Hajnówka, 2020-02-19

Numer sprawy: OA. 272.8.2020

ZAPROSZENIE

Zapraszam do złożenia oferty cenowej w prowadzonym postępowaniu o udzielenie zamówienia na: **"Przeprowadzenie audytu bezpieczeństwa informacji oraz wykonanie testów podatności systemów informatycznych i infrastruktury sieciowej w Starostwie Powiatowym w Hajnówce”**

Postępowanie prowadzone jest bez stosowania ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień (Dz.U. z 2019 r. poz. 1843 ze zm.) właściwe dla zamówień o równowartości poniżej 30.000 euro, zgodnie z art. 4 pkt 8 tejże ustawy.

W załączeniu przesyłam Warunki zamówienia.

S T A R O S T A

Andrzej Skiepko

Klauzula informacyjna

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest Powiat Hajnowski z siedzibą w Hajnówce, ul. A. Zina 1; 17-200 Hajnówka ; tel. +48 85 682 27 18, fax +48 85 682 42 20

- inspektorem ochrony danych osobowych w Starostwie Powiatowym w Hajnówce jest Pani Violetta Miniuk, kontakt: adres e-mail: iod@powiat.hajnowka.pl , telefon/ +48 85 682 45 77[*];

- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b i c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego prowadzonym w trybie zapytania ofertowego;

- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp";

- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych [**];
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO**.

---

[*] ***Wyjaśnienie:*** *informacja w tym zakresie jest wymagana, jeżeli w odniesieniu do danego administratora lub podmiotu przetwarzającego istnieje obowiązek wyznaczenia inspektora ochrony danych osobowych.*

[**] ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

[***] ***Wyjaśnienie:*** *prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

WARUNKI ZAMÓWIENIA

I. Nazwa i adres zamawiającego /pieczęć/:

Powiat Hajnowski
ul. Zina 1, 17-200 Hajnówka
Tel.: 85 682 27 18, faks: 85 682 42 20
NIP: 6030017563
e-mail: starostwo@powiat.hajnowka.pl
www.powiat.hajnowka.pl

II. Przedmiot zamówienia.

Tytuł zamówienia **"Przeprowadzenie audytu bezpieczeństwa informacji oraz wykonanie testów podatności systemów informatycznych i infrastruktury sieciowej w Starostwie Powiatowym w Hajnówce"**

1. Przedmiot zamówienia:
2. Przedmiotem zamówienia jest wykonanie w Starostwie Powiatowym w Hajnówce, audytu według wymogów rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań systemów teleinformatycznych (Dz. U. z 2017r., poz. 2247) w zakresie bezpieczeństwa informacji oraz wykonania testów podatności systemów informatycznych i infrastruktury sieciowej na opublikowane zagrożenia.
3. Przeprowadzenie szkolenia z zakresu ochrony danych osobowych dla wszystkich pracowników Urzędu Starostwa Powiatowego w Hajnówce.
4. Szczegółowy opis przedmiotu zamówienia zawiera Załącznik do warunków zamówienia.

4. Do porozumiewania się z oferentami w sprawie przedmiotu zamówienia upoważniony jest: Pan Włodzimierz Pietruczuk – pokój nr 21, Starostwa Powiatowego w Hajnówce, tel. 85 682 30 47

III. Termin wykonania zamówienia.

Termin wykonania przedmiotu zamówienia:

Od 1.03.2020 r. do 15.12.2020 r.

IV. Warunki zamówienia (wymagania zamawiającego)

1. Audyt powinien zostać przeprowadzony zgodnie z rozporządzeniem 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 systemów teleinformatycznych (Dz. U. z 2017r., poz. 2247)
2. W postępowaniu może wziąć udział Wykonawca, który posiada niezbędną wiedzę i doświadczenie w realizacji audytów oraz dysponuje odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia tj.:

1) Wykonawca zobowiązany jest udokumentować wykonanie w okresie trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej trzech audytów potwierdzonych referencjami dotyczących wykonania audytów na zgodność z Rozporządzeniem o Krajowych Ramach Interoperacyjności,
2) Wykonawca zobowiązany jest posiadać co najmniej 2 audytorów, uprawnionych do wykonania wyżej wymienionego audytu, uprawnienia powinny być potwierdzone odpowiednimi certyfikatami.

