Załącznik Nr 2
do Umowy głównej
nr KZGW/KLL3519/2019

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu …….. w ……, pomiędzy:

Państwowym Gospodarstwem Wodnym Wody Polskie Krajowym Zarządem Gospodarki Wodnej z siedzibą w Warszawie, 00-844 Warszawa, ul. Grzybowska 80/82, NIP: 527-282-56-16, REGON: 368302575, reprezentowanym przez:
Dyrektora Departamentu Zarządzania Zasobami Ludzkim – panią **Urszulę Kopcińską**
zwaną dalej **Administratorem,**
a
…… z siedzibą w ……., adres: ……., 04-386 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod nr ……., której dokumentacja przechowywana jest przez Sąd Rejonowy dla m.st. ……, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, o kapitale zakładowym …….. zł (opłaconym w całości) i numerze NIP: ……., **reprezentowaną przez: ……**
zwaną dalej **„Procesorem”,**

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

§1

Definicje

Ilekroć w niniejszej umowie powierzenia przetwarzania danych osobowych 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 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;
3. **„systemie informatycznym”** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
4. **„Umowie”** – rozumie się przez to niniejszą umowę powierzenia przetwarzania danych osobowych;
5. **„Umowie Głównej”** – rozumie się przez to umowę z dnia …… nr KZGW/KLL/2019/…… zawartą przez Strony niniejszej Umowy, której przedmiotem jest przeprowadzenie szkolenia na rzecz pracowników Państwowego Gospodarstwa Wodnego Wody Polskie z zakresu „MS Excel – poziom podstawowy, średniozaawansowany i zaawansowany”.

6. **„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.

7. **„Ustawie o ochronie danych osobowych”** lub **„UODO**” – rozumie się przez to Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).

§2

Przedmiot Umowy

1. Administrator i Procesor oświadczają, że zawarli w dniu ..... Umowę Główną nr KZGW/KLL/2019/…….. w związku z którą będą przetwarzane dane osobowe.
2. Niniejsza umowa powierzenia przetwarzania danych (Umowa) jest akcesoryjna względem Umowy Głównej i reguluje wzajemny stosunek stron i obowiązki w zakresie przetwarzania danych osobowych w związku z obowiązkami Procesora wynikającymi z Umowy Głównej.
3. Przetwarzanie danych osobowych odbywać się będzie w zgodzie i w oparciu o:
   a. Ogólne rozporządzenie o ochronie danych.
   b. Ustawę o ochronie danych osobowych,
4. Przedmiotem Umowy jest powierzenie Procesorowi przez Administratora, przetwarzania danych osobowych, w związku z realizacją obowiązków określonych w Umowie Głównej.
5. Administrator oświadcza, że jest administratorem danych[1], o których mowa w §3 ust. 1 Umowy.
6. Podmiotem przetwarzającym[2], któremu Administrator powierza przetwarzanie danych osobowych jest Procesor.
7. Administrator powierza Procesorowi przetwarzanie danych osobowych, a Procesor zobowiązuje się do ich przetwarzania zgodnego z prawem, Umową Główną i niniejszą Umową.
8. Procesor będzie przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie.

§3

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Procesorowi przetwarzanie danych osobowych pracowników tj.: imię i nazwisko, służbowy adres e-mail, służbowy numer telefonu.
2. Powierzenie nie obejmuje danych osobowych, o których mowa w art. 9-10 Ogólnego rozporządzenia o przetwarzaniu danych osobowych.
3. Cel i zakres powierzenia przetwarzania danych osobowych wynika bezpośrednio i ogranicza się wyłącznie do zadań wynikających z zawartej Umowy Głównej, tj.: przeprowadzenie szkolenia na rzecz pracowników Państwowego Gospodarstwa Wodnego Wody Polskie z zakresu „MS Excel – poziom podstawowy, średniozaawansowany i zaawansowany”.
4. Na danych osobowych, z związku z realizacją celu, o którym mowa w ust. 3, będą wykonywane w szczególności następujące operacje: ***zbieranie, utrwalanie, porządkowanie, przechowywanie, przeglądanie, wykorzystywanie, usuwanie, niszczenie***, a także czynności

[1] W rozumieniu art. 4 ust 7 RODO
[2] W rozumieniu art. 4 ust 8 RODO

polegające na tworzeniu kopii bezpieczeństwa oraz czynności związane z odtworzeniem danych z kopii bezpieczeństwa.

