Chodzież dn. 20.05.2022 r.

Znak: SG.271.1.2022

ZAPYTANIE OFERTOWE

Wójt Gminy Chodzież zaprasza do składania ofert na wykonanie zadania pn.:

Przeprowadzenie diagnozy cyberbezpieczeństwa w projekcie Cyfrowa Gmina w ramach Działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia" dotyczącego realizacji projektu grantowego „Cyfrowa Gmina" o numerze POPC.05.01.00-00- 0001/21-00

I. Zamawiający:

Gmina Chodzież
ul. Notecka 28
64-800 Chodzież
NIP: 6070016311
Tel.: +48 67 2821608
E-mail: sekretariat@gminachodziez.pl

II. 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. 2021 poz. 1129 z późn. zm.) na podstawie art. 2 ust. 1 pkt 1).

III. Opis przedmiotu zamówienia:

1. Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" w Urzędzie Gminy Chodzież zgodnie z zakresem oraz formularzem stanowiącym obowiązujący na dzień wykonywania audytu załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina zakończonego raportem, opublikowanego na stronie Centrum Projektów Polska Cyfrowa pod adresem https://www.gov.pl/web/cppc/cyfrowa-gmina.
2. Zamawiający dopuszcza wykonania diagnozy cyberbezpieczeństwa w sposób zdalny. Badanie zabezpieczeń, w tym przeprowadzenie wszelakich testów penetracyjnych sieci LAN, diagnozy cyberbezpieczeństwa, podatności systemów, Wykonawca może wykonać zdalnie.
   Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 6 do zapytania ofertowego.
3. Po przeprowadzeniu diagnozy, Wykonawca zobligowany jest do przekazania wypełnionego i podpisanego elektronicznie formularza diagnozy (przeprowadzonej przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) Zamawiającemu.
4. Zamawiający informuje, iż zamówienie jest finansowane w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności za zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina".

IV. Warunki udziału Wykonawcy w postępowaniu:

1. Diagnoza cyberbezpieczeństwa musi zostać przeprowadzona przez osobę posiadająca 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 ww. 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 Govemance 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.
2. Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
3. Wykonawca złoży w tym zakresie oświadczenie stanowiące **załączniki nr 2** do oferty.
4. Wykonawca posiada doświadczenie w wykonywaniu audytów wynikających z Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Wykonawca złoży w tym zakresie oświadczenie będące **załącznikiem nr 3** do oferty wraz z dokumentami potwierdzającymi przeprowadzenie minimum 1 diagnozy cyberbezpieczeństwa w ramach programu Cyfrowa Gmina lub zrealizował co najmniej 3 audyty bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie w ostatnich 3 latach przed złożeniem oferty.
   Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu z udziału w postępowaniu. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.
5. 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 certyfikatu uprawniającego 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 nie dostarczenia dokumentu w wymaganym terminie oferta zostanie odrzucona.

6. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).

V. Kryteria i sposób oceny oferty:

1. Przy wyborze oferty do realizacji Zamawiający będzie się kierował kryterium: Cena-100%.
2. Cenę za wykonanie zamówienia należy podać w formularzu oferty.
3. Cena winna obejmować wszelkie koszty niezbędne do zrealizowania zamówienia. Wykonawca sporządzając ofertę powinien przewidzieć wszelkie okoliczności mogące mieć wpływ na cenę.

VI. Termin i miejsce realizacji zamówienia:

Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie 30 dni od dnia zawarcia umowy i obejmuje badaniem siedzibę i systemy Urzędu Gminy Chodzież zlokalizowanego przy ul. Noteckiej 28; 64-800 Chodzież.

VII. Sposób przygotowania oferty:

1. Kompletny, wypełniony formularz ofertowy, podpisany przez osobę upoważnioną do reprezentacji Wykonawcy stanowiący **załącznik nr 1;**
2. Kompletne, wypełnione oświadczenie stanowiące **załącznik nr 2**;
3. Kompletne, wypełnione oświadczenie stanowiące **załącznik nr 3;**
4. Kompletne, wypełnione oświadczenie stanowiące **załącznik nr 4**;
5. Parafowany przez osobę upoważnioną do reprezentowania Wykonawcy wzór umowy stanowiący **załącznik nr 5;**
6. Dokumenty potwierdzające wymagane kwalifikacje do przeprowadzenia diagnozy cyberbezpieczeństwa;
7. Parafowany niewypełniony formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa;
8. Referencje potwierdzające prawidłowe wykonanie diagnozy cyberbezpieczeństwa lub audytu.
9. Podpisana klauzula informacyjna RODO. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

VIII. Miejsce i termin składania ofert:

1. Termin składania ofert **07.06.2022r. do godz. 10:00**
2. Ofertę cenową sporządzoną w języku polskim należy złożyć w siedzibie Zamawiającego lub przesłać na adres: Urząd Gminy Chodzież, ul. Notecka 28; 64-800 Chodzież w sekretariacie (I piętro),w zamkniętej kopercie z dopiskiem: **OFERTA: „Przeprowadzenie diagnozy cyberbezpieczeństwa w ramach projektu Cyfrowa Gmina" NIE OTWIERAĆ PRZED 07.06.2022 r. godz. 10:00.**
3. Oferty złożone po terminie bądź w inny sposób nie będą rozpatrywane.

