



## Cyberbezpieczny Samorząd

Sępólno Krajeńskie, 12.05.2026 r.

Znak sprawy: IRG.271.1.12.2026

Zamawiający: **Gmina Sępólno Krajeńskie**

ul. Tadeusza Kościuszki 11, 89-400 Sępólno Krajeńskie

### ZAPYTANIE OFERTOWE

*Dotyczy:* projektu pn. „**Poprawa Cyberbezpieczeństwa w Gminie Sępólno Krajeńskie**”, dofinansowanego w ramach programu grantowego „Cyberbezpieczny Samorząd” z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

#### **I. NAZWA PRZEDMIOTU ZAMÓWIENIA**

**ZADANIE I:** Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI w tym: Polityka Bezpieczeństwa Informacji, Polityka ochrony danych osobowych, Polityka zarządzania systemem informatycznym, Polityka zarządzania ciągłością działania, Procedura zarządzania incydentami cyberbezpieczeństwa, Przeprowadzenie Analizy Ryzyka Systemu Zarządzania Bezpieczeństwem Informacji, Przygotowanie dokumentacji zgodnie z wymogami ustawy o KSC dla **Urzędu Miejskiego w Sępólnie Krajeńskim**

**ZADANIE II:** Przeprowadzenie Audytu Bezpieczeństwa Informacji zgodnie z przepisami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 roku w sprawie Krajowych Ram Interoperacyjności oraz końcowej ankiety dojrzałości cyberbezpieczeństwa dla **Urzędu Miejskiego w Sępólnie Krajeńskim oraz jednostek podległych tj. Centrum Usług Społecznych; Centrum Małego Dziecka i Rodziny; Centrum Sportu i Rekreacji**

#### **Kody CPV:**

72150000-1 Usługi doradztwa w zakresie audytu komputerowego oraz sprzętu komputerowego

79417000-0 Usługi doradcze w zakresie bezpieczeństwa

#### **II. POSTANOWIENIA OGÓLNE**

Do udzielenia przedmiotowego zamówienia nie stosuje się przepisów Ustawy z dnia 11 września 2019r.- Prawo zamówień publicznych.

#### **III. OPIS PRZEDMIOTU ZAMÓWIENIA**

**ZADANIE I:** Przedmiotem zamówienia jest Przygotowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w tym: Polityka Bezpieczeństwa Informacji, Polityka ochrony danych osobowych, Polityka zarządzania systemem informatycznym, Polityka zarządzania ciągłością działania, Procedura zarządzania incydentami cyberbezpieczeństwa, Przeprowadzenie Analizy Ryzyka Systemu Zarządzania Bezpieczeństwem Informacji, Przygotowanie dokumentacji zgodnie z wymogami ustawy o KSC dla Urzędu Miejskiego w Sępólnie Krajeńskim



## Cyberbezpieczny Samorząd

### Zakres zadania:

W ramach realizacji przedmiotu zamówienia wykonawca opracuje dokumenty Systemu Zarządzania Bezpieczeństwem Informacji. Dokumentacja SZBI będzie wykonana w oparciu o:

- rozporządzenie Rady Ministrów z dnia 21 maja 2024 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773) (w zakresie dotyczącym bezpieczeństwa informacji),
- 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),
- ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

### Etapy realizacji usługi:

- 1) Etap I: „Polityka Bezpieczeństwa Informacji jako podstawowy element systemu zarządzania bezpieczeństwem informacji” obejmuje następujące czynności:**
  - a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Bezpieczeństwa Informacji realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
  - b) przygotowanie i przekazanie Polityki Bezpieczeństwa Informacji;
  - c) doradztwo we wdrożeniu Polityki Bezpieczeństwa Informacji i bieżące wsparcie ekspertów przez czas trwania Umowy;
- 2) Etap II: „Polityka Zarządzania Systemem Teleinformatycznym” obejmuje następujące czynności:**
  - a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Systemem Informatycznym realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
  - b) przygotowanie i przekazanie Polityki Zarządzania Systemem Informatycznym wraz z Planami Ciągłości Działania w obszarze IT;
  - c) doradztwo we wdrożeniu Polityki Zarządzania Systemem Informatycznym i bieżące wsparcie ekspertów przez czas trwania Umowy;
- 3) Etap III: „Polityka Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT” obejmuje następujące czynności:**
  - a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Ciągłością Działania realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
  - b) przygotowanie i przekazanie Polityki Zarządzania Ciągłością Działania wraz z Planami Ciągłości Działania w obszarze IT;
  - c) doradztwo we wdrożeniu Polityki Zarządzania Ciągłością Działania i bieżące wsparcie ekspertów przez czas trwania Umowy;
- 4) Etap IV: „Polityka Zarządzania Incydentami Cyberbezpieczeństwa” obejmuje następujące czynności:**
  - a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Zarządzania Incydentami Cyberbezpieczeństwa realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;



