

Nowy Dwór Gdański, 12 maja 2026 r.

ZAPYTANIE OFERTOWE

na

Organizację i przeprowadzenie szkoleń z zakresu zarządzania urządzeniami Fortigate (szkolenie FortiOs Administrator dla 2 osób) oraz zarządzania bezpieczeństwem w środowisku MS Windows Server i Windows 10/11 (1 osoba) dla Informatyków zatrudnionych w Starostwie Powiatowym w Nowym Dworze Gdańskim

w ramach projektu pn. „Cyberbezpieczny Powiat Nowodworski”

I. ZAMAWIAJĄCY

Powiat Nowodworski
ul. gen. Władysława Sikorskiego 23
82-100 Nowy Dwór Gdański
NIP 5792231171
REGON 192644808
tel. 55 247 36 71

II. TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie przeprowadzone jest zgodnie z Regulaminem udzielania zamówień publicznych o wartości mniejszej niż 170.000,00 złotych netto wprowadzonym Zarządzeniem Nr 71/2025 Starosty Nowodworskiego z dnia 19 grudnia 2025 r. w sprawie uchwalenia regulaminu udzielania zamówień publicznych przez Powiat Nowodworski realizowanych w Starostwie Powiatowym w Nowym Dworze Gdańskim, o wartości mniejszej niż 170 000,00 zł netto.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

Organizacja i przeprowadzenie szkoleń:

1. Szkolenie FortiOS Administrator dla informatyka (2 osoby).
2. Szkolenie z zarządzania bezpieczeństwem w środowisku MS Windows Server i Windows 10/11 (1 osoba).

Powyższe szkolenia przeznaczone są dla informatyków zatrudnionych w Starostwie Powiatowym w Nowym Dworze Gdańskim i mają na celu podniesienie kompetencji kadry i podniesienie poziomu bezpieczeństwa informatycznego w Starostwie Powiatowym w Nowym Dworze Gdańskim w ramach grantu pn. „Cyberbezpieczny Powiat Nowodworski”.

1. Terminy szkoleń:

- a) Szkolenia zostaną przeprowadzone w dni robocze w terminie do 26 czerwca 2026 r.
- b) Szkolenia zostaną przeprowadzone w języku polskim lub angielskim.
- c) Ostateczny termin każdego ze szkoleń zostanie uzgodniony z Zamawiającym za pośrednictwem poczty elektronicznej pod adresem informatyk@nowydworgdanski.pl – co najmniej 1 tydzień przed planowanym terminem szkolenia.

2. Opis zakresu szkoleń:

I szkolenie - Szkolenie FortiOS Administrator

Typ szkolenia: Zdalne (wykład+ćwiczenia praktyczne). Wymagane minimum 12 godzin wykładów oraz minimum 10 godzin ćwiczeń praktycznych.

Zakres szkolenia powinien obejmować przynajmniej poniższe zagadnienia administrowania urządzeniami FortiGate z FortiOS w najnowszej dostępnej wersji w dniu składania ofert. Po ukończeniu kursu uczestnik będzie w stanie:

- 1) Skonfigurować podstawowe ustawienia sieciowe FortiGate od ustawień fabrycznych
- 2) Skonfigurować i kontrolować dostęp administratora do FortiGate
- 3) Korzystać z GUI i CLI do administracji
- 4) Opisać metody rejestracji urządzeń
- 5) Wyświetlać i wyszukiwać logi na FortiGate i FortiAnalyzer
- 6) Konfigurować polityki firewall dla IPv4
- 7) Stosować przekierowanie portów, NAT źródłowy i NAT docelowy
- 8) Analizować tablicę routingu FortiGate
- 9) Konfigurować routing statyczny
- 10) Implementować redundancję tras i równoważenie obciążenia
- 11) Skonfigurować zdalne serwery uwierzytelniania LDAP i RADIUS na FortiGate
- 12) Monitorować użytkowników firewall z poziomu GUI FortiGate
- 13) Wdrażać Fortinet Single Sign-On (FSSO) zintegrowany z Microsoft Active Directory (AD)
- 14) Opisać funkcje szyfrowania i certyfikaty
- 15) Opisać inspekcję SSL na FortiGate
- 16) Konfigurować profile bezpieczeństwa neutralizujące zagrożenia i niewłaściwe użycie,

