Nr sprawy: JZDZ-DD-2301-963/2025

ZAPROSZENIE DO SKŁADANIA OFERT

W niniejszym postępowaniu nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (j.t.: Dz. U. z 2024 r., poz. 1320 ze zm.). *Szacowana wartość zamówienia nie przekracza kwoty 130 000 zł.*

Instytut Nafty i Gazu - Państwowy Instytut Badawczy w Krakowie,
przy ul. Lubicz 25 A, 31-503 Kraków, tel. 12 421 00 33,
https://www.inig.pl , e-mail: office@inig.pl ,
zwany dalej Zamawiającym, zaprasza do złożenia oferty na

usługę przeprowadzenia audytu bezpieczeństwa i testów penetracyjnych aplikacji internetowej „Moduł KZR”.

1. PRZEDMIOT ZAMÓWIENIA I WYMAGANIA WOBEC WYKONAWCY:

A) Przedmiotem zamówienia jest świadczenie usługi przeprowadzenia audytu bezpieczeństwa i testów penetracyjnych aplikacji internetowej „Moduł KZR”. Szczegółowy opis przedmiotu zamówienia znajduje się w Załączniku nr 1 do Zaproszenia.

B) ZAMAWIAJĄCY WYMAGA, ABY WYKONAWCA:

i. zapewnił świadczenia usługi przez co najmniej dwóch (2) inżynierów, który to każdy z nich posiada **OSCP (Offensive Security Certified Professional)** oraz dodatkowo minimum jeden z certyfikatów związanych z bezpieczeństwem IT z następującej listy:
   - **CEH** (Certified Ethical Hacker),
   - **CISSP** (Certified Information Systems Security Professional),
   - **CRISC** (Certified in Risk and Information Systems Control),
   - **OSCE** (Organization for Security and Co-operation in Europe).

   Zamawiający dopuszcza łączenie posiadania ww. certyfikatów przez jedną lub dwie osoby.

ii. posiadał wdrożony oraz certyfikowany system zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001.
   Certyfikat ISO 27001 lub dokument potwierdzający posiadanie i wdrożenie systemu zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001 musi być aktualny na dzień składania oferty.

iii. w okresie ostatnich pięciu lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie posiadał doświadczenie w realizacji usług przeprowadzania audytów aplikacjach moblinych, internetowych oraz desktopowych w różnych technologiach potwierdzone referencjami lub innymi dokumentami potwierdzającymi należyte wykonywanie wskazanych usług.

2. TERMIN REALIZACJI USŁUGI:

Termin realizacji zamówienia:

- I etap – wykonanie całości audytu bezpieczeństwa i testów penetracyjnych i zakończonych przekazaniem raportem końcowym z audytu - 15 dni roboczych od dnia zawarcia umowy,
- II etap – spotkanie Wykonawcy z zespołem technicznym Zamawiającego w celu omówienia wyników oraz ustalenia harmonogramu wdrożenia zaleceń – termin zostanie uzgodniony w trybie roboczym po zakończeniu etapu I,

- III etap – wykonanie re-testów wdrożonych poprawek w celu weryfikacji ich skuteczności oraz aktualizacja raportu końcowego z audytu – po usunięciu podatności przez zamawiającego ale nie później niż w terminie 12 miesięcy od dnia podpisania protokołu odbioru etapu I bez zastrzeżeń. W terminie 5 dni roboczych od daty zakończenia re – testów Wykonawca przekaże zaktualizowany raport końcowy. Łącznie etap III zostanie wykonany nie później niż w terminie 13 miesięcy od dnia podpisania protokołu odbioru etapu I bez zastrzeżeń.

3. DOKUMENTY WYMAGANE:

a) Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
b) Wykaz inżynierów będących w dyspozycji Wykonawcy potwierdzający spełnienie warunku określonego w pkt. 1, ppkt. B), tiret i) – załącznik nr 3 do Zaproszenia;
c) Certyfikat ISO 27001 lub dokument potwierdzający posiadanie i wdrożenie systemu zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001;
d) Wykaz usług Wykonawcy potwierdzający spełnienie warunku określonego w pkt. 1, ppkt. B), tiret iii) – załącznik nr 4 do Zaproszenia;
e) Dokumenty / referencje potwierdzające wykonywanie usług wskazanych w wykazie – załączniku nr 4.

4. SPOSÓB SPORZĄDZENIA OFERTY.

Ofertę można sporządzić na załączniku nr 2 do Zaproszenia. Oferta musi zawierać:

- **Nazwę, adres, numer telefonu, e-mail Wykonawcy,**
- **Cenę oferty wraz z terminem realizacji,**
- **<u>Dokumenty wskazane w pkt 3,</u>**
- Kserokopię polisy wraz z Ogólnymi Warunkami Ubezpieczenia i potwierdzeniem zapłaty składki/składek – jeśli Wykonawca posiada,
- **Sprawozdanie z wyników audytu – raport końcowy (szablon).**
  Raport końcowy, w którym audytor udokumentuje wyniki audytu, winien zawierać sekcje takie jak:
  - **Podsumowanie audytu** – ogólne wnioski i ocena bezpieczeństwa, wydajności;
  - **Wykryte luki** – szczegółowy opis zidentyfikowanych problemów, ich klasyfikacja (np. krytyczne, średnie, niskie);
  - **Zalecenia** – proponowane działania naprawcze, wraz z priorytetami;
  - **Plan naprawczy** – rekomendacje dla zespołu developerskiego oraz administratorów w celu zaadresowania problemów.

Cenę oferty należy podać w złotych polskich (PLN) netto/brutto, w zaokrągleniu do dwóch miejsc po przecinku.
W przypadku złożenia oferty przez wykonawcę mającego swoją siedzibę poza granicami Polski (Wykonawca zagraniczny), zobowiązany on jest do podania tylko wartości netto, wyrażonej w złotych polskich.
Zamawiający, w celu zapewnienia możliwości porównania cen, doliczy do ceny oferty podatek VAT, który miałby obowiązek rozliczyć zgodnie z przepisami o podatku od towarów i usług.

Wykonawca powinien uwzględnić w oferowanej cenie wszelkie niezbędne koszty związane z realizacją i rozliczeniem przedmiotu zamówienia.

Oferta oraz wszystkie załączniki wymagają podpisu osoby / osób uprawnionych do reprezentowania Wykonawcy, zgodnie z aktem rejestracyjnym, wymaganiami ustawowymi oraz przepisami prawa.
Ofertę należy sporządzić na piśmie, w języku **polskim**, w formie zapewniającej pełną czytelność jej

treści. Zamawiający dopuszcza przedstawienie prospektów, katalogów i innych materiałów producenta, stanowiących szczegółowy opis techniczny oferowanego reduktora, w języku angielskim, z wymogiem wyraźnego zaznaczenia tych fragmentów, które zawierają opis parametrów oferowanego produktu.
W przypadku wskazania przez Wykonawcę dostępności dokumentów, o których mowa powyżej, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobierze samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty. W takim przypadku w ofercie należy umieścić linki kierujące bezpośrednio do ww informacji lub dokumentów.

Oferta niekompletna, nie posiadająca ww. wymaganych dokumentów nie będzie rozpatrywana.
Zamawiający zastrzega sobie prawo wyjaśniania treści złożonych ofert.
UWAGA: *Zgodnie z obowiązującymi procedurami wewnętrznymi: Zamawiający może nie rozpatrywać oferty złożonej przez dostawcę, który wcześniej wykonał zamówienie dla Zamawiającego z nienależytą starannością.*

5. Kryteria oceny ofert

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami:

a. cena ogółem brutto: **70%;**
b. dodatkowe certyfikaty osób wykonujących przedmiot zamówienia: 20%;
c. posiadanie ubezpieczenia na kwotę 1.000.000 zł: 10 %.

a) Ocena ofert w kryterium „cena" nastąpi wg wzoru poniżej:

$$Wc = \frac{\text{cena najniższa}}{\text{cena przedstawiona w badanej ofercie}} \times 70 \text{ pkt}$$

b) Oferta będzie oceniana w kryterium „Dodatkowe certyfikaty osób wykonujących przedmiot zamówienia":
Wykonawcy będą poddani ocenie w oparciu o przedstawiony w ofertą wykaz osób skierowanych do realizacji zamówienia z potwierdzeniem posiadania wymaganych certyfikatów, zgodnie z warunkiem określonym w pkt. 1, ppkt. B), tiret i) Zaproszenia.
Zamawiający przyzna 0 pkt. Wykonawcy, który wykaże spełnienie wymogu, o którym mowa w pkt. 1 ppkt B), tiret i) Zaproszenia.
Dodatkowe punkty zostaną przyznane Wykonawcy, który wskaże, że osoby wykazane podsiadają dodatkowe certyfikaty określone przez Zamawiającego – wykonawca otrzyma 5 pkt za każdy certyfikat z listy, **nie więcej jednak niż 20 pkt**.