IX. Termin związania ofertą:

1. Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.

X. Podstawy unieważnienia postępowania

1. Zamawiający unieważnia postępowanie, jeżeli:
   a) nie złożono żadnej oferty,
   b) wszystkie oferty podlegały odrzuceniu,
   c) cena lub koszt najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę jaką Zamawiający może przeznaczyć na sfinansowanie zamówienia, chyba, że Zamawiający może zwiększyć kwotę do wysokości ceny najkorzystniejszej lub kosztu najkorzystniejszej oferty,
   d) na podstawie innych przyczyn, istotnych dla Zamawiającego
   e) w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu publikacji niniejszego zapytania ofertowego.

XI. Postanowienia końcowe:

1. Zamawiający zastrzega sobie prawo odstąpienia, bądź unieważnienia zapytania ofertowego bez podania przyczyny w przypadku zaistnienia okoliczności nieznanych Zamawiającemu w dniu publikacji niniejszego zapytania ofertowego.
2. Zapytanie może zostać zmienione przed upływem terminu składania ofert przewidzianym w zapytaniu ofertowym. Zmiana zapytania oraz treść pytań wraz z wyjaśnieniami zostanie przesłana wszystkim zainteresowanym.

XII. Zasady Przetwarzania danych

1. Zasady przetwarzania danych osobowych w programie Polska Cyfrowa 2014-2020 (POPC 2014- 2020) Ze względu na to, że to Minister Funduszy i Polityki Regionalnej - jako Instytucja Zarządzająca POPC 2014-2020 - określa: jakie dane osobowe, w jaki sposób i w jakim celu będą przetwarzane w związku z realizacją Programu, pełni on rolę administratora danych osobowych przetwarzanych w związku z realizacją POPC 2014-2020 w rozumieniu RODO [Rozporządzenie 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) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1) Przy czym jest on administratorem zarówno wobec danych osobowych, które samodzielnie pozyskał, jak i wobec danych osobowych pozyskanych przez inne podmioty zaangażowane w realizację Programu (tj. przez innych administratorów, którzy w tym przypadku pełnią dodatkowo funkcję podmiotów przetwarzających dane osobowe [Podmiotami przetwarzającymi są: Instytucja Pośrednicząca POPC 2014-2020, beneficjenci oraz inne podmioty zaangażowane w realizację POPC 2014-2020, którym Minister (lub inny upoważniony podmiot) powierzył przetwarzanie danych osobowych w ramach POPC 2014-2020]).
   Minister Funduszy i Polityki Regionalnej jest także administratorem danych osobowych, które przetwarza jako beneficjent projektów współfinansowanych ze środków POPC 2014-2020. Minister Funduszy i Polityki Regionalnej jest również administratorem danych zgromadzonych w zarządzanym przez niego Centralnym Systemie Teleinformatycznym wspierającym realizację POPC 2014-2020.

2. Cel przetwarzania danych osobowych :
   Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe w celu realizacji zadań przypisanych Instytucji Zarządzającej POPC 2014-2020, w zakresie, w jakim jest to niezbędne dla realizacji tego celu. Minister Funduszy i Polityki Regionalnej przetwarza dane osobowe w szczególności w celach:
   1.udzielania wsparcia beneficjentom ubiegającym się o dofinansowanie i realizującym projekty,
   2. potwierdzania kwalifikowalności wydatków,
   3. wnioskowania o płatności do Komisji Europejskiej,
   4. raportowania o nieprawidłowościach,
   5. ewaluacji,
   6. monitoringu,
   7. kontroli,
   8. audytu,
   9. sprawozdawczości oraz
   10.działań informacyjno-promocyjnych.

