ISTOTNE WARUNKI UDZIELENIA ZAMÓWIENIA

w związku z art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.*).*

Dotyczy postępowania o udzielenie zamówienia publicznego o wartości równej lub przekraczającej równowartość kwoty 6 000 euro i nieprzekraczającej równowartości 30 000 euro na **przeprowadzenie audytu bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych**.

I. Nazwa i adres Zamawiającego:

Zamawiający: Zarząd Transportu Metropolitalnego.

Adres do korespondencji: ul. Barbary 21A, 40-053 Katowice.

Godziny pracy Zamawiającego: poniedziałek – piątek od godz. 7.00. do godz. 15.00.

Tel. 32 74 38 401, faks 32 25 19 745

II. Opis przedmiotu zamówienia:

Przedmiotem zamówienia jest diagnoza stanu spełniania przez Zarząd Transportu Metropolitalnego wymagań dot. bezpieczeństwa informacji stawianych przed administratorem danych osobowych wskazanych w art. 32 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), wymogów określonych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz doradztwo w zakresie dostosowania i wdrożenia zmian w obecnym Systemie Zarządzania Bezpieczeństwem Informacji (SZBI).

Zamówienie obejmuje przeprowadzenie następujących zadań:

Zadanie I – Diagnozę stanu obecnego, mającą na celu ocenę stanu dokumentacji i procedur obowiązujących u Zamawiającego (audyt),

Zadanie II – Diagnozę stanu obecnego w zakresie stosowanych rozwiązań informatycznych, mającą na celu ocenę stanu zabezpieczeń systemów informatycznych u Zamawiającego (testy penetracyjne),

Zadanie III – Usługi doradcze obejmujące:

Analizę ryzyka (opracowanie dokumentacji metodyki szacowania ryzyka, przeprowadzenie analizy ryzyka wraz z klasyfikacją informacji przy udziale wydziałów merytorycznych Zamawiającego) uwzględniającą ryzyka dotyczące przetwarzania danych osobowych.

Opracowanie zmian w obecnym SZBI uwzględniając wymogi określone w ustawie o krajowym systemie cyberbezpieczeństwa.

1. Specyfikacja głównych wymagań:
   1) Diagnoza stanu obecnego, mającą na celu ocenę stanu dokumentacji i procedur obowiązujących u Zamawiającego (audyt).

      Audyt powinien objąć wszelkie niezbędne działania w celu określenia stopnia zgodności z przepisami prawa i zaleceniami norm PN-ISO/IEC 27001, ISO/IEC 27701, PN-ISO/IEC 22301, PN-ISO/IEC 20000

      w tym:

      - analizę obowiązujących regulacji wewnętrznych i zewnętrznych Zamawiającego;
      - opracowanie planu audytu;
      - przeprowadzenie audytu.

        Zakres zadania powinien objąć wszystkie obszary, o których mowa w normie PN−ISO/IEC 27001 i załączniku A.

Wykonawca opracuje raport zawierający ocenę odnoszącą się do poszczególnych obszarów normy. Raport będzie oparty na wynikach przeprowadzonego audytu i wskazywał elementy zgodne z normą, wymagające poprawy. Raport będzie podstawą prac w zadaniu III.

2) Diagnoza stanu obecnego w zakresie stosowanych rozwiązań informatycznych, mającą na celu ocenę stanu zabezpieczeń systemów informatycznych u Zamawiającego (testy penetracyjne).

   Wykonawca przeprowadzi testy penetracyjne infrastruktury IT m.in.:

   a) badanie luk systemów, urządzeń sieciowych, serwerów, sieci Wi-Fi,
   b) identyfikację podatności systemów i sieci na ataki typu: Dos, DDoS, Sniffing, Spoofing, XSS, Backdoor, http Flooding, Session hijacking, inne wybrane przez Wykonawcę na podstawie analizy ryzyka,
   c) skanowanie urządzeń sieci komputerowej, w szczególności: routery, przełączniki, serwery, zapory sieciowe i stacje robocze pod względem występowania podatności, luk oraz błędów w konfiguracji mających wpływ na bezpieczeństwo,
   d) skanowanie z autentykacją w celu znalezienia ewentualnych podatności systemów operacyjnych oraz oprogramowania pakietów biurowych i systemu poczty elektronicznej,
   e) uwzględniające pierwsze dziesięć podatności wymienione w ostatnim raporcie OWASP (Open Web Application Security Project) na dzień składania oferty.

