Załącznik nr 2 do Umowy:

Przykładowy zakres informacji o zapewnieniu przez Wykonawcę odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych art. 24 ust. 1 i 2 oraz art. 32 RODO

Formularz dla podmiotu przetwarzającego dane osobowe w ramach czynności przetwarzania w związku z realizacją Instrumentu „Łącząc Europę" (CEF) w sektorze transportu, na temat posiadanych środków ochrony			
Instrukcja wypełniania formularza: 1) Podmiot, wobec którego planowane jest powierzenie przetwarzania danych osobowych / któremu powierzono przetwarzanie danych osobowych w ramach ww. czynności, wypełnia kolumny pn. *Odpowiedź* oraz *Uwagi*. 2) W przypadku wypełniania przez podmiot formularza po powierzeniu mu przetwarzania danych osobowych, treść niektórych pytań, odpowiadających tej sytuacji, zawarto w przypisie. 3) W części pn. *Ocena zgodności i rekomendacje* administrator danych osobowych może zgłosić podmiotowi, któremu planuje powierzyć przetwarzanie danych osobowych / któremu powierzył przetwarzanie danych osobowych, pewne zalecenia i rekomendacje (bez oficjalnie wiążącego ich charakteru), mające na celu poprawę stopnia bezpieczeństwa przetwarzanych danych poprzez modyfikację stosowanych środków technicznych i organizacyjnych.			
lp.	**PYTANIE**	**ODPOWIEDŹ** (tak / nie / nie dotyczy)	**UWAGI** (dodatkowe informacje)
KWESTIE OGÓLNE			
1.	Czy podmiot przetwarzający powołał w swojej jednostce Inspektora Ochrony danych (IOD) lub inną osobę do wykonywania zadań związanych z ochroną danych osobowych?		
2.	Czy podmiotowi, do zrealizowania umowy, która zostanie / została zawarta z administratorem, niezbędne jest przetwarzanie danych osobowych? Należy wskazać w uwagach kategorie danych, których przetwarzanie jest niezbędne		

	do zrealizowania umowy, która zostanie / została zawarta z administratorem/podmiotem przetwarzającym[1].		
3.	Czy podmiot posiada doświadczenie w pełnieniu roli podmiotu, któremu powierzono przetwarzanie danych osobowych?		
4.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO[2]?		
PROCEDURY			
5.	Czy podmiot przetwarzający posiada procedury w obszarze ochrony danych osobowych? Czy te procedury uwzględniają - oprócz zadań administratora - również zadania wynikające z pełnienia roli podmiotu przetwarzającego, o których mowa w art. 28 RODO?		
6.	Czy podmiot przetwarzający stosuje w swojej działalności zasady *privacy by design* oraz *privacy by default*?		
7.	Czy zastosowano środki kontroli dostępu fizycznego w stosunku do budynku lub budynków podmiotu przetwarzającego, gdzie realizowana będzie umowa z administratorem?		

[1] Ten punkt ma charakter informacyjny, zakres danych powierzonych do przetwarzania określa finalnie Administrator (jeśli zakres będzie inny niż wskazany przez podmiot przetwarzający – odpowiednia adnotacja zostanie zamieszczona w zaleceniach i rekomendacjach ze strony administratora). W przypadku wypełniania formularza przed podpisaniem umowy powierzenia, zakres danych planowanych do powierzenia powinien być ograniczony do takich danych, które są niezbędne do zrealizowania celu zawieranej umowy . W przypadku wypełniania formularza po zawarciu umowy powierzenia, należy wziąć pod uwagę zakres danych powierzonych do przetwarzania - w uwagach można wskazać, że przetwarzany będzie jedynie ten zakres danych.

[2] W przypadku wypełniania formularza już po powierzeniu przetwarzania danych osobowych, przedmiotowe pytanie brzmi następująco:

Czy w związku z przetwarzaniem danych osobowych w ramach czynności przetwarzania w związku z realizacją Instrumentu „Łącząc Europę" (CEF) w sektorze transportu, podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zgodnie z art. 30 ust. 2 RODO?

