Załącznik nr 2 do zapytania ofertowego

Umowa nr .....

zawarta w dniu ……..2026 r. roku, pomiędzy:

Gminą Stara Dąbrowa
reprezentowaną przez:
Wójta Gminy Stara Dąbrowa
przy kontrasygnacie:
.....
zwanymi w dalszej części umowy dalej „Zamawiającym"
a
.....
zwanym dalej „Wykonawcą", reprezentowanym przez:
.....
o następującej treści:

Zamówienie finansowane ze środków Unii Europejskiej w ramach konkursu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

W wyniku wyboru najkorzystniejszej oferty po przeprowadzeniu zapytania ofertowego, została zawarta umowa o następującej treści:

Przedmiot umowy

§ 1

1. Zamawiający zleca a Wykonawca przyjmuje do wykonania usługi obejmujące w szczególności:
   1) **Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Urzędu Gminy w Starej Dąbrowie.**
   2) **Przeprowadzenie Audytu Krajowych Ram Interoperacyjności jako wymóg końcowego rozliczenia projektu.**
   3) **Przeprowadzenie testów socjotechnicznych.**

2. Szczegółowy opis przedmiotu zamówienia w zakresie **opracowania wraz z wdrożeniem dokumentacji SZBI dla Urzędu Gminy w Starej Dąbrowie** obejmuje czynności związane z realizacją zadania zgodnego z poniższymi wymaganiami:
   1. W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do aktualizacji dokumentacji z zakresu bezpieczeństwa informacji posiadanej przez Zamawiającego oraz opracowania i wdrożenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
   2. W ramach wykonywanych prac Wykonawca zapewni zgodność dokumentacji z poniższymi wymaganiami:
      a) rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
      b) ustawa z dnia z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa wraz z nowelizacjami ustawy, które zostaną dokonane w czasie realizacji zamówienia;
      c) 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);

d) wymagania norm ISO 27001, a w szczególności PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO-27005 i w oparciu o główne założenia norm ISO 31000 w zakresie zarządzania ryzykiem oraz PN-EN ISO 22301 w zakresie ciągłości działania;

e) wymagania regulaminu konkursu grantowego oraz umowy o powierzenie grantu zawartej w ramach projektu „Cyberbezpieczny Samorząd".

3. Wdrażany System Zarządzania Bezpieczeństwem Informacji powinien składać się z obszarów regulujących następujące obszary:
   a) zarządzanie aktywami,
   b) zarządzanie ryzykiem,
   c) zapewnienie bezpieczeństwa systemów informatycznych oraz ich rozwoju,
   d) zapewnienie bezpieczeństwa fizycznego,
   e) kontrola dostępu do oprogramowania i infrastruktury sieciowej,
   f) klasyfikacja informacji oraz nadzoru nad dokumentacją,
   g) zapewnienie bezpieczeństwa zasobów ludzkich,
   h) wykonywanie kopii zapasowych,
   i) stosowanie kryptografii,
   j) obsługa incydentów i realizacja działań korygujących,
   k) prowadzenie wewnętrznych audytów bezpieczeństwa,
   l) prowadzenie przeglądów zarządzania,
   m) zapewnienie ciągłości działania i przywracania normalnej działalności po wystąpieniu zakłóceń,
   n) zapewnienie bezpieczeństwa łańcucha dostaw,
   o) postępowanie z podatnościami systemów i sieci,
   p) Deklaracja stosowania (w oparciu o załącznik A do normy ISO/IEC 27001:2022).
4. W ramach wdrażania Systemu Zarządzania Bezpieczeństwem Informacji powinny zostać uregulowane zabezpieczenia określone w załączniku A do normy ISO/IEC 27001:2022.

