



Luzino, dnia 18.12.2025 r.

Gmina Luzino
ul. Ofiar Stutthofu 11
82-242 Luzino

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 oraz audyt SZBI dla Gminy i jednostek podległych w ramach projektu grantowego 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

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 doradztwo ds. KSC oraz aktualizacja i wdrożenie nowych procedur systemu zarządzania bezpieczeństwem informacji oraz audyt wdrożonego SZBI

Wykonawca będzie zobowiązany do realizowania przedmiotu zamówienia w oparciu o wytyczne Regulaminu Konkursu Grantowego oraz zalecenia dotyczące projektu pn. „Cyberbezpieczny Samorząd” zamieszczone na stronie:

<https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad>.

Przedmiot zamówienia składa się z 3 zadań:



1. Usługi doradcze w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa
2. Opracowanie oraz wdrożenie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Gminy i jednostek podległych
3. Audyt wdrożonego Systemu Bezpieczeństwa Informacji obejmujący zgodność z kryteriami zawartymi w 20 ust. 2 ww. rozporządzenia KRI wraz z przeprowadzeniem Ankiety Dojrzałości Cyberbezpieczeństwa w JST

Termin realizacji zamówienia:

Przedmiot zamówienia należy zrealizować na miesiąc przed końcem realizacji projektu grantowego, tj. do 30.04.2025 r.

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

Kryteria jakie będzie musiał spełniać potencjalny wykonawca usługi

- I. Przedmiot zamówienia musi być realizowany przez osobę/y posiadającą/e:
 - 1) co najmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999) lub równoważne poświadczenia/ certyfikaty z zakresu cyberbezpieczeństwa,
 - 2) co najmniej 2-letnie doświadczenie zawodowe w opracowaniu i wdrożeniu lub aktualizacji i wdrożeniu SZBI oraz przeprowadzaniu audytów SZBI
 - 3) co najmniej 2-letnie doświadczenie zawodowe w prowadzeniu i wdrażaniu projektów w zakresie cyberbezpieczeństwa,
 - 4) doświadczenie w opracowaniu i wdrożeniu lub aktualizacji i wdrożeniu min. 1 SZBI.
- II. 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 przepisów prawa)
 - c) pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,



- d) pozostawanie 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
 - e) pozostawanie 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) 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.
 - 3) 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).
- I. Spełniają wymagania określone w Regulaminie projektu pn. „Cyberbezpieczny samorząd”
 - II. Prowadzą działalność na podstawie aktualnego wpisu do KRS lub CEIDG;

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Usługi doradcze w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa dla Gminy i 6 jednostek podległych

Gminy jako podmioty publiczne, są objęte przepisami ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i spoczywają na nich konkretne obowiązki w tym zakresie. Usługi doradcze mają na celu wsparcie gminy w spełnieniu tych wymogów i podniesieniu ogólnego poziomu cyberbezpieczeństwa.

I. Zakres usług doradczych w zakresie KSC dla gminy i jednostek podległych:

1) Analiza i ocena zgodności:

- o Audyt obecnego stanu bezpieczeństwa systemów informacyjnych i infrastruktury IT pod kątem zgodności z wymaganiami KSC oraz normą PN-ISO/IEC 27001.

2) Opracowanie procedury, w tym dokumentacji dotyczącej reagowania na incydenty, zarządzania ryzykiem, utrzymania wewnętrznej polityki bezpieczeństwa IT, a w szczególności:

- o **Polityki Bezpieczeństwa Informacji (PBI):** Główny dokument określający zasady, role, odpowiedzialność i ogólny zakres bezpieczeństwa w urzędzie.
- o **Procedury zarządzania ryzykiem:** Kluczowa dla KSC, pozwala zidentyfikować zagrożenia specyficzne dla gminy (np. ataki na systemy e-usług, wyciek danych osobowych) i dobrać adekwatne środki zaradcze.
- o **Procedury reagowania na incydenty:** Określa kroki postępowania w sytuacji naruszenia bezpieczeństwa – kto, kogo i w jakim czasie informuje, jak izolować zagrożenie i przywracać systemy do działania, co wejdzie w skład kompletnej dokumentacji wdrożenia SZBI.

