WYROK

z dnia 1 marca 2019 r.

Krajowa Izba Odwoławcza – w składzie:

Przewodniczący: Piotr Kozłowski
Beata Konik
Jan Kuzawiński

Protokolant: Klaudia Ceyrowska

po rozpoznaniu na rozprawie **26 lutego 2019 r.** w Warszawie odwołań wniesionych **14 lutego 2019 r.** do Prezesa Krajowej Izby Odwoławczej przez wykonawców:
A.„Comtegra" S.A. z siedzibą w Warszawie (sygn. akt KIO 265/19)
B.Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie (sygn. akt KIO 266/19)

w postępowaniu pn. *Zakup licencji – rozbudowa oprogramowania systemu ochrony stacji końcowych użytkowników i serwerów* (nr postępowania 0000-ZP.261.15.2018)

prowadzonym przez zamawiającego: **Kasa Rolniczego Ubezpieczenia Społecznego z siedzibą w Warszawie**

przy udziale wykonawców zgłaszających swoje przystąpienia do postępowania odwoławczego:
A.Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie – po stronie odwołującego w sprawie o sygn. akt KIO 265/19
B.4PRIME sp. z o.o. z siedzibą w Warszawie –po stronie zamawiającego w sprawach o sygn. akt KIO 265/19 i KIO 266/19

orzeka:

1.Uwzględnia odwołania i nakazuje zamawiającemu Kasie Rolniczego Ubezpieczenia Społecznego z siedzibą w Warszawie:

1)unieważnienie odrzucenia ofert złożonych przez „Comtegrę" S.A. z siedzibą w Warszawie i Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie,
2)uznanie przy powtórnym badaniu ofert złożonych przez „Comtegrę" S.A. z siedzibą w Warszawie i Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie, że:

a)spełniają one wymogi z pkt 1.1.2. i 1.2.2. opisu przedmiotu zamówienia,
b)dla oceny spełniania przez nie wymogów z pkt 1.3.2. i 1.3.6. opisu przedmiotu zamówienia konieczne jest uprzednie wezwanie do przedstawienia specyfikacji technicznej oferowanego rozwiązania, a w razie powstania wątpliwości odnośnie treści oferty – wezwanie wykonawcy do ich wyjaśnienia.

2.Kosztami postępowania **w obu sprawach** obciąża **zamawiającego Kasę Rolniczego Ubezpieczenia Społecznego z siedzibą w Warszawie** i:

1)zalicza w poczet kosztów postępowania odwoławczego kwotę **30000 zł 00 gr** (słownie: trzydzieści tysięcy złotych zero groszy) uiszczoną łącznie przez **odwołujących** tytułem wpisów od odwołań,
2)zasądza od **zamawiającego** na rzecz **każdego z odwołujących** kwotę **18600 zł 00 gr** (słownie: osiemnaście tysięcy sześćset złotych zero groszy) – stanowiącą koszty postępowania odwoławczego poniesione z tytułu wpisu od odwołania oraz uzasadnionych kosztów strony obejmujących wynagrodzenie pełnomocnika.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2018 r. poz. 1986 ze zm.) na niniejszy wyrok – w terminie 7 dni od dnia jego doręczenia – przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do **Sądu Okręgowego w Warszawie.**

Przewodniczący:……

……

……

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

{KIO 265/19, KIO 266/19}
Zamawiający Kasa Rolniczego Ubezpieczenia Społecznego z siedzibą w Warszawie {dalej również: „KRUS"} prowadzi na podstawie ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2018 r. poz. 1986 ze zm.) {dalej również: „ustawa pzp" lub „pzp") w trybie przetargu nieograniczonego postępowanie o udzielenie zamówienia publicznego na dostawy pn. *Zakup licencji – rozbudowa oprogramowania systemu ochrony stacji końcowych użytkowników i serwerów* (nr postępowania 0000-ZP.261.15.2018).
Ogłoszenie o tym zamówieniu 22 września 2019 r. zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej nr 2018/S_183 pod poz. 413530.
Wartość przedmiotowego zamówienia przekracza kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy pzp.
4 lutego 2019 r. Zamawiający zawiadomił drogą elektroniczną o odrzuceniu ofert złożonych przez: po pierwsze – „Comtegrę" S.A. z siedzibą w Warszawie {dalej w uzasadnieniu również: „Comtegra"}, po drugie – Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie {dalej w uzasadnieniu również: „Intertrading" lub „IST"}.