c) Oferta będzie oceniana w kryterium „**posiadanie ubezpieczenia na kwotę 1.000.000 zł":**
Wykonawca otrzyma **10 punktów** w tym kryterium w przypadku **posiadania przez okres realizacji przedmiotu zamówienia umowy ubezpieczenia od odpowiedzialności cywilnej (OC), obejmującej ochronę ubezpieczeniową działalność zgodną z przedmiotem zamówienia i opiewającą na sumę gwarancyjną nie niższą niż 1.000.000,00 zł na jedno i wszystkie zdarzenia**. Umowa ubezpieczenia powinna obejmować odpowiedzialność cywilną Wykonawcy za szkody z tytułu czynów niedozwolonych (odpowiedzialność deliktową) oraz odpowiedzialność cywilną za szkody, wynikające z niewykonania lub nienależytego wykonania zobowiązania (odpowiedzialność kontraktowa) w związku z prowadzoną przez Wykonawcę działalnością lub posiadanym mieniem, a w tym szkody rzeczowe i osobowe wyrządzone osobom trzecim. Kserokopia polisy wraz z Ogólnymi Warunkami Ubezpieczenia i potwierdzeniem zapłaty składki/składek będzie stanowić podstawę do dokonania oceny oferty w kryterium.

W przypadku braku takiej polisy Wykonawca otrzyma w tym kryterium zero (0) punktów.

Za ofertę najkorzystniejszą uznana zostanie oferta, która uzyska łącznie największą ilość punktów w kryteriach.
Jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych.

6. Termin związania ofertą: 30 dni.
Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

7. Miejsce oraz termin składania ofert.

- Ofertę należy złożyć **w formie elektronicznej**
  - w postaci skanu wypełnionego i podpisanego formularza ofertowego

  lub
  - w postaci dokumentów podpisanych podpisem elektronicznym

  – należy przesłać na adres: przetargi@inig.pl . Jako temat wiadomości prosimy wpisać: **„Oferta na usługę przeprowadzenia audytu bezpieczeństwa i testów penetracyjnych aplikacji internetowej „Moduł KZR", nr sprawy: JZDZ-DD-2301-963/2025".**
  Termin składania ofert upływa dnia 18 lipca 2025 r. o godz. 10:00.
- W przypadku składania oferty w formie elektronicznej (wiadomość e-mail) – o terminie złożenia oferty decyduje termin dostarczenia wiadomości na wskazany adres e-mail Zamawiającego, a nie data i godzina jej wysłania.
- Oferty złożone po terminie nie będą rozpatrywane i zostaną zwrócone Wykonawcy.
- Koszty związane z przygotowaniem i złożeniem oferty ponosi Wykonawca.

8. Sposób porozumiewania się z Wykonawcami:
Wszystkie wnioski, pisma, zapytania należy kierować na adres: przetargi@inig.pl .
Odpowiedzi na pytania zadawane przez Wykonawców zamieszczane będą na stronie prowadzonego zapytania i stanowić będą integralną część zaproszenia do składania ofert.

9. Warunki umowy, które zostaną wprowadzone do umowy.

- Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę. Wzór umowy opracuje Zamawiający i przekaże wybranemu Wykonawcy.
- Wynagrodzenie Wykonawcy będzie płatne 2 transzach:
  a) 70% wynagrodzenia za wykonanie zamówienia – po podpisaniu przez przedstawicieli obu Stron protokołu odbioru etapu I, bez zastrzeżeń,
  b) 30% wynagrodzenia za wykonanie zamówienia – po podpisaniu przez przedstawicieli obu Stron protokołu odbioru etapu III, bez zastrzeżeń.
- Umowa zawarta zostanie z uwzględnieniem postanowień i wymagań wynikających z treści niniejszego zapytania ofertowego, danych i cen zawartych w ofercie. Załącznikiem do umowy o realizację zamówienia będzie porozumienie o zachowaniu poufności (NDA) według wzoru Zamawiającego. Na etapie realizacji zamówienia Zamawiający będzie oczekiwał ponadto, aby wszystkie osoby z ramienia Wykonawcy zaangażowane w audyt podpisały indywidualne oświadczenia zobowiązujące je do zachowania poufności według wzoru dostarczonego przez Zamawiającego.
- W przypadku, jeżeli na etapie składania ofert Wykonawca będzie oczekiwał udzielenia dalszych informacji dotyczących przedmiotu zamówienia (innych niż przedstawione w zapytaniu ofertowym) warunkiem przekazania tych informacji przez Zamawiającego osobie/podmiotowi żądającej/emu informacji będzie podpisanie przez ten podmiot/osobę porozumienia o zachowaniu

poufności (NDA) według wzoru dostarczonego przez Zamawiającego. Wzór umowy o poufności (NDA) stanowi Załącznik nr 5 do Zaproszenia.

10. Ogłoszenia wyników zapytania ofertowego.

Wynik postępowania zostanie zamieszczony na stronie internetowej Zamawiającego http://www.inig.pl/zamowienia-pub oraz przesłany Wykonawcom, którzy złożyli oferty.

11. Klauzula informacyjna dotycząca przetwarzania danych osobowych.

OCHRONA DANYCH OSOBOWYCH

1. **Wykonawca zobowiązany jest do poinformowania osób uprawnionych do jego reprezentacji, których dane osobowe zawarte są w jakimkolwiek załączniku lub dokumencie składanym w postępowaniu (w szczególności w pełnomocnictwie), o przetwarzaniu ich danych osobowych przez Zamawiającego. Wykonawca przekazuje tym osobom informację w następującym zakresie:**

1.1. ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych jest Instytut Nafty i Gazu – Państwowy Instytut Badawczy z siedzibą w Krakowie, ul. Lubicz 25 A, 31-503 Kraków, tel.: +48 12 421 00 33, fax: +48 12 430 38 85, e-mail: office@inig.pl .

1.2. DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych poprzez e-mail: daneosobowe@inig.pl lub pisemnie na adres siedziby administratora.

1.3. ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH

Pani/Pana dane osobowe zostały udostępnione Zamawiającemu przez reprezentowany przez Panią/Pana podmiot (Wykonawcę) w związku z ubieganiem się o udzielenie Zamówienia oraz pozyskane przez Instytut Nafty i Gazu – Państwowy Instytut Badawczy z rejestrów publicznych (KRS, CEIDG).

1.4. KATEGORIE DANYCH OSOBOWYCH

Zakres przekazanych danych osobowych obejmuje imię i nazwisko, zajmowane stanowisko, reprezentowany podmiot, dane ujawnione w jawnych rejestrach, dane ujawnione w treści pełnomocnictwa (jeśli zostało ono Pani/Panu udzielone).

1.5. CELE PRZETWARZANIA I PODSTAWA PRAWNA

Pani/Pana dane będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia nieobjętego przepisami Prawa zamówień publicznych, w tym wyboru najkorzystniejszej oferty, a w razie wyboru oferty – także wykonania umowy zawartej na skutek udzielonego zamówienia.

Podstawa prawną przetwarzania danych są:

a) przepisy prawa (art. 6 ust. 1 lit. c RODO[†]):

- ustawa z dnia 23.04.1964 r. Kodeks cywilny (w brzmieniu aktualnie obowiązującym),
- ustawy z dnia 6.09.2001 o dostępie do informacji publicznej (w brzmieniu aktualnie obowiązującym),
- ustawa z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym),

b) uzasadniony interes administratora, w tym zapewnienie wiarygodnej identyfikacji podmiotu ubiegającego się o udzielnie zamówienia nieobjętego przepisami Prawa zamówień publicznych i reprezentującej/ych ten podmiot osoby/osób, wykonania, zawarcia i wykonania umowy oraz ustalenie, dochodzenie lub obrona roszczeń (art. 6 ust. 1 lit. f RODO).

1.6. ODBIORCY DANYCH

Dane pozyskane w związku z postępowaniem mogą być przekazywane wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia jest jawne.

Ponadto odbiorcami danych osobowych mogą być jednostki audytujące, podmioty przetwarzające dane osobowe na zlecenie administratora (np. podmioty obsługujące systemy informatyczne), inne organy w oparciu o przepisy prawa, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu, np. podmioty prowadzące działalność pocztową lub kurierską.

1.7. OKRES PRZECHOWYWANIA DANYCH

Pani/Pana dane osobowe w przypadku postępowań o udzielenie zamówienia nieobjętego przepisami Prawa zamówień publicznych będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt Instytutu Nafty i Gazu – Państwowego Instytutu Badawczego, który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym) został przygotowany w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych.

