

Projekt „Cyberbezpieczny Samorząd” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Gmina Łazy

42-450 Łazy ul. Traugutta 15 woj. śląskie powiat zawierciański

tel. 32/ 67 29 326 fax.32/ 67 29 448

NIP : 6492268348

REGON: 276258865

Osoby uprawnione do kontaktów z Wykonawcami:

W sprawach proceduralnych: Małgorzata Ściślicka tel. 32 6729422 w 124, e-mail: wirum@lazy.pl

W sprawach merytorycznych: Michał Utracki tel. 32 6729422 w 102, e-mail: mutracki@lazy.pl

ZAPROSZENIE DO ZŁOŻENIA PROPOZYCJI CENOWEJ

zamówienia publicznego o wartości poniżej 130 000 PLN

W imieniu: Gminy Łazy zapraszam do złożenia propozycji cenowej na realizację zadania pn.

Kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach w ramach projektu Cyberbezpieczny Samorząd.

I. PRZEDMIOT ZAMÓWIENIA:

Przedmiotem zamówienia jest kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach, obejmująca:

1. **Przegląd, aktualizację i dostosowanie dokumentacji** związanej z bezpieczeństwem teleinformatycznym (m.in. polityki bezpieczeństwa informacji, procedury, instrukcje), w celu zapewnienia jej zgodności z aktualnymi przepisami prawa oraz najlepszymi praktykami.
2. **Stworzenie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)** zgodnego z normami ISO/IEC 27001 lub równoważnymi standardami, dostosowanego do struktury organizacyjnej Urzędu.
3. **Pełnienie funkcji Inspektora Ochrony Danych (IOD)** – zapewnienie usług IOD dla Zamawiającego przez okres obowiązywania umowy.
4. **Przeprowadzenie dwóch audytów cyberbezpieczeństwa:**
 - a) pierwszy w terminie **do miesiąca od rozpoczęcia współpracy** (audyt początkowy oceniający stan bieżący i zgodność z wymaganiami),
 - b) drugi **na miesiąc przed zakończeniem umowy** (audyt końcowy weryfikujący wprowadzone zmiany i poziom poprawy bezpieczeństwa).



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt „Cyberbezpieczny Samorząd” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

II. SZCZEGÓŁOWE WYMAGANIA W ZAKRESIE AUDYTU CYBERBEZPIECZEŃSTWA

Audyt obejmie całość sprzętu informatycznego Urzędu Miasta, w tym:

1. Dane ilościowe i lokalizacja umożliwiające ustalenie zakresu oferty

1.1. Lokalizacje:

- a) pomieszczenia, będące w użytkowaniu Urzędu w budynku przy ul. Traugutta 15, 42-450 Łazy;
- b) pomieszczenia, będące w użytkowaniu Urzędu w budynku przy ul. Spółdzielczej 2, 42-450 Łazy.

1.2. Ilość pracowników: 67 osób (objąć usługą wszystkich pracowników obecnych w trakcie diagnozy i ew. szkoleń).

1.3. Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, switchy, Access Pointy, urządzenia VoIP etc.) :

W przybliżeniu:

~ 135 hostów (w tym komputery),

~ 12 serwerów (w tym wirtualne)

~ 67 komputerów użytkowników

Ilość serwerowni - 1

Ilość adresów zewnętrznych – 2

Wdrożone Active Directory - TAK

- 2. Prace wymagające udziału pracowników Urzędu muszą być realizowane w godzinach pracy Urzędu. Wykonawca przedstawi do uzgodnienia szczegółowy program realizacji zamówienia w terminie do 7 dni roboczych od podpisania umowy
- 3. Audyt cyberbezpieczeństwa powinien obejmować m.in. trzy główne obszary i być przeprowadzony zgodnie z wymaganiami KRI, uoKSC, powinien uwzględniać specyficzne wymagania obu aktów prawnych, ze szczególnym naciskiem na cyberbezpieczeństwo, zarządzanie ryzykiem, reagowanie na incydenty oraz ochronę systemów informatycznych:

3.1. Audyt Dokumentacji

- 1) Ocena zgodności istniejącej dokumentacji z normami ISO/IEC 27001, RODO oraz ustawą o krajowym systemie cyberbezpieczeństwa (uoKSC).
- 2) Przegląd procedur bezpieczeństwa, instrukcji operacyjnych i polityk ochrony informacji.
- 3) Weryfikacja spisu sprzętu i oprogramowania w kontekście cyberbezpieczeństwa.
- 4) Ocena analizy ryzyka i polityki zarządzania incydentami.
- 5) Przegląd planów zarządzania ciągłością działania (BCP) i odzyskiwania po awarii (DRP).

