OGŁOSZENIE O WSTĘPNYCH KONSULTACJACH RYNKOWYCH

I. Nazwa i adres Zamawiającego

Centralny Ośrodek Informatyki
Aleje Jerozolimskie 132-136
02-305 Warszawa
e-mail: zamowienia.publiczne@coi.gov.pl
www.coi.gov.pl/zamowienia-publiczne
nr tel.: +48 (22) 250 28 83 oraz 22 250 28 85

Osoby wyznaczone do kontaktu:

Jakub Wojtkowski, e-mail: jakub.wojtkowski@cyfra.gov.pl; zamowienia.publiczne@coi.gov.pl .

Uwaga: Wszelką korespondencję kierowaną do Zamawiającego należy opatrzyć dopiskiem: **„Wstępne Konsultacje Rynkowe związane z postępowaniem o udzielenie zamówienia na dostawę systemu do zarządzania ryzykiem w bezpieczeństwie informacji, ciągłości działania oraz zarządzania analizą wpływu na biznes (BIA)”**.

II. Podstawa prawna

Wstępne Konsultacje Rynkowe prowadzone są na podstawie art. 84 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2023 r. poz. 1605, z późn. zm.) oraz zgodnie z *Regulaminem przeprowadzania Wstępnych Konsultacji Rynkowych w Centralnym Ośrodku Informatyki,* stanowiącym załącznik nr 2 do niniejszego Ogłoszenia.

III. Przedmiot zamówienia oraz cel prowadzenia Wstępnych Konsultacji Rynkowych

Centralny Ośrodek Informatyki informuje, że zamierza prowadzić Wstępne Konsultacje Rynkowe dotyczące „Dostawy systemu do zarządzania ryzykiem w bezpieczeństwie informacji, ciągłości działania oraz zarządzania analizą wpływu na biznes (BIA)", w zakresie niezbędnym do przygotowania postępowania o udzielenie zamówienia publicznego, a w szczególności do: oszacowania wartości zamówienia, przygotowania specyfikacji warunków zamówienia (w tym opisu przedmiotu zamówienia) oraz określenia warunków umowy.

IV. Celem Konsultacji jest uzyskanie informacji, w szczególności w poniższym zakresie:

1. Analiza najlepszych i najnowszych rozwiązań technicznych i funkcjonalnych w zakresie systemu do zarządzania ryzykiem w bezpieczeństwie informacji:
    - Klasyfikacja informacji
    - Identyfikacja i ocena zasobów (odpowiedzialnych za przetwarzanie informacji)
    - Identyfikacja zagrożeń
    - Identyfikacja i ocena podatności zasobów oraz zabezpieczeń
    - Ocena ryzyka
    - Planowanie działań związanych z ryzykiem,

- Monitorowanie działań, ocena skuteczności, ponowna analiza ryzyka oraz raportowanie na poziomie grup informacji i zasobów

2. Analiza najlepszych i najnowszych rozwiązań technicznych i funkcjonalnych w zakresie systemu do analizy wpływu na biznes (BIA)
   - Kontekst organizacji, usługi, procesy, działania wspierające dostarczanie wyrobów i usług
   - Identyfikacja rodzajów wpływu i kryteriów oddziaływania
   - Oszacowanie potencjalnych strat/ skutków przerwania/ zakłócenia usługi
   - Określenie wymagań wznowienia usług (MTPD, RTO, RPO)
   - Określenie procesów krytycznych/ określenie priorytetów odtwarzania procesów
   - Określenie minimalnych zasobów do utrzymania ciągłości procesów.
   - Określenie zależności i współzależności priorytetowych działań
3. Analiza najlepszych i najnowszych rozwiązań technicznych i funkcjonalnych w zakresie systemu do zarządzania ryzykiem w ciągłości działania:
   - Inwentaryzacja zasobów
   - Klasyfikacja i wycena zasobów (określenie istotności)
   - Identyfikacja, ocena podatności i zabezpieczeń w odniesieniu do zasobów
   - Ocena ryzyka z uwzględnieniem wpływu zdarzeń
   - Planowanie działań związanych z ryzykiem,
   - Monitorowanie działań, ocena skuteczności, ponowna analiza ryzyka oraz raportowanie na poziomie zasobów
4. Poznanie funkcjonujących na rynku rozwiązań, w tym zaprezentowanie przez Uczestników działania systemów.
5. Określenie optymalnej dla organizacji metodyki analizy wpływu na biznes oraz oceny ryzyka w bezpieczeństwie informacji i ciągłości działania realizowanej przy użyciu systemu teleinformatycznego.
6. Określenie koncepcji realizacji dla przedsięwzięcia związanego z wdrożeniem prezentowanego rozwiązania (rekomendacje dotyczące wdrożenia, propozycje działania, usprawnienia, inne).
7. Określenie szacowanego zarysu kosztów realizacji zamówienia dla powyższego przedsięwzięcia (w tym koszt dostawy, wdrożenia, wsparcia technicznego, ewentualne koszty rozwojowe).
8. Określenie wymagań dotyczących infrastruktury po stronie Zamawiającego.
9. Określenie szacowanego terminu dostawy i wdrożenia.