8.	Czy podmiot przetwarzający stosuje odpowiednie zabezpieczenia w systemach informatycznych, w których będą przetwarzane dane osobowe w ramach czynności przetwarzania w związku z realizacją Instrumentu „Łącząc Europę" (CEF) w sektorze transportu? W uwagach należy wskazać, jakie zabezpieczenia są stosowane, lub odwołać się do dokumentów regulujących tę kwestię.		
9.	Czy systemy informatyczne podmiotu przetwarzającego wymuszają okresową zmianę haseł?		
10.	Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na komputerach używanych przez jednostkę?		
11.	Czy oprogramowanie, używane w podmiocie przetwarzającym, posiada licencję i jest na bieżąco aktualizowane?		
12.	Czy dyski komputerów przenośnych używane przez podmiot przetwarzający są szyfrowane?		
13.	W jaki sposób są zabezpieczone urządzenia mobilne, używane w podmiocie przetwarzającym? Czy są one zabezpieczone co najmniej hasłem?		
PRACOWNICY			
14.	Czy podmiot przetwarzający zapewnia nowozatrudnionym pracownikom - przed podjęciem przez nich czynności związanych z przetwarzaniem danych osobowych - szkolenie w tym obszarze, w szczególności w zakresie obowiązujących w jednostce procedur wewnętrznych?		
15.	Czy do przetwarzania danych osobowych podmiot przetwarzający dopuszcza jedynie osoby, które otrzymały upoważnienia do dokonywania tej czynności?		

16.	Czy podmiot przetwarzający zobowiązuje pracowników do stosowania obowiązujących w jego jednostce procedur w obszarze ochrony danych osobowych i weryfikuje ich stosowanie? Należy wskazać w uwagach, w jaki sposób potwierdzane jest to zobowiązanie, oraz jak odbywa się weryfikacja jego realizacji.		
17.	Czy pracownicy podmiotu przetwarzającego, którzy przetwarzają dane osobowe, zostali zobowiązani do zachowania ich w tajemnicy / w poufności?		
18.	Czy podmiot przetwarzający weryfikuje, czy pracownicy podmiotu przetwarzającego nie pozostawiają w miejscach ogólnodostępnych wydruków lub dokumentów zawierających dane osobowe? Należy wskazać w uwagach, w jaki sposób odbywa się weryfikacja jego realizacji.		
19.	Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do stosowania zasady tzw. „czystego biurka”? Czy i w jaki sposób podmiot przetwarzający weryfikuje jej stosowanie w praktyce?		
20.	Czy pracownicy przetwarzający dane osobowe w formie papierowej - po zakończeniu pracy - przechowują je w zamykanych szafach i zabezpieczają je przed dostępem do nich nieuprawnionych osób?		
INNE			
21	Czy podmiot przetwarzający prowadzi rejestr naruszeń ochrony danych osobowych?		
22	Czy podmiot przetwarzający posiada wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych?		
23.	Czy w przypadku incydentu w zakresie danych osobowych zapewniono możliwość szybkiego przywrócenia danych i dostępu do nich?		

24.	Czy podmiot przetwarzający dokonał oszacowania ryzyka przetwarzania danych osobowych i czy w jego wyniku konieczne okazało się sporządzenie oceny skutków dla ochrony danych (DPIA)?		
25.	Czy i w jaki sposób podmiot przetwarzający zapewnia realizację praw osób, których dane dotyczą? Czy posiada w tym zakresie ustalone procedury postępowania?		
26	Czy podmiot przetwarzający posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzenia bezpieczeństwa informacji?		
27	Czy podmiot przetwarzający planuje dokonywać transferów powierzonych do przetwarzania danych do państw poza EOG??[3]		
OCENA ZGODNOŚCI Z RODO PRZEDSTAWIONYCH PRZEZ PODMIOT PRZETWARZAJACY INFORMACJI **ORAZ EWENTUALNE ZALECENIA I REKOMENDACJE ZE STRONY ADMINISTRATORA**			

Jeżeli zastosowane zostały dodatkowo inne środki niewymienione w udostępnionych listach, należy je wyszczególnić poniżej:

……

…

ZAMAWIAJĄCY

……

WYKONAWCA

……

[3] Założeniem Administratora jest nie dokonywanie transferów danych powierzonych do przetwarzania do państw poza EOG. Jeżeli taki transfer miałby następować – należy wskazać mechanizm legalizujący taki transfer.

……

……