ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Załącznik nr 1 do umowy powierzenia danych osobowych nr: ..... z dnia: ..... .

Podmiot przetwarzający:	
Imię I Nazwisko osoby wypełniającej	
Stanowisko	
Adres e-mail i nr telefonu	

Lp.	Pytanie	Odpowiedź	Uwagi
1	Proszę podać ilość lokalizacji i kraje, w których będą przetwarzane powierzone dane osobowe.		
2	Czy Państwa personel został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
3	Czy personel przetwarzający powierzone dane osobowe w pozostałych krajach został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
4	Czy powierzone dane osobowe będą przekazywane poza EOG? Np. ze względu na lokalizację systemu IT, będą przetwarzane przez osoby zlokalizowane poza EOG lub osoby te będą miały możliwość dostępu do tych danych?		
5	Jeśli tak to w jakim kraju?		
6	Czy w Państwa organizacji przeprowadzane są okresowe audyty zgodności z przepisami ochrony danych osobowych?		
7	Czy w Państwa organizacji przeprowadzane są okresowe audyty bezpieczeństwa IT?		
8	Czy posiadają Państwo wdrożoną politykę bezpieczeństwa przetwarzania danych osobowych zgodną z zasadami RODO?		
9	Czy prowadzą Państwo rejestr czynności przetwarzania, w tym dla procesora, zgodnie z art. 30 RODO?		
10	Czy jesteście Państwo zobowiązani do wyznaczenia IOD, zgodnie z art. 37 RODO?		
11	Jeśli tak, to czy wyznaczono IOD?		
12	Jeśli nie, to czy wyznaczyli Państwo osobę, która będzie odpowiedzialna za zapewnienie zgodności przetwarzania danych z przepisami i bezpieczeństwa danych?		
13	Czy do przetwarzania danych w Państwa organizacji są dopuszczone wyłącznie osoby posiadające upoważnienia?		
14	Czy osoby te zostały zobowiązane do zachowania poufności danych oraz informacji o stosowanych przez Państwa zabezpieczeniach?		

15	Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych?		
16	Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO?		
17	Czy wdrożyli Państwo instrukcję postępowania w przypadku sytuacji naruszenia ochrony danych osobowych?		
18	Jeśli tak, to czy zgodnie z tą instrukcją zdołają Państwo przekazać administratorowi danych informacje o incydencie w ciągu 24 godzin od stwierdzenia naruszenia?		
19	Czy w celu zaplanowania środków bezpieczeństwa przeprowadzono analizę ryzyka?		
20	Czy wdrożyli Państwo system zarządzania bezpieczeństwem informacji np. ISO 27001?		
21	Czy do przetwarzania danych w Państwa pomieszczeniach, stosuje się fizyczne zabezpieczenia przed dostępem osób nieuprawnionych? Proszę krótko opisać jakie np. system kontroli dostępu, drzwi zamykane na klucz, system alarmowy, ochrona fizyczna, monitoring wizyjny.		
22	Czy przetwarzanie danych było już przedmiotem zewnętrznych audytów lub kontroli, np. PUODO w Państwa organizacji?		
23	Jeśli tak, proszę zwięźle opisać wyniki kontroli/ audytów		
24	Czy posiadają Państwo wdrożoną instrukcję zarządzania systemami IT służącymi do przetwarzania danych osobowych lub inne dokumenty wewnętrzne regulujące zasady zarządzania infrastrukturą IT?		
25	Czy Państwa systemy IT zapewniają rozliczalność operacji wykonywanych na danych osobowych, tzn. czy istnieje odnotowują nazwę użytkownika, datę oraz charakter operacji wykonanej na konkretnym rekordzie w bazie?		
26	Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane?		
27	Czy stosują Państwo pseudonimizację i szyfrowanie danych?		
28	Czy podjęli Państwo środki, aby zapewnić zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania?		
29	Czy w Państwa organizacji są stosowane środki służące ochronie systemów IT przed działaniem tzw. złośliwego oprogramowania?		
30	Jeśli tak, to czy podlegają one cyklicznej aktualizacji?		
31	Czy podjęli Państwo środki, aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? Np. regularny backup		
32	Czy dostęp do systemów IT wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		
33	Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?		