Sygn. akt: KIO 492/13

WYROK
z dnia 15 marca 2013 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Izabela Kuciak

Protokolant: Łukasz Listkiewicz

po rozpoznaniu na rozprawie w dniu 15 marca 2013 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 4 marca 2013 r. przez wykonawcę **Enigma Systemy Ochrony Informacji Sp. z o.o., 02-230 Warszawa, ul. Jutrzenki 116** w postępowaniu prowadzonym przez **Komendę Główną Straży Granicznej, 00-463 Warszawa, ul. Podchorążych 38**

orzeka:

1. Oddala odwołanie.

2. Kosztami postępowania obciąża wykonawcę **Enigma Systemy Ochrony Informacji Sp. z o.o., 02-230 Warszawa, ul. Jutrzenki 116** i:
   2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawcę **Enigma Systemy Ochrony Informacji Sp. z o.o., 02-230 Warszawa, ul. Jutrzenki 116** tytułem wpisu od odwołania,
   2.2. zasądza od wykonawcy **Enigma Systemy Ochrony Informacji Sp. z o.o., 02-230 Warszawa, ul. Jutrzenki 116** na rzecz **Komendy Głównej Straży Granicznej, 00-463 Warszawa, ul. Podchorążych 38** kwotę **3 600 zł 00 gr** (słownie: trzy tysiące sześćset złotych zero groszy) stanowiącą koszty postępowania odwoławczego poniesione z tytułu wynagrodzenia pełnomocnika.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2010 r. 113, poz. 759 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: ……

Sygn. akt: KIO 492/13

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

Zamawiający prowadzi, w trybie przetargu nieograniczonego, postępowanie o udzielenie zamówienia publicznego, którego przedmiotem jest „*Rozbudowa systemu CBD EWIDA - Etap II - zakup platformy sprzętowo-programowej, podprojekt: Modernizacja niejawnej sieci teleinformatycznej - zakup szyfratorów IP*." Ogłoszenie o zamówieniu zostało opublikowane w dniu 21 lutego 2013 r. w Dzienniku Urzędowym Unii Europejskiej pod numerem 2013/S 037-058589.

Odwołujący wniósł odwołanie wobec treści ogłoszenia o zamówieniu oraz postanowień SIWZ, zarzucając Zamawiającemu naruszenie m.in. art. 29 ust. 1, 2 i 3 i art. 30 ustawy Pzp przez sporządzenie opisu przedmiotu zamówienia w sposób utrudniający uczciwą konkurencję i równe traktowanie wykonawców oraz zaniechanie dopuszczenia rozwiązań równoważnych oraz naruszenie art. 7 ust. 1 i 3 ustawy Pzp przez prowadzenie postępowania w sposób naruszający zasadę zachowania uczciwej konkurencji i równego traktowania wykonawców. Odwołujący wniósł o uwzględnienie odwołania i nakazanie Zamawiającemu dokonania zmiany postanowień ogłoszenia oraz SIWZ w zakresie i w sposób wskazany w uzasadnieniu odwołania, ewentualnie o unieważnienie postępowania ze względu na to, iż postępowanie obarczone jest niemożliwą do usunięcia wadą, uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego, na podstawie art. 93 ust. 1 pkt 7 w zw. z art. 146 ust. 6 ustawy Pzp.

W uzasadnieniu swojego stanowiska Odwołujący podniósł, że przy utrzymaniu obecnej treści SIWZ jedynym urządzeniem spełniającym jej wymagania jest urządzenie - IP KRYPTON K2, oferowane jedynie przez KRYPTON Polska sp. z o.o. z siedzibą w Warszawie.

Odwołujący zwrócił uwagę, iż przepis art. 29 ust. 2 ustawy Pzp zakazuje stosowania opisu przedmiotu zamówienia w sposób utrudniający dostęp do zamówienia wykonawcy, który potencjalnie jest w stanie wykonać to zamówienie. Formułując wymogi w zakresie opisu przedmiotu zamówienia zamawiający winien kierować się celem, jakiemu zamawiane produkty mają służyć. Ponadto, każde wymaganie ma znajdować uzasadnienie w obiektywnych potrzebach zamawiającego.

Odwołujący szeroko powołał się również na orzecznictwo w tym przedmiocie. I tak, Odwołujący zwrócił uwagę, że Zespół Arbitrów w orzeczeniu z dnia 24 sierpnia 2007 r. (sygn. akt UZP/ZO/0-1040/07 oraz UZP/ZO/0-1045/07) stwierdził, iż *„wymagania muszą mieć walor*

istotnych, znaczących dla przedmiotu, nie mogą mieć charakteru subiektywnych, albo więcej - zmierzających do wyeliminowania niektórych podmiotów, bądź wyrażać preferencji dla konkretnego przedmiotu". Zaś w wyroku Krajowej Izby Odwoławczej z dnia 1 lutego 2011 r., sygn. akt KIO 79/11, KIO 89/11, KIO 90/11 wskazano, że „*Wystarczającym dla stwierdzenia naruszenia zasady wyrażonej w art. 29 ust. 2 Pzp jest takie zestawienie przez zamawiającego charakterystycznych lub granicznych parametrów nabywanych produktów, że wskazuje ono na konkretny produkt, eliminując jednocześnie możliwość zaoferowania produktów innych producentów. Zgodnie z poglądem wyrażonym przez Izbę w wyroku o sygn. akt KIO 361/10 "należy (...) odmówić zamawiającym prawa do zupełnie dowolnego kształtowania postanowień siwz, które mogą prowadzić do nadmiernego ograniczenia konkurencji i preferencji dla określonych wykonawców w stopniu ponad potrzeby zamawiającego wykraczającym*." Dalej w wyroku Krajowej Izby Odwoławczej z dnia 22 lipca 2009 r., sygn. akt: KIO/UZP 874/09 podkreślono, iż „*swoboda zamawiającego w kształtowaniu opisu przedmiotu zamówienia nie jest nieograniczona - nie może prowadzić do nieuzasadnionego ograniczenia kręgu potencjalnych wykonawców. (…) W sytuacji, gdy określone przez zamawiającego wymagania mogą ograniczyć krąg potencjalnych wykonawców, zamawiający zobowiązany jest wykazać, że są one niezbędne w świetle celu założonego w danym postępowaniu*."

