Załącznik nr 2 – projekt umowy

**UMOWA NR ……………../2022**

Zawarta w dniu **…………………….. 2022 r**. w Trzcińsku-Zdroju, pomiędzy:

Gminą Trzcińsko-Zdrój

ul. Rynek 15

74-510 Trzcińsko-Zdrój

zwaną dalej „Zleceniodawcą” reprezentowanym przez:

Bartłomieja Wróbla – Burmistrza Gminy Trzcińsko-Zdrój

przy kontrasygnacie

Czesławy Trautman – Skarbnik

a firmą

………………………………………………,

NIP:……………………….,

REGON………………………..,

zwaną dalej „Zleceniobiorcą”, reprezentowanym przez:

………………………………………. – ……………………………………

**Postanowienia ogólne**

1. Przedmiotem niniejszej umowy jest wykonanie przez Wykonawcę **przeprowadzenie audytu z zakresu KRI, RODO i diagnozy cyberbezpieczeństwa wraz ze szkoleniem pracowników** w zakresie określonym w zapytaniu ofertowym stanowiącym załącznik do niniejszej umowy

**§ 2**

**Zakres audytu**

## 2.1. 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.

## 2.2. 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.

## 2.3. 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, 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.

## 2.4. 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.

## 2.5. 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.

## 2.6. Dodatkowe wymagania:

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

**§ 3**

**Oświadczenia i obowiązki Wykonawcy**

1. Wykonawca zobowiązuje się do wykonania umowy z zachowaniem zasad należytej staranności i profesjonalizmu wynikających z zawodowego charakteru prowadzonej działalności.
2. Wykonawca przeprowadzi audyt przy ścisłej współpracy z Zamawiającym.
3. Wykonawca zobowiązuje się, że wykonane w ramach przeprowadzonego audytu prace, materiały i informacje oraz wykorzystywane przez niego oprogramowanie nie narusza praw osób trzecich, a w szczególności prawa autorskiego i praw pokrewnych.
4. Wykonawca ponosi odpowiedzialność za działania i zaniechania osób, którymi posłużył się przy wykonywaniu umowy, jak za własne działania czy zaniechania.
5. Wykonawca oświadcza, że wyznaczony przez niego Audytor do realizacji niniejszej umowy posiada przynajmniej jeden z certyfikatów wymienionych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz.U. 2010 nr 177 poz. 1195).

**§ 4**

**Obowiązki i oświadczenia Zamawiającego**

1. Zamawiający zobowiązuje się do zapewnienia Wykonawcy w siedzibie Zamawiającego dostępu do informacji niezbędnych do realizacji umowy.
2. Zamawiający zobowiązuje się do przekazywania niezwłocznie, osobiście lub za pośrednictwem wyznaczonego pracownika, w terminie nie dłuższym niż 3 dni robocze, żądanych przez Wykonawcę informacji niezbędnych do wykonania umowy.
3. Brak przedłożenia w/w informacji skutkować może niewykonaniem audytu w zakresie objętym brakiem.
4. W przypadku powstania przeszkód po stronie Zamawiającego w wykonaniu przedmiotu umowy, Zamawiający poinformuje Wykonawcę o powyższym niezwłocznie, pisemnie lub za pośrednictwem poczty elektronicznej, na adres wskazany w umowie. Okres czasowej przeszkody w wykonaniu umowy powstały po stronie Zamawiającego powoduje przesunięcie terminu realizacji umowy o liczbę dni, w trakcie których Wykonawca z nie swojej winy nie mógł wykonywać umowy.
5. Zamawiający wyraża zgodę na przeprowadzenie przez Wykonawcę czynności w zakresie objętym audytem, w tym udziela Wykonawcy zgody na przetwarzanie danych zgromadzonych podczas audytu, wyłącznie w celach związanych z realizacją umowy.
6. Zamawiający oświadcza, że w przypadku awarii sprzętu komputerowego lub oprogramowania, w trakcie trwania audytu, Wykonawca nie będzie ponosił z tego tytułu żadnej odpowiedzialności, o ile awaria nie była spowodowana zawinionym działaniem Wykonawcy.