3.2. Audyt Fizyczny i Środowiskowy

- 1) Weryfikacja fizycznych zabezpieczeń serwerowni i pomieszczeń IT.

Projekt „Cyberbezpieczny Samorząd” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

- 2) Sprawdzenie procedur kontroli dostępu i monitoringu.
- 3) Ocena zabezpieczeń urządzeń przenośnych i sieciowych.
- 4) Analiza stosowanych mechanizmów ochrony przed ujawnieniem, modyfikacją lub utratą danych.

3.3. Audyt Teleinformatyczny

- 1) Weryfikacja polityki haseł i dostępów użytkowników.
- 2) Ocena bezpieczeństwa sieci (firewalle, UTM, VPN).
- 3) Analiza podatności systemów informatycznych i procedur zarządzania aktualizacjami.
- 4) Testy penetracyjne w środowisku testowym.
- 5) Ocena systemu wykrywania i reagowania na incydenty.

4. Po zakończeniu audytu Wykonawca przygotowuje raport zawierający:

- 1) **Wprowadzenie:** Cel, zakres, kluczowe obszary audytowane, datę przeprowadzenia audytu oraz opis objętych audytem jednostek, systemów, procedur i obszarów.
- 2) **Opis zastosowanych metod i działań audytowych.**
- 3) **Ocenę zgodności z przepisami:** Ogólna ocena zgodności z uoKSC, KRI oraz innymi regulacjami (np. RODO, ISO 27001).
- 4) **Identyfikację niezgodności:** Wskazanie obszarów niezgodnych z wymogami prawnymi lub procedurami wewnętrznymi, z klasyfikacją (np. krytyczna, wysoka, średnia, niska).
- 5) **Wyniki audytu:**
 - a) Opis mocnych stron, w których Urząd spełnia wymogi i stosuje dobre praktyki w zakresie zarządzania bezpieczeństwem informacji,
 - b) Wskazanie słabych punktów, takich jak podatności, niezgodności lub braki w procedurach i zabezpieczeniach technicznych i organizacyjnych.
 - c) Ocenę ryzyka – analizę ryzyk związanych z integralnością, poufnością i dostępnością informacji oraz systemów.
- 6) **Rekomendacje i zalecenia audytorów:**
 - a) Zalecane działania naprawcze (np. wzmocnienie polityk bezpieczeństwa, poprawa procedur reagowania na incydenty, dostosowanie zabezpieczeń),
 - b) Priorytetyzację działań (krytyczne, pilne, zalecane), umożliwiającą organizacji skuteczne planowanie działań naprawczych w celu zapewnienia zgodności.
- 7) **Podpisy i oświadczenia audytorów** dotyczące rzetelności przeprowadzonego audytu i pełnego przedstawienia wyników oraz wniosków.
- 8) **Załączniki:** Lista uczestników audytu, przeanalizowanych dokumentów, polityk i procedur.

III. WYMAGANIA DOTYCZĄCE STWORZENIA LUB DOSTOSOWANIA DOKUMENTACJI

1. **Dostosowanie dokumentacji SZBI** do standardów ISO/IEC 27001, uoKSC oraz KRI.
2. **Przygotowanie brakujących procedur i polityk** dotyczących cyberbezpieczeństwa i ochrony danych osobowych.