Odwołujący podniósł, iż w zakresie przedmiotu zamówienia ustawą szczególną *(lex specialis)* w stosunku do Prawa zamówień publicznych jest ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne tekst jednolity z dnia 7 grudnia 2012 r. (Dz. U. z 2013 r. poz. 235). Jak wskazuje Odwołujący, ustawa ta skutecznie uzupełnia regulację ustawy Pzp i określa zasady m.in. *(...) wymiany informacji w postaci elektronicznej **z** podmiotami publicznymi oraz ustalania Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji,* a także ustala zasady *dostosowania systemów teleinformatycznych używanych do realizacji zadań publicznych do minimalnych wymagań dla systemów teleinformotycznych używanych do realizacji zadań publicznych oraz do Krajowych Ram Interoperacyjności systemów teleinformatycznych w sposób gwarantujący neutralność technologiczną i jawność używanych standardów i specyfikacji.*

Cytowana ustawa nakłada na zamawiającego obowiązek zagwarantowania neutralności technologicznej, jest to zasada równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań. Ustawa ta wzmacnia nieprzekraczalne dla Zamawiającego granice wyznaczone przez art. 7 i 29 ustawy Pzp.

Jak podaje Odwołujący, zgodnie z pkt. 3.1.3 załącznika nr 1 do SIWZ *Opis przedmiotu zamówienia* (OPZ) szyfrator musi posiadać w momencie dostawy Certyfikat Ochrony Kryptograficznej wydany przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego, zapewniający ochronę informacji niejawnych o klauzuli poufne z terminem ważności minimum na 4 lata licząc od dnia dostawy urządzeń szyfrujących IP do Zamawiającego. Odwołujący nie kwestionuje prawa Zamawiającego do żądania ww. certyfikatu, ale zdaniem Odwołującego, wymóg co najmniej czteroletniego okresu ważności tego certyfikatu i to liczony od dnia dostawy urządzeń nie jest uzasadniony.

Odwołujący wyjaśnił, iż Zamawiający w 2012 r. prowadził postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na *„zakup szyfratorów IP"*. Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku urzędowym Unii Europejskiej dnia 1 września 2012 r., nr ogłoszenia S168-278649. W odwołaniu z dnia 13 września 2012 r. wykazano, iż na świecie dostępne jest wyłącznie jedno urządzenie kryptograficzne KRYPTON K2 w wersji 1.3.0, produkcji KRYPTON Polska sp. z o.o., które spełnia kwestionowany wymóg posiadania certyfikatu ochrony kryptograficznej. Powyższe zostało potwierdzone przez Izbę w uzasadnieniu wyroku z dnia 27 września 2012 r., sygn. akt KIO 1942/12, w którym wskazano *„odnośnie stanu faktycznego Izba uznaje, że odwołujący wykazał, iż na dzień rozpatrywania istnieje jedno urządzenie spełniające wymogi siwz postawione w zakresie okresu ważności certyfikatu."* Stan ten nie uległ zmianie na dzień wniesienia niniejszego odwołania.

Odwołujący stoi na stanowisku, iż Zamawiający ma świadomość, że proces certyfikacji jest bardzo czasochłonny i wymaga podjęcia szeregu czynności, a co za tym idzie, że żaden wykonawca pomimo dołożenia wszelkich starań nie miał możliwości uzyskania certyfikatu od momentu przeprowadzenia poprzedniego postępowania. Przebieg procesu certyfikacji został przedstawiony w skierowanym do Odwołującego piśmie ABW z dnia 23 października 2012 r.

Zdaniem Odwołującego, fakt, iż KIO w uzasadnieniu wyroku z dnia 27 września 2012 r. stwierdziła, że *„Zamawiający opisując przedmiot zamówienia miał prawo sformułować opis uwzględniając cel, jakim jest zminimalizowanie ryzyka użytkowania urządzenia kryptograficznego nie posiadającego ważnego certyfikatu",* nie przesądza, że wymóg ten nie może prowadzić do naruszenia podstawowej dla prawa zamówień publicznych zasady zachowania uczciwej konkurencji. W szczególności Zamawiający nie jest uprawniony do takiego określenia warunków postępowania, prowadzonego w trybie przetargu nieograniczonego, które są spełniane wyłącznie przez jednego wykonawcę, czy też jeden produkt. Jeśli nawet po stronie Zamawiającego istniałyby przesłanki uzasadniające takie opisanie przedmiotu zamówienia, to Zamawiający - mając świadomość, iż wyłącznie jeden

wykonawca spełnia warunki udziału, po prostu powinien zastosować zamówienie z wolnej ręki.

Odwołujący podnosi, że zarówno przepisy ustawy, jak i orzecznictwo jasno wskazują, iż niedopuszczalne ograniczenie konkurencji może wynikać nie tylko ze sposobu skonstruowania warunków udziału w postępowaniu, ale także z wymogów postawionych przy opisie przedmiotu zamówienia. Przy czym, niekoniecznie muszą to być naruszenia wyczerpujące przesłanki niezgodności z art. 29 ust. 3 ustawy Pzp, a więc polegające na posłużeniu się w specyfikacji bezpośrednim wskazaniem znaków towarowych, nazw producenta itp. Wystarczające jest sformułowanie i dobranie wymogów w taki sposób, który *de facto* umożliwia złożenie oferty tylko wąskiej grupie lub wręcz tylko jednemu wykonawcy. Tak, m.in. w wyroku KIO z dnia 6 maja 2010 r.; sygn. akt: KIO 634/10, wyroku Sądu Okręgowego we Wrocławiu z dnia 27 maja 2010 r., Sygn. akt X Ga 123/1, wyrok KIO z dnia 24 marca 2010 r., sygn. akt: KIO/UZP 178/10.

