

KWESTIONARIUSZ SPRAWDZAJĄCY DLA PODMIOTU PRZETWARZAJĄCEGO

L.P.	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? Prosimy o udokumentowanie świadczenia przedmiotowych usług.		
2.	Czy przepisy RODO wymagają, aby dany podmiot przetwarzający wyznaczył Inspektora ochrony danych?		art. 37 RODO
3.	Czy podmiot przetwarzający wyznaczył Inspektora ochrony danych?		art. 37 RODO
4.	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?		
5.	Czy osoby po stronie podmiotu przetwarzającego dedykowane do obsługi spółki <i>PGE Energetyka Kolejowa S.A.</i> zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?		
6.	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?		
7.	Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie zasad bezpieczeństwa informacji?		
WIARYGODNOŚĆ			
8.	Czy podmiot przetwarzający posiada referencje od innych podmiotów, które obsługuje/obsługiwał w zakresie Przetwarzania danych osobowych na ich zlecenie? <i>[Jeśli tak, to prosimy o przedstawienie takich referencji].</i>		
9.	Czy stwierdzono prawomocną decyzją GIODO/PUODO lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?		
10.	Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania?		art. 40 RODO
11.	Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?		art. 41 RODO
12.	Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO?		art. 42 RODO
13.	Kryterium wewnętrzne do oceny przez spółkę <i>PGE Energetyka Kolejowa S.A.</i> : Czy rozważany podmiot jest znany na rynku jako podmiot wykonujący danego rodzaju usługi? Jeżeli tak, jaką ma renomę? Jakie są opinie o tym podmiocie, o współpracy z tym podmiotem,		

	o stosowanych przez niego zabezpieczeniach czy przetwarzaniu danych?		
14.	Kryterium wewnętrzne do oceny przez <i>spółkę PGE Energetyka Kolejowa S.A.</i> Czy jakakolwiek spółka GK PGE w przeszłości współpracowała z rozważanym podmiotem? Jeżeli tak, jakie są doświadczenia współpracy z tym podmiotem i opinie o nim?		
ZASOBY			
1.	Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych osobowych lub podobną procedurę? <i>[Jeśli tak, prosimy o jej przedstawienie].</i>		art. 24 RODO
2.	Czy podmiot przetwarzających wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?		art. 33 i 34 RODO
3.	Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?		art. 33 RODO
4.	Czy podmiot przetwarzający prowadzi Rejestry Czynności przetwarzania danych osobowych (jako Administrator Danych Osobowych oraz jako procesor)?		art. 30 RODO
5.	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?		
	Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp.?		
6.	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, 35 RODO
7.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem?		
8.	Czy podmiot przetwarzający okresowo przeprowadza kolejne 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?		
9.	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.		

10.	Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych osobowych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?		art. 32 ust. 1 lit. d RODO
11.	Czy wnioski z audytów zostały udokumentowane, np. w raporcie poaudytowym?		
12.	Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez spółkę PGE Energetyka Kolejowa S.A. lub audytora upoważnionego przez spółkę PGE Energetyka Kolejowa S.A.?		art. 28 ust. 3 lit. h RODO
13.	Czy osoby delegowane do obsługi spółki PGE Energetyka Kolejowa S.A. posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane?		art. 29 oraz art. 32 ust. 4 RODO
14.	Czy osoby upoważnione do przetwarzania danych w ramach obsługi spółki PGE Energetyka Kolejowa S.A. zostały zobowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?		Art. 28 ust. 3 lit. b RODO
15.	Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w Przetwarzaniu danych osobowych do ich przetwarzania?		art. 29 oraz art. 32 ust. 4 RODO

Podpis Administratora danych podmiotu przetwarzającego lub uprawnionej osoby