1.8. PRAWA PODMIOTÓW DANYCH

Przysługuje Pani/Panu:

- prawo dostępu do danych (art. 15 RODO),
- prawo żądania ich sprostowania (art. 16 RODO), przy czym skorzystanie z tego prawa nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w tym zakresie,
- prawo ograniczenia przetwarzania, przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego praw (art. 18 ust. 1 RODO),
- prawo do usunięcia danych,
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
- prawo sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 21 RODO, z przyczyn związanych z Pani/Pana

[†]RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 4.05.2016 r., L 119/1 z późn. zm.).

szczególną sytuacją.

1.9. PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim Pani/Pana zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. W Polsce organem takim jest Urząd Ochrony Danych Osobowych.

1.10. INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH

Podanie danych osobowych w związku udziałem w postępowaniu o zamówienia nieobjętego przepisami Prawa zamówień publicznych jest dobrowolne. Brak podania danych będzie skutkował niemożliwością udziału w prowadzonym postępowaniu, zawarcia i wykonania umowy.

1.11. INFORMACJA O ZAUTOMATYZOWANYM PODEJMOWANIU DECYZJI, W TYM PROFILOWANIU

Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

2. Wykonawca zobowiązany jest do poinformowania osób fizycznych, których dane osobowe zawarte są w składanej ofercie lub jakimkolwiek załączniku lub dokumencie składanym w postępowaniu, o przetwarzaniu ich danych osobowych przez Zamawiającego. Wykonawca przekazuje tym osobom informację w następującym zakresie:

2.1. ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych jest Instytut Nafty i Gazu – Państwowy Instytut Badawczy z siedzibą w Krakowie,
ul. Lubicz 25 A, 31-503 Kraków, tel.: +48 12 421 00 33, fax: +48 12 430 38 85, e-mail: office@inig.pl .

2.2. DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych poprzez e-mail: daneosobowe@inig.pl lub pisemnie na adres siedziby administratora.

2.3. ŹRÓDŁO POCHODZENIA DANYCH OSOBOWYCH

Pani/Pana dane osobowe zostały udostępnione Zamawiającemu przez Wykonawcę w związku z ubieganiem się o udzielenie Zamówienia.

2.4. KATEGORIE DANYCH OSOBOWYCH

Zakres przekazanych danych osobowych obejmuje imię i nazwisko, zajmowane stanowisko, nr telefonu służbowego, służbowy adres e-mail. Ponadto w przypadku udzielenia przez Wykonawcę pełnomocnictwa do podpisania oferty lub/oraz przesyłania wraz z ofertą dokumentów (świadectw, certyfikatów, poświadczeń) potwierdzających dysponowanie przez Wykonawcę lub inny podmiot osobami zdolnymi do wykonania Przedmiotu Zamówienia zakres przekazanych danych może dotyczyć również nr pesel, nr dowodu osobistego, daty urodzenia i adresu zamieszkania osoby fizycznej wskazanej w pełnomocnictwie lub w w/w dokumentach. Zakres danych może również obejmować inne dane osobowe, które zostaną przedstawione przez Wykonawcę w składanej ofercie lub jakimkolwiek załączniku lub dokumencie składanym w postępowaniu.

2.5. CELE PRZETWARZANIA I PODSTAWA PRAWNA

Pani/Pana dane będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia nieobjętego przepisami Prawa zamówień publicznych, w tym wyboru najkorzystniejszej oferty, a w razie wyboru oferty – także wykonania umowy zawartej na skutek udzielonego zamówienia.

Podstawa prawną przetwarzania danych są:

a) przepisy prawa (art. 6 ust. 1 lit. c RODO[‡]):

- ustawa z dnia 23.04.1964 r. Kodeks cywilny (w brzmieniu aktualnie obowiązującym),
- ustawy z dnia 6.09.2001 o dostępie do informacji publicznej (w brzmieniu aktualnie obowiązującym),
- ustawa z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym),

b) uzasadniony interes administratora, w tym umożliwienie Zamawiającemu przeprowadzenia postępowania, zawarcia i wykonania umowy oraz ustalenie, dochodzenie lub obrona roszczeń (art. 6 ust. 1 lit. f RODO).

2.6. ODBIORCY DANYCH

Dane pozyskane w związku z postępowaniem mogą być przekazywane wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia jest jawne.

Ponadto odbiorcami danych osobowych mogą być jednostki audytujące, podmioty przetwarzające dane osobowe na zlecenie administratora (np. podmioty obsługujące systemy informatyczne), inne organy w oparciu o przepisy prawa, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu, np. podmioty prowadzące działalność pocztową lub kurierską.

2.7. OKRES PRZECHOWYWANIA DANYCH

Pani/Pana dane osobowe w przypadku postępowań o udzielenie zamówienia nieobjętego przepisami Prawa zamówień publicznych będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt Instytutu Nafty i Gazu – Państwowego Instytutu Badawczego, który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym) został przygotowany w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych.

2.8. PRAWA PODMIOTÓW DANYCH

Przysługuje Pani/Panu:

- prawo dostępu do danych (art. 15 RODO),
- prawo żądania ich sprostowania (art. 16 RODO), przy czym skorzystanie z tego prawa nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w tym zakresie,
- prawo ograniczenia przetwarzania, przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego praw (art. 18 ust. 1 RODO),

[‡]RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 4.05.2016 r., L 119/1 z późn. zm.).

- prawo do usunięcia danych,
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
- prawo sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 21 RODO, z przyczyn związanych z Pani/Pana szczególną sytuacją.

2.9. PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim Pani/Pana zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. W Polsce organem takim jest Urząd Ochrony Danych Osobowych.

2.10. INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH

Podanie danych osobowych w związku udziałem w postępowaniu o zamówienia nieobjętego przepisami Prawa zamówień publicznych jest dobrowolne. Brak podania danych będzie skutkował niemożliwością udziału w prowadzonym postępowaniu, zawarcia i wykonania umowy.

2.11. INFORMACJA O ZAUTOMATYZOWANYM PODEJMOWANIU DECYZJI, W TYM PROFILOWANIU

Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

3. Wykonawca zobowiązany jest do złożenia oświadczenia potwierdzającego wykonanie powyższego obowiązku wobec osób wymienionych w pkt 1 i 2. Treść tego oświadczenia zawarta jest we wzorze FORMLARZA OFERTOWWGO.

4. Wykonawca będący osobą fizyczną, przystępując do Postępowania potwierdza, że jest świadomy informacji o przetwarzaniu danych osobowych w poniższym zakresie:

4.1. ADMINISTRATOR DANYCH OSOBOWYCH

Administratorem danych jest Instytut Nafty i Gazu – Państwowy Instytut Badawczy z siedzibą w Krakowie,
ul. Lubicz 25 A, 31-503 Kraków, tel.: +48 12 421 00 33, fax: +48 12 430 38 85, e-mail: office@inig.pl .

4.2. DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH

Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych poprzez e-mail: daneosobowe@inig.pl lub pisemnie na adres siedziby administratora.

4.3. CELE PRZETWARZANIA I PODSTAWA PRAWNA

Pani/Pana dane będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia nieobjętego przepisami Prawa zamówień publicznych, w tym wyboru najkorzystniejszej oferty, a w razie wyboru oferty – także wykonania umowy zawartej na skutek udzielonego zamówienia.

Podstawa prawną przetwarzania danych są:

a) przepisy prawa (art. 6 ust. 1 lit. c RODO[§]), w tym:
- ustawa z dnia 23.04.1964 r. Kodeks cywilny (w brzmieniu aktualnie obowiązującym),
- ustawy z dnia 6.09.2001 o dostępie do informacji publicznej (w brzmieniu aktualnie obowiązującym),
- ustawa z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym),

b) uzasadniony interes administratora, w tym ustalenie, dochodzenie lub obrona roszczeń związanymi z prowadzonym postępowaniem o udzielnie zamówienia (art. 6 ust. 1 lit. f RODO),

c) w razie zawarcia umowy – w celu jej wykonania– podstawą prawną jest niezbędność przetwarzania do wykonania umowy, której Wykonawca jest stroną lub podjęcie działań na żądanie podmiotu danych przed zawarciem umowy (art. 6 ust. 1 lit b RODO).

4.4. ODBIORCY DANYCH

Dane pozyskane w związku z postępowaniem mogą być przekazywane wszystkim zainteresowanym podmiotom i osobom, gdyż co do zasady postępowanie o udzielenie zamówienia jest jawne.

Ponadto odbiorcami danych osobowych mogą być jednostki audytujące, podmioty przetwarzające dane osobowe na zlecenie administratora (np. podmioty obsługujące systemy informatyczne), inne organy w oparciu o przepisy prawa, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu, np. podmioty prowadzące działalność pocztową lub kurierską.

4.5. OKRES PRZECHOWYWANIA DANYCH

Pani/Pana dane osobowe w przypadku postępowań o udzielenie zamówienia nieobjętego przepisami Prawa zamówień publicznych będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt Instytutu Nafty i Gazu – Państwowego Instytutu Badawczego, który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym) został przygotowany w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych.