Zachowanie zasad uczciwej konkurencji przy opisie przedmiotu zamówienia podlega badaniu każdorazowo na potrzeby danego postępowania, zależy ono bowiem od aktualnych warunków rynkowych, których nie da się powtórzyć w innych okolicznościach, a które Zamawiający, odpowiedzialny za prawidłowy przebieg postępowania, ma obowiązek uwzględnić.

Odwołujący wyjaśnia, iż w przypadku cofnięcia/utraty certyfikatu ochrony kryptograficznej (i to niezależnie od przyczyny tego zdarzenia Zamawiający) i tak nie może korzystać z urządzenia. W konsekwencji wprowadzenie długiego okresu ważności certyfikatu aż do 4 lat nie prowadzi do zwiększenia bezpieczeństwa Zamawiającego (na taki cel Zamawiający wskazywał w poprzednim postępowaniu, uzasadniając wymóg posiadania certyfikatu ważnego przez okres 4 lat) - gdyż certyfikat taki może być cofnięty w każdej chwili przez właściwe służby. Zamawiający nie przewidział w umowie obowiązku natychmiastowego przedstawienia nowego certyfikatu (ważnego 4 lata lub dłużej) w przypadku ewentualnego cofnięcia/utarty certyfikatu, którym wykonawca posłużył się na etapie składania oferty. Odwołujący wyjaśnia, iż utrata certyfikatu następuje np. w przypadku utraty (zagubienie, kradzież) choć jednego urządzenia - w takim przypadku cały proces certyfikacji należy powtórzyć. Paradoksalnie, im dłuższy okres ważności certyfikatu, tym większe prawdopodobieństwo jego cofnięcia/utraty. Gdyby celem Zamawiającego faktycznie było zminimalizowanie ryzyka użytkowania urządzenia kryptograficznego nieposiadającego ważnego certyfikatu to jedynym rozwiązaniem gwarantującym Zamawiającemu bezpieczne użytkowanie szyfratorów jest wskazanie sposobu i terminu zmiany szyfratorów w przypadku ewentualnej utraty/cofnięcia certyfikatu, a takiego rozwiązania Zamawiający nie przewidział.

Przygotowując przedmiotowe postępowanie Zamawiający posiadał wiedzę, że istnieje tylko jedno urządzenie spełniające wymogi SIWZ postawione w zakresie okresu

ważności certyfikatu, a co za tym idzie, który z wykonawców uzyska zamówienie. Wiedzę tę Zamawiający powziął w toku prowadzonego uprzednio postępowania, co najmniej z korespondencji prowadzonej z Odwołującym. W korespondencji tej Odwołujący wielokrotnie informował Zamawiającego, że postawienie warunku 4-letniego okresu ważności certyfikatu od chwili dostawy szyfratorów do Zamawiającego jest równoznaczne ze wskazaniem konkretnego producenta, a mianowicie KRYPTON Polska sp. z o.o., tak m.in. w piśmie Odwołującego do Zamawiającego z dnia 5 listopada 2012 r. oraz piśmie z dnia 20 września 2012 r. Nadto, wynika to z faktu, iż listy urządzeń posiadających certyfikat są publikowane i powszechnie znane - tylko urządzenie KRYPTON K2 ma certyfikat o okresie ważności zgodny z wymaganiami wskazanymi w SIWZ.

Wobec powyższego, Odwołujący wniósł o zmianę treści ogłoszenia i SIWZ przez określenie, iż oferowany przez wykonawcę szyfrator IP będzie posiadał ważny certyfikat ochrony kryptograficznej, a wykonawca zobowiązuje się do utrzymania ważności tego certyfikatu przez cały okres obowiązywania gwarancji, ewentualnie nakazanie Zamawiającemu dopuszczenia rozwiązań/wymagań równoważnych.

Stosownie do pkt. 3.1.1 OPZ oferowane szyfratory IP muszą być kompatybilne, zapewniać wymianę informacji w ramach rozwiązania obecnie posiadanego przez Zamawiającego, bez konieczności modyfikowania tego rozwiązania. We wstępie do OPZ wskazano, iż etap I modernizacji niejawnej sieci IP SSG został zrealizowany pod koniec IV kwartału 2012 r., w ramach tego postępowania Zamawiający zakupił urządzenia szyfrujące IP KRYPTON K2.

Zgodnie z definicją sformułowania „kompatybilny" podawaną przez Słownik języka polskiego PWN, kompatybilny oznacza „*mogący działać łącznie z innymi urządzeniami tego typu, odpowiadający czemuś lub przystosowany do czegoś pod każdym względem*".

Jedynym urządzeniem szyfrującym, które jest kompatybilne z rozwiązaniem obecnie posiadanym przez Zamawiającego (tj. szyfratorami IP KRYPTON K2) są szyfratory IP KRYPTON K2. Agencja Bezpieczeństwa Wewnętrznego opracowuje na potrzeby każdego producenta indywidualną wersję algorytmu, co za tym idzie na rynku nie jest dostępny żaden inny szyfrator, który mógłby odpowiadać i być w pełni przystosowany do urządzenia oferowanego przez KRYPTON Polska sp. z o.o. z siedzibą w Warszawie. Takie działanie Zamawiającego nie może być uznane choćby za pozór zapewnienia neutralności technologicznej i zapewnienie równości wykonawców i uczciwej konkurencji.

