ZAPYTANIE OFERTOWE
NA WYKONANIE AUDYTU BEZPIECZEŃSTWA INFORMACJI – AUDYTU ZGODNOŚCI RODO W URZĘDZIE MIEJSKIM W GIŻYCKU

Giżycko, 28.03.2018, r.

I. Postanowienia ogólne

Uwzględniając fakt, że Zamawiający planuje przeznaczyć na realizację zadania kwotę poniżej wyrażonej w złotych równowartości kwoty 30 000 euro, niniejsze postępowanie – w związku z art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych będzie procedowane na podstawie przepisów Kodeksu cywilnego (art. 70^1 i kolejne).

II. Zamawiający : Gmina Miejska w Giżycku (Urząd Miejski w Giżycku), al. 1 Maja 14, 11-500 Giżycko

III. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa informacji – audytu zgodności RODO w jednostce - Urząd Miejski w Giżycku, al. 1 Maja 14, a w szczególności:

- audyt infrastruktury bezpieczeństwa informacji, w tym w szczególności:
  -przegląd systemu ochrony technicznej i fizycznej
  - ocena systemu zabezpieczeń

- audyt zgodności KRI, w tym w szczególności:
  -systemów informatycznych, w tym audyt legalności oprogramowania, audyt bezpieczeństwa aplikacji, ochrony i zabezpieczenia danych osobowych (ochrona na poziomie sprzętu i oprogramowania komputerowego oraz infrastruktury
  - przegląd stacji roboczych, serwerów, urządzeń sieciowych (procesy, autoryzacja, zabezpieczenia, analiza systemu zarządzania kopiami zapasowymi, konfiguracja systemu),
  -przegląd konfiguracji oprogramowania, sieci LAN
  -inwentaryzacja oprogramowania, dokumentacji licencyjnej
  - skanowanie
  -weryfikacja zgodności z KRI

- audyt zgodności z RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE:

- przeprowadzenie szkolenia.

Wykonawca przy realizacji przedmiotu zamówienia zobowiązany jest w szczególności do uwzględnienia przepisów oraz wytycznych określonych w:

- rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

- ustawie z dnia 29 sierpnia 1997r. o ochronie danych osobowych (z odniesieniem się do projektowanych zmian),

- ustawie z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne,

- rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych .

Audyt winien być zakończony opracowaniem i przekazaniem raportu o stosownym poziomie poufności wraz z projektami niezbędnej zaktualizowanej dokumentacji w formie pisemnej.

Informacje uzupełniające:

- liczba stacji roboczych (komputerów) w Urzędzie: 110 szt.

- liczba urządzeń mobilnych (laptopy/tablety): laptopy- 10 szt., tablety 22 szt.

- liczba serwerów fizycznych 6

- liczba serwerów wirtualnych 2

- liczba usług teleinformatycznych ok. 39

- liczba użytkowanych systemów IT 80

- liczba pracowników – 83 osoby

W ramach usługi mają zostać przeprowadzone m.in.: następujące działania:

I. Weryfikacja spójności, kompletności i zgodności z przepisami prawa oraz Krajowymi Ramami Interoperacyjności dokumentacji odnoszącej się do:

II. Ocena podatności systemów informatycznych za pomocą profesjonalnego skanera:

1. Przegląd konfiguracji stacji roboczych obejmuje:
2. Przegląd konfiguracji serwerów obejmuje:
3. Przegląd konfiguracji urządzeń sieciowych obejmuje:
4. Przegląd konfiguracji i oprogramowania zabezpieczającego obejmuje:
5. Przegląd konfiguracji baz danych obejmuje:
6. Badanie podatności z sieci LAN za pomocą regularnie aktualizowanego automatycznego skanera bezpieczeństwa obejmuje:

8. Badanie stanu ochrony fizycznej i technicznej. Weryfikacja procedur zarządzania systemami teleinformatycznymi.

III. Audyt Legalności Oprogramowania:

1. Inwentaryzacja zainstalowanego na dyskach twardych oprogramowania (skanowanie wszystkich komputerów będących w posiadaniu Zleceniodawcy).

2. Inwentaryzacja dokumentacji licencyjnej przedstawionej przez Zleceniodawcę.

3. Weryfikacja zgodności zainstalowanego oprogramowania z posiadanymi licencjami.

4. Przygotowanie i przekazanie poufnego raportu wynikowego o stanie legalności oprogramowania po pierwszym skanowaniu w ciągu 14 dni od dnia rozpoczęcia audytu:

5. Omówienie rozbieżności między zainstalowanym na komputerach oprogramowaniem, a posiadanymi licencjami, wykazanie ewentualnych braków w dokumentacji licencyjnej oraz wskazanie sposobów ich eliminacji.

6. Wskazanie najkorzystniejszych możliwości, uzupełnienia brakujących licencji.

7. Sporządzanie spisu oprogramowania do usunięcia lub uzupełnienia licencji.

8. Merytoryczna pomoc przy opracowaniu właściwych firmowych Zasad Zarządzania Oprogramowaniem oraz przekazanie wzorów dokumentów (porozumienie, metryka, zarządzenie).

10. Przygotowanie i przekazanie końcowego raportu wynikowego z przeprowadzonego audytu przed terminem zakończenia audytu.

