Fundusze Europejskie Polska Cyfrowa | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Boguszów – Gorce, dnia 10.05.2023 r.

Znak sprawy: ZP.271.12.2023

Wszyscy Wykonawcy

Dotyczy postępowania pn.: ***Dostawa sprzętu informatycznego - w ramach realizacji projektu grantowego „Cyfrowa Gmina”***

Zamawiający działając na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych (Dz.U. z 2022r. poz. 1710 ze zm.) dalej ustawa Pzp, **udziela odpowiedzi na pytania** oraz działając zgodnie z art. 286 ust. 1 ustawy Pzp, Zamawiający **modyfikuje zapisy przedmiotowej Specyfikacji Warunków Zamówienia.**

Pytanie 1.
Czy Zamawiający będzie wymagał, aby każdy komputer posiadał naklejkę hologramową potwierdzającą oryginalność zainstalowanego systemu operacyjnego, a także - w przypadku oprogramowania Microsoft typu OEM - wymagał dostarczenia pełnego pakietu OEM (koperta z nadrukiem, płyta DVD z obrazem systemu wraz z hologramem) lub
Czy Zamawiający, w przypadku zaoferowania przez potencjalnych oferentów oprogramowania firmy Microsoft typu DOEM, będzie weryfikował posiadanie przez producenta komputera ważnej umowy z firmą Microsoft (dotyczy także oprogramowania w wersji edukacyjnej, do którego odsprzedaży są upoważnieni tylko oficjalni partnerzy firmy Microsoft)?
Należy zwrócić uwagę, że używanie klucza licencyjnego systemu operacyjnego zaimplementowanego w BIOS (zaszytego w procesie OA3.0), jest możliwe tylko dla producentów sprzętu komputerowego, posiadających ważną umowę z firmą Microsoft na sprzedaż urządzeń z systemami Windows.
Lista partnerów firmy Microsoft, upoważnionych do sprzedaży komputerów z oprogramowaniem Microsoft typu DOEM (w tym Microsoft Windows w wersji edukacyjnej) posiadających ważną umowę z firmą Microsoft jest dostępna pod adresem: https://www.microsoft.com/pl-pl/dlapartnerow/doem/ .
Pytanie to uzasadniamy tym, że w ostatnim czasie w zamówieniach publicznych coraz więcej firm oferuje używane oraz podrabiane oprogramowanie komputerowe Microsoft, co może narazić Zamawiającego na konsekwencje prawne i problemy związane z użytkowaniem oprogramowania niezgodnie z postanowieniami licencyjnymi producenta oprogramowania. Krótka odpowiedź „TAK” na powyższe pytanie zabezpiecza w 100% Zamawiającego przed zarówno podrabianym jak i używanym wcześniej na innych komputerach oprogramowaniem OEM lub DOEM.

Odpowiedź:
Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich, wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego

z zasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.
W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.

Pytanie 2.
Czy Zamawiający wymaga fabrycznie nowego systemu operacyjnego (nieużywanego nigdy wcześniej), w wersji z oryginalnym nośnikiem producenta oraz certyfikatem autentyczności dla każdej licencji ?

W przeciwnym razie Zamawiający - jako odbiorca końcowy, ponoszący odpowiedzialność za oprogramowanie które zakupił – narazi się na konsekwencje finansowe i prawne, związane z użytkowaniem nielegalnego lub zabronionego, używanego wcześniej oprogramowania.

Odpowiedź:
Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich, wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego z zasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytanie 3.
Czy dla wszystkich licencji oprogramowania systemowego, Zamawiający w celu uniknięcia potencjalnego oferowania przez Wykonawców nielegalnych systemów operacyjnych w wersji OEM (w tym używanych i wcześniej aktywowanych systemów operacyjnych) zgodzi się na dodanie do swz bądź projektu umowy następującego zapisu:
„Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego systemu operacyjnego nieużywanego oraz nie aktywowanego nigdy wcześniej na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku systemu operacyjnego naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta”?

Jesteśmy przekonani, że dzięki takiemu zapisowi do wzoru umowy Zamawiający otrzyma od potencjalnego Wykonawcy w pełni oryginalne oprogramowanie zgodne z warunkami licencjonowania producenta oprogramowania.

W przeciwnym razie Zamawiający - jako odbiorca końcowy, ponoszący odpowiedzialność za oprogramowanie które zakupił – narazi się na konsekwencje finansowe i prawne, związane z użytkowaniem nielegalnego lub zabronionego, używanego wcześniej oprogramowania.