Odwołujący podkreśla, iż w poprzednio prowadzonym postępowaniu Zamawiający nie stawiał takiego wymogu. Wymóg ten pojawił się dopiero w przedmiotowym postępowaniu, a zatem już po dokonaniu przez Zamawiającego zakupu urządzeń szyfrujących IP KRYPTON K2. Postawiony przez Zamawiającego wymóg, dotyczący kompatybilności, nie znajduje

uzasadnienia merytorycznego. Z technicznego punktu widzenia możliwe jest bowiem skuteczne eksploatowanie systemu składającego się z kilku rodzajów szyfratorów, które wzajemnie same z sobą nie są kompatybilne, natomiast możliwa jest ich zgodna współpraca w ramach jednej sieci (jednego systemu przetwarzania informacji niejawnych). Zastosowanie różnych szyfratorów nie uniemożliwia prawidłowego funkcjonowania systemu. Zatem przedmiotowy wymóg jest wymogiem nadmiernym, nie znajdującym uzasadnienia - a jednocześnie ogranicza krąg wykonawców, którzy mogą zaoferować swoje produkty wyłącznie do jednego wykonawcy.

Co więcej, wymóg ten pozostaje w sprzeczności z ustawowym wymaganiem neutralności technologicznej. Zgodnie z art. 3 pkt 19 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity z dnia 7 grudnia 2012 r., Dz. U. z 2013 r. poz. 235) neutralność technologiczna oznacza „*zasadę równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań*".

Wobec tego, Odwołujący wniósł o zmianę treści ogłoszenia i SIWZ przez usunięcie przedmiotowego wymogu, ewentualnie nakazanie Zamawiającemu dopuszczenia rozwiązań równoważnych.

W opinii Odwołującego, wymaganie klawiatury i wbudowanego wyświetlacza samo w sobie nie narusza ustawy. Problem polega na tym, iż Zamawiający wymaga jednoczesnego spełnienia kilku wymogów. I tak, połączenie wymogu (hasłowo) kompatybilności z wymogiem posiadania przez urządzenie klawiatury i wyświetlacza wbudowanego w panelu przednim jednoznacznie wskazuje na produkt KRYPTON K2 firmy KRYPTON Polska sp. z o.o.

Zgodnie z pkt 3.1.19 OPZ szyfrator IP musi posiadać klawiaturę oraz wyświetlacz wbudowany w panelu przednim urządzenia. Zamawiający nie określił, w jakim celu wymaga, aby szyfrator był wyposażony w ww. elementy. Standardowo, wyświetlacz wykorzystywany jest w celu przekazywania informacji o stanie pracy (statusie) urządzenia.

Formułując wymogi w zakresie opisu przedmiotu zamówienia Zamawiający winien kierować się celem, jakiemu zamawiane produkty mają służyć, a każde wymaganie musi znajdować uzasadnienie w obiektywnych potrzebach zamawiającego. Wymóg, aby oferowane szyfratory posiadały wbudowany wyświetlacz nie znajduje uzasadnienia merytorycznego. Rezultat w postaci przekazywania informacji o stanie pracy urządzenia, może zostać osiągnięty również przy zastosowaniu innych alternatywnych rozwiązań np. systemu sygnałów dźwiękowych.

Także w tym przypadku, jedynym szyfratorem IP spełniającym wymagania jest obecnie urządzenie szyfrujące IP KRYPTON K2. Wprawdzie oferowany przez Odwołującego szyfrator ETA VPN 100P ma wbudowany wyświetlacz, ale jak wcześniej wskazano Zamawiający wie, iż nie posiada on certyfikatu na okres wymagany przez Zamawiającego.

W związku z powyższym, Odwołujący wniósł o zmianę treści ogłoszenia i SIWZ przez wskazanie, iż urządzenie szyfrujące (szyfrator IP) musi posiadać klawiaturę oraz system umożliwiający przekazywania informacji o stanie urządzenia, ewentualnie nakazanie Zamawiającemu dopuszczenia rozwiązań równoważnych.

W przypadku, gdyby przedstawiona argumentacja i twierdzenia okazałyby się niewystarczające, Odwołujący wniósł o przeprowadzenie dowodu z opinii biegłego z zakresu informatyki w dziedzinie urządzeń szyfrujących na okoliczność wskazania ile modeli szyfratorów posiada parametry zgodne z wymaganiami zamawiającego i ilu wykonawców oferuje takie szyfratory.

Za szczególnie ważne, w ocenie Odwołującego, należy uznać ustalenia zawarte w wyroku Sądu Apelacyjnego w Warszawie VI Wydział Cywilny z dnia 24 stycznia 2012 r. sygn. akt: VI ACa 965/11, który wskazał: „*W ocenie Sądu Apelacyjnego w ramach niniejszego postępowania na powodzie spoczywał ciężar wykazania, że sposób opisu przedmiotu zamówienia mógł utrudniać uczciwą konkurencję i przedstawione przez powoda dowody, w szczególności opinia biegłego sądowego, dają podstawy do uznania, że sposób sformułowania specyfikacji istotnych warunków zamówienia w zakresie opisu przedmiotu zamówienia wskazuje, mimo braku powołania się na określone znaki towarowe, patent czy pochodzenie, że tylko jeden model pojazdów oferowanych na rynku w dacie wszczęcia postępowania o udzielenie zamówienia publicznego spełniał postawione przez zamawiającego wymagania. (…) Wobec powyższego to na pozwanych [tj. zamawiającym] spoczywał obowiązek wykazania, że wymagania określone w SIWZ wynikają ze zobiektywizowanych potrzeb zamawiającego i nie są na tyle wygórowane, aby mogły utrudnić lub uniemożliwić dostęp do przedmiotu zamówienia innym wykonawcom. W ocenie Sądu Apelacyjnego pozwani powyższych okoliczności w toku postępowania nie wykazali, zaś dokonanie przez zamawiającego opisu przedmiotu zamówienia polegające na posłużeniu się zestawem cech właściwych wyłącznie dla konkretnego wyrobu niewątpliwie utrudnia uczciwą konkurencję*."

