Mietków, dnia 29 czerwca 2023 r.

Znak sprawy: Rp.271.4.2023

ZAPYTANIE OFERTOWE

na realizację zamówienia o wartości szacunkowej poniżej równowartości 130 000 zł

Zamawiający:
Gmina Mietków
ul. Kolejowa 35, 55-081 Mietków, NIP 913-10-25-850

Zaprasza uprawnione podmioty do złożenia oferty cenowej na realizację zadania:

Przeprowadzenie diagnozy i audytu cyberbezpieczeństwa w Urzędzie Gminy Mietków zgodnie z zakresem określonym w formularzy stanowiącym załącznik nr 8 dostępnym na stronach Centrum Projektów Polska Cyfrowa *https://www.gov.pl/web/cppc/cyfrowa-gmina* oraz w ramach Osi Priorytetowej V Rozwój cyfrowej JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU Działania 5.1 Rozwój cyfrowej JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

1. Opis przedmiotu Zamówienia stanowi *załącznik nr 1* do niniejszego zapytania ofertowego.

2. O udzielenie niniejszego zamówienia mogę się ubiegać Wykonawcy nie podlegający wykluczeniu, którzy spełniają następujące warunki udziału w postepowaniu, dotyczące **zdolności technicznej lub zawodowej:**

a) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizowali (realizacja się zakończyła):
   - co najmniej dwa zamówienia, których przedmiotem było wykonanie audytu cyberbezpieczeństwa, zgodnego z Ustawą z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* oraz Rozporządzeniem 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 dla systemów teleinformatycznych*, obejmującego każdorazowo co najmniej: audyt organizacyjny, audyt fizyczny i środowiskowy oraz audyt teleinformatyczny,
   - co najmniej dwa zamówienia, których przedmiotem było przeprowadzenie diagnozy cyberbezpieczeństwa, zgodnie z zakresem określonym w formularzu stanowiącym załącznik nr 8 do dokumentacji 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,

b) dysponują lub będą dysponować osobami zdolnymi do wykonania zamówienia, które będą uczestniczyć w jego realizacji, tj. **co najmniej 2 audytorami z których każdy:**
   - posiada wykształcenie wyższe,
   - posiada certyfikat audytora wiodącego ISO/IEC 27001 w wersji 2007 lub nowszej lub inny certyfikat wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
   - ma co najmniej trzyletnie doświadczenie w prowadzeniu audytów bezpieczeństwa informacji zgodnie z wymaganiami zawartymi w Krajowych Ramach Interoperacyjności, polegające na przygotowywaniu planu audytów, przeprowadzaniu ich oraz sporządzaniu raportów z audytów (wymagane jest doświadczenie we wszystkich tych czynnościach), poświadczone udziałem w przynajmniej dwóch audytach,
   - brała udział jako audytor wiodący w przynajmniej trzech audytach bezpieczeństwa informacji zgodnie z wymaganiami zawartymi w Krajowych Ramach Interoperacyjności.

3. W postępowaniu mogą brać udział Wykonawcy, którzy:
1) Posiadają uprawnienia w zakresie prowadzenia działalności związanej z realizacją przedmiotu zamówienia, w szczególności Wykonawca powinien posiadać uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
2) Posiadają niezbędne zasoby do wykonywania Zamówienia.
Oferty Wykonawców nie spełniających ww. warunków nie będą rozpatrywane.
Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Wykonawcę dokumentów, wykazów, danych i informacji.
4. Termin realizacji Zamówienia: **do 14 dni od dnia podpisania umowy**
5. Miejsce realizacji Zamówienia: **Urząd Gminy Mietków ul. Kolejowa 35 – Zamawiający nie dopuszcza możliwości wykonania diagnozy zdalnie.**
6. Zamawiający zobowiązuje się udostępnić Wykonawcy wszelkie dostępne informacje i dane niezbędne do realizacji Zamówienia.
7. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

a) **cena brutto – 60%**
Punktacja zostanie obliczona zgodnie z poniższym wzorem:

$$\frac{\text{Cena najtańszej z ofert nie podlegającej odrzuceniu}}{\text{Cena badanej oferty}} \times 60 \text{ pkt.}$$

Wynik zostanie zaokrąglony do dwóch miejsc po przecinku zgodnie z regułami matematycznymi.