Projekt „Cyberbezpieczny Samorząd” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

3. **Opracowanie polityki zarządzania incydentami** i wdrożenie procedur reagowania na incydenty.
4. **Stworzenie systemu klasyfikacji informacji** oraz zasad dostępu do danych zgodnych z najlepszymi praktykami.
5. **Przegląd i aktualizacja polityki ochrony danych osobowych**, w tym rejestr czynności przetwarzania, analiza DPIA oraz regulamin dostępu do danych.
6. **Opracowanie strategii zarządzania ryzykiem**, w tym analiza zagrożeń i plan zarządzania ciągłością działania.
7. **Dokumentacja powinna być dostosowana do struktury organizacyjnej Urzędu** i obejmować wszystkie kluczowe obszary działalności w zakresie bezpieczeństwa informacji.
8. **Wykonanie dokumentacji oraz jej wdrożenie wraz ze współpracą z IOD-em ma być przeprowadzone po przeprowadzonym audycie wstępnym uwzględniając jego zalecenia, ale nie później niż na 3 miesiące przez przeprowadzeniem audytu końcowego.**

IV. ZAKRES OBOWIĄZKÓW INSPEKTORA OCHRONY DANYCH (IOD)

IOD będzie odpowiedzialny m.in. za:

1. Monitorowanie zgodności przetwarzania danych z przepisami RODO.
2. Informowanie i doradzanie Administratorowi w zakresie obowiązków wynikających z ochrony danych.
3. Szkolenia pracowników z zakresu RODO.
4. Pełnienie funkcji punktu kontaktowego dla Prezesa UODO.
5. Przeprowadzanie audytów ochrony danych osobowych.
6. Konsultacje w zakresie oceny skutków dla ochrony danych (DPIA).
7. Obecność w siedzibie Zamawiającego **raz w miesiącu przez 6 godzin** w uzgodnionym wspólnie terminie oraz zdalna dostępność w dni robocze w godz. 8:00-16:00.
8. Całość zadań IOD-a jak i zakres ma być realizowany zgodnie z zaleceniami PUODO
9. **Zamawiający przedstawi w Ofercie zaoferowany przez siebie zakres usług IOD-a.**

V. TERMIN REALIZACJI

Termin realizacji zamówienia: od 1 kwietnia 2025 r. do 30 kwietnia 2026 r.

Projekt „Cyberbezpieczny Samorząd” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

VI. OPIS SPOSOBU OBLICZENIA CENY OFERTY

1. Cena oferty, wynikająca bezpośrednio z formularza ofertowego musi być wyrażona w złotych polskich w sposób jednoznaczny i winna obejmować całkowity koszt realizacji zamówienia oraz podatek VAT.
2. Rozliczenia między Wykonawcą a zamawiającym będą prowadzone w złotych polskich.
3. Wszystkie ceny, w tym ceny jednostkowe, należy podawać z dokładnością nie większą jak dwa miejsca po przecinku.
4. **Cenę oferty należy podać w formie wynagrodzenia ryczałtowego.** W związku z powyższym cena oferty musi zawierać wszelkie koszty niezbędne do zrealizowania zamówienia bez których nie można prawidłowo wykonać zamówienia.
5. Ofertowa cena brutto musi być podzielona na następujące składniki:
 - 1) **Koszt przeprowadzenia dwóch audytów cyberbezpieczeństwa.**
 - 2) **Koszt pełnienia funkcji IOD przez cały okres umowy.**
 - 3) **Koszt dostosowania dokumentacji i wdrożenia SZBI.**

VII. KRYTERIA OCENY OFERT

1. Zamawiający informuje, że zamówienie zostanie udzielone Wykonawcy, który zaoferuje najniższą cenę.

Oferta najtańsza, spośród ofert nie odrzuconych, otrzyma 100 punktów. Pozostałe proporcjonalnie mniej, według formuły:

$(C_n / C_{of.b.} \times 100) \times 100\% = \text{ilość punktów},$

gdzie:

C_n – najniższa cena spośród ofert

C_{of.b.} – cena oferty badanej

100 – wskaźnik stały,

100% – procentowe znaczenie kryterium ceny

2. Jeżeli cena oferty będzie budzić wątpliwości Zamawiającego, co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający w celu ustalenia, czy oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia, może zwrócić się do Wykonawcy o udzielenie wyjaśnień dotyczących elementów oferty, mających wpływ na wysokość ceny oraz dowodów potwierdzających obliczenie ceny. Zamawiający może żądać w szczególności złożenia kalkulacji obliczenia ceny.

3. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy. Zamawiający odrzuci ofertę Wykonawcy, który nie złoży wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdzi, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

Projekt „Cyberbezpieczny Samorząd” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

4. Wykonawca zobowiązany jest do ujęcia w cenie oferty wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym np. Koszty ewentualnego zakwaterowania, dojazdu, wyżywienia, wydruku i skanu dokumentów itd

VIII. WARUNKI UDZIAŁU W POSTĘPOWANIU:

O udzielenie mogą się ubiegać Wykonawcy, którzy

- 1) posiadają niezbędne uprawnienia do realizacji przedmiotu zamówienia,
- 2) posiadają niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zamówienia,
 - a) Zamawiający wymaga, żeby oferent wykazał się realizacją **co najmniej dwóch porównywalnych projektów (w zakresie minimum takim jakiego wymaga Zamawiający lub szerszym w jednostce o takiej samej lub bardzo zbliżonej specyfice typu Urząd Miasta, Gminy, Powiat itp)**, potwierdzonych referencjami.
- 3) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,

4) DODATKOWE WYMAGANIA:

- a) **Kwalifikacje wykonawcy:** Wykonawca musi dysponować personelem o odpowiednich kwalifikacjach, potwierdzonych certyfikatami z zakresu bezpieczeństwa informatycznego. Preferowane są certyfikaty uznawane w branży, takie jak m.in. **Auditor Wiodący ISO/IEC 27001, CISA, CISSP, CISM** lub równoważne, potwierdzające kompetencje w obszarze audytu i zarządzania bezpieczeństwem informacji.
- b) **Wymagania dot. pełnienia funkcji IOD:** W ramach realizacji usługi Inspektora Ochrony Danych Wykonawca zapewni, że wyznaczony IOD będzie **obecny fizycznie** w siedzibie Zamawiającego przynajmniej **raz w miesiącu** przez około **6 godzin**, w celu prowadzenia wymaganych czynności na miejscu (np. szkolenia, konsultacje, sprawdzenie dokumentacji). Ponadto IOD powinien być **dostępny zdalnie** (telefonicznie lub mailowo) w pozostałym czasie, tak aby zapewnić bieżące wsparcie i konsultacje w zakresie ochrony danych osobowych przez cały okres trwania umowy.

IX. SPOSÓB SKŁADANIA OFERT

1. Propozycję cenową należy złożyć do dnia **17. 03. 2025r. do godz. 10.00** w siedzibie Zamawiającego, Gmina Łazy, 42-450 ul. Traugutta 15, biuro obsługi – parter.
2. Zamawiający dodatkowo dopuszcza składanie ofert elektronicznie. Oferty można składać przesyłając drogą elektroniczną w formie podpisanego przez Wykonawcę skanu na adres: informatyk@lasy.pl do dnia **17.03.2025r. do godz. 10.00 (należy w tym przypadku niezwłocznie dostarczyć wersję papierową potwierdzającą wersję elektroniczną).**
3. Wykonawca może również przesłać ofertę na adres: informatyk@lasy.pl do dnia **17.03.2025r. do godz. 10.00** w formie elektronicznej (zalecany pdf) podpisaną elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym – w tym przypadku oferta stanowi oryginał dokumentu i wykonawca nie jest zobowiązany do dostarczenia niezwłocznie formy papierowej dokumentu.
4. W przypadku przesłania oferty wraz z wymaganymi dokumentami drogą pocztową, za termin złożenia oferty przyjmuje się termin, w którym oferta (przesyłka) znalazła się



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

w siedzibie Zamawiającego.

5. Na opakowaniu oferty należy zamieścić następujące informacje:
 - **nazwę i adres Zamawiającego;**
 - **nazwę i adres Wykonawcy;**
 - oraz zapis: **Oferta na wykonanie zadania: Kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach w ramach projektu Cyberbezpieczny Samorząd.**

X. OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Złożenie oferty jest jednoznaczne z akceptacją bez zastrzeżeń w całości warunków określonych w niniejszym zapytaniu ofertowym.
2. Oferta musi być złożona z zachowaniem formy pisemnej, w języku polskim pod rygorem nieważności.
3. Jeden Wykonawca może złożyć tylko jedną ofertę.
4. Treść oferty musi odpowiadać treści zapytania ofertowego.
5. Wykonawca może, przed upływem terminu do składania ofert, zmienić lub wycofać ofertę.
6. Naniesienie zmian w ofercie przez Wykonawcę zobowiązuje go do złożenia podpisu w każdym miejscu dokonania zmiany.
7. Wykonawca ponosi wszystkie koszty związane z przygotowaniem i złożeniem oferty.
8. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.
9. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
10. Ofertę stanowi
 - 1). Wypełniony formularz oferty
 - 2). Pełnomocnictwo do podpisania oferty, jeżeli nie wynika bezpośrednio z załączonych dokumentów
 - 3). Oświadczenie o spełnianiu warunków udziału w postępowaniu.
 - 4). Oświadczenie dotyczące posiadanego doświadczenia wraz z dokumentami potwierdzającymi należyte wykonanie usługi

XI. WARUNKI PŁATNOŚCI:

1. Wynagrodzenie płatne będzie na podstawie prawidłowo wystawionej faktury Vat z terminem płatności do 14 dni w oparciu o podpisany przez Wykonawcę i Zamawiającego protokół zdawczo – odbiorczy, odrębnie dla poszczególnych części zamówienia, czyli:
 - 1) W zakresie audytów: pierwsza faktura po przeprowadzonym Audycie wstępnym, kolejna po Audycie końcowym.
 - 2) Pełnienie Funkcji IOD-a w jednostce na koniec realizacji zlecenia.
 - 3) Po sporządzeniu, dostosowaniu dokumentacji SZBI.

XII. Zamawiający zastrzega sobie prawo odwołania, unieważnienia postępowania lub zmiany warunków postępowania bez podawania przyczyn.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

XIII. INFORMACJA DOTYCZĄCA RODO

W związku ze zbieraniem danych osobowych na potrzeby realizacji zamówienia pn.: **Kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach w ramach projektu Cyberbezpieczny Samorząd.**

Stosownie do art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. U. UE. L. Nr 119 poz. 1 z 2016 r.) - dalej RODO, informujemy że:

1. Administratorem Pana/Pani danych osobowych jest Burmistrz Łaz z siedzibą w Urzędzie Miejskim w Łazach, ul. Traugutta 15, 42-450 Łazy, tel. 32 6729434, fax. 32 6729448, e-mail: um@lasy.pl.
2. Dane kontaktowe Inspektora Ochrony Danych Osobowych to: iod@lasy.pl, tel. 326729434 lub pocztą na adres: Urząd Miejski w Łazach, 42-450 Łazy, ul. Traugutta 15.
3. Administrator danych osobowych przetwarza Pani/Pana dane osobowe na podstawie obowiązujących przepisów prawa, zawartych umów oraz na podstawie udzielonej zgody.
4. Podstawą prawną przetwarzania danych osobowych jest:
 - a) zgoda na przetwarzanie danych osobowych – art. 6 ust. 1 lit. a RODO. Na jej podstawie przetwarzane są dane podawane przez Pana/Panią dobrowolnie np. numer telefonu celem zapewnienia szybkiej i sprawnej komunikacji związanej z realizacją złożonego wniosku,
 - b) wykonanie umowy, której jest Pan/Pani stroną lub podjęcie działań na Pana/Pani żądanie przed zawarciem umowy - art. 6 ust. 1 lit. b RODO,
 - c) wypełnienia obowiązku wynikającego z przepisu prawa - art. 6 ust. 1 lit. c RODO,
 - d) wykonania zadania realizowanego w interesie publicznym przez administratora - art. 6 ust. 1 lit. e RODO.
5. Na podstawie obowiązujących przepisów prawa, jeśli będzie to konieczne, Pana/Pani dane będą udostępniane innym administratorom, podmiotom przetwarzającym oraz osobom upoważnionym do przetwarzania danych osobowych, które muszą mieć dostęp do danych, aby wykonywać swoje obowiązki. Wymienieni odbiorcy danych zostaną zobowiązani do zachowania danych osobowych w poufności w procesie ich przetwarzania.
6. Pana/Pani dane osobowe nie będą przekazywane do państwa trzeciego.
7. Dane osobowe będą przechowywane przez okres wyznaczony przepisami prawa, w tym przez okres wskazany w instrukcji kancelaryjnej.
8. Przysługuje Panu/Pani prawo do:
 - a) żądania dostępu do danych dotyczących osoby, której dotyczy,
 - b) sprostowania danych osobowych,
 - c) żądania usunięcia danych osobowych,
 - d) żądania ograniczenia przetwarzania,
 - e) wniesienia sprzeciwu wobec przetwarzania,
 - f) cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
 - g) wniesienia skargi do organu nadzorczego,z wyjątkami zastrzeżonymi obowiązującymi przepisami prawa.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