Krajowa Izba Odwoławcza ustaliła, co następuje:

W części 3. pkt 3.1 ppkt 3 Opisu przedmiotu zamówienia (załącznik nr 1 do SIWZ) Zamawiający postawił wymóg: „*urządzenie szyfrujące IP (szyfrator IP) musi posiadać w momencie dostawy Certyfikat Ochrony Kryptograficznej wydany przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego, zapewniający*

ochronę informacji niejawnych o klauzuli „poufne", z terminem ważności minimum na 4 lata licząc od dnia dostawy urządzeń szyfrujących IP do Zamawiającego." Jednocześnie zgodnie z ppkt 1 przedmiotowe urządzenie musi „*być kompatybilne, zapewniać wymianę informacji w ramach rozwiązania obecnie posiadanego przez Zamawiającego, bez konieczności modyfikowania tego rozwiązania*", a ponadto winno posiadać „klawiaturę oraz wyświetlacz wbudowany w panelu przednim urządzenia" (ppkt 19).

Izba dopuściła i przeprowadziła dowód z dokumentów przedłożonych przez Odwołującego wraz z pismem procesowym.

Krajowa Izba Odwoławcza zważyła, co następuje:

Odwołanie nie zasługuje na uwzględnienie.

Zarzut naruszenia przepisu art. 29 ust. 1 ustawy Pzp okazał się bezpodstawny. Zgodnie z powołanym przepisem przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności, mogące mieć wpływ na sporządzenie oferty. Odwołujący nie tylko nie wskazał jakichkolwiek okoliczności faktycznych, potwierdzających naruszenie wskazanego przepisu, ale w ogóle jakichkolwiek okoliczności faktycznych, stanowiących uzasadnienie przedmiotowego zarzutu. Powyższe prowadzi do wniosku, że zarzut ten w ogóle nie poddaje się ocenie.

Na marginesie należy jedynie zauważyć, iż w *petitum* odwołania, naruszenie powyższego zarzutu Odwołujący upatruje w sporządzeniu opisu przedmiotu zamówienia w sposób utrudniający uczciwą konkurencję i równe traktowanie wykonawców oraz w zaniechaniu dopuszczenia rozwiązań równoważnych, co jednoznacznie wskazuje, że w istocie brak związku pomiędzy uzasadnieniem prawnym i faktycznym. Wskazane okoliczności nie są bowiem objęte hipotezą normy prawnej, zawartej w przepisie art. 29 ust. 1 ustawy Pzp.

W ocenie Izby, nie znalazł również potwierdzenia zarzut naruszenia przepisu art. 29 ust. 2 ustawy Pzp. Zgodnie z normą prawną, zawartą we wskazanym przepisie, przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. Na tle przywołanej normy w orzecznictwie ukształtował się pogląd, że jakkolwiek zamawiający, prowadzący postępowanie w celu nabycia określonych dóbr ma możliwość swobodnego wyartykułowania swoich wymagań, jednakże swoboda ta nie oznacza dowolności, bowiem zamawiający ma obowiązek uwzględnienia możliwości potencjalnych wykonawców do ubiegania się o zamówienie. Nie jest jednak tak, iż zapewnienie uczciwej konkurencji oznacza dopuszczenia do udziału w postępowaniu wszystkich wykonawców, którzy są w stanie wykonać zamówienie. To z kolei oznaczałoby bowiem, że możliwości wykonawców

mają dominujące znaczenie przy formułowaniu wymogów zamawiającego, zarówno podmiotowych, jak i przedmiotowych.

Niezbędne jest zatem, na co wielokrotnie również zwracano uwagę w orzecznictwie, aby wymagania znajdowały uzasadnienie w potrzebach Zamawiającego a nie zmierzały do ograniczenia dostępu do zamówienia potencjalnym wykonawcom. To z kolei każdorazowo wymaga uwzględnienia okoliczności konkretnego zamówienia.

Przechodząc do oceny pierwszego z wymogów Zamawiającego, a mianowicie certyfikatu ochrony kryptograficznej, a ściślej terminu jego ważności, należy zwrócić uwagę, iż niniejsze postępowanie o udzielenie zamówienia publicznego stanowi kolejny etap realizowanego przez Zamawiającego zdania, polegającego na modernizacji niejawnej sieci teleinformatycznej, w tym zakupu szyfratorów. Proces ten został zapoczątkowany we wrześniu 2012 r., kiedy to Zamawiający dokonał ogłoszenia o zamówieniu na „*zakup szyfratorów IP*" (sprawa numer 44/ZP/BŁN/12). W załączniku nr 1 do SIWZ, odnoszącej się do wskazanego, poprzedzającego niniejsze postępowanie zamówienia wskazano, że „*Straż Graniczna eksploatuje rozległą sieć teleinformatyczną wykorzystywaną do przetwarzania informacji niejawnych sklasyfikowanych jako „poufne". Sieć ta oparta jest o ponad 100 urządzeń szyfrujących IP i obejmuje swoim zasięgiem Komendę Główną SG, komendy Oddziałów i Ośrodków szkoleń SG oraz placówki i dywizjony SG. Zamiarem Zamawiającego jest docelowo pełna modernizacja niejawnej sieci IP poprzez zakup nowych urządzeń wraz z niezbędną infrastrukturą zarządzającą posiadających aktualny certyfikat ochrony kryptograficznej, wydany przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego, zgodnie z art. 50 ust. 2 ustawy o ochronie informacji niejawnych. Z uwagi na możliwość pozyskania środków finansowych, Zamawiający zakłada, że docelowa modernizacja całej niejawnej sieci IP zostanie zrealizowana w kilku etapach. Realizacją przedmiotowego zamówienia będzie I etapem modernizacji niejawnej sieci IP SG*."