V. Wymagania funkcjonalne systemu do zarządzania ryzykiem w bezpieczeństwie informacji, ryzykiem utraty ciągłości działania oraz zarządzania analizą wpływu na biznes (funkcje *must have*):

1. System ma posiadać logiczne i funkcjonalne mechanizmy umożliwiające zarządzanie ryzykiem w bezpieczeństwie informacji.
2. System ma posiadać logiczne i funkcjonalne mechanizmy umożliwiające zarządzanie ryzykiem w ciągłości działania.
3. System ma posiadać logiczne i funkcjonalne mechanizmy umożliwiające zarządzanie analizą wpływu na biznes.
4. System ma mieć w przyszłości możliwość rozbudowy, aby była możliwość wykonania następujących czynności:
   4.1. przygotowanie, utrzymanie i zarządzanie planami i procedurami ciągłości działania;
   4.2. zadania z zakresu obsługi niezgodności i działań naprawczych;

4.3. Zadania z zakresu zarządzania incydentami (rejestracja incydentu / zdarzenia ciągłości, zarządzanie działaniami wynikającymi z incydentu zgodnie z obowiązującymi wymaganiami prawnymi i międzynarodowymi standardami, prowadzenia rejestru, raportowanie);
4.4. zadania z zakresu ochrony danych osobowych;
4.5. zadania z zakresu zarządzania zgodnością (compliance);
4.6. zadania wynikające z Krajowego Systemu Cyberbezpieczeństwa.

5. System powinien posiadać możliwość szczegółowego określenia zasobów, w tym:
   5.1. identyfikację, opis i tworzenie listy procesów, podprocesów (w tym biznesowych, wspierających i innych);
   5.2. możliwość opracowania „workflow" w celu uzyskiwania akceptacji i zatwierdzania danych na różnych poziomach uprawnień użytkowników;
   5.3. Objęcie systemem następujących obszarów:
      a) wszystkich komórek organizacyjnych,
      b) wszystkich Placówek (oddziałów).
6. System powinien działać w środowisku Windows Server lub Linux. System musi posiadać włączoną funkcją szyfrowania TLS 1.2 lub wyższy, z udostępnionym przez Zamawiającego certyfikatem.
7. System musi umożliwić śledzenie, audyt zmian w konfiguracji oprogramowania i bazy danych. Baza danych powinna mieć zaimplementowaną i włączoną funkcję audytu bazy danych, polegającą na rejestrowaniu działań przez użytkowników.
8. System (jeżeli funkcjonalność systemu tego wymaga) musi po stronie klienta być obsługiwany poprzez znane bezpieczne przeglądarki wiodących dostawców rozwiązań (np. Edge, Chrome) i w przypadku zidentyfikowanych podatności być na bieżąco aktualizowany, aby w czasie trwania umowy zapewnić ciągłość działania poprzez m.in. wsparcie i obsługę.
9. System posiada intuicyjny interfejs wraz z mechanizmami podpowiedzi (samouczków) prowadzących użytkownika przez poszczególne, ekrany / widoki/ formularze i zakładki.
10. Instrukcja obsługi dla użytkowników i administratorów w systemie – poza dostarczoną w wersji PDF – powinna być dodatkowo (jeżeli to możliwe) zaszyta w systemie w formie „dymków" lub podpowiedzi.
11. System do zarządzania ryzykiem w obszarze bezpieczeństwa informacji, ciągłości działania oraz zarządzania analizą wpływu na biznes będzie pochodził bezpośrednio od producenta lub od autoryzowanego dystrybutora w polskiej wersji językowej wraz ze wsparciem w języku polskim.
12. Wymagania funkcjonalne ogólne:
    12.1. Możliwość integracji z Active Directory co najmniej w zakresie zarządzania uprawnieniami i autoryzacji dostępu;
    12.2. Możliwość automatycznej / półautomatycznej integracji (minimum w zakresie importu / eksportu danych) z innymi źródłami np.: systemami, bazami danych, itp.;
    12.3. Możliwość integracji z systemem poczty elektronicznej;
    12.4. Interfejs użytkownika oparty na kreatorach (opcjonalnie);
    12.5. System musi umożliwiać realizację wszystkich zadań wynikających z procesu zarządzania ryzykiem w bezpieczeństwie informacji (w aspekcie identyfikacji, analizy, ewaluacji, postępowania z ryzykiem, monitorowania, komunikacji) i generować stosowne dokumenty i raporty;
    12.6. System musi umożliwiać realizację wszystkich zadań wynikających z procesu zarządzania analizą wpływu na biznes (BIA) – (kontekst, usługi, procesy, rodzaje wpływów i kryteria oddziaływania, szacowanie strat zakłóceń, wymagania wznowienia usług, priorytety odtwarzania, minimalne zasoby do utrzymania ciągłości, zależności priorytetowych działań) i generować stosowne dokumenty i raporty;