5. Przetwarzanie powierzonych danych odbywać się będzie z wykorzystaniem systemów informatycznych.

6. Administrator nie wyraża zgody na przetwarzanie danych osobowych poza EOG.

§4

Obowiązki Procesora

1. Procesor będzie przetwarzał powierzone mu dane osobowe na warunkach i zgodnie z treścią obowiązujących w tym zakresie przepisów prawa.

2. Procesor oświadcza, że przetwarzanie powierzonych mu danych osobowych, będzie odbywało się z poszanowaniem przepisów Ogólnego rozporządzenia o ochronie danych oraz wydanych na jego podstawie krajowych przepisów z zakresu ochrony danych osobowych.

3. W związku z powierzeniem przetwarzania danych osobowych Procesor zobowiązuje się do:

   3.1. przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora; Za udokumentowane polecenie uznaje się zadania zlecone do wykonywania w drodze Umowy Głównej.

   3.2. dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie, o których mowa w art. 29 RODO oraz przeszkolone z zakresu przepisów dotyczących ochrony danych osobowych,

   3.3. zobowiązania osób upoważnionych do przetwarzania danych osobowych do zachowania tajemnicy,

   3.4. 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 technicznych i organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu temu ryzyku, w tym między innymi w stosownym przypadku:

      3.4.1. pseudonimizacji i szyfrowania danych osobowych;

      3.4.2. zapewnienia bezpiecznego (kryptograficznie zabezpieczonego) transferu danych w procesie świadczonej usługi - wdrożenia mechanizmów uwierzytelniania oraz nadzoru działań w systemie przez odnotowywanie zdarzeń na przetwarzanych danych (logowanie działań);

      3.4.3. zapewnienia w działaniach serwisowych (w tym wymiana uszkodzonych zasobów dyskowych), by dostęp do zasobów był ograniczony do osób upoważnionych;

      3.4.4. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

      3.4.5. zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

      3.4.6. regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;

3.5. aktywnej współpracy z Administratorem przez cały okres trwania powierzenia przetwarzania danych osobowych, która w szczególności polega na tym, iż Procesor 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 Administratorowi wywiązywać się z obowiązków w zakresie zagwarantowania bezpieczeństwa danych osobowych.

4. Procesor realizując zadania wynikające z Umowy Głównej:

4.1. zastosuje odpowiednie środki organizacyjne w celu zgodnego z przepisami przetwarzania danych osobowych";

4.2. zastosuje środki zabezpieczenia określone w art. 32 RODO - wdrożone środki zabezpieczenia muszą być adekwatne do zidentyfikowanych ryzyk dla zakresu powierzonego przetwarzania danych;

4.3. udzieli pomocy Administratorowi w zakresie;

a. realizacji obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;

b. zapewnienia realizacji obowiązków wynikających z art. 32-36 RODO;

4.4. po zakończeniu przetwarzania danych osobowych niezwłocznie zwróci powierzone mu dane lub dokona ich zniszczenia chyba, że obowiązujące przepisy prawa nakazują przechowywanie tych danych osobowych;

4.5. wyznaczy Inspektora Ochrony Danych (o ile wynika z obowiązku prawnego) oraz, rozpocznie prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zgodnie z wymaganiami art. 30 ust 2 RODO i pisemnie poinformuje o tym Administratora.

5. Procesor zobowiązuje się niezwłocznie (nie później niż w ciągu 36 godzin) zawiadomić Administratora o:

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

5.2. każdym nieupoważnionym dostępie do danych osobowych, wycieku danych;

5.3. 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 upoważniony przez Administratora.