Jednocześnie zauważyć należy, że skoro uprzednie postępowanie dotyczyło zakupu m.in. 33 szt. szyfratorów oraz biorąc pod uwagę podane przez Zamawiającego informacje (sieć oparta obecnie o ponad 100 szt. urządzeń szyfrujących), wykonawcy tym samym uzyskali wiedzę, że modernizacja sieci teleinformatycznej wymagać będzie zakupu kolejnych (kilkudziesięciu) urządzeń szyfrujących. Racjonalnie należało również przyjąć, że wymogi dotyczące szyfratorów w toku kolejnych postępowań o udzielenie zamówienia publicznego będą przynajmniej takie, jak te, które zostały przez Zamawiającego określone pierwotnie (ważność certyfikatu kryptograficznego została ustalona na 4 lata od dnia dostawy).

W ocenie Izby, działający z należytą starannością wykonawca, powziąwszy informacje, o których była mowa wyżej, winien podjąć niezbędne kroki, zmierzające do uzyskania wymaganego przez Zamawiającego certyfikatu, w celu zapewnienia sobie

dostępu do zamówienia. Skoro nie zadbał o powyższe, za nieuprawnione należy uznać jego twierdzenia, że wymogi, dotyczące ważności przedmiotowego certyfikatu zmierzają do ograniczenia konkurencji.

Izba nie podziela stanowiska Odwołującego, że uzyskanie certyfikatu nie było możliwe. Po pierwsze, błędne jest stanowisko Odwołującego, że mając na względzie poprzednie postępowanie i terminy, wynikające z niniejszego zamówienia, na uzyskanie rzeczonego certyfikatu miał jedynie 3 miesiące. W żadnym razie bowiem nie można przyjąć, iż dopiero od momentu zakończenia poprzedniego postępowania o udzielenie zamówienia publicznego mógł podjąć czynności zmierzające do uzyskania przedmiotowego certyfikatu. Skoro ogłoszenie o zamówieniu zostało opublikowane z dniem 1 września 2012 r., to Odwołujący miał uzasadnione podstawy do podjęcia działań w tym przedmiocie. Nie zasługuje również na aprobatę twierdzenie Odwołującego, że termin na uzyskanie spornego certyfikatu upływał z dniem publikacji ogłoszenia o niniejszym zamówieniu, skoro termin ważności certyfikatu został określony przez Zamawiającego i liczony jest od dnia dostawy urządzeń, a rzeczony certyfikat winien być dostarczony z przedmiotem umowy (§ 10 ust. 1 projektu umowy).

Oznacza to, że gdyby Odwołujący podjął działania niezwłocznie po ogłoszeniu o zamówieniu, którego przedmiotem był pierwszy etap modernizacji sieci teleinformatycznej Zamawiającego, Odwołujący miałby do dyspozycji około 10 miesięcy na uzyskanie wymaganego certyfikatu. Skoro zaś sam Odwołujący twierdzi, że proces certyfikacji trwa od kilku do kilkunastu miesięcy, to nie sposób przyjąć, wobec braku wykazania przedmiotowej okoliczności, że w odniesieniu do urządzenia, które Odwołujący zamierzał zaoferować w ramach niniejszego zamówienia, przekraczałby 10 miesięcy. Terminy przeprowadzania poszczególnych etapów procesu certyfikacji, wskazane przez Odwołującego w piśmie procesowym z dnia 15 marca 2013 r., a wynikające z *Zarządzenia nr 45 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 17 sierpnia 2012 r. w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych*, stanowią łącznie 6 miesięcy (§ 6 ust. 8, § 7 ust. 1, § 8 ust. 4, § 10 ust. 2 powołanego zarządzenia), brak zaś informacji o czasie prowadzenia badań, bo ten każdorazowo jest określany w treści zawartego porozumienia (§ 7 ust. 4 przedmiotowego zarządzenia). Nie sposób zatem przyjąć, przy hipotetycznym określeniu czasu trwania badań certyfikacyjnych i uwzględnieniu okoliczności, że wskazane terminy mają charakter instrukcyjny, że Odwołujący nie miał obiektywnych możliwości uzyskania spornego certyfikatu, od momentu, w którym mógł podjąć działania do dnia dostawy.

W tym miejscu, zwrócenia uwagi wymaga również okoliczność, że określenie przez ABW czasu przeprowadzania poszczególnych prac badawczych, następuje z uwzględnieniem terminów maksymalnych oraz, że poszczególne etapy prac badawczych

mogą być wykonywane równolegle. Podstawą wskazanych wniosków są postanowienia (w szczególności § 6 ust. 3 i 5), zawarte we wzorze porozumienia, zawieranego pomiędzy Szefem ABW a wnioskodawcą, który to wzorzec przedstawił Odwołujący.

Istotne znaczenie dla rozstrzygnięcia niniejszej sprawy ma okoliczność, że proces certyfikacji nie musi być tak długotrwały, jak wskazywał Odwołujący, a uzyskanie spornego certyfikatu na potrzeby realizacji niniejszego zamówienia było możliwe. Zwrócić należy uwagę, że w piśmie z dnia 23 października 2012 r. ABW w odpowiedzi na zapytanie Odwołującego, informuje, że proponowany „*termin wystawienia certyfikatu w sytuacji, gdy nawet nie został jeszcze złożony wniosek WK 01, może być trudny do realizacji.*" Jakkolwiek nie wiadomo, jaki termin został wskazany przez Odwołującego, bowiem Odwołujący zaniechał przedłożenia treści pisma z dnia 18 października 2012 r., co wydaje się nie być bez znaczenia, to jednak na tej podstawie, przy uwzględnieniu okoliczności, że powołana korespondencja była prowadzona, w celu realizacji zamówienia, dotyczącego pierwszego etapu modernizacji sieci teleinformatycznej Zamawiającego, zaś termin dostawy został przewidziany na dzień 21 grudnia 2012 r. można przyjąć, że proces certyfikacji może być przeprowadzony w ciągu kilku miesięcy. Stanowisko powyższe wydaje się być uzasadnione również i z tej przyczyny, że Odwołujący, czy też podmioty powiązane kapitałowo z Odwołującym, wielokrotnie inicjowały procesy certyfikacji, a doświadczenie w tym względzie, z pewnością nie pozostaje bez wpływu na czas trwania tego procesu.

