Załącznik nr 2

Umowa nr

podpowierzenia przetwarzania danych osobowych

zawarta w dniu ..... roku w Węglińcu pomiędzy:

Skarbem Państwa – Państwowym Gospodarstwem Leśnym Lasy Państwowe
Nadleśnictwem Węgliniec z siedzibą w Węglińcu
ul. Piłsudskiego 6,
59 – 940 Węgliniec
NIP: 6150025281,
REGON: 931024126
reprezentowanym
przez:
Nadleśniczego – Marka Kmiecia
przy kontrasygnacie Głównego Księgowego – Krzysztofa Lenkiewicza
zwanym w dalszej części umowy **„Powierzającym"**

a

NIP:
zwany w dalszej części **„Przyjmującym"**,

Mając na uwadze, że Nadleśnictwu Węgliniec zostało powierzone przetwarzanie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości, zaś ..... uprawnione jest do dalszego powierzenia przetwarzania danych osobowych z ww. zbioru, a Strony zawarły umowę, w związku z wykonywaniem której niezbędne jest przetwarzanie danych osobowych imieniem Administratora przez Podmiot Przetwarzający, który to Podmiot Przetwarzający zapewnia należyte gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przepisów prawa i chroniło prawa osób, których dane dotyczą – Strony postanowiły zawrzeć niniejszą umowę podpowierzenia przetwarzania danych (zwaną dalej: Umową) następującej treści:

Niniejsza umowa została zawarta na podstawie przepisów ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125), zwanego w dalszej części „**Ustawą**".

§ 1.

Podpowierzenie przetwarzania danych osobowych

1. Powierzający powierza Przyjmującemu, w trybie art. 34 Ustawy, dane osobowe do przetwarzania na zasadach i w celu określonym w niniejszej Umowie.
2. Administratorem danych, o których mowa a niniejszej umowie jest Główny Inspektor Straży Leśnej, ul. Grójecka 127, 02-124 Warszawa.
3. Nadleśnictwo Węgliniec oświadcza, iż przetwarza dane w związku z zapobieganiem i zwalczaniem przestępczości na podstawie umowy powierzenia nr 421/2020 zawartej pomiędzy Głównym Inspektorem Straży Leśnej a Nadleśnictwem Węgliniec.
4. Powierzający oświadcza, że jest Podmiotem przetwarzającym danych, które powierza Przyjmującemu.
5. Przyjmujący zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
6. Przyjmujący oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Ustawy, określone w § 3 ust. 1 niniejszej Umowy.

§ 2.

Zakres i cel przetwarzania danych

1. Przyjmujący będzie przetwarzał powierzone na podstawie niniejszej Umowy dane. Dane te i kategoria osób zostały określone w załączniku nr 1 do umowy.
2. Powierzone przez Powierzającego dane osobowe będą przetwarzane przez Przyjmującego wyłącznie w charakterze i celu określonym w załączniku nr 1.

§ 3.

Obowiązki i prawa Stron

1. Przyjmujący zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień

bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Ustawy.

2. Przyjmujący określa ogólny opis zabezpieczeń w załączniku nr 2.
3. Przyjmujący zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Przyjmujący zobowiązuje się zapewnić zachowanie w tajemnicy (poufności, o której mowa w art. 34 ust. 5 pkt 3 Ustawy) przetwarzanych danych oraz środków technicznych ich zabezpieczenia przez osoby, które upoważnia do przetwarzania danych osobowych, w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich u Przyjmującego, jak i po jego ustaniu.
5. Przyjmujący, po zakończeniu świadczenia usług związanych z przetwarzaniem, zobowiązany jest do działania określonego w załączniku nr 1.
6. W miarę możliwości, Przyjmujący pomaga Administratorowi oraz Powierzającemu, w niezbędnym zakresie, wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków, określonych w art. 32, 37, 38-40, 43-45 Ustawy.
7. Przyjmujący, po stwierdzeniu naruszenia ochrony danych osobowych, niezwłocznie zgłasza je Powierzającemu, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, a zgłoszenie winno odpowiadać wymogom art. 44 Ustawy.
8. W celu realizacji obowiązków o których mowa w ust. 6 i 7 powyżej, Przyjmujący jest zobowiązany do zabezpieczenia dowodów, które pomogą ustalić i wyjaśnić szczegóły naruszenia, w tym chwilę zdarzenia, osoby odpowiedzialne, charakter naruszenia oraz jego skalę i ewentualne negatywne skutki, osoby poszkodowane.
9. Powierzający, ma prawo kontroli, czy środki zastosowane przez Przyjmującego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, spełniają postanowienia Umowy.
10. Powierzający realizować będzie prawo kontroli, zgodnie z załącznikiem nr 1.
11. Przyjmujący zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli, w terminie wskazanym przez Powierzającego.
12. Przyjmujący udostępnia Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków, określonych w art. 34 Ustawy.