12.7. System musi umożliwiać realizację wszystkich zadań wynikających z procesu zarządzania ryzykiem w ciągłości działania (identyfikacji, analizy, ewaluacji, postępowania z ryzykiem, monitorowania, komunikacji) i generować stosowne dokumenty i raporty;

12.8. System musi umożliwiać tworzenie i definiowanie metodyk zarządzania ryzykiem w oparciu o różne wzory i mechanizmy dostosowane do obszarów i kontekstu podstawowych atrybutów takich jak poufność, integralność dostępność oraz niezawodność i rozliczalność (w obszarze ciągłości działania). W szczególności system musi umożliwiać dowolne agregowanie podstawowych aktywów organizacji wprowadzonych do systemu, stosowanie wobec w/w agregacji innych metodyk zarządzania ryzykiem w celu odwzorowania specyficznych procesów biznesowych;

12.9. System musi umożliwiać wprowadzanie i utrzymywanie rejestru zasobów oraz import aktywów z innych baz;

12.10. System musi umożliwiać wypełnienie i wygenerowanie metryki / paszportu zasobu zawierającego minimum:

12.10.1. - nazwę

12.10.2. - typ

12.10.3. - właściciela

12.10.4. - zasoby podrzędne i narzędny (z wyraźnym rozgraniczeniem)

12.10.5. Umiejscowienie;

12.11. Dla zidentyfikowanych aktywów system musi umożliwiać wskazanie podmiotów zewnętrznych odpowiedzialnych za (dostarczenie, nadzór, serwisowanie lub wsparcie);

12.12. System musi umożliwiać wskazanie działań związanych z danym aktywem (np. czasowe wyłączenie, serwis, audyt) oraz zapewnić komunikację zdarzeń, przypomnienia i raportowanie;

12.13. Możliwość odwzorowania struktury organizacyjnej na podstawie struktury z Active Directory (w sposób zautomatyzowany lub półzautomatyzowany), za pomocą aktywnych obiektów graficznych lub drzewa posiadających odpowiedniki w bazie danych i umożliwiających ich wykorzystanie, powiązanie w innych obszarach funkcjonalnych;

12.14. Możliwość zaimportowania struktury organizacyjnej z systemu kadrowego;

12.15. Możliwość zarządzania rolami poprzez grupowanie w ramach roli obiektów dowolnego poziomu struktury organizacyjnej (komórka organizacyjna, stanowisko, rola);

12.16. Możliwość zgłaszania w systemie przez użytkowników propozycji zmiany, uwag i ryzyk do modelu i obiektów z poziomu systemu (z możliwością dołączania dokumentów przez użytkownika do zgłaszanej propozycji) oraz za pomocą wbudowanego workflow automatyzować przebieg zmiany (opiniowania, zatwierdzania, wdrażania);

12.17. System musi posiadać kokpity menadżerskie prezentujące syntetycznie wyniki analizy BIA, analizy ryzyka;

12.18. Możliwość automatycznego generowania dokumentów w postaci plików takich jak: doc, docx, xls, xlsx, rtf , pdf, txt w oparciu o zdefiniowane szablony wykorzystujące dane wprowadzone do narzędzia (systemu);