3. Audytorzy Wykonawcy muszą udokumentować łącznie stosownymi certyfikatami posiadanie wiedzy z zakresu:
- ochrony danych osobowych
- analizy ryzyka
- analizy bezpieczeństwa w kontekście rozporządzenia KRI
4. Jako Wykonawca audytu legalności oprogramowania udokumentowuje on posiadanie statusu partnera Microsoft z kompetencją Software Asset Management.
5. W celu potwierdzenia spełniania powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z ofertą certyfikatów oraz wykazu zrealizowanych audytów bezpieczeństwa w urzędach administracji publicznej lub jednostkach samorządu terytorialnego.
6. Wykonawca ubiegający się o zamówienie powinien być podmiotem niezależnym od audytowanych jednostek,
7. Przy wyborze oferty do realizacji zamówienia zamawiający będzie się kierował kryterium: najniższa cena -100%,
8. Powyższe zapytanie oraz przesłane oferty cenowe nie zobowiązują Zamawiającego do zawarcia umowy z Wykonawcą

V. Tryb postępowania.

Postępowanie prowadzone jest bez stosowania ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień (Dz.U. z 2019 r. poz. 1843)) właściwe dla zamówień o równowartości poniżej 30 000 euro, zgodnie z art. 4 pkt 8 w/w ustawy.

VI. Opis sposobu obliczenia ceny oferty.

1. Cena oferty powinna być obliczona w złotych polskich z uwzględnieniem ewentualnych upustów, jakie oferent oferuje i należy ją określić w wysokości netto i brutto (z podatkiem od towarów i usług VAT).
2. Kwota ta musi zawierać wszystkie koszty związane z realizacją zadania niezbędne do wykonania przedmiotu zamówienia. Tak wyliczoną cenę netto oraz cenę brutto (z podatkiem VAT) należy wykazać w „Formularzu oferty", stanowiącym załącznik nr 1 do niniejszych Warunków zamówienia.
3. Kryteria oceny ofert:
- Przy wyborze oferty do realizacji zamówienia zamawiający będzie się kierował kryterium:
Najniższa cena – 100%
- Za najkorzystniejszą zostanie wybrana oferta z najniższą ceną zaoferowaną przez Wykonawcę i odpowiadająca warunkom zamówienia.
- Cena podana przez Wykonawcę za świadczoną usługę obowiązuje przez cały okres obowiązywania umowy i nie będzie podlegała zmianie.
- Wybór oferty nastąpi w terminie 10 dni od daty upływu terminu składania ofert.
- Powyższe zapytanie nie zobowiązuje Zamawiającego do zawarcia umowy z Wykonawcą.
- O wyborze najkorzystniejszej oferty Zamawiający zawiadomi oferentów, którzy uczestniczyli w postępowaniu.

VII. Oferta powinna zawierać:

1.Wypełniony „Formularz oferty"
2. Parafowany wzór umowy
3. Wzór oświadczenia wymaganego od Wykonawcy w zakresie wypełnienia obowiązków informacyjnych wynikających z RODO
4. Wykaz wykonanych usług
5. Wykaz osób, które uczestniczyć będą w realizacji zamówienia

VIII. Miejsce oraz termin składania ofert:

Oferty należy złożyć do dnia 27.02.2020 r. do godz. 12:00

1. Osobiście w Starostwie Powiatowym w Hajnówce, ul. A. Zina 1, sekretariat(I piętro pok. 19) w zaklejonej kopercie na której należy wpisać :

Nazwę i adres Wykonawcy oraz " Przeprowadzenie audytu bezpieczeństwa informacji oraz wykonanie testów podatności systemów informatycznych i infrastruktury sieciowej w Starostwie Powiatowym w Hajnówce”

2. Drogą pocztową (adres jw.) decyduje data i godzina wpływu oferty.

Oferty złożone po terminie nie będą brane pod uwagę i zostaną zwrócone na adres Wykonawcy.

IX. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy.

Z oferentem, który złoży najkorzystniejszą ofertę zostanie podpisana umowa, której wzór stanowi załącznik do Warunków zamówienia.

X. Unieważnienie postępowania o udzielenie zamówienia:

„Zamawiający zastrzega sobie możliwość unieważnienia zapytania ofertowego i nie wybrania żadnej z przedstawionych ofert bez podania przyczyny. W przypadku zaistnienia powyższych okoliczności Oferentom nie przysługują żadne roszczenia w stosunku do Zamawiającego”.

XI. Załączniki do niniejszych warunków zamówienia stanowią:

1. Druk „Formularz oferty” – załącznik nr 1 do WZ.
2. Wzór umowy – załącznik Nr 2 do WZ
3. Wzór oświadczenia wymaganego od Wykonawcy w zakresie wypełnienia obowiązków informacyjnych wynikających z RODO – zał. Nr 3 do WZ
4. Wykaz wykonanych usług – Załącznik Nr 4 do WZ
5. Wykaz osób uczestniczących w wykonywaniu zamówienia spełniających warunki określone w zapytaniu – Załącznik Nr 5 do WZ

….....….....…….....……
(podpis i pieczęć Naczelnika Wydziału/osoby upoważnionej)

Zatwierdził:

…..….....
Starosta /Wicestarosta
Hajnówka, 2020-02-19

Załącznik Nr 1 warunków zamówienia - Szczegółowy opis przedmiotu zamówienia

Podstawowym celem audytu jest ustalenie aktualnego stanu całego systemu informatycznego Zamawiającego, wykrycie potencjalnych zagrożeń i nieprawidłowości oraz ocenę bezpieczeństwa przetwarzania danych, ze szczególnym uwzględnieniem przetwarzania danych osobowych i zgodności z aktualnie obowiązującymi aktami prawnymi.

