Załącznik nr ….....

do ….....

Motyw 81 RODO:

Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje - w szczególności jeżeli chodzi ***o wiedzę fachową, wiarygodność i zasoby*** *- wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Administrator i podmiot przetwarzający mogą postanowić skorzystać z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez Komisję albo które zostały przyjęte przez organ nadzorczy zgodnie z mechanizmem spójności, a następnie przyjęte przez Komisję. Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien - zgodnie z decyzją administratora - zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych.*

WIEDZA FACHOWA	
1. Czy podmiot przetwarzający ma obowiązek powołać Inspektora Ochrony Danych? [1] 2. Jeżeli tak, czy podmiot przetwarzający wyznaczył i zgłosił do UODO Inspektora Ochrony Danych?	Jeżeli tak, prosimy o podanie danych kontaktowych (imię i nazwisko IOD, adres e-mail. ew. nr telefonu).
3. Czy podmiot przetwarzający zapoznał pracowników/współpracowników z zasadami przetwarzania danych?	
4. Czy podmiot przetwarzający dysponuje odpowiednią wiedzą fachową w zakresie ochrony danych osobowych?	
5. Czy podmiot przetwarzający dysponuje wiedzą i zasobami umożliwiającymi pomoc administratorowi w realizacji praw podmiotów danych (np. wsparcie w przypadku żądania kopii danych, usunięcia danych, poprawienia danych)?	Czy podmiot przetwarzający ma zasoby, aby bez przerw realizować usługi (zapewnienie ciągłości działania)?
6. Czy podmiot przetwarzający ma świadomość treści wymogów RODO i zakresu odpowiedzialności podmiotu przetwarzającego?	
7. Czy podmiot przetwarzający ma świadomość obowiązków związanych z nadzorowaniem komu nadaje się dostępy do danych osobowych (pracownicy, współpracownicy, podwykonawcy, dostawcy zewnętrzni IT)?	
WIARYGODNOŚĆ	
8. Czy u podmiotu przetwarzającego w ciągu ostatnich dwóch lat prowadzona była kontrola Prezesa Urzędu Ochrony Danych Osobowych? *Jeżeli tak to jakie były skutki kontroli – czy wydano decyzję nakładającą administracyjną karę pieniężną lub upomnienie w związku z naruszeniem przepisów?*	

[1]*) Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:*
a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

9. Czy pracownicy/współpracownicy mają świadomość, czym jest naruszenie ochrony danych w rozumieniu RODO (incydent bezpieczeństwa) i jak należy postępować w przypadku wystąpienia naruszenia (incydent bezpieczeństwa)?	
10. Czy podmiot przetwarzający jest w stanie likwidacji/upadłości?	
11. Czy podmiot przetwarzający odpowiednio zabezpieczył zasoby (np. komputery przenośne), z których będzie korzystał w toku realizacji umowy powierzenia ?	
12. Czy przetwarzanie będzie odbywać się na terenie UE?	
13. Czy pracownicy/współpracownicy zobowiążą się do zachowania poufności (obowiązek powinien trwać przez okres umowy powierzenia i po jej zakończeniu, tj. bezterminowo z wyłączeniem możliwości wypowiedzenia tego oświadczenia)?	
ZASOBY	
14. Czy podmiot przetwarzający odbiera dostępy do systemów służących przetwarzaniu danych najpóźniej w ostatnim dniu obowiązywania umowy o pracę/współpracę[2]?	
15. Czy podmiot przetwarzający wdrożył bezpieczne metody uwierzytelniania do systemów służących przetwarzaniu danych (np. hasło/wieloskładnikowa autoryzacja)?	
16. Czy podmiot przetwarzający wdrożył i zakomunikował swoim pracownikom jasne zasady bezpiecznego użytkowania systemów informatycznych[3]?	
17. Czy w pomieszczeniach, w których odbywa się przetwarzanie (niezależnie czy chodzi o pracę zdalną czy nie), wdrożono odpowiednie zabezpieczenia danych (np. kontrola tego, kto ma dostęp do urządzeń służących przetwarzaniu danych)?	
18. Czy podmiot przetwarzający dysponuje narzędziami IT służącymi przetwarzaniu danych, które umożliwiają usuwanie danych/zwrot po zakończeniu umowy powierzenia?	
19. Czy podmiot przetwarzający dba o aktualizowanie systemów IT?	
20. Czy podmiot przetwarzający dysponuje urządzeniami umożliwiającymi bezpieczne przechowywanie danych tradycyjnych (chodzi o przechowywanie danych na nośnikach tradycyjnych)?	

.....

Podpis i pieczęć osoby upoważnionej

[2]) *Art. 28 ust. 3 lit b) (...) Podmiot przetwarzający "zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy"*

[3]) *Przykład zasad: https://techinfo.uodo.gov.pl/709-2/ ale również ISO 27001 zawiera takie zasady czy ENISA https://www.enisa.europa.eu/risk-level-tool/methodology*