9. W sytuacji, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby, której dane dotyczą, podanie przez Panią/Pana danych osobowych Administratorowi ma charakter dobrowolny. Podanie przez Panią/Pana danych osobowych jest obowiązkowe, w sytuacji gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa lub zawarta między stronami umowa.
10. Pana/Pani dane nie będą przetwarzane dla zautomatyzowanego podejmowania decyzji i nie będą podlegały profilowaniu.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Załącznik nr 1 do zaproszenia

Pełna nazwa Wykonawcy:.....

Adres siedziby Wykonawcy:.....

Nr telefonu**:Nr faksu: e-mail

NIPREGON

** Numer telefonu podawany jest dobrowolnie i będzie służył tylko i wyłącznie w celu przeprowadzenia postępowania

OFERTA

W odpowiedzi na zaproszenie do złożenia propozycji cenowej w postępowaniu o wartości poniżej 130 000 PLN na realizację zadania pn **Kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach w ramach projektu Cyberbezpieczny Samorząd** oferuję wykonanie zadania **za cenę ryczałtową** :

Netto:

VAT:

Razem brutto:.....

SŁOWNIE:

W tym:

1) **Koszt przeprowadzenia dwóch audytów cyberbezpieczeństwa.**

Netto:

VAT:

Razem brutto:.....

2) **Koszt pełnienia funkcji IOD przez cały okres umowy**

Netto:

VAT:

Razem brutto:.....

3) **Koszt dostosowania dokumentacji i wdrożenia SZBI.**

Netto:

VAT:

Razem brutto:.....



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

1. **Oferujemy termin realizacji: od 1 kwietnia 2025 r. do 30 kwietnia 2026 r.**
2. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez okres 30 dni.
3. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO³⁾ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.*

* W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

Miejsce i data

Podpis.....

*Podpis osoby uprawnionej lub osób uprawnionych
do reprezentowania Wykonawcy*



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Załącznik nr 2 do Zaproszenia

Pełna nazwa Wykonawcy:

Adres siedziby Wykonawcy:.....

**Kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach
w ramach projektu Cyberbezpieczny Samorząd**

OŚWIADCZENIE WYKONAWCY

Wykonawca oświadcza, że:

- posiada niezbędne uprawnienia do realizacji przedmiotu zamówienia,
- posiada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zamówienia,
- znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
- dysponuje osobami (personalem) zdolnym do realizacji niniejszej usługi, posiadającym wymagane uprawnienia i certyfikaty.

.....

(miejscowość, data)

.....

(podpis i pieczęć Wykonawcy)



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Projekt „**Cyberbezpieczny Samorząd**” jest realizowany w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Załącznik nr 3 do Zaprośzenia

.....

.....

(nazwa, adres, nr telefonu, fax, e-mail Wykonawcy)

**Kompleksowa usługa podniesienia poziomu cyberbezpieczeństwa Urzędu Miejskiego w Łazach
w ramach projektu Cyberbezpieczny Samorząd**

OŚWIADCZENIE WYKONAWCY

Wykonawca oświadcza, że w przeciągu 3 lat poprzedzających złożenie oferty, wykonał następujące usługi:

Lp.	Nazwa i opis usługi	Nazwa Zamawiającego	Data zakończenia wykonywania usługi
1.			
2.			

Dokumenty potwierdzające wykonanie powyższej usługi/powyższych usług (kopie dokumentów załączone do niniejszego oświadczenia):

1.
2.

.....

(miejscowość, data)

.....

(podpis i pieczęć Wykonawcy)