3. Podstawy prawne przetwarzania Przetwarzanie danych osobowych w związku z realizacją POPC 2014-2020 odbywa się zgodnie z RODO. Podstawą prawną przetwarzania danych jest konieczność realizacji obowiązków spoczywających na Ministrze Funduszy i Polityki Regionalnej - jako na Instytucji Zarządzającej - na podstawie przepisów prawa europejskiego i krajowego (art. 6 ust. 1 lit. c RODO). Obowiązki te wynikają m.in. z przepisów ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 oraz przepisów prawa europejskiego:
   1) rozporządzenia Parlamentu Europejskiego i Rady nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego, oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego Rozporządzenie Rady (WE) nr 1083/2006,
   2) rozporządzenia wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi.
4. Podstawą przetwarzania danych osobowych przez Ministra są również:
   a. konieczność realizacji umowy, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b RODO) - podstawa ta ma zastosowanie m. in. do danych osobowych osób prowadzących samodzielną działalność gospodarczą, z którymi Minister zawarł umowy w celu realizacji POPC 2014-2020,
   b. wykonywanie zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Ministrowi (art. 6 ust. 1 lit e

RODO) - podstawa ta ma zastosowanie m. in. do organizowanych przez Ministra konkursów i akcji promocyjnych dotyczących Programu,

c. uzasadniony interes prawny Ministra Funduszy i Polityki Regionalnej (art. 6 ust. 1 lit f RODO) – podstawa ta ma zastosowanie m.in. do danych osobowych przetwarzanych w związku z realizacją umów w ramach Funduszy Europejskich. W ramach POPC 2014-2020 w działaniu 3.1 - Działania szkoleniowe na rzecz rozwoju kompetencji cyfrowych przetwarzane są dane szczególnej kategorii (dane o niepełnosprawności). Podstawą prawną ich przetwarzania jest wyraźna zgoda osoby, której dane dotyczą (art. 9 ust. 2 lit a RODO).

5. Rodzaje przetwarzanych danych Minister Funduszy i Polityki Regionalnej w celu realizacji POPC 2014-2020 przetwarza dane osobowe m. in.:
   1) pracowników, wolontariuszy, praktykantów i stażystów reprezentujących lub wykonujących zadania na rzecz podmiotów zaangażowanych w obsługę i realizację POPC 2014-2020,
   2) osób wskazanych do kontaktu, osób upoważnionych do podejmowania wiążących decyzji oraz innych osób wykonujących zadania na rzecz wnioskodawców, beneficjentów i partnerów,
   3) uczestników szkoleń, konkursów, konferencji, komitetów monitorujących, grup roboczych, grup sterujących oraz spotkań informacyjnych lub promocyjnych organizowanych w ramach POPC 2014-2020,
   4) kandydatów na ekspertów oraz ekspertów zaangażowanych w proces wyboru projektów do dofinansowania lub wykonujących zadania związane z realizacją praw i obowiązków właściwych instytucji, wynikających z zawartych umów o dofinansowanie projektów,
   5) osób, których dane będą przetwarzane w związku z badaniem kwalifikowalności środków w projekcie, w tym w szczególności: personelu projektu, uczestników komisji przetargowych, oferentów i wykonawców zamówień publicznych, osób świadczących usługi na podstawie umów cywilnoprawnych.

Wśród rodzajów danych osobowych przetwarzanych przez Ministra można wymienić:

1) dane identyfikacyjne, w szczególności: imię, nazwisko, miejsce zatrudnienia/formę prowadzenia działalności gospodarczej, stanowisko; w niektórych przypadkach także nr PESEL/NIP/REGON,
2) dane dotyczące stosunku pracy, w szczególności otrzymywane wynagrodzenie oraz wymiar czasu pracy,
3) dane kontaktowe, które obejmują w szczególności adres e-mail, nr telefonu, nr fax, adres do korespondencji,
4) dane o charakterze finansowym, w szczególności nr rachunku bankowego, kwotę przyznanych środków, informacje dotyczące nieruchomości (nr działki, nr księgi wieczystej, nr przyłącza gazowego), kwotę wynagrodzenia,
5) dane zbierane w celu realizacji obowiązków sprawozdawczych do których realizacji zobowiązane są państwa członkowskie, obejmujące w szczególności: płeć, wiek w chwili przystąpienia do projektu, wykształcenie, wykonywany zawód, narodowość, informacje o niepełnosprawności. Dane pozyskiwane są bezpośrednio od osób, których dane dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację programów operacyjnych, w szczególności wnioskodawców, beneficjentów i partnerów. W przypadku, gdy dane pozyskiwanie są bezpośrednio od osób, których dane dotyczą, podanie danych jest dobrowolne. Odmowa podania danych jest jednak równoznaczna z brakiem

możliwości podjęcia stosownych działań, np. ubiegania się o środki w ramach POPC 2014-2020.

6. Okres przechowywania danych Dane osobowe będą przechowywane przez okres wskazany w art. 140 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. oraz jednocześnie przez czas nie krótszy niż 10 lat od dnia przyznania ostatniej pomocy w ramach POPC 2014-2020 - z równoczesnym uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. W niektórych przypadkach, np. prowadzenia kontroli u Ministra przez organy Unii Europejskiej, okres ten może zostać wydłużony.
7. Odbiorcy danych Odbiorcami danych osobowych mogą być:
   a) podmioty, którym Instytucja Zarządzająca POPC 2014-2020 powierzyła wykonywanie zadań związanych z realizacją Programu, w tym w szczególności Instytucja Pośrednicząca POPC, a także eksperci, podmioty prowadzące audyty, kontrole, szkolenia i ewaluacje,
   b) instytucje, organy i agencje Unii Europejskiej (UE), a także inne podmioty, którym UE powierzyła wykonywanie zadań związanych z wdrażaniem POPC 2014-2020,
   c) podmioty świadczące na rzecz Ministra usługi związane z obsługą i rozwojem systemów teleinformatycznych oraz zapewnieniem łączności, w szczególności dostawcy rozwiązań IT i operatorzy telekomunikacyjni.
8. Prawa osoby, której dane dotyczą Osobom, których dane przetwarzane są w związku z realizacją POPC 2014-2020 przysługują następujące prawa:
   1) prawo dostępu do danych osobowych i ich sprostowania. Realizując te prawo, osoba której dane dotyczą może zwrócić się do Ministra z pytanie m.in. o to czy Minister przetwarza jej dane osobowe, jakie dane osobowe przetwarza i skąd je pozyskał, jaki jest cel przetwarzania i jego podstawa prawna oraz jak długo dane te będą przetwarzane. W przypadku, gdy przetwarzane dane okażą się nieaktualne, osoba, której dane dotyczą może zwrócić się do Ministra z wnioskiem o ich aktualizację;
   2) prawo usunięcia lub ograniczenia ich przetwarzania – jeżeli spełnione są przesłanki określone w art. 17 i 18 RODO. Żądanie usunięcia danych osobowych realizowane jest w szczególności gdy dalsze przetwarzanie danych nie jest już niezbędne do realizacji celu Ministra lub dane osobowe były przetwarzane niezgodnie z prawem. Szczegółowe warunki korzystania z tego prawa określa art. 17 RODO. Ograniczenie przetwarzania danych osobowych powoduje, że Minister może jedynie przechowywać dane osobowe. Minister nie może przekazywać tych danych innym podmiotom, modyfikować ich ani usuwać.
   3) Ograniczanie przetwarzania danych osobowych ma charakter czasowy i trwa do momentu dokonania przez Ministra oceny, czy dane osobowe są prawidłowe, przetwarzane zgodnie z prawem oraz niezbędne do realizacji celu przetwarzania.
   4) Ograniczenie przetwarzania danych osobowych następuje także w przypadku wniesienia sprzeciwu wobec przetwarzania danych – do czasu rozpatrzenia przez Ministra tego sprzeciwu;
   5) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
   6) prawo do cofnięcia zgody, w każdym momencie - w przypadku, gdy podstawą przetwarzania danych jest zgoda (art. 9 ust. 2 lit a RODO). Cofnięcie zgody nie spowoduje, że dotychczasowe przetwarzanie danych zostanie uznane za niezgodne z prawem;

7) prawo otrzymania danych osobowych w ustrukturyzowanym powszechnie używanym formacie, przenoszenia tych danych do innych administratorów lub żądania, o ile jest to technicznie możliwe, przesłania ich przez administratora innemu administratorowi - w przypadku, gdy podstawą przetwarzania danych jest zgoda lub realizacja umowy z osobą, której dane dotyczą (art. 6 ust. 1 lit b RODO);
8) prawo wniesienia sprzeciwu wobec przetwarzania danych osobowych - w przypadku, gdy podstawą przetwarzania danych jest realizacja zadań publicznych administratora lub jego prawnie uzasadnionych interesów (art. 6 ust. 1 lit e lub f RODO).
Wniesienie sprzeciwu powoduje zaprzestanie przetwarzania danych osobowych przez Ministra, chyba że wykaże on, istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

9. Zautomatyzowane podejmowanie decyzji - dane nie podlegają procesowi zautomatyzowanego podejmowania decyzji.

XIII. Załączniki:

1. Załącznik nr 1 – Formularz ofertowy;
2. Załącznik nr 2 – Oświadczenie o posiadaniu niezbędnego do wykonania zamówienia potencjału technicznego i osobowego;
3. Załącznik nr 3 – Oświadczenie o wykonaniu w okresie 3 lat poprzedzających złożenie oferty minimum 1 diagnozy cyberbezpieczeństwa w ramach programu Cyfrowa Gmina oraz zrealizowania co najmniej 3 audytów bezpieczeństwa w jednostkach administracji publicznej o podobnym zakresie;
4. Załącznik nr 4 – Oświadczenie o niepodleganiu wykluczeniu z udziału w postępowaniu;
5. Załącznik nr 5 - Wzór umowy;
6. Załącznik nr 6 - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa;
7. Załącznik nr 7 - Klauzula informacyjna RODO.

Signature Not Verified

Dokument podpisany przez Kamila Szejner; UG Chodzież
Data: 2022.05.26 12:33:46 CEST