12.19. Posiadać mechanizm utrzymania repozytorium załączonych plików;

12.20. Możliwość ustawienia mierników KPI oraz mierzenia ich efektywności (opcjonalnie).

13. W ramach wdrożenia mają zostać opracowane podstawowe interfejsy:

13.1. Active Directory – autentykacja oraz autoryzacja użytkowników;

13.2. MS Exchange – integracja z pocztą elektroniczną.

14. W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka system powinien:
    14.1. posiadać zautomatyzowany proces analizy ryzyka w oparciu o zasoby z uwzględnieniem procesów realizowanych z ich udziałem;
    14.2. posiadać możliwość samodzielnego dostosowania i określenia skali ocen oraz progów prawdopodobieństwa i wpływu (dla ryzyka oraz szansy);
    14.3. posiadać możliwość przeprowadzenia klasyfikacji informacji;
    14.4. posiadać możliwość przeprowadzenia identyfikacji i oceny zasobów (odpowiedzialnych za przetwarzanie informacji);
    14.5. posiadać predefiniowany katalog zagrożeń;
    14.6. posiadać możliwość porównania ryzyka dla danego zasobu / procesu;
    14.7. umożliwić identyfikację technicznych, ludzkich, naturalnych i realnych ryzyk dla dowolnej lokalizacji wraz z ich oceną i wpływem;
    14.8. posiadać możliwość identyfikacji i pomiaru potencjalnych zagrożeń dla dowolnej lokalizacji lub obiektu;
    14.9. umożliwiać dokonywanie oceny ryzyka (w tym szans) przy pomocy wprowadzonych skal ocen;
    14.10. umożliwiać powiązanie zdarzenia materializacji ryzyka z poszczególnymi ryzykami;
    14.11. umożliwić określenie sposobu postępowania z ryzykiem;
    14.12. posiadać możliwość zarządzania zadaniami określonymi po przeprowadzeniu analizy ryzyka;
    14.13. umożliwić dostosowanie do wymagań wybranej metodyki przeprowadzenia analizy ryzyka wraz z oceną;
    14.14. posiadać możliwość opracowania raportu pokazującego prawdopodobieństwo i dotkliwość zagrożeń;
    14.15. umożliwić opracowanie planu postępowania z ryzykiem (listy kontrolne, zadania/kroki, śledzenie statusów, powiadamianie odbiorców, itp.);
    14.16. automatyzować planowanie działań wynikających z analizy ryzyka z określeniem ról i odpowiedzialności. Poprzez mechanizmy workflow obsługiwać proces realizacji działań wynikających z planu postępowania z ryzykiem (powiadomienie o zadaniu, okresowe raportowanie, zrealizowanie zadania wraz ze wskazaniem wyników, ocenę skuteczności działań);
    14.17. umożliwiać zarządzanie planami ciągłości działania w postaci repozytorium planów. Repozytorium planów ma mieć drzewiastą postać, a każdy plan ma posiadać odrębna metrykę, która umożliwia zarządzanie zmianą i komunikację planu dla wskazanych obiektów struktury organizacyjnej (komórka, stanowisko, osoba);
    14.18. umożliwiać powiązanie incydentu z ryzykiem w przyszłości po rozbudowie o moduł zarz. incydentami);
    14.19. umożliwiać powiązanie incydentu z procesem oraz zasobem w przyszłości po rozbudowie o moduł zarz. incydentami);
    14.20. umożliwiać agregację ryzyk (integrację i powiązanie) w ramach hierarchii ryzyk;
    14.21. umożliwiać generowanie mapy ryzyka i reakcji na ryzyko.
15. W obszarze zarządzania analizą wpływy na biznes BIA:
    15.1. System umożliwia modelowanie diagramów procesów przynajmniej w dwóch notacjach:

15.1.1. – BPMN,
15.1.2. - EPC;

15.2. System umożliwia przeprowadzenie procesu identyfikacji kontekstu organizacji, usług, procesów, działań wspierających dostarczanie wyrobów i usług, niezbędnego do przeprowadzenia analizy BIA;

15.3. System umożliwia przeprowadzenie procesu identyfikacji rodzajów wpływu i kryteriów oddziaływania;

15.4. System umożliwia wykonanie analizy wpływu na biznes (BIA) dla procesów poprzez mechanizmy samooceny skutków przestoju przez właścicieli procesów;

15.5. System umożliwia przeprowadzenie BIA w kontekście wielu kryteriów skutku i czasu;

15.6. System umożliwia wskazanie jakie zasoby są niezbędne do realizacji (utrzymania ciągłości) procesów i wykazanie ich na karcie oceny/procesu;

15.7. System umożliwi określenie oraz automatyzuje wyliczenie czasów (wymagań wznowienia usług):

15.7.1. RTO,
15.7.2. RPO,
15.7.3. MTPD (opcjonalnie);

15.8. System umożliwia przeprowadzenie procesu określania procesów krytycznych/ określania priorytetów odtwarzania procesów;

15.9. System umożliwia określenie zależności i współzależności priorytetowych działań;

15.10. System ma posiadać mechanizm okresowego przeglądu analizy BIA, pozwalający na zautomatyzowanie ponownej oceny w kolejnym okresie;

16. W obszarze zarządzania ryzykiem w ciągłości działania:

16.1. System posiada zautomatyzowany proces analizy ryzyka w oparciu o zasoby z uwzględnieniem procesów realizowanych z ich udziałem;