Odpowiedź:
Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich, wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego z zasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
W ramach procedury odbioru związanej z wykonaniem umowy o udzielenie zamówienia publicznego, Zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem.
W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytanie 4.
Czy Zamawiający, w celu zabezpieczenia swojego interesu (zarówno finansowego, jak i prawnego) skorzysta z przysługującego mu prawa do weryfikacji dostarczonego sprzętu na etapie dostawy pod kątem legalności oprogramowania?

Pragniemy zauważyć, że według ostrożnych szacunków firmy Microsoft ok. połowa oprogramowania obecnie sprzedawanego w Polsce w sektorze zamówień publicznych może być podrabiana, szczególnie zaś problem ten dotyczy oprogramowania Microsoft Windows (aby zobaczyć jak bardzo poważny jest to problem, wystarczy wpisać w popularnym serwisie aukcyjnym frazę: „windows 10” i zobaczyć jak duża jest rozpiętość cenowa oferowanego tam rzekomo oryginalnego oprogramowania) ale również Microsoft Office Home&Business (również wystarczy wpisać w popularnym serwisie aukcyjnym frazę „Home & Business” by zauważyć jaka jest rozpiętość cenowa „oryginalnego i nowego licencjonowanego oprogramowania”.

Dodatkowo chcemy poinformować Zamawiającego, że taka weryfikacja legalności oprogramowania na etapie dostawy jest całkowicie bezpłatna oraz, że nasza firma może pomóc Zamawiającemu przy weryfikacji takiego oprogramowania na etapie dostawy.

Odpowiedź:
Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga aby oprogramowanie było legalne. Zamawiający zastrzega sobie prawo sprawdzenia legalności oprogramowania przed spisaniem protokołu odbioru. Zgodnie z zapisami projektu umowy w przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.

Niezależnie od powyższego Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytanie 5.
Czy Zamawiający, w przypadku oprogramowania OEM (Original Equipment Manufacturer) będzie wymagał dostarczenia pełnego pakietu OEM, tj koperty z nadrukiem, nośnikiem DVD z obrazem systemu oraz hologramem?

W ostatnim czasie w wielu zamówieniach publicznych pojawiają się wykonawcy, którzy w ramach dostawy dostarczają tylko sticker z kluczem produktu (tego typu stickery można znaleźć na portalach aukcyjnych z Chin) – stickery te nie spełniają podstawowych wymagań dotyczących legalności.
Zgodnie z warunkami licencjonowania oprogramowania Windows, firmy Microsoft, tylko dostarczenie całości produktu OEM, tj. koperty z nadrukiem, wewnętrznej części, w której umieszczony jest sticker oraz zabezpieczonej hologramami płyty DVD z obrazem systemu, jest zgodne z warunkami licencjonowania.

Natomiast ten wzór naklejki COA w przypadku oprogramowania Windows na naszym rynku nie jest w sprzedaży od co najmniej trzech lat – więc jest rzeczą oczywistą, że te stickery, mimo, że są do złudzenia podobne do oryginalnych, nie są przeznaczone na nasz rynek a co za tym idzie Zamawiający odbierając taką dostawę naraża się na zablokowanie tych kluczy w perspektywie kilku miesięcy i problemy natury prawnej.

Dodatkowo, Microsoft na swoich stronach pod adresami:
https://www.microsoft.com/en-us/howtotell/Shop.aspx
https://www.microsoft.com/en-us/howtotell/software-packaged
pokazuje jak wyglądają obecnie sprzedawane klucze produktów OEM oraz BOX i jak w sposób łatwy sprawdzić, czy posiadają one odpowiednie zabezpieczenia (takie jak hologramy, mikrodruki, druk widoczny w świetle UV itp.)

Odpowiedź:
Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich,

wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego z zasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.
W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.

Pytanie 6.
Czy Zamawiający przeprowadzi weryfikację otrzymanego oprogramowania poprzez podanie kodu (kod QR + w formacie np. X11-11111 (gdzie 1 oznacza różne cyfry) na infolinii firmy Microsoft?
Kod ten znajduje się po prawej stronie stickera, zawierającego klucz produktu.
Podanie tego kodu pozwoli na uzyskanie szybkiej i jednoznacznej informacji, czy dostarczone Zamawiającemu licencje są przeznaczone na nasz rynek, czy też są to licencje z Chin lub innych krajów, a co za tym idzie ich użytkowanie w naszym kraju jest niezgodne z prawem i naraża Zamawiającego na spore problemy natury prawnej.
Dodatkowo, w przypadku wątpliwości Zamawiającego co do otrzymanego oprogramowania zachęcamy do kontaktu z naszą firmą – umożliwimy Zamawiającemu dużo sprawniejszy dostęp do osób w Microsoft zajmujących się problemem nielegalnego oprogramowania, które obecnie zalewa nasz rynek.

