Kraków, dn. .....

Umowa podpowierzenia przetwarzania danych osobowych

Stanowiąca uzupełnienie do umowy na pełnienie nadzoru przyrodniczego podczas realizacji zadania pn.: *„Działania informacyjno-promocyjne na zakończenie projektu pn.: Zachowanie i ochrona środowiska, promowanie efektywnego gospodarowania zasobami wodnymi oraz zapobieganie i zarządzanie ryzykiem powodziowym, poprzez poprawę bezpieczeństwa powodziowego Węzła Oświęcimskiego”*, z dnia .....

zawarta w dniu 06.02.2019 r. w Krakowie, pomiędzy:

Państwowym Gospodarstwem Wodnym Wody Polskie z siedzibą w Warszawie,
ul. Żelazna 59 A, 00-848 Warszawa, NIP: 5272825616, REGON: 368302575,
reprezentowanym przez:
Panią/Pana Małgorzatę Sikorę – Dyrektora Regionalnego Zarządu Gospodarki Wodnej w Krakowie, działającą/ego na podstawie pełnomocnictwa z dnia 9 sierpnia 2018 r. (znak: KOP.012.59.5.2018.BM),
ul. Marsz. J. Piłsudskiego 22, 31-109 Kraków,
zwanym dalej **Podmiotem przetwarzającym**
a
.....
.....
.....

reprezentowany przez: .....
(imię, nazwisko reprezentanta Wykonawcy),

zwanym dalej **Podprocesorem**

(zwanymi dalej łącznie jako: **„Strony")**

§1
Definicje

Ilekroć w niniejszej Umowie Powierzenia mowa o:

1) **danych osobowych** – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
2) **przetwarzaniu** – 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;

3) **Rozporządzeniu** – 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 z późn. zm.);
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 Powierzenia** – rozumie się przez to niniejszą umowę podpowierzenia przetwarzania danych osobowych;
6) **Umowie Głównej** – rozumie się przez to umowę z dnia .... zawartą przez Strony niniejszej Umowy Powierzenia, której przedmiotem jest realizacja usługi na pełnienie nadzoru przyrodniczego podczas realizacji zadania *pn.: „**Działania informacyjno-promocyjne na zakończenie projektu pn.: Zachowanie i ochrona środowiska, promowanie efektywnego gospodarowania zasobami wodnymi oraz zapobieganie i zarządzanie ryzykiem powodziowym, poprzez poprawę bezpieczeństwa powodziowego Węzła Oświęcimskiego**"* w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020, działanie 2.1 *„Adaptacja do zmian klimatu wraz z zabezpieczeniem i zwiększeniem odporności na klęski żywiołowe, w szczególności katastrofy naturalne oraz monitoring środowiska"*;
7) **ustawie o ochronie danych osobowych** – rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781 z późn. zm.).

§2
Przedmiot umowy

1. Podmiot przetwarzający i Podprocesor oświadczają, że zawarli Umowę Główną w związku z którą będą przetwarzane dane osobowe.
2. Niniejsza Umowa Powierzenia jest akcesoryjna względem Umowy Głównej oraz reguluje wzajemny stosunek stron i ich obowiązki w zakresie przetwarzania danych osobowych w związku z obowiązkami Podprocesora wynikającymi z Umowy Głównej.
3. Przetwarzanie danych osobowych odbywać się będzie w zgodzie i w oparciu o Rozporządzenie, ustawę o ochronie danych osobowych i innymi powszechnie obowiązującymi przepisami o ochronie danych osobowych.
4. Przedmiotem Umowy jest powierzenie Podprocesorowi przez Podmiot przetwarzający, przetwarzania danych osobowych, w imieniu i na rzecz Administratora danych osobowych, na warunkach przewidzianych niniejszą Umową, w związku z realizacją obowiązków określonych w Umowie Głównej
5. Podmiot przetwarzający oświadcza, że:
   1) Administratorem danych osobowych, w rozumieniu art. 4 pkt 7 RODO, jest Minister Finansów, Funduszy i Polityki Regionalnej, pełniący funkcję Instytucji Zarządzającej Programem Operacyjnym Infrastruktura i Środowisko 2014-2020 (POIiŚ 2014-2020), z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa.
   2) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej z siedzibą przy ul. Konstruktorskiej 3a, 02-673 Warszawa jest podmiotem przetwarzającym dane osobowe na

podstawie porozumienia zawartego z Administratorem danych osobowych w dniu 17 grudnia 2015 r.,