{KIO 265/19}
14 lutego 2019 r. Odwołujący Comtegra S.A. z siedzibą w Warszawie wniósł w formie pisemnej do Prezesa Krajowej Izby Odwoławczej odwołanie (zachowując wymóg przekazania jego kopii Zamawiającemu) od odrzucenia jego oferty przez Zamawiającego.

Odwołujący zarzucił Zamawiającemu naruszenie art. 7 ust. 1 w zw. z art 89 ust. 1 pkt 2 w zw. z art 87 ust. 1 ustawy pzp, polegające na bezpodstawnym odrzuceniu zgodnej z treścią specyfikacji istotnych warunków zamówienia {dalej w uzasadnieniu również: „specyfikacja", „SIWZ" lub „s.i.w.z."} oferty Comtegry, ewentualnie na zaniechaniu wezwania Wykonawcy do wyjaśnienia treści złożonej oferty w sytuacji, gdy Zamawiający miał wątpliwości co do spełniania przez zaoferowany produkt wszystkich jego wymogów.

Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu:
1.Unieważnienia odrzucenia oferty Comtegry.
2.Ponownego dokonania oceny ofert z uwzględnieniem oferty Comtegry.

Z odwołania wynikają następujące okoliczności dotyczące przebiegu postępowania.

Zamawiający poinformował, że w jego ocenie zaoferowane oprogramowanie Symantec Endpoint Protection with Endpoint Detection and Response nie spełnia wymagań Szczegółowego opisu przedmiotu zamówienia {dalej w uzasadnieniu również: „OPZ"} z pkt:
1.1.2. – współegzystowania z istniejącymi w organizacji rozwiązaniami zabezpieczeń stacji końcowych (np. AntyVirus, HIPS itp.) w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwymi kodami wykonywalnymi;
1.2.2. – posiadania 3-warstwowej architektury składającej się z konsoli, serwera zarządzania oraz serwera bazy danych oraz umożliwienia instalacji i uruchomienia wszystkich trzech komponentów na jednym serwerze sprzętowym lub instalacji rozproszonej;
1.3.2. – możliwości monitorowania i zapobiegania atakom poprzez blokowanie szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/lub usługi chmurowej i nie bazując na metodzie sygnaturowej;
1.3.6. – niestosowania technik analizy exploitów wykorzystujących zasoby sprzętowe, takich jak lokalne środowisko symulacyjne typu „sandbox" lub zwirtualizowany kontener.

Odwołujący nie zgodził się z powyższą oceną Zamawiającego, w następujący sposób odnosząc się do uzasadnienia podanego przez Zamawiającego:
Ad 1.1.2.

Wskazany przez Zamawiającego dokument.TECH104806.html odnosi się do jednej funkcjonalności tj. do skanowania plików pod względem malware. Tymczasem zaoferowane rozwiązanie bazuje na innych komponentach i nie będzie wykonywać opisanych we wskazanym dokumencie funkcji skanowania plików.

Ponadto powołany przez Zamawiającego dokument odnosi się do rozwiązania Symantec Endpoint Protection, nie zaś do zaoferowanego rozwiązania Symantec Endpoint Protection with Endpoint Detection and Response.
Ad 1.2.2.

Zaoferowane rozwiązanie składa się z 3-warstwowej architektury i zawiera konsolę zarządczą, serwer zarządczy i bazę danych (opartą o Elasticsearch) oraz zgodnie z SIWZ wykorzystuje architekturę rozproszoną.

Powołany przez Zamawiającego dokument nie odnosi się do zaoferowanego rozwiązania Symantec Endpoint Protection with Endpoint Detection and Response.
Ad. 1.3.2.

Rozwiązanie Symantec Endpoint Protection with Endpoint Detection and Response posiada zaimplementowaną definicję technik ataków exploitacyjnych w formie zewnętrznych plików, które nie są statycznie zakodowane w kliencie. Pozwala to na zmniejszenie pliku instalacyjnego agenta oraz elastyczność – w przypadku powstania nowej metody ataku nie trzeba wymieniać agenta na stacji tylko wydawany jest nowy opis ataku. Definicja ataku jest scenariuszem operacji, jakie należy wykonać w pamięci operacyjnej komputera, aby wyeksploitować aplikację. Symantec pliki definicji ataków nazwał na własne potrzeby „sygnaturami", co nie jest tożsame z sygnaturami malware, które są zbiorem informacji o każdej wersji malware. Sygnatury malware publikowane są kilkukrotnie w ciągu dnia, pliki definicji ataków eksploitacyjnych pobierane są przez klienta tylko raz po instalacji. Nie jest to więc rozwiązanie wymagające ściąganych na bieżąco list złośliwego oprogramowania w formie sygnatur.