Odpowiedź:
Zgodnie z zapisami SWZ oraz jego załącznikami w ramach procedury odbioru związanej z wykonaniem umowy o udzielenie zamówienia publicznego, Zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytanie 7.
Czy Zamawiający wymaga, aby dostarczone licencje na system posiadały aktywną możliwość maksymalnej ilości aktywacji przy pomocy połączenia internetowego oraz telefonicznego przewidzianej przez producenta oprogramowania?

Odpowiedź:
Zamawiający wymaga aby dostarczone licencje na system były zgodne z zapisami SWZ oraz jego załącznikami.

Pytanie 8.
Czy Zamawiający celem zabezpieczenia się przed otrzymaniem w ramach przedmiotowego postępowania fałszowanego bądź używanego oprogramowania będzie żądał na etapie dostawy przedstawienia dokumentów dotyczących zakupu tego oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania?

Pragniemy poinformować Zamawiającego, że każda sztuka systemu operacyjnego w wersji OEM posiada swój unikalny numer seryjny który jest także zapisany na dokumencie zakupu w przypadku zakupu w oficjalnym kanale dystrybucyjnym producenta. W naszej ocenie, wymaganie tych dokumentów wraz ze sprawdzeniem zgodności w/w dokumentów z dostarczonymi licencjami oprogramowania, jest obecnie jedyną możliwością zabezpieczenia się przed otrzymaniem podrabianego bądź używanego (niezgodnego z zasadami licencjonowania EULA) oprogramowania.

Odpowiedź:
Zamawiający nie będzie wymagać dokumentów dotyczących zakupu tego oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich, wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego z zasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
W ramach procedury odbioru związanej z wykonaniem umowy o udzielenie zamówienia publicznego, Zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem.
W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytanie 9.
W jaki sposób Zamawiający zamierza zweryfikować czy w przypadku zaoferowania przez Wykonawców oprogramowania używanego (aktywowanego przynajmniej drugi raz) zostało ono odinstalowane z poprzedniego urządzenia? Czy Zamawiający zweryfikuje to bezpośrednio u producenta?

Odpowiedź:
W przypadku powzięcia przez Zamawiającego wątpliwości co do niespełnienia wymagań Zamawiającego w zakresie oprogramowania, Zamawiający przewiduje możliwość jego weryfikacji, jednakże na tym etapie nie poda szczegółów tej weryfikacji.

Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich, wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego zzasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
W ramach procedury odbioru związanej z wykonaniem umowy o udzielenie zamówienia publicznego, Zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem.
W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytanie 10.
Mając na uwadze powyżej opisane zagrożenia, jesteśmy przekonani, że istnieje konieczność nałożenia na dostawców, przez zamawiające jednostki rządowe ogłaszające przetargi publiczne, obowiązku złożenia oświadczenia, w ramach dokumentacji wymaganej przez zamawiającego, o zaproponowanej poniżej lub zbliżonej treści. W związku z tym czy Zamawiający będzie żądał na etapie składania ofert następującego oświadczenia wykonawcy: „Będąc świadomym konsekwencji wynikających z przepisów prawa: niniejszym oświadczam, że uzyskanie, zwielokrotnianie i rozpowszechnianie oprogramowania [---] dokonywane w celu wykonania przedmiotowego zamówienia publicznego, nie naruszyło i nie będzie naruszać praw własności intelektualnej żadnej osoby trzeciej i jest zgodne z Ustawą o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r., Prawem własności przemysłowej z dnia 30 czerwca 2000 r. (Dz. U. z 2013, poz. 1410), oraz innymi obowiązującymi przepisami polskiego prawa. Oświadczam również, że certyfikaty i etykiety producenta oprogramowania dołączone do oprogramowania [---] i inne elementy oprogramowania, są oryginalne, a oprogramowanie jest nowe i nie używane nigdy wcześniej”?

Odpowiedź:
Zamawiający nie będzie wymagał dodatkowego oświadczenia w powyższym zakresie.
Zamawiający, zgodnie z zapisami SWZ oraz jego załącznikami wymaga fabrycznie nowego oprogramowania, pochodzącego z oficjalnych kanałów dystrybucji, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu, wolnego od obciążeń osób trzecich,