3) Państwowe Gospodarstwo Wodne Wody Polskie jest podmiotem przetwarzającym dane osobowe jako beneficjent projektu pn.: ***„Działania informacyjno-promocyjne na zakończenie projektu pn.: Zachowanie i ochrona środowiska, promowanie efektywnego gospodarowania zasobami wodnymi oraz zapobieganie i zarządzanie ryzykiem powodziowym, poprzez poprawę bezpieczeństwa powodziowego Węzła Oświęcimskiego"***, realizowanego w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020, na podstawie umowy o dofinansowanie nr POIS.02.01.00-00-0024/17-00 z dnia 25.04.2018 r. zawartej z Narodowym Funduszem Ochrony Środowiska i Gospodarki Wodnej.

4) Powierzenie przetwarzania danych osobowych pomiędzy instytucjami wymienionymi powyżej, nastąpiło w ramach zbiorów: 1) Program Operacyjny Infrastruktura i Środowisko 2014-2020 oraz 2) Centralny system teleinformatyczny, wspierający realizację programów operacyjnych w zakresie niezbędnym do realizacji zadań związanych z Programem Operacyjnym Infrastruktura i Środowisko 2014-2020.

5. Podmiotem przetwarzającym, w rozumieniu art. 4 ust. 8 Rozporządzenia, któremu Podmiot przetwarzający powierza przetwarzanie danych osobowych jest Podprocesor.
6. Podmiot przetwarzający powierza Podprocesorowi przetwarzanie danych osobowych, a Podprocesor zobowiązuje się do ich przetwarzania zgodnego z prawem, Umową Główną i niniejszą Umową Powierzenia.
7. Procesor będzie przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w niniejszej Umowie Powierzenia.

§3
Powierzenie przetwarzania danych osobowych

1. Podmiot przetwarzający powierza Podprocesorowi przetwarzanie danych osobowych:
   1) Dane identyfikacyjne pracowników Podmiotu przetwarzającego.
   2) Dane identyfikacyjne osób innych wykonawców i ich pracowników.
   3) Dane identyfikacyjne właścicieli nieruchomości (imię, nazwisko, adres, położenie i nr działki)

   Dane dotyczą podmiotów objętych realizacją projektu bądź podmiotów uprawnionych do uzyskania informacji w związku z realizacja projektu.

2. Powierzenie nie obejmuje przetwarzania danych osobowych, o których mowa w art. 9-10 Rozporządzenia.
3. Cel i zakres powierzenia przetwarzania danych osobowych wynika bezpośrednio i ogranicza się wyłącznie do zadań wynikających z zawartej Umowy Głównej.
4. Na danych osobowych, z związku z realizacją celu, o którym mowa w ust. 3, będą wykonywane w szczególności następujące operacje: ☒zbierania, ☒utrwalania, ☒organizowania, ☒porządkowania, ☒przechowywania, ☒adaptowania lub modyfikowania, ☒pobierania, ☒wykorzystywania, ☒ujawniania poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, a także czynności polegające na tworzeniu kopii bezpieczeństwa oraz czynności związane z odtworzeniem danych osobowych z kopii bezpieczeństwa.

5. Przetwarzanie powierzonych danych osobowych będzie odbywać się z wykorzystaniem systemów informatycznych.
6. Podmiot powierzający nie wyraża zgody na przetwarzanie danych osobowych poza Europejskim Obszarem Gospodarczym.

§4
Obowiązki Podprocesora

1. Podprocesor oświadcza, że przetwarzanie powierzonych mu danych osobowych, będzie odbywało się z poszanowaniem przepisów Rozporządzenia, ustawy o ochronie danych osobowych i innych powszechnie obowiązujących przepisów z zakresu ochrony danych osobowych.
2. W związku z powierzeniem przetwarzania danych osobowych Podprocesor zobowiązuje się do:
   1) przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Podmiotu powierzającego; za udokumentowane polecenie uznaje się zadania zlecone do wykonywania w drodze Umowy Głównej;
   2) dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie, o którym mowa w art. 29 Rozporządzenia, oraz przeszkolonych z zakresu przepisów o ochronie danych osobowych;
   3) zobowiązania osób upoważnionych do przetwarzania danych osobowych do zachowania tajemnicy;
   4) 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 ochrony fizycznej, środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej, środków ochrony w ramach narzędzi programowych i baz danych oraz środków organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu temu ryzyku, w tym m. in. w stosownym przypadku:
      a) pseudonimizacji i szyfrowania danych osobowych,
      b) zapewnienia bezpiecznego (kryptograficznie zabezpieczonego) transferu danych osobowych w procesie świadczonej usługi – wdrożenia mechanizmów uwierzytelniania oraz nadzoru działań w systemie informatycznym przez odnotowywanie zdarzeń na przetwarzanych danych osobowych (logowanie działań),
      c) zapewnienia w działaniach serwisowych (w tym wymiana uszkodzonych zasobów dyskowych), by dostęp do zasobów był ograniczony do osób upoważnionych,
      d) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów informatycznych i usług przetwarzania,
      e) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
      f) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych;
   5) przestrzegania określonych w § 7 niniejszej Umowy Powierzenia warunków podpowierzenia przetwarzania danych osobowych innemu podmiotowi;
   6) aktywnej współpracy z Podmiotem powierzającym 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 Podmiotowi powierzającemu wywiązywać się z obowiązków względem osób, których dane dotyczą, oraz – uwzględniając charakter przetwarzania i dostępne mu informacje – będzie pomagał Podmiotowi powierzającemu wywiązywać się z obowiązków w zakresie zagwarantowania bezpieczeństwa danych osobowych.

3. Podprocesor realizując zadania wynikające z Umowy Głównej:
   1) zastosuje odpowiednie środki organizacyjne w celu zgodnego z przepisami przetwarzania powierzonych danych osobowych;
   2) zastosuje środki zabezpieczenia określone w art. 32 Rozporządzenia – wdrożone środki zabezpieczenia muszą być adekwatne do zidentyfikowanych ryzyk dla zakresu powierzonego przetwarzania danych osobowych;
   3) udzieli pomocy Podmiotowi powierzającemu w zakresie:
      a) realizacji obowiązku udzielania odpowiedzi na żądania osób, których dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia,
      b) zapewnienia realizacji obowiązków wynikających z art. 32-36 Rozporządzenia;
   4) po zakończeniu przetwarzania danych osobowych niezwłocznie zwróci powierzone mu dane osobowe lub dokona ich zniszczenia – adekwatnie do woli Podmiotu powierzającego;
   5) wyznaczy Inspektora Ochrony Danych (o ile wynika to z obowiązku prawnego) oraz rozpocznie prowadzenie rejestru wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora zgodnie z wymaganiami art. 30 ust. 2 Rozporządzenia i pisemnie poinformuje o tym Podmiot powierzający.
4. Podprocesor zobowiązuje się niezwłocznie (nie później niż w ciągu 24 godzin) zawiadomić Podmiot powierzający o:
   1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia Podmiot powierzający wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia,
   2) każdym żądaniu otrzymanym bezpośrednio od osoby, której dane osobowe przetwarza, w zakresie przetwarzania dotyczącej jej danych osobowych, powstrzymując się jednocześnie od odpowiedzi na żądanie, chyba że zostanie do tego upoważniony przez Podmiot powierzający.
5. Wykaz środków, o których mowa w ust. 2 pkt 4 oraz ust. 3 pkt 1-2, stanowi Załącznik nr 1 do niniejszej Umowy.
6. Podprocesor na każdy pisemny wniosek Podmiotu powierzającego zobowiązany jest do udzielenia kompleksowej, pisemnej odpowiedzi, na skierowane przez Podmiot powierzający pytania dotyczące kwestii związanych z przetwarzaniem powierzonych danych osobowych.
7. Odpowiedzi, o której mowa w ust. 5, Podrocesor udzieli niezwłocznie, nie później niż w terminie 7 dni roboczych od dnia otrzymania wniosku Podmiotu powierzającego.