## Cyberbezpieczny Samorząd

- b) przygotowanie i przekazanie Polityki Zarządzania Incydentami Cyberbezpieczeństwa;
  - c) przygotowanie i przekazanie Planu Reagowania na Incydenty;
  - d) przygotowanie i przekazanie Planu Zarządzania Podatnościami;
  - e) doradztwo we wdrożeniu dokumentacji i bieżące wsparcie ekspertów przez czas trwania Umowy;
- 5) ***Etap V: „Polityka Ochrony Danych” obejmuje następujące czynności:***
- a) konsultacje z przedstawicielem Zamawiającego w celu przygotowania dedykowanej Polityki Ochrony Danych realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
  - b) przygotowanie i przekazanie Polityki Ochrony Danych;
  - c) doradztwo we wdrożeniu Polityki Ochrony Danych i bieżące wsparcie ekspertów przez czas trwania Umowy;
- 6) ***Etap VI: „Analiza Ryzyka Bezpieczeństwa Informacji” obejmuje następujące czynności:***
- a) konsultacje z przedstawicielem Zamawiającego w celu przeprowadzenia analizy ryzyka realizowane w formie on-line/wizyty stacjonarnej w siedzibie Zamawiającego;
  - b) przygotowanie i przekazanie Raportu z przeprowadzonej analizy ryzyka wraz z omówieniem obszarów o podniesionym ryzyku wraz z rekomendacjami ekspertów.
- 7) ***Etap VII: W ramach realizowanej usługi, ponad czynności o których mowa w pkt 1-6, zostaną przygotowane przez Wykonawcę lub dostosowane w przypadku ich posiadania przez Zamawiającego, następujące dokumenty:***
- a) procedury korzystania z urządzeń mobilnych,
  - b) procedury pracy zdalnej,
  - c) postępowanie z nośnikami,
  - d) procedury kontroli dostępu,
  - e) zabezpieczenie pomieszczeń i obiektów,
  - f) procedury czystego biurka,
  - g) procedury czystego ekranu,
  - h) procedury kopii zapasowych,
  - i) procedury ochrony logów,
  - j) bezpieczeństwo komunikacji,
  - k) zarządzanie bezpieczeństwem sieci,
  - l) przesyłanie informacji,
  - m) plany ciągłości działania,
  - n) procedury zarządzania incydentami,
  - o) prywatność i ochrona danych osobowych,
  - p) szacowanie ryzyka w obszarze bezpieczeństwa informacji,
  - q) szkolenia personelu,
  - r) plan zarządzania podatnościami,
  - s) plan reagowania na incydenty,
  - t) plan przywracania.

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami oraz wszelkich innych informacji uzyskanych w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji.

**ZADANIE II:** Przedmiotem zamówienia jest Przeprowadzenie Audytu Bezpieczeństwa Informacji zgodnego z przepisami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 roku w sprawie



## Cyberbezpieczny Samorząd

Krajowych Ram Interoperacyjności oraz końcowej ankiety dojrzałości cyberbezpieczeństwa dla Urzędu Miejskiego w Sępólnie Krajeńskim oraz jednostek podległych tj. Centrum Usług Społecznych; Centrum Małego Dziecka i Rodziny; Centrum Sportu i Rekreacji

Zakres zadania:

- 1) weryfikacja zgodności przyjętych procedur z przepisami 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 (t. j. Dz. U. 2024 r., poz. 773);
- 2) weryfikacja zgodności przyjętych procedur z zakresu cyberbezpieczeństwa wynikających z obowiązków określonych w przepisach Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r., poz. 913,);
- 3) weryfikacja zgodności przyjętych procedur z przepisami z zakresu ochrony danych wynikających z obowiązków określonych w przepisach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych Dz. U. UE. L. 2016, poz. 119.1 i 2. – dalej „RODO”) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781);
- 4) testy podatności infrastruktury teleinformatycznej;
- 5) audyt infrastruktury sieciowej;
- 6) przygotowanie i przekazanie raportu z Audytu końcowego;
- 7) omówienie wyników Audytu końcowego oraz wydanie rekomendacji Zamawiającemu
- 8) Przeprowadzenie ankiety dojrzałości cyberbezpieczeństwa w oparciu o załącznik nr. 6 umieszczony na stronie <https://www.gov.pl/web/cppc/cyberbezpieczny-samorząd>

### III. TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania przedmiotu zamówienia:

**ZADANIE I: do 45 dni od dnia udzielenia zamówienia**

**ZADANIE II: do 15 dni od dnia protokolarnego przekazania zrealizowanego ZADANIA I**

### IV. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. W postępowaniu mogą wziąć udział wykonawcy, którzy są zdolni do wykonania przedmiotu zamówienia i spełniają warunki w zakresie:

a) posiadania kompetencji/uprawnień do prowadzenia działalności zawodowej, o ile wynika to z odrębnych przepisów – złożyć w tym zakresie oświadczenie na formularzu ofertowym;



