

ANKIETA
weryfikacyjna podmiotu przetwarzającego

Podmiot powierzający	Nazwa		
	Adres		
	NIP		
	REGON		
	KRS		
Podmiot przetwarzający	Nazwa		
	Adres		
	NIP		
	REGON		
	KRS		
Data			
Imię i nazwisko osoby udzielającej odpowiedzi			
Lp.	Pytanie	Odpowiedź (najlepiej tak/nie)	Uwaga lub uzasadnienie do odpowiedzi
1. Organizacja			
1.1.	Czy podmiot przetwarzający ma doświadczenie lub wiedzę w zakresie świadczenia usług związanych z przetwarzaniem danych osobowych? Jeśli tak, proszę o opis doświadczenia lub przedstawienie dokumentów potwierdzających posiadaną wiedzę.		
1.2.	Czy podmiot przetwarzający musi wyznaczyć IOD?		
1.3.	Czy podmiot przetwarzający wyznaczył IOD?		
1.4.	Czy IOD posiada odpowiedni poziom wiedzy i doświadczenia?		
1.5.	Czy podmiot przetwarzający ma dział compliance/security?		
1.6.	Czy w przypadku braku wyznaczenia IOD podmiot przetwarzający ma specjalistę z zakresu ochrony danych?		
1.7.	Czy specjalista z zakresu ochrony danych ma odpowiedni poziom wiedzy i doświadczenia?		
1.8.	Czy IOD lub specjalista z zakresu ochrony danych ma odpowiednio wsparcie prawne lub techniczne w zależności od potrzeb?		
1.9.	Czy podmiot przetwarzający gwarantuje, że IOD ma zasoby niezbędne do wykonania zadań, a także zasoby niezbędne do utrzymania jego wiedzy fachowej?		
1.10.	Czy członkowie personelu zostali przeszkoleni i zapoznani z przepisami o ochronie danych osobowych? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia.		
1.11.	Czy członkowie personelu zostali przeszkoleni w zakresie obsługi, w tym bezpiecznego korzystania z systemów i urządzeń informatycznych? Czy jest to		

	udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia.		
1.12.	Czy członkowie personelu zostali przeszkoleni w zakresie zasad bezpieczeństwa informacji, w szczególności ochrony danych osobowych? Czy jest to udokumentowane? Jeśli tak, proszę wskazać termin ostatniego szkolenia.		
1.13.	Czy podmiot przetwarzający przystąpił i stosuje kodeks postępowania dla swojej branży? Jeśli nie, proszę uzasadnić.		
1.14.	Czy podmiot przetwarzający jest objęty monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?		
1.15.	Czy podmiot przetwarzający ma certyfikat zgodności z RODO zgodnie z przepisami rozporządzenia? Jeśli tak, proszę wskazać wystawcę certyfikatu oraz datę uzyskania.		
1.16.	Czy podmiot przetwarzający zamierza korzystać lub korzysta z usług dalszych podmiotów przetwarzających? Jeśli tak, proszę wskazać, w jakim zakresie oraz udzielić informacji, czy dokonał weryfikacji takich podmiotów.		
2. Zabezpieczenia			
2.1.	Czy podmiot przetwarzający prowadzi regularne audyty bezpieczeństwa, w szczególności ochrony danych osobowych? Jeśli tak, proszę wskazać datę ostatniego audytu.		
2.2.	Czy podmiot przetwarzający posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzania bezpieczeństwem informacji? Jeśli tak, proszę wskazać jakie.		
2.3.	Czy, a jeśli tak, to z jakich urządzeń informatycznych (hardware) korzysta podmiot przetwarzający przy przetwarzaniu powierzonych danych? Czy takie urządzenia są zabezpieczone adekwatnie do ryzyka?		
2.4.	W jakich lokalizacjach podmiot przetwarzający przetwarza powierzone dane osobowe? Czy te lokalizacje są zabezpieczone adekwatnie do ryzyka?		
2.5.	Czy podmiot przetwarzający korzysta z rozwiązań chmury obliczeniowej? Jeśli tak, proszę podać, jakiego rodzaju (prywatna/publiczna/hybrydowa) i od jakich dostawców.		
2.6.	Czy podmiot przetwarzający korzysta z systemów informatycznych (software) opartych na modelu rozwiązań chmury obliczeniowej (SAS)? Jeśli tak, proszę podać, jakiego rodzaju jest to oprogramowanie.		
2.7.	Czy podmiot przetwarzający będzie przetwarzał powierzone dane osobowe w formie papierowej? Jeśli tak, to czy te dokumenty będą zabezpieczone adekwatnie do ryzyka?		
2.8.	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem?		
3. Incydenty, postępowania organu, decyzje itp.			
3.1.	Czy u podmiotu przetwarzającego doszło w ciągu ostatnich 12 miesięcy do incydentów bezpieczeństwa? Jeśli tak, to		