Wreszcie zauważyć należy, iż zgodnie z przepisem art. 50 ust. 3 ustawy o ochronie informacji niejawnych proces certyfikacji inicjuje sam zainteresowany. Brak w ustawie jakichkolwiek ograniczeń co do terminu składania wniosku o przeprowadzenie certyfikacji urządzenia, w sytuacji, w której urządzenie posiada jeszcze ważny certyfikat. Skoro tak, to należy przyjąć, iż objęte jest to wolą wnioskodawcy. Co istotne, na jakiekolwiek ograniczenia w tym przedmiocie, nawet wynikające z przyjętej przez ABW praktyki, nie wskazuje również sam Dyrektor Departamentu Bezpieczeństwa Teleinformatycznego ABW w powoływanym już piśmie z dnia 23 października 2012 r. Stąd za nieuzasadnione należy uznać twierdzenia zawarte w opinii z dnia 13 marca 2013 r.

Nadto, co istotne, Odwołujący nie przedstawił porozumienia zawartego z ABW, dotyczącego urządzenia, które zamierzał zaoferować w niniejszym postępowaniu, z którego w sposób jednoznaczny mogłoby wynikać, że proces certyfikacji, w szczególność badania certyfikacyjne, z uwagi na planowany czas ich trwania, nie pozwalają Odwołującemu na uzyskanie spornego certyfikatu w terminie, umożliwiającym ubieganie się o udzielenie niniejszego zamówienia.

Jednocześnie Izba podziela stanowisko Zamawiającego, że zważywszy na przedmiot zamówienia i potrzeby Zamawiającego, był on uprawniony do żądania certyfikatu ochrony kryptograficznej z terminem ważności 4 lata od dnia dostawy urządzenia. W pierwszej

kolejności wskazać należy, że rzeczone certyfikaty, zgodnie z przepisem art. 50 ust. 4 ustawy o ochronie informacji niejawnych, wydawane są na minimum trzy lata. Nadto, obecnie praktyka wydawania certyfikatów przez ABW jest taka, co wynika z opinii z dnia 13 marca 2013 r., przedłożonej przez Odwołującego, że są one wydawane na okres 6 lat. Zwrócić również należy uwagę, że w przypadku urządzeń kryptograficznych, przeznaczonych do ochrony informacji niejawnych o klauzuli „poufne" posiadanie przez konkretny egzemplarz urządzenia wymaganych certyfikatów, stanowi o możliwości zastosowania urządzenia w systemie teleinformatycznym, podlegającym akredytacji lub już akredytowanym (§ 4 ust. 2 powoływanego zarządzenia nr 45 Szefa ABW). Jednocześnie uwzględniając okoliczność, że modernizacja sieci teleinformatycznej będzie polegała na zakupie nowych urządzeń i będzie przebiegała w kilku etapach, którą Zamawiający jest zobowiązany ukończyć z upływem roku 2013, nie sposób przyjąć, że potrzeby Zamawiającego zostaną zabezpieczone w sytuacji, w której sporny certyfikat będzie ważny do 27 lutego 2014 r. W ocenie Izby, Zamawiający ma prawo oczekiwać, że ważność certyfikatu będzie jak najdłuższa, bowiem powyższe, nie uwzględniając zdarzeń nadzwyczajnych, np. kradzież, gwarantuje możliwość kilkuletniego wykorzystania urządzeń i co do zasady, ciągłość ich wykorzystania, co uwzględniając, zadania Zamawiającego i wymogi w przedmiocie akredytacji użytkowanej sieci teleinformatycznej, ma istotne znaczenie.

Nadto, nie sposób również nie zauważyć, że wymóg dotyczący terminu ważności spornego certyfikatu jest nie tylko możliwy do spełnienia i uzasadniony, ale nie jest również wygórowany. Biorąc pod uwagę, że certyfikaty wydawane są na minimum 3 lata, zaś zazwyczaj na okres lat 6., należało dojść do przekonania, że wymóg ten jest określony racjonalnie.

Reasumując, jeśli nawet w momencie rozpatrywania niniejszej sprawy jest tylko jeden wykonawca, który legitymuje się żądanymi przez Zamawiającego certyfikatami, dotyczącymi szyfratorów IP, to w ocenie Izby, okoliczności niniejszej sprawy nie pozwalają na stwierdzenie, że opisanie przedmiotu zamówienia nastąpiło z naruszeniem zasady uczciwej konkurencji. Przytoczone wyżej okoliczności, zdaniem Izby, świadczą o tym, iż Odwołujący nie dochował należytej staranności i nie podjął działań zmierzających do uzyskania spornego certyfikatu w terminie, zabezpieczającym jego interesy w przedmiotowym postępowaniu o udzielenie zamówienia publicznego. Konieczność poniesienia kolejnych opłat związanych z przeprowadzeniem badań oraz konieczność wskazania priorytetu w certyfikacji produktów, na co wskazano w piśmie z dnia 23 października 2012 r., potwierdza stanowisko, że Odwołujący podjął konkretne decyzje biznesowe i dokonał wyboru o pierwszeństwie kontynuowania już rozpoczętej certyfikacji innego urządzenia niż to, które zamierzał zaoferować w niniejszym postępowaniu, a które spełniałoby wymagania Zamawiającego.