   Wykonawca opracuje raport zawierający ocenę infrastruktury IT w zakresie podatności, uwzględniając pierwszych dziesięć podatności wymienionych w lit. e niniejszego ustępu wraz ze wskazaniem elementów wymagających poprawy i spełniających wymagania. Raport będzie podstawą prac w zadaniu III.

   Przy wykonaniu zamówienia należy uwzględnić, że Zamawiający dysponuje infrastrukturą, na którą składa się:

   a) do 350 stacji roboczych,
   b) do 65 maszyn wirtualnych,
   c) do 6 serwerów fizycznych,
   d) do 20 zarządzalnych przełączników,
   e) do 15 zapór sieciowych typu UTM,
   f) do 5 zasobów dyskowych typu NAS.

3) Usługi doradcze obejmujące:

   a) analizę ryzyka (opracowanie dokumentacji metodyki szacowania ryzyka, przeprowadzenie analizy ryzyka wraz z klasyfikacją informacji przy udziale wydziałów merytorycznych Zamawiającego dla 2 wybranych procesów związanych z obsługą reklamacji lub windykacji) uwzględniającą ryzyka dotyczące przetwarzania danych osobowych oraz zalecenia ujęte w raporcie wskazanym w pkt 1 i 2,
   b) opracowanie zmian w obecnym SZBI uwzględniając wymogi określone w ustawie o krajowym systemie cyberbezpieczeństwa uwzględniającą zalecenia ujęte w raporcie wskazanym w pkt 1 i 2.

4) Zadania I i II Wykonawca przeprowadzi w następujących lokalizacjach z uwzględnieniem ich specyfiki pod względem wykonywanych zadań:

   a) Biuro: Katowice przy ul. Barbary 21A,
   b) Punkty Obsługi Pasażera:
      1. **Bytom**, pl. Wolskiego,

2. **Chorzów,** Rynek 8/1,
3. **Gliwice**, pl. Piastów 2,
4. **Katowice**, dworzec kolejowy Katowice,
5. **Katowice**, ul. Pocztowa 10,
6. **Katowice**, ul. Barbary 21A (siedziba ZTM),
7. **Piekary Śląskie,** ul. Papieża Jana Pawła II 46,
8. **Sosnowiec, ul.** Warszawska 3/17,
9. **Tychy,** al. Marszałka Piłsudskiego 12.

2. Termin wykonania zamówienia – 80 dni od daty zawarcia umowy jednak nie później niż do 15 grudnia 2020 r.
3. Wykonawca jest związany ofertą 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
4. Wzór umowy stanowi załącznik nr 5 do IWUZ.

