

***Zadanie współfinansowane przez Unię Europejską w ramach projektu „Cyfrowa Gmina”***

***Realizowanego w ramach Programu Operacyjnego Polska Cyfrowa 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**

IRG.271.6.2022.IRG

**PRZEDMIOT ZAMÓWIENIA:**

**„Przeprowadzenie audytu z zakresu KRI, RODO i diagnozy cyberbezpieczeństwa wraz ze szkoleniem pracowników”**

**TRYB POSTĘPOWANIA:**

**Zapytanie ofertowe**

[1. ZAMAWIAJĄCY 3](#_Toc100904490)

[2. NAZWA ZADANIA 3](#_Toc100904491)

[3. OPIS ZADANIA 3](#_Toc100904492)

[3.1. Zakres audytu RODO: 3](#_Toc100904493)

[3.2. Zakres audytu Krajowych Ram Interoperacyjności: 4](#_Toc100904494)

[3.3. Przeprowadzenie diagnozy cyberbezpieczeństwa. 6](#_Toc100904495)

[3.4. Przeprowadzenie szkolenia z cyberbezpieczeństwa dla urzędników. 6](#_Toc100904496)

[3.5. Ramowy zakres szkolenia: 7](#_Toc100904497)

[3.6. Dodatkowe wymagania: 7](#_Toc100904498)

[4. CZĘŚCI ZAMÓWIENIA 8](#_Toc100904499)

[5. WYMAGANY TERMIN REALIZACJI ZAMÓWIENIA: 8](#_Toc100904500)

[6. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY ICH SPEŁNIENIA: 8](#_Toc100904501)

[1. Zamawiający nie stawia żądnych warunków udziału w postepowaniu 8](#_Toc100904502)

[7. WYMAGANE DOKUMENTY 8](#_Toc100904503)

[8. PODSTAWY WYKLUCZENIA 8](#_Toc100904504)

[9. ODRZUCENIE OFERTY 9](#_Toc100904505)

[10. WYJAŚNIENIA I ZMIANA TREŚCI ZAPYTANIA 9](#_Toc100904506)

[11. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI: 10](#_Toc100904507)

[12. OSOBY UPRAWNIONE DO KONTAKTU: 10](#_Toc100904508)

[13. OPIS SPOSOBU PRZYGOTOWANIA OFERTY: 10](#_Toc100904509)

[14. MIEJSCE, TERMIN ZŁOŻENIA I OTWARCIA OFERT: 10](#_Toc100904510)

[15. OPIS SPOSOBU OBLICZENIA CENY OFERTY: 11](#_Toc100904511)

[16. KRYTERIA OCENY OFERT: 11](#_Toc100904512)

[17. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY. 12](#_Toc100904513)

[18. INFORMACJE DOTYCZĄCE ZAWARCIA UMOWY: 12](#_Toc100904514)

[19. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ PRZEZ NIEGO WPROWADZONE DO TREŚCI UMOWY LUB WZÓR UMOWY: 12](#_Toc100904515)

[20. INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH: 12](#_Toc100904516)

[21. ZAŁĄCZNIKI 14](#_Toc100904517)

**ZAPYTANIE OFERTOWE**

**Data publikacji: 19.04.2022**

Zapraszam do złożenia oferty na zadanie pn: „**Przeprowadzenie audytu z zakresu KRI, RODO i diagnozy cyberbezpieczeństwa wraz ze szkoleniem pracowników**”

1. ZAMAWIAJĄCY

Gmina Trzcińsko-Zdrój

ul. Rynek 15

74-510 Trzcińsko-Zdrój

um@trzcinsko-zdroj.pl

# 2. NAZWA ZADANIA

Przedmiotem zamówienia jest „**Przeprowadzenie audytu z zakresu KRI, RODO i diagnozy cyberbezpieczeństwa wraz ze szkoleniem pracowników**”**. Zadanie współfinansowane przez Unię Europejską w ramach projektu „Cyfrowa Gmina”, Realizowanego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Oś Priorytetowa V: Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU.**

# 3. OPIS ZADANIA

## 3.1. Zakres audytu RODO:

1) audyt organizacyjny:

1. Audyt polityk ochrony danych osobowych wprowadzonych/stosowanych przez organizację (w kontekście uwzględnienia atrybutu poufności, dostępności i integralności)
2. Weryfikacja: czynności przetwarzania danych/kategorii czynności przetwarzania, kategorii przetwarzanych danych, dotychczasowych odbiorców danych osobowych,
3. Weryfikacja klauzul informacyjnych w zakresie przetwarzania danych (weryfikacja ich treści, sposobu ich spełniania)
4. Weryfikacja przyjętych regulacji w zakresie ochrony danych w fazie projektowania oraz domyślnej ochrona danych
5. Weryfikacja stosowanego wzoru umowy powierzenia przetwarzania danych oraz audyt wprowadzonych do obiegu umów powierzenia przetwarzania danych osobowych
6. Audyt działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (w ślad za Ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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)
7. Weryfikacja przyjętych regulacji w zakresie zarządzania naruszeniem/ incydentem/uchybieniem.
8. Audyt komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań naprawczych.
9. Weryfikacja zarządzania ryzykiem w kontekście ryzyka ogólnego oraz ryzyka dla podmiotów danych (oceny skutków) – w ślad za Komunikatem Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony.
10. Audyt procesów zapewniających szkolenia osób zaangażowanych w proces przetwarzania danych ze szczególnym uwzględnieniem takich zagadnień, jak: zagrożenia bezpieczeństwa przetwarzanych danych, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo.
11. informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

## 3.2. Zakres audytu Krajowych Ram Interoperacyjności:

1. § 15 ust. 1 KRI Audyt działań projektowych, wdrożeniowych oraz eksploatacyjnych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
2. § 20 ust. 1 KRI Audyt Systemu Zarządzania Bezpieczeństwem Informacji pod kątem poufności, dostępności i integralności.
3. § 20 ust. 2 pkt 1 KRI Audyt regulacji wewnętrznych w zakresie zmieniającego się otoczenia pod kątem aktualizacji.
4. § 20 ust. 2 pkt 2 KRI Audyt utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.
5. § 20 ust. 2 pkt 3 KRI Audyt okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
6. § 20 ust. 2 pkt 4 KRI Audyt działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.
7. § 20 ust. 2 pkt 6 KRI Audyt procesów zapewniających szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

- zagrożenia bezpieczeństwa informacji,

- skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

- stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

1. § 20 ust. 2 pkt 7 KRI Audyt ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, pod kątem:

- monitorowania dostępu do informacji,

- czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

- zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

1. § 20 ust. 2 pkt 8 KRI Audyt ustanowionych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.
2. § 20 ust. 2 pkt 9 KRI Audyt zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.
3. § 20 ust. 2 pkt 10 KRI Audyt umów serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji.
4. § 20 ust. 2 pkt 11 KRI Audyt zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.
5. § 20 ust. 2 pkt 12 KRI Audyt odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

- dbałości o aktualizację oprogramowania,

- minimalizowaniu ryzyka utraty informacji w wyniku awarii,

- ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

- zapewnieniu bezpieczeństwa plików systemowych,

- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

1. § 20 ust. 2 pkt 12 lit. b KRI Audyt poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.
2. § 20 ust. 2 pkt 13 KRI Audyt komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
3. § 20 ust. 2 pkt 14 KRI Audyt ciągłości wykonywania audytu wewnętrznego.
4. § 20 ust. 4 KRI Audyt występowania dodatkowych zabezpieczeń, niezależnych od zakresu, o którym mowa w § 20 ust. 2 pkt 1:14, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne.
5. § 21 ust. 2 KRI Audyt prowadzenia / występowania dzienników systemowych odnotowujących działania użytkowników lub obiektów systemowych, polegających na dostępie do:

- systemu z uprawnieniami administracyjnymi,

- konfiguracji systemu, w tym konfiguracji zabezpieczeń,

- przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

1. § 21 ust. 3 KRI Audyt występowania procedur spoza zakresu § 20 ust. 2 pkt 1:14, mogących stanowić odnotowywanie działań użytkowników lub obiektów systemowych, a także innych zdarzeń związanych z eksploatacją systemu w postaci:

- działań użytkowników nieposiadających uprawnień administracyjnych,

- zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,

- zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny,

– w zakresie wynikającym z analizy ryzyka.

1. § 21 ust. 4 KRI Audyt procedur związanych z dziennikami systemowymi,
2. aspekty ujęte w przepisach ustawy z dnia 5 lipca 2018r. o krajowym systemie cyber-bezpieczeństwa,
3. weryfikacji procedur jednostki.

## 3.3. Przeprowadzenie diagnozy cyberbezpieczeństwa.

1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa – Urzędu Miejskiego w Trzcińsku-Zdroju.
2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa” stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina (załącznik nr 3 do zapytania – diagnoza)
3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
4. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.
5. Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowa Gmina” są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek
samorządowych. Wykonawca jest zobowiązany mieć na uwadze powyższy cel przeprowadzenia diagnozy i jej przeznaczenia.

## 3.4. Przeprowadzenie szkolenia z cyberbezpieczeństwa dla urzędników.

Wymagania ogólne dla szkoleń:

1. Planowany czas trwania zajęć ok. 2,5 godziny zegarowe na każdą grupę,

ilość grup 2.

1. Termin planowanego szkolenia maj 2022 r. dzień (przystosujemy się do wykładowcy)
2. Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia.
3. Dopuszczamy metodę prowadzenia szkolenie przez wideokonferencję.

## 3.5. Ramowy zakres szkolenia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
6. Bezpieczeństwo stacji roboczych (komputery użytkownika).
7. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
8. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
9. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
10. Prawidłowe korzystanie z oprogramowania antywirusowego.
11. Zasady aktualizacji programów i aplikacji.
12. Szyfrowanie dokumentów i poczty elektronicznej.
13. Polityka haseł, zarządzanie dostępem i tożsamością.
14. Bezpieczeństwo sieci LAN i Wi-Fi.
15. Bezpieczeństwo aplikacji ministerialnych oraz wewnątrzorganizacyjnych.
16. Bezpieczeństwo stacji roboczych (komputery użytkownika).
17. Zarządzanie tożsamością w internecie oraz wewnątrz organizacji.
18. Bezpieczeństwo baz danych i infrastruktury.
19. Bezpieczeństwo mobilne.
20. Odzyskiwanie po awarii – planowanie ciągłości działania.
21. Odpowiednie zabezpieczenie techniczne sieci.
22. Optymalna architektura systemowo-serwerowa.
23. Techniki socjotechniki (inżynieria społeczna).
24. Bezpieczeństwo sieci LAN i Wi-Fi,
25. Zarządzanie tożsamością w internecie oraz wewnątrz organizacji,
26. Bezpieczeństwo baz danych i infrastruktury,
27. Odzyskiwanie po awarii – planowanie ciągłości działania,
28. Odpowiednie zabezpieczenie techniczne sieci,
29. Optymalna architektura systemowo-serwerowa,

## 3.6. Dodatkowe wymagania:

1. W ramach usługi zostaną przeszkolone 22 osoby w grupach maksimum 11-osobowych.

# 4. CZĘŚCI ZAMÓWIENIA

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Zamawiający nie przewiduje udzielenia zamówień uzupełniających.
3. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

# 5. WYMAGANY TERMIN REALIZACJI ZAMÓWIENIA:

1. Planowane terminy realizacji zamówienia:
2. Rozpoczęcie: 1 maj 2022 r.
3. Zakończenie – 31 maj 2022.

6. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY ICH SPEŁNIENIA:

1. Zamawiający nie stawia żądnych warunków udziału w postepowaniu

7. WYMAGANE DOKUMENTY

1. Formularz oferty wg załączonego wzoru – załącznik nr 1 do zapytania.
2. Wymagane dokumenty powinny być przedstawione w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem na każdej zapisanej stronie kopii przez osobę lub osoby, uprawnione do reprezentowania Wykonawcy.
3. W przypadku załączenia do oferty dokumentów sporządzonych w innym języku niż polski, Wykonawca zobowiązany jest załączyć tłumaczenia na język polski, poświadczone przez Wykonawcę.
4. Zamawiający może wezwać Wykonawców którzy nie złożyli wymaganych oświadczeń, dokumentów lub pełnomocnictw, albo którzy złożyli wymagane przez zamawiającego oświadczenia i dokumenty, zawierające błędy lub którzy złożyli wadliwe pełnomocnictwa, do ich złożenia w wyznaczonym terminie. Złożone na wezwanie Zamawiającego oświadczenia i dokumenty powinny potwierdzać spełnianie przez wykonawcę warunków udziału w postępowaniu wymagań określonych przez zamawiającego, nie później niż w dniu, w którym upłynął termin składania ofert.
5. Zamawiający może wezwać w wyznaczonym przez siebie terminie, do złożenia wyjaśnień dotyczących złożonej oferty, oświadczeń lub dokumentów.

8. PODSTAWY WYKLUCZENIA

1. Zamówienie nie może zostać udzielone podmiotowi powiązanemu osobowo lub kapitałowo z zamawiającym. Przez powiązania osobowe lub kapitałowe rozumie się wzajemne powiązania między zamawiającym, lub osobami upoważnionymi do zaciągania zobowiązań w jego imieniu, lub osobami wykonującymi w jego imieniu czynności związane z przygotowaniem i przeprowadzeniem postępowania w sprawie wyboru wykonawcy a wykonawcą, polegające na:
	* uczestniczeniu jako wspólnik w spółce cywilnej lub osobowej;
	* posiadaniu co najmniej 10% udziałów lub akcji spółki kapitałowej;
	* pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta lub pełnomocnika;
	* pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli;
	* pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że może to budzić uzasadnione wątpliwości co do bezstronności tych osób.
2. niezastosowanie się do wezwania do uzupełnienia dokumentów lub do udzielenia wyjaśnień, spowoduje wykluczenie z postępowania.

9. ODRZUCENIE OFERTY

1. Oferta podlega odrzuceniu w przypadku, gdy:

jej treść nie odpowiada treści zapytania ofertowego lub została złożona przez podmiot:

- powiązany osobowo lub kapitałowo z zamawiającym lub osobami, o których mowa w punkcie 8 zapytania,

- lub została złożona po terminie składania ofert określonym w zapytaniu ofertowym.

1. Oferta nie podlega odrzuceniu, mimo że została złożona przez podmiot powiązany osobowo lub kapitałowo z osobą, o której mowa w punkcie 8 zapytania, jeżeli osoba ta nie będzie brała udziału w dalszym postępowaniu w sprawie wyboru przez zamawiającego wykonawcy danego zadania ujętego w zestawieniu rzeczowo-finansowym operacji.
2. Oferta dodatkowa podlega odrzuceniu w przypadku, gdy:

- zawiera cenę lub koszt wyższe niż w złożonej ofercie pierwotnej lub

- została złożona po terminie składania ofert dodatkowych określonym przez zamawiającego w wezwaniu do złożenia tych ofert dodatkowych.

1. Zastrzega się możliwość zakończenia postępowania bez wyboru żadnej z ofert.

10. WYJAŚNIENIA I ZMIANA TREŚCI ZAPYTANIA

1. Wykonawca może zwrócić się pisemnie do zamawiającego o wyjaśnienie treści niniejszego zapytania ofertowego. Zamawiający udzieli wyjaśnień nie później niż na 2 dni przed upływem terminu składania ofert, z zastrzeżeniem pkt 2.poprzez platformę zakupową.
2. Jeżeli wniosek o wyjaśnienie treści zapytania ofertowego wpłynie do zamawiającego później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert lub dotyczy udzielonych wyjaśnień, zamawiający może udzielić wyjaśnień lub pozostawić wniosek bez rozpoznania.
3. Ewentualna zmiana terminu składania ofert nie powoduje przesunięcia terminu, o którym mowa w pkt 2, po upłynięciu którego zamawiający może pozostawić wniosek o wyjaśnienie treści zapytania bez rozpoznania.
4. Zamawiający może zmienić zapytanie ofertowe przed upływem terminu składania ofert:

a) w zmienionym zapytaniu ofertowym przedłużony zostanie termin składania ofert o czas niezbędny do wprowadzenia zmian w ofertach, o ile przedłużenie tego terminu jest konieczne z uwagi na istotną zmianę zapytania ofertowego polegającą w szczególności na zmianie:

- opisu zadania,

- warunku udziału w postępowaniu lub sposobu dokonywania oceny spełniania danego warunku w tym postępowaniu,

- kryterium oceny ofert.

11. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI:

1. Zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują drogą elektroniczną.
2. Jeżeli Zamawiający lub Wykonawca przekazują zawiadomienia oraz informacje, o których mowa w pkt 1, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
3. Obowiązuje forma elektroniczna złożenia oferty i jej załączników, oświadczeń i dokumentów oraz pełnomocnictw.

12. OSOBY UPRAWNIONE DO KONTAKTU:

Osobami uprawnionymi do kontaktów z Wykonawcami w imieniu Zamawiającego
w związku z niniejszym zapytaniem są: Mariusz Piątkowski - tel.: (91) 414 80 01,
e-mail: informatyk@trzcinsko-zdroj.pl.’

13. OPIS SPOSOBU PRZYGOTOWANIA OFERTY:

1. Ofertę - pod rygorem nieważności – należy złożyć w języku polskim, w formie elektronicznej za pośrednictwem platformy zakupowej o nazwie platformazakupowa.pl (zwanej dalej także: „platformą”) pod adresem: <https://platformazakupowa.pl/pn/trzcinsko_zdroj>. Komunikacja, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między Zamawiającym a Wykonawcami, odbywa się przy użyciu środków komunikacji elektronicznej;
2. Wykonawcy lub ich pełnomocnik muszą złożyć podpisy elektroniczne lub kwalifikowalne na ofercie i tych załącznikach do oferty, które sporządzili.
3. W przypadku składania oferty przez pełnomocnika, do oferty musi być dołączone odpowiednie pełnomocnictwo, podpisane przez osoby uprawnione do reprezentowania Wykonawcy.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
6. Zamawiający może poprawić oczywiste omyłki pisarskie oraz rachunkowe w obliczeniu ceny, powiadamiając o tym fakcie wykonawcę.

14. MIEJSCE, TERMIN ZŁOŻENIA I OTWARCIA OFERT:

1. Ofertę należy złożyć w terminie do dnia 27 kwietnia 2022r. do godz. 10:00.
2. Oferta otrzymana przez Zamawiającego po terminie podanym w pkt 1 będzie podlegała odrzuceniu.
3. Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę przed upływem terminu do jej składania.
4. Otwarcie złożonych ofert nastąpi w dniu 27 kwietnia 2022 godz. 10:30 w siedzibie Zamawiającego przy ul. Rynek 15, 74 – 510 Trzcińsko-Zdrój, pokój nr 10.
5. Zapytanie unieważnia się gdy:
6. nie złożono żadnej oferty,
7. cena najkorzystniejszej oferty lub oferta z najniższą ceną przewyższa kwotę, którą zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty,
8. wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć,
9. z analizy złożonych ofert wynika, że udzielenie zamówienia naruszałoby zasady dokonywania wydatków publicznych, określone w art. 44 ust. 3 ustawy z dnia 27 sierpnia 2009r. o finansach publicznych (t.j. Dz. U. z 2021 r. poz. 305, ze zm. ).

15. OPIS SPOSOBU OBLICZENIA CENY OFERTY:

1. Obowiązującym rodzajem wynagrodzenia jest ryczałt. Podstawą obliczenia ceny ofertowej powinna być dla Wykonawcy jego własna wycena oraz oparta na rachunku ekonomicznym kalkulacja.
2. Cena oferty musi uwzględniać wszystkie wymagania niniejszego zapytania ofertowego oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytego wykonania przedmiotu zamówienia, w tym również wszystkie koszty związane z prawidłowym przygotowaniem i zabezpieczeniem wszelkich materiałów niezbędnych do prawidłowego wykonania przedmiotu zamówienia. Wykonawca musi przewidzieć wszystkie okoliczności, które mogą wpłynąć na cenę zamówienia.
3. Koszty pracy, które zostaną przyjęte do ustalenia ceny nie mogą być niższe od minimalnego wynagrodzenia za pracę albo minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 roku o minimalnym wynagrodzeniu za pracę (t.j. Dz.U. z 2020 roku poz. 2207
4. Wykonawca oblicza cenę oferty jako sumę cen za poszczególne elementy objęte przedmiotem niniejszego zamówienia i tak wyliczoną cenę wraz z podatkiem VAT zamieszcza w Formularzu Ofertowym.
5. Cena oferty musi być wyrażona w polskich złotych, liczbowo z dokładnością do dwóch miejsc po przecinku.
6. Prawidłowe ustalenie stawki należnego podatku VAT należy do obowiązków Wykonawcy, zgodnie z przepisami ustawy o podatku od towarów i usług oraz o podatku akcyzowym. Zastosowanie przez Wykonawcę stawki podatku VAT od towarów i usług niezgodnej z obowiązującymi przepisami może spowodować odrzucenie oferty.
7. Wynagrodzenie ryczałtowe należne Wykonawcy płatne będzie w sposób określony we wzorze umowy, która stanowi załącznik do niniejszego zapytania.

16. KRYTERIA OCENY OFERT:

Cena (brutto) – 100 %

1. Opis sposobów dokonywania oceny ofert.
2. Kryterium – najniższa cena 100 %
3. Zamawiający wzywa Wykonawców, którzy złożyli oferty o takiej samej najniższej cenie, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych w zakresie dotyczącym ceny.
4. Wykonawcy, składając oferty dodatkowe, nie mogą przedstawić ceny wyższej niż w złożonych ofertach.
5. W przypadku niezłożenia żadnej oferty dodatkowej albo złożenia ofert dodatkowych o takiej samej najniższej cenie albo odrzucenia wszystkich ofert dodatkowych, Zamawiający kończy postępowanie bez wyboru żadnej z ofert.

17. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY.

O wyborze najkorzystniejszej oferty Zamawiający zawiadomi wszystkich potencjalnych wykonawców, którzy złożyli oferty za pośrednictwem platformy zakupowej.

18. INFORMACJE DOTYCZĄCE ZAWARCIA UMOWY:

* 1. Wykonawca, którego oferta została wybrana, jest zobowiązany podpisać umowę na realizację zamówienia w siedzibie Zamawiającego w terminie wskazanym przez Zamawiającego.
	2. Umowa będzie zawierać wszystkie uwarunkowania zawarte w złożonej ofercie.
	3. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez ponownego przeprowadzania ich oceny.

19. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ PRZEZ NIEGO WPROWADZONE DO TREŚCI UMOWY LUB WZÓR UMOWY:

1. Wzór umowy został zamieszczony w załączniku nr 2 do Zapytania ofertowego.
2. Przyjmuje się, że zapisy projektu umowy zostaną przyjęte przez Wykonawcę bez zastrzeżeń w chwili jej podpisania.
3. Zasady dokonywania i zakres dopuszczalnych zmian postanowień zawartej umowy określa projekt umowy.

20. INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH:

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 („RODO”), informujemy o zasadach przetwarzania danych osobowych oraz o przysługujących prawach z tym związanych z uwzględnieniem zasad wynikających z art. 19 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych z dnia 11 września 2019 r. (tj. Dz. U. z 2021 r. poz. 1129 ze zm.) („ustawa Pzp”) .

1. Administratorem danych osobowych jest: Gmina Trzcińsko-Zdrój reprezentowana przez Burmistrza Gminy Trzcińsko-Zdrój, ul. Rynek 15, 74-510 Trzcińsko-Zdrój.
2. Jeśli są pytania dotyczące sposobu i zakresu przetwarzania danych osobowych, a także przysługujących uprawnień, można się skontaktować z Inspektorem Ochrony Danych Osobowych: tel. 91 414 8001 wew.33, adres email: iod@trzcinsko-zdroj.pl.
3. Administrator przetwarza dane osobowe na podstawie art. 6 ust. 1 lit. c rozporządzenia RODO czyli przetwarzanie niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. „**Przeprowadzenie audytu z zakresu KRI, RODO i diagnozy cyberbezpieczeństwa wraz ze szkoleniem pracowników**”.
4. W przypadku wyboru oferty najkorzystniejszej dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z realizacją umowy na „**Przeprowadzenie audytu z zakresu KRI, RODO i diagnozy cyberbezpieczeństwa wraz ze szkoleniem pracowników**”
5. Odbiorcami danych osobowych będą osoby lub podmioty którym udostępniona zostanie dokumentacja postępowania w związku z ustawa Pzp i na jej podstawie, osoby lub podmioty, którym na podstawie odrębnych przepisów prawa przysługuje prawo kontroli, jak również osoby lub podmioty którym dane, zostaną udostępnione w oparciu o przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U.2020.2176 z późn.zm);
6. Dane osobowe będą przechowywane, zgodnie z ustawą Pzp, przez okres 4 lat od dnia zakończenia postepowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekroczy 4 lata, okres przechowywania obejmuje cały czas trwania umowy. Zgodnie z art. 269 ust. 3 ustawy Pzp okres przechowywania danych osobowych zamieszczanych w Biuletynie Zamówień Publicznych określa Prezes Urzędu Zamówień Publicznych.
7. Podanie danych osobowych jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego, bez którego nie można udzielić zamówienia w przypadku wyboru najkorzystniejszej oferty.
8. Państwa dane nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą podlegać profilowaniu oraz nie będą przekazywane do państw trzecich lub organizacji międzynarodowej.
9. Przysługuje Panu/Pani:
	1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących, przy czym zamawiający może żądać od osoby występującej z żądaniem wskazania dodatkowych informacji, mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia (art. 75 ustawy Pzp);
	2. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych\*\*;
	3. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO, przy czym zgłoszenie żądania ograniczenia przetwarzania nie ogranicza przetwarzania danych osobowych do czasu zakończenia tego postępowania (art. 19 ust. 3 ustawy Pzp) \*\*\*;
	4. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
10. nie przysługuje Panu/Pani:
	1. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
	2. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
	3. **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.**
11. Zamawiający dołoży wszelkich starań, aby zapewnić odpowiednie środki ochrony danych osobowych przed ich przypadkowym lub umyślnym zniszczeniem, przypadkową utratą, zmianą, nieuprawnionym ujawnieniem, wykorzystaniem czy dostępem, zgodnie z obowiązującymi przepisami prawa.

***\*\* Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym zustawą  oraz nie może naruszać integralności dokumentacji postępowania w tym protokołu oraz jego załączników.*

***\*\*\* Wyjaśnienie:*** *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.*

21. ZAŁĄCZNIKI

1) Załącznik nr 1 - wzór oferty,

2) Załącznik nr 2 - projekt umowy

3) Załącznik nr 3 - Formularz diagnozy cyberbezpieczeństwa