16.2. System posiada możliwość samodzielnego dostosowania i określenia skali ocen oraz progów prawdopodobieństwa i wpływu (dla ryzyka oraz szansy);

16.3. System posiada predefiniowany katalog zagrożeń;

16.4. System umożliwia inwentaryzację zasobów niezbędnych do utrzymania ciągłości działania;

16.5. System umożliwia klasyfikację i wycenę zasobów (określenie istotności);

16.6. System umożliwia dokonywanie oceny ryzyka (w tym szans) przy pomocy wprowadzonych skal ocen;

16.7. System umożliwia powiązanie zdarzenia materializacji ryzyka z poszczególnymi ryzykami;

16.8. System umożliwia stworzenie karty procesu, za pomocą dedykowanego elektronicznego formularza elektronicznego, z prezentacją ryzyk oraz zasobów wykorzystywanych w procesie;

16.9. System umożliwia określenie sposobu postępowania z ryzykiem;

16.10. System posiada możliwość zarządzania zadaniami określonymi po przeprowadzeniu analizy ryzyka;

16.11. System umożliwia dostosowanie do wymagań wybranej metodyki przeprowadzenia analizy ryzyka wraz z oceną;

16.12. System posiada możliwość opracowania raportu pokazującego prawdopodobieństwo i dotkliwość zagrożeń;

16.13. System umożliwia opracowanie planu postępowania z ryzykiem (listy kontrolne, zadania/kroki, śledzenie statusów, powiadamianie odbiorców, itp.);

16.14. System pozwala automatyzować planowanie działań wynikających z analizy ryzyka z określeniem ról i odpowiedzialności. Poprzez mechanizmy workflow obsługiwać proces realizacji działań wynikających z planu postępowania z ryzykiem (powiadomienie o zadaniu, okresowe raportowanie, zrealizowanie zadania wraz ze wskazaniem wyników, ocenę skuteczności działań);

16.15. System umożliwia zarządzanie planami ciągłości działania w postaci repozytorium planów. Repozytorium planów ma mieć drzewiastą postać, a każdy plan ma posiadać odrębna metrykę, która umożliwia zarządzanie zmianą i komunikację planu dla wskazanych obiektów struktury organizacyjnej (komórka, stanowisko, osoba);

16.16. System umożliwia powiązanie incydentu z ryzykiem w przyszłości po rozbudowie o moduł zarz. incydentami);

16.17. System umożliwia powiązanie incydentu z procesem oraz zasobem w przyszłości po rozbudowie o moduł zarz. incydentami);

16.18. System umożliwia agregację ryzyk (integrację i powiązanie) w ramach hierarchii ryzyk;

16.19. System umożliwia generowanie mapy ryzyka i reakcji na ryzyko.

17. Funkcjonalność ogólna powinna mieć:

17.1. możliwość rozpoczęcia wskazanych czynności dla wszystkich procesów w wybranym terminie;

17.2. możliwość wysłania automatycznego powiadomienia do wybranych osób/ról dla zdefiniowanego workflow (poczta elektroniczna), m.in. przypomnienia o nadchodzących terminach, nowych ryzykach, incydentach, zdarzeniach, przekroczeniach poziomów ryzyk poza zdefiniowany poziom; możliwość weryfikacji kompletności/statusu realizacji poszczególnych zadań w zdefiniowanych punktach kontrolnych (np.: nieaktualna analiza, brak danych) – w definiowalnych interwałach czasowych;

17.3. możliwość elastycznego raportowania – opracowanie widoków dynamicznych, szablonów dokumentacji;

17.4. możliwość opracowania przekrojowych raportów analitycznych;

17.5. możliwość definiowania za pomocą kreatora szablonów raportu, planów, procedur, etc.;

17.6. możliwość customizacji layoutu danego raportu (kolorystyka, znaki graficzne / logo);

17.7. możliwość automatycznej dystrybucji list kontrolnych i kwestionariuszy;

17.8. możliwość akceptacji wyników zgodnie z modelem uprawnień i roli użytkownika;

17.9. możliwość ręcznego i automatycznego przypomnienia o konieczności aktualizacji danych dotyczących procesu, list kontaktowych, analiz, etc.;

17.10. możliwość podglądu danych historycznych z poprzednich wersji (listy kontaktowe, listy procesów/zasobów, etc.) wraz z możliwością porównywania danych;

17.11. możliwość śledzenia, przeglądu „zaciągania" pobierania danych historycznych, np. już wykonanego szacowania i analizy ryzyka w szczególności każdego ryzyka z osobna, wykonanej analizy BIA;

17.12. wbudowany mechanizm raportowania z predefiniowanymi wzorcami jak i z możliwością tworzenia własnych raportów;

17.13. możliwość weryfikacji przez użytkownika (wykonującego ocenę) jak również przez zarządzających oceną ryzyka/ analizą BIA statusu swojego zadania/wszystkich zadań (dot. zarządzającego oceną) oraz wglądu do treści wykonanej oceny/ zadania;

17.14. określone dokładnie warunki licencjonowania (np. liczba użytkowników, możliwość korzystania równoczesnego z dostępu do systemu, itp.);

17.15. udzielenie bezterminowej licencji.