3) Wsparcie w identyfikacji i klasyfikacji incydentów bezpieczeństwa Wsparcie w ocenie zdarzeń, ponieważ nie każde zdarzenie jest "incydentem", a incydenty podlegają różnej klasyfikacji (krytyczne, poważne, o niskim wpływie), co determinuje sposób i termin zgłaszania.

4) Świadczenie pomocy w przygotowywaniu zgłoszeń do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego – CSIRT. Wsparcie polega na pomocy w formalnym, terminowym i poprawnym zgłoszeniu incydentu zgodnie z obowiązującymi wzorami i kanałami komunikacji.

5) Doradztwo w zakresie przekazanych zaleceń pokontrolnych dotyczących usunięcia stwierdzonych nieprawidłowości, wydanych w protokole kontroli przez organ właściwy do spraw cyberbezpieczeństwa - Usługa ma na celu przełożenie często sformalizowanych zaleceń pokontrolnych na konkretne



działania techniczne i organizacyjne, możliwe do zrealizowania w warunkach samorządowych.

- 6) Przygotowywanie projektów informacji do organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń. Formalne zamknięcie procesu kontroli, wymagające sporządzenia pisemnego sprawozdania lub planu naprawczego, które musi zostać zaakceptowane przez organ kontrolujący.
- 7) Sporządzenie informacji dotyczących prawnych zagadnień bezpieczeństwa informacji oraz cyberbezpieczeństwa. Analiza i synteza przepisów prawnych (KSC, RODO, ustawy sektorowe) w kontekście specyfiki działania urzędu gminy.
- 8) Rekomendacje dotyczące środków technicznych i organizacyjnych dla zapewnienia poziomu bezpieczeństwa adekwatnego do ryzyk. Konkretnie porady dotyczące zakupu lub wdrożenia konkretnych narzędzi (np. systemy backupu, szyfrowanie danych, VPN, szkolenia, restrukturyzacja sieci IT) wynikające z przeprowadzonej analizy ryzyka.
- 9) 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. Element kluczowy dla budowania kultury bezpieczeństwa i realizacji obowiązku szkoleniowego. Broszura powinna być dostosowana językowo i merytorycznie do pracowników urzędu, a nie tylko do informatyków.

II. W wyniku realizacji zamówienia Wykonawca dostarczy w szczególności:

- 1) Zestaw rekomendacji dotyczących dostosowania działalności Zamawiającego do obowiązków ustawowych. Raport otwarcia/zamknięcia zawierający jasną mapę drogową (roadmap) wdrożenia KSC.
- 2) Zaktualizowane lub nowe procedury/dokumenty niezbędne w prawidłowym wypełnianiu obowiązków wynikających z KSC oraz innych aktów wykonawczych. Produkty końcowe prac doradczych, gotowe do wdrożenia, podpisania przez Wójta i dystrybucji (np. Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym, Rejestr Incydentów).



- 3) Efektem realizacji zadania będzie raport z przeprowadzonych działań i oceny oraz wydane rekomendacje w przypadku stwierdzonych braków, które będą stanowiły podstawę do aktualizacji, dostosowania i przygotowania wewnętrznej dokumentacji, co ma wpływać na poprawę cyberbezpieczeństwa.
- 4) Bieżące odpowiedzi eksperckie potwierdzające interpretację KSC. Usługa "helpdesku prawnego/technicznego" w trakcie trwania umowy, pozwalająca na szybkie rozwianie wątpliwości bez konieczności długotrwałego poszukiwania interpretacji przepisów.