wolnego od wad fizycznych i prawnych, objętego wsparciem producenta oraz zgodnego z zasadami licencjonowania, a także wymaga aby było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności np. certyfikatami autentyczności, hologramami itp.
W ramach procedury odbioru związanej z wykonaniem umowy o udzielenie zamówienia publicznego, Zamawiający zastrzega sobie prawo weryfikacji czy oprogramowanie i powiązane z nim elementy, takie jak certyfikaty/etykiety producenta oprogramowania dołączone do oprogramowania są oryginalne i licencjonowane zgodnie z prawem.
W przypadku identyfikacji nielicencjonowanego lub podrobionego oprogramowania lub jego elementów, w tym podrobionych lub przerobionych certyfikatów/etykiet producenta, Zamawiający zastrzega sobie prawo do wstrzymania płatności do czasu dostarczenia oprogramowania i certyfikatów/etykiet należycie licencjonowanych i oryginalnych oraz do odstąpienia od umowy w terminie 7 dni od daty dostawy. Ponadto, powyższe informacje zostaną przekazane właściwym organom w celu wszczęcia stosownych postępowań.
Zamawiający wskazuje również, że Wykonawca ponosi pełną odpowiedzialność za wady prawne dostarczonego sprzętu i oprogramowania.

Pytania dotyczy punktu 1 oraz 2 OPZ - zestaw komputerowy/komputer stacjonarny

Pytanie 11.
W punkcie 12 - bezpieczeństwo Zamawiający opisał dedykowany układ służący do tworzenia i zarządzania kluczami. Czy Zamawiający dopuści zatem układ TPM w wersji programowalnej tzw. fTPM, gdyż obecnie większość producentów stosuje to rozwiązanie?

Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie.
Zamawiający dokona modyfikacji SWZ - Szczegółowego Opisu Przedmiotu Zamówienia w tym zakresie zgodnie z zapisem dla odpowiedzi dla pytanie nr 12.

Pytanie 12.
W punkcie 11 i 12 Zamawiający opisał wbudowany w obudowie system diagnostyczny oraz system diagnostyczny z graficznym interfejsem użytkownika.
Zapis ten ogranicza jedynie konkurencję i możliwości dobrania komputerów polskich producentów takich jak NTT czy Petrosoft, które jakościowo dorównują firmą z czołówki rynku jednakże są znacznie tańsze ponieważ nie dopłaca się zbędnie za markę. Wykreślenie tego zapisu spowoduje zwiększenie konkurencyjności ofert, a jednocześnie pozwoli Zamawiającemu zmniejszyć ostateczną kwotę przeznaczoną na realizację zamówienia.
Dlatego też wnioskujemy o usunięcie tych zapisów z OPZ.

Odpowiedź:
Zamawiający dokona modyfikacji SWZ - Szczegółowego Opisu Przedmiotu Zamówienia w tym zakresie zgodnie z poniższym zapisem:

Było:

„1. Zestaw komputerowy - 6 sztuk:

11	**Obudowa**	Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. Wszystkie połączenia pomiędzy podzespołami komputera muszą być wykonane wewnątrz obudowy.
12	**Bezpieczeństwo**	Ukryty w laminacie płyty głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie posiada możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS lub w menu boot'owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do Internetu, braku dostępu do sieci, bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.

2. Komputer stacjonarny - 10 sztuk:

10	**Obudowa**	Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. Wszystkie połączenia pomiędzy podzespołami komputera

		muszą być wykonane wewnątrz obudowy.
11	**Bezpieczeństwo**	Ukryty w laminacie płyty głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie posiada możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS lub w menu boot'owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do Internetu, braku dostępu do sieci, bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.

”

Jest:

„1. Zestaw komputerowy - 6 sztuk:

11	**Obudowa**	Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. Wszystkie połączenia pomiędzy podzespołami komputera muszą być wykonane wewnątrz obudowy.
12	**Bezpieczeństwo**	Urządzenie musi być wyposażone w technologię służącą do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza. Zaimplementowany w BIOS lub w menu boot'owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do Internetu, braku dostępu do sieci,

		bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.

2. Komputer stacjonarny - 10 sztuk:

10	**Obudowa**	Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS. Wszystkie połączenia pomiędzy podzespołami komputera muszą być wykonane wewnątrz obudowy.
11	**Bezpieczeństwo**	Urządzenie musi być wyposażone w technologię służącą do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza. Zaimplementowany w BIOS lub w menu boot'owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do Internetu, braku dostępu do sieci, bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.

”

Uwaga! W związku z wyżej udzielonymi odpowiedziami na pytania oraz dokonanymi modyfikacjami SWZ, Zamawiający w załączeniu do niniejszego pisma udostępnia Wykonawcom nowe/ aktualne załączniki takie jak:
a) Szczegółowy Opis Przedmiotu Zamówienia (SOPZ) – Załącznik nr 4 do SWZ
b)Oświadczenie o zgodności przedmiotu oferty z opisem przedmiotu zamówienia – Załącznik 1a.

Burmistrz Miasta Boguszowa – Gorc

Sylwia Dąbrowska

Sporz.
A.Wojtczak