Załącznik nr 11 do Zapytania ofertowego

W nawiązaniu do uruchomionego postępowania zakupowego na <u>świadczenie usług, których realizacja będzie wymagała przetwarzania danych osobowych</u>, powierzonych przez Polską Spółkę Gazownictwa sp. z o.o. (PSG), 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 **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 zasobami własnymi 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 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, 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

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.

    Odnotowanie 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 rozwiązanie 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 Parametr 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