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

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

§5

Prawo kontroli

1. Administrator ma prawo do kontroli przetwarzania przez Procesora powierzonych mu danych osobowych z punktu widzenia zgodności tego przetwarzania z przepisami prawa oraz postanowieniami Umowy w postaci audytu realizowanego przez Administratora lub audytora upoważnionego przez Administratora.
2. Procesor zobowiązany jest:
   2.1. udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków spoczywających na Podmiocie Przetwarzającym;
   2.2. umożliwić Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych;
   2.3. zastosować się do zaleceń poaudytowych przekazanych przez Administratora.
3. Informacja o terminie i zakresie audytu, o którym mowa w ust. 1 powyżej, będzie przekazana Procesorowi z co najmniej 3 dniowym wyprzedzeniem. Administrator będzie realizował prawo do audytu (w tym inspekcji) w godzinach pracy Procesora bez zakłócenia jego czynności biznesowych po wcześniejszym ustaleniu terminu. Audyt powinien zostać przeprowadzony z poszanowaniem zasady proporcjonalności działań oraz nie prowadzić grozić lub skutkować naruszeniem tajemnicy przedsiębiorstwa Procesora, jego podwykonawców lub klientów. Przedstawiciel procesora ma prawo być obecny przy wszystkich czynnościach związanych z przeprowadzeniem audytu nie częściej niż raz na pół roku. Nienależnie od powyższego w każdorazowym wypadku stwierdzenie naruszenia ochrony danych osobowych administratorowi przysługiwać będzie dodatkowy audyt.
4. Procesor umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora, przeprowadzanie audytu, o którym mowa w ust. 1 i przyczynia się do niego. W szczególności, Procesor zobowiązany jest udostępnić wgląd do wszystkich materiałów oraz systemów, w których realizowane jest przetwarzanie danych Administratora oraz umożliwić dostęp do pracowników zaangażowanych w ich przetwarzanie.
5. Administrator lub audytor upoważniony przez Administratora, 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

Odpowiedzialność Procesora

1. Podmiot Przetwarzający oświadcza, że wdrożył i stosuje środki techniczne i organizacyjne co najmniej w takim zakresie, w jakim zostało to określone w Załączniku nr 1 do Umowy Powierzenia i zawsze w stopniu nie mniejszym niż wymagany na mocy art. 32 RODO.
2. Procesor jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności udostępnienie ich osobom nieuprawnionym.
3. W przypadku ujawnienia okoliczności uznanych przez Administratora za uchybienia w zakresie wykonywania Umowy lub obowiązujących w tym zakresie przepisów prawa, Procesor

zobowiązuje się do ich usunięcia w wyznaczonym terminie. W razie niezastosowania się przez Procesora do wydanych przez Administratora wytycznych, Administrator jest uprawniony do nałożenia kary umownej w wysokości 1000 zł (słownie: tysiąc zł) za każdy przypadek stwierdzonej nieprawidłowości, przy czym łączna wysokość nałożonych kar nie będzie większa niż 10% wartości Umowy Głównej, o której mowa w § 2 pkt. 1.

4. Jeżeli podobne nieprawidłowości zostaną ujawnione ponownie lub nie zostanie dotrzymany termin usunięcia uchybień (pkt.3 wyżej), Administrator jest uprawniony do nałożenia kary umownej bez wyznaczania terminu do ich usunięcia.

5. W przypadku naruszenia postanowień Umowy lub obowiązujących w tym zakresie przepisów prawa z przyczyn leżących po stronie Procesora, w następstwie, czego Administrator, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Procesor zobowiązuje się do zapłaty Administratorowi równowartości roszczeń osób trzecich, kar oraz równowartości kosztów postępowania sądowego, które będą wynikiem nieprawidłowego działania Procesora.

6. Administratorowi przysługuje względem Procesora prawo do dochodzenia odszkodowania przewyższającego zastrzeżoną karę umowną – do pełnej wysokości poniesionej szkody.

§7

Usunięcie lub zwrot danych osobowych

1. W terminie do 14 dni roboczych od dnia zakończenia Umowy, Procesor 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.