4.6. PRAWA PODMIOTÓW DANYCH

Przysługuje Pani/Panu:
- prawo dostępu do danych (art. 15 RODO),
- prawo żądania ich sprostowania (art. 16 RODO), przy czym skorzystanie z tego prawa nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w tym zakresie,
- prawo ograniczenia przetwarzania, przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego praw (art. 18 ust. 1 RODO),
- prawo do usunięcia danych,
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
- prawo sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 21 RODO, z przyczyn związanych z Pani/Pana szczególną sytuacją.

4.7. PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO

Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w

[§]RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 4.05.2016 r., L 119/1 z późn. zm.).

państwie członkowskim Pani/Pana zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. W Polsce organem takim jest Urząd Ochrony Danych Osobowych.

4.8. INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH

Podanie danych osobowych w związku udziałem w postępowaniu o zamówienia nieobjętego przepisami Prawa zamówień publicznych jest dobrowolne. Brak podania danych będzie skutkował niemożliwością udziału w prowadzonym postępowaniu, zawarcia i wykonania umowy.

4.9. INFORMACJA O ZAUTOMATYZOWANYM PODEJMOWANIU DECYZJI, W TYM PROFILOWANIU

Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

12. Załączniki:

Nr 1 – Szczegółowy opis przedmiotu zamówienia;

Nr 2 - Formularz ofertowy;

Nr 3 – Wykaz osób skierowanych do realizacji zamówienia z potwierdzeniem posiadania wymaganych certyfikatów, zgodnie z warunkiem określonym w pkt. 1, ppkt. B), tiret i) Zaproszenia;

Nr 4 – Wykaz usług Wykonawcy potwierdzający spełnienie warunku określonego w pkt. 1, ppkt. B), tiret iii) Zaproszenia;

Nr 5 – Wzór umowy o poufności (NDA).

ZATWIERDZAM

Dyrektor Instytutu Nafty i Gazu – Państwowego Instytut Badawczego

Załącznik nr 1
Nr sprawy: JZDZ-DD-2301-963/2025

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wstęp

1.1 Cel audytu

Instytut Nafty i Gazu - Państwowy Instytut Badawczy, jako Zamawiający, zleca przeprowadzenie oceny skuteczności obecnych zabezpieczeń aplikacji „Moduł KZR" oraz infrastruktury IT w kontekście odporności na cyberataki, a także identyfikację wszelkich ryzyk, które mogą zagrozić bezpieczeństwu organizacji, **w szczególności w kontekście podjętych prac mających na celu integrację aplikacji "Moduł KZR" z Europejską Bazą Danych UDB,** w celu umożliwienia automatycznego przesyłania danych.

Celem audytu jest przeprowadzenie szczegółowej oceny aplikacji internetowej pod kątem bezpieczeństwa, wydajności oraz zgodności z przepisami prawa. Audyt ma na celu identyfikację potencjalnych zagrożeń, słabych punktów oraz wskazanie zaleceń mających na celu poprawę jakości i bezpieczeństwa aplikacji.
Podjęte prace mają zapewnić:

- Przeprowadzenie testów penetracyjnych aplikacji oraz infrastruktury IT w celu symulacji rzeczywistych ataków i identyfikacji słabych punktów systemu - aplikacja internetowa „Moduł KZR" dalej „aplikacja".
- Identyfikację podatności oraz ocena ryzyk związanych z bezpieczeństwem informacji, które mają wpływ na poufność, integralność oraz dostępność przetwarzanych danych.
- Analiza konfiguracji systemów oraz logiki biznesowej aplikacji pod kątem bezpieczeństwa, zgodnie z obowiązującymi standardami (np. OWASP).
- Opracowanie szczegółowych rekomendacji mających na celu usunięcie zidentyfikowanych podatności, minimalizację ryzyka oraz poprawę ogólnego stanu bezpieczeństwa aplikacji.
- Przeprowadzenie re-testów wdrożonych poprawek w celu weryfikacji ich skuteczności oraz aktualizacja raportu końcowego.

1.2 Zakres audytu- opis ogólny

Audyt obejmuje następujące obszary aplikacji internetowej:

- **Bezpieczeństwo** (testy penetracyjne, analiza podatności, zabezpieczenia danych).
- **Wydajność** (obciążenie aplikacji, optymalizacja zasobów).
- **Zgodność z przepisami prawa:**

  1. Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (KSC) (Dz.U.2024.1077 t.j. z dnia 2024.07.19);

  2. Rozporządzenie 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 (Dz.U.2024.773 z dnia 2024.05.22);

  3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2024.1557 t.j. z dnia 2024.10.21);

  4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE z 4.05.2016 r., L 119/1 z późn. zm.);

  5. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781 t.j. z dnia 2019.09.19);

6. Ustawa – Prawo telekomunikacyjne i ustawy sektorowe;
7. Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (KSC) (Dz.U.2024.1077 t.j. z dnia 2024.07.19);
8. Rozporządzenie 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 (Dz.U.2024.773 z dnia 2024.05.22);
9. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2024.1557 t.j. z dnia 2024.10.21).

- **Analiza jakości kodu i architektury aplikacji**.

1.3 Termin realizacji

- I etap – wykonanie całości audytu bezpieczeństwa i testów penetracyjnych i zakończonych przekazaniem raportem końcowym z audytu - 15 dni roboczych od dnia zawarcia umowy,
- II etap – spotkanie Wykonawcy z zespołem technicznym Zamawiającego w celu omówienia wyników oraz ustalenia harmonogramu wdrożenia zaleceń – termin zostanie uzgodniony w trybie roboczym po zakończeniu etapu I,
- III etap – wykonanie re-testów wdrożonych poprawek w celu weryfikacji ich skuteczności oraz aktualizacja raportu końcowego z audytu – po usunięciu podatności przez zamawiającego ale nie później niż w terminie 12 miesięcy od dnia podpisania protokołu odbioru etapu I bez zastrzeżeń. W terminie 5 dni roboczych od daty zakończenia re – testów Wykonawca przekaże zaktualizowany raport końcowy. Łącznie etap III zostanie wykonany nie później niż w terminie 13 miesięcy od dnia podpisania protokołu odbioru etapu I bez zastrzeżeń.

2. Zakres audytu – opis szczegółowy

2.1 **Audyt bezpieczeństwa**

- **Testy penetracyjne**: Przeprowadzenie testów mających na celu identyfikację podatności aplikacji na ataki, z uwzględnieniem specyficznych zagrożeń dla aplikacji.
- **Analiza mechanizmów uwierzytelniania i autoryzacji**: Sprawdzenie efektywności zabezpieczeń w zakresie logowania, autoryzacji użytkowników oraz sesji.
- **Weryfikacja polityki haseł**: Ocena siły haseł użytkowników i mechanizmów ochrony przed atakami typu brute-force,.
- **Analiza podatności na ataki**: Sprawdzanie podatności na ataki takie jak SQL injection, Cross-Site Scripting (XSS) czy Cross-Site Request Forgery (CSRF),.
- **Zabezpieczenia danych osobowych**: Weryfikacja zgodności z RODO (GDPR) i najlepszymi praktykami ochrony danych osobowych w aplikacjach internetowych

2.2 **Audyt wydajności**

- **Testy obciążeniowe**: Przeprowadzenie testów mających na celu określenie, jak aplikacja działa pod dużym obciążeniem, np. przy dużej liczbie jednoczesnych użytkowników.
- **Optymalizacja zapytań do bazy danych**: Weryfikacja zapytań SQL w kontekście Identyfikacja ewentualnych problemów z wydajnością, takich jak zbyt duża liczba zapytań do bazy danych lub nieoptymalne zapytania.
- **Analiza frontendu i back-endu**: Ocena wydajności frontendu (np. React, Angular, jeśli wykorzystywane) oraz backendu aplikacji.

2.3 **Audyt zgodności z przepisami**

- **Zgodność z RODO**: Weryfikacja zgodności aplikacji z przepisami ochrony danych osobowych (RODO), w tym implementacja mechanizmów ochrony danych wrażliwych w aplikacjach internetowych,
- **Dostępność aplikacji**: Audyt zgodności aplikacji z wytycznymi WCAG (Web Content Accessibility Guidelines), w celu zapewnienia dostępności dla osób z niepełnosprawnościami,

- **Zgodność z przepisami**:
  a. Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (KSC) (Dz.U.2024.1077 t.j. z dnia 2024.07.19);
  b. 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 (Dz.U.2024.773 z dnia 2024.05.22);
  c. Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2024.1557 t.j. z dnia 2024.10.21).