18. Minimalne wymagania co do zgodności:

18.1. wymagane jest, aby funkcjonalność systemu do zarządzania ryzykiem w bezpieczeństwie informacji, zarządzania ryzykiem w ciągłości działania oraz zarządzania analizą wpływu na biznes była zgodna w szczególności z aktualnie obowiązującymi następującymi normami: ISO 27001, ISO 27005; ISO 31000 oraz ISO 22301;

18.2. zgodność z obowiązującą ustawą o krajowym systemie cyberbezpieczeństwa wraz z rozporządzeniami szczególnie w kontekście zakresu obowiązków podmiotów publicznych;

18.3. Zamawiający wymaga, aby system był aktualizowany i modyfikowany na bieżąco, co do zgodności z obowiązującym prawem oraz wewnętrznymi aktami prawnymi i regulaminami.

Kluczowe zagadnienia (informacje, które Centralny Ośrodek Informatyki chce uzyskać)

1. Automatyzację procesów analizy ryzyka w BI i BCM oraz procesu BIA.
2. Ujednolicenie rejestrów i danych w scentralizowanej bazie.
3. Usprawnienie procesu oceny ryzyka w bezpieczeństwie informacji i ciągłości działania.
4. Otwartość – możliwości współpracy i wymiany danych z innymi systemami i bazami danych.
5. Interfejs użytkownika – możliwość pracy przez przeglądarkę WWW oraz urządzenia mobilne.
6. Bezpieczeństwo – system zarządzania prawami dostępu do funkcjonalności systemu, raportów i danych.
7. Sprawną komunikację w obszarze zarządzania ryzykiem – możliwość przydzielania zadań z planów postepowania z ryzykiem pracownikom oraz zautomatyzowany i szybki sposób komunikowania o realizacji zadania przez pracownik.
8. Usprawnienie procesu raportowania.
9. Zaawansowane funkcje raportowe – możliwości elastycznej budowy raportów w oparciu o dane z wielu źródeł.
10. Mobilność – dostępność do raportów, danych poprzez urządzenia mobilne.

VI. Zgłoszenie do udziału we Wstępnych Konsultacjach Rynkowych

1. Podmioty zainteresowane udziałem we Wstępnych Konsultacjach Rynkowych składają zgłoszenia do udziału, według wzoru stanowiącego załącznik nr 1 do niniejszego Ogłoszenia, zwane dalej „Zgłoszeniem" wraz z innymi dokumentami wskazanymi w niniejszym Ogłoszeniu[1].

[1] Jeśli dotyczy, zgodnie z § 6 ust. 1 zd. 1 *Regulaminu przeprowadzania Wstępnych Konsultacji Rynkowych*, Zamawiający może zaprosić do udziału w Konsultacjach Uczestników wybranych spośród wszystkich podmiotów, które złożą prawidłowo sporządzone zgłoszenie do udziału w Konsultacjach oraz ewentualnie dodatkowe oświadczenia, stanowiska lub dokumenty, których Zamawiający zażąda w Ogłoszeniu, działając zgodnie z zasadami prowadzenia Konsultacji.

2. Zgłoszenia można składać za pośrednictwem poczty elektronicznej na adres **zamowienia.publiczne@coi.gov.pl.** Zamawiający zaleca, aby Zgłoszenie było podpisane z wykorzystaniem kwalifikowanego podpisu elektronicznego, przez osobę upoważnioną do działania w imieniu Wykonawcy.
3. Termin składania zgłoszeń upływa w dniu: **26.03.2024 r.**

