Załącznik 4b do Procedury korzystania z usług podmiotów przetwarzających dane

„Wzór”

Ankieta bezpieczeństwa dla podmiotu przetwarzającego

……..……/*wskazać nazwę*

PROCEDURA WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE W PRZEDSIĘBIORSTWIE BUDOWY KOPALŃ PEBEKA S.A.

<u>Uwaga wewnętrzna:</u> Najbardziej istotne pytania zostały zaznaczone na żółto – powinny one być zadane wszystkim podmiotom przetwarzającym.

L.P.	PYTANIE	TAK/NIE	UWAGI
I.	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 podmiot przetwarzający powołał inspektora ochrony danych (IOD) ?		
	Jeśli tak, to: 1/ czy zgłoszenie powołania IOD zostało przesłane do rejestracji ?		
3.	W sytuacji braku powołania IOD - Czy zadania z dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych w organizacji pełnią inne osoby ?		
	Czy wyznaczone osoby do wykonywania w/w zadań posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z tego zakresu?		
4.	Czy przepisy prawa wymagają, aby dany podmiot przetwarzający wyznaczył inspektora ochrony danych ? *art. 37 RODO		
5.	Czy osoby po stronie podmiotu przetwarzającego dedykowane do obsługi administratora danych 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?		
II.	WIARYGODNOŚĆ		
8.	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.		
9.	Czy stwierdzono prawomocną decyzją PUODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający ?		
10.	Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów podstępowania ? *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		
III.	ZASOBY		
1.	Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? *art. 24 RODO		

2.	Czy podmiot przetwarzający wdrożył instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych ?		
3.	Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych ?		
4.	Czy podmiot przetwarzający prowadzi wykaz lub/i rejestr przetwarzanych zbiorów danych osobowych?		
5.	Czy podmiot przetwarzający prowadzi rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako procesor) ? *art. 30 RODO Jeżeli nie, prosimy o wskazanie powodów.		
6.	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) [dla podmiotów publicznych] zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności ?		
	d) [dla podmiotów podlegających pod Komisję Nadzoru Finansowego] zasady zarządzania bezpieczeństwem informacji zgodne z odpowiednimi wytycznymi KNF ?		
	Czy podmiot wdrożył inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji, itp. ?		
7.	Czy podmiot przetwarzający dobrał 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 ? *Odniesienie do Art. 24, 25, 32 RODO		
8.	Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania ?		

9.	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?		
10.	Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem (*art. 32 ust. 1 lit. a)-c) RODO), w tym:		
	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.		
11.	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		
12.	Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym ?		
13.	Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych ?		
14.	Czy osoby delegowane do obsługi administratora posiadają nadane upoważnienia do przetwarzania danych ? Czy zostało to udokumentowane ? Prosimy o przedłożenie listy osób upoważnionych, które będą obsługiwać administratora ?		

15.	Czy osoby upoważnione do przetwarzania danych w ramach obsługi administratora zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane ?		
16.	Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania?		

IV. KRYTERIA/PYTANIA WEWNĘTRZNE (Poniższe pytania należy zadać osobom wewnątrz organizacji administratora lub wewnątrz grupy kapitałowej administratora) ***Poniższe odpowiedzi wskazuje komórka przygotowująca umowę powierzenia***		ODPOWIEDŹ
1.	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?	
2.	Czy Spółka (administrator) lub inna Spółka z grupy kapitałowej w przeszłości współpracowała z rozważanym podmiotem? Jeżeli tak, jakie są doświadczenia współpracy z tym podmiotem i opinie o nim?	

……
Podmiot Przetwarzający - procesor

……..
/Rekomendacja IOD administratora danych/