§ 5.

Naruszenie bezpieczeństwa danych osobowych

1. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych, Podprocesor bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 24 godzin od momentu

pozyskania informacji o wystąpieniu naruszenia lub podejrzeniu jego wystąpienia – zgłasza je Podmiotowi powierzającemu. Zgłoszenie powinno zawierać informacje wskazane w art. 33 ust. 3 Rozporządzenia.

2. Podprocesor zobowiązuje się zapewnić odpowiednie wsparcie wymagane przez Podmiotu powierzający lub organ nadzorczy w celu podjęcia sprawnych i odpowiednich działań w przedmiocie naruszenia bezpieczeństwa danych osobowych.
3. Podprocesor odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które Rozporządzenie nakłada bezpośrednio na Podprocesora, lub gdy działał poza zgodnymi z prawem instrukcjami Podmiotu powierzającego lub wbrew tym instrukcjom. Podprocesor odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.

§ 6.
Prawo audytu

1. Podmiotu powierzającego ma prawo do audytu przetwarzania przez Podprocesora powierzonych mu danych osobowych z punktu widzenia zgodności tego przetwarzania z przepisami prawa oraz postanowieniami niniejszej Umowy Powierzenia w postaci audytu realizowanego przez Podmiot powierzający lub audytora upoważnionego przez Podmiot powierzający.
2. Podprocesor zobowiązany jest:
   1) udostępnić Podmiotowi powierzającemu lub audytorowi upoważnionemu przez Podmiot powierzający wszelkie informacje niezbędne do wykazania spełnienia obowiązków spoczywających na Podprocesorze;
   2) umożliwić Podmiotowi powierzającemu lub audytorowi upoważnionemu przez Podmiot powierzający przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych;
   3) zastosować się do zaleceń poaudytowych przekazanych przez Podmiot powierzający lub audytora upoważnionego przez Podmiot powierzający.
3. Informacja o terminie i zakresie audytu, o którym mowa w ust. 1, będzie przekazana Podprocesorowi z co najmniej 24-godzinnym wyprzedzeniem.
4. Podprocesor umożliwia Podmiotowi powierzającemu lub audytorowi upoważnionemu przez Podmiot powierzający, 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 informatycznych, w których realizowane jest przetwarzanie powierzonych danych osobowych oraz umożliwić dostęp do pracowników zaangażowanych w ich przetwarzanie.
5. Podmiot powierzający lub audytor upoważniony przez Podmiot powierzający przed rozpoczęciem czynności audytowych podpisze zobowiązanie o zachowaniu w poufności wszelkich informacji uzyskanych podczas realizacji audytu, w tym danych osobowych, których administratorem jest Podrocesor.

§ 7.
Podpowierzenie

1. Podprocesor ma prawo podpodpowierzania danych osobowych, o których mowa w § 3 ust. 1, jedynie w zakresie i celu niezbędnym do realizacji celu powierzenia przetwarzania danych

osobowych określonego w § 3 ust. 3 (ogólna zgoda Podmiotu powierzającego na podpodpowierzenie przetwarzania danych osobowych).