III. Informacja o oświadczeniach i dokumentach, jakie mają dostarczyć Wykonawcy.

1. Zamawiający wymaga, by każda oferta zawierała minimum następujące dokumenty:
   1) Wypełniony i podpisany przez Wykonawcę formularz cenowo – ofertowy – wzór formularza stanowi załącznik nr 1 do IWUZ.
   2) Oświadczenie, że w okresie ostatnich dwóch lat przed upływem terminu składania ofert Wykonawca należycie wykonał przynajmniej 3 audyty bezpieczeństwa informacji lub audyt ochrony danych osobowych w oparciu o normę PN-ISO/IEC 27001. Wzór oświadczenia stanowi załącznik nr 2 do IWUZ
   3) Oświadczenia, że Wykonawca dysponuje osobami zdolnymi do wykonania zamówienia, tj.:
      a) co najmniej dwoma audytorami wiodącymi, posiadającymi ważny certyfikat audytora wiodącego w zakresie PN-ISO/IEC 27001 i przynajmniej trzyletnie doświadczenie audytowe jako audytor wiodący w ramach przedmiotowej normy,
      b) co najmniej dwoma audytorami, posiadającymi ważny certyfikat audytora w zakresie ISO/IEC 27701 i przynajmniej trzyletnie doświadczenie audytowe w zakresie audytów systemu zarządzania bezpieczeństwem informacji,
      c) co najmniej dwoma audytorami wiodącymi, posiadającymi ważny certyfikat audytora wiodącego w zakresie PN-ISO/IEC 22301 i przynajmniej trzyletnie doświadczenie audytowe w ramach przedmiotowej normy,
      d) co najmniej dwoma audytorami wiodącymi, posiadającymi ważny certyfikat audytora wiodącego w zakresie PN-ISO/IEC 20000 i przynajmniej trzyletnie doświadczenie audytowe w ramach przedmiotowej normy.

         Wzór oświadczenia stanowi załącznik nr 3 do IWUZ.
      e) co najmniej czteroma audytorami bezpieczeństwa informacji z przynajmniej 2 letnim stażem audytowym w zakresie audytów przeprowadzanych w ramach przynajmniej jednej z ww. norm.

         Wzór oświadczenia stanowi załącznik nr 4 do IWUZ.

   Zamawiający nie dopuszcza w zakresie spełnienia ww. warunków dotyczących audytorów wiodących (lit. a, c, d) łączenia funkcji przez jednego audytora.

2. Postępowanie prowadzone jest w języku polskim.

IV. Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów:

1. Wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy mogą przekazywać pisemnie, w tym przy użyciu poczty elektronicznej, z zastrzeżeniem pkt VI.1 (oferta w formie pisemnej).
2. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.

V. Osoby po stronie Zamawiającego uprawnione do porozumiewania się z Wykonawcami.

1. Osobą uprawnioną do porozumiewania się z Wykonawcami i udzielania wyjaśnień w sprawach proceduralnych jest: Pan Grzegorz Włoczyk, e-mail gwloczyk@metropoliaztm.pl
2. Osobą uprawnioną do porozumiewania się z Wykonawcami i udzielania wyjaśnień w sprawach merytorycznych jest: Pan Tomasz Haska, e-mail thaska@metropoliaztm.pl
3. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie Istotnych Warunków Udzielenia Zamówienia od poniedziałku do piątku w godzinach od 8:00 do 14:00 do dnia 4 września do godziny 14:00.
4. Na zapytania doręczone Zamawiającemu po terminie wskazanym w ust. 3 Zamawiający nie będzie miał obowiązku odpowiedzi.

VI. Miejsce i termin składania i otwarcia ofert.

1. Ofertę należy złożyć **w formie pisemnej** w siedzibie Zamawiającego – ul. Barbary 21A, 40-053 Katowice pok. nr 011 (Kancelaria) w terminie do **10 września 2020 do godziny 14:00**.
2. Ofertę należy umieścić w jednym nieprzejrzystym opakowaniu oznaczonym w sposób następujący: **„Oferta na audyt dotyczący bezpieczeństwa informacji”**. Opakowanie powinno być opatrzone nazwą i adresem Wykonawcy oraz nazwą i adresem Zamawiającego, jak również napisem: **„Nie otwierać przed dniem 11.09.2020 r., godzina 12^{30}”**
3. Informacje, o których mowa w pkt VII.1, zawarte w ofertach zostaną podane w dniu **11 września 2020 r. o godz. 12:30** w siedzibie Zamawiającego w pok. nr 014.

VII. Opis sposobu obliczenia ceny.

1. Na formularzu cenowo – ofertowym (załącznik nr 1 do IWUZ) należy przedstawić cenę netto i brutto realizacji przedmiotu zamówienia oraz stawkę podatku VAT.
2. Wartość cenową należy wpisać w złotych polskich do dwóch miejsc po przecinku oraz słownie.
3. Cena ma zawierać wszystkie koszty przedmiotu zamówienia.

