Załącznik nr 5 do SIWZ

Oświadczenie podmiotu o zastosowaniu odpowiednich środków technicznych i organizacyjnych gwarantujących ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, o których mowa w art. 32 ogólnego rozporządzenia.

Ankieta weryfikacji podmiotu przetwarzającego pod kątem jego zgodności z przepisami RODO

Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Art. 28 ust. 1 ogólnego rozporządzenia

„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”.

Motyw 81 ogólnego rozporządzenia

*„**Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje - w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby - wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania”.***

Dane podmiotu przetwarzającego	

Dotyczy oferty/zamówienia/umowy	

	Pytanie	**Odpowiedzi**

Załącznik nr 5 do SIWZ

ZAGADNIENIA OGÓLNE			
1	Czy podmiot realizując swoją działalność przeprowadza procesy przetwarzania danych w innych krajach? ***Jeśli tak, proszę wskazać gdzie.***	Tak/Nie	
2	Czy w celu realizacji umowy niezbędne okaże się przekazanie danych administratora do innego kraju UE lub do państwa trzeciego? ***Jeśli tak, proszę wskazać gdzie.***	Tak/Nie	
3	Czy realizując przedmiotową umowę podmiot będzie korzystał z usług innych wykonawców? ***Jeżeli tak proszę wskazać te podmioty.*** ***Dotyczy to również sytuacji związanych z hostingiem, serwisem technicznym.***	Tak/Nie	
4	Czy inni wykonawcy, z których usług korzysta podmiot, a przetwarzający dane administratora zostali przez niego sprawdzeni pod kątem bezpieczeństwa danych osobowych? ***Jeśli tak, proszę wskazać sposób dokonania sprawdzenia***	Tak/Nie	
5	Czy podmiot realizując swoją działalność obsługiwał lub obsługuje podmioty, z którymi ma zawarte umowy powierzenia przetwarzania danych?	Tak/Nie	
6	Czy podmiot posiada i stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 lub zatwierdzony mechanizm certyfikacji, o	Tak/Nie	

	którym mowa w art. 42. ***Jeżeli tak proszę wskazać jego nazwę i przez jaki organ został przyjęty.*** ***W przypadku posiadania certyfikatu, proszę o przesłanie kopii dokumentu.***		
ZASOBY KADROWE			
7	Czy podmiot jest zobowiązany na podstawie art. 37 ogólnego rozporządzenia do wyznaczenia inspektora ochrony danych?	Tak/Nie	
8	Jeśli podmiot powołał inspektora ochrony danych, proszę wskazać informację o sposobie kontaktu z IOD, w szczególności: numer telefonu, adres mailowy, adres korespondencyjny.		
9	Czy pracownicy podmiotu biorący udział w procesie przetwarzania danych zostali zapoznani z przepisami regulującymi ochronę danych osobowych oraz przeszkolone? ***Jeżeli tak, proszę wskazać jakie dokumenty będące w posiadaniu podmiotu potwierdzają powyższe okoliczności np. listy szkoleń, certyfikaty szkoleniowe itp.***	Tak/Nie	
10	Czy pracownicy podmiotu upoważnieni do przetwarzania danych osobowych systematycznie pogłębiają nabytą wiedzę poprzez cykliczne szkolenia? ***Jeżeli tak proszę wskazać jakie dokumenty będące w posiadaniu podmiotu potwierdzają powyższe okoliczności oraz częstotliwość tych szkoleń.***	Tak/Nie	

11	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? ***Jeżeli tak proszę wskazać jakie dokumenty będące w posiadaniu podmiotu potwierdzają powyższe okoliczności***	Tak/Nie	
12	Czy pracownicy wykonujący operacje na danych osobowych posiadają pisemne upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych wraz z poleceniem?	Tak/Nie	
13	Czy podmiot prowadzi ewidencję osób upoważnionych?	Tak/Nie	
14	Czy podmiot wdrożył procedurę przyznawania pracownikom uprawnień do przetwarzania danych osobowych w systemach informatycznych?	Tak/Nie	
15	Czy pracownicy podmiotu biorący udział w procesie przetwarzania danych przy wykorzystaniu systemów informatycznych zostali przeszkoleni z ich obsługi w sposób gwarantujących bezpieczeństwo przetwarzanych tam danych? ***Jeżeli tak, proszę wskazać jakie dokumenty będące w posiadaniu podmiotu potwierdzają powyższe okoliczności.***	Tak/Nie	
16	Czy pracownicy zostali zobowiązani do każdorazowego zgłaszania incydentów naruszenia ochrony danych osobowych?	Tak/Nie	

17	Czy została wdrożona procedura/instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych? ***Jeżeli tak, proszę o przekazanie kopii stosownego dokumentu.***	Tak/Nie	
18	Czy pracownicy niszczą zbędne dokumenty papierowe zawierające dane osobowe przy użyciu niszczarki dokumentów?	Tak/Nie	
ZABEZPIECZENIE PRZETWARZANYCH DANYCH OSOBOWYCH			
19	Czy podmiot wdrożył system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? ***Jeżeli tak proszę przekazać dokument potwierdzający powyższą okoliczność.***	Tak/Nie	
20	Czy podmiot wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, w tym:	Tak/Nie	
	• pseudonimizację i szyfrowanie danych osobowych	Tak/Nie	
	• zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania	Tak/Nie	
	• zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego	Tak/Nie	
21	Czy podmiot stosuje się do zasad zarządzaniem bezpieczeństwem informacji zgodnie z	Tak/Nie	

