

Ankieta oceny podmiotu przetwarzającego dane osobowe

.....
(nazwa firmy)

.....
(adres)

Lp.	PYTANIE	TAK/NIE	WYMÓG
WIEDZA FACHOWA			
1.	Czy podmiot przetwarzający posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie?		
2.	Czy dany podmiot przetwarzający wyznaczył inspektora ochrony danych?		Art.37 RODO
3.	Czy podmiot przetwarzający wyznaczył inspektora ochrony danych, mimo że nie wymagają tego przepisy prawa lub też inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji?		
4.	Czy osoby po stronie podmiotu przetwarzającego delegowane do obsługi ZDiZ w Gdyni zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?		
5.	Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez podmiot przetwarzający?		
WIARYGODNOŚĆ			
6.	Czy podmiot przetwarzający posiada referencje od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, to prosimy o przedstawienie takich referencji.		
7.	Czy stwierdzono prawomocną decyzją UODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?		
8.	Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania?		Art. 40 RODO
9.	Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?		Art. 41 RODO
10.	Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO?		Art. 42 RODO
ZASOBY			
11.	Czy podmiot przetwarzający opracował i wdrożył Politykę ochrony danych osobowych?		Art. 24 RODO
12.	Czy podmiot przetwarzający wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?		
13.	Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?		
14.	Czy podmiot przetwarzający prowadzi rejestry czynności /rejestr kategorii czynności przetwarzania danych osobowych (jako ADO oraz jako procesor)?		art. 30 RODO
15.	Czy podmiot przetwarzający wdrożył zasady zarządzania bezpieczeństwem informacji, w tym:		

	a) system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat?		
	b) zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?		
	c) <i>[dla podmiotów publicznych]</i> zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności?		
	Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.?		
16.	Czy podmiot przetwarzający dobiera zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - Privacy Impact Assessment)?		Odniesienie do Art. 24, 25, 32 RODO
17.	Czy podmiot przetwarzający okresowo przeprowadza działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?		
18.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub dokument, w którym opisano cele stosowania zabezpieczeń oraz zabezpieczenia, które odnoszą się do ochrony danych osobowych?		
19.	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:		Art. 32 ust. 1 lit a)-c) RODO
	a) pseudonimizację i szyfrowanie danych,		
	b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,		
	c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.		
20.	Czy podmiot przetwarzający prowadzi 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?		Art. 32 ust. 1 lit d) RODO
21.	Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?		
22.	Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez ZDiZ w Gdyni lub audytora upoważnionego przez ZDiZ w Gdyni?		
23.	Czy osoby delegowane do obsługi ZDiZ w Gdyni posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane?		
24.	Czy osoby upoważnione do przetwarzania danych w ramach obsługi ZDiZ w Gdyni zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?		

.....
(data, pieczęć, podpis osoby wypełniającej ankietę)