

11.08.2026

Zapytanie ofertowe numer: PSG/2/001983/26

Polska Spółka Gazownictwa sp. z o.o. z siedzibą w Tarnowie, ul. Wojciecha Bandrowskiego 16, 33-100 Tarnów, Oddział Wsparcia w Warszawie, adres: ul. Krucza 6/14, 00-537 Warszawa, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia w Krakowie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000374001, NIP 525 24 96 411, REGON 142739519, będąca czynnym podatnikiem podatku VAT zaprasza do złożenia oferty:

„Serwisowanie i konserwacja systemu zarządzania drukiem SafeCom oraz usługa wsparcia technicznego (maintenance) producenta oprogramowania SafeCom.”

Polska Spółka Gazownictwa sp. z o.o. (dalej: PSG) w zakresie ww. postępowania planuje podpisanie umowy jednorazowej.

I. WARUNKI SKŁADANIA OFERT:

1. Oferent przyjmuje do wiadomości i akceptuje, że złożenie oferty odbywa się w ramach postępowania zakupowego prowadzonego przez PSG i stanowi jeden z etapów negocjacji w rozumieniu art. 72 k.c., a tym samym nie mają zastosowania przepisy dotyczące oferty w rozumieniu art. 66 k.c.
2. Ofertę należy złożyć w terminie do dnia 21.08.2026 r., do godziny 12:00.
3. Określenie terminu ważności oferty (związania ofertą) – wymagany termin minimum 90 dni od upływu terminu wyznaczonego na składanie ofert.

II. PRZEDMIOT ZAPYTANIA OFERTOWEGO:

Przedmiotem Zapytania ofertowego jest określenie warunków współpracy w zakresie świadczenia na rzecz Zamawiającego usług serwisowania i konserwacji systemu zarządzania drukiem SafeCom oraz usługi wsparcia technicznego (maintenance) producenta oprogramowania SafeCom.

Zapytanie ofertowe podzielone jest na 2 części:

Część 1: Usługa serwisowania i konserwacji systemu zarządzania drukiem SafeCom.

Część 2: Zapewnienie wsparcia technicznego (maintenance) producenta oprogramowania SafeCom.

Oferent może złożyć ofertę zarówno na jedną jak i dwie części.

Szacowany termin realizacji: dla obydwu części od 01.01.2027 do 31.12.2028 r.

Szczegółowy zakres przedmiotu Zapytania ofertowego zawierają wzory umów, stanowiące **Załącznik nr 3.1. i 3.2.** do niniejszego Zapytania ofertowego.

III. SPOSÓB SKŁADANIA OFERT:

1. Oferty należy składać w formie elektronicznej za pośrednictwem Platformy Zakupowej Connect (dalej: Connect) znajdującej się na stronie: <https://connect.orklen.pl/>. Oferty przesłane inną drogą (np. pisemną lub za pośrednictwem poczty elektronicznej) nie będą uwzględniane podczas postępowania.
2. Oferta musi być złożona w terminie wymaganym w Connect, w języku polskim poprzez wypełnienie wszystkich pozycji formularza oraz załączenie wymaganych w Zapytaniu ofertowym informacji/dokumentów.
3. Oferta musi być kompletna i przygotowana z uwzględnieniem wszystkich informacji podanych w Zapytaniu ofertowym.
4. Oczekujemy wyczerpujących i konkretnych odpowiedzi na wszystkie podane w Zapytaniu zagadnienia. Odpowiedzi tych należy udzielić w formie zwięzłych opisów, a tam gdzie to jest wymagane - w formie załączników.

UWAGA: każdy z załączników powinien odnosić się do kryterium, do którego jest załączany. W szczególności niedopuszczalne jest umieszczenie jakiegokolwiek informacji cenowej lub handlowej w dokumentach dołączanych do kryteriów formalnych i merytorycznych; w przypadku wystąpienia takiej sytuacji PSG zastrzega sobie możliwość **odrzućenia oferty bez jej oceny**.

5. W trakcie trwania etapu składania ofert, Oferent ma prawo zgłaszać pytania dotyczące Zapytania ofertowego za pośrednictwem Connect – poprzez zakładkę „Zadaj pytanie zamawiającemu”.

Ważne, aby w treści zadawanych pytań nie było informacji pozwalających zidentyfikować Oferenta, który zadał pytanie. Na podstawie zadanych pytań, PSG przygotuje jednolitą informację zwrotną – taką samą dla wszystkich Oferentów.

Jednocześnie PSG zastrzega sobie prawo nieudzielenia odpowiedzi na zgłoszone pytania bez podania przyczyn.

6. **PSG przewiduje jednostopniowy proces składania ofert.**

Wszystkie dokumenty/ Ofertę należy składać w Connect w formie zeskanowanych dokumentów lub w formie dokumentów elektronicznych podpisanych kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, a tam gdzie jest to wymagane, również w formie edytowalnej.

- 1) **Dokumenty formalne** oferty wymienione w **Załączniku nr 1** należy dołączyć w Zakładce; Załączniki pn. „**OFERTA - dokumenty formalne**”.
- 2) **Dokumenty techniczne/merytoryczne** oferty wymienione w **Załączniku nr 1** należy dołączyć w zakładce: Załączniki pn. „**OFERTA - dokumenty techniczne/merytoryczne**”.
- 3) **Dokumenty handlowe** wymienione w **Załączniku nr 1** należy dołączyć w Zakładce; Załączniki pn. „**OFERTA HANDLOWA**” oraz jeżeli wymagane ustawieniami Connect wprowadzić wartość oferty.

Przedstawiona w ofercie cena musi zawierać wszystkie koszty Oferenta związane z realizacją przedmiotu zakupu.

Jeśli w ofercie złożonej przez danego Oferenta występują braki formalne lub techniczne/merytoryczne, PSG przekazuje Oferentowi informację o konieczności ich uzupełnienia w wyznaczonym terminie. W przypadku nieuzupełnienia przez Oferenta części formalnej oferty w wyznaczonym terminie, PSG odrzuca ofertę albo wyznacza dodatkowy termin na jej uzupełnienie.

7. **Wszystkie koszty związane z przygotowaniem i złożeniem oferty ponosi Oferent** i nie przysługuje mu prawo roszczenia o zwrot tych kosztów. Niezależnie od wyników postępowania, PSG nie będzie odpowiedzialna, ani dłużna w jakikolwiek sposób, w odniesieniu do kosztów lub strat poniesionych przez Oferenta w związku z przygotowaniem i złożeniem oferty.

IV. SPOSÓB OCENY OFERT:

1. Oceny złożonych ofert dokonuje powołany w tym celu Zespół zakupowy, na podstawie kryteriów i ich wag ustalonych przed publikacją niniejszego Zapytania. Zasady oceny poszczególnych ofert pozostają informacją poufną PSG, która nie jest udostępniana Oferentom.
2. Za najkorzystniejszą uznana będzie oferta w najwyższym stopniu spełniająca przyjęte kryteria pod względem formalnym, technicznym/merytorycznym i handlowym.
3. Proces oceny ofert jest przeprowadzany w kolejno następujących po sobie etapach:

- 1) weryfikacja i ocena informacji i dokumentów formalnych,
- 2) weryfikacja i ocena informacji i dokumentów technicznych/merytorycznych,
- 3) weryfikacja i ocena informacji i dokumentów handlowych.
4. PSG informuje Oferenta, który złożył najkorzystniejszą ofertę, o przyjęciu jego oferty, a po podpisaniu umowy z Dostawcą, pozostałych Oferentów o niewybraniu ich ofert.
5. PSG dopuszcza możliwość złożenia ofert przez konsorcja. Szczegóły zostały określone w **Załączniku nr 1**.

V. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY:

1. PSG będzie żądał wniesienia przez Oferenta przed zawarciem Umowy zabezpieczenia należytego wykonania umowy (dalej: „Zabezpieczenie”) w wysokości:
 - dla części 1: **7% wartości brutto umowy;**
 - dla części 2: **7% wartości brutto umowy.**
2. Zabezpieczenie może być wniesione w pieniądzu, gwarancjach bankowych, gwarancjach ubezpieczeniowych.
3. Zabezpieczenie wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy PSG **Bank PEKAO S.A.**, nr rachunku: 73 1240 6292 1111 0010 5525 6950 z dopiskiem **„Zabezpieczenie umowy – Serwisowanie i konserwacja systemu zarządzania drukiem SafeCom oraz usługa wsparcia technicznego producenta oprogramowania SafeCom nr cz. [...], nr sprawy [...]”** oraz NIP Oferenta.
4. Jeżeli Zabezpieczenie wniesiono w pieniądzu, PSG przechowuje je na oprocentowanym rachunku bankowym.
5. PSG zwraca Zabezpieczenie w terminie 21 dni od dnia wykonania umowy i uznania go przez PSG za należyte wykonanie.
6. W przypadku Zabezpieczenia wniesionego w pieniądzu PSG zwraca zabezpieczenie wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Oferenta.
7. W przypadku Zabezpieczenia wniesionego w formie gwarancji bankowej lub ubezpieczeniowej

sporządzonej w wersji papierowej PSG zwraca oryginał dokumentu, pozostawiając w dokumentacji jego kopię, a z czynności przekazania dokumentów sporządza stosowny protokół. Dokumenty wystawione elektronicznie nie są zwracane.

8. Zamawiający może, na wniosek Oferenta, wyrazić zgodę na zmianę formy wniesionego zabezpieczenia. Zmiana formy zabezpieczenia dokonywana jest w sposób zachowujący ciągłość zabezpieczenia i nie może powodować zmniejszenia jego wysokości, chyba że umowa pomiędzy PSG, a Oferentem przewiduje systematyczne zmniejszanie wysokości zabezpieczenia w miarę wykonywania umowy.
9. W przypadku wnoszenia zabezpieczenia w formie gwarancji, w treści gwarancji powinny się znaleźć postanowienia, z których będzie wynikać, iż przedmiotowa gwarancja jest nieodwołalna, bezwarunkowa i płatna na pierwsze żądanie.
10. Zabezpieczenie w formie gwarancji bankowej winno być wystawione przez podmiot posiadający zezwolenie wydane przez Komisję Nadzoru Finansowego na prowadzenie działalności bankowej oraz aktualną ocenę ratingową, nadanej przez agencję ratingową, na poziomie inwestycyjnym nie niższym niż Baa3 dla Agencji Moody's lub BBB- dla Agencji Standard and Poor's, lub BBB- dla Agencji Fitch. Zabezpieczenie należytego wykonania umowy w formie gwarancji ubezpieczeniowej winno być wystawione przez podmiot posiadający zezwolenie wydane przez Komisję Nadzoru Finansowego na prowadzenie działalności ubezpieczeniowej.

VI. DODATKOWE INFORMACJE:

1. PSG dopuszcza możliwość powierzenia wykonania umowy w części osobom trzecim.
2. PSG zastrzega sobie możliwość wykluczenia z postępowania Oferenta, który oferuje produkt lub usługę, pochodzące z Państwa trzeciego.
Państwo trzecie - inne niż państwo członkowskie Unii Europejskiej albo inne niż państwo będące stroną Porozumienia Światowej Organizacji Handlu (WTO) w sprawie zamówień rządowych, albo inne niż państwo będące stroną umowy międzynarodowej z UE, która gwarantuje wzajemny i równy dostęp do rynku zamówień publicznych.
3. Oferent odpowiada, jak za własne działania lub zaniechania, za działania i zaniechania podwykonawców, z których pomocą wykonuje Umowę, jak również za działania i zaniechania podwykonawców, którym powierza wykonanie Umowy.
4. Z Oferentem wyłonionym na bazie postępowania zakupowego planowane jest podpisanie umowy jednorazowej na czas określony (odrębnie dla części 1 jak i 2). Wzory umów stanowią **Załącznik nr 3.1. i 3.2.** do niniejszego Zapytania ofertowego.

5. Oferent zobowiązuje się do zachowania w tajemnicy wszelkich informacji wynikających z niniejszego Zapytania ofertowego, w tym informacji dotyczących faktu zaproszenia Oferenta do udziału w niniejszym postępowaniu ofertowym, faktu złożenia oferty, prowadzenia negocjacji handlowych oraz zawartych umów. Informacje te mogą być udzielane przez Oferenta jedynie po uzyskaniu pisemnej zgody PSG na przekazywanie ich osobom trzecim lub publikację.
6. PSG informuje, że przekazane dane osobowe będą przetwarzane zgodnie z informacją zawartą w „Obowiązku informacyjnym” dostępnym na stronie internetowej Polskiej Spółki Gazownictwa sp. z o.o. pod adresem www.psgaz.pl, w zakładce: *Dla kontrahenta/Obowiązek informacyjny*.
7. PSG zastrzega sobie prawo do:
- swobodnego wyboru Oferenta lub Oferentów według przyjętych kryteriów oceny;
 - możliwości ograniczenia zakresu przedmiotu postępowania oraz odstąpienia od procedury wyboru oferty i od negocjacji bez podania przyczyn. Z tego tytułu Oferentom nie przysługują żadne roszczenia wobec PSG;
 - dokonywania wyjaśnień i uściśleń zakresu przedmiotu postępowania w czasie oceny ofert;
 - przeprowadzenia negocjacji w różnych formach tj. elektronicznej, telekonferencji lub bezpośrednich spotkań;
 - przeprowadzenia aukcji elektronicznej za pośrednictwem Connect.
 - a. O ewentualnym przeprowadzeniu aukcji zostaną poinformowani przez Connect Oferenci, którzy spełnili wymagania określone w Zapytaniu ofertowym.
 - b. Szczegółowe instrukcje dotyczące aukcji elektronicznej zawarte będą w Parametryzacji aukcji oraz Regulaminie aukcji elektronicznej realizowanej na Platformie Connect, które każdy Oferent przed przystąpieniem do aukcji musi zaakceptować.
 - c. Parametrem jaki będzie licytowany w aukcji elektronicznej będzie całkowita cena netto za realizację Zamówienia.
 - d. PSG przewiduje możliwość przeprowadzenia testowej aukcji elektronicznej (szkoleniowej). Oferenci zainteresowani udziałem w testowej aukcji elektronicznej powinni skontaktować się bezpośrednio z Kupcem prowadzącym postępowanie (Osoba do kontaktu wskazana poniżej);
 - prowadzenia negocjacji ze wszystkimi Oferentami, którzy spełnili wymagania określone w Zapytaniu ofertowym;

- odrzucenia oferty niekompletnej lub gdy na etapie oceny ofert stwierdzi, po weryfikacji danych, iż podane przez Oferenta dane są nieprawdziwe i może się to przełożyć na wynik postępowania.

Osoby do kontaktu

Osobą odpowiedzialną za proces ze strony Obszaru Zakupów jest: Szczepan Rzepecki
e-mail: Szczepan.Rzepecki@psgaz.pl .

Załączniki

Integralną część przedmiotowego Zapytania ofertowego stanowią niżej wymienione załączniki:

1. **Załącznik nr 1** - Dokumenty i informacje wymagane do złożenia oferty
2. **Załącznik nr 2** - Oświadczenie oferenta – część formalna
3. **Załącznik nr 2.1** - Oświadczenie Beneficjent Rzeczywisty
4. **Załącznik nr 3.1.** - Wzór umowy wraz z Załącznikami dla części 1;
5. **Załącznik nr 3.2.** - Wzór umowy wraz z Załącznikami dla części 2;
6. **Załącznik nr 3.3.** - Wzór umowy o PPDO dla części 1;
7. **Załącznik nr 4** - Informacja o sposobie rozliczenia zamówienia na gruncie VAT przez Oferenta mającego siedzibę za granicą
8. **Załącznik nr 5** – Formularz RODO – część formalna
9. **Załącznik nr 6** - Formularz cenowy - część handlowa
10. **Załącznik nr 7** - Wykaz usług – część techniczna
11. **Załącznik nr 8** - Wykaz osób – część techniczna

ZAŁĄCZNIK Nr 1 - Dokumenty i informacje wymagane do złożenia oferty

Oferta ma zawierać nw. dokumenty i informacje:

I. Dokumenty formalne

1. Wyciąg z Krajowego Rejestru Sądowego (KRS)¹ lub zaświadczenie o wpisie do ewidencji działalności gospodarczej (CEIDG)² lub równoważnego dokumentu rejestrowego Oferenta.
2. Aktualne zaświadczenie z Urzędu Skarbowego o braku zaległości podatkowych³.
3. Aktualne zaświadczenie z ZUS o niezaleganiu z opłacaniem składek³.
4. Sprawozdanie o przychodach, kosztach i wyniku finansowym oraz o nakładach na środki trwałe (druk F-01/I-01) albo sprawozdania finansowe (Rachunek Zysków i Strat oraz Bilans) – w przypadku Spółek, za ostatnie 2 lata oraz za zamknięte kwartały w danym roku,
5. PIT – 28 albo PIT 36L – w przypadku jednoosobowej działalności gospodarczej, za ostatnie 2 lata,
6. Zaświadczenie z banku lub oddziału banku na terytorium Polski o prowadzeniu na rzecz Oferenta bankowego rachunku rozliczeniowego (w rozumieniu art. 49 ust.1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe), na który ma być dokonana zapłata wynagrodzenia.
7. Oryginał pełnomocnictwa osoby podpisującej ofertę albo kopię pełnomocnictwa poświadczoną za zgodność z oryginałem przez osobę upoważnioną, lub wskazanie, że umocowanie wynika bezpośrednio z treści KRS bądź innego rejestru.
8. Przedstawienie osób upoważnionych do prowadzenia negocjacji wraz z podaniem numerów telefonów kontaktowych i stosownych pełnomocnictw, chyba że umocowanie wynika bezpośrednio z treści KRS bądź innego rejestru oraz osoby do kontaktów (wraz z podaniem nr telefonu kontaktowego) upoważnionej do aktualizacji oferty i prowadzenia w imieniu Oferenta korespondencji na Connect.
9. Zaświadczenie właściwego naczelnika urzędu skarbowego o zarejestrowaniu Oferenta jako czynnego podatnika VAT bądź odpowiedni wydruk z Portalu Podatkowego prowadzonego przez Ministra Finansów, wystawione nie wcześniej niż 2 miesiące przed upływem terminu składania ofert. Jeżeli Oferent nie jest podatnikiem VAT czynnym lub zwolnionym, zamiast dokumentów, o których mowa w niniejszym punkcie składa dokument potwierdzający brak rejestracji.
10. Jeżeli Oferent ma siedzibę lub miejsce zamieszkania za granicą:
 - 10.1. nie składa dokumentu, o którym mowa w pkt. 9, składa natomiast pisemną informację w języku polskim, dotyczącą sposobu rozliczenia umowy na gruncie VAT, sporządzoną zgodnie ze wzorem zawartym w **Załączniku nr 4** do Zapytania ofertowego;
 - 10.2. zaświadczenie, o którym mowa w pkt. 9 może dotyczyć rachunku bankowego prowadzonego przez bank w kraju siedziby Oferenta, z zastrzeżeniem pkt. 10.3. poniżej.
 - 10.3. składa oryginał ważnego certyfikatu rezydencji podatkowej w przypadku świadczenia usług, o których mowa w art. 21 ust. 1 ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (Dz. U. z 2025 r. poz. 278 ze zm.) lub art. 29 ust. 1 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (tj. Dz. U. z 2025 r. poz. 163 ze zm.). Jeżeli miejsce siedziby lub zamieszkania Oferenta dla celów podatkowych zostało udokumentowane certyfikatem rezydencji niezawierającym okresu jego ważności, przyjmuje się, że certyfikat jest ważny przez okres kolejnych dwunastu miesięcy od dnia jego wydania. W przypadku, gdy Oferent ma siedzibę lub miejsce zamieszkania za granicą, ale będzie realizować usługi wymienione w dwóch ww. artykułach poprzez zakład położony w Polsce (w rozumieniu art. 4a pkt 11 ustawy o podatku dochodowym od osób prawnych oraz art. 5a pkt 22 ustawy o podatku dochodowym od osób fizycznych) składa dodatkowo pisemne oświadczenie, że wypłacane na podstawie umowy należności związane są z działalnością tego zakładu.
11. Podpisane i uzupełnione:
 - 11.1. oświadczenie Oferenta według wzoru stanowiącego **Załącznik nr 2** do zapytania ofertowego wraz z załącznikami oraz
 - 11.2. oświadczenie dotyczące Beneficjenta Rzeczywistego wg wzoru stanowiącego **Załącznik nr 2.1.** do zapytania – jeżeli dotyczy
 - 11.3. **Załącznik nr 5 – Formularz RODO.**

¹ Wypis z KRS - w przypadku spółek prawa handlowego, wystawione nie wcześniej, niż 6 miesięcy przed upływem terminu składania ofert,

² Zaświadczenie z CEIDG - w przypadku przedsiębiorców - osób fizycznych prowadzących indywidualną działalność gospodarczą oraz w przypadku wspólników spółek cywilnych, wystawione nie wcześniej, niż 6 miesięcy przed upływem terminu składania ofert,

³ Wystawione nie wcześniej, niż 3 miesiące przed upływem terminu składania ofert

12. **DLA CZĘŚCI 1:** opłacona polisę lub inny dokument ubezpieczenia potwierdzający, że Oferent jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej, na sumę gwarancyjną co najmniej 100 000,00 PLN (słownie: sto tysięcy złotych 00/100).
13. **DLA CZĘŚCI 2:** opłacona polisę lub inny dokument ubezpieczenia potwierdzający, że Oferent jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej, na sumę gwarancyjną co najmniej 400 000,00 PLN (słownie: czterysta tysięcy złotych 00/100).

II. Dokumenty techniczne³

Dla części nr 1:

1. Przedstawienie oświadczenia o posiadaniu umowy partnerskiej z Tungsten/SafeCom potwierdzone poprzez załączenie do oświadczenia np. korespondencji e-mailowej z producentem lub przedstawienie zaświadczenia o posiadaniu statusu partnerskiego podpisane przez producenta oferowanego rozwiązania poświadczające o kwalifikacjach
2. Przedstawienie wykazu usług (Załącznik nr 7) wraz z dokumentami potwierdzającymi, iż usługi przedstawione w wykazie zostały wykonane należycie (np. referencje, protokół odbioru, rekomendacje, poświadczenie wykonania) potwierdzające, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, należycie zrealizowali (a w przypadku świadczeń okresowych lub ciągłych również realizują) co najmniej jedną usługę, która polegała na wdrożeniu systemu SafeCom lub świadczeniu supportu technicznego tego rozwiązania z liczbą urządzeń w wydruku podążającym powyżej 100. Dokumentami, o których mowa powyżej, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów - oświadczenie Wykonawcy. W przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
3. Przedstawienie wykazu osób (Załącznik nr 8) wraz z kopiami posiadanych certyfikatów technicznych SafeCom poświadczających posiadane kwalifikacje potwierdzające dysponowanie przynajmniej 1 osobą posiadającą autoryzowane szkolenia producenta oprogramowania, potwierdzone zdobyciem certyfikatów technicznych SafeCom.
4. Przedstawienie listy potencjalnych podwykonawców z podaniem zakresu prac i udziałem procentowym jaki zostanie im powierzony w przypadku zawarcia umowy, wraz z referencjami spełniającymi warunki określone w pkt 2. (jeżeli dotyczy).

Dla części nr 2:

1. Brak.

III. Dokumenty handlowe

1. Podanie wynagrodzenia za prace objęte zakresem zapytania ofertowego w formie wypełnionego i podpisanego **Załącznik nr 8** do zapytania ofertowego
Kwoty przedstawione w ofercie handlowej powinny być wyrażone w kwocie netto.

Uwaga!

