod nr 292595-2025.

W dniu 18 lipca 2025 r. wykonawca GRUPA E Sp. z o.o. z siedzibą w Tychach (dalej: „Odwołujący") wniósł do Prezesa Krajowej Izby Odwoławczej odwołanie wobec czynności
i zaniechań Zamawiającego polegających na:

- zaniechaniu odrzucenia oferty wykonawcy COIG S.A. z siedzibą w Katowicach (dalej: „COIG") mimo jej niezgodności z treścią dokumentów zamówienia polegającej na niespełnianiu przez zaoferowane oprogramowanie Eset Protect Elite wymogu integracji
z zaawansowaną zaporą sieciową Palp Alto PA5420 (dalej: UTM Palo Alto), którą dysponuje w swoim zasobie Zamawiający;

- niedopuszczalnej negocjacji treści oferty wybranego wykonawcy po terminie składania ofert, w wyniku której doszło do uzgodnienia między Zamawiającym a wybranym wykonawcą do ustaleń skutkujących zmianą treści oferty wybranego wykonawcy.

Odwołujący zarzucił Zamawiającemu naruszenie:

- art. 223 ust. 1 ustawy Pzp przez przeprowadzenie niedopuszczalnych negocjacji treści oferty wykonawcy COIG po terminie składania ofert, w wyniku której doszło między Zamawiającym a wybranym wykonawcą do ustaleń co do treści oferty COIG skutkujących istotną zmianą treści tej oferty w stosunku do jej pierwotnego brzmienia ustalonego w dniu składania i otwarcia ofert;

- art. 226 ust. 1 pkt 5) ustawy Pzp przez zaniechanie odrzucenia oferty wybranego wykonawcy, mimo że jest ona niezgodna z warunkami zamówienia w ten sposób, że zaoferowane
w ramach wybranej oferty oprogramowanie Eset Protect Elite nie spełnia wymogu integracji

z UTM Palo Alto wymaganego postanowieniami aut. 2.2. w związku 3.18. załącznika nr 10 do SWZ pn.*Opis Przedmiotu Zamówienia Usługi monitoringu infrastruktury za pomocą narzędzi XDR Urzędu Miasta Katowice dla projektu: Wdrożenie systemu klasy XDR w Urzędzie Miasta Katowice* (dalej „OPZ"), natomiast zmieniona w wyniku niedopuszczalnych negocjacji oferta COIG opiewa na dwa odrębne systemy i nie spełnia wymogu jednego spójnego interfejsu.

Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu:

- unieważnienia czynności wyboru najkorzystniejszej oferty z 8 lipca 2025 r.,

- powtórzenia czynności badania i oceny ofert oraz odrzucenia oferty wybranego wykonawcy jako niezgodnej z warunkami zamówienia,

- zasądzenie od Zamawiającego na rzecz Odwołującego kosztów postępowania, w tym kosztów reprezentacji wg przedstawionych na rozprawie rachunków.

Odwołujący wskazał, że Zamawiający prowadzi postępowanie na usługę wsparcia i monitoringu w zakresie cyberbezpieczeństwa infrastruktury sieciowo-serwerowej. Usługa ma być realizowana przy użyciu narzędzia XDR, tj. oprogramowania cyberbezpieczeństwa, które integruje i automatyzuje wykrywanie oraz reagowanie na zagrożenia w wielu warstwach zabezpieczeń. Zgodnie z rozdziałem. 1.1. OPZ pt.*Wstęp: Usługi będą realizowane poprzez narzędzia XDR, które zostaną dostarczone, udostępnione i zainstalowane w infrastrukturze Urzędu Miasta Katowice oraz zostanie uruchomiona obsługa SOC 24h przez okres trwania projektu. Infrastruktura musi zostać monitorowana systemem klasy XDR (Extended\Endpoint Detection and Response, tzn. zaawansowane oprogramowanie ochrony stacji roboczych i serwerów przed zagrożeniami cyberbezpieczeństwa posiadające m.in. funkcjonalność ochrony antywirusowej, możliwość gromadzenia informacji o zdarzeniach oraz rozbudowane funkcje reakcji na incydenty).*

Jak wskazał Odwołujący, zgodnie z wyliczeniem zawartym w rozdziale 2.2. OPZ pt. Infrastruktura Zamawiającego objęta zamawianymi usługami Zamawiający wskazał następujące urządzenia, które mają być nimi objęte:

Zamawiający posiada w swojej infrastrukturze następujące urządzenia, które muszą zostać objęte usługami XDR lub integracją z dostarczanym systemem lub dostarczanymi systemami XDR:

1. *Komputer klasy PC z zainstalowanym Microsoft Windows w domenie AD – 1400 szt.*
2. *Serwery wirtualne Windows Server i Linux w infrastrukturze Wmware – 319 szt.*
3. *Serwer pocztowy MS Exchange pracujący w klastrze z filtrowaniem poprzez proxy Baracuda Email Gateway Security – 1 system*
4. *UTM Palo Alto 5420 w wersji Appliance – 2 szt.*

Wymaga się, aby systemy UTM i Proxy były zintegrowane z dostarczaną infrastrukturą XDR.