2. Opracowanie oraz wdrożenie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) dla Gminy

Przedmiotem Zadania 2 jest opracowanie i wdrożenie kompletnego Systemu Zarządzania Bezpieczeństwem Informacji dla Gminy oraz 6 jednostek podległych (6 szkół podstawowych).

Zakres terytorialny i organizacyjny:

Wdrożony SZBI musi stanowić jednolity i spójny system obejmujący całą jednostkę samorządu terytorialnego, tj. Urząd Gminy oraz wszystkie podległe jej jednostki organizacyjne.

Centralizacja Zarządzania: System ma zapewniać scentralizowane zarządzanie bezpieczeństwem informacji, polityką bezpieczeństwa, procesem szacowania ryzyka oraz planowaniem ciągłości działania na poziomie całej JST.

Wykaz Jednostek Objętych Zakresem:

- Urząd Gminy Luzino, ul. Ofiar Stutthofu 11
- Szkoła Podstawowa nr 1 im. Lecha Bądkowskiego w Luzinie, ul. Szkolna 13
- Szkoła Podstawowa nr 2 im. Gerarda Labudy w Luzinie, ul. Mickiewicza 22
- Szkoła Podstawowa im. Płk. Stanisława Dąbka w Sychowie, ul. Szkolna 4
- Szkoła Podstawowa im. Janusza Korczaka w Wyszecinie, ul. Szkolna 2
- Szkoła Podstawowa im. Jana Pawła II w Kębłowie, ul. Wiejska 49
- Szkoła Podstawowa im. Jana Twardowskiego w Barłominie, ul. Szkolna 3

Wykonawca jest zobowiązany uwzględnić specyfikę działania, strukturę organizacyjną, infrastrukturę IT oraz unikalne procesy przetwarzania informacji (w tym danych osobowych) występujące w każdej z jednostek podległych. W celu precyzyjnego opisanie i wdrożenia adekwatnych zabezpieczeń, dla każdej



z jednostek podległych wymagane jest opracowanie przez Wykonawcę odrębnych dokumentów wykonawczych/aneksów, stanowiących uszczegółowienie głównej Polityki Bezpieczeństwa Informacji JST. W ramach tych odrębnych załączników dla każdej jednostki, Wykonawca musi dostarczyć m.in. (o ile dotyczy):

- Szczegółową analizę ryzyka specyficzną dla danej jednostki (rejestr aktywów, scenariusze zagrożeń).
- Precyzyjny spis aktywów informacyjnych i systemów IT używanych wyłącznie w danej lokalizacji.
- Mapę procesów przetwarzania danych (w tym RODO) unikalnych dla danej jednostki (np. rekrutacja do szkół, wydawanie decyzji administracyjnych).
- Lokalne procedury operacyjne i instrukcje stanowiskowe (np. procedura tworzenia kopii zapasowych w szkolnej pracowni komputerowej, instrukcja awarii sieci).

I. W ramach zadania Wykonawca przeprowadzi następujące działania:

- 1) Przeprowadzenie analizy ryzyka, dzięki której zidentyfikowane zostaną kluczowe zasoby informacyjne gminy, potencjalne zagrożenia i podatności oraz ocenić prawdopodobieństwo i skutki ich wystąpienia
- 2) Wykonanie oceny obecnie dostępnej dokumentacji i obowiązujących procedur oraz określenie stanu faktycznego zabezpieczeń danych w systemach informatycznych w oparciu o m. in. wywiad z informatykami
- 3) Wykonawca kompleksowo przeprowadzi Zamawiającego przez proces wdrożenia systemowego podejścia do zarządzania bezpieczeństwem i ciągłością działania, poczynając od ustalenia kontekstu organizacji i celów bezpieczeństwa, przygotuje wymagane normą PN-EN ISO/IEC 27001:2023 dokumenty (ich rozszerzenia), a następnie wdroży je do użytku w urzędzie i jednostkach podległych
- 4) wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, które będzie polegało na zapewnieniu zgodności z wymaganiami KRI lub normy PN-ISO/IEC 27001 lub równoważnej oraz sposobem działania jednostki, zgodnie z minimalnymi wymaganiami wykonania usługi określonymi poniżej. Wdrożenie ma obejmować procesy, procedury, dokumenty. Etapy budowania SZBI muszą być dokonywane w oparciu o wskazania, wymagania i rekomendowane działania ujęte w „Poradniku Cyberbezpieczny Samorząd”, zamieszczonym na stronie