**§ 5**

**Upoważnienie**

1. Zamawiający zobowiązany jest do wyznaczenia pracownika, który obecny będzie przy wykonywaniu umowy, w zakresie czynności objętych audytem.
2. Zamawiający zobowiązany jest do zapewnienia obecności administratora systemu informatycznego w trakcie czynności w zakresie przeprowadzanego audytu.
3. Niezapewnienie obecności pracownika wyznaczonego, o ile nie jest to konieczne, nie wstrzymuje czynności objętych przedmiotem niniejszej umowy.

**§ 6**

**Audyt i raport**

1. W terminie nie później niż 7 dni od podpisania niniejszej umowy Wykonawca we współpracy z IOD prześle Zamawiającemu harmonogram i plan audytu.
2. Wykonawca zobowiązuje się przekazać Zamawiającemu wstępny raport z audytu do dnia **……………….. r.** Zamawiający zastrzega sobie prawo zgłoszenia uwag i zastrzeżeń dotyczących raportu w ciągu **4 dni** roboczych od dnia jego otrzymania.
3. Wykonawca przekaże Zamawiającemu raport końcowy do dnia **31.05.2022 r.**
4. Raporty, o których mowa w pkt 2 i 3 należy przekazać w formie:

4.1 elektronicznej na adres **informatyk@trzcinsko-zdroj.pl**

4.2 papierowej złożonej w sekretariacie Wykonawcy.

**§ 7**

**Wynagrodzenie**

1. Zamawiający zapłaci Wykonawcy tytułem wykonania umowy wynagrodzenie ryczałtowe w kwocie łącznej netto …………... zł (słownie zł: ……………………) powiększoną   
   o obowiązującą stawkę podatku VAT (23% ).
2. Podstawą zapłaty jest faktura z terminem płatności wynoszącym 30 dni od dnia doręczenia faktury Zamawiającemu.
3. Faktura wystawiona zostanie przez Wykonawcę po przekazaniu Zamawiającemu raportu końcowego, którego otrzymanie zostanie potwierdzone przez Zamawiającego. W razie uwag Zamawiającego do przekazanych dokumentów, faktura zostanie wystawiona przez Wykonawcę po ich uwzględnieniu i dostarczeniu przez Wykonawcę poprawionych dokumentów i ich przyjęciu bez uwag Zamawiającego.
4. Zapłata nastąpi na rachunek bankowy wskazany w fakturze. Za dzień zapłaty uznaje się dzień obciążenia kwotą rachunku bankowego Zamawiającego.
5. Zamawiający upoważnia Wykonawcę do wystawienia faktury bez podpisu Zamawiającego.
6. Wykonawcy nie przysługuje prawo cesji wierzytelności wynikającej z niniejszej umowy, bez uzyskania pisemnej zgody Zamawiającego.

**§ 8**

**Poufność i zabezpieczenie danych**

1. Wykonawca ponosi odpowiedzialność za naruszenie praw osób trzecich, w tym za ujawnienie informacji, jakie uzyskane zostały w trakcie przeprowadzenia audytu w szczególności w zakresie bezpieczeństwa systemu informatycznego Zamawiającego, danych osobowych pracowników Zamawiającego, w tym za ujawnienie tych informacji przez swoich pracowników i osoby, z którymi się posługuje przy wykonaniu umowy.
2. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji otrzymanych pośrednio lub bezpośrednio w trakcie trwania audytu i po jego zakończeniu, o ile informacje te nie stanowią informacji ogólnodostępnych (ochrona tajemnicy uzyskanej w ramach audytu).
3. Zabrania się wynoszenia przez Wykonawcę poza obszar Urzędu zgromadzonych dowodów audytowych i innych informacji potrzebnych do wykonania przedmiotu umowy. Wyjątek stanowi jedynie kopia gotowego raportu stanowiącego dowód wykonania umowy.