2.4 **Analiza kodu źródłowego**

- **Przegląd jakości kodu**: Ocena jakości kodu źródłowego, w tym analiza struktury aplikacji, organizacji kodu oraz zgodności z najlepszymi praktykami programowania.
- **Weryfikacja dokumentacji technicznej**: Sprawdzenie kompletności dokumentacji oraz zgodności kodu z wymaganiami projektowymi i architektonicznymi.

3. Wymagania techniczne

3.1 **Opis aplikacji oraz technologii**

Aplikacja „Moduł KZR" składa się z modułu administracyjnego (aplikacja główna) oraz modułu dla klientów (aplikacja BOK dla uczestników i jednostek certyfikujących).

Moduł administracyjny KZR obejmuje następujące funkcjonalności:

- Wnioski o rejestrację – rejestr elektronicznych wniosków o rejestrację w Systemie KZR, złożonych przez stronę internetową w aplikacji BOK, rejestr umożliwia obsługę wniosku przez pracowników INiG-PIB;
- Wnioski o odnowienie umowy – wnioski Uczestników o odnowienie umowy złożone w aplikacji
- BOK;
- Wnioski o zmianę danych Uczestnika – wnioski o zmianę danych Uczestnika, złożone przez aplikację BOK, zatwierdzenie wniosku automatycznie aktualizuje dane Uczestnika we wskazanym zakresie;
- Klienci – rejestr uczestników Systemu KZR, zawiera dane szczegółowe klienta oraz zakładki z danymi dodatkowymi: lista kont klienta, lista certyfikatów, lista audytów, raporty kwartalne, wnioski
- Jednostki Certyfikujące
- Audyty
- Certyfikaty KZR
- Certyfikaty KZR (uzupełnienie rejestru)
- Raporty kwartalne
- Raporty Jednostek
- Raporty rozbieżności
- Raporty do KE
- Raporty UDB
- Wiadomości
- Ważne dokumenty
- Konfiguracja

Moduł dla klientów (BOK) obejmuje:

- Ekran dla Uczestnika
- Ekran dla Jednostki Certyfikującej

Zarządzanie systemem. Moduł administracyjny, obejmujący:

- Konta użytkowników – rejestr użytkowników systemu, umożliwia zarządzanie kontami (m.in. login, hasło, czy aktywny, wymuszenie zmiany hasła, możliwa autoryzacja przez LDAP, przydział do grup, uprawnienia, log aktywności);
- Grupy systemowe – umożliwia tworzenie grup użytkowników, w ramach grupy możliwy przydział uprawnień, użytkownik może należeć do wielu grup;
- Struktura organizacyjna – zarządzanie strukturą organizacyjną (hierarchiczne drzewo komórek organizacyjnych), użytkownik może należeć tylko do jednej komórki organizacyjnej;
- Obszary zarządzania – funkcja umożliwia tworzenie obszarów informacji w ramach aplikacji, do których dostęp mają wskazane grupy użytkowników, obszar może zawierać hierarchiczną listę kategorii dokumentów, dla których możliwe jest nadanie szczegółowych uprawnień;
- Uprawnienia do dokumentów – funkcja umożliwiająca przydział uprawnień do wybranych kategorii dokumentów w dostępnych obszarach zarządzania dla wskazanych grup użytkowników;
- Słowniki – zestaw parametrów systemowych, pogrupowanych w hierarchiczne kategorie, zawierające listy elementów (klucz – wartość);
- Szablony dokumentów – rejestr szablonów dokumentów, umożliwia wersjonowanie wzorów dokumentów, szablon może zawierać znaczniki, które podczas wydruku zostaną uzupełnione danymi z systemu;
- Zadania serwisowe – rejestr zadań serwisowych (wykonywanych cyklicznie przez aplikację serwisową), umożliwia włączenie/wyłączenie zadania, zmianę częstotliwości wykonywania zadania i ustawienie parametrów zadania, zawiera również historię wykonanych zadań z informacją, czy zadanie wykonało się prawidłowo, czy wystąpił błąd;
- Log systemowy – historia wszystkich akcji podjętych przez użytkowników w systemie (zalogowanie do aplikacji, dodanie, modyfikacja lub usunięcie danych).

W aplikacji funkcjonują głównie ekrany list i ekrany szczegółów, natomiast ekrany szczegółów zawierają zakładki, na których znajdują się formularze (z możliwością wprowadzania/edycji danych) lub listy obiektów zależnych.
Poniżej tabela z liczbą ekranów i zakładek w każdym z modułów

MODUŁ	EKRANY LIST	EKRANY SZCZEGÓŁÓW	ZAKŁADKI
Rejestr pism	5	5	18
Certyfikacja	6	2	8
KZR	16	17	102
Rejestry pomocnicze	6	7	16
Zarządzanie systemem	10	9	25
RAZEM	**48**	**40**	**169**

Poziomy uprawnień użytkowników.
W aplikacji są trzy stany związane z pojedynczym uprawnieniem:
- brak prawa (uprawnienie nieustawione/niezaznaczone),
- prawo przyznane,
- prawo odebrane.

Użytkownik może posiadać prawa indywidualne oraz prawa grupowe, wynikające z przynależności użytkownika do różnych grup. Efektywne uprawnienia użytkownika wynikają z sumy praw grupowych i indywidualnych z zastosowaniem następujących zasad:

- odmowa uprawnienia ma wyższy priorytet niż nadanie uprawnienia,
- prawa indywidualne mają wyższy priorytet niż prawa grupowe.

Stąd też wynika następująca hierarchia uprawnień (od najniższego priorytetu do najwyższego):

1. przyznanie prawa grupowego
2. odmowa prawa grupowego
3. przyznanie prawa indywidualnego
4. odmowa prawa indywidualnego

3.2 **Zewnętrzne API i integracje**

Aplikacja obecnie nie integruje się z zewnętrznymi API.

3.3 **Infrastruktura serwerowa**

Aplikacja zainstalowana jest na dwóch serwerach wirtualnych działających na systemach operacyjnych Windows Server w odizolowanej sieci VLAN.

Szczegółowe informacje „PBC.ERP-INiG - informacje do audytu.pdf", „Opis infrastruktury serwerowej", „Schemat_sieci_KZR" które zostaną dostarczone Wykonawcy po podpisaniu umowy NDA. Wzór umowy NDA jest dokumentem Zamawiającego i nie podlega negocjacją i zmianie.

4. Metodyka audytu

4.1 **Analiza statyczna**

Audytorzy przeprowadzą analizę statyczną kodu źródłowego aplikacji, w tym:

- Sprawdzenie struktury aplikacji, organizacji plików, zgodności z wytycznymi kodowania.
- Identyfikacja problemów z bezpieczeństwem i wydajnością w kodzie oraz wykorzystanych bibliotek.

4.2 **Testy dynamiczne**

Audyt obejmuje testy dynamiczne, w tym:

- Testy penetracyjne (manualne i automatyczne) przy użyciu narzędzi takich jak Burp Suite, OWASP ZAP, oraz specyficzne testy podatności dla aplikacji.
- Testy funkcjonalności i integralności aplikacji w warunkach rzeczywistych, w tym interakcja z bazą danych

4.3 **Używane narzędzia audytowe**

Audyt będzie przeprowadzony z użyciem następujących narzędzi lub równoważnych:

- **Burp Suite** – do testów penetracyjnych aplikacji webowej.
- **OWASP ZAP** – do automatycznego skanowania aplikacji pod kątem podatności.
- **Nessus** – do skanowania infrastruktury i aplikacji pod kątem luk bezpieczeństwa.
- **Fiddler** lub **Wireshark** – do analizy ruchu sieciowego i wykrywania podatności związanych z komunikacją między aplikacją a serwerem.

5. Raport z audytu

5.1 **Raport końcowy**

Po zakończeniu audytu, Wykonawca dostarczy szczegółowy raport, który będzie zawierał:

- **Podsumowanie wyników**: Krótkie podsumowanie wyników audytu.
- **Zidentyfikowane problemy**: Szczegółowy opis problemów, luk i zagrożeń.
- **Zalecenia naprawcze**: Konkretne rekomendacje mające na celu poprawę jakości aplikacji.
- **Priorytety działań**: Określenie priorytetów dla działań naprawczych w zależności od wagi zidentyfikowanych problemów.

5.2 **Prezentacja wyników**

Po przedstawieniu raportu odbędzie się spotkanie z zespołem technicznym w celu omówienia wyników oraz ustalenia harmonogramu wdrożenia zaleceń.

