W nawiązaniu do uruchomionego postępowania zakupowego na <u>świadczenie usług, których realizacja będzie wymagała przetwarzania danych osobowych</u>, powierzonych przez Spółkę ORLEN BUDONAFT Sp. z o.o., prosimy potencjalnego 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 wyznaczyli 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.		
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 **<u>wszystkie</u>** „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 podpowierzane 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) – prośba 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/administratora – 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 Spółki GK ORLEN, 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, zobowiązuję się do niezwłocznego (nie później niż przed podpisaniem Umowy) poinformowania o tych zmianach zlecającego/administratora.		

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

Data wypełnienia formularza: …….

Podpis osoby reprezentującej potencjalnego oferenta/podmiot przetwarzający: ……

Załącznik nr 1

MINIMALNE WYMAGANIA FORMALNE I TECHNICZNE W ZAKRESIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

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.

Wymagania techniczne (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.:
   8.1. tworzenia kopii zapasowych oraz testy przywracania z kopii zapasowych.
   8.2. 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:
    10.1. 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;
    10.2. dla każdej osoby, której dane osobowe są przetwarzane, system teleinformatyczny zapewnia odnotowanie:
        10.2.1. daty pierwszego wprowadzenia danych do systemu,
        10.2.2. identyfikatora użytkownika wprowadzającego dane,
        10.2.3. rejestracje wszelkich zmian wykonanych na danych.

    Odnotowanie informacji, o których mowa powyżej, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych do systemu.
    10.3. w przypadku udostępnienia danych osobowych, system zapewnia:
        10.3.1. odnotowanie informacji o odbiorcach,
        10.3.2. dacie udostępnienia,
        10.3.3. zakresie udostępnionych danych.

Podpis osoby reprezentującej potencjalnego oferenta/podmiot przetwarzający: …….