**§ 9**

**Obowiązki RODO**

1. Zamawiający i Wykonawca na potrzeby realizacji niniejszego przedmiotu zamówienia ustalają postanowienia w zakresie ochrony danych osobowych, które Zamawiający będzie przetwarzał w toku realizacji niniejszej umowy jak i po jej zakończeniu.
2. Administratorem danych osobowych jest: Gmina Trzcińsko-Zdrój reprezentowana przez Burmistrza Gminy Trzcińsko-Zdrój, ul. Rynek 15, 74-510 Trzcińsko-Zdrój.
3. 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.
4. 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 Krajowych Ram Interoperacyjności i diagnozy z zakresu cyberbezpieczeństwa wraz ze szkoleniem pracowników**”.
5. 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 Krajowych Ram Interoperacyjności i diagnozy z zakresu cyberbezpieczeństwa wraz ze szkoleniem pracowników**”
6. 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);
7. 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.
8. 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.
9. Państwa dane nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą podlegać profilowaniu oraz nie będą przekazywane do państw trzecich lub organizacji międzynarodowej.
10. Przysługuje Panu/Pani:

* 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);
* na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych\*\*;
* 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) \*\*\*;
* prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

1. nie przysługuje Panu/Pani:

* w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
* prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
* **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.**

1. 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.*

**§ 10**

**Odstąpienie od Umowy i kara umowna**

1. Wykonawca zapłaci karę umowną:
   1. za odstąpienie od umowy przez Zamawiającego z winy Wykonawcy w wysokości 10% wartości brutto umowy,
   2. za opóźnienie w wykonaniu określonych w umowie usług w wysokości 0,2% wartości umowy brutto za każdy dzień opóźnienia.
2. Zapłata kar umownych nie wyłącza odpowiedzialności odszkodowawczej (uzupełniającej) Wykonawcy wobec Zamawiającego, na zasadach określonych w Kodeksie Cywilnym.

Zamawiający może odstąpić od umowy w trybie natychmiastowym w przypadku wykonywania umowy w sposób niezgodny z obowiązującymi przepisami lub w przypadku niezgodności z postanowieniami umowy w tym m.in. nie zachowania umownego terminu.

**§ 11**

**Siła wyższa**

W czasie trwania siły wyższej strony umowy zwolnione będą od wszelkiej odpowiedzialności za niewykonanie umowy, jeżeli okoliczności zaistnienia siły wyższej będą stanowiły przeszkodę w wykonaniu umowy.

1. Przez siłę wyższą należy rozumieć zdarzenia zewnętrzne, których nie można było przewidzieć i niemożliwe było ich zapobieżenie, przy czym chodzi tu w szczególności o powódź, włamanie, długotrwały zanik energii elektrycznej wywołany awarią dostawcy energii, uszkodzenie sprzętu komputerowego.
2. Strona uprawniona jest do powołania się na siłę wyższą tylko w przypadku, gdy poinformuje pisemnie o powyższym drugą stronę niezwłocznie, nie później niż w dniu następnym po dniu kiedy powstało zdarzenie uniemożliwiające wykonywanie Umowy.

**§ 12**

**Prawa autorskie**

1. W ramach wynagrodzenia, o którym mowa w niniejszej umowie Wykonawca zobowiązany jest do przeniesienia na Zamawiającego wszystkich przysługujących mu autorskich praw majątkowych do korzystania z utworów powstałych na podstawie niniejszej umowy  
2. Przeniesienie autorskich praw majątkowych do utworu oraz własność utworu w powyższym zakresie nastąpi z dniem przekazania egzemplarza utworu.

3. Wykonawca oświadcza, że dostarczony utwór będzie wolny od wad fizycznych i prawnych, oraz że służą mu wyłączne majątkowe prawa autorskie do utworu w zakresie niezbędnym do przeniesienia tych praw na Zamawiającego.

**§ 13**

**Postanowienia końcowe**

1. Strony zgodnie ustalają, że formą kontaktu wiążącą przy realizacji umowy jest kontakt listowny (na adresy podane w umowie) oraz kontakt za pośrednictwem poczty elektronicznej:
   1. Adres poczty elektronicznej Zamawiającego **informatyk@trzcinsko-zdroj.pl**
   2. Adres poczty elektronicznej Wykonawcy ……………………….
2. Zmiana postanowień umowy wymaga formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy Kodeksu Cywilnego.
4. Wszelkie spory mogące powstać w związku z wykonaniem niniejszej umowy strony zobowiązują się w pierwszej kolejności poddać pod mediację. W przypadku braku porozumienia właściwym dla rozstrzygnięcia sporów jest Sąd właściwy według siedziby Zamawiającego.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym egzemplarzu dla każdej ze stron.

**ZAMAWIAJĄCY WYKONAWCA**