2. Powierzenie przetwarzania danych osobowych trwa do upływu wyżej wskazanego terminu.

§8

Czas trwania i wypowiedzenie Umowy

1. Umowa zawarta jest na czas określony odpowiadający okresowi obowiązywania Umowy Głównej

2. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym z dniem rozwiązania lub wygaśnięcia Umowy Głównej, a także, gdy Procesor:

   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 Administratora nie zwalnia Procesora od zapłaty należnych kar umownych i odszkodowania.

§9

Pozostałe postanowienia

1. Przetwarzanie danych dozwolone jest wyłącznie w celu określonym w §3 ust. 3 Umowy.

2. Wykorzystanie przez Procesora danych Administratora w celach innych niż określone Umową wymaga każdorazowo pisemnej zgody Administratora.

§10

Postanowienia końcowe

1. Umowa stanowi udokumentowanie polecenie Administratora, o którym mowa w art. 28 ust. 3 lit. a Ogólnego rozporządzenia o ochronie danych.
2. W sprawach nieuregulowanych postanowieniami Umowy zastosowanie będą mieć właściwe w tym zakresie przepisy prawa polskiego.
3. Wszelkie zmiany, uzupełnienia lub rozwiązanie Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
4. W przypadku zmian w przepisach prawa stanowiących podstawę przetwarzania danych na podstawie Umowy, Procesor przed wejściem w życie zmian sformułuje rekomendacje dla ewentualnych zmian w Umowie, zgodnie z zasadami określonymi w Umowie Głównej.
5. 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 dla siedziby Administratora.
6. Umowa została sporządzona w czterech jednobrzmiących egzemplarzach, trzech dla Administratora i jednym dla Procesora.

Administrator ……	**Procesor:** ……

Załącznik nr 1

Środki techniczne i organizacyjne …… w zakresie bezpieczeństwa danych

1. **Mechanizmy kontroli dostępu fizycznego**

- Ustanowienie kontroli dostępu fizycznego do pomieszczeń (np. karta magnetyczna, karta chip, czytnik ID)
- Procedury dotyczące nadawania fizycznego dostępu zapewniające weryfikację tożsamości i zakresu nadawanego dostępu
- Posiadanie działającego systemu alarmowego, systemu CCTV na terenie siedziby
- Zabezpieczenie komputerów osobistych oraz innych urządzeń przetwarzających dane przed dostępem osób niepowołanych

2. **Mechanizmy kontroli dostępu logicznego**

- Zapewnienie jednoznacznej identyfikacji działań w systemach informatycznych za pomocą unikalnego ID użytkownika
- System zarządzania hasłami (minimalna długość, złożoność, częstotliwość zmiany, możliwość powtórnego użycia hasła, szyfrowanie przechowywanych haseł)
- Automatyczne blokowanie ekranu po okresie bezczynności użytkownika
- Monitorowanie nieudanych prób zalogowania się do systemu
- Szyfrowanie komunikacji zawierającej dane osobowe lub przesyłanie zaszyfrowanych danych osobowych

3. **Kontrola nadawanych uprawnień do systemów informatycznych**

- Posiadanie wewnętrznej procedury nadawania uprawnień
- Proces monitorowania oraz logowania dostępów do systemów informatycznych
- Procedury nadawania, odbierania, modyfikacji dostępów do systemów informatycznych

4. **Kontrola wycieków informacji**

- Szyfrowanie danych
- Rejestrowanie aktywności użytkowników

5. **Monitorowanie zmian danych w systemach informatycznych**

- Rejestrowanie oraz monitorowanie aktywności użytkowników w systemach informatycznych

- Przeglądy aktywności użytkowników

6. Zapewnienie dostępności danych

- Proces tworzenia kopii zapasowej danych
- Zastosowanie zasilaczy UPS
- Posiadanie lub wykorzystywanie centrum przetwarzania danych (ang. data center)
- Systemy antywirusowe i firewalle
- Stosowanie kopii lustrzanej twardych dysków/disk mirroring'u (np. wykorzystując technologię RAID)

7. Separacja

- Separacja środowisk baz danych
- Stosowanie reguł rozdziału obowiązków
- Rozdzielanie sieci informatycznej
- Ograniczenie dostępu do Danych Osobowych