Załącznik nr 13 do Polityki Ochrony Danych Osobowych

KRYTERIA WYBORU PROCESORA

L.P.	PYTANIE	TAK/NIE	WYMÓG
	WIEDZA FACHOWA		
1.	**[Ważne]** Czy Procesor posiada **doświadczenie** w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Prosimy o **udokumentowanie** świadczenia przedmiotowych usług.		
2.	Czy przepisy prawa wymagają, aby dany Procesor wyznaczył inspektora ochrony danych osobowych (IOD)?		art. 37 RODO
3.	[**Ważne**]: czy dany Procesor wyznaczył IOD?		art. 37 RODO
4.	Czy Procesor wyznaczył IOD, mimo że nie wymagają tego przepisy prawa lub też inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji?		
5.	[**Ważne**] Czy osoby po stronie **Procesora dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?**		
6.	Czy osoby zatrudnione u Procesora przy przetwarzaniu danych zostały **przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez Procesora?**		
7.	Czy osoby zatrudnione u Procesora przy przetwarzaniu danych zostały **przeszkolone w zakresie zasad bezpieczeństwa informacji?**		

WIARYGODNOŚĆ			
8.	[**Ważne]** Czy Procesor posiada **referencje** od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, to prosimy o przedstawienie takich referencji.		
9.	Czy stwierdzono prawomocną decyzją GIODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez Procesora?		
10.	[**Ważne**] Czy Procesor stosuje się do przyjętych przez organ nadzorczy kodeksów podstępowania?		art. 40 RODO
11.	[**Ważne]** Czy Procesor objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?		art. 41 RODO
12.	[**Ważne]** Czy Procesor otrzymał certyfikat zgodności z RODO?		art.42 RODO
13.	Kryterium wewnętrzne: Czy rozważany Procesor jest znany na rynku jako podmiot wykonujący danego rodzaju usługi? Jeżeli tak, jaką ma renomę? Jakie są opinie o tym podmiocie, o współpracy z tym podmiotem, o stosowanych przez niego zabezpieczeniach czy przetwarzaniu danych?		
ZASOBY			
1.	Czy Procesor opracował i wdrożył Politykę bezpieczeństwa danych osobowych oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych?		
2.	[**Ważne]** Czy Procesor opracował i wdrożył politykę ochrony danych lub podobną procedurę?		art. 24 RODO
3.	Czy Procesor wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?		
4.	Czy Procesor prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?		

5.	Czy Procesor prowadzi wykaz lub/i rejestr przetwarzanych zbiorów danych osobowych?		
6.	[**Ważne**] Czy Procesor prowadzi rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako procesor)?		art. 30 RODO
7.	Czy Procesor 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?		
	Czy Procesor wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.?		
8.	[**Ważne**] 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
9.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania (Statement of Applicability)?		
10.	Czy Procesor 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?		
11.	[**Ważne**] Czy Procesor 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.		
12.	Czy Procesor 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?		Art. 32 ust. 1 lit d) RODO
13.	Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?		
14.	Czy Procesor jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych?		
15.	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?		
16.	[**Ważne**] Czy osoby upoważnione do przetwarzania danych w ramach obsługi ADO zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?		
17.	Czy Procesor wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania?		