I Szczegółowy zakres audytu KRI:

1. Audyt bezpieczeństwa informacji we wszystkich obszarach funkcjonowania Starostwa:
   - audyt organizacyjny,
   - regulacje w zakresie zarządzania bezpieczeństwem informacji,
   - odpowiedzialność za bezpieczeństwo informacji
   - koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji,
   - dokumentacja z zakresu ochrony danych osobowych,
   - przeprowadzenie wywiadów z wybranymi pracownikami

2. Audyt fizyczny i środowiskowy:
   - weryfikacja granic obszaru bezpiecznego,
   - weryfikacja zabezpieczeń wejścia/wyjścia,
   - weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
   - weryfikacja bezpieczeństwa okablowania strukturalnego,
   - weryfikacja systemów chłodzenia,
   - weryfikacja systemów alarmowych

3. Audyt teleinformatyczny:
   - weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
   - weryfikacja ochrony przed oprogramowaniem szkodliwym,
   - weryfikacja procedur zarządzania kopiami zapasowymi,
   - weryfikacja procedur związanych z rejestracją błędów,
   - weryfikacja procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
   - weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
   - weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania),
   - inwentaryzacja oprogramowania i dokumentacji licencyjnej,
   - analiza i ocena mechanizmów zarządzania aktualizacjami.

4. Audyt ochrony danych osobowych:
   - przegląd zgodności przetwarzania danych osobowych z wymaganiami przepisów prawa,
   - przegląd istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych,
   - weryfikacja dokumentacji wewnętrznej pod kątem kompletności i aktualności

5. Zewnętrzne i wewnętrzne testy penetracyjne infrastruktury informatycznej:
   - testy styku sieci lokalnej z internetem przeprowadzane ze stacji roboczej podłączonej do sieci internet,
   - analiza topologii brzegu sieci,

- weryfikacja mechanizmów ochronnych,
- próba wykrycia usług sieciowych udostępnianych do internetu,
- detekcja wersji oraz typu oprogramowania dostępnego z sieci internet,
- przedstawienie rozwiązań zwiększających bezpieczeństwo styku sieci lokalnej z siecią internet.

6. Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z zewnątrz Starostwa:

- analiza topologii sieci LAN,
- weryfikacja mechanizmów ochronnych w sieci,
- analiza komunikacji sieciowej,
- skanowanie portów TCP/UDP próba wykrycia usług sieciowych,
- skanowanie hostów aktywnych w sieci,
- przedstawienie rozwiązań zwiększających bezpieczeństwo w sieci LAN.

7. Dokonanie identyfikacji zdarzeń, które mogłyby zagrozić bezpieczeństwu informacji przetwarzanych w Starostwie oraz ocenę ryzyka związanych z tymi zdarzeniami.
8. Szkolenie z Ochrony Danych Osobowych ma być przeprowadzone w siedzibie Zamawiającego i powinno uwzględniać następujące zagadnienia:

- reformę przepisów ochrony danych osobowych;
- status i zadania Administratora Danych Osobowych;
- status i zadania Inspektora Ochrony Danych;
- podstawy prawne przetwarzania danych osobowych;
- realizację obowiązku informacyjnego w praktyce;
- prawa obywateli w zakresie ochrony ich danych osobowych;
- zabezpieczenia techniczne i organizacyjne obszaru przetwarzania danych osobowych;
- wymogi formalne tj.: polityka ochrony danych, rejestr czynności przetwarzania danych;
- zadania i rola Urzędu Ochrony Danych Osobowych;
- konsekwencje prawne naruszenia zasad przetwarzania danych oraz nowe zasady kontroli.

II Zasady opracowania raportu z audytu.

Raport powinien zawierać:

1. ocenę poziomu spełnienia każdego z wymagań bezpieczeństwa określonych w § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej ora minimalnych wymagań dla systemów teleinformatycznych;
2. wykaz stwierdzonych niezgodności w odniesieniu do każdego wymagania określonego w Krajowych Ramach Interoperacyjności;

- ocenę stopnia spełnienia wymogów ustawy o ochronie danych osobowych i rozporządzenia RODO;
- ocenę spełnienia skuteczności stosowanych zabezpieczeń;
- rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności;
- określenie zakresu i priorytetu działań naprawczych.