Tym samym należało oddalić wniosek Odwołującego o przeprowadzenie dowodu z opinii biegłego, jako nieprzydatnego dla rozstrzygnięcia niniejszej sprawy.

Odnosząc się do wymogu Zamawiającego w przedmiocie zapewnienia kompatybilności na poziomie urządzeń szyfrujących IP, który to wymóg rzekomo ogranicza uczciwą konkurencję, należało dojść do przekonania, że skoro, jak wskazał Odwołujący w toku rozprawy, nie można wykluczyć, iż ABW nada ten sam algorytm urządzeniom, pochodzącym od różnych producentów, zarzut o możliwość zapewnienia kompatybilności jedynie pomiędzy urządzeniami KRYPTON K2, a tym samym o możliwości zaoferowania w toku niniejszego postępowania, jedynie wskazanych urządzeń, należało uznać za nieudowodniony. Tym samym brak podstaw do stwierdzenia naruszenia powoływanej przez Odwołującego zasady neutralności technologicznej.

Nadto, należało uznać, że wobec zajętego w toku rozprawy przez Odwołującego stanowiska należało uznać, iż dokument prywatny w postaci pisemnej opinii, sporządzonej w celu wykazania braku możliwości osiągnięcia kompatybilności pomiędzy urządzeniami szyfrującymi różnych producentów, jest niepełny i został sporządzony jedynie na potrzeby niniejszego postępowania odwoławczego i jest elementem taktyki procesowej Odwołującego.

Przechodząc do oceny ostatniego z wymogów, a mianowicie dotyczącego wyposażenia urządzenia szyfrującego w klawiaturę i wyświetlacz, umieszczony w panelu przednim urządzenia, zauważyć należy, iż przedmiotowy wymóg nie jest kwestionowany przez Odwołującego jako wymóg samoistny, którego Odwołujący nie jest w stanie obiektywnie spełnić, bowiem nie posiada urządzenia o podanych cechach, a jest jedynie negowany wespół z wymogiem kompatybilności bądź terminu ważności certyfikatu. Powyższe wskazuje, że w istocie, gdyby wymogu w przedmiocie kompatybilności i spornego certyfikatu nie postawiono, urządzenie, które zamierza zaoferować Odwołujący, spełniałoby przedmiotowe wymaganie. Osią sporu nie jest więc wymóg odnoszący się do klawiatury i wyświetlacza, ale w istocie pozostałe wymogi.

Nadto, Odwołujący nie udowodnił, że urządzenie, które uzyska certyfikat w marcu br. spełnia wszystkie wymogi Zamawiającego, poza tymi, które dotyczą klawiatury i wyświetlacza.

Zgodnie z przepisem art. 29 ust. 3 ustawy Pzp, przedmiotu zamówienia nie można opisywać przez wskazanie znaków towarowych, patentów lub pochodzenia, chyba że jest to uzasadnione specyfiką przedmiotu zamówienia i zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń, a wskazaniu takiemu towarzyszą wyrazy "lub równoważny". Na tle powołanej regulacji należy wyrazić pogląd, że Izba nie

podziela stanowiska Odwołującego, że hipotezą normy prawnej, zawartej w powołanym przepisie jest objęta sytuacja, w której nawet w przypadku braku opisania przedmiotu zamówienia przy użyciu znaków towarowych, patentów lub wskazania pochodzenia, stwierdzić należy naruszenie wskazanego przepisu. Zdaniem Izby, opisanie przedmiotu zamówienia w taki sposób, który daje możliwość złożenia oferty jedynie jednemu wykonawcy podlega ocenie w świetle regulacji przepisu art. 29 ust. 2 ustawy Pzp.

Jeśli nawet by przyjąć za Odwołującym, sposób interpretacji powołanej normy, to również brak podstaw do uwzględnienia przedmiotowego zarzutu. Po pierwsze bowiem, jak wskazał sam Odwołujący, nie jest wykluczone, że wymóg kompatybilności jest możliwy do spełnienia na poziomie sprzętowym, również w przypadku urządzeń różnych producentów. Po drugie, na moment rozstrzygnięcia niniejszej sprawy sporny certyfikat posiada jedynie firma KRYPTON Sp. z o.o., jednakże Odwołujący nie wykazał, że w chwili dostawy inni wykonawcy nie będą dysponowali rzeczonym certyfikatem, w tym on sam.

Izba nie podziela również twierdzeń Odwołującego w przedmiocie ciężaru dowodu. W ocenie Izby, ciężar ten spoczywa na Odwołującym, nie mamy bowiem do czynienia z domniemaniami prawnymi. Nie inaczej wypowiedział się również w cytowanym przez Odwołującego wyroku, Sąd Apelacyjny w Warszawie, który stwierdził, że *„na powodzie spoczywał ciężar wykazania, że sposób opisu przedmiotu zamówienia mógł utrudniać uczciwą konkurencję”.*

Brak podstaw do uznania trafności zarzutów naruszenia przepisów art. 29 ust. 1, 2 i 3 ustawy Pzp powoduje, że zarzut naruszenia przepisów art. 7 ust. 1 i 3 ustawy Pzp również nie zasługiwał na uwzględnienie.

Wobec powyższego orzeczono jak w sentencji.

O kosztach postępowania orzeczono stosownie do wyniku sprawy, na podstawie art. 192 ust. 9 i 10 w zw. z § 3 pkt 1 lit. a i b 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 (Dz. U. Nr 41, poz. 238), zaliczając do kosztów postępowania odwoławczego wpis od odwołania w wysokości 15.000,00 zł oraz wynagrodzenie pełnomocnika Zamawiającego w kwocie 3.600,00 zł.

Przewodniczący: ……