w tym wirusy, torrenty i nieodpowiednie strony WWW

- 17) Stosować techniki kontroli aplikacji do monitorowania i kontrolowania ruchu aplikacyjnego, również na niestandardowych portach i protokołach
- 18) Konfigurować tunele IPsec VPN za pomocą kreatora i metodą manualną
- 19) Konfigurować SD-WAN i weryfikować dystrybucję ruchu
- 20) Rozpoznawać zadania urządzenia głównego i zapasowego w klastrze HA
- 21) Identyfikować różne tryby działania HA z wykorzystaniem protokołu FGCP
- 22) Diagnozować i korygować typowe problemy
- 23) Identyfikować FortiGate VM oraz FortiGate CNF w chmurze
- 24) Identyfikować FortiSASE oraz jego zastosowania

Wymagania dodatkowe dotyczące szkolenia FortiOS Administrator:

- 1) Szkolenie powinno przygotowywać do egzaminu FCP – FortiOS.
- 2) Uczestnik otrzyma certyfikat ukończenia szkolenia podpisany przez Fortinet.

II szkolenie – Zarządzanie bezpieczeństwem w środowisku MS Windows Server oraz Windows 10/11

Typ szkolenia: Zdalne. Czas trwania minimum 5 dni (minimum 30 godzin).

Zakres szkolenia powinien zwiększać świadomość w zakresie zagrożeń i zarządzania bezpieczeństwem środowisk opartych o produkty serwerowe i klienckie systemy operacyjne firmy Microsoft.

Szkolenie obejmować przynajmniej poniższe zagadnienia:

- 1) Identyfikacja zagrożeń występujących w środowisku Windows wg norm ISO/IEC
 - a) Klasyfikacja współczesnych zagrożeń
 - b) Zakres systemu zarządzania bezpieczeństwem
- 2) Bezpieczne uwierzytelnianie i ochrona poświadczeń w systemie Windows

- a) Przegląd metod uwierzytelniania
 - b) Analiza ryzyka procesu uwierzytelniania
 - c) Ataki typu Offline - eskalacja uprawnień
 - d) Ataki Pass-the-hash i Pass-the-Ticket
 - e) Legacy LAPS i Windows LAPS
 - f) Zarządzanie politykami haseł domenowych z uwzględnieniem PSO
 - g) Zarządzalne konta serwisowe (gMSA)
 - h) Credential Guard
 - i) Tymczasowa przynależność do grup zabezpieczeń ADDS (Just in Time Administration)
- 3) Autoryzacja dostępu do zasobów
 - a) Kontrola i inspekcja dostępu na podstawie ACL
 - b) Projektowanie zaawansowanych zasad inspekcji
 - c) Autoryzacja oparta na oświadczeniach
 - 4) Kontrola praw i uprawnień użytkowników
 - a) Przegląd i konfiguracja uprawnień użytkowników
 - b) Optymalizacja narzędzia UAC
 - c) Restrykcje dotyczące korzystania z nośników zewnętrznych
 - d) Reguły AppLocker dotyczące uruchamianego oprogramowania
 - e) Limitowane sesje PowerShell (Just Enough Administration)
 - 5) Infrastruktura Klucza Publicznego
 - a) Planowanie, wdrożenie i utrzymanie roli AD CS
 - b) Metody dystrybucji i zarządzanie certyfikatami
 - c) Zabezpieczanie komunikacji – protokoły TLS i IPsec oraz rola Windows Defender Firewall with Advanced Security
 - d) Podpisywanie cyfrowe dokumentów MS Office i plików PDF
 - e) Podpisywanie skryptów PowerShell
 - 6) Uwierzytelnianie dwuskładnikowe
 - a) Przegląd infrastruktury kart inteligentnych i tokenów
 - b) Dwuskładnikowe uwierzytelnianie na stacjach roboczych
 - 7) Szyfrowanie danych w oparciu o dobre praktyki
 - a) Bitlocker i Bitlocker To Go

- b) Encrypted File System
- 8) Network Policy Server (serwer zasad sieciowych)
 - a) Kontrola dostępu do sieci bezprzewodowych z wykorzystaniem serwera RADIUS
- 9) Analiza ruchu sieciowego
 - a) Działania mające na celu zabezpieczenie protokołu SMB
 - b) Zabezpieczenie systemu rozwiązywania nazw DNS
- 10) Konfiguracja uprawnień usług systemowych
- 11) Analiza bezpieczeństwa i hardening systemów
 - a) Zaawansowane monitorowanie bezpieczeństwa systemów w oparciu o Sysmon
 - b) Security Compliance Toolkit (SCT)
 - c) Restricted Groups
 - d) Tiering Active Directory
 - e) Polityki uwierzytelniania
 - f) Idea wykorzystania stacji uprzywilejowanego dostępu (PAW) oraz serwerów przesiadkowych (Jump servers)
- 12) Zarządzanie poprawkami systemowymi i omówienie mechanizmu Windows Update

Wymagania dodatkowe dotyczące szkolenia:

- 1) Uczestnik szkolenia Zarządzanie bezpieczeństwem w środowisku MS Windows Server i Windows 10/11 (on-premises) otrzyma certyfikat wystawiony imiennie.

IV. O udzielenie niniejszego zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki:

1. Informacje dotyczące wymagań w zakresie przeprowadzenia szkolenia:

- 1) Wykonawca w ramach otrzymanego wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres.
- 2) Certyfikaty dla osób uczestniczących w szkoleniu muszą być odpowiednio oznakowane, jednoznacznie wskazujące na projekt i źródło jego finansowania.
- 3) Czas trwania szkolenia:
FortiOS Administrator: minimum 12 godzin wykładów i minimum 10 godzin ćwiczeń praktycznych.

Szkolenie z zakresu zarządzania bezpieczeństwem w środowisku MS Windows Server i Windows 10/11 (on-premises): minimum 5 dni (minimum 30 godzin).

- 4) Wykonawca nie może bez zgody Zamawiającego przekazać w całości praw i obowiązków wynikających z treści niniejszej umowy na rzecz osób trzecich.
- 5) W realizacji zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. W ramach szkoleń przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane dokumentacje będą musiały być dostarczone w formie papierowej lub elektronicznej z możliwością powiększania treści.

2. Wymagania dotyczące Wykonawcy:

- 1) O udzielenia zamówienia może ubiegać się Wykonawca niepodlegający wykluczeniu spełniający warunki udziału w postępowaniu, tj.:
 - a) mający co najmniej 2 letnie doświadczenie w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń oraz w przygotowaniu i przeprowadzeniu szkoleń z zakresu zarządzania urządzeniami Fortigate, co Zamawiający zweryfikuje na podstawie oświadczenia Wykonawcy, zawartego w załączniku nr 1 – formularz ofertowy.
 - b) zrealizował przynajmniej 3 zamówienia obejmujące wykonanie szkoleń z zakresu zarządzania urządzeniami Fortigate oraz przynajmniej 3 zamówienia z zakresu zarządzania bezpieczeństwem w środowisku MS Windows Server i Windows 10/11, co Zamawiający zweryfikuje na podstawie wykazu usług zrealizowanych w okresie trzech ostatnich lat – wzór wykazu stanowi załącznik nr 3 do niniejszego zapytania ofertowego
 - c) dysponuje lub będzie dysponował co najmniej 1 trenerem, który będzie uczestniczył w realizacji zamówienia i który:
 - o posiada oficjalny certyfikat trenera (Fortinet Certified Trainer dla szkolenia FortiOS, Microsoft Certified Trainer dla szkolenia z zarządzania bezpieczeństwem w środowisku MS Windows Server i Windows 10/11)
 - o przeprowadził w okresie ostatnich dwóch lat przed upływem terminu składania ofert przynajmniej 20 godzin (zegarowych) szkoleń z zakresu opisanego w szczegółach każdego ze szkoleń. W przypadku wyznaczenia jednego trenera Zamawiający wymaga aby posiadał on udokumentowane doświadczenie w obu obszarach.
- 2) Na potwierdzenie spełnienia ww. warunków Wykonawca zobowiązany jest przedstawić:
 - a) wykaz usług zrealizowanych w okresie ostatnich trzech lat – wzór wykazu stanowi załącznik nr 3 do niniejszego zapytania ofertowego wraz z dokumentami potwierdzającymi ich wykonanie (referencje, protokoły, faktury etc.)
- 3) W przypadku szkoleń realizowanych poprzez Autoryzowane Centrum Szkoleniowe Fortinet (dla szkoleń Fortigate) oraz Partnera usług szkoleniowych firmy Microsoft (dla szkoleń z zarządzania bezpieczeństwem) Wykonawca może przedstawić odpowiednie certyfikaty lub listy certyfikowanych partnerów publikowane przez firmy Fortinet oraz Microsoft

potwierdzające iż jednostka prowadząca oferowane szkolenie posiada odpowiednie doświadczenie. W takim przypadku Zamawiający nie wymaga udokumentowania doświadczenia wspomnianego w pkt. 1) ppkt. b , pkt 1) ppkt. c) oraz w pkt. 2)

- 4) Wykonawca, który nie wykaże spełnienia warunków udziału w postępowaniu, podlegać będzie wykluczeniu z udziału w postępowaniu. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą.
- 5) Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Wykonawcę dokumentów, wykazów, danych i informacji.
- 6) O udzielenie zamówienia nie może ubiegać się Wykonawca w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w 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 (Dz. U. z 2025 r. poz. 514); Zamawiający wykluczy z postępowania wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:
 - a) uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej,
 - b) posiadaniu co najmniej 10% udziałów lub akcji, pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
 - c) 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.
- 7) Kody CPV: 80510000-2 Usługi szkolenia specjalistycznego.

V. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Oferent powinien stworzyć ofertę na formularzu załączonym do niniejszego zapytania ofertowego.
2. Do oferty należy dołączyć:
 - 1) Kompletny, wypełniony formularz ofertowy stanowiący **załącznik nr 1** do zapytania ofertowego,
 - 2) Oświadczenie o braku powiązań osobowych lub kapitałowych stanowiące załącznik nr 2 do zapytania ofertowego,
 - 3) Wykaz usług stanowiący załącznik nr 3 do zapytania ofertowego,
 - 4) Wykaz osób stanowiący załącznik nr 4 do zapytania ofertowego.

3. Oferta powinna:
 - 1) zawierać adres lub siedzibę oferenta, numer telefonu, numer NIP,
 - 2) być podpisana przez osobę upoważnioną/osoby upoważnione do reprezentowania Wykonawcy. Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie do jej reprezentowania nie wynika z dokumentów rejestrowych (KRS, CEiDG lub innego właściwego rejestru), Wykonawca dołączy do oferty odpowiednie pełnomocnictwo.
4. Wykonawca ma prawo złożyć tylko 1 ofertę. Złożenie przez Wykonawcę więcej niż 1 oferty, skutkuje odrzuceniem wszystkich ofert złożonych przez tego Wykonawcę.
5. Wszelkie koszty przygotowania oferty ponosi Wykonawca.
6. Nie przewiduje się zwrotu kosztów udziału w postępowaniu.
7. Wykonawca informuje Zamawiającego o informacjach zawartych w ofercie stanowiących tajemnicę przedsiębiorstwa.
8. Zamawiający nie dopuszcza składania ofert częściowych.
9. Zamawiający nie dopuszcza składania ofert wariantowych.
10. Zamawiający nie przewiduje udzielania zamówień uzupełniających.
11. Zamawiający zwraca uwagę, że szkolenia będące przedmiotem zamówienia mają charakter kształcenia zawodowego i są finansowane w całości ze środków publicznych, w związku z czym są one zwolnione z podatku od towarów i usług na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz.U. 2023 poz. 955).

VI. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

1. Ofertę wraz z załącznikami należy złożyć osobiście w sekretariacie pokój numer 20 Starostwa lub wysłać pocztą lub kurierem na adres Starostwo Powiatowe w Nowym Dworze Gdańskim ul. gen. Władysława Sikorskiego 23, 82-100 Nowy Dwór Gdański w terminie do **dnia 19.05.2026 r. do godziny 14.00, na kopercie wpisując „Szkolenia Fortigate „Cyberbezpieczny Powiat Nowodworski” z dopiskiem „Nie otwierać przed terminem składania ofert”**.
2. O terminowym złożeniu oferty decyduje data wpływu na wskazany powyżej adres.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
4. Oferta winna być sporządzona w języku polskim pod rygorem nieważności. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem przysięgłym na język polski.
5. **Zamawiający nie dopuszcza innej formy i sposobu składania ofert niż wskazany ust. 1.** Niespełnienie tego wymogu oznacza niezgodność oferty z Zapytaniem. Oferty złożone w inny sposób zostaną odrzucone przez Zamawiającego.

VII. OCENA OFERT

1. Przy wyborze oferty Zamawiający będzie się kierował następującym kryterium:

- 1) Jedynym kryterium oceny ofert (100%) będzie cena całkowita za wykonanie przedmiotu zamówienia, wynikająca z oferty sporządzonej przez Wykonawcę zgodnie z formularzem ofertowym, stanowiącym załącznik nr 1 do niniejszego zapytania.

W kryterium cena, ocena ofert zostanie przeprowadzona wg formuły:

$$\text{Otrzymane punkty} = \left(\frac{\text{Cena najniższa spośród złożonych ofert}}{\text{Cena badanej oferty}} \right) \times 100$$

2. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie przez Zamawiającego umowy z kolejnym Wykonawcą, który w postępowaniu uzyskał kolejną najwyższą liczbę punktów.
3. Zamawiający może w toku badania i oceny ofert żądać od Oferentów dodatkowych wyjaśnień dotyczących treści złożonych załączników do oferty.
4. Zamawiający wyjaśni i poprawi w formularzu ofertowym:
 - oczywiste omyłki pisarskie,
 - oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
 - inne omyłki polegające na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty.
6. Poprawienie przez Zamawiającego oczywistych omyłek pisarskich oraz rachunkowych konsekwencji rachunkowych dokonanych poprawek nie wymaga uzyskania zgody wykonawcy. Wykonawca może nie wyrazić zgody na poprawienie przez zamawiającego innych omyłek polegających na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Brak zgody Wykonawca musi wnieść na piśmie w wyznaczonym przez Zamawiającego terminie.
7. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, bez podania przyczyny, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.

VIII. WYNAGRODZENIE WYKONAWCY

Wynagrodzenie za wykonanie przedmiotu zamówienia nastąpi zgodnie z § 4 wzoru umowy stanowiącym załącznik nr 5 do zapytania ofertowego.

IX. KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH

1. W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy iż odrębnymi administratorami Państwa danych są:

- 1) Minister Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021- 2027 (dalej jako FERC) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
 - 2) Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Instytucji Pośredniczącej (IP) FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,
 - 3) Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.
 - 4) Powiat Nowodworski w zakresie w jakim pełni funkcje Grantobiorcy, Zamawiającego.
2. Powiat Nowodworski jako Zamawiający wyznaczył Inspektora Ochrony Danych Osobowych, Pana Jakuba Neumanna, z którym w sprawach dotyczących przetwarzania danych osobowych można skontaktować się za pośrednictwem poczty elektronicznej pod adresem iod@nowydworgdanski.pl lub poczty tradycyjnej na adres: Starostwo Powiatowe w Nowym Dworze Gdańskim ul. gen. Władysława Sikorskiego 23, 82-100 Nowy Dwór Gdański.
3. Administratorzy będą przetwarzać dane osobowe na podstawie:
- 1) art.6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia;
 - 2) art. 6 ust. 1 lit. c RODO w związku z przepisami:
art. 87 z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027) (tekst jednolity Dz.U. z 2024 r. poz. 1717),
 - a) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079 z późn. zm.),
 - b) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2024 r. poz. 572),
 - c) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2024 r. poz. 1530, z późn. zm.),
 - d) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027” z 2.02.2023 r.,
 - e) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405).
4. Powiat Nowodworski przetwarza jedynie dane osobowe niezbędne do realizacji określonego celu przetwarzania, w tym w szczególności:
- 1) imię, nazwisko, adres poczty elektronicznej, adres korespondencyjny, numer telefonu/faxu, adres zamieszkania, NIP, REGON – przekazane przez Wykonawcę będącego osobą fizyczną lub uzyskane z publicznego rejestru (CEIDG),
 - 2) imię, nazwisko, stanowisko służbowe, adres poczty elektronicznej, numer telefonu/faxu – pełnomocników oraz osób wskazanych przez Wykonawcę do kontaktu, zawarcia lub realizacji umowy,

5. inne dane osobowe przekazane przez Wykonawcę niezbędne do realizacji przedmiotu umowy.
6. Pani/Pana dane osobowe będą przechowywane przez okres wskazany w Umowie o powierzenie grantu zawartej przez Zamawiającego z Beneficjentem (Grantodawcą). Okres ten może zostać przedłużony do czasu upływu okresu przedawnienia ewentualnych roszczeń, jeśli przetwarzanie danych osobowych będzie niezbędne do dochodzenia lub obrony przed takimi roszczeniami.
7. Pani/Pana dane osobowe mogą być powierzane lub udostępniane:
 - 1) podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zleciliśmy wykonywanie zadań w ramach realizacji FERC,
 - 2) instytucji audytowej, o której mowa w art. 71 rozporządzenia Parlamentu Europejskiego Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizyjowej,
 - 3) instytucjom Unii Europejskiej (UE) lub podmiotom, którym UE powierzyła zadania dotyczące wdrażania FERC,
 - 4) podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.
8. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO.
9. Posiada Pani/Pan:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - 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 ^{**};
 - 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 Pani/Panu:
 - 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."

** Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień*

umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności 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 państw członkowskich.

X. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą.

XI. DODATKOWE INFORMACJE

1. Po stronie Zamawiającego osobą do kontaktów w sprawie zamówienia jest:
Pan Marcin Karbownik oraz Pan Krzysztof Firko
tel.: +48 55 247 36 71 wew. 171
e-mail: starostwo@nowydworgdanski.pl
2. W tytule wiadomości należy wpisać „Zapytanie Szkolenie Fortigate Administrator Cyberbezpieczny Powiat Nowodworski”.
3. Każdy Wykonawca ma prawo zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego. Pytania Wykonawców muszą być przekazane za pośrednictwem poczty elektronicznej na wyżej wskazany adres.
4. Zamawiający udzieli odpowiedzi najpóźniej na 2 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści zapytania ofertowego wpłynął do zamawiającego nie później niż 4 dni przed upływem terminu składania ofert.
5. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 4, przedłuży termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia oferty.
6. W przypadku, gdy wniosek o wyjaśnienie treści zapytania ofertowego nie wpłynął w terminie, o którym mowa w ust. 4, Zamawiający nie ma obowiązku udzielania wyjaśnień oraz obowiązku przedłużania terminu składania ofert.
7. Jeżeli zaoferowana cena będzie rażąco niska w stosunku do przedmiotu zamówienia lub będzie budziła wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego, Zamawiający zwróci się do Wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu będzie spoczywać na Wykonawcy.

8. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa powyżej lub jeżeli dokonana ocena tych wyjaśnień wraz ze złożonymi dowodami potwierdzi, że zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

XII. ZAŁĄCZNIKI

1. Załącznik nr 1 - Formularz ofertowy,
2. Załącznik nr 2 – Oświadczenie o braku powiązań,
3. Załącznik nr 3 – Wykaz usług,
4. Załącznik nr 4 – Wykaz osób,
5. Załącznik nr 5 – Wzór umowy,
6. Załącznik nr 6 – Klauzula informacyjna FERC.

WICESTAROSTA
(-)
Lubomir Głowacki