2. Wykaz podmiotów podpodprzetwarzających (podpodprocesorów) zawiera Załącznik nr 2 do niniejszej Umowy.
3. Podrocesor jest zobowiązany do poinformowania Podmiotu powierzającego o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów podpodprzetwarzających, dając tym samym Podmiotowi powierzającemu możliwość wyrażenia sprzeciwu wobec takich zmian. Informację w tym zakresie należy przekazać na adres e-mail: riod.krakow@wody.gov.pl.
4. Jeżeli do wykonania w imieniu Podmiotu powierzającego konkretnych czynności przetwarzania danych osobowych Podprocesor korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający, w drodze umowy zawartej pomiędzy tym podmiotem a Podprocesorem, nałożone zostaną te same obowiązki ochrony danych osobowych, jak w § 4 niniejszej Umowy Powierzenia, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych ochrony danych.
5. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Podmiotu powierzającego za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Podprocesorze.

§ 8.
Odpowiedzialność Podprocesora

1. Podprocesor, dla zapewnienia, iż spełnia wymagania Rozporządzenia, zobowiązany jest:
   1) przed rozpoczęciem świadczenia usługi uzyskać akceptację Podmiotu powierzającego w zakresie spełniania wymagań dotyczących zabezpieczenia przetwarzanych danych osobowych w zakresie prawidłowości implementacji tych wymagań w dokumentacji bezpieczeństwa;
   2) przynajmniej raz w roku dostarczyć raport z audytu zabezpieczenia środowiska informacyjnego, w którym przetwarzane są powierzone Umową Główną dane osobowe.
2. Podrocesor jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z niniejszą Umową Powierzenia, a w szczególności udostępnienie ich osobom nieuprawnionym.
3. W przypadku ujawnienia okoliczności uznanych przez Podmiot powierzający za uchybienia w zakresie wykonywania niniejszej Umowy Powierzenia lub obowiązujących w tym zakresie przepisów prawa, Podprocesor zobowiązuje się do ich usunięcia w wyznaczonym terminie. W razie niezastosowania się przez Podprocesora do wydanych przez Podmiot powierzający wytycznych, Podmiot powierzający jest uprawniony do nałożenia kary umownej w wysokości 1 000 zł (słownie złotych: jeden tysiąc złotych) za każdy przypadek stwierdzonej nieprawidłowości.
4. Jeżeli podobne nieprawidłowości zostaną ujawnione ponownie lub nie zostanie dotrzymany termin usunięcia uchybień, o którym mowa w ust. 3, Podmiot powierzający jest uprawniony do nałożenia kary umownej bez wyznaczania terminu do ich usunięcia.
5. W przypadku naruszenia postanowień niniejszej Umowy Powierzenia lub obowiązujących w tym zakresie przepisów prawa z przyczyn leżących po stronie Podrocesora, w następstwie czego Podmiot powierzający, jako administrator danych osobowych, zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Podprocesor zobowiązuje się do zapłaty

Podmiotowi powierzającemu równowartości roszczeń osób trzecich, kar oraz równowartości kosztów postępowania sądowego, które będą wynikiem nieprawidłowego działania Podprocesora.

6. Podmiotowi powierzającemu przysługuje względem Podprocesora prawo do dochodzenia odszkodowania przewyższającego zastrzeżoną karę umowną – do pełnej wysokości poniesionej szkody.

§ 9.
Usunięcie lub zwrot danych osobowych

1. Zależnie od decyzji Podmiotu powierzającego w tym zakresie, w terminie do 14 dni roboczych od dnia zakończenia niniejszej Umowy Powierzenia, Podprocesor jest zobowiązany do usunięcia lub zwrotu wszelkich powierzonych mu danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba że obowiązujące przepisy prawa nakazują ich przechowywanie.
2. Powierzenie przetwarzania danych osobowych trwa do upływu wyżej wskazanego terminu.