W przypadku oferty składanej przez Konsorcjum:

1. *Wymagane jest przedłożenie dokumentów opisanych w pkt. I Dokumenty formalne ppkt. 1-4, 8-10 przez wszystkich uczestników konsorcjum.*
2. *W przypadku konsorcjum wymagane zapytaniem ofertowym dokumenty składają wszyscy uczestnicy konsorcjum, z zastrzeżeniem, że wymagane oświadczenia i deklaracje mogą być złożone przez lidera konsorcjum w imieniu każdego z uczestników konsorcjum, z zastrzeżeniem pkt. 1 powyżej.*
3. *Wymagane jest złożenie umowy konsorcjum – w formie oryginału albo kopii poświadczonej za zgodność z oryginałem przez osobę upoważnioną (ze zdefiniowanymi obowiązkami konsorcjantów oraz informacją o procentowym zaangażowaniu poszczególnych uczestników konsorcjum w łącznej szacunkowej wartości oferty) oraz pełnomocnictwa dla lidera konsorcjum do reprezentowania pozostałych członków konsorcjum (dopuszcza się udzielenie pełnomocnictwa jednemu z uczestników konsorcjum w umowie konsorcjum).*
4. *Lider konsorcjum ponosi odpowiedzialność za realizację wszystkich formalnych wymagań wobec PSG.*

³ Kryteria/dokumenty techniczne mogą być określone w Connect jako kryteria/dokumenty merytoryczne

5. *Informacje dostarczone przez Oferentów występujących jako konsorcjum, potwierdzające posiadanie przez nich odpowiedniej i wymaganej wiedzy i doświadczenia, potencjału kadrowego i technicznego oraz sytuacji ekonomicznej i finansowej, podlegają sumowaniu i łącznej ocenie przez PSG. W przypadku wymogu posiadania odpowiednich uprawnień, dopuszcza się możliwość spełnienia ich tylko przez tych członków konsorcjum, którzy będą faktycznie realizować część zakresu umowy, do której wykonania wymagane jest posiadanie tych uprawnień.*
6. *W przypadku konsorcjum weryfikacji finansowej podlegają wszyscy uczestnicy konsorcjum.*

Prosimy o przygotowanie oferty zgodnie z ww. punktami.

ZAŁĄCZNIK Nr 2- Oświadczenie Oferenta – część formalna

OŚWIADCZENIE OFERENTA BIORĄCEGO UDZIAŁ W POSTĘPOWANIU ZAKUPOWYM

Działając w imieniu oraz na rzecz Oferenta _____,
(firma spółki, działalność gospodarcza prowadzona pod firmą)

Osoba/y do kontaktu, upoważniona/e do prowadzenia negocjacji, aktualizacji oferty i prowadzenia korespondencji na

Connect: _____ tel. _____, e-mail: _____

oświadczam/-y, że Oferent:

a) składa ofertę⁴:

1. samodzielnie

(firma spółki, działalność gospodarcza prowadzona pod firmą)

z siedzibą w _____

Numer REGON: _____

Numer NIP: _____

Rejestracja VAT-UE w innym kraju niż Polska:

☐ Tak, kraj rejestracji _____, numer VAT-UE _____,

☐ Nie

Numer VAT (VIES) – dotyczy podmiotów zagranicznych: _____

2. jako konsorcjum, w którego w skład wchodzi:

• Lider: _____,
(firma spółki, działalność gospodarcza prowadzona pod firmą)

Numer REGON: _____

Numer NIP: _____

Rejestracja VAT-UE w innym kraju niż Polska:

☐ Tak, kraj rejestracji _____, numer VAT-UE _____,

☐ Nie

Numer VAT (VIES) – dotyczy podmiotów zagranicznych: _____

• Członkowie: _____,
(firma spółki, działalność gospodarcza prowadzona pod firmą)

Numer REGON: _____

⁴ Niepotrzebne skreślić 1 albo 2

Numer NIP: _____

Rejestracja VAT-UE w innym kraju niż Polska:

☐ Tak, kraj rejestracji _____, numer VAT-UE _____,

☐ Nie

Numer VAT (VIES) – dotyczy podmiotów zagranicznych: _____

- b) spełnia warunki udziału w Postępowaniu oraz braku podstaw do odrzucenia oferty,
- c) spełnia wymagania dotyczące bezpieczeństwa informacji i przetwarzania danych osobowych,
- d) przyjmuje do wiadomości, że w przypadku podania przeze mnie nieprawdziwych informacji poniosę odpowiedzialność prawną i pokryję wszelkie szkody i koszty poniesione przez PSG z tego tytułu,
- e) numer bankowego rachunku rozliczeniowego, wskazanego w Umowie lub na fakturze, na który ma zostać dokonana płatność jest zgodny z numerem rachunku bankowego, otwartym w związku z prowadzoną działalnością gospodarczą, który został zgłoszony w Urzędzie Skarbowym oraz widnieje w elektronicznym Wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT prowadzonym na stronie Ministerstwa Finansów,
- f) nie wszczęto wobec mnie postępowania restrukturyzacyjnego, likwidacyjnego lub upadłościowego, ani nie toczy się w stosunku do mnie postępowanie egzekucyjne,
- g) jest w sporze sądowym ze Spółką lub ze Spółką z GK ORLEN
 - ☐ Tak,
 - ☐ Nie,
- h) był w sporze sądowym ze Spółką lub ze Spółką z GK ORLEN
 - ☐ Tak,
 - ☐ Nie,
- i) zobowiązuje się do przestrzegania tajemnicy informacji i nie rozpowszechniania informacji i materiałów uzyskanych w trakcie postępowania zakupowego w zakresie prac objętych zapytaniem ofertowym (tajemnicą informacji objęte są nieujawnione do wiadomości publicznej informacje, co do rozwiązań technicznych, technologicznych, informacje handlowe lub organizacyjne z zakresu działalności PSG),
- j) jest związany niniejszą ofertą dni **[uzupełnia Oferent – nie może być mniej niż wskazane w pkt. I.3. Zapytania ofertowego]** od upływu terminu składania ofert,
- k) wdrożył odpowiednie środki techniczne i organizacyjne, zapewniające zgodność przetwarzania danych osobowych z przepisami RODO i ochronę praw osób, których dane dotyczą,
- l) zapozna się i zastosuje Wymagania dla Oferentów zewnętrznych, w szczególności: Ogólne Warunki Umów, Ogólne Wytyczne Dotyczące Ubezpieczeń oraz Wymagania w zakresie BHP, Ppoż i Ochrony środowiska, wraz z załącznikami, dostępne na stronie www.psgaz.pl w zakładce *Dla Kontrahenta/ Pliki do pobrania*.
- m) posiada status dużego przedsiębiorcy w rozumieniu art. 4 pkt 6) Ustawy z dnia 8 marca 2013 roku o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych.
 - ☐ Tak,
 - ☐ Nie,
- n) ma prawo do wystawiania dokumentu: „Informacja o kwocie obniżenia wpłat na Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych” (dokumentu INFu)
 - ☐ Tak,
 - ☐ Nie,
- o) Oferent, jak i jego podmioty zależne, dominujące oraz członkowie jego organów są zgodne z przepisami sankcyjnymi wprowadzonymi przez Organizację Narodów Zjednoczonych, Unię Europejską, państwa członkowskie Unii Europejskiej i Europejskiego Obszaru Gospodarczego, Stany Zjednoczone Ameryki Północnej, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej („Przepisy sankcyjne”) oraz nie są objęte jakimikolwiek sankcjami nałożonymi na podstawie przepisów sankcyjnych.
- p) zastrzega tajemnicę przedsiębiorstwa:
 - ☐ Tak
 - ☐ Nie

Informacje zawarte w dołączonych plikach, oznaczonych nazwą „Tajemnica przedsiębiorstwa”, stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji i jako takie nie mogą być ogólnie udostępnione. W celu wykazania, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa dołączam oświadczenie wraz z uzasadnieniem.

- q) oferuje produkt lub usługę pochodzącą z Państwa trzeciego

☐ Tak, z *[oferent wskazuje kraj/kraje]*

☐ Nie.

