ROZDZIAŁ V SWZ - PYTANIA DO POTENCJALNEGO PODMIOTU PRZETWARZAJĄCEGO (PROCESORA) W CELU REALIZACJI OBOWIĄZKU ADMINISTRATORA DANYCH OSOBOWYCH, O KTÓRYM JEST MOWA W ART. 28 UST. 1 RODO.

L.P.	PYTANIE	TAK/NIE	WYMÓG
	WIEDZA FACHOWA		
1.	*[Pytanie ogólne]* Czy podmiot przetwarzający posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Potencjalny podmiot przetwarzający powinien udokumentować świadczenie przedmiotowych usług.		
2.	*[Pytanie ogólne]* Czy przepisy prawa wymagają, aby dany podmiot przetwarzający wyznaczył inspektora ochrony danych? *Procesor powinien wyznaczyć inspektora ochrony danych, jeżeli co najmniej jedna z następujących przesłanek jest spełniona:* *a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;* *b) główna działalność podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub* *c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.*		art. 37 RODO
3.	*[Pytanie po 25 maja 2018 r.]:* czy dany podmiot przetwarzający wyznaczył inspektora ochrony danych?		art. 37 RODO
4.	*[Pytanie po 25 maja 2018 r.]:* 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?		
5.	*[Pytanie ogólne]* Czy osoby po stronie **podmiotu przetwarzającego dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?**		

6.	*[Pytanie ogólne]* 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? Czy jest to udokumentowane?**		
7.	*[Pytanie ogólne]* Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały **przeszkolone w zakresie zasad bezpieczeństwa informacji? Czy jest to udokumentowane?**		
WIARYGODNOŚĆ			
1.	*[Pytanie ogólne]* Czy podmiot przetwarzający posiada **referencje** od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, to potencjalny podmiot przetwarzający powinien przedstawić takie referencje.		
2.	*[Pytanie ogólne]* Czy stwierdzono prawomocną decyzją GIODO lub PUODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?		
3.	*[Pytanie po 25 maja 2018 r.]:* Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania?		art. 40 RODO
4.	*[Pytanie po 25 maja 2018 r.]:* Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?		art. 41 RODO
5.	*[Pytanie po 25 maja 2018 r.]:* Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO?		art. 42 RODO
ZASOBY			
1.	*[Pytanie po 25 maja 2018 r.]* Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? Jeśli tak, prosimy o jej przedstawienie.		art. 24 RODO
2.	*[Pytanie ogólne]* Czy podmiot przetwarzający wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?		
3.	*[Pytanie ogólne]* Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?		

4.	*[Pytanie po 25 maja 2018 r.]* Czy podmiot przetwarzający prowadzi rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako podmiot przetwarzający)?		art. 30 RODO
5.	*[Pytania ogólne]* 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) Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.?		
6.	*[Pytanie po 25 maja 2018 r.]* 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)?		Odniesienie do Art. 24, 25, 32 RODO
7.	*[Pytanie po 25 maja 2018 r.]* Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania (Statement of Applicability)?		
8.	*[Pytanie po 25 maja 2018 r.]* 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.	*[Pytanie po 25 maja 2018 r.]* Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:		Art. 32 ust. 1 lit a)-c) RODO
	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.	*[Pytanie ogólne]* 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 oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?		Art. 32 ust. 1 lit d) RODO
11.	*[Pytanie ogólne]* Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?		
12.	*[Pytanie ogólne]* Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych?		
13.	*[Pytanie ogólne]* Czy osoby delegowane do obsługi ADO posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane? Prosimy o przedłożenie listy osób upoważnionych, które będą obsługiwać ADO.		
14.	*[Pytanie ogólne]* Czy osoby upoważnione do przetwarzania danych w ramach obsługi ADO zostały zobowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?		
15.	*[Pytanie ogólne]* Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania (upoważnienie osób może tez stanowić część innej ogólnej procedury)? Należy udokumentować istnienie takiej procedury.		