## Cyberbezpieczny Samorząd

- b) sytuacji finansowej umożliwiającej realizację przedmiotu zamówienia – złożyć w tym zakresie oświadczenie na formularzu ofertowym;
- c) posiadania potencjału technicznego i osobowego niezbędnego do wykonania przedmiotu zamówienia – złożyć w tym zakresie oświadczenie na formularzu ofertowym;
- d) **posiadania wiedzy i doświadczenia w wykonywaniu przedmiotu zamówienia - złożyć w tym zakresie potwierdzenie doświadczenia na bazie załącznika nr 4 i złożyć dokumenty potwierdzające min. 2-letnie doświadczenie w przeprowadzeniu audytów z zakresu cyberbezpieczeństwa** w postaci poświadczenia lub innych dowodów potwierdzających posiadanie doświadczenia. W przypadku gdy Wykonawca nie złoży, lub złoży niewystarczające dowody posiadania doświadczenia, Zamawiający zwróci się o ich uzupełnienie do Wykonawcy, którego oferta została oceniona jako najkorzystniejsza.
- e) **dysponowania min. 1 osobą posiadającą certyfikat: audytor wewnętrzny lub zewnętrzny normy PN-ISO/IEC 27001, lub CISA, lub CIA lub równoważne poświadczenia/ certyfikaty z zakresu cyberbezpieczeństwa**- złożyć w tym zakresie potwierdzenie dysponowania osobą na bazie załącznika nr. 4 i złożyć wraz z formularzem ofertowym dokumenty potwierdzające posiadanie certyfikatu. W przypadku gdy Wykonawca nie złoży, lub złoży niewystarczające dowody posiadania doświadczenia, Zamawiający zwróci się o ich uzupełnienie do Wykonawcy, którego oferta została oceniona jako najkorzystniejsza
- f) złożyć formularz ofertowy według wzoru stanowiącego załącznik nr 1 do zapytania ofertowego.

2. O zamówienie mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu:

- a) na podstawie przesłanek wynikających z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego na co złożyć wraz z formularzem ofertowym oświadczenia według wzoru stanowiącego załącznik nr 3 do zapytania ofertowego;
- b) w związku i istnieniem powiązań kapitałowych lub osobowych z Zamawiającym, zgodnie z treścią oświadczenia (załącznik nr 3)

*Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym (lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przeprowadzeniem procedury wyboru wykonawcy) a wykonawcą, polegające w szczególności na:*

- uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
- pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związaniu z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,
- pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.



## Cyberbezpieczny Samorząd

### V. POSTANOWIENIA DOTYCZĄCE PRZEDMIOTU POSTĘPOWANIA ORAZ WARUNKI SZCZEGÓŁOWE

**Termin realizacji zamówienia:**

**Dla ZADANIA I:** wynosi do 45 dni kalendarzowych od podpisania umowy, a za jego zakończenie rozumiane jest protokolarne przekazanie dokumentacji SZBI. Brak wykonania zadania w terminie 45 dni kalendarzowych od dnia podpisania umowy, upoważnia Zamawiającego do odstąpienia od zamówienia.

**Dla ZADANIA II:** wynosi do 15 dni kalendarzowych od dnia protokolarnego przekazania zrealizowanego ZADANIA I, a za jego zakończenie rozumiane jest protokolarne przekazanie audytów oraz ankiet dojrzałości cyberbezpieczeństwa. Brak wykonania zadania w terminie 15 dni kalendarzowych od dnia protokolarnego przekazania zrealizowanego ZADANIA I, upoważnia Zamawiającego do odstąpienia od zamówienia.

Dopuszcza się wykonanie zamówienia w trybie stacjonarnym lub online. Zakończenie prac musi zostać potwierdzone protokołami odbioru, podpisanymi przez Wykonawcę i Zamawiającego.

Rozliczenia między Zamawiającym, a Wykonawcą będą następować na podstawie faktur częściowych po zrealizowaniu każdego z zadań odrębnie, z terminem płatności 30 dni każda. Rozliczenia między Zamawiającym, a Wykonawcą będą prowadzone w złotych polskich (PLN).

Zamawiający nie wymaga wniesienia wadium ani zabezpieczenia należytego wykonania umowy.

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

Postępowanie jest prowadzone w języku polskim. Zamawiający nie dopuszcza złożenia ofert w innym języku.

Wykonawca ma prawo złożyć tylko jedną ofertę.

Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.

**Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podania przyczyny.**

### VI. TERMIN SKŁADANIA I OTWARCIA OFERT.

Oferty stanowiące odpowiedź na niniejsze postępowanie należy złożyć na załączonym formularzu oferty (załącznik nr 1 do postępowania) poprzez adres email: [zamowienia@gmina-sepolno.pl](mailto:zamowienia@gmina-sepolno.pl) w terminie do **20.05.2026 r., do godz. 11:00**

Do formularza oferty należy dołączyć Oświadczenie o braku podstaw wykluczenia (załącznik nr 3 do zapytania ofertowego) oraz potwierdzenie doświadczenia (załącznik nr 4). Wykonawca, który nie złoży w/w dokumentu z ofertą, zostanie wezwany o jego uzupełnienie przed potencjalnym złożeniem zamówienia.



## Cyberbezpieczny Samorząd

**Ofertę wraz pozostałymi załącznikami należy podpisać przez osobę upoważnioną z ramienia Wykonawcy**

Oferty złożone lub przesłane po tym terminie zostaną odrzucone

O zachowaniu terminu decyduje data wpływu oferty do Zamawiającego. Oferty, które wpłyną po wskazanym terminie nie będą rozpatrywane.

1. Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.

W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.

### **VII. OCENA OFERT**

Wybór najkorzystniejszej oferty nastąpi w oparciu o kryterium: najniższa cena - 100% cena

### **VIII. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY**

O wyborze najkorzystniejszej oferty Zamawiający zawiadomi wykonawcę mailowo.

**Zamawiający zastrzega sobie możliwość unieważnienia postępowania bez podania przyczyny.**

### **IX. Klauzula informacyjna z art. 13 RODO:**

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „Rozporządzenie”, informuję, że:

1. Administratorem Pani/Pana danych osobowych jest Gmina Sępólno Krajeńskie reprezentowana przez Burmistrza Sępólna Krajeńskiego z siedzibą przy ul. T. Kościuszki 11, 89-400 Sępólno Krajeńskie, tel. /52/ 389 42 30, e-mail: [sekretariat@gmina-sepolno.pl](mailto:sekretariat@gmina-sepolno.pl).
2. W sprawach z zakresu ochrony danych osobowych może się Pani/Pan kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: [iodo@gmina-sepolno.pl](mailto:iodo@gmina-sepolno.pl).
3. Pani/Pana dane osobowe będą przetwarzane w celu związanym z postępowaniem prowadzonym z wyłączeniem przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz.U. z 2024 r., poz. 1320 z późn. zm.).
4. Pani/Pana dane osobowe będą przetwarzane przez okres 5 pełnych lat kalendarzowych, licząc od 1 stycznia roku następnego po roku, w którym nastąpiło zakończenie sprawy (6 lat) na podstawie Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.



## Cyberbezpieczny Samorząd

5. Podstawą prawną przetwarzania Pani/Pana danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia w związku z przepisami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2025 r. poz. 1483 z późn. zm.).
6. Pani/Pana dane osobowe będą ujawniane osobom działającym z upoważnienia administratora, mającym dostęp do danych osobowych i przetwarzającym je wyłącznie na polecenie administratora, chyba że wymaga tego prawo UE lub prawo państwa członkowskiego. Pani/Pana dane mogą zostać przekazane podmiotom zewnętrznym na podstawie umowy powierzenia przetwarzania danych osobowych - dostawcy usług poczty mailowej, strony BIP, dostawcy usług informatycznych w zakresie programów księgowo-ewidencyjnych.
7. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych związanym z udziałem w postępowaniu; konsekwencją niepodania danych jest brak możliwości udziału w postępowaniu.
8. Osoba, której dane dotyczą ma prawo do:
  - dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania,
  - w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów Rozporządzenia służy prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.
9. Osobie, której dane dotyczą nie przysługuje:
  - w związku z art. 17 ust. 3 lit. b, d lub e Rozporządzenia prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 Rozporządzenia;
  - na podstawie art. 21 Rozporządzenia prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c Rozporządzenia.
10. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.
11. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 Rozporządzenia, nie może skutkować zmianą wyniku postępowania ani zmianą postanowień umowy.
12. Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 Rozporządzenia, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania.
13. Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 ust. 1 Rozporządzenia, spowoduje



## Cyberbezpieczny Samorząd

ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, Administrator nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 Rozporządzenia.

14. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.
15. Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 Rozporządzenia, nie może naruszać integralności protokołu oraz jego załączników.
16. Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 Rozporządzenia.

### **X. WYKAZ ZAŁĄCZNIKÓW**

Załącznik nr 1 Formularz oferty.

Załącznik nr 2 Wzór umowy.

Załącznik nr 3 Oświadczenia.

Załącznik nr 4 Potwierdzenie doświadczenia.

Załącznik nr 5 Klauzula informacyjna FERC

Załącznik nr 6 Wzór umowy powierzenia przetwarzania danych osobowych