§ 10.
Czas trwania i wypowiedzenie Umowy Powierzenia

1. Niniejsza Umowa Powierzenia zawarta jest na czas określony odpowiadający okresowi obowiązywania Umowy Głównej
2. Podmiot powierzający ma prawo wypowiedzieć niniejszą Umowę Powierzenia w trybie natychmiastowym z dniem rozwiązania lub wygaśnięcia Umowy Głównej, a także, gdy Podprocesor:
   1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową Powierzenia;
   2) wykonuje niniejszą Umowę Powierzenia niezgodnie z obowiązującymi w tym zakresie przepisami prawa;
   3) nie zaprzestał niewłaściwego przetwarzania danych osobowych;
   4) zawiadomił o swojej niezdolności do wypełnienia niniejszej Umowy Powierzenia, a w szczególności wymagań określonych w § 4 niniejszej Umowy Powierzenia.
3. Wypowiedzenie niniejszej Umowy Powierzenia przez Podmiot powierzający nie zwalnia Podprocesora od zapłaty należnych kar umownych i odszkodowania.

§ 11.
Pozostałe postanowienia

1. Przetwarzanie powierzonych danych osobowych dozwolone jest wyłącznie w celu określonym w § 3 ust. 3 niniejszej Umowy Powierzenia.
2. Wykorzystanie przez Podprocesora powierzonych danych osobowych w celach innych niż określone niniejszą Umową Powierzenia wymaga każdorazowo pisemnej zgody Podmiotu powierzającego.

§ 12.
Postanowienia końcowe

1. Niniejsza Umowa Powierzenia stanowi udokumentowane polecenie Podmiotu przetwarzającego, o którym mowa w art. 28 ust. 3 lit. a Rozporządzenia.
2. W sprawach nieuregulowanych postanowieniami niniejszej Umowy Powierzenia zastosowanie będą mieć właściwe w tym zakresie przepisy prawa polskiego.

3. Wszelkie zmiany, uzupełnienia lub rozwiązanie niniejszej Umowy Powierzenia wymagają zachowania formy pisemnej pod rygorem nieważności.
4. W przypadku zmian w przepisach prawa stanowiących podstawę przetwarzania danych osobowych na podstawie niniejszej Umowy Powierzenia, Podprocesor przed wejściem w życie zmian, sformułuje rekomendacje dla ewentualnych zmian w niniejszej Umowie Powierzenia, zgodnie z zasadami określonymi w Umowie Głównej.
5. Strony zgodnie oświadczają, iż w przypadku sporów powstałych na tle realizacji niniejszej Umowy Powierzenia 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 dla siedziby Podmiotu przetwarzającego.
6. Niniejsza Umowa Powierzenia została sporządzona w 2 jednobrzmiących egzemplarzach, w tym 1 egzemplarze dla Podmiotu przetwarzającego i 1 egzemplarz dla Podprocesora.

Podmiot przetwarzający	**Podprocesor**
.....	.....

Załączniki:
1. Środki odpowiedniego zabezpieczenia powierzonych do przetwarzania danych osobowych stosowane przez podmiot przetwarzający;
2. Wykaz podmiotów podprzetwarzających (podprocesorów);
3. Klauzula informacyjna.

Załącznik nr 1 do umowy podpowierzenia przetwarzania danych osobowych

ŚRODKI ODPOWIEDNIEGO ZABEZPIECZENIA POWIERZONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH STOSOWANE PRZEZ PODMIOT PRZETWARZAJĄCY

Środki ochrony fizycznej powierzonych do przetwarzania danych osobowych		
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, objęty jest 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, w czasie nieobecności zatrudnionych tam pracowników jest 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 szafie 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 szafie 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: ▪ technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania; ▪ opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych; ▪ sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji; ▪ sprzętowych i programowych środków ochrony poufności danych osobowych przesyłanych drogą elektroniczną (środków ochrony transmisji); ▪ sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzania danych osobowych.		
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 wymuszające 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 osobowych 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 Procesora w celu ochrony danych osobowych, takich jak: instrukcje, szkolenia, zobowiązania.		
1	☒	Osoby zatrudnione przy przetwarzaniu danych osobowych 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 osobowe.
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.
6	☐	Wyznaczono inspektora ochrony danych osobowych, nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych: ..... *(imię i nazwisko, nr telefonu, adres e-mail inspektora ochrony danych).*
7	☒	Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie w przedmiotowym zakresie.
8	☒	Prowadzona jest ewidencja/rejestr osób upoważnionych do przetwarzania danych osobowych.

9	☒	Została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych, spełniająca wymagania określone dla środków organizacyjnych, o których mowa w art. 24 ust. 2 Rozporządzenia.

Załącznik nr 2 do umowy powierzenia przetwarzania danych osobowych

WYKAZ PODMIOTÓW PODPRZETWARZAJĄCYCH (PODPROCESORÓW)

PODPROCESOR	ŚWIADCZONE USŁUGI
..... *(nazwa podprocesora)*	..... *(usługa)*
..... *(nazwa podprocesora)*	..... *(usługa)*
..... *(nazwa podprocesora)*	..... *(usługa)*
..... *(nazwa podprocesora)*	..... *(usługa)*
..... *(nazwa podprocesora)*	..... *(usługa)*

Załącznik nr 3 do umowy podpowierzenia przetwarzania danych osobowych

KLAUZULA INFORMACYJNA

Program Operacyjny Infrastruktura i Środowisko (POIiŚ) 2014-2020

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych osobowych) (dalej jako: RODO) Państwowe Gospodarstwo Wodne Wody Polskie informuje, iż:

1. Administratorem przetwarzanych danych osobowych jest Minister Finansów, Funduszy i Polityki Regionalnej, 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.

   Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej z siedzibą przy ul. Konstruktorskiej 3a, 02-673 Warszawa jest podmiotem przetwarzającym dane osobowe na podstawie porozumienia zawartego z administratorem (tzw. procesorem).

2. Dane osobowe przetwarzane będą na potrzeby realizacji PO IiŚ 2014-2020, w szczególności w celu realizacji i rozliczenia projektu/ów w ramach działań Programu Operacyjnego Infrastruktura i Środowisko 2014-2020.

3. 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.

4. Przetwarzanie danych osobowych odbywa się w związku:

   1) z realizacją ciążącego na administratorze obowiązku prawnego (art. 6 ust. 1 lit. c RODO), wynikającego z następujących przepisów prawa:

      - 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,

      - **rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr** 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 27 sierpnia 2009 r. o finansach publicznych,

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).

5. Minister może przetwarzać różne rodzaje danych, 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 kontaktowe, w tym w szczególności: adres e-mail, nr telefonu, nr fax, adres do korespondencji,

3) dane o charakterze finansowym, w tym szczególności: nr rachunku bankowego, kwotę przyznanych środków,

6. 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.

7. 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.

8. 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.

9. 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 do przenoszenia swoich danych (art. 20 RODO) - jeśli przetwarzanie odbywa się na podstawie umowy: w celu jej zawarcia lub realizacji (w myśl art. 6 ust. 1 lit. b RODO), oraz w sposób zautomatyzowany,
- prawo wniesienia sprzeciwu wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO),

10. 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.
11. W przypadku pytań, kontakt z Inspektorem Ochrony Danych Osobowych Ministerstwa Funduszy i Polityki Regionalnej jest możliwy:
    - pod adresem: ul. Wspólna 2/4, 00-926 Warszawa,
    - pod adresem: e-mail: *IOD@mfipr.gov.pl*
12. Dane osobowe nie będą objęte procesem zautomatyzowanego podejmowania decyzji, w tym profilowania.