ANKIETA OCENY PODMIOTU W ZWIĄZKU Z ZAMIAREM POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH					
Wyjaśnienie (podstawa prawna) Zgodnie z art. 28 ust. 1 RODO* *„Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”*.					
Nr	**TREŚĆ PYTANIA**	**WYJAŚNIENIE**	**ODPOWIEDZI**		
			TAK/NIE/ND	**UWAGI/KOMENTARZE**	**OCENA ORGANIZACJI (dokonuje MOPS)**
Przestrzeganie wymogów prawa					
1.	**Czy w Państwa organizacji wdrożono Politykę(i) ochrony danych lub inny dokument(y) regulujący(-ce) zasady ochrony danych osobowych?**	*Obowiązek wdrożenia odpowiednich środków organizacyjnych (np. polityk) wynika m.in. z art. 24 i 32 RODO.*			
2	**Czy w Państwa organizacji wdraża się środki organizacyjne i techniczne, aby przetwarzanie danych odbywało się zgodnie z RODO, dokonując analizy ryzyka?**	*Obowiązek prowadzenia stosownej analizy przewiduje m.in. art. 24 i 32 RODO?*			
3.	**Czy w Państwa organizacji prowadzony jest rejestr naruszeń ochrony danych osobowych?**	*Rejestr naruszeń jest dokumentem, w którym powinny być ewidencjonowane wszelkie incydenty naruszenia ochrony danych osobowych. W rejestrze. opisuje się zdarzenie, które miało miejsce, skutki naruszenia oraz podjęte działania zaradcze, mające na celu usunięcie skutków naruszenia oraz zminimalizowanie prawdopodobieństwa powtórzenia się naruszenia w przyszłości.*			

4.	**Czy w Państwa organizacji prowadzone są stosowne rejestry czynności przetwarzania danych?**	*Rejestr czynności przetwarzania danych i Rejestr kategorii czynności przetwarzania danych osobowych są dokumentem, w którym powinny być wpisane co najmniej informacje o których mowa w art. 30 RODO?*			
5.	**Czy Państwa pracownicy / współpracownicy są upoważnieni do przetwarzania danych osobowych?**	*Każda osoba mająca dostęp do danych osobowych powinna zostać upoważniona do ich przetwarzania przez administratora lub podmiot przetwarzający. Pytanie ma na celu zweryfikowanie, czy organizacja udzieliła swoim pracownikom / współpracownikom ww. upoważnień.*			
6.	**Czy osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?**	*Wymóg zobowiązania do zachowania tajemnicy przez osoby przetwarzające dane z upoważnienia podmiotu przetwarzającego wynika z art. 28 RODO. Konieczne jest zatem, aby osoby upoważnione do przetwarzania danych podpisały zobowiązanie do zachowania poufności (może to być odrębny dokument lub takie zobowiązanie może być częścią umowy zawartej pomiędzy organizacją a jego pracownikiem / współpracownikiem).*			
7.	**Jeżeli Państwa organizacja dokonuje transferów danych do państw poza EOG, to czy zapewniony jest mechanizm legalizujący taki transfer?**	*W przypadku transferów danych poza EOG (EOG obejmuje kraje UE oraz Islandię, Norwegię oraz Liechtenstein) należy zapewnić, aby taki transfer był legalny (przykładem mechanizmu legalizującego transfer jest zawarcie umowy z kontrahentem w brzmieniu zgodnym ze standardowymi klauzulami umownymi przyjętymi przez Komisję Europejską). Przykładem, gdy dochodzi do transferu, jest sytuacja, w której zawarta została umowa na świadczenie usług hostingowych z usługodawcą, którego serwery znajdują się w USA.*			

Kryteria dodatkowe - ocena wiedzy fachowej oraz wiarygodności podmiotu					
8.	**Czy został powołany Inspektor Ochrony Danych (IOD) lub została wyznaczona osoba do wykonywania zadań związanych z zapewnieniem zgodności przetwarzania danych osobowych w Państwa organizacji zgodnie z obowiązującym prawem?**	*IOD jest powoływany w przypadkach określonych w art. 37 RODO, a także gdy dany podmiot zdecyduje się na jego wyznaczenie w sytuacji, gdy przepisy nie narzucają takiego obowiązku. Jeżeli nie ma formalnie powołanego IOD, wówczas należy wskazać, czy została wyznaczona inna osoba, która jest odpowiedzialna za wykonywanie zadań w zakresie ochrony danych osobowych w organizacji.*			
9.	**Czy IOD lub inna osoba wyznaczona do wykonywania zadań związanych z ochroną danych osobowych posiada odpowiednie kwalifikacje, dające gwarancję zgodności przetwarzania danych osobowych z przepisami prawa?**	*Za osobę spełniającą wskazany wymóg uważa się w szczególności: osobę, która posiada co najmniej 1-letnie doświadczenie w pełnieniu funkcji IOD/ administratora bezpieczeństwa informacji, osobę, która ukończyła studia podyplomowe w dziedzinie ochrony danych osobowych lub bezpieczeństwa informacji na uczelni wyższej, radcę prawnego lub adwokata z co najmniej 1-letnim doświadczeniem w dziedzinie ochrony danych osobowych.*			
10.	**Czy Państwa organizacja posiada wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych?**	*Celem tego pytania jest zweryfikowanie, czy organizacja posiada dostateczną wiedzę i kompetencje, aby być w stanie zidentyfikować oraz ocenić naruszenia ochrony danych osobowych w jego organizacji.*			
11.	**Czy Państwa organizacja dysponuje odpowiednio wyposażonymi i zabezpieczonymi pomieszczeniami umożliwiającymi bezpieczne**	*Celem tego pytania jest zweryfikowanie, czy organizacja posiada zasoby do zapewniające bezpieczeństwo fizyczne danych osobowych (np. zamykane na klucz szafy, pomieszczenia, zabezpieczenie pomieszczeń/budynku alarmem z zapewnieniem interwencji).*			

	przetwarzanie danych osobowych?				
12.	**Czy Państwa organizacja dysponuje odpowiednio zabezpieczonym systemem informatycznym umożliwianym przetwarzanie danych osobowych w formie elektronicznej?**	*Celem tego pytania jest zweryfikowanie, czy organizacja posiada zasoby do zapewniające bezpieczeństwo informatyczne danych osobowych (np. zapewnienie dostępu do systemu informatycznego co najmniej za pomocą identyfikatora i hasła, stosowanie środków ochrony przed szkodliwym oprogramowaniem, stosowanie systemu Firewall do ochrony dostępu do sieci komputerowej).*			
13.	**Czy Państwa organizacja posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji?**	*Chodzi o certyfikaty takie jak np.: certyfikat bezpieczeństwa informacji 27001, certyfikat CISA (Certified Information Systems Auditor), certyfikat CISSP (Certified Information Systems Security Professional) itp.*			

……..
(podpis Oferenta/Zleceniobiorcy/Wykonawcy)

ND-nie dotyczy

*rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)