3.Szczegółowy opis przedmiotu zamówienia w zakresie **przeprowadzenie Audytu Krajowych Ram Interoperacyjności jako wymóg końcowego rozliczenia projektu** obejmuje czynności związane z realizacją zadania zgodnego z poniższymi wymaganiami:

W ramach realizowanego przedmiotu zamówienia Wykonawca jest zobowiązany do zapewnienia:

a) Realizacji audytu bezpieczeństwa informacji w siedzibie Zamawiającego (nie jest przewidziana zdalna realizacja);

b) Wypełnienie ankiety dojrzałości z zakresu cyberbezpieczeństwa, zgodnej z regulaminem projektu „Cyberbezpieczny Samorząd" dla urzędu oraz wszystkich jednostek objętych projektem;

c) Zapewnienia zgodności realizowanego audytu bezpieczeństwa informacji z następującymi wymaganiami:
   1. Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych- Ustawy o Krajowym Systemie Cyberbezpieczeństwa;
   2. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
   3. wymagań określonych w normie ISO 27001.

d) Opracowanie raportu z audytu wraz z rekomendacjami do wdrożenia w ramach projektu „Cyberbezpieczny Samorząd", w szczególności w odniesieniu do wyników ankiety wypełnionej przez Zamawiającego, zgodnie z regulaminem projektu „Cyberbezpieczny Samorząd".

Szczegółowy zakres audytu powinien objąć następujące obszary:

a) prawidłowości prowadzonej przez Zamawiającego dokumentacji aktualnej oraz planowanej, dotyczącej Systemu Zarządzania Bezpieczeństwa Informacji w zakresie jego poufności, dostępności i integralności informacji,
b) zapewniania przez Zamawiającego aktualizacji regulacji wewnętrznych w zakresie, dotyczącym zmieniającego się otoczenia,
c) utrzymywania przez Zamawiającego aktualności inwentaryzacji sprzętu i oprogramowania, służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację,
d) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
e) podejmowania 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,
f) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji z uwzględnieniem aspektów związanych z bezpieczeństwem informacji,
g) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
h) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
i) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
j) ustalonych zapisów zawieranych w umowach serwisowych gwarantujących odpowiedni poziom bezpieczeństwa informacji,
k) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
l) zapewnienia odpowiedniego określonego przez KRI poziomu bezpieczeństwa w systemach teleinformatycznych,
m) sposobu postępowania z incydentami związanymi z bezpieczeństwem informacji, w tym bezzwłocznego zgłaszania takich incydentów,
n) przeglądu zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa,
o) przeglądu istniejących regulacji wewnętrznych odnośnie bezpieczeństwa przetwarzania danych osobowych,
p) przeglądu aktualnie wykorzystywanych dokumentów mających związek z ochroną danych osobowych,
q) weryfikacji istniejących procedur zarządzania systemami teleinformatycznymi,
r) weryfikacji ochrony przed oprogramowaniem szkodliwym,
s) weryfikacji procedur zarządzania kopiami zapasowymi,
t) weryfikacji procedur dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,

u) weryfikacji zabezpieczeń stacji roboczych i nośników danych w szczególności tych, na których przetwarzane są dane osobowe,
v) weryfikacji haseł,
w) analizy i oceny mechanizmów zarządzania aktualizacjami.

W ramach audytu powinna zostać wykonana analiza techniczna (obejmująca odrębny raport) w zakresie monitorowania sieci internetowej urzędu wraz z wydaniem zaleceń i rekomendacji w zakresie wdrożenia systemów SOC. Analiza powinna zostać opracowania bezpośrednio przez osoby wskazane w ofercie i posiadające uprawnienia w zakresie wymaganych certyfikatów.

Wymagany zakres opracowania:

