

AOK/220/26/JKU/2017

Radomsko, 14.11.2017r.

ZAPROSZENIE DO SKŁADANIA OFERT

1. Nazwa i adres zamawiającego.

Powiatowy Urząd Pracy w Radomsku, ul. Tysiąclecia 2, 97-500 Radomsko

2. Tryb udzielenia zamówienia.

Postępowanie prowadzone jest w oparciu o obowiązujący „Regulamin udzielania zamówień publicznych w Powiatowym Urzędzie Pracy w Radomsku” o wartości nie przekraczającej wyrażonej w złotych równowartości kwoty o której mowa w art. 4 pkt 8 ustawy z dnia 29 stycznia 2004r. Prawo Zamówień Publicznych (Dz. U. z 2017r. poz. 1579).

3. Opis przedmiotu zamówienia

Usługa -przeprowadzenie Audytu Bezpieczeństwa Informacji na potrzeby Powiatowego Urzędu Pracy w Radomsku .

I. Audyt ochrony danych osobowych, określający zgodność przetwarzanych danych w Powiatowym Urzędzie Pracy w Radomsku z wymaganiami ustawy o ochronie danych osobowych.

Prace obejmować będą:

- identyfikację i weryfikację zbiorów danych osobowych oraz systemów informatycznych służących do przetwarzania danych osobowych,
- ocenę wdrożonych rozwiązań, środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych,
- rekomendacje związane z zapewnieniem skutecznego poziomu bezpieczeństwa ochrony danych osobowych,
- weryfikacja dopełnienia obowiązku powołania Administratora Bezpieczeństwa Informacji,
- weryfikacja realizacji przez Administratora Bezpieczeństwa Informacji wymaganych czynności i dokumentów,
- weryfikacja poprawności powierzenia przetwarzania danych osobowych (firmy zewnętrzne, kontrole zewnętrzne).

Podstawę prac stanowią wymagania określone w:

- a) ustawie z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (zwane dalej ustawą);
- b) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (zwanym dalej Rozporządzeniem);
- c) opinii i stanowiska Generalnego Inspektora Ochrony Danych Osobowych, wyrażone w szczególności w sprawozdaniach z działalności GIODO, w zakresie stosowanych zabezpieczeń danych osobowych.

Szczegółowe ustalenia:

Identyfikacja zbiorów danych osobowych zgodnie z definicją zawartą w art. 6 ustawy obejmować będzie zarówno zbiory przetwarzane w postaci elektronicznej jak i zbiory przetwarzane tylko w postaci papierowej. Identyfikacja zbiorów winna zostać przeprowadzona w oparciu o:

- analizę posiadanej przez Zamawiającego dokumentacji,
- analizę zakresu odpowiedzialności poszczególnych komórek organizacyjnych Zamawiającego w celu zidentyfikowania obszarów, w których są lub mogą być przetwarzane dane osobowe,
- wywiady z pracownikami Zamawiającego,
- analizę funkcjonalności i zakresu danych przetwarzanych w poszczególnych systemach informatycznych, w szczególności poprzez wizje lokalne, analizę dokumentacji systemów oraz wywiady z użytkownikami.

W trakcie identyfikacji zbiorów, inwentaryzacji podlegać będą również systemy informatyczne, w których odbywa się przetwarzanie danych osobowych, tj:

Analiza i ocena środków technicznych i organizacyjnych zapewniających należyte zabezpieczenie przetwarzanych danych osobowych, przeprowadzona zostanie w oparciu o wymagania wynikające z ustawy i rozporządzenia, z uwzględnieniem interpretacji tych wymagań przez GIODO. W szczególności analiza obejmować będzie:

- Określenie i zabezpieczenie obszaru przetwarzania danych osobowych,
- Zabezpieczenie nośników danych osobowych – zarówno elektronicznych jak i papierowych,
- Dokumentowanie czynności związanych z przetwarzaniem danych osobowych,
- Dopelnienie obowiązków informacyjnych określonych w art. 24 i art. 25 Ustawy,
- Lokalizacje komponentów systemów informatycznych (w tym monitorów ekranowych),
- Funkcjonalność systemów informatycznych przetwarzających dane osobowe:
 - Mechanizmy identyfikacji i uwierzytelnienia użytkownika
 - Sposób przechowywania i przesyłania danych uwierzytelniających
 - Mechanizmy autoryzacji dostępu do danych
 - Odnotowywanie i raportowanie informacji określonych w §7 Rozporządzenia
 - Zakres operacji na danych osobowych

- Zabezpieczenia kryptograficzne przesyłanych danych
- Zabezpieczenia kryptograficzne składowanych danych, w tym danych przetwarzanych na komputerach przenośnych
- Mechanizmy ochrony przed złośliwym oprogramowaniem
- Mechanizmy tworzenia kopii zapasowych
- Zabezpieczenie infrastruktury sieciowej, w szczególności styku z sieciami publicznymi
- Zabezpieczenie zasilania
- Umowy o powierzeniu przetwarzania danych osobowych
- Procesy zarządzania bezpieczeństwem danych osobowych, w tym:
 - * Zarządzanie dostępem do danych osobowych,
 - * Zarządzanie danymi uwierzytelniającymi (w szczególności hasłami),
 - * Udostępnianie danych osobowych,
 - * Zarządzanie kopiami zapasowymi,
 - * Zarządzanie kluczami kryptograficznymi wykorzystywanymi do ochrony kryptograficznej danych
- Monitorowanie działania systemów informatycznych
- Wprowadzanie zmian w systemach informatycznych przetwarzających dane osobowe
- Wprowadzanie zmian w zakresie przetwarzanych danych osobowych
- Serwis i konserwacja systemów informatycznych

Wyniki prac winny zostać ujęte w raporcie zawierającym rekomendacje w zakresie zapewnienia skutecznego poziomu bezpieczeństwa ochrony danych osobowych.

Rekomendacje te zostaną podzielone na:

- Rekomendacje wynikające z niezgodności z obowiązującymi wymaganiami prawnymi,
- Rekomendacje wynikające z niezgodności ze znanymi interpretacjami przepisów prawnych przez GIODO,
- Rekomendacje wynikające z dobrych praktyk, których wdrożenie zoptymalizuje techniczne i/lub organizacyjne mechanizmy zabezpieczające dane osobowe.

II. Weryfikacja dokumentacji wymaganej przez KRI

Szczegółowe ustalenia:

Sprawdzenie obecnego stanu i analiza zgodności dokumentacji związanej z bezpieczeństwem i ciągłością działania systemów informatycznych, z wymaganiami normatywnymi wskazanymi w Krajowych Ramach Interoperacyjności.

Podczas przedmiotowej weryfikacji należy przeprowadzić analizę zgodności posiadanej przez Urząd dokumentacji, z wymaganiami określonymi w Krajowych Ramach Interoperacyjności. Analizie podlegać będzie przede wszystkim dokumentacja związana z zarządzaniem bezpieczeństwem systemów informatycznych. Wyniki weryfikacji umożliwią dostosowanie procesów zarządzania bezpieczeństwem informacji i bezpieczeństwem systemów informatycznych do wymagań Krajowych Ram Interoperacyjności, co jednocześnie zapewni wysoki poziom bezpieczeństwa informacji przetwarzanych w systemach informatycznych Urzędu i usprawni procesy związane z zarządzaniem infrastrukturą informatyczną.

Analiza dokumentacji

Analiza dokumentacji ma zostać przeprowadzona pod kątem zgodności z wymaganiami Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r w sprawie Krajowych Ram Interoperacyjności oraz wskazanych w nim, aktualnie obowiązujących norm, to jest:

- PN-ISO/IEC 27001
- PN-ISO/IEC 27002
- PN-ISO/IEC 27005
- PN-ISO/IEC 24762
- PN-ISO/IEC 20000-1
- PN-ISO/IEC 20000-2

W ramach analizy dokumentacji weryfikowane będą w szczególności następujące zagadnienia:

- Ustanowienie i eksploatacja systemu zarządzania bezpieczeństwem informacji,
- Zarządzanie ciągłością działania systemów informatycznych,
- Analiza ryzyka informatycznego,
- Klasyfikacja informacji,
- Odpowiedzialność za zarządzanie bezpieczeństwem IT,
- Bezpieczeństwo we współpracy z podmiotami zewnętrznymi świadczącymi usługi związanymi z utrzymaniem IT,
- Fizyczne i środowiskowe zabezpieczenie systemów informatycznych,
- Serwis i konserwacja systemów informatycznych,
- Wycofywanie i przekazywanie sprzętu informatycznego,
- Zasady zabezpieczenia nośników danych,
- Zarządzanie uprawnieniami do systemów informatycznych,
- Zarządzanie mechanizmami chroniącymi przed złośliwym oprogramowaniem,
- Zarządzanie kopiami zapasowymi i archiwalnymi,
- Zabezpieczenie sieci informatycznych - architektura infrastruktury sieciowej, zarządzanie urządzeniami sieciowymi,
- Zasady bezpiecznej wymiany informacji w ramach systemów informatycznych,
- Zarządzanie mechanizmami kryptograficznymi,
- Zarządzanie zmianami w systemach informatycznych,
- Monitorowanie systemów informatycznych,
- Zarządzanie incydentami
- Działania kontrolne w zakresie bezpieczeństwa systemów informatycznych,
- Zarządzanie usługami informatycznymi,
- Zarządzanie personelem w kontekście bezpieczeństwa informacji,

Analizę dokumentacji należy przeprowadzić (na podstawie zebranych informacji) w siedzibie Wykonawcy.

Raport

Podsumowanie wyników prac, objętych zakresem części I, II, III, zostanie zawarte w raporcie zawierającym zarówno prawidłowe działania urzędu - analizowane wg szczegółowych ustaleniach audytu. W raporcie powinny zostać również wymienione zagadnienia, które nie zostały uregulowane lub zostały uregulowane w stopniu niezadowalającym w analizowanej dokumentacji. W sytuacji stwierdzenia nieprawidłowości Wykonawca gwarantuje wsparcie w usunięciu nieprawidłowości, czy braków.

Raport powinien zostać sporządzony po zakończeniu realizacji usługi i doręczony, po uzgodnieniach, do Zamawiającego, do końca m-ca grudnia 2017 roku.

4. Termin realizacji zamówienia.

Od dnia podpisania umowy do **20 grudnia 2017r.**

5. Miejsce , termin i sposób składania ofert.

- a) Ofertę należy złożyć w siedzibie Zamawiającego, tj. w Biurze Podawczym **Powiatowego Urzędu Pracy w Radomsku, ul. Tysiąclecia 2 , 97-500 Radomsko, bądź przesłać na adres: Powiatowy Urząd Pracy w Radomsku, ul. Tysiąclecia 2, 97-500 Radomsko , w terminie do dnia 22 listopada 2017r., do godziny 12: 00** Decydujące znaczenie dla oceny zachowania powyższego terminu ma data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską.
- b) Wykonawca powinien umieścić ofertę w zamkniętej kopercie. Na kopercie powinna widnieć nazwa i adres Zamawiającego oraz oznaczenie: „Postępowanie o udzielenie zamówienia publicznego –odpowiedź na zapytanie ofertowe : **Audyt bezpieczeństwa informacji** .
- c) Na kopercie należy podać nazwę i adres Wykonawcy oraz opatrzyć ją pieczęcią Wykonawcy.
- d) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
- e) Otwarcie ofert jest jawne i nastąpi w dniu 22 listopada 2017r. o godz. 13.00.
- f) Formularz oferty oraz dokumenty złożone przez Wykonawcę powinny być podpisane przez osoby upoważnione do składania oświadczeń woli w imieniu Wykonawcy.