§ 4.

Dalsze powierzenie danych do przetwarzania

1. Przyjmujący nie jest uprawniony powierzyć do dalszego przetwarzania dane osobowe powierzone mu przez Powierzającego. na postawie Umowy – bez uprzedniej zgody wyrażonej na zasadach określonych w art. 34 ust. 5 pkt 7 oraz ust. 6 Ustawy.
2. Dalsze powierzenie danych do przetwarzania, odbywa się na podstawie umowy, która spełnia wymagania określone przepisami Ustawy, a Przyjmujący może powierzyć dane osobowe, objęte niniejszą Umową, do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy zawartej pomiędzy stronami i po uzyskaniu uprzedniej, pisemnej zgody Powierzającego.
3. Na wypadek dalszego powierzenia do przetwarzania danych powierzonych Przyjmującemu przez Powierzającego – dalszy przetwarzający winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot Przetwarzający w Umowie oraz wynikające z przepisów prawa, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Ustawy.
4. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Powierzającego, chyba że obowiązek taki nakłada na Przyjmującego przepis prawa. W takim przypadku, przed rozpoczęciem przetwarzania, Przyjmujący informuje Powierzającego o tym obowiązku prawnym, o ile przepis prawa nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
5. Przyjmujący ponosi pełną odpowiedzialność wobec Powierzającego za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
6. Podmioty, którym dane Powierzającego zostały powierzone przez Przyjmującego, wymienia się w załączniku nr 1.

§ 5.

Odpowiedzialność Podmiotu przetwarzającego

1. Przyjmujący ponosi odpowiedzialność za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Przyjmujący zobowiązuje się do niezwłocznego poinformowania Powierzającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przyjmującego danych osobowych, określonych w Umowie, a także:
   a) o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przyjmującego;
   b) o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przyjmującego tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Powierzającego.
3. Przyjmujący odpowiada za szkody majątkowe lub niemajątkowe jakie powstały u Powierzającego. lub osób trzecich, w wyniku przetwarzania powierzonych Przyjmującemu danych osobowych, niezgodnego z przepisami prawa lub Umową.
4. Przyjmujący ponosi odpowiedzialność – jak za własne działania lub zaniechania – za działania lub zaniechania podmiotów, którym powierzył dalsze przetwarzanie danych powierzonych Podmiotowi Przetwarzającemu na podstawie Umowy.
5. W przypadku naruszenia przepisów prawa lub Umowy powierzenia, z przyczyn leżących po stronie Przyjmującego, w następstwie czego Powierzający zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany administracyjną karą pieniężną - Przyjmujący zobowiązuje się zrekompensować Powierzającemu poniesione straty i koszty z tego tytułu. Przyjmujący może uwolnić się od obowiązku zapłaty odszkodowania, pokrycia strat i kosztów, jeżeli udowodni, że zdarzenie, które doprowadziło do powstania szkody, nie jest przez niego zawinione.

§ 6.

Czas obowiązywania Umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas określony w załączniku nr 1.
2. Każda ze stron może wypowiedzieć niniejszą Umowę, z zachowaniem okresu opisanego w załączniku nr 1.

§ 7.

Rozwiązanie umowy

1. Powierzający może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Przyjmujący:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli, nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z Umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi, bez zgody Administratora

§ 8.

Zasady zachowania poufności

1. Przyjmujący zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Powierzającego i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne"). Podjęte zobowiązanie pozostaje w mocy w czasie trwania i po zakończeniu przetwarzania w ramach powierzenia danych osobowych.
2. Przyjmujący oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Powierzającego, w innym celu niż wykonania Umowy, chyba że konieczność ujawnienia informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 9.