- Identyfikacja kluczowych elementów infrastruktury teleinformatycznej Urzędu, obejmującej urządzenia sieciowe, serwery, stacje robocze, systemy operacyjne, usługi sieciowe oraz wykorzystywane rozwiązania bezpieczeństwa.
- Przygotowanie metodyki prowadzenia monitoringu obejmującej zakres monitorowanych zasobów, źródła logów, sposób pozyskiwania danych oraz kryteria oceny zdarzeń bezpieczeństwa.
- Ocena kompletności logów generowanych przez urządzenia sieciowe, systemy operacyjne, aplikacje oraz rozwiązania zabezpieczające, wraz z identyfikacją obszarów wymagających uzupełnienia.
- Weryfikacja aktualnie stosowanych mechanizmów bezpieczeństwa, obejmujących m.in. zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, ochronę punktów końcowych, systemy uwierzytelniania oraz rozwiązania do zarządzania tożsamością.
- Analiza zidentyfikowanych zdarzeń oraz konfiguracji infrastruktury pod kątem występowania podatności technicznych.
- Analiza istniejących procedur monitorowania, wykrywania i obsługi incydentów bezpieczeństwa, z uwzględnieniem obowiązujących regulacji wewnętrznych oraz dobrych praktyk wynikających z norm i standardów bezpieczeństwa informacji.
- Określenie stopnia przygotowania infrastruktury oraz procesów organizacyjnych do wdrożenia usług Security Operations Center, ze wskazaniem braków technicznych, organizacyjnych i proceduralnych.
- Przygotowanie szczegółowych rekomendacji obejmujących:
    - proponowany model funkcjonowania SOC (wewnętrzny, zewnętrzny lub hybrydowy),
    - zakres monitorowanych systemów,
    - wymagane źródła logów,
    - rekomendowaną architekturę rozwiązania,
    - niezbędne działania organizacyjne i techniczne poprzedzające wdrożenie,
    - priorytety wdrożeniowe oraz harmonogram realizacji.
    - opracowanie listy działań mających na celu podniesienie poziomu cyberbezpieczeństwa, usunięcie zidentyfikowanych niezgodności oraz zwiększenie skuteczności monitorowania i reagowania na incydenty.
- Wykonawca sporządzi raport końcowy zawierający co najmniej:
    - charakterystykę analizowanego środowiska teleinformatycznego,

- zestawienie potencjalnych zagrożeń,
- ocenę aktualnego poziomu bezpieczeństwa infrastruktury,
- analizę gotowości do wdrożenia rozwiązania klasy SOC,
- rekomendacje techniczne, organizacyjne i proceduralne,
- podsumowanie oraz wnioski końcowe.

Raport końcowy powinien zostać przekazany w formie elektronicznej (format PDF oraz edytowalny DOCX) i stanowić kompletną dokumentację z przeprowadzonych prac. Dokument powinien zawierać jednoznaczne wnioski oraz rekomendacje umożliwiające Zamawiającemu podjęcie decyzji dotyczącej wdrożenia rozwiązania klasy Security Operations Center (SOC), zgodnie z najlepszymi praktykami w zakresie cyberbezpieczeństwa oraz obowiązującymi standardami.

4. Szczegółowy opis przedmiotu zamówienia w zakresie **przeprowadzenie testów socjotechnicznych** obejmuje czynności związane z realizacją zadania zgodnego z poniższymi wymaganiami:

   a) W ramach wykonywanych prac Wykonawca przeprowadzi kompleksową weryfikację wiedzy z zakresu przestrzegania zasad bezpieczeństwa informacji poprzez wykonanie testu socjotechnicznego.
   b) Wykonawca wspólnie z Zamawiający ustali szczegółowy scenariusz testu socjotechnicznego, który będzie odpowiadał na aktualne problemy związane z pracą Zamawiającego lub sytuacją społeczno – gospodarczą.
   c) Wykonawca przeprowadzi test socjotechniczny z dedykowanego adresu mailowego opartego na specjalnie założonej stronie internetowej pozwalającej na uwiarygodnienie wiadomości.
   d) Wykonawca zaprojektuje minimum jeden szablon wiadomości mailowej, która będzie wysyłana z dedykowanej strony internetowej.
   e) Zamawiający przekaże Wykonawcy adresy mailowe pracowników objętych testem.
   f) Wykonawca przeprowadzi wysyłkę wiadomości mailowych, przyjmując odpowiedni podział pracowników.
   g) W trakcie realizacji testu Wykonawca będzie odpowiedzialny za monitorowanie reakcji pracowników, analizowanie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami, a także wprowadzanie zmian w realizowanej kampanii, w celu zapewnienia efektywności testu.
   h) Wykonawca przeanalizuje wyniki testów oraz na tej podstawie opracuje raport, który zostanie przekazany Zamawiającemu, a następnie będzie stanowił podstawę do odpowiedniej analizy tematyki szkoleń i zostanie przedstawiony pracownikom podczas szkoleń.