- r) akceptuje minimum 30-dniowy termin płatności faktury/faktur.
- s) zobowiązuje się do wniesienia zabezpieczenia należytego wykonania Umowy w wysokości i formie określonej w Zapytaniu Ofertowym
- t) zobowiązuje się do realizacji Usług objętych Umową w terminach określonych w Umowie

.....
data

.....
podpis Oferenta
(osoby upoważnione do składania oświadczeń woli)

Załącznik nr 2.1 Oświadczenie Beneficjent Rzeczywisty

OŚWIADCZENIE Beneficjent Rzeczywisty

Czy papiery wartościowe spółki są dopuszczone do obrotu na rynku regulowanym podlegającym wymogom ujawnienia informacji wynikających z przepisów prawa Unii Europejskiej lub odpowiadającym im przepisom prawa państwa trzeciego:

- ☐ Tak
- ☐ Nie*
- ☐ Nie dotyczy**

*Jeżeli zaznaczono „☐ Nie” wypełnij poniższy formularz

***☐ Nie dotyczy” zaznacza Oferent, który nie jest zobowiązany do wypełnienia niniejszego oświadczenia

Nazwa Oferenta	adres	NIP/Nr VAT	KRS/ CEIDG	dane kontaktowe (telefon, mail)	ID DUNS (opcjonalnie)

Oświadczenie o Beneficjencie rzeczywistym

Niniejszym oświadczam, że posiadam Beneficjenta rzeczywistego w rozumieniu Dyrektywy Parlamentu Europejskiego i Rady UE w tym VI Dyrektywy UE o przeciwdziałaniu praniu pieniędzy (6AMLD) i wcześniejszych, oraz w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U z 2025 poz. 644).

Poniżej wskazuję dane Beneficjenta rzeczywistego:

Imię i nazwisko: _____

Obywatelstwo: _____

Data urodzenia: _____

Dane REPREZENTANTA/OSOBY UPOWAŻNIONEJ

I.p.	Imię i nazwisko	Pesel	Obywatelstwo	Data i państwo urodzenia (w przypadku osób nieposiadających pesel)
1.				
2.				
3.				

(Podpis/Podpisy)

Wyjaśnienie dot. wypełnienia oświadczenia

Oświadczenie wypełniają: spółki jawne, spółki komandytowe, spółki komandytowo-akcyjne, spółki z ograniczoną odpowiedzialnością, proste spółki akcyjne, spółki akcyjne (z wyjątkiem spółek publicznych w rozumieniu ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych), trusty, których powiernicy lub osoby zajmujące stanowiska równoważne mają miejsce zamieszkania lub siedzibę na terytorium RP lub nawiązują stosunki gospodarcze lub nabywają nieruchomości na terytorium RP w imieniu lub na rzecz trustu, spółki partnerskie, europejskie zgrupowania interesów gospodarczych, spółki europejskie, spółdzielnie, spółdzielnie europejskie, stowarzyszenia podlegające wpisowi do KRS, fundacje.

Wyjaśnienie, jak wypełnić oświadczenie:

Beneficjentem rzeczywistym może być wyłącznie osoba fizyczna lub osoby fizyczne. Oferent weryfikuje powiązania korporacyjne albo właścicielskie w ramach prowadzonej działalności gospodarczej, celem ustalenia, czy dana osoba fizyczna, lub osoby fizyczne sprawują nad nim kontrolę.

Żeby ustalić, kto jest beneficjentem rzeczywistym, w pierwszej kolejności Oferent sprawdza, czy w organizacji jest osoba lub osoby sprawujące bezpośrednio lub pośrednio nad nim kontrolę, poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania przez niego podejmowane.

Jeżeli Oferent jest spółką z ograniczoną odpowiedzialnością lub niepubliczną spółką akcyjną to jego beneficjentem rzeczywistym może być:

- a. osoba fizyczna będąca twoim udziałowcem lub akcjonariuszem, której przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji,
- b. osoba fizyczna dysponująca więcej niż 25% ogólnej liczby głosów w organie stanowiącym, także jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu,
- c. osoba fizyczna sprawująca kontrolę nad osobą prawną lub osobami prawnymi, którym łącznie przysługuje prawo własności więcej niż 25% ogólnej liczby twoich udziałów lub akcji, lub łącznie dysponującą więcej niż 25% ogólnej liczby głosów w organie spółki Oferenta, także jako zastawnik albo użytkownik, lub na podstawie porozumień z innymi uprawnionymi do głosu
- d. osoba fizyczna sprawująca kontrolę jako jednostka dominująca,

Oferent analizując, kto jest jego beneficjentem rzeczywistym, rozważa która z powyższych sytuacji jego dotyczy, a jeżeli dotyczy go więcej niż jedna sytuacja, to który z podmiotów ma silniejsze uprawnienia.

Jeśli Oferent uważa, że żadna z sytuacji wskazanych w punktach (a-d) go nie dotyczy, to jego beneficjentem rzeczywistym jest osoba fizyczna zajmująca wyższe stanowisko kierownicze.

Załącznik nr 3.1. i 3.2. Wzory umów cz. 1 i 2

W odrębnych załącznikach

Załącznik nr 3.3

Wzór umowy o powierzeniu przetwarzania danych osobowych dla części 1

(w odrębnym pliku)

Załącznik nr 4

Informacja o sposobie rozliczenia zamówienia na gruncie VAT przez Oferenta mającego siedzibę za granicą

W imieniu z siedzibą w (dalej: Oferent zagraniczny), w związku z Zapytaniem ofertowym na Serwisowanie i konserwacja systemu zarządzania drukiem SafeCom oraz usługą wsparcia technicznego (maintenance) producenta oprogramowania SafeCom informuję, że transakcja zostanie zrealizowana:

- 1) przez Oferenta zagranicznego, działającego bezpośrednio w zakresie realizacji Umowy,
- 2) przez Oddział Oferenta zagranicznego o nazwie
.....
z siedzibą w
zarejestrowany w KRS pod numerem *

Jednocześnie informuję, że transakcja zostanie zrealizowana w formie (zaznaczyć właściwy kwadrat):

- ☐ wewnątrzwspólnotowej dostawy towarów,
- ☐ dostawy z terytorium kraju,
- ☐ dostawy łańcuchowej z terytorium UE,
- ☐ dostawy łańcuchowej z terytorium kraju trzeciego,
- ☐ importu,
- ☐ dostawy z montażem,
- ☐ innej ** (proszę wskazać jakiej).

(miejsce i data)

Imię, nazwisko i podpis osoby
umocowanej do reprezentacji

*niepotrzebne skreślić

**zaznaczyć także w przypadku, gdy Oferent nie jest podatnikiem VAT

Załącznik nr 5 Formularz oceny Oferenta dot. RODO – cz. 1

– część formalna

W nawiązaniu do uruchomionego zapytania ofertowego na świadczenie usług, których realizacja będzie wymagała przetwarzania danych osobowych, powierzonych przez PSG, prosimy Oferenta /podmiot przetwarzający (dalej: Państwa) o uzupełnienie poniższego formularza:

	FORMULARZ OCENY KONTRAHENTA – PYTANIA	tak/nie	komentarz
1	Czy wdrożyli Państwo polityki ochrony danych osobowych zgodnie z art. 24 RODO?		
2	Czy wdrożyli Państwo instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?		
3	Czy w Państwa organizacji jest osoba wyznaczona do kontaktu i obsługi zgłoszeń o naruszeniu ochrony danych?		
4	Czy wdrożyli Państwo politykę/procedurę obsługi żądań podmiotów danych?		
5	Czy w Państwa organizacji jest osoba wyznaczona do kontaktu i realizacji procedury rozpatrywania żądań podmiotów danych?		
6	Czy po Państwa stronie osoby wyznaczone do realizacji zlecenia/umowy zostały przeszkolone i zapoznane z przepisami o ochronie danych osobowych, zasad bezpieczeństwa informacji oraz w zakresie bezpiecznego korzystania z systemu informatycznego?		
7	Czy po Państwa stronie osoby wyznaczone do realizacji zlecenia/umowy posiadają stosowne upoważnienie do przetwarzania danych osobowych, obejmujące dane powierzone do Państwa?		
8	Czy osoby upoważnione przez Państwa do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy?		
9	Czy wyznaczili Państwo inspektora ochrony danych lub też inną osobę lub zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji?		
10	Jak można się skontaktować z osobami, o których mowa w pyt.9? Prośba o wpisanie w polu komentarz dni/godzin pracy, formy kontaktu.	X	
11	Czy w ciągu ostatnich 5 lat stwierdzono prawomocną decyzją PUODO lub innego organu nadzorczego, lub prawomocnym wyrokiem sądu naruszenie przepisów o ochronie danych osobowych w Państwa organizacji?		
12	Czy w chwili obecnej w Państwa organizacji toczą się postępowania wyjaśniające, kontrole lub inne działania prowadzone przez PUODO lub inny organ nadzorczy w związku z realizowanymi przez Państwa usługami?		
13	Czy w ciągu ostatnich 6 miesięcy doszło u Państwa do naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia organowi nadzorczemu?		
14	Czy wdrożyli Państwo odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, zgodnie z art. 32 ust.1 lit a-c RODO oraz czy spełniają Państwo wszystkie „Minimalne wymagania formalne i techniczne w zakresie bezpieczeństwa danych osobowych” stanowiące załącznik 1 do niniejszego formularza oceny kontrahenta?		
15	Czy prowadzą Państwo regularnie audyty dotyczące zasad bezpieczeństwa danych osobowych, w celu weryfikacji spełniania wymogów RODO, w tym testowania, mierzenia		