	jakiej kategorii i jak często (np. zgubienie pendrive'a bez danych osobowych raz w roku albo włamanie bez kradzieży danych dwa razy w roku)?		
3.2.	Czy u podmiotu przetwarzającego doszło w ciągu ostatnich 12 miesięcy do naruszeń ochrony danych osobowych? Jeśli tak, to jakiej kategorii były to naruszenia, w tym, czy podlegały zgłoszeniu do organu nadzorczego (np. zgubienie niezaszyfrowanego laptopa z danymi osobowymi, dwa razy w zeszłym roku, podlegało zgłoszeniu)?		
3.3.	Jeśli na pytanie 3.2. odpowiedź brzmiała „tak”, to jakie zostały podjęte kroki w celu zaradzenia naruszeniu, w tym przeciwdziałania podobnym naruszeniom w przyszłości?		
3.4.	Czy wobec podmiotu przetwarzającego prowadzona była kontrola Prezesa Urzędu Ochrony Danych Osobowych? Jeśli tak, to kiedy i jaki był jej wynik?		
3.5.	Czy wobec podmiotu przetwarzającego było prowadzone postępowanie Prezesa Urzędu Ochrony Danych Osobowych na skutek skargi podmiotu danych? Jeśli tak, to kiedy postępowanie było prowadzone, co było przedmiotem skargi i jaki był wynik postępowania?		
3.6.	Czy podmiot przetwarzający występuje w jakiegokolwiek sprawie sądowej lub sądowno-administracyjnej dot. ochrony danych osobowych? Jeśli tak, to w jakim charakterze, czego dotyczy sprawa oraz jakie jest rozstrzygnięcie?		
4. Przetwarzanie transgraniczne poza EOG			
4.1.	Czy podmiot przetwarzający lub dalszy podmiot przetwarzający, z którego usług korzysta podmiot przetwarzający, przetwarza dane osobowe poza EOG?		
4.2.	Jeśli tak, to w jakim kraju?		
4.3.	Jeśli tak, to na jakiej podstawie dane osobowe są transferowane poza EOG?		
4.4.	Jeśli tak, to w jakim celu?		
4.5.	Jeśli tak, to czy jest to związane z rozwiązaniami technicznymi, np. korzystanie z serwerów?		
4.6.	Jeśli powierzone dane są przetwarzane na terenie krajów, co do których może zostać utracone prawo do transferu danych, to czy podmiot przetwarzający posiada odpowiednią procedurę w celu legalizacji takiego przetwarzania?		
5. Polityki i procedury			
5.1.	Czy podmiot przetwarzający posiada politykę ochrony danych osobowych lub podobną? Jeśli tak, proszę przedstawić potwierdzenie przyjęcia takiej polityki i jej wdrożenia.		
5.2.	Czy podmiot przetwarzający posiada procedury realizacji praw osób, których dane dotyczą oraz spełniania obowiązku informacyjnego? Jeśli tak, proszę przedstawić potwierdzenie przyjęcia takich procedur i ich wdrożenia.		
5.3.	Czy podmiot przetwarzający posiada procedurę postępowania w sprawie naruszenia? Jeśli tak, proszę przedstawić potwierdzenie przyjęcia takiej procedury i jej wdrożenia.		

5.4.	Czy podmiot przetwarzający nadaje upoważnienia do przetwarzania danych osobowych personelowi?		
5.5.	Czy podmiot przetwarzający prowadzi rejestr nadanych upoważnień?		
5.6.	Czy podmiot przetwarzający zobowiązuje personel do zachowania w tajemnicy wszelkich danych osobowych?		
5.7.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania?		
5.8.	Czy podmiot przetwarzający przeprowadził analizę ryzyka?		
5.9.	Czy podmiot przetwarzający korzysta z narzędzia wspomagającego zarządzanie bezpieczeństwem danych osobowych? Jeśli tak, to z jakiego?		