VII. Zasady prowadzenia Wstępnych Konsultacjach Rynkowych

1. Warunkiem udziału we Wstępnych Konsultacjach Rynkowych jest złożenie Zgłoszenia przez osobę umocowaną do działania w imieniu Wykonawcy, w terminie określonym w niniejszym Ogłoszeniu.
2. Zamawiający nie określa szczegółowych warunków jakie należy spełnić w celu wzięcia udziału we Wstępnych Konsultacjach Rynkowych.
3. Zamawiający wyśle zaproszenie do udziału we Wstępnych Konsultacjach Rynkowych do podmiotów, które złożyły Zgłoszenia w terminie określonym w pkt IV.3 niniejszego Ogłoszenia, na adres e-mail wskazany w Zgłoszeniu.
4. Wstępne Konsultacje Rynkowe prowadzone będą w języku polskim. Do dokumentów sporządzonych w językach innych niż polski należy dołączyć tłumaczenia na język polski.
5. Wstępne Konsultacje Rynkowe mają charakter jawny, za wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U z 2022 r., poz. 1233 z późn.zm.), jeżeli Wykonawca, nie później niż wraz z przekazaniem informacji Zamawiającemu, skutecznie zastrzegł, że nie mogą być udostępniane innym podmiotom.
6. Wstępne Konsultacje Rynkowe prowadzone będą z wykorzystaniem środków bezpośredniego porozumiewania się na odległość (Teams). Link zostanie wysłany po zgłoszeniu uczestnictwa. Dopuszcza się także wymianę korespondencji w postaci elektronicznej.
7. Zamawiający może rozpocząć procedurę Wstępnych Konsultacji Rynkowych od momentu skutecznego nadesłania Zgłoszenia przez pierwszego uczestnika.
8. Informacja o terminie zakończenia Wstępnych Konsultacji Rynkowych zostanie umieszczona na stronie internetowej Zamawiającego, jak również przekazana w formie elektronicznej zaproszonym uczestnikom Wstępnych Konsultacji Rynkowych.
9. Po zakończeniu Wstępnych Konsultacji Rynkowych Zamawiający przygotuje Protokół opisujący zakres udzielonych informacji oraz przedłoży do odpisu Wykonawców uczestniczących we Wstępnych Konsultacjach Rynkowych.

VIII. INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH OSÓB FIZYCZNYCH - WYKONAWCÓW W TOKU WSTĘPNYCH KONSULTACJI RYNKOWYCH

Szczegółowe informacje dotyczące przetwarzania danych osobowych	
Administrator danych	Administratorem Twoich danych osobowych Centralny Ośrodek Informatyki z siedzibą w Warszawie (dalej: ,,my“). Możesz się z nami skontaktować w następujący sposób: - listownie na adres: ul. Aleje Jerozolimskie 132/136, 02-305 Warszawa; - przez e-mail: iod@coi.gov.pl; odo@coi.gov.pl; - telefonicznie: 22 250 28 83, 22 250 28 85; - osobiście w naszej siedzibie.
Inspektor ochrony danych	Wyznaczyliśmy inspektora ochrony danych. Jest to osoba, z którą możesz się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych. Z inspektorem ochrony danych możesz się kontaktować w następujący sposób: - listownie na adres: ul. Aleje Jerozolimskie 132/136, 02-305 Warszawa; - przez e-mail: iod@coi.gov.pl
Cele przetwarzania danych oraz podstawa prawna przetwarzania	**W ramach Wstępnych Konsultacji Rynkowych będziemy przetwarzać Twoje dane osobowe, aby:** - ustalić termin spotkań z poszczególnymi wykonawcami, przeprowadzić takie spotkania oraz udokumentować ich przebieg. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. f RODO tj. prawnie uzasadniony interes administratora w związku z uprawnieniami wynikającymi z art. 84 Pzp
Okres przechowywania danych	Będziemy przechowywać Twoje dane osobowe przez okres 5 lat od dnia zakończenia postępowania o udzielenie zamówienia.
Odbiorcy danych	Będziemy przekazywać Twoje dane osobowe: - osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania, w tym innym podmiotom biorącym udział w postępowaniu o udzielenie zamówienia publicznego oraz podmiotom uprawnionym na podstawie przepisów prawa, jeśli wystąpią z takim żądaniem

Obowiązek podania danych	Podanie danych osobowych jest dobrowolne jednak konieczne do wzięcia udziału we Wstępnych Konsultacjach Rynkowych
Twoje prawa	Masz następujące prawa: a. prawo **dostępu** do Twoich danych osobowych; b. prawo **żądania sprostowania** Twoich danych osobowych; c. prawo **żądania ograniczenia przetwarzania** Twoich danych osobowych; d. prawo **wniesienia sprzeciwu** wobec przetwarzania Twoich danych osobowych ze względu na szczególną sytuację; e. prawo do usunięcia danych osobowych. Aby skorzystać z powyższych praw, skontaktuj się z nami lub z naszym inspektorem ochrony danych (dane kontaktowe w wierszu 1 i 2 niniejszej tabeli). **Prawo wniesienia sprzeciwu** W zakresie, w jakim Twoje dane są przetwarzane na podstawie naszego prawnie uzasadnionego interesu – masz prawo zgłoszenia sprzeciwu wobec przetwarzania danych ze względu na Twoją szczególną sytuację. **Prawo wniesienia skargi do organu** Przysługuje Ci także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych.