	i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, zgodnie z art. 32 ust. 1 lit d RODO?		
16	Czy mają Państwo wdrożone normy ISO lub kodeksy branżowe (o ile występują), mające wpływ na bezpieczeństwo informacji? W przypadku odpowiedzi TAK, prosimy o wskazanie tych norm/kodeksów w polu komentarz.		
17	Czy dysponują Państwo <u>zasobami własnymi</u> do samodzielnej realizacji umowy ze zlecającym/administratorem?		
18*	W przypadku odpowiedzi NIE na pyt.17 (tj. w sytuacji, gdy zakładają Państwo potrzebę dalszego podpowierzenia danych osobowych) - prosimy o wskazanie w polu komentarz zakresu, w jakim dane osobowe miałyby być podpowierane przez Państwa do dalszego podmiotu przetwarzającego.		
19*	W przypadku odpowiedzi NIE na pyt.17 (tj. w sytuacji, gdy zakładają Państwo potrzebę dalszego podpowierzenia danych osobowych) - czy będą Państwo dokonywać transferów poza EOG danych powierzonych w związku z realizacją usługi?		
20*	W przypadku odpowiedzi TAK na pyt. 19 (tj. w sytuacji, gdy zakładają Państwo potrzebę dalszego podpowierzenia danych osobowych do krajów spoza EOG) – prosba o podanie w polu komentarz nazw tych krajów wraz z informacją, w jaki sposób zapewniają Państwo mechanizm legalizujący taki transfer?		
*	[ew. dodatkowe pytania właściciela procesu po stronie zlecającego/administradora – istotne w kontekście konkretnego zlecenia]		

!	Oświadczam, że organizacja, w imieniu której wypełniam niniejszy formularz, posiada niezbędne zasoby (ludzie, wiedza organizacji, infrastruktura, inne) gwarantujące rzetelną realizację usługi na rzecz PSG, w tym przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami o ochronie danych osobowych (RODO, ustawa o ochronie danych osobowych).		
!	Oświadczam, że w przypadku, gdy przed zakończeniem postępowania ofertowego wystąpią istotne zmiany w organizacji, której dotyczy niniejszy formularz, mogące wpłynąć na udzielane gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, o których mowa w RODO i niniejszym formularzu, zobowiązuje się do niezwłocznego (nie później niż przed podpisaniem Umowy) poinformowania o tych zmianach zlecającego/administradora.		

	Dane osoby wypełniającej formularz	imię i nazwisko:	
		stanowisko:	
		służbowy numer telefonu:	
		służbowy adres email:	

Data wypełnienia formularza oraz podpis osoby reprezentującej Oferenta/podmiot przetwarzający:

Załącznik do FORMULARZA OCENY OFERENTA (RODO)

I. MINIMALNE WYMAGANIA FORMALNE I TECHNICZNE W ZAKRESIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

A. Wymagania formalne:

1. Przetwarzający zobowiązuje się do wykonania przedmiotu Umowy przestrzegając zasad bezpieczeństwa teleinformatycznego.
2. Przetwarzający zobowiązany jest posiadać politykę bezpieczeństwa teleinformatycznego, która ma w szczególności wyraźne zastosowanie do usług świadczonych w ramach realizacji przedmiotu Umowy.
3. Przetwarzający zobowiązany jest zapewnić, że zarządzanie infrastrukturą teleinformatyczną oraz aplikacjami wykorzystywanymi do realizacji przedmiotu Umowy jest prowadzone zgodnie z dobrymi, uznanymi praktykami bezpieczeństwa teleinformatycznego.
4. Przetwarzający zobowiązuje się do niezwłocznego powiadamiania Administratora o zaistniałych naruszeniach lub incydentach bezpieczeństwa teleinformatycznego mających bezpośredni wpływ na powierzone dane osobowe.
5. W przypadku, gdy wykonanie Umowy wiąże się z ryzykiem utraty atrybutów bezpieczeństwa danych (poufności, integralności i dostępności danych), Przetwarzający zobowiązany jest poinformować o tym Administratora przed przystąpieniem do wykonywania jakichkolwiek prac oraz umożliwić Administratorowi przeprowadzenie działań zapewniających zachowanie ww. atrybutów.
6. Przetwarzający odpowiada za skutki działań pracowników oraz osób trzecich, którym powierzył wykonanie czynności na rzecz Administratora tak, jak za czynności własne.

B. Wymagania dla systemów teleinformatycznych Przetwarzającego:

1. Przetwarzający zobowiązuje się do zapewnienia kontroli dostępu w systemach teleinformatycznych.
2. Logowanie do systemów teleinformatycznych możliwe jest wyłącznie w oparciu o indywidualny login użytkownika i hasło lub inne środki zapewniające atrybut rozliczalności.
3. Przetwarzający zobowiązany jest posiadać działające mechanizmy anonimizacji, pseudonimizacji oraz usuwania danych na wniosek właściciela danych.
4. Przetwarzający zobowiązany jest posiadać zabezpieczenia systemów teleinformatycznych przed złośliwym oprogramowaniem, w tym przed kradzieżą lub zniszczeniem danych.
5. Przetwarzający zobowiązuje się do stosowania mechanizmów szyfrowania, w tym m.in.: komputery, pendrive, smartphone oraz przy przesyłaniu danych.
6. Przetwarzający zobowiązany jest do zapewnienia zabezpieczenie dostępu zdalnego do systemów teleinformatycznych poprzez stosowanie bezpiecznych i szyfrowanych połączeń VPN.
7. Przetwarzający zobowiązany jest do zarządzania podatnościami w systemach teleinformatycznych, w tym m.in.: testowanie cyberbezpieczeństwa infrastruktury i aplikacji, procedury zarządzania aktualizacjami.
8. Przetwarzający zobowiązany jest do zarządzania ciągłością działania, w tym m.in.:
 - 1) tworzenia kopii zapasowych oraz testy przywracania z kopii zapasowych.
 - 2) mechanizmy zapewniające wysoką dostępność systemów.
9. Przetwarzający zobowiązany jest posiadać systemy monitorowania infrastruktury oraz sieci teleinformatycznych pod kątem cyberbezpieczeństwa.
10. O ile wynika to z zakresu Umowy, Przetwarzający zobowiązany jest zapewnić w systemie teleinformatycznym poniższe funkcjonalności:
 - 1) dla każdej osoby, której dane osobowe są przetwarzane w systemie teleinformatycznym, system zapewnia wyeksportowanie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, wszystkie zgromadzone dane osoby, której dane dotyczą; System umożliwia odnotowanie informacji o zgodzie na przetwarzanie danych osobowych, osoby, której dane dotyczą;
 - 2) dla każdej osoby, której dane osobowe są przetwarzane, system teleinformatyczny zapewnia odnotowanie:

- a) daty pierwszego wprowadzenia danych do systemu,
- b) identyfikatora użytkownika wprowadzającego dane,
- c) rejestracje wszelkich zmian wykonanych na danych.

Odnoszenie informacji, o których mowa powyżej, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych do systemu.

- 3) w przypadku udostępnienia danych osobowych, system zapewnia:
 - a) odnotowanie informacji o odbiorcach,
 - b) dacie udostępnienia,
 - c) zakresie udostępnionych danych.