6. Inne wymagania

Wykonawca podpisze porozumienie o zachowaniu o poufności (NDA) według wzoru dostarczonego przez Zamawiającego. Porozumienie o zachowaniu poufności będzie stanowiło załącznik do umowy o realizację zamówienia. Na etapie realizacji zamówienia Zamawiający będzie oczekiwał ponadto, aby wszystkie osoby z ramienia Wykonawcy zaangażowane w audyt podpisały indywidualne

oświadczenia zobowiązujące je do zachowania poufności według wzoru dostarczonego przez Zamawiającego.
W przypadku, jeżeli na etapie składania ofert Wykonawca będzie oczekiwał udzielenia dalszych informacji dotyczących przedmiotu zamówienia (innych niż przedstawione w zapytaniu ofertowym) warunkiem przekazania tych informacji przez Zamawiającego osobie/podmiotowi żądającej/emu informacji będzie podpisanie przez ten podmiot/osobę porozumienia o zachowaniu poufności (NDA) według wzoru dostarczonego przez Zamawiającego.

Załącznik nr 2
Nr sprawy: JZDZ-DD-2301-963/2025

FORMULARZ OFERTOWY

Nazwa Wykonawcy: ……..

Adres Wykonawcy: ……

Numer NIP: ……

E-mail: ……...

oferujemy wykonanie usługi **przeprowadzenia audytu bezpieczeństwa i testów penetracyjnych aplikacji internetowej „Moduł KZR":**

cena netto: ……... zł.
plus obowiązująca stawka podatku od towarów i usług VAT: ……%
brutto: ……... zł.
(słownie: .....)

Podana cena jest obowiązująca w całym okresie ważności umowy.
*W przypadku złożenia oferty przez Wykonawcę będącego osobą zagraniczną, nie podlegającą obowiązkowi podatkowemu na terenie Rzeczpospolitej Polskiej, zobowiązany jest on zamieścić taką informację wraz z podaną ceną. Wykonawca zagraniczny **podaje tylko cenę ofertową netto**. Zamawiający, w celu zapewnienia możliwości porównania cen, doliczy do ceny oferty podatek VAT.*

Termin realizacji zamówienia:

- I etap – wykonanie całości audytu bezpieczeństwa i testów penetracyjnych i zakończonych przekazaniem raportem końcowym z audytu - 15 dni roboczych od dnia zawarcia umowy,
- II etap – spotkanie Wykonawcy z zespołem technicznym Zamawiającego w celu omówienia wyników oraz ustalenia harmonogramu wdrożenia zaleceń – termin zostanie uzgodniony w trybie roboczym po zakończeniu etapu I,
- III etap – wykonanie re-testów wdrożonych poprawek w celu weryfikacji ich skuteczności oraz aktualizacja raportu końcowego z audytu – po usunięciu podatności przez zamawiającego ale nie później niż w terminie 12 miesięcy od dnia podpisania protokołu odbioru etapu I bez zastrzeżeń. W terminie 5 dni roboczych od daty zakończenia re – testów Wykonawca przekaże zaktualizowany raport końcowy. Łącznie etap III zostanie wykonany nie później niż w terminie 13 miesięcy od dnia podpisania protokołu odbioru etapu I bez zastrzeżeń.

Osoba do kontaktu: ……..
tel. ……..……., e-mail ……..

Oświadczamy, że posiadamy wszelkie uprawnienia, kwalifikacje i możliwości potrzebne dla zrealizowania przedmiotu zapytania.

Oświadczamy, że uważamy się za związanych niniejszą ofertą przez okres 30 dni od upływu ostatecznego terminu składania ofert.
Oświadczamy, że zobowiązujemy się w przypadku wybrania naszej oferty do zawarcia umowy na warunkach określonych przez Zamawiającego.

Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić

do powstania u Zamawiającego obowiązku podatkowego, zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług, wskazując nazwę (rodzaj) towaru, których dostawa będzie prowadzić do jego powstania, wskazując ich wartość bez kwoty podatku VAT oraz wskazując stawki podatku od towaru i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.

☐ Wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług**.**

lub

☐ Wybór naszej oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, w związku z tym podajemy wartość bez kwoty podatku VAT. Poniżej wskazujemy nazwę/rodzaj towaru

Nazwa/rodzaj towaru:.....
….....

Wartość wskazanych towarów: ……. zł. netto

Stawka podatku od towaru i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie: …….. %

W przypadku, gdy Wykonawca nie zaznaczy w formularzu ofertowym odpowiednich informacji, Zamawiający przyjmuje, że wybór oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego.

Oświadczenie Wykonawcy w zakresie przekazywania osobom, których dane osobowe zawarte są w składanej ofercie lub jakimkolwiek załączniku lub dokumencie składanym w postępowaniu informacji o przetwarzaniu danych osobowych.

Oświadczam/y, że:

1. Wykonawca wypełnił obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[**] wobec osób fizycznych, od których dane osobowe zostały bezpośrednio lub pośrednio pozyskane w celu ubiegania się o udzielenie zamówienia w niniejszym postępowaniu;
2. Wykonawca poinformował wszystkie osoby fizyczne, których dane zostały przekazane Zamawiającemu w związku z prowadzonym postępowaniem, o przetwarzaniu ich danych osobowych przez Zamawiającego, zgodnie z treścią rozdz. 11 ZAPROSZENIA DO SKŁADANIA OFERT.
3. Wykonawca zobowiązuje się do przekazania informacji, w zakresie, o którym mowa w pkt 2) powyżej, także osobom, których dane zostaną przekazane Zamawiającemu w ww. celu na dalszych etapach postępowania.

Załącznikami do niniejszego formularza ofertowego są:

- Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
- Wykaz inżynierów będących w dyspozycji Wykonawcy potwierdzający spełnienie warunku określonego w pkt. 1, ppkt. B), tiret i) Zaproszenia;
- Certyfikat ISO 27001 lub dokument potwierdzający posiadanie i wdrożenie systemu zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001;
- Wykaz usług Wykonawcy potwierdzający spełnienie warunku określonego w pkt. 1, ppkt. B), tiret iii) Zaproszenia;
- Dokumenty / referencje potwierdzające wykonywanie usług wskazanych w wykazie;
- Sprawozdanie z wyników audytu – raport końcowy (szablon);

[**] rozporządzenie 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. Urz. UE L 119 z 04.05.2016, str. 1).

- Kserokopia polisy wraz z Ogólnymi Warunkami Ubezpieczenia i potwierdzeniem zapłaty składki/składek – jeśli Wykonawca posiada;
- Pełnomocnictwo w przypadku, gdy dokumenty podpisywane są przez osobę inną niż wskazana w dokumentach rejestrowych, upoważnioną do reprezentowania Wykonawcy.
- ……

.....

podpis osoby / osób upoważnionych do reprezentowania Wykonawcy

Załącznik nr 3
Nr sprawy: JZDZ-DD-2301-963/2025

WYKAZ OSÓB, KTÓRE BĘDĄ UCZESTNICZYĆ W WYKONANIU ZAMÓWIENIA

Wykaz osób skierowanych do realizacji zamówienia z potwierdzeniem posiadania wymaganych certyfikatów, zgodnie z warunkiem określonym w pkt. 1, ppkt. B), tiret i) Zaproszenia.

Lp.	Imię i nazwisko	Informacje na temat kwalifikacji zawodowych, niezbędnych do wykonania zamówienia*	Posiadane certyfikaty związane z bezpieczeństwem IT*	Zakres powierzonych czynności	Podstawa dysponowania osobą**
1.					
2.					
3.					

***** Wykonawca powinien podać informacje, na podstawie których Zamawiający będzie mógł ocenić spełnienie warunku.

****** W przypadku, gdy wskazana osoba jest Wykonawcą lub związana jest z Wykonawcą stosunkiem prawnym: pracownik Wykonawcy (umowa o pracę), Zleceniobiorca na podstawie umowy cywilno-prawnej (np. umowa zlecenie, umowa o dzieło), itp. - w tabeli należy wpisać „zasób własny".
W przypadku, gdy wskazana osoba jest udostępniona Wykonawcy przez inny podmiot będący jej pracodawcą w tabeli należy wpisać „zasób udostępniony". W takiej sytuacji należy złożyć zobowiązanie podmiotu udostępniającego zasoby, do oddania ich do dyspozycji - na okres ich udziału w wykonaniu zamówienia.

**niepotrzebne skreślić*

.....
podpis osoby / osób upoważnionych do reprezentowania Wykonawcy

Załącznik nr 4
Nr sprawy: JZDZ-DD-2301-963/2025

WYKAZ USŁUG WYKONAWCY

Wykaz zrealizowanych usług, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, potwierdzających spełnienie warunku określonego w pkt. 1, ppkt. B), tiret iii) Zaproszenia

Lp.	*Nazwa i adres Zlecającego*	*Opis wykonanych usług*	*Okres wykonania (data rozpoczęcia – data zakończenia)*
1	*2*	*3*	*4*
1.			
2.			
3.			

Dowody potwierdzające, iż wykazane usługi zostały wykonane należycie stanowi załącznik do niniejszego wykazu. Tylko zamówienia potwierdzone tymi dowodami będą uwzględniane w ocenie spełnienia tego warunku.