Zgodnie z rozdziałem 3.1. OPZ pt. *Wymagania podstawowe* Zamawiający wskazał, że celem Zamawiającego jest dostawa subskrypcji na system bezpieczeństwa klasy XRD (dalej System) na okres minimum 2 lat dla wszystkich wymienionych wyżej endpointów (urządzeń – przypis Odwołującego).

Dalej w ust. 9, 10 i 13 rozdziału 3.1. OPZ pt.*Wymagania podstawowe* Zamawiający wskazał: (9) *System w całości ma być dostarczony od jednego producenta, a jeżeli jest to uzasadnione jakościowo system może być złożony hybrydowo z maksymalnie oprogramowanie dwóch producentów.* (10) *System musi umożliwiać zarządzanie przez pojedynczy webowy interfejs graficzny z wykorzystaniem graficznej przeglądarki internetowej, dostępny po https (co najmniej TLS 1.2). Nie dopuszcza się, aby webowy interfejs graficzny korzystał z technologii flash, silverlight lub java z uwzględnieniem pkt. wyżej.;* (13) *Wszystkie składniki systemu XDR muszą być konfigurowalne i zarządzane przez spójny interfejs.*

W rozdziale 3.18. OPZ pt.*Integracja z UTM* Zamawiający jasno określił, że *Dostarczany system musi mieć możliwość zbierania i wyświetlania logów z systemów UTM Zamawiającego. Licencje na dostęp do UTM firmy Palo Alto zostaną w przyszłości dostarczone przez Zamawiającego.*

Odwołujący wskazał, że przedmiotem oferty wybranego wykonawcy, zgodnie z ofertą z 5 czerwca 2025 r., jest system Eset Protect Elite wyprodukowany przez słowackiego producenta ESET, co jasno wynika z formularza oferty COIG oraz załączonego do oferty załącznika pn. Numery oferowanych licencji lub cechy użytkowe – załącznik pecyfikacja_eset.pdf. Odwołujący zwrócił uwagę, że z żadnego z dokumentów lub oświadczeń złożonych przez wybranego wykonawcę do terminu skłania ofert nie wynika, że przedmiotem jego oferty jest jakiekolwiek inne oprogramowanie jakiegokolwiek innego producenta w zakresie dostawy subskrypcji na system bezpieczeństwa klasy XDR wymagane w pkt 3 OPZ. Odwołujący wskazał ponadto, że wykonawca COIG był dwukrotnie wzywany przez Zamawiającego do złożenia wyjaśnień – pisma z dnia 11 czerwca 2025 r. i 18 czerwca 2025 r. COIG złożył wyjaśnienia pismami z dnia 13 czerwca 2025 r. oraz 23 czerwca 2025 r.

Uzasadniając zarzut naruszenia art. 223 ust. 1 ustawy Pzp –niedozwolone negocjacje treści oferty po terminie składani ofert Odwołujący stwierdził, że oczywiste jest, że przedmiotem oferty wybranego wykonawcy jest system cyberbezpieczeństwa klasy XDR pn. ESET Protect Elite, co jasno wynika z formularza ofertowego COIG oraz załączonego do oferty przez tego wykonawcę oświadczenia pn. Numery oferowanych licencji lub cechy użytkowe – załącznik specyfikacja_eset.pdf, który zawierał wyspecyfikowanie oferowanego przez COIG oprogramowania (licencji).

Jak zauważył Odwołujący, w wyniku badania ofert Zamawiający zwrócił uwagę na niezgodność oferowanego przez COIG systemu XDR ESET Protect Elite z dokumentami zamówienia w postaci braku możliwości integracji z urządzeniami UTM Palo Alto, które znajdują się w infrastrukturze Zamawiającego, które ma objąć zamawiana usługa.

Odwołujący zwrócił uwagę, że po terminie składania ofert, w odpowiedzi na wezwanie do wyjaśnień, wybrany wykonawca oświadczył, że w dla zabezpieczenia integracji
z urządzeniami UTM Palo Alto oferuje system SIEM/SOAR SecureVisio produkowany
i wspierany przez producenta Esecure sp. z o.o. z Rzeszowa.