C. WYMAGANIA BEZPIECZEŃSTWA W PRZYPADKU POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH POZA INFRASTRUKTURĄ PSG W MODELU CHMURY OBLICZENIOWEJ LUB HOSTINGU

1. Wykonawca zobowiązany jest wdrożyć określone w niniejszym rozdziale skuteczne i adekwatne organizacyjno – techniczno - prawne mechanizmy gwarantujące bezpieczeństwo przetwarzania Danych oraz poufność, integralność, dostępność i rozliczalność powierzonych Danych.
2. Obowiązek, o którym mowa w pkt 1 powyżej, Wykonawca realizuje poprzez wdrożenie zabezpieczeń chroniących Dane przed ich przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, zmianą, nieupoważnionym ujawnieniem lub dostępem, w szczególności poprzez:
 - 1) szyfrowanie Danych, które stosuje się zarówno wobec „informacji w tranzycie”, jak i informacji przechowywanych na serwerach, w kopiach zapasowych oraz wobec mechanizmów autoryzacji,
 - 2) bezpieczne składowanie kluczy szyfrujących, w tym w szczególności poprzez składowanie ich w odseparowaniu od serwera/serwerów, w których zlokalizowane będą Dane podlegające szyfrowaniu oraz wdrożenie procedury zarządzania dostępem do tych Danych gwarantującej ich bezpieczeństwo oraz dostęp wyłącznie upoważnionym przedstawicielom PSG,
 - 3) wirtualne środowiska dedykowane wyłącznie na potrzeby PSG dostępne wyłącznie przez kanał VPN i tylko z klasy adresowej IP PSG z wdrożonymi mechanizmami separującymi (co najmniej na poziomie logicznym) Dane od danych osobowych osób trzecich (innych odbiorców usług Wykonawcy) lub inne, zaakceptowane przez PSG rozwiązania zapewniające separację Danych od danych osobowych osób trzecich,
 - 4) opracowanie i wdrożenie procedury dostępu do Danych zapewniającej:
 - a) dostęp do Danych wyłącznie dla osób upoważnionych przez PSG (**Użytkowników Usługi**),
 - b) silne dwuskładnikowe uwierzytelnianie,
 - c) bezpieczne przechowywanie danych uwierzytelniających Użytkowników Usługi,
 - d) rozliczalność, rozumianą jako możliwość jednoznacznego przypisania działań do konkretnego Użytkownika Usługi,
 - 5) usunięcie przez Wykonawcę z nośników wycofywanych z eksploatacji wszystkich powierzonych Danych z tym zastrzeżeniem, że usunięcie Danych musi być dokonane w sposób bezpowrotny (czyli w taki sposób, żeby ich ponowne odtworzenie ani w całości, ani w części nie było możliwe), a w przypadku, gdy bezpowrotne usunięcie Danych z ww. nośników metodą programową nie jest możliwe, nośniki, na których przetwarzane są Dane muszą zostać fizycznie zniszczone; Wykonawca jest zobowiązany dostarczyć protokół z czynności wymienionych w niniejszym punkcie opisujący szczegółowo co zostało wykonane, przez kogo, z zastosowaniem jakich narzędzi i algorytmów oraz jakich/których Danych te czynności dotyczyły.
3. Wykonawca zobowiązany jest do opracowania i wdrożenia procedur identyfikacji i zarządzania podatnościami bezpieczeństwa, w tym dokonywania regularnych aktualizacji oprogramowania komponentów infrastruktury i oprogramowania znajdujących się pod kontrolą Wykonawcy.
4. Wykonawca zobowiązany jest do stosowania skutecznych środków zapewniających ciągłość świadczenia Usługi, w tym do:
 - 1) stosowania adekwatnych systemów, zasobów i procedur pozwalających na zachowanie ciągłości i regularności działania Usługi, w tym tworzenie aktualnych kopii zapasowych umożliwiających w sytuacji awaryjnej lub w przypadku katastrofy odtworzenie informacji

- wraz z oprogramowaniem oraz przygotowanie i wdrożenie procedur zapewniających ich regularne testowanie oraz odtwarzanie,
- 2) opracowania i testowania procedur awaryjnych i okresowego testowania infrastruktury rezerwowej. Wykonawca jest zobowiązany przedstawiać PSG niezwłocznie do wglądu raporty z przedmiotowych testów,
 - 3) zabezpieczenia przed utratą połączenia sieciowego, awarią zasilania, przerwą w dostawie prądu, uszkodzeniem sprzętu,
 - 4) zabezpieczenia przed atakiem typu DDoS (*distributed denial of service*).
5. Wszystkie komponenty Usługi muszą być wolne od znanych podatności.
 6. Usługa nie może posiadać znanych podatności technicznych, będzie na bieżąco aktualizowana (min. raz w miesiącu) o poprawki udostępniane przez producenta danego rozwiązania.
 7. Usługa podlegać będzie cyklicznemu procesowi utwardzania konfiguracji np. zgodnie z ogólnodostępnymi dla danego rozwiązania zaleceniami (np. CIS Benchmark).
 8. Wszystkie komponenty Usługi, w tym system operacyjny, serwery baz danych i aplikacyjne będą stosowane w aktualnej, oficjalnie wspieranej przez ich producenta wersji.
 9. Wszystkie komputery i serwer, na którym będą przetwarzane Dane będą wyposażone w komercyjny program antywirusowy z automatycznie aktualizowaną na bieżąco bazą sygnatur.
 10. Wszystkie stosowanie w Usłudze połączenia sieciowe będą szyfrowane za pomocą protokołów, algorytmów i ich konfiguracji powszechnie uznawanych za bezpieczne (np. TLS 1.3).
 11. Każdy z Użytkowników Usługi będzie posiadał indywidualne konto, pozwalające na jednoznaczną identyfikację osoby fizycznej, która uzyskała dostęp do Danych.
 12. Każdy z Użytkowników Usługi będzie korzystał z mocnych haseł lub z metod mocnego uwierzytelnienia.
 13. Hasło Użytkownika Usługi musi składać się z minimum 12 znaków. Hasło musi zawierać:
 - 1) małe litery łacińskie,
 - 2) duże litery łacińskie,
 - 3) cyfry,
 - 4) znaki specjalne.
 14. W przypadku jeżeli Usługa dostępna jest w sieci publicznej, każdy z Użytkowników Usługi (w tym też administratorzy komponentów systemowych) będą mogli uzyskać dostęp tylko po mocnej autoryzacji (wymagane jest MFA – multifactor authentication).
 15. W przypadku dostępu do Usługi poprzez sieć Internet (zdalnie) wymagane jest stosowanie mocnej autoryzacji (np. dla połączenia VPN) tj. wymagane jest MFA – multifactor authentication.
 16. Usługa musi posiadać możliwość konfigurowalnego raportowania i automatycznego monitorowania i logowania aktywności Użytkowników Usługi.
 17. W Usłudze zostały zaprojektowane role wraz ze wskazaniem ich zakresu zadań i odpowiedzialności.
 18. W Usłudze uwzględniono zasadę przyznawania Użytkownikom Usługi minimalnych uprawnień, niezbędnych do wykonywania obowiązków służbowych.
 19. Sposobem transmisji danych do przeglądarki WWW jest szyfrowanie przepływu danych, w szczególności należy wykorzystać szyfrowanie danych protokołem TLS (w jego bezpiecznej wersji np. TLS 1.3) podczas komunikacji przy pomocy przeglądarki. Usługa jest wyposażona w certyfikaty SSL (w jego bezpiecznej wersji) dla serwerów WWW, a transmisja danych powinna odbywać się z wykorzystaniem do tego celu protokołu HTTPS.
 20. Ruch sieciowy pomiędzy wszystkimi elementami Usługi musi być szyfrowany za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Wymagane jest stosowanie protokołów TLSv1.2, TLS1.3 lub ich nowszych wersji, preferowane jest stosowanie protokołu TLSv1.3. Nie jest dopuszczalne stosowanie protokołu IPSec oraz protokołów SSL 2.0, SSL 3.0, TLS 1.0 i TLS 1.1 i starszych.
 21. Wymagane jest stosowanie protokołów, algorytmów oraz ich konfiguracji powszechnie uznanych za bezpieczne.
 22. Wymagane jest stosowanie zaufanych certyfikatów X.509 dostarczonych przez komercyjne, globalnie zaufane CA. Dopuszczalne jest też stosowanie certyfikatów dostarczonych przez PSG. Wymagana, minimalna długość klucza dla ECC to 384 bitów, dla RSA to 2048 bitów. Usługa jest objęta archiwizacją danych.