VIII. Kryteria oceny ofert.

1. Zamawiający będzie się kierował następującym kryterium oceny ofert:
   CENA OFERTY – 100 %
2. Jeżeli w postępowaniu nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Wykonawcy składając oferty dodatkowe nie mogą zaoferować cen wyższych, niż zaoferowane w złożonych ofertach.
3. Jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający

w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.

IX. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia.

1. O wyborze oferty Zamawiający zawiadomi niezwłocznie Wykonawców, którzy złożyli oferty.
2. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza, przed podpisaniem umowy poda Zamawiającemu w wyznaczonym terminie, informacje niezbędne do podpisania umowy, w szczególności wykaz członków zespołu audytowego (załącznik nr 1 do Umowy), o którym mowa w pkt III.1 pkt 3 IWUZ oraz certyfikaty, do wglądu, o których mowa w tym samym punkcie.
3. Zamawiający zawrze umowę niezwłocznie po przekazaniu zawiadomienia o wyborze oferty.
4. Jeżeli Wykonawca, którego oferta została wybrana, uchyli się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.
5. Zamawiający przekazuje wzór umowy (załącznik nr 5 do IWUZ) zawierającej warunki wykonania zamówienia. Zamawiający będzie żądał, aby umowa została zawarta i zrealizowana na warunkach w nim określonych.

X. Klauzula informacyjna.

Zgodnie z art. 13 ust. 1 i ust. 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 (zwanym dalej RODO) informujemy, iż:

1) Administratorem Pani/Pana danych osobowych jest Zarząd Transportu Metropolitalnego, z siedzibą przy ul. Barbary 21A, 40-053 Katowice, adres email: kancelaria@metropoliaztm.pl, strona internetowa: bip.metropoliaztm.pl;
2) Została wyznaczona osoba do kontaktu w sprawie przetwarzania danych osobowych, adres email: iod@metropoliaztm.pl;
3) Pani/Pana dane osobowe będą przetwarzane w następujących celach:
   a) oceny złożonych ofert i wyboru najkorzystniejszej,
   b) archiwizacja dokumentacji.

   Podstawą prawną przetwarzania danych osobowych jest:
   a) niezbędność przetwarzania do zrealizowania zadania w interesie publicznym (art. 6 ust. 1 lit. e rozporządzenia) wynikająca z art. 44 i art. 47 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
   b) obowiązek prawny administratora wynikający z art. 6 ustawy o narodowym zasobie archiwalnym i archiwach (art. 6 ust. 1 lit. c RODO).
4) Pani/Pana dane osobowe będą ujawniane osobom upoważnionym przez administratora danych osobowych oraz podmiotom upoważnionym na podstawie przepisów prawa, operatorowi pocztowemu lub kurierowi w zakresie korespondencji papierowej, podmiotom świadczącym usługi informatyczne ZTM. Ponadto w zakresie stanowiącym informację publiczną dane będą ujawniane każdemu zainteresowanemu taką informacją lub publikowane na portalu BIP;
5) Pani/Pana dane osobowe będą przechowywane przez okres wynikający z przepisów prawa dot. archiwizacji lub do wyrażenia skutecznego sprzeciwu wobec przetwarzania.
6) Przysługuje Pani/Panu prawo dostępu do treści swoich danych oraz prawo żądania ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wyrażenia sprzeciwu wobec przetwarzania, prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;

7) Podanie przez Panią/Pana danych osobowych jest obowiązkowe a konsekwencją niepodania danych osobowych będzie nieuwzględnienie oferty.
8) Pani/Pana dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji ani profilowania, o którym mowa w art. 22 RODO.

XI. Postanowienia końcowe.

1. W prowadzonym postępowaniu nie przysługują środki ochrony prawnej określone w przepisach ustawy Prawo zamówień publicznych.
2. Postępowanie prowadzone jest na podstawie wewnętrznych uregulowań organizacyjnych, bez zastosowania przepisów ustawy Prawo zamówień publicznych.
3. Zamawiający zastrzega możliwość unieważnienia postępowania bez podania uzasadnienia.