IX. INFORMACJA O PRZETWARZANIU DANYCH OSOBOWYCH OSÓB FIZYCZNYCH KTÓRYCH DANE SĄ PRZEKAZYWANE ZAMAWIAJĄCEMU PRZEZ WYKONAWCĘ W TOKU WSTĘPNYCH KONSULTACJI RYNKOWYCH**2**

Szczegółowe informacje dotyczące przetwarzania danych osobowych	
Administrator danych	Administratorem Twoich danych osobowych Centralny Ośrodek Informatyki z siedzibą w Warszawie (dalej: ,,my“). Możesz się z nami skontaktować w następujący sposób: - listownie na adres: ul. Aleje Jerozolimskie 132/136, 02-305 Warszawa; - przez e-mail: iod@coi.gov.pl; odo@coi.gov.pl; - telefonicznie: 22 250 28 83, 22 250 28 85; - osobiście w naszej siedzibie.
Inspektor ochrony danych	Wyznaczyliśmy inspektora ochrony danych. Jest to osoba, z którą możesz się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych. Z inspektorem ochrony danych możesz się kontaktować w następujący sposób: - listownie na adres: ul. Aleje Jerozolimskie 132/136, 02-305 Warszawa; - przez e-mail: iod@coi.gov.pl.
Cele przetwarzania danych oraz podstawa prawna przetwarzania	**W ramach Wstępnych Konsultacji Rynkowych będziemy przetwarzać Twoje dane osobowe, aby:** ustalić termin spotkań z poszczególnymi wykonawcami, przeprowadzić takie spotkania oraz udokumentować ich przebieg. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. f) RODO tj. prawnie uzasadniony interes administratora w związku z uprawnieniami wynikającymi z art. 84 Pzp. - Bronić się przed ewentualnymi roszczeniami lub dochodzić ewentualnych roszczeń związanych z realizacją zamówienia – jeżeli powstanie spór. Podstawą prawną przetwarzania danych jest nasz prawnie uzasadniony interes polegający na możliwości obrony przed roszczeniami lub dochodzenia roszczeń.

[2] Dot. art. 14 RODO.

Okres przechowywania danych	Będziemy przechowywać Twoje dane osobowe przez okres 5 lat od dnia zakończenia postępowania o udzielenie zamówienia – w związku z którym prowadzone są Wstępne Konsultacje Rynkowe.
Źródło danych i kategorie danych	Otrzymaliśmy Twoje dane osobowe od wykonawcy biorącego udział we Wstępnych Konsultacjach Rynkowych - Twojego pracodawcy, podmiotu, z którym współpracujesz lub podmiotu, który zwrócił się do Ciebie w związku z chęcią wzięcia we wstępnych konsultacjach rynkowych. Wykonawca przekazał nam Twoje imię i nazwisko, służbowe dane kontaktowe, obejmujące adres poczty elektronicznej oraz numer telefonu - wymagane do kontaktu prowadzonego w ramach Wstępnych Konsultacji Rynkowych.
Odbiorcy danych	Będziemy przekazywać Twoje dane osobowe: - osobom lub podmiotom, którym udostępniona zostanie dokumentacja postępowania, w tym innym podmiotom biorącym udział w postępowaniu o udzielenie zamówienia oraz podmiotom uprawnionym na podstawie przepisów prawa, jeśli wystąpią z takim żądaniem.
Twoje prawa	Masz następujące prawa: a. prawo **dostępu** do Twoich danych osobowych; b. prawo **żądania sprostowania** Twoich danych osobowych; c. prawo **żądania ograniczenia przetwarzania** Twoich danych osobowych; d. prawo **wniesienia sprzeciwu** wobec przetwarzania Twoich danych osobowych ze względu na szczególną sytuację; e. prawo do usunięcia danych osobowych. Aby skorzystać z powyższych praw, skontaktuj się z nami lub z naszym inspektorem ochrony danych (dane kontaktowe w wierszu 1 i 2 niniejszej tabeli). **Prawo wniesienia sprzeciwu** W zakresie, w jakim Twoje dane są przetwarzane na podstawie naszego prawnie uzasadnionego interesu – masz prawo zgłoszenia sprzeciwu wobec przetwarzania danych ze względu na Twoją szczególną sytuację. **Prawo wniesienia skargi do organu** Przysługuje Ci także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych.

Załącznik:

1. Wzór Zgłoszenia do udziału we Wstępnych Konsultacjach Rynkowych;
2. Regulamin przeprowadzania Wstępnych Konsultacji Rynkowych w Centralnym Ośrodku Informatyki.