Dowodami, o których wyżej mowa, są:
- referencje bądź inne dokumenty wystawione przez podmiot, na rzecz, którego dostawy były wykonywane,
- oświadczenie Wykonawcy – jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać dokumentów, o którym wyżej mowa.

*Oświadczam, iż wykazane powyżej usługi zostały wykonane przez Wykonawcę, którego reprezentuję.
lub
*Oświadczam, iż wykazując spełnianie warunku polegam na wiedzy i doświadczeniu podmiotu/firmy: ..... z siedzibą w ..... przy ul. ..... nr ..... i w związku z tym składam pisemne zobowiązanie tego podmiotu** do oddania Wykonawcy do dyspozycji wiedzy i doświadczenia na okres korzystania z niego przy wykonywaniu zamówienia.

* niepotrzebne skreślić

.....
podpis osoby / osób upoważnionych do reprezentowania Wykonawcy

Załącznik nr 5
Nr sprawy: JZDZ-DD-2301-963/2025

Porozumienie o zachowaniu poufności
(„Porozumienie")

zawarte dnia ..... w Krakowie pomiędzy:
1. Instytutem Nafty i Gazu – Państwowym Instytutem Badawczym z siedzibą w Krakowie, pod adresem: ul. Lubicz 25 A, 31-503 Kraków, wpisanym do rejestru przedsiębiorców przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000075478, NIP 6750001277, REGON: 000023136, reprezentowanym przez:
Jana Brożka – Dyrektora Instytutu, uprawnionego do samodzielnej reprezentacji,

zwaną dalej „**INIG – PIB**" lub „**Stroną przekazującą**",
a
2. _____ [nazwa spółki] z siedzibą w_____, pod adresem: _____, wpisaną do rejestru przedsiębiorców przez Sąd Rejonowy dla _____ w _____, Wydział ___ Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS _____, NIP: _____, REGON: _____, kapitał zakładowy: _____ zł, reprezentowaną przez:
_____ – członka Zarządu, uprawnionego do samodzielne reprezentacji/_____ oraz _____ - członków Zarządu, uprawnionych do łącznej reprezentacji,

zwaną dalej „**Podmiotem**" lub „**Stroną odbierającą**",

a łącznie zwanymi „**Stronami**", a każda z osobna „**Stroną**"
Zważywszy, że:
- Strony prowadzą negocjacje w celu uzgodnienia warunków współpracy dotyczących przeprowadzenia **Audytu bezpieczeństwa oraz testów penetracyjnych aplikacji internetowej „Moduł KZR"** (dalej: „**Projekt**"),
- negocjacje wiążą się możliwością uzyskania przez Podmiot dostępu do wielu istotnych informacji z punktu widzenia interesu INIG – PIB, w tym takich, które mogą stanowić jego tajemnicę przedsiębiorstwa lub jego kontrahentów, oraz przez INIG – PIB dostępu do wielu istotnych informacji z punktu widzenia interesu Podmiot,
Strony postanawiają co następuje:

§ 1.

1. Informacjami Poufnymi w rozumieniu Porozumienia są:
   1) wszelkie informacje dotyczące aplikacji internetowej „Moduł KZR" i innych systemów informatycznych, z których korzysta INiG-PIB oraz infrastruktury technicznej INiG-PIB, niezależnie od formy i sposobu pozyskania przez Podmiot, a także bez konieczności ich jakiegokolwiek oznaczania przez INiG-PIB,
   2) wszelkie inne informacje przekazane przez Stronę przekazującą lub osoby działające w jej imieniu (w jakiejkolwiek formie tj. w szczególności ustnej, pisemnej, elektronicznej) Stronie odbierającej, w szczególności dotyczące Projektu, a także informacje uzyskane przez Stronę odbierającą w inny sposób w trakcie wzajemnej współpracy w ramach Projektu, jak i w toku negocjacji warunków współpracy w ramach Projektu, które to informacje dotyczą Strony przekazującej lub jej kontrahentów, w tym także dokumenty opracowane w ramach realizacji Projektu, bez konieczności ich jakiegokolwiek oznaczania,

   dalej „**Informacje Poufne**".

2. Informacje Poufne przekazane przez Stronę przekazującą, pozostają jej własnością. Przekazanie jakiejkolwiek Informacji Poufnej Stronie odbierającej nie może być traktowane jako udzielenie licencji lub przekazanie jakichkolwiek praw do tej informacji.

§ 2.

1. Strona odbierająca zobowiązuje się:
   1) nie wykorzystywać Informacji Poufnych, w innym celu, niż dla realizacji Projektu,
   2) zachować w tajemnicy Informacje Poufne i nie ujawniać ich osobom trzecim,
   3) zwrócić niezwłocznie Stronie przekazującej, na każde jej żądanie, nie później niż w terminie 10 dni od dnia otrzymania takiego żądania, wszelkie otrzymane od Strony przekazującej dokumenty w jakiejkolwiek postaci lub nośniki danych, zawierające Informacje Poufne, a gdyby zwrot nie był możliwy z jakiegokolwiek powodu, zniszczyć posiadane dane lub dokumenty bez pozostawiania kopii i poinformować o tym fakcie na piśmie Stronę przekazującą, z zastrzeżeniem zdań następnych. Strona przekazująca może zażądać zwrotu lub zniszczenia nośników Informacji Poufnych, w każdym terminie,
   4) informować Stronę przekazującą niezwłocznie na piśmie (lub za pośrednictwem e-mail) o każdym wiadomym Stronie odbierającej, nieuprawnionym (także przez osoby trzecie), w tym z naruszeniem Porozumienia, wykorzystaniu Informacji Poufnych, niezależnie od źródła i sposobu uzyskania tej wiedzy;
   5) zachować szczególną dbałość o zachowanie poufności, integralności i dostępności informacji zawartych zarówno w przekazanych mi dokumentach w formie papierowej jak również w elektronicznej, jak i na innych nośnikach danych, oraz chronienia informacji oraz nośników, na których są utrwalone, przed ich przypadkowym lub umyślnym zniszczeniem, utratą lub nieuprawnioną modyfikacją.
2. Obowiązek zachowania poufności nie dotyczy sytuacji, gdy Strona odbierająca wykaże, że:
   1) Informacje Poufne stały się publicznie dostępne, w inny sposób niż przez naruszenie Porozumienia,
   2) Strona przekazująca udzieliła uprzedniej, pisemnej pod rygorem nieważności zgody na ujawnienie Informacji Poufnej,
   3) Informacje Poufne w dniu podpisania Porozumienia były informacjami dostępnymi publicznie,
   4) została zobowiązana do ujawienia Informacji Poufnej przez organ państwowy, sąd lub organ ścigania, jeżeli obowiązek ujawnienia Informacji Poufnej wynika w tej sytuacji z bezwzględnie obowiązujących przepisów prawa, przy czym Strona odbierająca zobowiązana jest w takiej sytuacji niezwłocznie powiadomić Stronę przekazującą o takim żądaniu (o ile nie będzie to pozostawało w sprzeczności z obowiązującymi przepisami prawa), a w razie możliwości, podjąć wszelkie przewidziane prawem działania, zmierzające do uchylenia się od takiego obowiązku. W każdym przypadku ujawnienia Informacji Poufnych zgodnie z niniejszym punktem, Strona odbierająca zobowiązana jest do ujawnienia tylko takiej części Informacji Poufnych, jaka jest wymagana przez bezwzględnie obowiązujące przepisy oraz do podjęcia wszelkich możliwych działań celem zapewnienia, iż ujawnione Informacje Poufne będą traktowane w sposób poufny i wykorzystywane tylko dla celów uzasadnionych celem ujawnienia.
3. Strona odbierająca zobowiązuje się chronić Informacje Poufne z należytą starannością, stosując do nich środki ochrony nie mniejsze niż stosowane do ochrony własnych informacji poufnych, o ile większy zakres ochrony nie wynika z Porozumienia. Strona odbierająca zapewnia, że stosowane przez nią środki ochrony oraz środki zabezpieczające zapewniają odpowiednią ochronę przed nieupoważnionym ujawnieniem, kopiowaniem lub wykorzystywaniem Informacji Poufnych, przez jakiekolwiek osoby trzecie.