Odwołujący podkreślił, że próżno szukać w ofercie COIG informacji, że przedmiotem jego oferty są dwa systemy: XDR ESET Protect Elite oraz SIEM/SOAR SecureVisio - oświadczenie o oferowaniu przez COIG licencji na system SIEM/SOAR SecureVisio pojawia się dopiero na etapie wyjaśnień, w reakcji na wyraźne braki systemu XDR ESET Protect Elite. Odwołujący zaznaczył, że składając ofertę w Postępowaniu COIG nie ofertował systemu SIEM/SOAR SecureVisio.

Zdaniem Odwołującego, akceptując ww. wyjaśnienia treści oferty COIG Zamawiający wprost dopuścił się uznania zmiany przedmiotu treści oferty COIG po terminie składania ofert przez rozszerzenie jej przedmiotu o nowy, dodatkowy element.

W zakresie zarzutu naruszenia art. 226 ust. 1 pkt 5 ustawy Pzp przez zaniechanie odrzucenia oferty niezgodnej z dokumentami zamówienia Odwołujący wskazał, że Zamawiający zwrócił uwagę na niezgodność oferowanego przez COIG systemu XDR ESET Protect Elite z dokumentami zamówienia w postaci braku możliwości integracji z urządzeniami UTM Palo Alto, które znajdują się w infrastrukturze Zamawiającego, które ma objąć zamawiana usługa.

Odwołujący stwierdził, że oferta COIG opiewająca na dostawę licencji na system XDR ESET Protect Elite jest niezgodna z dokumentami zamówienia, tj. z postanowieniem 3.18. OPZ, w którym Zamawiający postawił wymóg, aby to zamawiany system XDR był możliwy do zintegrowania z urządzeniami UTM Palo Alto w jego infrastrukturze i realizował zbieranie logów z urządzeń UTM Palo Alto.

W ocenie Odwołującego, zarówno wezwanie Zmawiającego, jak i wyjaśnienia COIG potwierdzają, że oferowany przez COIG system XDR pn. ESET Protec Elite nie jest możliwy do zintegrowania w zakresie zbierania i wyświetlania logów z urządzeniami UTM Palo Alto. Za tą przyczyną COIG po terminie składania ofert dla obsłużenia urządzeń UTM Palo Alto dodatkowo „rozszerzył" swoją ofertę o drugi system SIEM/SOAR SecureVisio dla obsłużenia funkcjonalności, o której mowa w rozdziale 3.18. OPZ, tj. integracji z urządzeniami UTM Palo Alto.

Odwołujący stwierdził, że treść wyjaśnień COIG w powiązaniu z wcześniejszym wezwaniem potwierdza, że okoliczność niespełniania przez samo XDR ESET Protect Elite wymogu z pkt 3.18 OPZ, jest okolicznością przyznaną przez COIG i Zamawiającego. Zdaniem Odwołującego, gdyby było inaczej nie byłoby potrzeby „uzupełniania" przedmiotu oferty wobec jej pierwotnej części. W konsekwencji, jak stwierdził Odwołujący, okoliczność ta nie wymaga dalszego dowodzenia.

Odwołujący zauważył ponadto, że nie jest możliwe tłumaczenie faktu niewpisania
w oferty oprogramowania SecureVisio tym, że COIG ma świadczyć na rzecz Zamawiającego usługę SOC. Odwołujący zwrócił uwagę, że konstrukcja dokumentacji zamówienia, w tym
w szczególności formularza ofertowego jednoznacznie wymagała wyszczególnienia
i odrębnego wskazania oprogramowania oferowanego Zamawiającego obok samej usługi SOC (obie te części były przedmiotem odrębnych rozliczeń).

Jak wskazał Odwołujący, licencje dodane w późniejszych wyjaśnieniach, a nie będące przedmiotem pierowtnej oferty (tj. SIEM/SOAR SecureVisio) umożliwiają wtórnie COIG spełnienie wymagań funkcji jednoznacznie oczekiwanej i opisanej (por. pkt 3.18 OPZ). Odwołujący podał, że funkcja ta jest ważna z wielu powodów. Przede wszystkim, System XDR (Extended Detection and Response) to zaawansowane rozwiązanie do cyberbezpieczeństwa, które łączy i analizuje dane z różnych źródeł, takich jak punkty końcowe, sieci, serwery
i chmura, w celu wykrywania i reagowania na zaawansowane zagrożenia. System XDR zapewnia holistyczne podejście do bezpieczeństwa, oferując usprawnione wykrywanie zagrożeń, analizę incydentów i automatyzację reakcji.