<https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> przy jednoczesnym uwzględnieniu doświadczeń, kompetencji i potrzeb Gminy

- 5) opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji musi być zgodne z regulacjami zewnętrznymi oraz wewnętrznymi i obejmować obszary, o których mowa w szczególności w KRI, uoKSC, RODO.
- 6) wdrożenie dokumentacji SZBI - utworzenie odpowiednich dokumentów po konsultacjach z pracownikami Zamawiającego, ustalenie odpowiednich zasad, procedur i dobrych praktyk, zatwierdzenie dokumentacji przez kierownictwo Zamawiającego oraz przeprowadzenie instruktażu pracowników w zakresie wykonywania obowiązków zgodnie z opracowanym sposobem postępowania w dokumentacji SZBI.
- 7) Przegląd wdrożonego SZBI - monitorowanie, przeglądy, ocena, poprawki, aktualizacja, audyt powdrożeniowy, deklaracja stosowania

II. Zalecany zakres dokumentacji:

- 1) Dokumentacja powinna być dostosowana do skali i specyfiki Gminy
- 2) dostosowanie zakresu dokumentacji do nowej normy PL 27001:2023. W normie są wskazania dokumentacji wymaganej. Sugerowane jest jednak przygotowanie dokumentacji rozszerzającej, wszędzie tam, gdzie można podnieść skuteczność SZBI.
- 2) W dokumentacji muszą znaleźć się następujące dokumenty:
 - a) Polityka Bezpieczeństwa Informacji wraz z uszczegółowieniem dla jednostek podległych jako aneksy do polityki JST;
 - 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;

III. Wynikiem wdrożenia dokumentacji będzie wprowadzony System Zarządzania Bezpieczeństwem Informacji, który będzie wykorzystywany w jednostce oraz pozwoli zapewnić zgodność podczas audytu.

IV. 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. Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do uwzględniania poprawek sporządzanej przez siebie dokumentacji, zgodnie z uwagami Zamawiającego na każdym etapie realizacji zamówienia.

V. W ramach dokumentacji SZBI ujęte zostaną minimum następujące procedury:

- 1) procedury korzystania z urządzeń mobilnych
- 2) procedury pracy zdalnej
- 3) postępowanie z nośnikami
- 4) procedury kontroli dostępu
- 5) zabezpieczenie pomieszczeń i obiektów
- 6) procedury czystego biurka
- 7) procedury czystego ekranu
- 8) procedury kopii zapasowych
- 9) procedury ochrony logów
- 10) bezpieczeństwo komunikacji
- 11) zarządzanie bezpieczeństwem sieci
- 12) przesyłanie informacji
- 13) plany ciągłości działania
- 14) procedury zarządzania incydentami
- 15) prywatność i ochrona danych osobowych
- 16) szacowanie ryzyka w obszarze bezpieczeństwa informacji

- VI. Wykonawca zobowiązany jest do przeprowadzenia szkolenia wdrożeniowego personelu Zamawiającego, tj. osób wyznaczonych przez Zamawiającego do przeszkolenia
- VII. Wykonawca realizuje usługę kompleksowo tj. wdraża SZBI oraz wypełnia wszystkie niezbędne dokumenty w wersji elektronicznej i papierowej oraz przekazuje je Zamawiającemu.
- VIII. Wdrożenie dokumentacji musi być z zachowaniem zasady rozliczalności, która umożliwi weryfikację dostosowania podmiotu do wymogów Rozporządzenia KRI.

- IX. Po wdrożeniu SZBI, Wykonawca przedstawi rekomendacje jakie trzeba wykonać prace w harmonogramie 5 - 8 miesięcznym w celu utrzymania i doskonalenia.

3. Audyt wdrożonego Systemu Bezpieczeństwa Informacji obejmujący zgodność z kryteriami zawartymi w 20 ust. 2 ww. rozporządzenia KRI wraz z przeprowadzeniem Ankiety Dojrzałości Cyberbezpieczeństwa w JST

- I. Podstawę audytu SZBI będą stanowiły, co najmniej:
- a) wywiady z przedstawicielami wskazanych komórek organizacyjnych,
 - b) obserwacje audytora, dotyczące bezpieczeństwa środowiskowego,
 - c) zgromadzone materiały audytowe w postaci dokumentacji bezpieczeństwa informacji i organizacyjnej obowiązującej u Zamawiającego.
- II. Wykonawca sporządzi plan audytu SZBI zawierający co najmniej listę planowanych działań audytowych oraz dla każdego z działań: termin wykonania działania, komórkę organizacyjną Zamawiającego wyznaczoną do współpracy, listę dowodów do przygotowania.
- III. Efektem realizacji Zadania będzie raport z przeprowadzonego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie papierowej i elektronicznej. Raport będzie zawierał co najmniej:
- a) podsumowanie,
 - b) opis wykonania planu audytu,
 - c) opis wykorzystanych standardów,
 - d) ocenę spełnienia wymagań,
 - e) wydanie rekomendacji w przypadku stwierdzonych niezgodności i braków, które będą stanowiły podstawę do aktualizacji, dostosowania lub przygotowania wewnętrznej dokumentacji
- IV. Odbiór raportu z przeprowadzonego audytu bezpieczeństwa odbywać się będzie na następujących warunkach:
- 1) Wykonawca, prześle drogą elektroniczną, na adres poczty elektronicznej osoby odpowiedzialnej za realizację Umowy ze strony Zamawiającego, przygotowany raport z przeprowadzonego audytu SZBI, nie później niż 15 dni przed datą zakończenia realizacji zadania, celem jego akceptacji,



- 2) Zamawiający w terminie do 4 dni roboczych od przekazania przez Wykonawcę raportu z przeprowadzonego audytu SZBI, powiadomi Wykonawcę, o jego akceptacji lub braku akceptacji i konieczności wprowadzenia zmian,
- 3) Wykonawca ma prawo, aby ustosunkować się do uwag Zamawiającego w formie pisemnej, przekazując swoje stanowisko na adres poczty elektronicznej osoby odpowiedzialnej za realizację Umowy ze strony Zamawiającego,
- 4) Zamawiający dopuszcza zorganizowanie spotkań on-line w celu omówienia koniecznych do wprowadzenia zmian, wskazanych przez Zamawiającego, z zastrzeżeniem, że spotkanie będzie obligatoryjne, w przypadku, jeżeli zażąda tego Zamawiający,
- 5) po uzgodnieniu zakresu zmian, Wykonawca wprowadzi je, w terminie do 3 dni roboczych od daty ich uzgodnienia i ponownie przedstawi Zamawiającemu raport z przeprowadzonego audytu SZBI, w celu jego akceptacji,
- 6) Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w przekazanym raporcie z przeprowadzonego audytu SZBI,
- 7) komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji raportu z przeprowadzonego audytu SZBI odbywać się będzie drogą elektroniczną na adresy poczty elektronicznej Wykonawcy i Zamawiającego,
- 8) w przypadku, gdy przekazany Zamawiającemu powtórnie poprawiony raport z przeprowadzonego audytu SZBI nadal nie będzie uwzględniać wyników uzgodnień i uwag Zamawiającego, Zamawiający zastrzega sobie prawo do odmowy odbioru raportu z przeprowadzonego audytu SZBI i odstąpienia od Umowy z winy Wykonawcy,
- 9) w przypadku, o którym mowa w pkt 8), Zamawiający może zlecić wykonanie raportu z przeprowadzonego audytu SZBI podmiotowi trzeciemu, a kosztami obciążyć Wykonawcę,
- 10) zaakceptowany raport z przeprowadzonego audytu SZBI zostanie przekazany Zamawiającemu w formie papierowej, w 1 egzemplarzu (format A4), oraz formie elektronicznej na adres poczty elektronicznej Zamawiającego, w formacie plików do edycji i PDF.



- V. Raport z audytu SZBI wraz z podsumowaniem powinien zostać omówiony na spotkaniu z najwyższym kierownictwem urzędu, Zespołem Informatyków, Inspektorem Ochrony Danych i innymi osobami wskazanymi przez Zamawiającego.
- VI. Wykonawca przeprowadzi audyt w terminie określonym w umowie, w siedzibie Zamawiającego. Zamawiający dopuszcza realizację części przedmiotu zamówienia przy użyciu zdalnych środków komunikacji - po wcześniejszym telefonicznym potwierdzeniu daty i w godzinach pracy Urzędu Gminy Luzino.
- VII. Wykonawca po wykonaniu audytu SZBI jest także zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie:
<https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad> (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych). W przypadku, jeśli beneficjent projektu „Cyberbezpieczny Samorząd” tj. Centrum Projektów Polska Cyfrowa zmodyfikuje plik formularza, o którym mowa w ust. 20, Wykonawca przekaże ankietę dojrzałości cyberbezpieczeństwa sporządzoną w oparciu o aktualną wersję pliku.

4. Dodatkowe wymagania

- 1) W ramach opracowania i wdrożenia dokumentacji SZBI Wykonawca na podstawie ankiety dojrzałości, analizy ryzyka, przeglądu procedur, przeprowadzonego audytu oraz infrastruktury technicznej w Urzędzie Gminy, opracuje i przedstawi do akceptacji przygotowane polityki, które powinny zawierać między innymi zakres: cele i wymagania 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

- 2) Wykonawca udzieli wsparcia merytorycznego dla ww. zadań w terminie do 6 miesięcy od dnia zawarcia umowy, polegającego na bieżącym wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem.
- 3) Zamawiający nie ponosi kosztów dojazdu, zakwaterowania oraz wyżywienia Wykonawcy, a także dodatkowych kosztów związanych z przygotowaniem dokumentacji związanej z wykonaniem przedmiotu zamówienia.

5. Szacowana wycena usługi:

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

Uprzejmie prosimy o przesłanie wyceny usługi drogą elektroniczną za pomocą platformy zakupowej <https://platformazakupowa.pl/transakcja/1238997> w terminie

do dnia 23.12.2025 r. do godz. 10:00

| | Przedmiot zamówienia | Cena netto |
|---|---|------------|
| 1 | Opracowanie oraz wdrożenie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji SZBI dla Gminy i 6 jednostek podległych | |
| 2 | Usługi doradcze w zakresie ustawy o Krajowym Systemie Cyberbezpieczeństwa dla Gminy i 6 jednostek podległych | |
| 3 | Audyt wdrożonego Systemu Bezpieczeństwa Informacji obejmujący zgodność z kryteriami zawartymi w 20 ust. 2 ww. rozporządzenia KRI dla Gminy i 6 jednostek 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 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz.U. z 2021 r. poz. 1129). 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 Luzino w zakresie w jakim pełni funkcję grantobiorcy FERC, z siedzibą przy ul. Ofiar Stutthofu 11, 84-242 Luzino.

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 zlecieliśmy 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.

Przekazywanie danych do państwa trzeciego

Nie zamierzamy przekazywać Państwu danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwu 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@mfipr.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 Luzino
 - 1) pocztą tradycyjną kierując korespondencję na adres: ul. ul. Ofiar Stutthofu 11, 84-242 Luzino



2) elektronicznie na adres e-mail: inspektor.abi2@gmail.com

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).