5. Wszystkie podejmowane przez Wykonawcę działania w ramach realizacji usługi będą uzgadnianie z Zamawiającym na każdym etapie realizacji umowy.

Termin realizacji

§ 2

1. Termin rozpoczęcia realizacji przedmiotu umowy: dzień podpisania umowy.
2. Termin realizacji przedmiotu umowy: 18 września 2026 roku

Wynagrodzenie za przedmiot umowy

§ 3

1. Za prace określone w § 1 ust. 2 Wykonawca otrzyma wynagrodzenie ryczałtowe w wysokości netto **.....** zł (**słownie: .....**) plus należny podatek VAT obowiązujący na dzień

składania oferty w wysokości ……., co daje łącznie wynagrodzenie ryczałtowe brutto w wysokości: **…….** zł (słownie: **……**)

1. **Opracowanie wraz z wdrożeniem dokumentacji SZBI dla Urzędu Gminy w Starej Dąbrowie –** kwota netto: **……** zł (**słownie: ……**), kwota brutto: **……** zł (**słownie: ……**)
2. **Przeprowadzenie Audytu Krajowych Ram Interoperacyjności jako wymóg końcowego rozliczenia projektu –** kwota netto: **……** zł (**słownie: ……**), kwota brutto: **……** zł (**słownie: ……**)
3. **Przeprowadzenie testów socjotechnicznych –** kwota netto: **……** zł (**słownie: ……**), kwota brutto: **……** zł (**słownie: ……**)

2. Cena określona w ust. 1 zawiera wszystkie koszty związane z realizacją zamówienia w ramach przedstawionego zakresu prac i w tym zakresie nie może ulec zmianie w trakcie trwania umowy, za wyjątkiem ustawowej zmiany wysokości podatku VAT, w przypadku której strony zgodnie dopuszczają możliwość zmiany wynagrodzenia brutto. Zmiana stawki podatku VAT nie wymaga zmiany umowy.

Rozliczenie i termin płatności

§ 4

1. Wynagrodzenie za przedmiot umowy będzie wypłacone Wykonawcy w terminie 14 dni od daty otrzymania prawidłowo wystawionej faktury przez Zamawiającego.
2. Zapłata wynagrodzenia nastąpi przelewem na konto Wykonawcy podane na fakturze w terminie określonym w ust. 1 niniejszego paragrafu.

Obowiązki stron

§ 5

1. Wykonawca oświadcza, że posiada niezbędną wiedzę i doświadczenie niezbędne do zrealizowania przedmiotu umowy.
2. Wykonawca zobowiązuje się wykonać przedmiot umowy z należytą starannością uwzględniając całość wymagań Zamawiającego zawartych w umowie wraz z załącznikami, z zachowaniem zasad należytej staranności i profesjonalizmu.
3. Wykonawca zrealizuje przedmiot umowy przy ścisłej współpracy z Zamawiającym, świadcząc konsultacje telefoniczne, e-mailowe oraz spotkania w siedzibie Zamawiającego.
4. Wykonawca zobowiązuje się, że wykonane w ramach realizacji przedmiotu umowy prace, materiały i informacje oraz wykorzystywane przez niego oprogramowanie nie narusza praw osób trzecich, a w szczególności prawa autorskiego i praw pokrewnych.
5. Wykonawca ponosi odpowiedzialność za działania i zaniechania osób, którymi posłużył się przy wykonywaniu umowy, jak za własne działania czy zaniechania.
6. Zamawiający zobowiązany jest współpracować z Wykonawcą, udostępniając niezwłocznie wszelkie informacje i dokumentacje niezbędne do realizacji umowy będące w posiadaniu zamawiającego.

