UMOWA PODPOWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ……. w Warszawie pomiędzy:

Fundacją WWF Polska, z siedzibą przy ul. Usypiskowej 11, 02-386 Warszawa, wpisaną do Rejestru Stowarzyszeń Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla miasta stołecznego Warszawy, XIII Wydział Gospodarczy pod numerem KRS: 0000160673, posiadającą NIP: 5213241055 oraz REGON: 015481019, reprezentowaną przez:

…….

zwaną dalej „**Procesorem**”

a

…….

zwanym dalej „**Podprocesorem**”,

dalej łącznie zwanymi „**Stronami**” lub pojedynczo „**Stroną**”.

§1

Definicje

Ilekroć w niniejszej umowie powierzenia przetwarzania danych osobowych mowa o:

1. **„Administratorze danych”** – Fundacja WWF Polska,
2. **„danych osobowych”** – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”),
3. **„przetwarzaniu danych”** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
4. **„systemie informatycznym”** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
5. **„Umowie”** – rozumie się przez to niniejszą umowę powierzenia przetwarzania danych osobowych,
6. **„Ustawie o ochronie danych osobowych”** – rozumie się przez to Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 z późn. zm.),
7. **„Ogólnym rozporządzeniu o ochronie danych” lub „RODO”** – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
8. **„organie nadzoru”** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych

§2

Przedmiot Umowy

1. Przedmiotem Umowy jest powierzenie Podprocesorowi przez Procesora, przetwarzania danych osobowych, w związku z realizacją Umowy nr ……. z dnia ……
2. Procesor oświadcza, że jest administratorem danych, o których mowa w §3 ust. 1 Umowy.
3. Procesor powierza Podprocesorowi przetwarzanie danych osobowych, a Podprocesor zobowiązuje się do ich przetwarzania zgodnego z prawem i Umową.
4. Podprocesor będzie przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie, przez okres nie dłuższy niż realizacja Umowy.

§3

Powierzenie przetwarzania danych osobowych

1. Procesor powierza Podprocesorowi przetwarzanie danych osobowych związanych z realizacją umowy wskazanej w §2 ust. 1. Strony oświadczają, że Procesor dokonał weryfikacji Podprocesora,

o której mowa w art. 28 ust. 1. Podprocesor oświadcza, że spełnia wymogi Procesora i RODO w zakresie przetwarzania danych osobowych i zapewnia odpowiedni poziom bezpieczeństwa przetwarzania danych osobowych (w Załączniku nr 2 wskazano zakres informacji o zapewnieniu przez podpowierzającego odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych art. 24 ust. 1 i 2 oraz art. 32 RODO.)

2. Zakres powierzonych do przetwarzania danych osobowych obejmuje następujące kategorie danych: imię i nazwisko, numer telefonu, adres zamieszkania, adres mailowy.
3. Rodzaj powierzonych danych nie obejmuje tzw. szczególnych kategorii danych oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych.
4. Celem powierzenia przetwarzania danych osobowych jest umożliwienie prawidłowej realizacji umowy, o której mowa w §2 ust. 1 Umowy, w szczególności wykonywanie zadań związanych z realizacją Programu Operacyjnego Infrastruktura i Środowisko 2014 – 2020 i umowy o dofinansowanie, której stroną jest Procesor i Administrator Danych.
5. Procesor, w zakresie realizacji celu określonego w ust. 4 powyżej, jest uprawniony do wykonywania następujących operacji na danych: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnienie, usuwanie, niszczenie.
6. Przetwarzanie powierzonych danych odbywać się będzie formie papierowej i przy wykorzystaniu systemów informatycznych.
7. Podprocesor jest zobowiązany do realizacji w imieniu i na rzecz Administratora obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO. Treść klauzuli informacyjnej stanowi załącznik nr 1 do umowy. Klauzula informacyjna będzie przekazywana przez Podporcesora najpóźniej w chwili pozyskania danych za pośrednictwem środków komunikacji na odległość, np. poprzez wysłanie e-maila zwrotnego, wskazania klauzuli na stronie internetowej, etc.

§4
Obowiązki Podprocesora

1. Podprocesor będzie przetwarzał powierzone mu dane osobowe na warunkach i zgodnie z treścią obowiązujących w tym zakresie przepisów prawa. W szczególności przetwarzanie powierzonych danych odbywało się będzie w zgodzie z postanowieniami: Ogólnego rozporządzenia o ochronie danych, Ustawy o ochronie danych osobowych oraz innych właściwych w zakresie przetwarzania danych osobowych przepisów prawa.
2. W związku z powierzeniem przetwarzania danych osobowych Podprocesor zobowiązuje się do:
    2.1. przetwarzania danych osobowych wyłącznie na podstawie Umowy lub innego udokumentowanego polecenia Procesora za jakie uważa się polecenie przekazane drogą pisemną lub elektroniczną,
    2.2. zapewnienia by osoby przetwarzające dane osobowe otrzymały pisemne upoważnienie i zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
    2.3. podjęcia wszelkich środków gwarantujących bezpieczeństwo powierzonych do przetwarzania danych osobowych, w tym m.in. do wdrożenia, przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, odpowiednich środków technicznych i organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu temu ryzyku, w tym między innymi w stosownym przypadku:
        2.3.1. pseudonimizacji i szyfrowania danych osobowych,
        2.3.2. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
        2.3.3. zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
        2.3.4. regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2.4. przestrzegania określonych w §6 Umowy warunków dalszego podpowierzenia przetwarzania danych osobowych innemu podmiotowi,

2.5. aktywnej współpracy z Procesorem przez cały okres trwania powierzenia przetwarzania danych osobowych, która w szczególności polega na tym, iż Podprocesor biorąc pod uwagę charakter przetwarzania, poprzez odpowiednie środki techniczne i organizacyjne, w miarę możliwości będzie pomagał Administratorowi wywiązywać się z obowiązków względem osób, których dane dotyczą oraz, uwzględniając charakter przetwarzania oraz dostępne mu informacje, będzie pomagał Procesorowi wywiązywać się z obowiązków w zakresie zagwarantowania bezpieczeństwa danych osobowych;

2.6. prowadzenia rejestru kategorii czynności przetwarzania oraz innej dokumentacji, spełniającej wymagania określone dla środków organizacyjnych i technicznych, o których mowa w art. 24 RODO;

2.7. przechowywanie dokumentów w sposób zapewniający bezpieczeństwo przed utratą, zabraniem, zniszczeniem, a także naruszeniem praw osób, których dane dotyczą.

3. Podprocesor zobowiązuje się niezwłocznie (nie później niż w ciągu 12 h) zawiadomić Procesora o:

3.1. każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia Procesora wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia,

3.2. każdym nieupoważnionym dostępie do danych osobowych,

3.3. każdym żądaniu otrzymanym bezpośrednio od osoby, której dane przetwarza, w zakresie przetwarzania dotyczącej jej danych osobowych, powstrzymując się jednocześnie od odpowiedzi na żądanie, chyba, że zostanie do tego pisemnie upoważniony przez Procesora.

4. Podprocesor, na każdy pisemny wniosek Procesora, zobowiązany jest do udzielenia kompleksowej, pisemnej odpowiedzi, na skierowane przez Procesora pytania dotyczące kwestii związanych z przetwarzaniem powierzonych danych osobowych.

5. Odpowiedzi, o której mowa w ust. 4 powyżej, Podprocesor udzieli niezwłocznie, nie później niż w terminie 7 dni roboczych od dnia otrzymania wniosku Procesora.

6. W przypadku wystąpienia incydentu zagrażającego bezpieczeństwu powierzonych do przetwarzania danych osobowych, tj. w szczególności wystąpienia lub podejrzenia wystąpienia któregokolwiek z: kradzieży, nieuprawnionego dostępu lub wykorzystania, ujawnienia, utraty, uszkodzenia lub zniszczenia powierzonych danych osobowych lub jakiegokolwiek innego niewłaściwego lub bezprawnego przetwarzania powierzonych danych osobowych, Podprocesor jest zobowiązany:

6.1. niezwłocznie po powzięciu wiadomości o incydencie, jednak w każdym przypadku nie później niż w ciągu dwudziestu czterech (24) godzin od powzięcia takiej wiadomości, powiadomić Procesora i Administratora o takim incydencie, a w szczególności przekazać mu informacje dotyczące:

6.1.1. daty i miejsca incydentu,

6.1.2. kategorii danych oraz przybliżonej liczby osób, których dotyczy incydent,

6.1.3. opisu incydentu,

6.1.4. możliwych konsekwencji incydentu,

6.1.5. ewentualnego podjęcia środków zaradczych,

6.2. zapewnić pomoc i przekazać dalsze informacje, które mogą być zasadnie wymagane przez Procesora i Administratora w związku z tym incydentem,

6.3. niezwłocznie po powzięciu wiadomości o incydencie podjąć wszelkie zasadne starania w celu przeprowadzenia dochodzenia w sprawie incydentu jak również usunięcia przyczyn oraz jego skutków, z zastrzeżeniem, że Podprocesor dołoży takich starań wyłącznie na polecenie Procesora i Administratora oraz wydane po powiadomieniu Procesora i Administratora o incydencie, oraz

6.4. wyłącznie, jeżeli zostanie to uprzednio zaakceptowane na piśmie przez Procesora, powiadomić o incydencie osoby, na które incydent miał wpływ.

§5
Prawo kontroli

1. Procesor ma prawo do kontroli przetwarzania przez Podprocesora powierzonych mu danych osobowych z punktu widzenia zgodności tego przetwarzania z przepisami prawa oraz postanowieniami Umowy w postaci audytu realizowanego przez Procesora lub audytora upoważnionego przez Procesora.
2. Informacja o terminie i zakresie audytu, o którym mowa w ust. 1 powyżej, będzie przekazana Podprocesorowi z co najmniej 5 dniowym wyprzedzeniem.
3. Podprocesor umożliwia Procesorowi lub audytorowi upoważnionemu przez Procesora, przeprowadzanie audytu, o którym mowa w ust. 1 i przyczynia się do niego. W szczególności, Podprocesor zobowiązany jest udostępnić wgląd do wszystkich materiałów oraz systemów, w których realizowane jest przetwarzanie powierzonych danych oraz umożliwić dostęp do pracowników zaangażowanych w ich przetwarzanie.
4. Procesor lub audytor upoważniony przez Procesora, przed rozpoczęciem czynności audytowych podpisze zobowiązanie o zachowaniu w poufności wszelkich informacji uzyskanych podczas realizacji audytu, w tym danych osobowych, których administratorem danych jest Procesor.

§6
Dalsze podpowierzenie i transfer do państw trzecich

1. Podprocesor ma prawo dalszego podpowierzania danych osobowych, o których mowa w §3 ust. 1 Umowy, w zakresie i celu niezbędnym do realizacji celu powierzenia przetwarzania danych osobowych określonego w §3 ust. 2 Umowy, wyłącznie po uzyskaniu pisemnej zgody Procesora.
2. Jeżeli do wykonania w imieniu Procesora konkretnych czynności przetwarzania Podprocesor korzysta z usług innego podmiotu przetwarzającego, zobowiązuje się on do tego, że:
   2.1. będzie korzystał wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by dokonywane przez nie przetwarzanie danych osobowych spełniało wymogi Ogólnego rozporządzenia o ochronie danych,
   2.2. na ten inny podmiot przetwarzający, w drodze zawartej pomiędzy tym podmiotem a Procesorem umowy, nałożone zostaną te same obowiązki ochrony danych jak w §4 Umowy, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych ochrony danych, a także prawo do umożliwienia przeprowadzenia przez Procesora u tych podmiotów kontroli na zasadach określonych w § 5 Umowy.
3. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Procesora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Podprocesorze.
4. Podprocesor na każde żądanie Procesora, jest zobowiązany do przedstawienia aktualnej listy innych podmiotów przetwarzających, którym podpowierzył powierzone mu przez Procesora dane osobowe. Podprocesor zobowiązuje się do prowadzenia pisemnego wykazu podmiotów, którym podpowierzył dane osobowe. Wykaz ma zawierać co najmniej nazwę podpowierzającego, nazwę i adres dalszego podprocesora, jego status (wykonawca, ekspert, trener, etc., datę zawarcia umowy podpowierzenia, datę zakończenia jej obowiązywania. Wykaz ten ma być prowadzony na bieżąco i przekazywany Procesorowi nie rzadziej niż raz na kwartał lub na każde żądanie Procesora.
5. Podprocesor nie może przekazywać danych osobowych do państwa trzeciego tj. kraju znajdującego się poza Europejskim Obszarem Gospodarczym, chyba że Procesor wyrazi na to pisemną zgodę. Po udzieleniu przez Administratora zgody na przekazanie danych osobowych do państwa trzeciego, Procesor może dokonać takiego transferu danych wyłącznie w przypadku, gdy:
   5.1. stwierdzone zostało w drodze decyzji Komisji Europejskiej, że docelowe państwo trzecie zapewnia adekwatny poziom ochrony danych osobowych, lub
   5.2. zapewnione zostały inne środki, które zgodnie z obowiązującymi przepisami legalizują transfer danych do tego państwa trzeciego takie jak: prawnie wiążący i egzekwowalny instrument, wiążące reguły korporacyjne, standardowe klauzule przyjęte przez Komisję

Europejską, standardowe klauzule przyjęte przez organ nadzorczy, kodeksy postępowań; mechanizm certyfikacji.

§7

Odpowiedzialność Podprocesora

1. Podprocesor jest odpowiedzialny za wszelkie szkody będące następstwem przetwarzania powierzonych mu danych osobowych, w sposób sprzeczny z Umową lub obowiązującymi przepisami prawa, w szczególności powstałych w wyniku udostępnienia danych osobom nieupoważnionym.
2. W przypadku wystąpienia okoliczności stanowiących niewykonanie lub niewłaściwe wykonanie przez Podprocesora jego zobowiązań wynikających z Umowy, Procesor wezwie Podprocesora do usunięcia uchybień w wyznaczonym terminie. W razie niezastosowania się przez Podprocesora do wydanych przez procesora wytycznych, Procesor będzie uprawniony do żądania zapłaty kary umownej w wysokości 15 000.00 zł (słownie: piętnaście tysięcy złotych) za każdy przypadek stwierdzonej nieprawidłowości.
3. Jeżeli podobne nieprawidłowości zostaną ujawnione ponownie, Procesor jest uprawniony do żądania zapłaty kary umownej bez wyznaczania terminu do ich usunięcia.
4. Kara umowna płatna będzie na podstawie noty obciążeniowej w terminie 14 dni od daty jej doręczenia.
5. W przypadku, gdy w wyniku naruszenia przez Podprocesora postanowień Umowy lub obowiązujących przepisów prawa (z przyczyn leżących po jego stronie), Procesor zostanie zobowiązany do wypłaty odszkodowania lub zadośćuczynienia, zapłaty kary grzywny, administracyjnej kary pieniężnej, Podprocesor zobowiązuje się do pokrycia wszelkich wynikających z tego tytułu kosztów jakie Procesor poniesienie lub jakie będzie zobowiązany ponieść, w tym również kosztów postępowania sądowego lub sądowo-administracyjnego.
6. Procesorowi przysługuje względem Podprocesora prawo do dochodzenia na zasadach ogólnych odszkodowania przewyższającego zastrzeżoną karę umowną – do pełnej wysokości poniesionej szkody.

§8

Usunięcie lub zwrot danych osobowych

1. Zależnie od decyzji Administratora lub Procesora w tym zakresie, w terminie do 14 dni roboczych od dnia zakończenia Umowy, Podprocesor jest zobowiązany do usunięcia lub zwrotu wszelkich powierzonych mu danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba, że obowiązujące przepisy prawa nakazują przechowywanie tych danych osobowych. Usunięcie / zwrot danych zostaną stwierdzone stosownym protokołem, w sposób i na zasadach określonych przez Administratora i Procesora.
2. Powierzenie przetwarzania danych osobowych trwa do upływu wyżej wskazanego terminu.

§9

Czas trwania i wypowiedzenie Umowy

1. Umowa zawarta jest na czas określony odpowiadający okresowi umowy, o której mowa w §2 ust. 1 Umowy.
2. Procesor ma prawo wypowiedzieć Umowę w trybie natychmiastowym, gdy Podprocesor:
   2.1. wykorzystał dane osobowe w sposób niezgodny z Umową,
   2.2. wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa,
   2.3. nie zaprzestał niewłaściwego przetwarzania danych osobowych,
   2.4. zawiadomił o swojej niezdolności do wypełnienia Umowy, a w szczególności wymagań określonych w §4 Umowy.
3. Wypowiedzenie Umowy przez Procesora nie zwalnia Podprocesora od zapłaty ewentualnej kary umownej i odszkodowania.
4. Jeżeli jedna ze Stron rażąco narusza zobowiązania wynikające z Umowy, druga Strona może wypowiedzieć Umowę ze skutkiem natychmiastowym oraz żądać naprawienia szkody poniesionej na skutek takiego naruszenia.

§10
Pozostałe postanowienia

1. Przetwarzanie danych dozwolone jest wyłącznie w celu określonym w §3 ust. 4 Umowy. Wykorzystanie przez Procesora danych Administratora w celach innych niż określone Umową wymaga każdorazowo uprzedniej, pisemnej zgody Administratora.
2. Zasady komunikacji między Stronami:
   2.1. W przypadku komunikacji w formy pisemnej – doręczenie pocztą (listem poleconym), pocztą kurierską lub osobiście na adresy podane w komparycji Umowy,
   2.2. W przypadku komunikacji w formie elektronicznej – na następujące adresy email:
      2.2.1. ze strony Procesora: email: aginalski@wwf.pl
      2.2.2. ze strony Podprocesora: email: .....
3. Zmiana danych, o których mowa w ust. 2 pkt 2.2. powyżej nie stanowi zmiany Umowy i wymaga jedynie pisemnego poinformowania drugiej Strony. Do czasu otrzymania informacji o zmianie danych za prawidłowe dane do kontaktów uznaje się dane dotychczasowe.
4. Doręczenia dokonane na zasadach określonych w ust. 2 powyżej uznaje się za prawidłowe z chwilą dojścia do adresata. Bez względu na potwierdzenie dotarcia oświadczenia do adresata uznaje się, że oświadczenie doszło do tego adresata po upływie 14 dni od dnia wysłania przez nadawcę.

§11
Postanowienia końcowe

1. Strony wspólnie postanawiają, że Umowa zastępuje wszelkie dotychczasowe uzgodnienia w zakresie przetwarzania danych osobowych związane ze świadczeniem przez Podprocesora usług na rzecz Procesora na podstawie umowy, o której mowa w §2 ust. 1 Umowy, w zakresie wspólnej realizacji projektu.
2. W sprawach nieuregulowanych postanowieniami Umowy zastosowanie będą mieć właściwe przepisy prawa.
3. Wszelkie zmiany, uzupełnienia lub rozwiązanie Umowy wymagają zachowania formy pisemnej pod rygorem nieważności, z zastrzeżeniem, tych sytuacji w których Umowa wprost przewiduje możliwość dokonywania zmian w innej formie.
4. Strony zgodnie oświadczają, iż w przypadku sporów powstałych na tle realizacji Umowy dążyć będą do polubownego ich załatwienia. W przypadku, gdy nie dojdzie do załatwienia sporu w powyższy sposób, właściwym do jego rozstrzygnięcia będzie sąd powszechny właściwy miejscowo według właściwości ogólnej.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Podprocesor: **Procesor:**

_____ _____

Załączniki:

1. Wzór klauzuli informacyjnej, stanowiącej realizację obowiązku informacyjnego.
2. Informacja o zapewnieniu przez podmiot przetwarzający odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych art. 24 ust. 1 i 2 oraz art. 32 RODO.

Załącznik nr 1 do Umowy Podpowierzenia

Wzór klauzuli informacyjnej, stanowiącej realizację obowiązku informacyjnego

Administratorem przetwarzanych danych osobowych jest Minister właściwy do spraw rozwoju regionalnego, pełniący funkcję Instytucji Zarządzającej Programem Operacyjnym Infrastruktura i Środowisko 2014-2020 (PO IiŚ 2014-2020), z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa.

Fundacja WWF Polska z siedzibą w Warszawie, ul. Usypiskowa 11, 02-386 Warszawa jest podmiotem przetwarzającym dane osobowe na podstawie porozumienia zawartego z administratorem (tzw. procesorem).

Dane osobowe przetwarzane będą na potrzeby realizacji PO IiŚ 2014-2020, w tym w szczególności w celu wykonywania zadań związanych z realizacją Programu Operacyjnego Infrastruktura i Środowisko 2014-2020, tj. realizacja UoD.

Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu, związanego z wdrażaniem Programu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Przetwarzanie danych osobowych odbywa się w związku [1]:

1. z realizacją ciążącego na administratorze obowiązku prawnego (art. 6 ust. 1 lit. c RODO [2]), wynikającego z następujących przepisów prawa [3]:
   - rozporządzenia Parlamentu Europejskiego i Rady nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego, oraz ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylającego Rozporządzenie Rady (WE) nr 1083/2006,
   - rozporządzenia wykonawczego Komisji (UE) nr 1011/2014 z dnia 22 września 2014 r. ustanawiającego szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi,
   - Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012,
   - ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020,
   - ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego,
   - ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
   - ustawy z dnia 21 listopada 2008 r. o służbie cywilnej,

[1] Należy wybrać jedną lub kilka podstaw.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE. L 119 z 04.05.2016, s.1-88).

[3] Należy wskazać jeden lub kilka przepisów prawa - możliwe jest ich przywołanie w zakresie ograniczonym na potrzeby konkretnej klauzuli.

- zarządzenia nr 70 Prezesa Rady Ministrów z dnia 6 października 2011 r. w sprawie wytycznych w zakresie przestrzegania zasad służby cywilnej oraz w sprawie zasad etyki korpusu służby cywilnej,

2. z wykonywaniem przez administratora zadań realizowanych w interesie publicznym lub ze sprawowaniem władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO),
3. z realizacją umowy, gdy osoba, której dane dotyczą, jest jej stroną, a przetwarzanie danych osobowych jest niezbędne do jej zawarcia oraz wykonania (art. 6 ust. 1 lit. b RODO).

Minister może przetwarzać różne rodzaje danych [4], w tym przede wszystkim:

1) dane identyfikacyjne, w tym w szczególności: imię, nazwisko, miejsce zatrudnienia / formę prowadzenia działalności gospodarczej, stanowisko; w niektórych przypadkach także PESEL, NIP, REGON,
2) dane dotyczące zatrudnienia, w tym w szczególności: otrzymywane wynagrodzenie oraz wymiar czasu pracy,
3) dane kontaktowe, w tym w szczególności: adres e-mail, nr telefonu, nr fax, adres do korespondencji,
4) dane o charakterze finansowym, w tym szczególności: nr rachunku bankowego, kwotę przyznanych środków, informacje dotyczące nieruchomości (nr działki, nr księgi wieczystej, nr przyłącza gazowego),

Dane pozyskiwane są bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację Programu, w tym w szczególności: od wnioskodawców, beneficjentów, partnerów.

Odbiorcami danych osobowych mogą być:

- podmioty, którym Instytucja Zarządzająca PO IiŚ 2014-2020 powierzyła wykonywanie zadań związanych z realizacją Programu, w tym w szczególności podmioty pełniące funkcje Instytucji Pośredniczących i Wdrażających,
- instytucje, organy i agencje Unii Europejskiej (UE), a także inne podmioty, którym UE powierzyła wykonywanie zadań związanych z wdrażaniem PO IiŚ 2014-2020,
- podmioty świadczące usługi, w tym związane z obsługą i rozwojem systemów teleinformatycznych oraz zapewnieniem łączności, w szczególności dostawcy rozwiązań IT i operatorzy telekomunikacyjni [5].

Dane osobowe będą przechowywane przez okres wskazany w art. 140 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. oraz jednocześnie przez czas nie krótszy niż 10 lat od dnia przyznania ostatniej pomocy w ramach PO IiŚ 2014-2020 - z równoczesnym uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Osobie, której dane dotyczą, przysługuje:

– prawo dostępu do swoich danych oraz otrzymania ich kopii (art. 15 RODO),
– prawo do sprostowania swoich danych (art. 16 RODO),
– prawo do usunięcia swoich danych (art. 17 RODO) - jeśli nie zaistniały okoliczności, o których mowa w art. 17 ust. 3 RODO,
– prawo do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
– prawo wniesienia sprzeciwu wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym

[4] Informacje podawane w przypadku wykonywania obowiązku informacyjnego na podstawie art. 14 RODO.

[5] O ile dotyczy.

lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO),

– prawo wniesienia skargi do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych (art. 77 RODO) - w przypadku, gdy osoba uzna, iż przetwarzanie jej danych osobowych narusza przepisy RODO lub inne krajowe przepisy regulujące kwestię ochrony danych osobowych, obowiązujące w Rzeczpospolitej Polskiej.

W przypadku pytań, kontakt z Inspektorem Ochrony Danych Osobowych Ministra właściwego do spraw rozwoju regionalnego (Instytucji Zarządzającej POIiŚ) jest możliwy:

- pod adresem: ul. Wspólna 2/4, 00-926 Warszawa,
- pod adresem e-mail: *IOD@mfipr.gov.pl*.

Dane osobowe nie będą objęte procesem zautomatyzowanego podejmowania decyzji, w tym profilowania.

Załącznik nr 2 do Umowy Podpowierzenia
Wzór informacji o zapewnieniu przez podmiot przetwarzający odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych art. 24 ust. 1 i 2 oraz art. 32 RODO

- ☐ został wyznaczony inspektor ochrony danych osobowych, nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych, należy podać dane kontaktowe (imię i nazwisko, numer telefonu oraz adres poczty elektronicznej)
- ☐ do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie w przedmiotowym zakresie,
- ☐ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
- ☐ została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych, spełniająca wymagania określone dla środków organizacyjnych, o których mowa w art. 24 ust. 2 RODO; należy ją wyszczególnić poniżej:
  - *matryca danych, ryzyka i zabezpieczeń - dokument analityczny, w którym przeprowadzono analizę stanu ochrony danych osobowych w organizacji, jak również oceniono potencjalne ryzyko;*
  - *lista kontrolna oraz jej aktualizacje – dokument analityczny stanowiący podsumowanie audytu oraz weryfikację spełniania wymogów dot. ochrony danych osobowych;*
  - *polityka ochrony danych osobowych;*
  - *upoważnienia dla pracowników oraz oświadczenia o zachowaniu w tajemnicy danych osobowych;*
  - *instrukcje dot. przetwarzania i ochrony danych osobowych;*
  - *rejestr czynności przetwarzania danych osobowych,*
  - *rejestr kategorii przetwarzania danych osobowych,*

Środki ochrony fizycznej danych		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do fizycznego zabezpieczenia przetwarzanych danych osobowych.		
1	☐	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi).
2	☐	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.
3	☐	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
4	☐	Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
5	☐	Pomieszczenia, w których przetwarzany jest zbiór danych osobowych, wyposażone są w system alarmowy przeciwwłamaniowy.
6	☐	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, objęte są systemem kontroli dostępu.
7	☐	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
8	☐	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
9	☐	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony.
10	☐	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.
11	☐	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie.
12	☐	Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej.

13	☐	Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
14	☐	Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.
15	☐	Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
16	☐	Zbiór danych osobowych przetwarzany jest w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
17	☐	Pomieszczenie, w którym przetwarzany jest zbiór danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i / lub wolnostojącej gaśnicy.
18	☐	Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do:

5. technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania,
6. opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych,
7. sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji,
8. sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji),
9. sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych.

1	☐	Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.
2	☐	Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.
3	☐	Zastosowano urządzenia typu UPS, generator prądu i / lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
4	☐	Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej / komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
5	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
6	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.
7	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.
8	☐	Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
9	☐	Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
10	☐	Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
11	☐	Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
12	☐	Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
13	☐	Zastosowano procedurę oddzwonienia (*callback*) przy transmisji realizowanej za pośrednictwem modemu.
14	☐	Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
15	☐	Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity.

16	☐	Użyto system Firewall do ochrony dostępu do sieci komputerowej.
17	☐	Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
Środki ochrony w ramach narzędzi programowych i baz danych		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.		
1	☐	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2	☐	Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3	☐	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4	☐	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.
5	☐	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.
6	☐	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
7	☐	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
8	☐	Zastosowano kryptograficzne środki ochrony danych osobowych.
9	☐	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
10	☐	Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
Środki organizacyjne		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do innych środków organizacyjnych zastosowanych przez administratora w celu ochrony danych, takich jak: instrukcje, szkolenia, zobowiązania.		
1	☐	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
2	☐	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
3	☐	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
4	☐	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
5	☐	Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

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

- *rozmieszczenie pomieszczeń biurowych uniemożliwia wgląd w dane osobowe osobom postronnym – każdorazowo pracownik lub właściciele firmy mają ogląd na stanowiska robocze innych pracowników,*
- *wejście do biura odgrodzone jest od pozostałych pomieszczeń biurowych stanowiskiem sekretariatu, przy którym zawsze znajduje się pracownik (brak możliwości wejścia osób nieupoważnionych),*
- *każdemu gościowi lub osobie zewnętrznej towarzyszy pracownik Podprocesora,*
- *dane elektroniczne nie są umieszczane na wspólnym serwerze lub chmurze danych. Pracownicy biurowi przechowują dane na własnych dyskach lokalnych lub indywidualnych*

skrzynkach poczty elektronicznej – w obydwu przypadkach dostęp do danych jest zabezpieczony indywidualnym hasłem i loginem, zaś tylko Ci pracownicy mają dostęp do wskazanych danych,

- *pracownicy posiadają swoje własne dedykowane stanowiska robocze wraz z dedykowanymi stacjami roboczymi,*
- *dane papierowe umieszczane są w teczkach i segregatorach, które z kolei przechowywane są w zamykanych szafach w odrębnym pomieszczeniu.*