	wymaganiami Krajowych Ram Interoperacyjności?		
22	Czy podmiot wdrożył odpowiednie środki fizycznego zabezpieczenia danych osobowych gwarantujące bezpieczeństwo przetwarzanych danych?	Tak/Nie	
23	Czy serwery podmiotu znajdują się w pomieszczeniach, do których dostęp ma tylko podmiot. Jeżeli w pomieszczeniach serwerowni znajdują się również serwery innych podmiotów proszę wskazać wdrożone środki bezpieczeństwa gwarantujące bezpieczeństwo danych przetwarzanych przez podmiot.	Tak/Nie	
24	Czy obszar przetwarzania danych osobowych zabezpieczony jest przed dostępem osób nieuprawnionych?	Tak/Nie	
25	Czy kopie zapasowe/archiwalne, na których umieszczone są dane osobowe przechowywane są w odrębnym pomieszczeniu?	Tak/Nie	
26	Czy podmiot stosuje programy do ochrony dostępu do sieci komputerowej?	Tak/Nie	
27	Czy podmiot stosuje systemy do wykrywania i blokowania ataków do sieci komputerowej?	Tak/Nie	
28	Czy systemy informatyczne zapewniają rejestrację dostępu do danych osobowych ze wskazaniem kto, kiedy dane wprowadzał, przeglądał, zmieniał, usuwał?	Tak/Nie	

29	Czy systemy operacyjne i przeglądarki mają instalowane aktualizacje?	Tak/Nie	
30	Czy zainstalowano wygaszacze ekranów chronione hasłem na stacjach roboczych?	Tak/Nie	
31	Czy pracownik, czasowo opuszczając stanowisko pracy, wylogowuje się z systemu?	Tak/Nie	
32	Czy ekrany monitorów zostały ustawione w sposób uniemożliwiający wgląd przez osoby nieupoważnione	Tak/Nie	
33	Czy nośniki informacji podłączone do stacji roboczej sprawdzane są oprogramowaniem antywirusowym	Tak/Nie	
34	Czy podmiot prowadzi rejestr kategorii czynności przetwarzania, zawierający wszystkie informacje wskazane w art. 30 ust. 2 ogólnego rozporządzenia?	Tak/Nie	
35	Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie bezpieczeństwa danych osobowych m. in. poprzez wdrożenie w jego organizacji procedur i dokumentacji ochrony danych osobowych?	Tak/Nie	
36	Czy podmiot gwarantuje realizacje praw osób, których dane dotyczą zgodnie z obowiązkami wynikającymi z rozdziału III ogólnego rozporządzenia?	Tak/Nie	
37	Czy podmiot ustalił procesy przetwarzania danych osobowych?	Tak/Nie	
38	Czy podmiot dokonał analizy ryzyka procesów przetwarzania danych osobowych?	Tak/Nie	

39	Czy podmiot okresowo przeprowadza kolejne działania szacowania ryzyka? ***Jeśli tak, proszę wskazać częstotliwość?***	Tak/Nie	
40	Czy szacowanie ryzyka pod kątem prywatności zostało udokumentowane (np. czy został opracowany plan postępowania z ryzykiem)? ***Jeżeli tak, proszę o przekazanie kopii dokumentacji***	Tak/Nie	
41	Czy podmiot wykonał ocenę skutków dla ochrony danych osobowych?	Tak/Nie	
42	Czy podmiot dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzania danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą?	Tak/Nie	
43	Czy podmiot prowadzi regularne audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełnienia wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? ***Jeżeli tak, proszę o wskazanie częstotliwości prowadzenia audytów.***	Tak/Nie	
44	Czy podmiot podda się audytowi/kontroli przetwarzania danych osobowych przeprowadzonej przez administratora lub audytora upoważnionego przez administratora?	Tak/Nie	

45	Czy w związku z realizacją prawa administratora do audytu/kontroli, administrator zobowiązany jest do zapłaty jakichkolwiek kwot na rzecz podmiotu (np. wynagrodzenia dla pracowników podmiotu za ich udział w audycie)?	Tak/Nie	
46	Czy w przypadku braku ustaleń co do wysokości wynagrodzenia dla podmiotu za przeprowadzenie audytu lub kontroli, podmiot umożliwi administratorowi przeprowadzenie takiego audytu/kontroli?	Tak/Nie	
INCYDENTY			
47	Czy podmiot dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.	Tak/Nie	
48	Czy w trakcie przetwarzania danych przez podmiot doszło *naruszenia* ochrony danych osobowych skutkującego koniecznością powiadomienia organu nadzorczego?	Tak/Nie	
49	*Czy naruszenie* ochrony danych osobowych zostało stwierdzone prawomocną decyzją organu nadzorczego lub wyrokiem sądu?	Tak/Nie	
50	Czy w trakcie przetwarzania danych przez podmiot doszło *naruszenia* ochrony danych osobowych skutkującego koniecznością zawiadomienia osób, których danych dotyczyło?	Tak/Nie	
RETENCJA DANYCH			
51	Czy dane osobowe przetwarzane są wyłącznie przez czas niezbędny do realizacji celu	Tak/Nie	

	przetwarzania?		
52	W jaki sposób podmiot ustala czy nie minął okres przechowywania danych osobowych?	Tak/Nie	

Oświadczam, że wszystkie podane informacje w **ankiecie są zgodne z prawdą.**

……

(miejscowość, data, imię i nazwisko osoby uprawnionej do reprezentowania podmiotu)

Załącznik nr 5 do SIWZ