Jednocześnie, jak zauważył Odwołujący, pkt 3.18 OPZ sprowadza się do tego, że Zamawiający wymagał integracji oferowanego systemu XDR w zakresie zbierania
i wyświetlania logów z systemów UTM Palo-Alto (czyli logi z Palo-Alto mają trafiać bezpośrednio do systemu XDR).

Jak wyjaśnił Odwołujący, tego rodzaju funkcjonalność jest ważna i oferowana przez najlepsze systemy XDR, a w szczególności pozwala na:

- analizę logów przez system XDR,

- wykrywania zagrożeń zawartych w logach z systemu UTM Palo-Alto,

- aktywne reagowanie na zaawansowane zagrożenia zawarte w logach z systemu UTM Palo-Alto, których nie wykrył UTM,

- automatyczną reakcję na wykryte zaawansowane zagrożenia,

- wyświetlania logów w jednej spójnej konsoli (wymóg OPZ).

W przypadku, kiedy system XDR nie analizuje logów z systemu UTM, Zamawiający potrzebuje kolejnego systemu tzw. Analizatora logów dedykowanego przez producenta, który oferuje oczekiwane funkcje zbierania logów, analizy, wykrywania zagrożeń, aktywnego reagowania na zaawansowane zagrożenia, automatyczną reakcję na wykryte zagrożenia. Odwołujący zaznaczył, że pod krótkim opisem wymogu: „zbierania i wyświetlania logów z systemów UTM" realnie kryje się szereg funkcji wynikających z wymaganej integracji, które w bardzo wysokim stopniu podnoszą poziom bezpieczeństwa danych, informacji zawartych w systemach Zamawiającego.

Odwołujący podkreślił, że brak wskazania w ofercie produktu odpowiedzialnego za wypełnienie wymogu z pkt 3.18, dotyczy bardzo ważnej funkcji. W ocenie Odwołującego, nie jest to coś, co można potraktować za nieistotną omyłkę w treści oferty.

Odwołujący podniósł, że „dodanie" SIEM/SOAR SecureVisio zmienia przedmiotowo ofertę COIG z jednorodnej produktowo (w znaczeniu tożsamego producenta), w ofertę „hybrydową" czyli złożoną w dwóch producentów. Tymczasem Zamawiający w SWZ wskazał co następuje: pkt 3.1 ppkt 9: *„System w całości musi być dostarczony od jednego producenta, a jeżeli jest to uzasadnione jakościowo system może być złożony hybrydowo z maksymalnie oprogramowania dwóch producentów*".

Odwołujący zaznaczył, że dopiero po wezwaniu Zamawiającego i zapewne zauważeniu swojego błędu wykonawca COIG w wyjaśnieniach dokonał istotnej zmiany treści oferty przez wskazanie nowego produktu (licencje SecureVisio) oraz wskazanie, że rozwiązania dla pozycji nr 3 świadczone będą przez system złożony hybrydowo z oprogramowania dwóch producentów (licencje ESET oraz SecureVisio), a nie system jednorodny.

Na marginesie Odwołujący zauważył, że Zamawiający dopuścił do zmiany treści oferty nawet nie korzystając w tym zakresie z konieczności poprawienia oferty w myśl art. 223 ust. 2 pkt 3 ustawy Pzp, co zdaniem Odwołującego, z wyżej wskazanych przyczyn i tak byłoby niedopuszczalne).

Przystąpienie do postępowania odwoławczego po stronie Zamawiającego zgłosił wykonawca COIG.

W dniu 21 sierpnia 2025 r. Zamawiający złożył odpowiedź na odwołanie, w której wniósł o oddalenie odwołania w całości.

Krajowa Izba Odwoławcza, po przeprowadzeniu rozprawy w przedmiotowej sprawie, na podstawie zebranego materiału dowodowego wskazanego w treści uzasadnienia, jak też po zapoznaniu się z oświadczeniami i stanowiskami stron i uczestnika postępowania złożonymi pisemnie oraz ustnie do protokołu w toku rozprawy zważyła, co następuje.

Izba stwierdziła, że Odwołujący legitymuje się interesem we wniesieniu środka ochrony prawnej, o którym mowa w art. 505 ust. 1 ustawy Pzp. Zakres zarzutów, w sytuacji ich potwierdzenia się, wskazuje na pozbawienie Odwołującego możliwości uzyskania zamówienia i jego realizacji, narażając tym samym Odwołującego na poniesienie w tym zakresie wymiernej szkody.

Rozpoznając przedmiotowe odwołanie Izba miała na uwadze, że czynność odrzucenia oferty z uwagi na niezgodność z treścią dokumentów zamówienia, jako czynność eliminująca wykonawcę z postępowania, musi być podjęta w okolicznościach nie pozostawiających wątpliwości. Niezgodność stanowiąca podstawę odrzucenia oferty musi być jednoznaczna.

W przedmiotowej sprawie Izba nie stwierdziła takiej niezgodności. Izba miała na uwadze, że w Formularzu oferty, którego wzór ustanowił Zamawiający, Zamawiający wymagał wyceny dwóch elementów, tj.

- dostawy licencji ograniczonych czasowo – subskrypcji oprogramowania EDR i XDR, inwentaryzacji infrastruktury Zamawiającego oraz wdrożenia oprogramowania do zwalczania cyberzagrożeń oraz

- świadczenia na rzecz Zamawiającego Usług Zarządzania Cyberbezpieczeństwem – SOC.

W tym samym Formularzu Zamawiający wymagał złożenia oświadczenia co do nazwy i liczby oferowanych licencji w zakresie systemu EDR/XDR. Takie oświadczenie wykonawca COIG złożył i nie jest ono kwestionowane.

Treść OPZ wskazuje, że usługa SOC mogła być świadczona z użyciem dowolnych narzędzi. Jednocześnie,

Zamawiający nie sformułował jednoznacznego wymogu złożenia oświadczenia w zakresie narzędzi dla SOC - w tym przedmiocie Zamawiający wymagał jedynie wskazania ceny za wykonywanie usługi SOC, tabela w punkcie 1b Formularza oferty nie odnosi się do tej usługi.

W ocenie Izby, skoro Zamawiający nie wymagał wprost wskazania w ofercie narzędzi dla usług zarządzani cyberbezpieczeństwem, nie można czynić wykonawcy zarzutu z tytułu ich nie podania.

W toku procedury składania wyjaśnień treści (wyjaśnienia z dnia 13 czerwca 2025 r. i 23 czerwca 2025 r.) wykonawca COIG poinformował, że w ramach SOC będzie używał systemu SecureVisio, który jednocześnie służy do zbierania logów z UTM. Tego rodzaju rozwiązanie spełnia wymagania Zamawiającego i nie stanowi niezgodności z treścią dokumentów zamówienia.

Wobec powyższego, Izba za niezasadny uznała zarzut naruszenia przez Zamawiającego art. 226 ust. 1 pkt 5 ustawy Pzp przez zaniechanie odrzucenia oferty złożonej przez COIG.

Nie potwierdził się również zarzut naruszenia przez Zamawiającego art. 223 ust. 1 ustawy Pzp przez przeprowadzenie negocjacji treści oferty złożonej przez COIG po terminie składania ofert.

Izba stwierdziła, że z uwagi na brak wymogu określenia w ofercie narzędzi dla usług zarządzania cyberbezpieczeństwem i wobec dopuszczenia świadczenia usługi SOC
z użyciem dowolnych narzędzi, w toku wyjaśnień nie doszło do zmiany treści oferty, a jedynie pozyskania przez Zamawiającego informacji co do sposobu realizacji zamówienia, na którego określenie w ofercie nie było miejsca.

Mając powyższe na uwadze, orzeczono jak w sentencji.

O kosztach postępowania odwoławczego orzeczono stosownie do jego wyniku na podstawie art. 557 i 575 ustawy Pzp oraz § 8 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. z 2020 r. poz. 2437, dalej jako „rozporządzenie").

Jak stanowi art. 557 ustawy Pzp, w wyroku oraz w postanowieniu kończącym postępowanie odwoławcze Izba rozstrzyga o kosztach postępowania odwoławczego, z kolei w myśl art. 575 ustawy Pzp strony oraz uczestnik postępowania odwoławczego wnoszący sprzeciw ponoszą koszty postępowania odwoławczego stosownie do jego wyniku.

Jak stanowi § 8 ust. 2 pkt 1 rozporządzenia, w przypadku oddalenia odwołania przez Izbę w całości, koszty ponosi odwołujący. W takiej sytuacji Izba zasądza od odwołującego na rzecz zamawiającego koszty, o których mowa w § 5 pkt 2 rozporządzenia.

W świetle powyższych regulacji, Izba obciążyła kosztami postępowania odwoławczego Odwołującego.

Przewodnicząca:……..