

Załącznik nr 4 do Uchwały Nr 5766/2026

Zarządu Województwa Opolskiego

z dnia 30 czerwca 2026 r.

Załącznik nr 4 do umowy Nr DOA-ZP.273. 2026

ANKIETA WERYFIKACYJNA

ANKIETA DLA PODMIOTU PRZETWARZAJĄCEGO

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.* Z uwagi na obowiązek weryfikacji podmiotu przetwarzającego nałożony przepisami RODO na administratora danych, proszę o uzupełnienie poniższej tabeli.

LP.	PYTANIE	TAK/NIE/NIE DOTYCZY	UWAGI
1.	Czy Państwa organizacja posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych lub inny dokument opisujący ochronę informacji/danych osobowych?		
2.	Czy Państwa organizacja prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?		
3.	Czy w Państwa organizacji dobrano zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do poziomu ryzyka naruszenia praw i wolności osób, których dane dotyczą zgodnie z art. 32 RODO, uwzględniając regularne testowanie oraz mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?		
4.	Czy Państwa organizacja podlega obowiązkowi wyznaczenia inspektora ochrony danych, zgodnie z art. 37 RODO?		
5.	Czy Państwa organizacja wyznaczyła inspektora ochrony danych? Proszę o umieszczenie danych kontaktowych do osoby pełniącej funkcję Inspektora Ochrony Danych w Państwa organizacji w kolumnie UWAGI.		
6.	Czy, w ramach realizacji zadań powierzonych przez Administratora Danych Osobowych dane osobowe będą przekazywane podmiotom trzecim? Jakim? Czy są podpisane z tymi podmiotami umowy powierzenia?		

7.	Czy, w ramach realizacji zadań powierzonych przez Administratora Danych Osobowych dochodzi do przekazywania danych do podmiotów spoza Europejskiego Obszaru Gospodarczego? Jeśli tak, to na jakiej podstawie dane te są przekazywane?		
8.	Czy Państwa organizacja gwarantuje, że podmioty, którym dane osobowe są podpowierane posiadają adekwatny system zabezpieczeń tych danych?		
9.	Czy Państwa pracownicy, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? (tzw. klauzula poufności)		
10.	Czy pracownicy i współpracownicy Państwa organizacji tj. osoby wykonujące operacje na danych osobowych otrzymały upoważnienia do przetwarzania danych?		
11.	Czy upoważnienia te zawierają określony zakres przetwarzanych osoby danych?		
12.	Czy nowo zatrudniony pracownik w Państwa organizacji przed podjęciem czynności związanych z przetwarzaniem danych osobowych jest odpowiednio przeszkolony z zakresu ochrony danych osobowych?		
13.	Czy dbacie Państwo o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?		
14.	Czy Państwa organizacja wdrożyła instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, w tym ich zgłaszania do Administratora Danych Osobowych?		
15.	Czy Państwa organizacja prowadzi rejestr naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?		
16.	Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?		
17.	Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowej zmiany haseł. Proszę o wskazanie w kolumnie UWAGI okresu, co jaki wymuszana jest zmiana hasła.		
18.	Czy w Państwa organizacji zostały określone wymagania co do budowy hasła? Jeśli tak, proszę w kolumnie UWAGI o wskazanie tych wymogów.		
19.	Czy pracownicy zostali zobowiązani do stosowania blokady komputera w momencie opuszczania stanowiska pracy?		

20.	Czy posiadają Państwo oprogramowanie antywirusowe na wszystkich stacjach roboczych?		
21.	Czy oprogramowanie posiada aktualne licencje i jest na bieżąco aktualizowane?		
22.	Czy w komputerach przenośnych zastosowano szyfrowanie dysków?		
23.	Czy Państwa organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?		
24.	Czy w Państwa organizacji jest stosowana polityka tzw. „czystego biurka”?		
25.	Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?		
26.	Czy Państwa organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?		
27.	Czy Państwa organizacja wdrożyła inne zasady, standardy, regulaminy, procedury, polityki lub zbiory najlepszych praktyk mające znaczenie dla ochrony informacji/danych osobowych? Jeśli tak proszę w kolumnie UWAGI proszę wskazać jakie.		
28.	Czy Państwa organizacja zapewnia możliwość całkowitego usunięcia danych osobowych/zwrotu danych osobowych przetwarzanych w związku z realizacją umowy z Administratorem Danych Osobowych?		
29.	Czy Państwa organizacja przechodzi niezależne audyty? Jeśli tak to takie?		
30.	Czy Państwa organizacja wdrożyła procedury oceny ryzyka i czy wszystkie procesy przetwarzane są z ryzykiem niskim?		

Oświadczenie

Oświadczam, że podane przeze mnie informacje są prawdziwe i odzwierciedlają rzeczywisty stan faktyczny w z siedzibą przy (dalej jako). Jednocześnie, w przypadku zawarcia umowy o współpracę, zobowiązuję się w imieniu, że powyższe informacje zostaną potwierdzone w formie oświadczenia, które stanowiłoby postanowienie umowne bądź załącznik do takiej umowy.

(data i czytelny podpis)