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej, pod rygorem nieważności.

2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, dla każdej ze Stron.
3. W sprawach nieuregulowanych, zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy, będzie sąd właściwy dla Powierzającego.
5. Jeżeli Przyjmujący naruszy przepisy Ustawy w zakresie określania celów lub sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania

Załączniki do umowy:

1. Załącznik nr 1 – szczegółowy zakres czynności przy usługach objętych umową.
2. Załącznik nr 2 - ankieta sprawdzająca podmiot przetwarzający.

Powierzający Przyjmujący

Załącznik nr 1 – szczegółowy zakres czynności przy usługach objętych umową.

1. Zakres powierzonych danych oraz kategoria osób:

2. *Charakter i cel przetwarzania powierzonych danych*

3. *Rodzaj działania z danymi po zakończeniu umowy*

4. *Kontrola podmiotu przetwarzającego*

5. *Podmioty dalszego podpowierzenia*

6. *Okres ważności umowy*

.

7. *Okres wypowiedzenia*

8. *Zastosowane zabezpieczenia – ogólny opis.*

Załącznik nr 2 - ankieta sprawdzająca podmiot przetwarzający.

Spełniane środki zabezpieczeń

Środki organizacyjne

- ☐ Został powołany Inspektor Ochrony Danych w celu przestrzegania zasad umieszczonych w niniejszym dokumencie.
- ☐ **Został powołany Administrator Systemu Informatycznego w celu zapewnienia prawidłowego funkcjonowania systemu informatycznego.**
- ☐ Została wprowadzona do stosowania dokumentacja bezpieczeństwa.
- ☐ **Każdy użytkownik, przetwarzający dane osobowe, posiada pisemne upoważnienie do przetwarzania danych osobowych.**
- ☐ **Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.**
- ☐ **Każdy użytkownik, który przetwarza dane osobowe, został przeszkolony z ochrony danych osobowych.**
- ☐ **Stosowana jest zasada „czystego biurka". Oznacza ona, że na stanowisku pracy powinny znajdować się tylko te dokumenty, na których obecnie pracownik pracuje. Inne dokumenty powinny być schowane.**
- ☐ **Dane w formie papierowej przechowywane są w zabezpieczonych pomieszczeniach.**
- ☐ **Do likwidowania zbędnych dokumentów służą niszczarki, dobierane według stopnia tajności danych.**

Środki techniczne

- ☐ **Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min.**
- ☐ Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
- ☐ Dane osobowe przechowywane są w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
- ☐ **Pomieszczenia, w których przetwarzane są zbiory danych osobowych, wyposażone są w system alarmowy przeciwwłamaniowy**
- ☐ **Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęte są systemem kontroli dostępu.**
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu, z zastosowaniem kamer przemysłowych.
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, w czasie nieobecności zatrudnionych tam pracowników, nadzorowany jest przez służbę ochrony.
- ☐ Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony.
- ☐ **Dane osobowe w formie papierowej przechowywane są w zamkniętej niemetalowej szafie.**
- ☐ Dane osobowe w formie papierowej przechowywane są w zamkniętej metalowej szafie.
- ☐ Dane osobowe w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej.
- ☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
- ☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie.
- ☐ Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej.
- ☐ Zbiory danych osobowych przetwarzane są w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach.
- ☐ **Pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.**
- ☐ Dokumenty zawierające dane osobowe, po ustaniu przydatności, są niszczone w sposób mechaniczny, za pomocą niszczarek dokumentów
- ☐ Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.
- ☐ Komputer służący do przetwarzania danych osobowych, nie jest połączony z lokalną siecią komputerową.
- ☐ Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

- ☐ **Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.**
- ☐ **Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.**
- ☐ 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.
- ☐ Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.
- ☐ Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
- ☐ **Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.**
- ☐ Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
- ☐ Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
- ☐ Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
- ☐ Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.
- ☐ Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
- ☐ **Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.**
- ☐ **Użyto system Firewall do ochrony dostępu do sieci komputerowej.**
- ☐ Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
- ☐ **Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.**
- ☐ **Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.**
- ☐ **Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.**
- ☐ **Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.**
- ☐ 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.