Powołany przez Zamawiającego dokument nie odnosi się do zaoferowanego rozwiązania Symantec Endpoint Protection with Endpoint Detection and Response.
Ad 1.3.6.

Zaoferowane rozwiązanie nie wykorzystuje dedykowanego rozwiązania sandbox. Symantec opracował wydajny emulator, który został zaimplementowany w agencie, wykorzystywany tylko dla niestandardowo skompresowanych programów destrukcyjnych. Emulator wydaje werdykt o poprawności pliku w czasie od 3,5 do 300 milisekund. Dostępne na rynku rozwiązania typu sandbox wymagają dedykowanego serwera i potrzebują od 5 do 30 min na wydanie werdyktu. Zamawiający nieopatrzenie zinterpretował opis emulatora w dokumentacji jako rozwiązanie sandbox. Ponownie należy wskazać, że

Powołany przez Zamawiającego dokument nie odnosi się do zaoferowanego rozwiązania Symantec Endpoint Protection with Endpoint Detection and Response.

Odwołujący zarzucił również Zamawiającemu, że w informacji o odrzuceniu oferty nie podał, dlaczego przyjął, że ogólne informacje znajdujące się na stronie producenta mają zastosowanie do tego konkretnego przedmiotu oferty, w sytuacji gdy powołane przez Zamawiającego artykuły zawierają jedynie ogólne tezy i nie precyzują specyfikacji technicznej rozwiązań.

Odwołujący podkreślił, że Zamawiający nie skierował do niego jakiegokolwiek wezwania do wyjaśnienia treści złożonej oferty, aby wyjaśnić posiadane przez niego wątpliwości.

W ocenie Odwołującego Zamawiający zaniechał również skierowania zapytania o zgodność oferowanego rozwiązania bezpośrednio do producenta, tj. firmy Symantec.
{KIO 266/19}
14 lutego 2019 r. Odwołujący Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie wniósł w stosownej formie elektronicznej do Prezesa Krajowej Izby Odwoławczej odwołanie (zachowując wymóg przekazania jego kopii Zamawiającemu) od od odrzucenia jego oferty przez Zamawiającego.
Odwołujący zarzucił Zamawiającemu następujące naruszenia przepisów ustawy pzp {lista zarzutów}:
1.Art. 89 ust. 1 pkt 2 – przez błędną ocenę oferty IST i uznanie, że jej przedmiot jest sprzeczny jest z treścią (wymaganiami) SIWZ w zakresie pkt 1.1.2., 1.2.2., 1.3.2. i 1.3.6. OPZ.
2.Art. 87 ust. 1 – przez zaniechanie zwrócenia się do Intertradingu o wyjaśnienia w zakresie sposobu spełnienia przez oprogramowanie Symantec wymogów określonych w pkt 1.1.2., 1.2.2., 1.3.2. i 1.3.6. OPZ.

Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu {lista żądań}:
1.Unieważnienia oceny ofert i dokonania ponownej oceny ofert.

2.Uznania oferty IST za najkorzystniejszą.
3.Względnie wcześniejsze zwrócenie się do IST o wyjaśnienia w zakresie sposobu spełnienia przez oprogramowanie Symantec wymogów określonych w pkt 1.1.2., 1.2.2., 1.3.2. i 1.3.6. OPZ

W uzasadnieniu odwołania Odwołujący zacytował brzmienie wymagań z poszczególnych pkt OPZ, uzasadnienie odrzucenia podane przez Zamawiającego oraz w następujący sposób je zakwestionował.

Ad 1.1.2.

Zgodnie z treścią pkt 1.1.2. OPZ*proponowane rozwiązanie musi współegzystować z istniejącymi w organizacji rozwiązaniami zabezpieczeń stacji końcowych (np. Antywirus, HIPS, itp.) w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwymi kodami wykonywalnymi.*

Według Zamawiającego oferowane oprogramowanie Symantec jest sprzeczne z powyższym postanowieniem (wymogiem), gdyż zgodnie z dokumentem technicznym znajdującym się na stronie firmy Symantec instalowanie oferowanego rozwiązania z innym oprogramowaniem antywirusowym jest nie wspierane. KRUS powołuje się przy tym na informacje pozyskane ze strony https://support.symantec.com/en_US/article.TECH 104806.html.

Przede wszystkim Zamawiający podaje informację, której nie ma na przywoływanej stronie www, gdzie nie zaleca się, aby dwa konkurencyjne rozwiązania jednocześnie były uruchamiane, a nie, że nie mogą być zainstalowane (*you should only run one anitivirus program at a tim*e; tłum.: *należy uruchamiać tylko jeden program anitiyirus na raz*).

Zatem nie ma przeciwskazań ze strony producenta co do instalacji oprogramowania Symantec wtedy, gdy zainstalowane jest także inne oprogramowanie. W konsekwencji oferowane oprogramowanie może współegzystować (współistnieć, współwystępować) z innymi rozwiązaniami zabezpieczeń.

KRUS nie stawiał żadnych wymogów odnośnie konieczności jednoczesnego działania tego rodzaju programów. Jest to o tyle istotne, że zasadą jest niedziałanie jednoczesne tego rodzaju programów, gdyż z jednej strony może to prowadzić do konfliktów tych dwóch programów, ponadto negatywnie wpływa na pracę sprzętu (kolokwialnie rzecz ujmując „zamula"). Gdyby Zamawiający chciał postawić wymóg jednoczesnego działania tych programów, powinien był to wprost zapisać, bo współegzystowanie na to nie wskazuje.

Zamawiający odniósł się w wymogu do współegzystowania z rozwiązaniami zabezpieczeń istniejącymi w organizacji, nie wskazując na konkretny poziom owej organizacji, w szczególności, czy dotyczy to organizacji jako takiej (czyli KRUS) czy też skonkretyzowanych stacji końcowych.

Skoro Zamawiający nie wyraził precyzyjnie w SIWZ co rozumie przez pojęcie współegzystowania, nie może na tym etapie postępowania rozszerzać tego pojęcia i dowolnie go definiować w sposób niekorzystny dla wykonawcy. Byłoby to działanie sprzeczne z art. 7 pzp i jako takie niedozwolone.

Szeroki i ugruntowany już dorobek orzeczniczy Izby, jak i sądów okręgowych, jednoznacznie wskazuje na to, że ewentualne nieprecyzyjności SIWZ obciążają zamawiającego jako jego twórcę, a nie wykonawców. Stąd tego rodzaju postanowienia należy interpretować w sposób korzystny dla wykonawców, a nie restrykcyjny.

Ad 1.2.2.

Zgodnie z treścią pkt 1.2.2. OPZ *Proponowane rozwiązanie musi posiadać 3warstwową architekturę składającą się z konsoli, serwera zarządzania oraz serwera bazy danych. Rozwiązanie musi umożliwiać instalację i uruchomienie wszystkich trzech komponentów na jednym serwerze sprzętowym lub instalację rozproszoną.*

Według Zamawiającego oferowane oprogramowanie Symantec jest sprzeczne z powyższym postanowieniem (wymogiem), gdyż składa się z dwóch, a nie jednego serwerów zarządzających i dwóch, a nie jednej konsoli.

Czynność Zamawiającego jest niezgodna z prawem, gdyż odnosi się do takiego wymogu, który nie został w ogóle postawiony. Wymóg z pkt 1.2.2. OPZ dotyczy trzech kwestii: po pierwsze – posiadania trójwarstwowej architektury (konsola-serwer zarządzania- serwer bazy danych), po drugie – umożliwienia instalacji i uruchomienie wszystkich komponentów na jednym serwerze sprzętowym lub, po trzecie – instalacji rozproszonej.

Wszystkie te trzy wymogi są spełnione, czego chyba zresztą nie kwestionuje nawet Zamawiający.

Natomiast Zamawiający twierdzi, że nie dopuszczał tego, aby rozwiązanie spełniane było przez dwie konsole lub dwa serwery zarządzania (*nota bene* wszystkie mogą być zainstalowane na jednym serwerze sprzętowym lub instalowane w sposób rozproszony). Tyle, że takiego zakazu nie było w żadnym postanowieniu SIWZ (nie tylko w pkt 1.2.2.).

W konsekwencji po raz kolejny KRUS wywodzi z treści SIWZ taki warunek (ograniczenie), którego nie było. Jest to niedopuszczalna na tym etapie postępowania nadinterpretacja SIWZ, a wręcz kreowanie nowych wymagań.

Ad 1.3.2.

Zgodnie z treścią pkt 1.3.2. OPZ:*Proponowane rozwiązanie musi zapewniać możliwości monitorowania i zapobiegania atakom poprzez blokowanie szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/iub usługi chmurowej i nie bazując na metodzie sygnaturowej.*

Według Zamawiającego oferowane oprogramowanie Symantec jest sprzeczne z powyższym postanowieniem (wymogiem), gdyż zgodnie z dokumentacją techniczną firmy Symantec funkcjonalność Memory Exploit Migration bazuje na sygnaturach, natomiast Zamawiający zastrzegł w SIWZ, iż ww. funkcjonalność ma nie bazować na metodzie sygnaturowej.

Oferowane oprogramowanie Symantec stanowi pewnego rodzaju całość i stąd nie można zaoferować go „częściowo" tj. np. bez określonych funkcjonalności, możliwe jest natomiast takie skonfigurowanie, aby dane funkcjonalności nie były wykorzystywane (co *de facto* jest równoznaczne z ich brakiem).

Oprogramowanie Symantec wykorzystuje więcej niż jedną metodę, w tym m.in. silnik Advanced Machine Learning, który nie bazuje na metodzie sygnaturowej, oraz firewall systemowy.

Wprawdzie oferowane oprogramowanie wykorzystuje też w pewnych zakresach metodę sygnaturową, jednakże tylko jako uzupełnienie innych metod (w żaden sposób nie kwestionowanych przez KRUS). Co istotne, bez żadnego uszczerbku dla skuteczności i poprawności działania przedmiotu oferty możliwe jest takie jego skonfigurowanie (ustawienie), aby metoda sygnaturowa nie była wykorzystywana przez oprogramowanie Symantec.

Ad 1.3.6.

Zgodnie z treścią pkt 1.3.6. OPZ:*Proponowane rozwiązanie nie może stosować technik analizy exploitów wykorzystanych zasoby sprzętowe, takich jak lokalne środowisko symulacyjne typu „sandbox" lub zwirtuaiizowany kontener.*

Według Zamawiającego oferowane oprogramowanie Symantec jest sprzeczne z powyższym postanowieniem (wymogiem), gdyż zgodnie z dokumentacją producenta produktu Symantec Endpoint Protection 14.2 używany jest wirtualny sandbox.

Tymczasem oferowane rozwiązanie Symantec nie wykorzystuje środowiska symulacyjnego w celu analizy technik exploitów – mechanizm Emulator w Symantec Endpoint Protection stanowi narzędzie wykrywające zawartość spakowanych i zaszyfrowanych plików. Natomiast mechanizmem właściwym dla wykrywania technik exploitów jest

Memory Exploit Mitigation, który nie wykorzystuje emulacji, sandboxingu i innych form środowisk symulacyjnych.
{KIO 265/19, KIO 266/19}

Do Prezesa Izby wpłynęły zgłoszenia przystąpień do postępowania odwoławczego w rozpatrywanych sprawach ze strony następujących wykonawców:
- Intertrading Systems Technology sp. z o.o. z siedzibą w Warszawie – po stronie Odwołującego Comtegra w sprawie o sygn. akt KIO 265/19;
- 4PRIME sp. z o.o. z siedzibą w Warszawie – po stronie zamawiającego w sprawach o sygn. akt KIO 265/19 i KIO 266/19.

Wobec dokonania powyższych zgłoszeń w odpowiedniej formie, z zachowaniem 3dniowego terminu od otrzymania kopii odwołania oraz wymogu przekazania kopii zgłoszenia Stronom tego postępowania – a więc zgodnie z art. 185 ust. 2 pzp – Izba nie miała podstaw do stwierdzenia nieskuteczności przystąpień, co do których nie zgłoszono również opozycji.

Ponieważ żadne z odwołań nie zawierało braków formalnych, a wpisy od nich zostały uiszczone – podlegały rozpoznaniu przez Izbę.

W toku czynności formalnoprawnych i sprawdzających Izba nie stwierdziła, aby którekolwiek z odwołań podlegało odrzuceniu na podstawie przesłanek określonych w art. 189 ust. 2 pzp. Na posiedzeniu z udziałem Stron i Przystępujących nie zostały również złożone w tym zakresie odmienne wnioski.

Z uwagi na brak podstaw do odrzucenia odwołania lub umorzenia postępowania odwoławczego obie sprawy zostały skierowane do rozpoznania na rozprawie, podczas której Odwołujący podtrzymali dotychczasowe stanowiska, a Zamawiający i Przystępujący po jego stronie wnieśli o oddalenie odwołań w całości.

Po przeprowadzeniu rozprawy z udziałem Stron i Przystępujących obu spraw, uwzględniając zgromadzony materiał dowodowy, jak również biorąc pod uwagę oświadczenia i stanowiska zawarte w odwołaniach, pisma Zamawiającego złożonego na rozprawie, zgłoszeniach przystąpień, a także wyrażone ustnie na rozprawie i odnotowane w protokole, Izba ustaliła i zważyła, co następuje:

Zgodnie z art. 179 ust. 1 pzp odwołującemu przysługuje legitymacja do wniesienia odwołania, gdy ma (lub miał) interes w uzyskaniu zamówienia oraz może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy.

W ocenie Izby Odwołujący legitymują się interesem w uzyskaniu przedmiotowego zamówienia, skoro złożyli oferty w postępowaniu o jego udzielenie. Jednocześnie ponieważ objęte zarzutami odwołania naruszenia przez Zamawiającego przepisów ustawy pzp dotyczą odrzucenia złożonych przez Odwołujących ofert, naraża ich to na szkodę, gdyż w przeciwnym razie mogliby liczyć na uzyskanie przedmiotowego zamówienia.

W szczególności Izba nie podzieliła stanowiska Zamawiającego, że Odwołujący Comtegra, którego oferta według kryteriów oceny ofert musiałaby zostać niżej oceniona niż oferta Odwołującego IST, nie spełnia przesłanek z art. 179 ust. 1 pzp, gdyż nie można powiedzieć, że na skutek czynności Zamawiającego może ponieść szkodę polegającą na nieuzyskaniu przedmiotowego zamówienia.

Umknęło uwadze Zamawiającego, że prowadzi postępowanie w tzw. procedurze odwróconej i na razie zdecydował się jedynie na odrzucenie dwóch ofert. Na tym etapie postępowania nie sposób odmawiać Odwołującemu Comtegrze legitymacji w rozumieniu art. 179 ust. 1 pzp. Gdyby Odwołujący nie zakwestionował odrzucenia swojej oferty, *de facto* zrezygnowałby z dalszego ubiegania się o przedmiotowe zamówienie i utraciłby możliwość weryfikacji kolejnych czynności podejmowanych przez Zamawiającego w celu wyłonienia oferty najkorzystniejszej.

Izba ustaliła, że Zamawiający przed odrzuceniem ofert we własnym zakresie pozyskał ze strony internetowej www.symantec.com dokumentację techniczną, którą uznał za adekwatny punkt odniesienia dla ustalenia, czy zaoferowane przez Odwołujących oprogramowanie odpowiada jego wymogom. Ostatecznie Zamawiający uznał, że zaoferowane w obu tych ofertach oprogramowanie firmy Symantec nie odpowiada 4 wymaganiom OPZ, pomimo że Wykonawcy w ofertach potwierdzili ich spełnianie. Oznacza to, że na podstawie treści złożonych ofert Zamawiający nie był w stanie stwierdzić tych niezgodności.

Zdaniem Izby taki sposób oceny, z pominięciem uprzedniego wezwania Wykonawców w trybie art. 87 ust. 1 pzp do wyjaśnienia wątpliwości odnośnie tych 4 (wymienionych powyżej w sentencji) pkt OPZ, był niewłaściwy.

Przede wszystkim do zamknięcia rozprawy Zamawiający nie wykazał, że prawidłowo ustalił treść specyfikacji technicznej oferowanego oprogramowania Symantec. Zamawiający w uzasadnieniu odrzucenia poprzestał na podaniu krótkich cytatów i linków do ich źródła. Skoro na rozprawie żadna ze stron, w szczególności Zamawiający, nie wnioskowała o dopuszczenie dowodu z opinii biegłego, złożony przez Zamawiającego na rozprawie jako dowód dokument pn. „Ekspertyza mająca na celu ocenę przesłanek odrzucenia…" mógł być poczytany co najwyżej za swoistą odpowiedź na odwołanie, gdyż Izba z urzędu nie stwierdziła, aby dla ustalenia istotnych dla rozstrzygnięcia sprawy okoliczności konieczne były wiadomości specjalne. Zresztą w treści tego pisma powtórzono treść cytatów zawartych w uzasadnieniu odrzucenia i dodano nowe oraz ponownie wskazano linki do stron internetowych, bez załączenia dokumentacji źródłowej. Oznacza to, że Zamawiający niczego nie udowodnił, gdyż do zamknięcia rozprawy nie przedstawił dokumentacji, na której podstawie odrzucił oferty Odwołujących.

W pozostałym zakresie „Ekspertyza" znacząco wykracza poza treść lakonicznego uzasadnienia przekazanego wykonawcom i stanowi spóźnioną próbę jego uzupełnienia. Enigmatyczne wytłumaczenie, dlaczego oprogramowanie zaoferowane przez Odwołujących nie spełnia wymagań OPZ, jest zresztą zupełnie nieprzekonujące i świadczy o tym, że Zamawiający w istocie nie jest pewny, co dokładnie objęte jest ofertą obu Wykonawców. Okazuje się wręcz, że w zakresie pkt 1.3.2. Zamawiający nie jest już pewny, czy prawidłowo odrzucił oferty.

Taki stan rzeczy potwierdza również okoliczność, że pomimo uzyskania, w trybie nieprzewidzianym w ustawie pzp ani SIWZ (Zamawiający nie żądał próbki oferowanego oprogramowania ani nie przewidział jego prezentacji na potrzeby badania i oceny ofert), plików instalacyjnych i przetestowania oprogramowania we własnym zakresie, nie wiadomo, jaki był wynik tego badania, gdyż uzasadnienie odrzucenia nie wspomina o tym.

Tymczasem Izba ustaliła, że Zamawiający nie wymagał złożenia w ofercie specyfikacji technicznej oferowanego oprogramowania, przewidując (w pkt 5.10 s.i.w.z.) jej złożenie dopiero na etapie po ustaleniu oferty najwyżej ocenionej według kryteriów oceny ofert (postępowanie prowadzone jest w tzw. procedurze odwróconej).

Skoro Zamawiający przewidział złożenie przez wykonawcę specyfikacji technicznej oferowanego przez niego oprogramowania, a jednocześnie bez sięgnięcia do jej treści Zamawiający nie jest w stanie jednoznacznie stwierdzić, czy jest ono zgodne z opisem przedmiotu zamówienia, nie może ustalać treści tej specyfikacji technicznej we własnym zakresie. Należy podkreślić, że to Zamawiający ustalił zakres treści składanej oferty i przesunął na późniejszy etap złożenie specyfikacji technicznej oferowanego oprogramowania.

Z drugiej strony postępowanie zgodnie z procedurą oceny i badania ofert przewidzianą w SIWZ w żaden sposób nie ogranicza możliwości odrzucenia przez Zamawiającego oferty, jeżeli po zapoznaniu się ze specyfikacją techniczną złożoną przez wykonawcę okaże się, że zaoferowane przez niego oprogramowanie nie odpowiada opisowi przedmiotu zamówienia. Co najwyżej wydłuży, zamiast skrócić, wyłanianie najkorzystniejszej oferty, gdyż Zamawiający może weryfikować pod tym względem wykonawców po kolei, a nie jednocześnie.

Zamawiający powinien również, jeżeli po złożeniu specyfikacji technicznej oferowanego oprogramowania, będzie miał dalej wątpliwości co do jego zgodności z opisem przedmiotu zamówienia, skorzystać z uprawnienia do żądania od wykonawcy wyjaśnień treści oferty.

Powyższe rozstrzygnięcie byłoby wystarczające, gdyby Izba nie stwierdziła, że w zakresie dwóch wymagań odrzucenie opiera się na ich interpretacji przez Zamawiającego, która nie znajduje oparcia w ich treści, tzn. nastąpiło w tym przypadku wyciągnięcie niekorzystnych dla Odwołujących skutków z niejednoznacznych postanowień OPZ, co według utrwalonego w orzecznictwie Izby i sądów okręgowych stanowiska jest niedopuszczalne.

W pkt 1.1.2. wprowadzono wymóg z użyciem terminu „współegzystowania", który nie ma ustalonego znaczenia w informatyce, bez jego dookreślenia, do czego obligował Zamawiającego art. 29 ust. 1 pzp. Treść SIWZ nie potwierdza stanowiska Zamawiającego z rozprawy, jakoby jego intencją nie był zakup standardowego produktu, lecz aby zakupione oprogramowanie stanowiło uzupełnienie ochrony zapewnianej przez oprogramowanie już posiadane. Intencja ta została wyrażona co prawda w nazwie postępowania, ale powinna znaleźć odzwierciedlenie w treści opisu przedmiotu zamówienia przez wskazanie konkretnych produktów, które Zamawiający aktualnie użytkuje, co nie nastąpiło, gdyż Zamawiający poprzestał na przykładowym wyliczeniu dwóch rodzajów zabezpieczeń, w ogóle nie precyzując nazw własnych użytkowanego oprogramowania. Brak również jakiejkolwiek konkretyzacji, co należy rozumieć przez „współegzystowanie" w ramach funkcjonalnego opisu przedmiotu zamówienia, na który zdecydował się Zamawiający. Biorąc pod uwagę, że okolicznością notoryjną dla każdego świadomego użytkownika komputera osobistego jest okoliczność, że nie jest zalecane jednoczesne użytkowanie dwóch programów antywirusowych, przeciwne wymaganie Zamawiającego musiało być szczegółowo opisane, aby mogło być egzekwowalne. Tymczasem strona przeciwna dowiodła, że również w przypadku produktu zaoferowanego przez Przystępującego po stronie Zamawiającego koegzystencja rozumiana w sposób, który Zamawiający przedstawił na rozprawie, również nie jest bezwarunkowa i gwarantowana w stosunku do każdego oprogramowania.

Z kolei w pkt 1.2.2. wprowadzono co prawda zrozumiały wymóg 3-warstwowej architektury, jednak dalsze sformułowanie, że ma się ona składać z konsoli, serwera zarządzania oraz serwera bazy danych, z punktu widzenia reguł fleksji i składni języka polskiego może również oznaczać wskazanie rodzajów elementów, a nie tylko, że ma być po jednym elemencie z każdego rodzaju. Okoliczność, że konsola czy serwer się dublują nie powoduje przecież, że architektura przestaje być 3-warstwowa (niesporne było, że oprogramowanie oferowane przez Odwołujących posiada taką architekturę). Jeśli Zamawiający nie życzył sobie z jakiś powodów dublowania tych elementów, powinien był dać temu wprost wyraz w treści SIWZ, czego nie uczynił.

Jeżeli dla Zamawiającego jednoczesne niezakłócone działanie oferowanego oprogramowania antywirusowego z dotychczas użytkowanym oraz sposób realizacji architektury trójwarstwowej miały istotne znaczenie, nie powinien poprzestać na hasłowym i enigmatycznym sformułowaniu powyżej wskazanych punktów OPZ, ale zgodnie z art. 29 ust. 1 pzp jednoznacznie i wyczerpująco, za pomocą dostatecznie dokładnych i zrozumiałych określeń, opisać swoje wymagania w tym zakresie.

Mając powyższe na uwadze, Izba stwierdziła, że naruszenie przez Zamawiającego art. 89 ust. 1 pkt 2 w zw. z art. 87 ust. 1 ustawy Prawo zamówień publicznych miało wpływ na wynik prowadzonego przez niego postępowania o udzielenie zamówienia, wobec czego – działając na podstawie art. 192 ust. 1, 2 i 3 pkt 1 tej ustawy – orzekła, jak w pkt 1 i 2 sentencji.

O kosztach postępowania odwoławczego orzeczono stosownie do jego wyniku na podstawie art. 192 ust. 9 i 10 w związku z § 3 pkt 1 i 2 lit. b oraz § 5 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 15 marca 2010 r. w sprawie wysokości i sposobu pobierania wpisu od odwołania oraz rodzajów kosztów w postępowaniu odwoławczym i sposobu ich rozliczania (t.j. Dz. U. z 2018 r. poz. 972). W pierwszej kolejności zaliczono do tych kosztów uiszczone przez Odwołujących wpisy – zgodnie z § 3 pkt 1 rozporządzenia. Po drugie, obciążono Zamawiającego tymi kosztami, na które złożyły się wpis oraz uzasadnione koszty w postaci wynagrodzeni pełnomocnika, na podstawie rachunku złożonego do zamknięcia rozprawy, zgodnie z § 5 ust. 2 rozporządzenia – zasądzając na rzecz każdego z Odwołujących te koszty od Zamawiającego.

Przewodniczący:……

……

……