Załącznik nr 8
do Specyfikacji Istotnych Warunków Zamówienia
wykonanie kontroli szczelności instalacji gazowej

Procesor: ……

(Nazwa dostawcy)

Ankieta wyboru podmiotu przetwarzającego

L.P.	PYTANIE	TAK/NIE (+ewentualne wyjaśnienie)
	WIEDZA FACHOWA	
1.	Czy podmiot przetwarzający posiada **doświadczenie** w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Prosimy o **udokumentowanie** świadczenia przedmiotowych usług.	
2.	Czy podmiot przetwarzający posiada wyznaczoną osobę, która wykonuje **zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych? (Zadanie to może być realizowane także przez podmiot zewnętrzny)**	
	Czy wyznaczone osoby do wykonywania w/w zadań posiadają odpowiednią wiedzę i przygotowane praktyczne do wykonywania swoich obowiązków z tego zakresu?	
3.	Czy przepisy prawa wymagają, aby dany podmiot przetwarzający wyznaczył inspektora ochrony danych?	
4.	Czy dany podmiot przetwarzający wyznaczył inspektora ochrony danych?	
5.	Czy podmiot przetwarzający wyznaczył inspektora ochrony danych, mimo że nie wymagają tego przepisy prawa lub też inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji?	
6.	Czy osoby po stronie **podmiotu przetwarzającego dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych?**	
7.	Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały **przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez podmiot przetwarzający?**	
8.	Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały **przeszkolone w zakresie zasad bezpieczeństwa informacji?**	
	WIARYGODNOŚĆ	
9.	Czy podmiot przetwarzający posiada **referencje** od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, to prosimy o przedstawienie takich referencji.	
10.	Czy stwierdzono prawomocną decyzją GIODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?	
11.	Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów podstępowania?	
12.	Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?	

13.	Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO?	
	ZASOBY	
1.	Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? Jeśli tak, prosimy o jej przedstawienie.	
2.	Czy podmiot przetwarzających wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?	
3.	Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?	
4.	Czy podmiot przetwarzający prowadzi rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako procesor)? Jeżeli nie, prosimy o wskazanie powodów.	
5.	Czy podmiot przetwarzający wdrożył zasady zarządzania bezpieczeństwem informacji, w tym:	
	a) system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat?	
	b) zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?	
	c) *[dla podmiotów publicznych]* zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności?	
	d) *[dla podmiotów podlegających pod Komisję Nadzoru Finansowego]* zasady zarządzania bezpieczeństwem informacji zgodne z odpowiednimi wytycznymi KNF?	
	Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.?	
6.	Czy podmiot przetwarzający dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - Privacy Impact Assessment)?	
7.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania (Statement of Applicability)?	
8.	Czy podmiot przetwarzający okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?	
9.	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:	
	a) pseudonimizację i szyfrowanie danych,	
	b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,	
	c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.	

10.	Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?	
11.	Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?	
12.	Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych?	
13.	Czy osoby delegowane do obsługi administratora posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane? Prosimy o przedłożenie listy osób upoważnionych, które będą obsługiwać administratora?	
14.	Czy osoby upoważnione do przetwarzania danych w ramach obsługi administratora zostały obowiązane do zachowania ich w tajemnicy?	
15.	Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania?	

data i podpis