23. Usługa umożliwia przechowywanie i zarządzanie zdarzeniami (logi) oraz ich eksport w formie zrozumiałej dla PSG.
24. Mechanizmy śledzenia zdarzeń i rozliczalności oraz informacje w dziennikach zdarzeń (logi) są chronione przed manipulacją i nieuprawnionym dostępem.
25. Do dzienników zdarzeń lub ich archiwów, mogą mieć dostęp wyłącznie osoby uprawnione. Usługa musi zapewniać integralność dzienników zdarzeń.
26. Pola zawierające dane uwierzytelniające nie są uzupełniane przez Usługę.
27. Wszystkie operacje dotyczące uwierzytelniania (takie jak rejestracja, aktualizacja profilu, przypomnienie loginu, przypomnienie hasła), które powodują odzyskanie dostępu do konta, posiadają przynajmniej takie same zabezpieczenia jak podstawowe mechanizmy uwierzytelniania.
28. Funkcja zmiany hasła zawiera konieczność podania hasła obecnie używanego, nowego hasła oraz konieczność ponownego wpisania nowego hasła.
29. Mechanizmy odzyskiwania hasła nie ujawniają dotychczasowych haseł i nowe hasło nie jest przesyłane w formie jawnej do Użytkownika Usługi.
30. Nie jest możliwa enumeracja wykorzystująca loginy Użytkowników Usługi, funkcję resetowania hasła lub funkcjonalność przypomnienia nazwy Użytkownika Usługi.
31. Platforma lub inne komponenty, z których korzysta Usługa nie używają domyślnych haseł (np. admin/password).
32. Wdrożono mechanizmy przeciwdziałające automatyzacji, aby zapobiegać testowaniu ujawnionych danych uwierzytelniających, atakom brute force i atakom blokującym konta.
33. Wdrożono mechanizmy blokujące użycie znanych lub słabych haseł.
34. Interfejs administracyjny nie jest dostępny dla stron niezaufanych.
35. Sesje są unieważniane po wylogowaniu się Użytkownika Usługi.
36. Usługa nie jest podatna na atak LDAP Injection lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takiego ataku.
37. Środowisko uruchomieniowe nie jest podatne na atak wstrzyknięcia komend systemu operacyjnego lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takiego ataku.
38. Usługa nie jest podatna na ataki zdalnego lub lokalnego dołączenia plików (Remote File Inclusion - RFI lub Local File Inclusion - LFI) gdy wykorzystywana jest treść będąca ścieżką do plików.
39. Usługa nie jest podatna na ataki XML Injection, XML External Entity, XPath query lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takich ataków.
40. Usługa jest zabezpieczona przed atakami typu HTTP Parameter Pollution.
41. Dane zapisywane po uwierzytelnieniu w pamięci przeglądarki np. w DOM są czyszczone po zakończeniu sesji.
42. Identyfikatory sesji nigdy nie są ujawniane w URL, w komunikatach błędów lub logach.
43. Każde pomyślne uwierzytelnienie, a także ponowne uwierzytelnienie, tworzy nową sesję z nowym identyfikatorem.
44. Identyfikatory sesji przechowywane w ciasteczkach mają ustawioną ścieżkę z wartością odpowiednio restrykcyjną dla danej aplikacji i tokeny sesji uwierzytelniania mają dodatkowo ustawione atrybuty "HttpOnly" i "secure".
45. Została wdrożona zasada minimalnych uprawnień – Użytkownicy Usługi powinni mieć dostęp tylko do funkcji, plików, linków URL, usług oraz innych zasobów, do których posiadają zezwolenie.
46. Usługa nie zwraca komunikatów o błędach lub śladów stosu (stack traces), które zawierają dane które mogą pomóc atakującym. Zawierają się w tym identyfikatory sesji, wersje oprogramowania / platformy.
47. Dla wszystkich połączeń (zewnętrznych i wewnętrznych), które są uwierzytelniane lub związane z danymi wymienionymi w ust. 46 lub funkcjami, jest wykorzystywany TLS a także nie jest możliwe pogorszenie parametrów połączenia do połączenia niezabezpieczonego. Preferowany jest najsilniejszy dostępny algorytm szyfrowania.
48. Wszystkie połączenia do zewnętrznych systemów są uwierzytelniane.
49. Nagłówki HTTP Strict Transport Security są włączone do wszystkich zapytań i dla wszystkich poddomen.
50. Używane są tylko silne algorytmy, szyfry i protokoły w ramach całej hierarchii certyfikatów, włącznie z certyfikatem root i certyfikatami pośrednimi w ramach wybranego urzędu certyfikacji.
51. Konfiguracja TLS jest zgodna z bieżącymi najlepszymi praktykami szczególnie dlatego, że popularne ustawienia, szyfry i algorytmy z czasem mogą okazać się niebezpieczne.

52. Usługa akceptuje tylko zdefiniowany zestaw metod zapytań HTTP, takich jak GET i POST oraz nieużywane metody (takie jak TRACE, PUT, DELETE) są w sposób wyraźny zablokowane.
53. Każda odpowiedź HTTP zawiera nagłówek „content type”, określający bezpieczny zestaw znaków (np. UTF-8, ISO 8859-1).
54. Nagłówki HTTP lub jakakolwiek część odpowiedzi HTTP nie ujawniają szczegółowej informacji o wersjach komponentów Usługi.
55. Wykonawca jest zobowiązany do przeprowadzania przez niezależny uznany podmiot trzeci (uzgodniony i zaakceptowany przez PSG) regularnych (nie rzadziej niż raz na 12 miesięcy) audytów bezpieczeństwa mających na celu zbadanie zgodności stosowanych zabezpieczeń z uznanymi międzynarodowymi standardami (w tym co najmniej ISO/IEC 27018 oraz ISO/IEC 27001) i niezwłocznego przedstawienia ich wyników PSG.
56. Wykonawca ma obowiązek przeprowadzać regularne, nie rzadziej niż raz na 12 miesięcy, testy bezpieczeństwa systemów oraz infrastruktury Wykonawcy służącej do świadczenia Usługi na rzecz PSG oraz niezwłocznie dostarczyć PSG wyniki z przeprowadzonych testów.
57. Wykonawca zapewnia, że użytkownicy innych klientów Wykonawcy nie będą mieli dostępu do przetwarzanych w ramach Umowy Danych oraz że Dane będą odseparowane co najmniej w sposób logiczny od informacji jakichkolwiek innych podmiotów, w tym innych klientów Wykonawcy zgodnie z postanowieniami.

Załącznik nr 6 – część handlowa

Formularz cenowy

w odrębnym pliku excel

Załącznik nr 7 – część techniczna

Dotyczy Zapytania ofertowego na „Serwisowanie i konserwacja systemu zarządzania drukiem SafeCom oraz usługa wsparcia technicznego (maintenance) producenta oprogramowania SafeCom”

Wykaz zrealizowanych usług

Oświadczam/y, że zrealizowaliśmy / realizujemy następujące zamówienia:

Lp.	Przedmiot zamówienia	Termin realizacji		Zamawiający (nazwa, adres)	Wartość netto
		Rozpoczęcie	Zakończenie		
I	II	III	IV	V	VI

.....dnia.....

.....
podpisy osób wskazanych w dokumencie uprawniającym do występowania w obrocie prawnym
lub posiadających stosowne pełnomocnictwo

UWAGA:

Do każdego zamówienia wymienionego w wykazie należy załączyć dokument potwierdzający, że zamówienia te zostały wykonane należycie. Dokumentami potwierdzającymi, iż usługi przedstawione w wykazie zostały wykonane należycie mogą być referencje a także inne dokumenty potwierdzające wykonanie zamówienia tj. protokoły odbioru, rekomendacje, poświadczenie wykonania.

Załącznik nr 8 – część techniczna

WYKAZ OSÓB

Dotyczy: Serwisowanie i konserwacja systemu zarządzania drukiem SafeCom oraz usługa wsparcia technicznego (maintenance) producenta oprogramowania SafeCom.

Wykaz osób przy pomocy, których będzie realizowany Przedmiot Zapytania

<i>L.P.</i>	<i>Imię i nazwisko</i>	<i>Pełniona funkcja</i>	<i>Doświadczenie</i>
1.			
2.			

(miejsce i data)

.....
(podpis upoważnionego przedstawiciela)