NAZWA PODMIOTU PRZETWARZAJĄCEGO:			ZNAK SPRAWY:	
Ankieta dla Podmiotu Przetwarzającego (Wykonawcy / Kontrahenta)*			DATA WYPEŁNIENIA ANKIETY:	
L.p.	**Obszar**	**Pytanie**	**Odpowiedź (wskazać: Tak/ Nie/ Nie dotyczy)**	**Uwagi**
1	**Weryfikacja ogólna**	**Czy Podmiot Przetwarzający stosuje zatwierdzony przez organ nadzorczy (tj. Prezesa Urzędu Ochrony Danych Osobowych) kodeks postępowania, o którym mowa w art. 40 RODO? (uwaga - brak stosowania kodeksu nie wpływa negatywnie na ocenę)**		
2	**Weryfikacja ogólna**	**Czy Podmiot Przetwarzający uzyskał certyfikat w zakresie ochrony danych osobowych, o którym mowa w art. 42 RODO? (uwaga - brak certyfikatu nie wpływa negatywnie na ocenę)**		
3	**Weryfikacja ogólna**	**Czy Podmiot Przetwarzający poddawał system zarządzania bezpieczeństwem informacji i system ochrony danych osobowych w ciągu ostatnich 12 miesięcy audytowi przeprowadzanemu przez niezależnych audytorów i uzyskał ocenę pozytywną?**		
4	**Weryfikacja procedur**	Czy Wykonawca jest w stanie wykazać, że posiada udokumentowaną, opracowaną i wdrożoną politykę ochrony danych osobowych, wewnętrzne procedury lub inne udokumentowane regulacje określające zasady ochrony danych osobowych?		
5	**Bezpieczeństwo fizyczne i organizacyjne**	Czy stosowana jest polityka czystego biurka (w szczególności - czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych na klucz szafach/szafkach/szufladach ograniczając możliwość dostępu do nich osób nieupoważnionych)?		
6	**Bezpieczeństwo fizyczne i organizacyjne**	Czy stosowana jest polityka czystego ekranu (stosowane są wygaszacze ekranu wymagające podania hasła do ponownego zalogowania na komputerze)?		
7	**Bezpieczeństwo fizyczne i organizacyjne**	Czy kontrahent zastosował środki kontroli dostępu fizycznego do obszaru przetwarzania danych/budynków (polityka kluczy, dozór ochrony, alarm antywłamaniowy itp.)?		
8	**Weryfikacja procedur**	Czy odpowiednie klauzule informujące o przetwarzaniu danych osobowych zostały opracowane i są udostępniane osobom, których dane dotyczą (zgodnie z art. 13 i 14 RODO)?		
9	**Weryfikacja procedur**	Czy opracowano procedurę realizacji praw osób, których dane dotyczą (art. 15 – art. 22 RODO)?		
10	**Weryfikacja procedur**	Czy podmiot przetwarzający, potrafi wykazać, że korzysta lub będzie korzystał z usług tylko takich podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?		
11	**Zarządzanie personelem**	Czy osoby mające dostęp do danych posiadają odpowiednie upoważnienia do przetwarzania danych osobowych (art. 29 RODO)?		
12	**Bezpieczeństwo systemu informatycznego**	Czy kontrahent zarządza dostępem do systemów oraz programów komputerowych poprzez audytowalny proces nadawania, przeglądu i odbierania uprawnień oraz stosowania bezpiecznych mechanizmów uwierzytelniania?		
13	**Zarządzanie personelem**	Czy osoby upoważnione do przetwarzania danych zostały zobowiązane do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?		
14	**Zarządzanie personelem**	Czy osoby upoważnione do przetwarzania są poddawane okresowym szkoleniom z zakresu ochrony danych?		
15	**Inwentaryzacja procesów**	Czy prowadzony jest lub prowadzony będzie rejestr kategorii czynności przetwarzania danych (zgodnie z art. 30 ust. 2 RODO)?		

16	**Zarządzanie dostępem**	Czy w celu ograniczania ryzyk dla osób, których dane dotyczą, zapewnia się stosowanie zabezpieczeń kryptograficznych – w tym szyfrowanie i pseudonimizację danych?		
17	**Analiza ryzyka**	Czy stosowane są środki bezpieczeństwa dotyczące zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania zgodnie z aktualnie przeprowadzanym szacowaniem ryzyka dla ochrony danych i oceną skutków dot. praw i wolności osób, których dane dotyczą (art. 35 RODO)?		
18	**Analiza ryzyka**	Czy zapewniono regularne testowanie, mierzenie i ocenianie skuteczności wdrożonych zabezpieczeń technicznych i organizacyjnych dla ochrony danych?		
19	**Zarządzanie incydentami**	Czy zapewniono zdolność do przywrócenia dostępności danych w przypadkach wystąpienia incydentów w akceptowalnym czasie?		
20	**Zarządzanie incydentami**	Czy opracowano i wdrożono procedurę reagowania na zidentyfikowane naruszenia ochrony danych, zgłaszania naruszeń do organu nadzorczego i informowania osób, których dane dotyczą o naruszeniu (art. 33 i art. 34 RODO)?		
21	**Zarządzanie incydentami**	Czy prowadzona i aktualizowana jest ewidencja naruszeń ochrony danych osobowych?		
22	**Weryfikacja ogólna**	Czy w Podmiocie Przetwarzającym wyznaczono inspektora ochrony danych lub inną osobę odpowiedzialną za nadzór nad ochroną danych osobowych?		
23	**Zapewnienie ciągłości działania**	Czy Podmiot Przetwarzający wdrożył plan ciągłości działania dla kluczowych procesów organizacji w przypadku wystąpienia sytuacji kryzysowych (w szczególności - czy wdrożono procedurę odtwarzania działania systemu informatycznego po awarii)?		
24	**Zapewnienie ciągłości działania**	Czy Podmiot Przetwarzający przechowuje kopie zapasowe w bezpiecznej lokalizacji oraz zabezpiecza kopie zapasowe przed nieuprawnionym dostępem?		
25	**Audyty**	Czy przeprowadzane są 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?		
			uzupełnij ankietę	
		Wynik końcowy:	**niekompletne dane**	

*** ankieta służy jako pomocne narzędzie przy przeprowadzania audytów, w tym inspekcji przez administratora, w ramach wykonywania swoich uprawień określonych w art. 28 ust. 3 lit. h RODO; w celu zawarcia umowy powierzenia przetwarzania danych, Podmiot Przetwarzający może być poproszony o przedłożenie dodatkowych informacji, w tym dowodów dotyczących udzielonych odpowiedzi**

Oświadczam, że podane przeze mnie informacje są zgodne ze stanem faktycznym

podpis osoby upoważnionej do reprezentacji podmiotu