Zatwierdzam
Zastępca Dyrektora ZTM
01.09.2020 r. ds. Administracyjnych
(-) Krzysztof Dzierwa
……..
(data, podpis)

Załączniki:

1. Formularz cenowo – ofertowy
2. Wzór oświadczenia dot. wykonania innych audytów
3. Wzór oświadczenia dot. audytorów wiodących
4. Wzór oświadczenia dot. audytorów
5. Wzór umowy

Załącznik nr 1 do IWUZ

……

Wykonawca

FORMULARZ CENOWO – OFERTOWY.

1. Oferujemy realizację przedmiotu zamówienia zgodnie z Istotnymi Warunkami Udzielenia Zamówienia (IWUZ) na **przeprowadzenie audytu bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowyc**h (*nr postępowania:* ZP/IOD/1/2020.), **za cenę:**

   netto: ……... złotych (słownie: ……..

   ……..),

   brutto: ……..…… złotych (słownie: ……..……

   ……..),

   w tym stawka należnego podatku VAT …..%.

2. Przedmiot zamówienia wykonamy po podpisaniu umowy, w terminie określonym w umowie.
3. Oświadczamy, iż uważamy się za związanych niniejszą ofertą w okresie zawartym w IWUZ.
4. Oświadczamy, że zapoznaliśmy się z postanowieniami zawartymi we wzorze umowy i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.
5. Na czas prowadzonego postępowania podajemy:
   a) adres do korespondencji: ……
   b) e-mail do korespondencji: ……..

…….. ……

miejscowość, data czytelny podpis lub podpis i pieczęć imienna

Załącznik nr 2 do IWUZ

……

Wykonawca

Oświadczenie dotyczące wykonania innych audytów

Oświadczamy, że w okresie ostatnich dwóch lat przed upływem terminu składania ofert należycie wykonaliśmy przynajmniej 3 audyty bezpieczeństwa informacji lub audyt ochrony danych osobowych w oparciu o normę ISO 27001.

…….. ……

miejscowość, data czytelny podpis lub podpis i pieczęć imienna

Załącznik nr 3 do IWUZ

……

Wykonawca

Oświadczenie dotyczące audytorów wiodących.

Oświadczamy, że dysponujemy osobami zdolnymi do wykonania zamówienia, tj.:

a) co najmniej dwoma audytorami wiodącymi, posiadającymi ważny certyfikat audytora wiodącego w zakresie PN-ISO/IEC 27001 i przynajmniej trzyletnie doświadczenie audytowe jako audytor wiodący w ramach przedmiotowej normy,
b) co najmniej dwoma audytorami, posiadającymi ważny certyfikat audytora w zakresie ISO/IEC 27701 i przynajmniej trzyletnie doświadczenie audytowe w zakresie audytów systemu zarządzania bezpieczeństwem informacji,
c) co najmniej dwoma audytorami wiodącymi, posiadającymi ważny certyfikat audytora wiodącego w zakresie PN-ISO/IEC 22301 i przynajmniej trzyletnie doświadczenie audytowe w ramach przedmiotowej normy,
d) co najmniej dwoma audytorami wiodącymi, posiadającymi ważny certyfikat audytora wiodącego w zakresie PN-ISO/IEC 20000 i przynajmniej trzyletnie doświadczenie audytowe w ramach przedmiotowej normy,

…….. ……

miejscowość, data czytelny podpis lub podpis i pieczęć imienna

Załącznik nr 4 do IWUZ

……

Wykonawca

Oświadczenie dotyczące audytorów.

Oświadczamy, że dysponujemy co najmniej czteroma audytorami bezpieczeństwa informacji z przynajmniej 2 letnim stażem audytowym w zakresie audytów systemów zarządzania bezpieczeństwem informacji.

……..
miejscowość, data

……
czytelny podpis lub
podpis i pieczęć imienna