Załącznik nr 1
do *„Umowy powierzenia przetwarzania danych osobowych”*

Załącznik nr 1
do umowy powierzenia przetwarzania danych osobowych
nr …… z dnia ……

ANKIETA OCENY PODMIOTU PRZETWARZAJĄCEGO

…… *(nazwa firmy)*

…… *(adres siedziby)*

…… *(strona www)*

LP.	PYTANIE	TAK/ NIE/ NIE DOTYCZY	UWAGI
1.	Czy *Podmiot przetwarzający* posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, jak długie?		
2.	Czy *Podmiot przetwarzający* posiada referencje od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, to prosimy o przedstawienie takich referencji.		
3.	Czy *Podmiot przetwarzający* wyznaczył inspektora ochrony danych?		
4.	Jeśli *Podmiot przetwarzający* nie ma obowiązku wyznaczenia inspektora ochrony danych, czy mimo wszystko wyznaczył inną osobę/zespół		

	odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji?		
5.	Czy stwierdzono prawomocną decyzją organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez *Podmiot przetwarzający*?		
6.	Czy *Podmiot przetwarzający* posiada opracowaną, zatwierdzoną i wdrożoną politykę ochrony danych osobowych lub inny dokument opisujący zasady ochrony informacji/danych osobowych?		
7.	Czy *Podmiot przetwarzający* prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?		
8.	Czy *Podmiot przetwarzający* wdrożył procedurę/instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?		
9.	Czy *Podmiot przetwarzający* prowadzi ewidencję naruszeń ochrony danych osobowych?		
10.	Czy *Podmiot przetwarzający* zapewnia realizacje praw osób, których dane dotyczą, w szczególności prawo do kopii danych, prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do usunięcia danych?		

11.	Czy *Podmiot przetwarzający* wdrożył zasady zarządzania bezpieczeństwem informacji, w tym:		
	– system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001/certyfikat?		
	– zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?		
	– inne zasady ochrony informacji, np. polityka bezpieczeństwa informacji, instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, procedury wewnętrzne regulujące zasady zarządzania infrastrukturą IT? Jeśli tak, prosimy wskazać w kolumnie „UWAGI" jakie.		
12.	Czy personel przetwarzający powierzone *Podmiotowi przetwarzającemu dane* osobowe został przeszkolony z zasad ochrony danych osobowych i zapoznany z obowiązującymi przepisami prawa w tym zakresie?		
13.	Czy zgodnie z art. 29 RODO personel przetwarzający powierzone *Podmiotowi przetwarzającemu dane* osobowe otrzyma od *Podmiotu przetwarzającego* upoważnienia do przetwarzania tych danych?		
14.	Czy personel *Podmiotu przetwarzającego*, upoważniony do przetwarzania danych, zostanie również zobowiązany do zachowania ich w tajemnicy?		
15.	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?		
16.	Czy *Podmiot przetwarzający* wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, w tym:		
	– pseudonimizację i szyfrowanie danych,		
	– zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,		
	– zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?		
17.	Czy *Podmiot przetwarzający* okresowo dokonuje przeglądu ryzyk związanych z przetwarzaniem danych osobowych?		
18.	Czy w przypadku zmiany poziomu ryzyka *Podmiot przetwarzający* dobiera nowe, odpowiednie środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?		
19.	Czy *Podmiot przetwarzający* przeprowadza regularne audyty / kontrole / przeglądy / sprawdzenia, dotyczące przestrzegania w organizacji przepisów związanych z ochroną danych osobowych?		

20.	Czy wnioski z audytów / kontroli / przeglądów / sprawdzeń, o których mowa w pytaniu powyżej, zostały udokumentowane?		
21.	Czy *Podmiot przetwarzający* jest przygotowany do poddania się audytowi przeprowadzonemu przez *Administratora* lub upoważnionego audytora *Administratora* w zakresie weryfikacji udzielonych odpowiedzi w niniejszej ankiecie i stosowanych rozwiązań w obszarze ochrony powierzonych danych osobowych?		
22.	Czy *Podmiot przetwarzający* korzysta z usług podwykonawców przy przetwarzaniu powierzonych danych osobowych? Jeśli tak, prosimy wskazać w kolumnie „UWAGI" dane podwykonawców (nazwa oraz adres siedziby)		
23.	Czy podwykonawcy zostali /zostaną poddani weryfikacji pod kątem wdrożenia środków ochrony danych osobowych?		
24.	Czy z podwykonawcami została/zostanie zawarta umowa powierzenia przetwarzania danych osobowych?		
25.	Czy powierzone dane osobowe będą przetwarzane poza granicami Unii Europejskiej (dokumenty papierowe, urządzenia elektroniczne, serwery z danymi, usługi chmurowe, itp.)? Jeśli tak, prosimy wskazać szczegóły w kolumnie „UWAGI".		

26.	Czy systemy informatyczne przetwarzające dane osobowe wykorzystywane przez *Podmiot przetwarzający* opierają się na rozwiązaniach chmurowych? Jeśli tak, prosimy o wskazanie w kolumnie „UWAGI" modelu usługi chmurowej (publiczna/prywatna).		
27.	Czy *Podmiot przetwarzający* stosuje fizyczne środki służące ochronie danych przed nieuprawnionym dostępem? Jeśli tak, prosimy je wymienić w kolumnie „UWAGI" (np. system kontroli dostępu, drzwi zamykane na klucz, system alarmowy, ochrona fizyczna, monitoring wizyjny).		
28.	Czy *Podmiot przetwarzający* stosuje techniczne środki służące ochronie danych przed nieuprawnionym dostępem? Jeśli tak, prosimy je wymienić w kolumnie „UWAGI" (np. oprogramowanie IDS/IPS, firewall, antywirus itp.)		
29.	Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane?		
30.	Czy dostęp do wykorzystywanych przez *Podmiot przetwarzający* systemów informatycznych, przetwarzających powierzone dane osobowe, wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		

31.	Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?		
32.	Czy systemy informatyczne przetwarzające dane osobowe wykorzystywane przez *Podmiot przetwarzający* pozwalają przypisać określone działanie w systemie do osoby lub procesu oraz umiejscowić je w czasie (zapewniają rozliczalność operacji wykonywanych na danych)?		

.....

(data, pieczątka,
podpis osoby wypełniającej ankietę)