

### LISTA WERYFIKACYJNA PODMIOTU PRZETWARZAJĄCEGO (PP)

Lista weryfikacyjna służy jako pomocne narzędzie przy przeprowadzania audytów, w tym inspekcji przez administratora, w ramach wykonywania swoich uprawnień określonych w art. 28 ust. 3 lit. h) RODO.

Lp.	OBSZAR	PYTANIE	ODPOWIEDŹ
1.	WERYFIKACJA OGÓLNA	Czy PP wyznaczył inspektora ochrony danych? Czy PP monitoruje obowiązek wyznaczenia IOD w organizacji?	
2.	WERYFIKACJA OGÓLNA	Kto wykonuje <b>zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych w organizacji</b> (w sytuacji braku powołania inspektora ochrony danych)?	
3.	WERYFIKACJA OGÓLNA	Czy PP miał kontrolę, postępowanie wyjaśniające lub inne działania prowadzone przez Prezesa UODO lub inny organ nadzorczy w związku z PP? <b>Jeżeli tak, prosimy o wskazanie co było przedmiotem działań prowadzonych przez Prezesa UODO i jakie są wyniki przeprowadzonych działań?</b>	
4.	WERYFIKACJA OGÓLNA	Czy PP stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania? Oczywiście o ile taki kodeks występuje w danej branży. Brak stosowania kodeksu nie wpływa samoistnie na negatywną ocenę PP.	
5.	WERYFIKACJA OGÓLNA	Czy PP objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący? Oczywiście o ile taki kodeks występuje w danej branży. Brak stosowania kodeksu nie wpływa samoistnie na negatywną ocenę PP.	
6.	WERYFIKACJA OGÓLNA	Czy PP otrzymał <b>certyfikat zgodności z RODO</b> ? Brak posiadania certyfikatu nie wpływa samoistnie na negatywną ocenę PP.	
7.	ZASOBY/ ZARZĄDZANIE PERSONELEM	Czy osoby wyznaczone do wykonywania zadań z zakresu PP <b>posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z zakresu przetwarzania powierzonych danych?</b> Prosimy uzasadnić odpowiedź [np. fakt odbycia szkolenia, posiadane certyfikaty, doświadczenie]	
8.	ZASOBY/ ZARZĄDZANIE PERSONELEM	Czy osoby delegowane do obsługi danych powierzonych przez administratora posiadają nadane upoważnienia do przetwarzania danych?	

Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych

9.	ZASOBY/ ZARZĄDZANIE PERSONELEM	Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania danych osobowych w tajemnicy?	
10	WERYFIKACJA PROCEDUR	Jak wygląda procedura realizacji praw osób, których dane dotyczą, uwzględniającą wspieranie administratora w realizacji tych praw? <b>[można załączyć wyciąg z odpowiedniej procedury]</b>	
11	ZARZĄDZANIE DOSTĘPEM	Czy PP zarządza dostępem do systemów oraz programów komputerowych, w którym są przetwarzane dane osobowe, poprzez proces nadawania, przeglądu i odbierania uprawnień oraz stosuje bezpieczne mechanizmy uwierzytelniania? <b>[można załączyć wyciąg z odpowiedniej procedury]</b>	
12	ZARZĄDZANIE DOSTĘPEM	Czy PP wdrożył i stosuje zasady <b>udzielania dostępu tylko do informacji niezbędnych do zakresu wykonywanych obowiązków</b> oraz zasady najmniejszego uprzywilejowania? W myśl zasady najmniejszego uprzywilejowania użytkownik ma mieć dostęp tylko do tych informacji i zasobów, które są mu niezbędne do wykonywania swojej pracy.	
13	ANALIZA RYZYKA	Czy PP dobrał odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych osobowych zgodnie z aktualnie przeprowadzoną analizą ryzyka naruszenia praw lub wolności osób fizycznych? <b>[można załączyć wyciąg z odpowiedniej procedury]</b>	
14	ŚRODKI BEZPIECZEŃSTWA	Jakie środki bezpieczeństwa stosuje PP w celu zapewnienia ochrony danych osobowych w czasie ich przechowywania? <b>[można załączyć wyciąg z odpowiedniej procedury]</b>	
15	KOPIA BEZPIECZEŃSTWA	Czy PP przechowuje kopie bezpieczeństwa w bezpiecznej lokalizacji oraz zabezpiecza kopie przed ich nieuprawnionym dostępem? <b>[można załączyć wyciąg z odpowiedniej procedury]</b>	
16	ZEWNĘTRZNE AUDYTY PP	Czy PP 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? <b>[można załączyć wyciąg z odpowiedniej procedury]</b>	

Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych

17	BEZPIECZEŃSTWO FIZYCZNE	Czy PP zapewnia nadzór - wykluczający dostęp do danych osobowych - przed osobami niebędącymi pracownikami PP, a przebywającymi w jego siedzibie?	
18	ZARZĄDZANIE INCYDENTAMI	Jak wygląda procedura postępowania w sytuacji naruszenia ochrony danych osobowych przetwarzanych w imieniu administratora? Prosimy o wskazanie odpowiedniej procedury/ fragmentów procedury.	
19	ZARZĄDZANIE INCYDENTAMI	Proszę wskazać kto u PP jest odpowiedzialny za kontakt i wykonywanie procedury postępowania w sytuacji naruszenia ochrony danych? <b>Prosimy o wskazanie odpowiedniego wyciągu z procedury.</b>	
20	ZARZĄDZANIE INCYDENTAMI	Czy PP prowadzi i aktualizuje ewidencję naruszeń ochrony danych osobowych?	