4. Strona odbierająca zobowiązuje się zapewnić, że jego pracownicy lub podwykonawcy, konsultanci i doradcy, którzy uzyskają dostęp do Informacji Poufnych w okresie obowiązywania obowiązku zachowania poufności, są (lub zostaną) zobowiązani na piśmie do ochrony tych informacji (w tym także po rozwiązaniu stosunku pracy). Strona odbierająca zapewni, że Informacje Poufne będą przekazywane pracownikom, podwykonawcom, konsultantom lub doradcom tylko w przypadku, gdy będzie to konieczne i po uzyskaniu od tych osób pisemnego zobowiązania do zachowania poufności według wzoru dostarczonego przez Zamawiającego z zastrzeżeniem zdania następnego. Z podwykonawcami Podmiot zobowiązany jest podpisać przez przekazanie Informacji Poufnych porozumienie o zachowaniu poufności na warunkach analogicznych jak niniejsze..
5. Strona odbierająca obowiązana jest zapewnić środki bezpieczeństwa i sposoby bezpiecznego przechowywania Informacji Poufnych oraz dołożyć wszelkich starań by zapobiec jakiemukolwiek nieupoważnionemu wykorzystaniu, ujawnieniu, czy dostępowi do tych informacji.
6. Wszelkie działania lub zaniechania osób wskazanych ust. powyżej, mających dostęp do Informacji Poufnych, traktowane będą jak działania i zaniechania Strony odbierającej.
7. Strona odbierająca przyjmuje do wiadomości, iż:
   1) Informacje Poufne mogą być także chronione na podstawie powszechnie obowiązujących przepisów, jak w szczególności ustawa o zwalczaniu nieuczciwej konkurencji, ustawa o ochronie danych osobowych lub ustawa o ochronie informacji niejawnych,
   2) postępowanie sprzeczne z zobowiązaniami przyjętymi w Porozumieniu może stanowić podstawę odpowiedzialności karnej i cywilnej osoby naruszającej te zobowiązania.

§ 3.

Porozumienie wchodzi w życie z dniem jego zawarcia i obowiązuje przez okres 5 lat.

§ 4.

W przypadku naruszenia przez Podmiot któregokolwiek z postanowień Porozumienia, INIG-PIB będzie uprawniony do obciążenia Podmiotu karą umowną w wysokości 200 000 zł (słownie: dwieście tysięcy złotych, 00/100) za każdy przypadek naruszenia. INIG-PIB będzie uprawniony do dochodzenia odszkodowania przekraczającego zastrzeżoną wysokość kar umownych. Powyższe nie wyłącza w żaden sposób innych sankcji i uprawnień INIG-PIB określonych w Porozumieniu oraz przepisach prawa, w tym w ustawie o zwalczaniu nieuczciwej. Kara umowna staje się wymagalna w terminie 7 dni od daty wezwania o jej zapłaty Podmiotu.

§ 5.

1. Na potrzeby realizacji Porozumienia Strony jako niezależni administratorzy danych udostępniać będą sobie nawzajem dane osobowe swoich reprezentantów lub przedstawicieli wskazanych w Porozumieniu oraz innych osób w związku z realizacją Porozumienia w zależności od potrzeb wynikających z postanowień Porozumienia.
2. Każda ze Stron zobowiązuje się do zabezpieczenia danych osobowych poprzez podjęcie odpowiednich środków technicznych i organizacyjnych wymaganych obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, jak też ponosi wszelką odpowiedzialność za szkody wyrządzone w związku z przetwarzaniem danych osobowych.
3. Strony zobowiązują się do poinformowania osób wymienionych w ust. 1 w terminie najpóźniej miesiąca po pozyskaniu danych osobowych lub przy pierwszej komunikacji z osobą, której dane dotyczą o konieczności przekazania ich danych na potrzeby realizacji Porozumienia, w tym o celu i zakresie przekazania danych, wskazanych w załączniku nr 1.

§ 6.

1. Wszelkie zmiany niniejszego Porozumienia wymagają formy pisemnej (lub elektronicznej z elektronicznym podpisem kwalifikowanym) pod rygorem nieważności.

2. Spory, wynikłe na tle realizacji lub zawarcia Porozumienia, będą rozstrzygane przez sąd miejscowo właściwy dla INIG – PIB.
3. Załączniki i aneksy do niniejszej Porozumienia stanowią jego integralną część.
4. Wszelkie oświadczenia, zawiadomienia oraz zgłoszenia dokonywane przez Strony, winny być dokonywane wyłącznie w formie pisemnej (lub elektronicznej). Strony ustalają, że adresy podane na wstępie Porozumienia są właściwe dla doręczeń. Strony zobowiązują się do niezwłocznego zawiadamiania o wszelkich zmianach adresów dla doręczeń pod rygorem uznania doręczenia pod ostatni wskazany adres za skuteczne.
5. W wypadku, gdy którekolwiek z postanowień Porozumienia okaże się z jakiejkolwiek przyczyny nieważne lub nieskuteczne, pozostałe postanowienia Porozumienia pozostają w całości ważne i skuteczne. Strony zastąpią nieważne lub nieskuteczne postanowienia Porozumienia takimi postanowieniami, które z punktu widzenia ekonomicznych i prawnych interesów Stron będą mogły zostać uznane na porównywalne.
6. Porozumienie sporządzono i podpisano w dwóch jednobrzmiących egzemplarzach po jednym dla każdej Strony.

W imieniu INIG – PIB: **W imieniu Podmiotu:**

Załącznik nr 1 do Porozumienia

KLAUZULA INFORMACYJNA

1. Administratorem danych jest Instytut Nafty i Gazu – Państwowy Instytut Badawczy z siedzibą w Krakowie, ul. Lubicz 25 A, 31-503 Kraków, tel.: +48 12 421 00 33, fax: +48 12 430 38 85, e-mail: office@inig.pl .
2. Z inspektorem ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych poprzez e-mail: daneosobowe@inig.pl lub pisemnie na adres siedziby administratora.
3. Pani/Pana dane osobowe, które zostały przekazane do Instytutu Nafty i Gazu – Państwowego Instytutu Badawczego przez ..... - podmiot współpracujący z INiG – PIB lub zamierzający współpracować z INiG – PIB stanowią, w zależności od rodzaju współpracy, dane niezbędne do reprezentacji osoby prawnej, dane identyfikacyjne (m.in. imię i nazwisko, dane ujawnione w rejestrach publicznych), dane kontaktowe (m.in. służbowy adres e-mail, służbowy numer telefonu, firma reprezentowanego podmiotu), dane zawarte w posiadanych przez Panią/Pana dokumentach potwierdzających uprawnienia lub doświadczenie.
4. Dane osobowe będą przetwarzane w celach:
   4.1. wypełnienia obowiązku prawnego, który ciąży na INiG – PIB, w tym związanym z archiwizacją, rozliczeniami księgowymi, podatkowymi, obsługą procesu reklamacji, innymi obowiązkami prawnymi nałożonymi na INiG – PIB (art. 6 ust. 1 lit. c) RODO),
   4.2. prawnie uzasadnionych interesów administratora, w tym zawarcia, wykonywania i monitorowania realizacji Umowy, której stroną jest klient/kontrahent INiG – PIB, określenia osób uprawnionych do reprezentacji podmiotu, bieżącego kontaktu i współpracy związanej z realizowaną umową, ustalenia, dochodzenia lub obrony przed roszczeniami (art. 6 ust. 1 lit. f) RODO).
5. Odbiorcami danych osobowych mogą być jednostki audytujące, podmioty przetwarzające dane osobowe na zlecenie administratora (np. podmioty obsługujące systemy informatyczne), inne organy w oparciu o przepisy prawa, jak również inni administratorzy danych osobowych przetwarzający dane we własnym imieniu, np. podmioty prowadzące działalność pocztową lub kurierską.
6. Dane osobowe nie będą przekazywane do państw trzecich lub organizacji międzynarodowej.
7. Dane osobowe będą przechowywane przez 2 lata od zakończenia realizacji umowy, a także po jej zakończeniu przez czas związany z wygaśnięciem roszczeń związanych z umową, przez czas określony przepisami podatkowymi oraz przepisami dotyczącymi sprawozdawczości finansowej a następnie, jeśli chodzi o materiały archiwalne, będą przechowywane przez okres oznaczony kategorią archiwalną wskazaną w Jednolitym Rzeczowym Wykazie Akt Instytutu Nafty i Gazu – Państwowego Instytutu Badawczego, który zgodnie z art. 6 ust. 2 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (w brzmieniu aktualnie obowiązującym) został przygotowany w porozumieniu z Naczelnym Dyrektorem Archiwów Państwowych.
8. Osobie której dane są przewarzane przysługuje: prawo dostępu do danych (art. 15 RODO), prawo żądania ich sprostowania (art. 16 RODO), prawo do usunięcia w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej (art. 17 RODO), prawo ograniczenia przetwarzania, przy czym przepisy odrębne mogą wyłączyć możliwość skorzystania z tego prawa (art. 18 ust. 1 RODO), prawo sprzeciwu wobec przetwarzania (art. 21 ust. 1 RODO).
9. Osobie której dane są przewarzane przysługuje prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim jej zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia. W Polsce organem takim jest Urząd Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza obowiązujące przepisy o ochronie danych osobowych.

10. Podanie danych osobowych jest dobrowolne, ale stanowi warunek zawarcia/realizacji umowy. Konsekwencją niepodania danych jest brak możliwości nawiązania lub kontynuowania współpracy.
11. Dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu