

Nowe, dnia 26.08.2025 r.

Gmina Nowe
Plac Św. Rocha 5
86-170 Nowe
Tel.: 523 337 210
E-mail: nowe@gminanowe.pl

Szacowanie wartości zamówienia

W celu oszacowania wartości zamówienia, zapraszamy Państwa do przedstawienia oferty na usługi doradcze w zakresie ustawy o KSC, opracowanie oraz wdrożenie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, audyt SZBI oraz ankieta końcowa dla Gminy i jednostek podległych w ramach projektu pn. „**Cyberbezpieczny samorząd**” Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC)

CPV 71621000-7 Usługi w zakresie analizy lub konsultacji technicznej

CPV 79417000-0 Usługi doradcze w zakresie bezpieczeństwa

CPV 79212000-3 Usługi audytu

CPV 79311000-7 Usługi w zakresie ankiet

KRI – Rozporządzenie Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
uoKSC – Ustawa z dnia 05.07.2018 r. o krajowym systemie cyberbezpieczeństwa

Przedmiotem szacowania jest wdrożenie SZBI, doradztwo ds. KSC oraz wdrożenie nowych procedur systemu zarządzania bezpieczeństwem informacji, audyt wdrożonego SZBI oraz ankieta końcowa.

Działania zaplanowane do realizacji w ramach projektu odnoszą się do Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2 pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

Przedmiot zamówienia składa się z następujących elementów:

1. Opracowanie oraz wdrożenie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI dla Urzędu Gminy i 2 jednostek podległych.

Zakres prac:

1) opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzi następujące dokumenty:

- a) Polityka Bezpieczeństwa Informacji;
- b) Polityka ochrony danych osobowych;
- c) Instrukcja zarządzania systemem informatycznym;

- d) Polityka zarządzania ciągłością działania;
- e) Procedura zarządzania incydentami cyberbezpieczeństwa
- f) Analiza ryzyka w zakresie Bezpieczeństwa Informacji;
- 2) 16 roboczogodzin konsultacji realizowanych w ramach doradztwa przy wdrożeniu dokumentacji SZBI (zakres ten może ulec zwiększeniu w zależności od potrzeb w ramach realizacji zamówienia)
- 3) W ramach dokumentacji SZBI ujęte zostaną następujące procedury:
 - 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

Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zleceniodawcy 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. Doradztwo dotyczące czynności wdrażających dokumentację nastąpi po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI.

2. Usługi doradcze w zakresie o Krajowym Systemie Cyberbezpieczeństwa – wspomagające prawidłowe wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym, opracowanie dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług

Zakres doradztwa:

- 1) Opracowanie procedury, w tym dokumentacji dotyczącej reagowania na incydenty
- 2) Pełnienie funkcji osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz wykonywania wobec tych podmiotów obowiązków
- 3) Świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CDIRT
- 4) Doradztwo w zakresie przekazanych zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa

- 5) Przygotowywanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń
- 6) Sporządzenie informacji dotyczących prawnych zagadnień bezpieczeństwa informacji oraz cyberbezpieczeństwa
- 7) Doradztwo w zarządzaniu incydentami oraz doradztwo w obsłudze incydentów
- 8) Opracowanie i aktualizacja broszury pozwalającej na zrozumienie zagrożenia w obszarze cyberbezpieczeństwa i stosowania praktycznych sposobów zabezpieczania się przed tymi zagrożeniami w związku z realizacją zadań publicznych z wykorzystaniem systemów informacyjnych.

3. Audyt wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji obejmujący zgodność z kryteriami zawartymi w par. 20 ust. 2 ww. rozporządzenia KRI wraz z przeprowadzeniem Ankiety Dojrzałości Cyberbezpieczeństwa w Urzędzie Gminy i 2 jednostkach podległych.

Zakres prac Audyt końcowy:

- 1) spotkanie otwierające Audyt końcowy;
- 2) 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);
- 3) 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);
- 4) 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);
- 5) testy podatności infrastruktury teleinformatycznej;
- 6) audyt infrastruktury sieciowej;
- 7) zamknięcie Audytu końcowego;
- 8) przygotowanie i przekazanie raportu z Audytu końcowego;
- 9) omówienie wyników Audytu końcowego oraz wydanie rekomendacji Zamawiającemu.
- 10) Opracowanie Ankiety Dojrzałości Cyberbezpieczeństwa - Ankieta stanowi Załącznik nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd”

W ramach opracowania i wdrożenia dokumentacji SZBI Wykonawca na podstawie ankiety dojrzałości, analizy ryzyka i przeglądu procedur oraz infrastruktury technicznej w Urzędzie Gminy i jednostkach podległych, opracuje i przedstawi do akceptacji przygotowane polityki, które powinny zawierać między innymi zakres, cele i wymogi prawne dotyczące ochrony informacji, role poszczególnych osób i ich odpowiedzialność oraz wykaz chronionych informacji. Polityki powinny dotyczyć takich obszarów jak: dane osobowe, system teleinformatyczny, sprzęt teleinformatyczny, zabezpieczenia fizyczne i oprogramowanie

zabezpieczające, podstawowe wymagania dla zachowania bezpieczeństwa, ciągłość działania, regulaminy i obowiązki dla pracowników. Przygotowana dokumentacja musi być zgodna z wymaganiami prawnymi w zakresie bezpieczeństwa informacji. Zamawiający ma prawo do wnoszenia uwag do przygotowanej dokumentacji.

Termin realizacji zamówienia:

Przedmiot zamówienia należy zrealizować przed końcem realizacji projektu wyznaczonym na dzień 30.06.2026 r.

Szczegółowy harmonogram prac i jego etapy zostaną ustalone z wybranym Wykonawcą.

Kryteria jakie będzie musiał spełniać potencjalny wykonawca usługi:

O zamówienie mogą ubiegać się wykonawcy, którzy:

1. Nie są powiązani osobowo lub kapitałowo z Zamawiającym poprzez:
 - a) uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
 - b) posiadanie co najmniej 10% udziałów lub akcji, (o ile niższy próg nie wynika z c) przepisów prawa)
 - d) pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
 - e) 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 Zamawiającym, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych Oferentów ubiegających się o udzielenie zamówienia
 - f) pozostawaniu z Zamawiającym w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia
2. Firma/osoba reprezentująca firmę nie została skazana za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia.
3. Nie podlegają wykluczeniu z postępowania oraz posiadający uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz.1999 z dnia 2018.10.18) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Potwierdzeniem spełnienia warunku posiadania ww. uprawnień będzie złożenie wraz z ofertą skanu oryginału certyfikatu.
4. Spełniają wymagania określone w Regulaminie projektu pn. „Cyberbezpieczny samorząd”
5. Prowadzą działalność na podstawie aktualnego wpisu do KRS lub CEIDG;
6. Nie podlegają wykluczeniu stosownie do art. 7 ust. 1 i 9 ustawy z dn. 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz.U. z 2023 r., poz. 1497).

Szacowana wycena usługi:

Prosimy o podanie szacunkowej ceny **netto** za podane poniżej poszczególne usługi.

Wykonawca może złożyć wycenę całościową lub na wybrane pozycje. Prosimy o jednoznaczne wskazanie, których pozycji dotyczy oferta.

Uprzejmie prosimy o przesłanie wyceny usługi drogą elektroniczną w terminie **do dnia 03.09.2025 r. do godz. 13:00** na adres e-mail: fundusze@gminanowe.pl

	Przedmiot zamówienia	Cena netto
1	Opracowanie oraz wdrożenie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI dla Urzędu Gminy i 2 jednostek podległych.	
2	Usługi doradcze w zakresie o Krajowym Systemie Cyberbezpieczeństwa – wspomagające prawidłowe wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym, opracowanie dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług	
3	Audyt wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji obejmujący zgodność z kryteriami zawartymi w par. 20 ust. 2 ww. rozporządzenia KRI wraz z przeprowadzeniem Ankiety Dojrzałości Cyberbezpieczeństwa w Urzędzie Gminy i 2 jednostkach podległych.	
	Łączna wartość zamówienia netto	

Zamawiający informuje, że przedmiotowe zaproszenie nie stanowi oferty w rozumieniu art. 66 KC ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz.U. z 2024 r. poz. 1320). Ma ono wyłącznie na celu rozeznanie cenowe rynku wśród firm mogących zrealizować powyższe zamówienie oraz uzyskanie wiedzy na temat szacunkowych kosztów związanych z planowanym zamówieniem publicznym.

Klauzula informacyjna FERC

W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy o zasadach przetwarzania Państwa danych osobowych:

Administrator danych

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 funkcję 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 funkcję Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.

4. Gmina Nowe reprezentowana przez Burmistrza z siedzibą Plac św. Rocha 5, 86-170 Nowe, tel.: 53 333 72 10, adres e- mail: nowe@gminanowe.pl.

Cel przetwarzania danych

Państwa dane osobowe będziemy przetwarzać w związku z realizacją FERC, w szczególności w związku z naborem 2.2 FERC. Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Podstawa przetwarzania

Będziemy przetwarzać Państwa dane osobowe w związku z tym, że:

1. Zobowiązuje nas do tego prawo (art. 6 ust. 1 lit. c RODO):
 - 1) art. 87 ustawy wdrożeniowej,
 - 2) 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),
 - 3) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),
 - 4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),
 - 5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027” z 2.02.2023 r.,
 - 6) 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),
2. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzoną nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
3. Przygotowujemy i realizujemy umowy, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

Rodzaje przetwarzanych danych

Możemy przetwarzać następujące rodzaje Państwa danych:

1. dane identyfikacyjne, wskazane w art. 87 ust. 2 pkt 1 ustawy wdrożeniowej, w tym: imię, nazwisko, adres, adres poczty elektronicznej, numer telefonu, numer faksu, PESEL, REGON, wykształcenie, identyfikatory internetowe,
2. dane związane z zakresem uczestnictwa osób fizycznych w projekcie, wskazane w art. 87 ust. 2 pkt 2 ustawy wdrożeniowej, w tym w szczególności: wynagrodzenie, formę i okres zaangażowania w projekcie,
3. dane osób fizycznych widniejące na dokumentach potwierdzających kwalifikowalność wydatków, wskazane w art. 87 ust. 2 pkt. 3 ustawy wdrożeniowej, m.in. numer rachunku bankowego, doświadczenie zawodowe, numer uprawnień budowlanych, numer księgi wieczystej,
4. dane dotyczące wizerunku i głosu osób uczestniczących w realizacji Programu lub biorących udział w wydarzeniach z nim związanych.

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację FERC w tym w szczególności od wnioskodawców, beneficjentów, partnerów.

Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy MFiPR oraz CPPC. Ponadto Państwa 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 rozporządzenie Parlamentu

Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i 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 Wizowej,

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.

Okres przechowywania danych

Będziemy przechowywać Państwa dane osobowe zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach, do momentu zakończenia realizacji przez IZ/IP/Beneficjenta wszelkich zadań związanych z realizacją i rozliczeniem FERC, z zastrzeżeniem przepisów, które mogą przewidywać dłuższy termin przeprowadzania kontroli, a ponadto przepisów dotyczących pomocy publicznej i pomocy *de minimis* oraz przepisów dotyczących podatku od towarów i usług.

Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. dostępu do swoich danych osobowych oraz otrzymania ich kopii (art. 15 RODO),
2. do sprostowania swoich danych (art. 16 RODO),
3. do usunięcia swoich danych (art. 17 RODO) - jeśli dotyczy,
4. do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. wniesienia sprzeciwu – wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO),
6. wniesienia skargi do organu nadzorczego (art. 77 RODO), tj. Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy prawa regulujące kwestię ochrony danych osobowych.

Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Przekazywanie danych do państwa trzeciego

Nie zamierzamy przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej zapewniamy, że odbędzie się to z zachowaniem warunków określonych w art. 45 lub 46 RODO.

Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez CPPC danych osobowych, prosimy kontaktować z Inspektorami Ochrony Danych Osobowych (dalej jako IOD) w następujący sposób:

1. IOD MFIPR:
 - 1) pocztą tradycyjną kierując korespondencję na adres: ul. Wspólna 2/4, 00-926 Warszawa,
 - 2) elektronicznie na adres e-mail: IOD@mfi.gov.pl,
2. IOD CPPC:
 - 1) pocztą tradycyjną kierując korespondencję na adres: ul. Spokojna 13A, 01-044 Warszawa,
 - 2) elektronicznie na adres e-mail: bezpieczenstwo@cppc.gov.pl.

3. IOD Gmina Nowe

- 1) pocztą tradycyjną kierując korespondencję na adres: ul. Plac Św. Rocha 5, 86-170 Nowe,
- 2) elektronicznie na adres e-mail: nowe@gminanowe.pl,

Podstawa prawna:

1. ustawa wdrożeniowa - ustawa 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),
2. RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE. L 119 z 4 maja 2016 r., s.1-88; Dz. Urz. UE L 127 z 23 maja 2018, str. 2 oraz Dz. Urz. UE L 74 z 4 marca 2021, str. 35).