

Książ Wielkopolski, 02.06.2023 r.

O.042.2.3.2022

ZAPYTANIE OFERTOWE

Realizacja usług związanych ze zwiększeniem bezpieczeństwa informacji w urzędzie oraz diagnozy cyberbezpieczeństwa zgodnie z wytycznymi

Konkursu Grantowego Cyfrowa Gmina

Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU
Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

1. Zamawiający:

Gmina Książ Wielkopolski
ul. Stacha Wichury 11a
63-130 Książ Wielkopolski
NIP: 785-16-61-188

2. Tryb postępowania:

1. Postępowanie o udzielenie zamówienia publicznego jest wyłączone z obowiązku stosowania ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2022 poz. 1710 ze zm.) na podstawie art. 2 ust. 1 pkt 1.
2. Postępowanie o udzielenie zamówienia publicznego prowadzone jest zgodnie z Zarządzeniem Nr 19/2021 Burmistrza Książa Wlkp. z dnia 29 stycznia 2021 r. w *sprawie wprowadzenia regulaminu udzielania zamówień publicznych o wartości szacunkowej nieprzekraczającej kwoty 130 000 zł.*
3. Rodzaj zamówienia: **usługa.**

3. Opis przedmiotu zamówienia

1. Zamawiający zamierza zlecić realizację następujących usług z zakresu cyberbezpieczeństwa:

Etap I Diagnoza wstępna

- 1) Analiza stanu zgodności bezpieczeństwa informacji w gminie w zakresie wymaganym w Ustawie o Krajowym Systemie Cyberbezpieczeństwa i Rozporządzeniu w sprawie Krajowych Ram Interoperacyjności.
- 2) Zebranie wstępnych odpowiedzi i dowodów audytowych.
- 3) Wspólne zdefiniowanie rekomendowanych zmian w zakresie objętym Diagnozą.



Etap II Usługi wdrożeniowo szkoleniowe

- 4) Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w zakresie wymaganym obligatoryjną diagnozą cyberbezpieczeństwa.
- 5) Przeprowadzenie testów bezpieczeństwa za pomocą komercyjnych skanerów podatności (Nessus Professional oraz Burp Suite Professional lub równoważne*) z aktualną na dzień badania bazą podatności, w zakresie:
 - a) strony dostępnej pod adresem: www.ksiaz-wlkp.pl,
 - b) styku sieci urzędu z Internetem,
 - c) ocenę mechanizmów kryptograficznych wykorzystywanych w środowisku IT,
 - d) napisanie raportu z wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących wraz z załączeniem wyników wygenerowanych przez wykorzystane skanery.
- 6) Wykonanie testów phishingowych dla 27 pracowników urzędu wraz ze wskazaniem jakie akcje oraz jakie dane zostały przez pracowników wykonane lub podane na stronie wyłudzającej.
- 7) Udostępnienie szkoleń elearningowych na platformie Wykonawcy z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa obejmujących co najmniej następujące zagadnienia:
 - a) Podstawy bezpieczeństwa informacji.
 - b) Kontrola dostępu do zasobów informacyjnych.
 - c) Szyfrowanie informacji.
 - d) Cyberbezpieczeństwo.
 - e) Bezpieczeństwo pracy zdalnej.
 - f) Test zdobytej wiedzy.
- 8) Przygotowanie raportu z przeprowadzonych szkoleń oraz testów socjotechnicznych z informacjami o wynikach przeprowadzonych szkoleń oraz testów.

Etap III Diagnoza ostateczna wykonana przez certyfikowanego audytora

- 9) Wywiady audytowe oraz zebranie dowodów po przeprowadzeniu usług wdrożeniowo-szkoleniowych.
Wykonanie obligatoryjnej diagnozy cyberbezpieczeństwa zgodnie z wytycznymi (oraz załącznikiem nr 8 do Regulaminu Konkursu) Regulaminu Konkursu Grantowego Cyfrowa Gmina Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia -REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Program Operacyjny Polska Cyfrowa na lata 2014-2020.

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

*przez skanery równoważne Zamawiający rozumie oprogramowanie dostępne komercyjnie o funkcjonalności nie gorszej od posiadanej przez Nessus Professional oraz Burp Suite Professional.

4. Termin wykonania zamówienia:

60 dni od dnia podpisania umowy.

5. Warunki udziału

W ofercie Wykonawca powinien wskazać zespół oddelegowany do realizacji prac uwzględniając fakt, że Diagnoza Cyberbezpieczeństwa musi zostać przeprowadzona przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:

- 1) Certified Internal Auditor (CIA)
- 2) Certified Information System Auditor (CISA)
- 3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób
- 4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób
- 5) Certified Information Security Manager (CISM)
- 6) Certified in Risk and Information Systems Control (CRISC)
- 7) Certified in the Governance of Enterprise IT (CGEIT)
- 8) Certified Information Systems Security Professional (CISSP)
- 9) Systems Security Certified Practitioner (SSCP)
- 10) Certified Reliability Professional
- 11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert Do oferty należy dołączyć certyfikat(y) osoby (osób) wykonując(ej)/ych) Diagnostę.

Wybrany w postępowaniu Wykonawca zobowiązany jest w terminie do 3 dni od otrzymania informacji o wyborze dostarczyć dane osoby, która będzie wykonywała diagnozę wraz z dokumentem potwierdzającym posiadanie przez niego/nią certyfikatu

uprawnającego do przeprowadzeniu audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. W przypadku niedostarczenia dokumentu w wymaganym terminie oferta zostanie odrzucona.

6. Miejsce i termin składania ofert

Ofertę należy złożyć do 14.06.2023 r. do godziny 10:00 za pomocą poczty elektronicznej na adres e-mail: dawid.wawrzynowicz@ksiaz-wlkp.pl

Oferty niekompletne i złożone po terminie nie będą rozpatrywane.

7. Ocena ofert

Zamawiający dokona wyboru oferty wśród ofert ważnych niepodlegających odrzuceniu w oparciu o kryterium ceny – 100%.

8. Informacja o wyborze oferty

Informacja o wyborze oferty zostanie podana w Biuletynie Informacji Publicznej Zamawiającego. Wybrany Wykonawca zostanie powiadomiony w formie elektronicznej.

9. Informacje dodatkowe

1. W przypadku gdy Wykonawca, którego oferta została wybrana, uchyla się od wykonania przedmiotu zamówienia określonego w ofercie Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzenia ich ponownego badania i oceny.
2. Zamawiający zastrzega sobie prawo do odstąpienia lub unieważnienia niniejszego na każdym jego etapie, bez podania przyczyny, bez wyboru którejkolwiek ze złożonych ofert bądź prawo do ograniczenia przedmiotu zamówienia.

10. Ochrona danych osobowych w ramach zamówienia bez stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

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 danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO”) informujemy, że:

- 1) administratorem Pani/Pana danych osobowych jest Burmistrz Książa Wielkopolskiego,
- 2) administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: inspektor@rodo-krp.pl, tel. +48 792 304 042,
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie zapytania ofertowego,
- 4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy Pzp,



- 5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 Pzp przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia,
- 6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisanych ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego,
- 7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO,
- 8) posiada Pani/Pan:
 - a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia),
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (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),
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (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),
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
- 9) nie przysługuje Pani/Panu:
 - a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
 - c) 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.



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

11. Załączniki:

1. Formularz oferty.
2. Projekt umowy.