Warunki udziału w zapytaniu ofertowym:

1. Wiedza i doświadczenie

Wykonawca zobowiązany jest wykazać, że w okresie ostatnich dwóch lat przed upływem terminu składania ofert, a jeśli okres prowadzenia działalności jest krótszy - w tym okresie, należycie wykonał co najmniej:

- 35 zamówień, polegające na wdrożeniu systemu bezpieczeństwa informatycznego lub przeprowadzeniu audytu systemu bezpieczeństwa informatycznego 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, (potwierdzonych pisemnymi referencjami)

2. Osoby zdolne do wykonania zamówienia:

Wykonawca zobowiązany jest wykazać, że dysponuje zespołem składającym się co najmniej z 2 osób z których każda posiada następujące certyfikaty z nadanym numerem:

- Audytor Wiodący ISO 27001;
- Audytor Wiodący ISO 22301

Osoby z podanymi certyfikatami muszą bezwzględnie przeprowadzać w urzędzie działania audytowe.

Kryteria oceny oferty:

70% - Cena.

30% -Doświadczenie polegające na przeprowadzeniu więcej niż 48 działań audytowych w jednostkach administracji publicznej w ciągu ostatnich 24 miesięcy:

-35 i mniej działań audytowych (jednostek audytowanych) 0 pkt

-36-47 działań audytowych (jednostek audytowanych) 10pkt

-48-50 działań audytowych (jednostek audytowanych) 30pkt

Dokumenty jakie winien przedłożyć Wykonawca:

1. Aktualny odpis z właściwego rejestru lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej wystawiony nie wcześniej niż 6 m-cy przed upływem terminu składania ofert.
2. Wykaz osób uczestniczących w wykonywaniu zamówienia sporządzony na podstawie wzoru stanowiącego załącznik nr 1 do zaproszenia ofertowego.
3. Wykaz wykonanych usług sporządzony na podstawie wzoru stanowiącego załącznik nr 2 do zaproszenia ofertowego.
4. W przypadku podpisywania dokumentów, przez osoby upoważnione/ pełnomocników, należy złożyć stosowne dokumenty potwierdzające upoważnienie / pełnomocnictwo.

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

7. Sposób porozumiewania się z Wykonawcami.

a) Wszelkich dodatkowych informacji dotyczących przedmiotowego zaproszenia udziela: **Joanna Kukielka – Starszy inspektor ds. administrowania siecią komputerową**, tel. 44 683 73 56 wew. 74, fax. 44 683 73 59, e-mail : lora@praca.gov.pl

b) W niniejszym postępowaniu wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje i wyjaśnienia przekazywane będą drogą elektroniczną.

c) Wykonawca, który uzna za niezbędne uzyskanie wyjaśnień dotyczących treści niniejszego zapytania ofertowego, powinien wystąpić z zapytaniem do Zamawiającego w sposób wskazany w pkt. b).

d) Wszelkie wyjaśnienia dotyczące zaproszenia zostaną udzielone niezwłocznie wszystkim Wykonawcom bez ujawnienia źródła zapytania. Wyjaśnienia zostaną przesłane do Wykonawców drogą elektroniczną oraz zostaną zamieszczone na stronie internetowej <http://bip.pup-radomsko.pl/>

6. Informacja o formalnościach, jakie powinny zostać dopełnione po wyborze ofert w celu zawarcia umowy w sprawie przedmiotowego zamówienia.

- a) O wyborze oferty Zamawiający zawiadomi niezwłocznie Wykonawców, którzy ubiegali się o udzielenie zamówienia.
- b) Zamawiający z wybranym Wykonawcą zawrze umowę niezwłocznie po przekazaniu zawiadomienia o wyborze oferty.

7. Informacje dodatkowe

- a) Zamawiający w związku z prowadzoną procedurą nie dopuszcza możliwości składania ofert częściowych, zamówienie należy potraktować całościowo.
- b) W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z właściwymi Wykonawcami w celu uzupełnienia przesłanych dokumentów lub doprecyzowania przesłanych dokumentów.
- c) Zamawiający zastrzega sobie prawo unieważnienia prowadzonego postępowania bez podania przyczyn.

Z poważaniem

DYREKTOR
Powiatowego Urzędu Pracy
w Radomsku

inż. Eukasz Więcek

St. INSPEKTOR
ds. Administracji Bieżącą Komputerową
Joanna Kukielka