b) **doświadczenie zespołu Wykonawcy – 40%**
Jeśli co najmniej jeden z audytorów (członków zespołu Wykonawcy) realizujących zamówienie wykaże się doświadczeniem w przeprowadzaniu diagnoz cyberbezpieczeństwa, zgodnie z zakresem określonym w formularzu stanowiącym załącznik nr 8 do dokumentacji 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*, punkty zostaną przyznane następująco:
1 diagnoza – 10 pkt.
2 diagnozy – 20 pkt.
3 diagnozy – 30 pkt.
4 diagnozy – 40 pkt.
Doświadczenia audytorów (członków zespołu Wykonawcy) nie sumują się. Uznane zostanie doświadczenie tylko jednego z audytorów. Niepodanie w ofercie liczby diagnoz wykonanych przez audytora będzie równoznaczne z wpisaniem liczy 0 (zero) i punkty nie zostaną przyznane. Podanie liczby większej, niż 4 diagnozy spowoduje przyznanie maksymalnej liczby punktów w tym kryterium, tj. 40 pkt.

Punkty uzyskane w obu kryteriach zostaną zsumowane. Wybrana zostanie oferta z największą liczbą punktów spośród ofert nieodrzuconych.
8. Podana w ofercie cena będzie ceną obejmującą wszystkie koszty wykonania pełnego zakresu Zamówienia wynikającej z opisu przedmiotu Zamówienia.
9. Ofertę należy sporządzić w języku polskim, czytelnie.
10. Wartość cenową należy podać w złotych polskich – cyfrą (z dokładnością do dwóch miejsc po przecinku) oraz słownie.
11. Oferta Wykonawcy powinna zawierać następujące dokumenty:
a. formularz oferty wg załączonego wzoru – *załącznik nr 2*
b. dokumenty potwierdzające posiadane kwalifikacje (certyfikaty)
c. zaparafowany wzór umowy
12. Cena podana przez Wykonawcę jest obowiązująca przez okres związania ofertą (30 dni – bieg terminu związania ofertą rozpoczyna się wraz z terminem składania ofert) i nie będzie podlegała waloryzacji w okresie jej trwania.
13. Termin składania ofert:
Oferta powinna być przesłana na adres mailowy: urzad@mietkow.pl

W temacie wiadomości należy zawrzeć: **Oferta na przeprowadzenie diagnozy i audytu cyberbezpieczeństwa – Gmina Mietków**
Termin składania ofert upływa w dniu 6 lipca 2023 r. godz. 10:00.
14. Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania bez podawania uzasadnienia, a także do pozostawienia postępowania bez wyboru oferty. Zamawiający nie przewiduje zwrotu kosztów postępowania. Zamawiający wymaga, aby Wykonawca składając ofertę uwzględnił wszystkie pozycje określone w zapytaniu ofertowym.

15. Jeśli w niniejszym postępowaniu nie będzie można dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie zamawiający zastrzega sobie możliwość wezwanie do złożenia oferty dodatkowej.
16. Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający zawiadomi wszystkich Wykonawców, którzy ubiegali się o udzielenie zamówienia. Zamawiający dopuszcza możliwość kontaktowania się z wykonawcami w formie elektronicznej.
17. Zamawiający zawrze pisemną umowę z wybranym Wykonawcą po przekazaniu zawiadomienia o wyborze Wykonawcy.
18. Przesłanie zawiadomienia o wyborze oferty nie stanowi zawarcia umowy.
19. Jeżeli Wykonawca, którego oferta została wybrana uchyli się od zawarcia umowy, Zamawiający wybierze kolejną ofertę – najkorzystniejszą spośród złożonych ofert, bez przeprowadzenia ich ponownej oceny.
20. Wykonawca pozostaje związany złożoną ofertą przez 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
21. W niniejszym postępowaniu nie mają zastosowania przepisy Ustawy Prawo Zamówień Publicznych
22. Zamawiający, w przypadku jeśli kwota oferty przekroczy środki Zamawiającego przeznaczone w budżecie, zastrzega sobie prawo do złożenia Zamówienia jedynie do wysokości przeznaczonych środków.
23. Osobami uprawnionymi do kontaktów z Wykonawcami są: Anna Stasiak, e-mail: anna.stasiak@mietkow.pl Grzegorz Guzik, e-mail: informatyk@mietkow.pl

WÓJT
Adam Kozarowicz

Załączniki stanowiące integralną część zapytania ofertowego:
Załącznik nr 1 – opis przedmiotu zamówienia
Załącznik nr 2 - Wzór formularza oferty
Załącznik nr 3 – Wzór umowy

Załącznik nr 1 Opis przedmiotu Zamówienia

Przedmiot zamówienia

Zamówienie jest realizowane w ramach grantu w projekcie „Cyfrowa Gmina" współfinansowanym przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach, Programu Operacyjnego Polska Cyfrowa (POPC) na lata 2014 – 2020, oś priorytetowa V *Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU*, działanie 5.1 *Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia*, w rozumieniu art. 35 ustawy z dnia 11 lipca 2014 r. *o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020* (tekst jednolity Dz. U. z 2020 r. poz. 818), zwanej dalej Ustawą Wdrożeniową, na podstawie ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (tekst jednolity Dz.U. z 2023 r. poz. 913) oraz zawarcia w dniu 01.02.2022 r. umowy o powierzenie grantu o numerze 3482/1/2021 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 osi priorytetowej V *Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU,* działanie 5.1 *Rozwój cyfrowy JT oraz wzmocnienie cyfrowej odporności na zagrożenia*, dotycząca realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.0 1.00-00-0001/21-00, zwanej dalej Umową Grantową.

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia diagnozy i audytu cyberbezpieczeństwa w Urzędzie Gminy Mietków zgodnie z zakresem określonym w formularzu stanowiącym załącznik nr 8 do dokumentacji 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. W ramach diagnozy ma zostać dokonana ocena istnienia i funkcjonowania oraz zgodności funkcjonujących w urzędzie i jednostkach podległych zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym przetwarzania danych osobowych, z obowiązującymi aktami prawnymi. W diagnoza musi obejmować odpowiedzi na pytania zawarte w formularzu stanowiącym załącznik do niniejszego zapytania ofertowego (plik: Diagnoza_cyberbezpieczenstwa.xlsx) i formularz musi zostać wypełniony. Formularz zostanie następnie przekazany przez Zamawiającego do NASK, zgodnie z wymaganiami grantu w projekcie „Cyfrowa Gmina". Ponadto, na potrzeby Zamawiającego musi zostać opracowany raport zawierający wnioski i rekomendacje w zakresie poprawy cyberbezpieczeństwa w urzędzie.

Następnie, po dokonaniu zakupów oraz instalacji i wdrożeniu sprzętu w ramach grantu Wykonawca jest zobowiązany do przeprowadzenia kompleksowego audytu cyberbezpieczeństwa (bezpieczeństwa informacji) w zakresie ustawowych obszarów działalności Urzędu (w tym w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów elektronicznych, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy systemów poczty elektronicznej, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w Urzędzie) oraz opracowania dokumentacji poaudytowej – raportu z wytycznymi do dalszego doskonalenia i rekomendacjami na przyszłość. Celem audytu jest m.in. na sprawdzenie, czy zrealizowane zostały zalecenia z diagnozy cyberbezpieczeństwa.

Zakres audytu

1. Audyt organizacyjny

1. Weryfikacja regulacji wewnętrznych Zamawiającego w obszarze zarządzania bezpieczeństwem informacji oraz procedur ich audytów i aktualizacji, w tym:
   a) zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji, nieuprawnionego dostępu, uszkodzeń lub zakłóceń i kradzieży środków przetwarzania informacji, w tym urządzeń mobilnych,
   b) zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,

c) zasad zgłaszania incydentów naruszenia bezpieczeństwa informacji i postępowania z tymi zgłoszeniami,
d) zasad działania w przypadku publikacji informacji o podatności technicznych systemów teleinformatycznych lub dostrzeżenia nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
e) zasad dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,

2. Weryfikacja zakresów odpowiedzialności, nadanych uprawnień i adekwatnego przeszkolenia pracowników w zakresie bezpieczeństwa informacji oraz koordynacja prac związanych z zarządzaniem bezpieczeństwem informacji (w tym danych osobowych) i nadawaniem uprawnień do przetwarzania informacji,
3. Weryfikacja procedur zmiany uprawnień, w przypadku zmiany zadań pracowników, o których mowa powyżej,
4. Analiza dokumentacji dotyczącej bezpieczeństwa informacji (w tym ochrony danych osobowych) w zakresie zapisów w umowach wykonawczych i serwisowych zawieranych ze stronami trzecimi,
5. Weryfikacja aktualności spisu sprzętu i oprogramowania służącego do przetwarzania informacji oraz procedury jej aktualizacji,
6. Analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz procedur minimalizujących to ryzyko, wraz z określeniem sposobu aktualizacji tej analizy.

2. Audyt fizyczny i środowiskowy

1. Weryfikacja granic obszaru bezpiecznego,
2. Weryfikacja zabezpieczeń wejścia/wyjścia,
3. Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
4. Weryfikacja zabezpieczenia informacji przed jej nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem (w tym bezpieczeństwa sieci wewnętrznej, komputerów i urządzeń mobilnych),
5. Weryfikacja zabezpieczenia informacji przed jej utratą (w tym systemów podtrzymania zasilania, chłodzenia i systemów alarmowych).

3. Audyt teleinformatyczny

1. Weryfikacja istniejących procedur zarządzania systemami teleinformatycznymi,
2. Przegląd zasobów informatycznych oraz stosowanych rozwiązań pod kątem utrzymania ciągłości działania,
   a) minimalizowaniu ryzyka utraty informacji w wyniku awarii (w tym weryfikacja procedur zarządzania kopiami zapasowymi),
   b) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   c) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
   d) zapewnieniu bezpieczeństwa plików systemowych,
   e) Weryfikacja ochrony przed oprogramowaniem szkodliwym;
3. Analiza i ocena mechanizmów zarządzania aktualizacjami oprogramowania,
4. Weryfikacja zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
5. Weryfikacja haseł (ich stosowanie, przyjęta polityka ich tworzenia oraz zmiany, mechanizmy ich przechowywania).

Wymagania ogólne

1. Diagnoza i audyt cyberbezpieczeństwa muszą zostać przeprowadzone zgodnie z Ustawą z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (t.j. Dz.U. z 2023 r. poz. 913) oraz Rozporządzeniem 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 dla systemów teleinformatycznych* (tj. Dz. U. 2017 poz. 2247) zwane dalej **Rozporządzeniem KRI**
2. Diagnoza i audyt cyberbezpieczeństwa muszą zostać przeprowadzone przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999).
   Wykaz certyfikatów wskazanych w tym rozporządzeniu:
   a) Certified Internal Auditor (CIA);
   b) Certified Information System Auditor (CISA);
   c) 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;
   d) 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;
   e) Certified Information Security Manager (CISM)
   f) Certified in Risk and Information Systems Control (CRISC);
   g) Certified in the Governance of Enterprise IT (CGEIT);
   h) Certified Information Systems Security Professional (CISSP);
   i) Systems Security Certified Practitioner (SSCP);
   j) Certified Reliability Professional;
   k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

3. Diagnoza i audyt cyberbezpieczeństwa mają zostać przeprowadzone w siedzibie Urzędu, gdzie znajdują się pomieszczenia biurowe i serwerownia.
4. W Urzędzie zatrudnionych jest 20 osób.
5. Struktura Urzędu:

   a) kierownictwo:
      - Wójt,
      - Zastępca Wójta
      - Sekretarz Gminy,
      - Skarbnik Gminy;

   b) samodzielne stanowiska pracy (stanowiska urzędnicze):
      - Stanowisko ds. organizacyjnych,
      - Stanowisko ds. obronnych,
      - Stanowisko ds. obsługi Rady Gminy,
      - Stanowisko ds. ewidencji ludności i dowodów osobistych,
      - Stanowisko ds. budownictwa,
      - Stanowisko ds. gospodarki komunalnej,
      - Stanowisko ds. gospodarki gruntami,
      - Stanowisko ds. gospodarowania odpadami,
      - Stanowisko ds. ochrony środowiska,
      - Stanowisko ds. płac,
      - Stanowisko ds. księgowości budżetowej,
      - Stanowisko ds. księgowości budżetowej i podatku vat,
      - Stanowisko ds. podatków i opłat,

- Stanowisko ds. wymiaru,
- Stanowisko ds. opłat za gospodarowanie odpadami,
- Radca prawny

6. Audytowi podlega całość sprzętu informatycznego będącego w posiadaniu Zamawiającego (w tym sprzęt nabywany w ramach grantu):
   a) serwery fizyczne – 1 szt.,
   b) komputery stacjonarne – 18 szt.,
   c) notebooki – 7 szt.,
   d) drukarki sieciowe – 7 szt.,
   e) urządzenie UTM – 1 szt.,
   f) macierze dyskowe – 1 szt.,
   g) dyski sieciowe NAS – 2 szt.
7. Audyt obejmuje 1 sieć lokalną i 2 sieci wirtualne VLAN.
8. Urząd posiada dwa łącze do sieci Internet.
9. W Urzędzie funkcjonuje usługa Active Directory.
10. Diagnoza cyberbezpieczeństwa musi zostać wykonana **w ciągu 14 dni od daty udzielenia zamówienia**.
11. Audyt cyberbezpieczeństwa musi zostać wykonany po dokonaniu zakupów oraz instalacji sprzętu i wdrożeniu oprogramowania w ramach grantu, jednakże **nie później niż do 15 września 2023 r.**

Załącznik nr 2 – Formularz ofertowy

miejscowość, data .....

(pieczęć firmy)

FORMULARZ OFERTOWY

Dane Zamawiającego:
Gmina Mietków
ul. Kolejowa 35, 55-081 Mietków,
NIP 913-10-25-850

Dane wykonawcy

.....

.....

Siedziba: .....

.....

Adres poczty elektronicznej: .....
Strona internetowa: .....
Numer telefonu: 0 (**) .....
Numer faksu: 0 (**) .....
Numer REGON: .....
Numer NIP: ....

Nawiązując do zapytania ofertowego oferujemy wykonanie zamówienia, zgodnie z opisem w zapytaniu, za cenę:

1. Diagnoza cyberbezpieczeństwa: .....,..... PLN netto;.....,..... PLN brutto (kwota słownie: .....

2. Audyt cyberbezpieczeństwa: .....,..... PLN netto;.....,..... PLN brutto (kwota słownie: .....

Osobą/osobami do kontaktów z Zamawiającym jest/są:

.....

tel. kontaktowy .....

1. Oświadczamy, że w realizacji zamówienia weźmie udział audytor, który posiada doświadczenie w przeprowadzeniu ..... (podać liczbę: 0 – 4) diagnoz cyberbezpieczeństwa, zgodnie z zakresem określonym w formularzu stanowiącym załącznik nr 8 do dokumentacji 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.*
2. Oświadczamy, że zapoznaliśmy się z zakresem przedmiotu za zapytania ofertowego, nie wnosimy żadnych zastrzeżeń oraz uzyskaliśmy informacje niezbędne do przygotowania oferty.
3. Oświadczamy, że akceptujemy projekt umowy, stanowiący załącznik do Zapytania ofertowego.
4. Oświadczamy, że uważamy się za związanych z ofertą przez okres 30 dni.

5. Oświadczamy, że posiadamy wymagane uprawnienia do przeprowadzenia diagnozy cyberbezpieczeństwa zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu
6. Oświadczamy, że załączone do zapytania ofertowego wymagania stawiane wykonawcy zostały przez nas zaakceptowane bez zastrzeżeń i zobowiązujemy się, w przypadku wyboru naszej oferty, do wykonania usługi w miejscu i terminie wyznaczonym przez Zamawiającego.
7. Oświadczamy, że zapoznaliśmy się z informacjami o przetwarzaniu danych osobowych.

.....

Czytelne podpisy osób uprawnionych do reprezentowania wykonawcy

Klauzula informacyjna przetwarzania danych

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:

1. Administratorem Pani/Pana danych osobowych jest Wójt Gminy Mietków, ul. Kolejowa 35, 55-081 Mietków.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się skontaktować pod adresem e-mail: iod@mietkow.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b, c RODO w celu przeprowadzanie postępowania, na wykonanie zadania określonego w zapytaniu ofertowym, o wartości szacunkowej poniżej równowartości 130 000 zł, pod nazwą: ***Przeprowadzenie diagnozy i audytu cyberbezpieczeństwa Urzędu Gminy Mietków w ramach projektu „Cyfrowa Gmina"*** oraz - w przypadku wybranej oferty – w celu realizacji przedmiotu umowy.
4. Podanie danych osobowych jest dobrowolne, a ewentualne konsekwencje niepodania danych to nierozpatrzenie oferty w ww. postępowaniu.
5. Dane osobowe nie będą udostępniane podmiotom zewnętrznym, z wyjątkiem przypadków przewidzianych przepisami prawa.
6. Dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.
7. Dane osobowe będą przetwarzane na podstawie przepisów prawa, przez okres niezbędny do realizacji wyżej określonych celów przetwarzania, lecz nie krócej niż okres wskazany w przepisach o archiwizacji.
8. Posiada Pani/Pan prawo dostępu do danych osobowych Pani/Pana dotyczących; prawo do sprostowania danych osobowych; prawo do przenoszenia danych osobowych, prawo żądania od administratora ograniczenia przetwarzania danych osobowych; 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. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, a dane nie będą poddawane profilowaniu.