Odszkodowanie

§ 6

1. Wykonawca zapłaci Zamawiającemu kary umowne za:
   - zwłokę w wykonaniu przedmiotu umowy w wysokości 0,1% kwoty wynagrodzenia brutto za każdy dzień zwłoki,
   - zwłokę w usunięciu wad w wysokości 0,1% kwoty wynagrodzenia brutto za każdy dzień zwłoki, przed naliczeniem kary Zamawiający wyznaczy Wykonawcy okres nie krótszy niż 7 dni na usunięcie wad,
   - odstąpienie przez Wykonawcę od umowy z przyczyn zależnych od Wykonawcy w wysokości 10% kwoty wynagrodzenia brutto.
2. Zamawiający zapłaci Wykonawcy kary umowne za:
   - odstąpienie przez Zamawiającego od umowy z przyczyn zależnych od Zamawiającego w wysokości 10% kwoty wynagrodzenia brutto.
3. Wysokość kar umownych nie może przekroczyć 30% wartość wynagrodzenia określonego w § 3 pkt. 1 niniejszej umowy.
4. Termin zapłaty kar umownych ustala się na 14 dni od daty otrzymania wezwania.

Poufność

§ 7

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich informacji technicznych, technologicznych, prawnych, organizacyjnych oraz innych informacji zamawiającego uzyskanych w trakcie wykonywania umowy, niezależnie od formy pozyskania tych informacji i ich źródła.
2. Wykonawca zobowiązuje się do wykorzystania informacji wyłącznie w celach określonych ustaleniami umowy oraz wynikającymi z obowiązujących uregulowań prawnych.
3. Wykonawca zobowiązuje się do ujawnienia informacji jedynie tym osobom, którym będą one niezbędne do wykonywania powierzonych im czynności i tylko w zakresie, w jakim osoba musi mieć do nich dostęp dla celów realizacji zadania wynikającego z tytułu realizacji umowy.
4. Wykonawca zobowiązuje się do niekopiowania, niepowielania, ani w jakikolwiek inny sposób nierozpowszechniania jakiejkolwiek części określonych informacji, z wyjątkiem uzasadnionej potrzeby do celów związanych z realizacją umowy po uprzednim uzyskaniu pisemnej zgody od zamawiającego, którego informacja lub źródło informacji dotyczy.
5. Obowiązek określony w ust. 1 nie dotyczy informacji powszechnie znanych lub udostępnianych na podstawie bezwzględnie obowiązujących przepisów prawa, a w szczególności na żądanie sądów, prokuratury, organów podatkowych lub organów kontrolnych, jak również informacji dostępnych publicznie, o których mowa w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej.
6. Wykonawca ponosi odpowiedzialność za zachowanie w poufności informacji przez swoich pracowników, podwykonawców i wszelkich innych osób, którymi będzie się posługiwać przy wykonywaniu umowy.
7. Wykonawca zobowiązuje się do podjęcia wszelkich niezbędnych kroków, aby zapewnić, że żaden pracownik wykonawcy lub inna osoba, o której mowa w ust. 6, otrzymująca powyższe informacje, nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części osobom lub podmiotom trzecim

bez uzyskania uprzednio wyraźnej pisemnej zgody zamawiającego, którego informacja lub źródło informacji dotyczy.

8. Obowiązek zachowania w poufności informacji przez wykonawcę i osoby, o których mowa w ust. 6, obowiązuje także po ustaniu umowy.
9. Wykonawca odpowiada za szkodę wyrządzoną zamawiającemu przez ujawnienie, przekazanie, wykorzystanie, zbycie lub oferowanie do zbycia informacji otrzymanych od zamawiającego, wbrew postanowieniom umowy. Zobowiązanie to wiąże wykonawcę również po wykonaniu przedmiotu umowy, jej rozwiązaniu, wygaśnięciu lub odstąpieniu, bez względu na przyczynę.
10. Wykonawca oświadcza, że każda z osób uczestniczących w realizacji przedmiotu umowy zobowiązała się wobec niego, jako wykonawcy, nie ujawniać żadnych informacji, z którymi zapozna się podczas wykonywania czynności zleconych do realizacji oraz zapoznała się z treścią ww. przepisów i zobowiązała się do ich przestrzegania, zarówno w czasie realizacji umowy, jak i po jej zakończeniu.

Odstąpienie od umowy

§ 8

1. Odstąpienie od umowy następuje w formie pisemnej pod rygorem nieważności i wymaga uzasadnienia.
2. Zamawiający może odstąpić od umowy całości lub w części w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu okoliczności uzasadniających odstąpienie w przypadku:
   a) nienależytej realizacji przedmiotu zamówienia przez Wykonawcę,
   b) co najmniej 20 dniowej zwłoki Wykonawcy w stosunku do terminu określonego w § 2 ust. 2 umowy,
   c) gdy Wykonawcy zostały naliczone kary umowne przekraczające 20 % wynagrodzenia umownego brutto.

Możliwość wprowadzenia zmian w umowie

§ 9

1. Dopuszcza się możliwość zmiany terminu wykonania umowy lub jej części, ze względu na przyczyny będące następstwem okoliczności, za które odpowiedzialność ponosi Zamawiający oraz siły wyższej, przez którą należy rozumieć zdarzenie zewnętrzne o charakterze niezależnych od obu stron, którego strony nie mogły przewidzieć przed zawarciem umowy i którego nie można było uniknąć ani któremu strony nie mogły zapobiec przy zachowaniu należytej staranności.
2. Przedłużenie terminu wykonania umowy lub jej części, może nastąpić o okres trwania tych okoliczności, a jeżeli okres ten wywołał kolejne konsekwencje w zakresie terminu wykonania, także o okres niezbędny do zakończenia wykonywania jej przedmiotu w sposób należyty.

Ochrona danych osobowych

§ 10

1. Klauzula informacyjna dotycząca przetwarzania danych osobowych przez Zamawiającego:

1) Administratorem danych osobowych jest Gmina Stara Dąbrowa, z którą można skontaktować się mailowo: ug@staradabrowa.pl

2) W sprawach dotyczących przetwarzania danych osobowych, w tym realizacji praw związanych z przetwarzaniem danych, można się skontaktować z wyznaczonym inspektorem ochrony danych (IOD) mailowo: iod@staradabrowa.pl
3) Dane osobowe będą przetwarzane w celu realizacji umowy (art. 6 ust. 1 lit. b) oraz zgodnie z przepisami prawa w zakresie zamówień realizowanych ze środków publicznych.
4) Odbiorcami danych osobowych mogą być inni wykonawcy biorący udział w postępowaniu. Dane osobowe mogą być przekazane podmiotom i osobom, które uprawnione są do ich otrzymania przepisami prawa. Ponadto mogą być one ujawnione podmiotom, z którymi administrator danych zawarł umowę na świadczenie usług, w ramach których odbywa się przetwarzanie danych osobowych.
5) Dane osobowe będą przechowywane przez okres zgodny z obowiązującymi przepisami archiwalnymi, tj. m.in. ustawą z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz rozporządzeniem Prezesa Rady Ministrów z 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.
6) Przysługuje Pani/Panu prawo do: dostępu do swoich danych oraz otrzymania ich kopii; prawo do sprostowania (poprawiania) swoich danych; prawo do usunięcia danych osobowych; ograniczenia przetwarzania danych osobowych; przenoszenia danych; wniesienia sprzeciwu wobec przetwarzania danych osobowych. Przepisy odrębne mogą wyłączyć możliwość skorzystania z wymienionych uprawnień.
7) Przysługuje Pani/Panu prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, adres: ul. Stawki 2, 00-193 Warszawa.
8) Podanie danych osobowych jest obowiązkowe, gdyż przesłankę przetwarzania danych osobowych stanowi przepis prawa. Nie podanie wymaganych danych może w konsekwencji doprowadzić do niepodpisania umowy.

Postanowienia końcowe

§ 11

1. Spory wynikłe na tle realizacji niniejszej umowy, rozstrzygane będą przez Sąd Powszechny właściwy dla Zamawiającego.
2. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy, kodeksu cywilnego, ustawy o prawie autorskim i prawach pokrewnych oraz aktów wykonawczych do tych ustaw.
3. Wszelkie zmiany niniejszej umowy wymagają dla swej ważności formy pisemnej pod rygorem nieważności.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

Zamawiający: **Wykonawca:**

....