11. Wystąpienie do firmy Microsoft z wnioskiem o nadanie Zleceniodawcy Certyfikatu „Microsoft Software Assets Management".

IV. Audyt zgodności RODO - Aktualizacja dokumentacji pod względem wdrożenia w UM Giżycko RODO.

V. Opracowanie raportu zawierającego wskazówki niezbędnych działań do spełnienia wymogów Krajowych Ram Interoperacyjności odnoszących się do Bezpieczeństwem Informacji.

VI. Przeprowadzenie szkolenia pracowników UM z ochrony danych osobowych (z uwzględnieniem RODO).

Termin wykonania zamówienia: termin realizacji – 30 dni od daty podpisania umowy.

Kryterium wyboru oferty: cena, doświadczenie, kwalifikacje wykonawcy
Kryteria oceny ofert:

70% - Cena.

25% - Doświadczenie osoby przeprowadzającej czynności - polegające na przeprowadzeniu więcej niż 15 działań audytowych w jednostkach administracji publicznej w ciągu ostatnich 24 miesięcy:

- 15 i mniej działań audytowych (jednostek audytowanych) – 0 pkt

- 16 – 20 działań audytowych (jednostek audytowanych) - 5 pkt

- 21-30 działań audytowych (jednostek audytowanych) - 10 pkt

- powyżej 30 działań audytowych jednostek audytowanych) – 25 pkt

VIII. Warunki udziału w postępowaniu oraz opis sposobu przygotowania oferty

Wymagania wobec Wykonawców/osób bezpośrednio realizujących przedmiot zamówienia:

- wykonali co najmniej 15 działań audytowych tożsamych z przedmiotem zamówienia w jednostkach administracji publicznej,

Dodatkowo pożądane: posiada uprawnienia Audytora Wiodącego ISO 27001:2013

Warunki udziału:

1. Wiedza i doświadczenie

Wykonawca lub Audytor bezpośrednio wykonujący zadanie audytowe zobowiązany jest wykazać, że w okresie ostatnich 36 miesiącach przed upływem terminu składania ofert, a jeśli okres prowadzenia działalności jest krótszy - w tym okresie, należycie wykonał co najmniej: 15 zamówień, polegających na wdrożeniu systemu bezpieczeństwa informatycznego lub przeprowadzeniu audytu systemu bezpieczeństwa informatycznego w jednostkach sektora publicznego, zgodnie z Rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych lub standardem ISO 27001.

2.Osoby zdolne do wykonania zamówienia:

Wykonawca zobowiązany jest wykazać, że dysponuje zespołem składającym się co najmniej z 2 osób, w tym audytora wiodącego legitymującego się niżej wymienionymi certyfikatami:

•Audytor Wiodący ISO 27001;
•Audytor wewnętrzny ISO 27001

Dodatkowo, pożądane:
•Microsoft MCP
•Microsoft MCSA

Dokumenty jakie winien przedłożyć Wykonawca:

1.Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

2.Wykaz osób uczestniczących w wykonywaniu zamówienia wraz z potwierdzeniem niezbędnych kwalifikacji, uprawnień.

3.Wykaz wykonanych usług wykonanych w ciągu ostatnich 36 miesięcy.

4. Oświadczenia osób bezpośrednio wykonujących audyt o niekaralności.

5. W przypadku podpisywania dokumentów, przez osoby upoważnione/ pełnomocników, należy złożyć stosowne dokumenty potwierdzające upoważnienie / pełnomocnictwo.

6. Szczegółowy harmonogram działań audytowych.

Niespełnienie warunków udziału w postępowaniu lub niezłożenie któregokolwiek z w/w dokumentów spowoduje odrzucenie oferty Wykonawcy.

UWAGA!!!

Oferta cenowa powinna obejmować kwotę netto i brutto w odniesieniu do każdego z niżej wymienionych elementów oddzielnie:

- **audyt infrastruktury bezpieczeństwa informacji, w tym w szczególności:**
- **audyt zgodności KRI**
- **audyt zgodności z RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE:**
- **szkolenie**

Termin, miejsce i forma składania ofert

Ofertę należy przesłać drogą elektroniczną na adres: przetargi@gizycko.pl w terminie do dnia **6 kwietnia 2018 r. r. do godz.11:00.**

UWAGA! Zamawiający zastrzega sobie prawo do:

1) dodatkowych, szczegółowych negocjacji z Wykonawcami,

2) dokonania wyboru wybranego zakresu zamówienia,

2) odwołania postępowania, unieważnienia go w całości lub w części w każdym czasie bez podania przyczyny,

3) zamknięcia postępowania bez dokonania wyboru oferty oraz bez uzasadnienia,

4) zmiany terminów wyznaczonych w ogłoszeniu,

5) żądania dokumentów, szczegółowych informacji i wyjaśnień od Wykonawców na każdym etapie przetargu,

6) wyłącznej interpretacji zapisów ogłoszenia, jak również jego załączników.

Wykonawcy nie przysługują roszczenia w związku z przygotowaniem oferty i udziałem w postępowaniu.

Z up. Burmistrza
Arkadiusz Wojciński
Sekretarz Gminy Miejskiej