Załącznik nr 4a do SWZ

Postępowanie nr 261/2022/PN/DZP

Pełna nazwa firmy (dalej: Podmiot)	
Adres siedziby firmy	
Data	

	Kategoria	PYTANIE	Odpowiedź (TAK/NIE/ND)	Opis uzupełniający odpowiedź
1.	**WIEDZA FACHOWA**	Czy Podmiot posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Proszę o wskazanie liczby lat?		
2.		Czy po wejściu w życie RODO Podmiot przetwarzający powołał Inspektora Ochrony Danych (IOD)? Czy analiza wymogu powołania IOD jest udokumentowana?		
3.		W sytuacji braku powołania IOD - Czy zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych w Podmiocie pełni inna wyznaczona osoba?		
		Czy wyznaczone osoby do wykonywania w/w zadań posiadają odpowiednią wiedzę i doświadczenie w ochronie danych osobowych? Prosimy o wskazanie posiadanych kompetencji.		
4.		Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie przepisów o ochronie danych osobowych, zasad bezpieczeństwa informacji i bezpiecznego korzystania z systemu informatycznego?		
5.	**WIARYGODNOŚĆ**	Czy podmiot przetwarzający posiada wdrożone standardy bezpieczeństwa informacji lub inne certyfikaty potwierdzające stosowane procedury i mechanizmy bezpieczeństwa? Prosimy o ich wskazanie.		
6.		Czy przez ostatnie 5 lat podmiot przetwarzający podlegał kontroli PUODO? Jeżeli tak to czy były wydane przez PUODO zalecenia i czy zostały one zrealizowane.		

7.		Czy stwierdzono przez ostanie 5 lat, prawomocną decyzją PUODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu, naruszenie ochrony danych osobowych przez podmiot przetwarzający?		
8.	**ŚRODKI TECHNICZNE I ORGANIZACYJNE**	Czy podmiot przetwarzający opracował i wdrożył wewnętrzne regulacje w obszarze bezpieczeństwa informacji i ochrony danych osobowych, np.: Polityka bezpieczeństwa informacji, Polityka ochrony danych osobowych?		
9.		Czy podmiot przetwarzający wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, incydentów bezpieczeństwa informacji?		
10.		Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?		
11.		Czy podmiot przetwarzający prowadzi rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania danych osobowych?		
12.		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 podlegających pod Komisję Nadzoru Finansowego]* zasady zarządzania bezpieczeństwem informacji zgodne z odpowiednimi wytycznymi KNF?		
13.		Czy podmiot przetwarzający wdrożył politykę lub standard opisujący proces zarządzania ryzykiem?		
14.		Czy podmiot przetwarzający dokonuje oceny skutków dla ochrony danych osobowy (DPIA) i czy jest to udokumentowane?		
15.		Czy podmiot przetwarzający dokonuje szacowania ryzyka naruszenia praw lub wolności osób, których dane dotyczą i czy zostało to udokumentowane, np. czy został stworzony plan postępowania z ryzykiem?		
16.		Czy podmiot przetwarzający okresowo przeprowadza działania związane z DPIA oraz szacowaniem ryzyka naruszenia praw lub wolności osób? Czy w przypadku zmiany poziomu ryzyka dobierane są nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?		
17.		Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem zgodnie z art. 32 RODO.		
18.		Czy i jak często podmiot przetwarzający prowadzi przeglądy zabezpieczeń, audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocenę skuteczności		

		środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (w tym testy penetracyjne systemów)?		
19.		Czy osoby dopuszczone do przetwarzania danych osobowych posiadają upoważnienie do ich przetwarzania. Czy jest prowadzony rejestr osób upoważnionych do przetwarzania danych osobowych.		
20.		Czy osoby upoważnione do przetwarzania danych osobowych zostały przeszkolone z zasad bezpieczeństwa i ochrony danych osobowych. Czy zostało to udokumentowane?		
21.		Czy osoby upoważnione do przetwarzania danych zostały zobowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?		
22.		Czy podmiot przetwarzający zleca czynności podwykonawcom stosując dalsze powierzenie przetwarzania danych osobowych?		
23.		Czy podmiot przetwarzający przekazuje dane do państw trzecich poza terytorium UE? Jeżeli tak, proszę wskazać państwa do których są przekazywane dane.		
24.	**PRZETWARZANIE POWIERZONYCH DANYCH PRZEZ PODMIOT W JEGO WŁASNYCH SYSTEMACH INFORMATYCZNYCH**	Czy podmiot przetwarzający jest właścicielem serwerów?		
25.		Czy podmiot przetwarzający korzysta z usług dzierżawy serwerów?		
26.		Czy serwery znajdują się na terenie UE? Jeżeli nie to proszę wskazać miejsce ich lokalizacji.		
27.		Czy systemy informatyczne przetwarzające dane osobowe opierają się na rozwiązaniach chmurowych (proszę o wskazanie modelu usługi chmurowej publiczna, prywatna, inna oraz wskazanie dostawcy takiej usługi)?		