

Umowa powierzenia przetwarzania danych osobowych

DC.....

zawarta dnia r. pomiędzy:

jednostkami organizacyjnymi Państwowego Gospodarstwa Leśnego Lasy Państwowe
(zwana dalej „Umową”)

**Zakładem Informatyki Lasów Państwowych z siedzibą w Sękocinie Starym, ul. Leśników
21c, 05-090 Raszyn**

Reprezentowanym przez:

..... – **Dyrektora Zakładu Informatyki Lasów
Państwowych**

Zwanym w dalszej części umowy „**Administratorem danych**”

a

.....
.....
Reprezentowanym przez:

.....
Zwany w dalszej części umowy „**Podmiotem przetwarzającym**”

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z zawarciem z dnia Umowy Głównej nr DZ....., na dostawę, wdrożenie i utrzymanie systemu informatycznego pn. System Informatyczny Straży Leśnej (nr postępowania DZ.270.104.2023) w związku z wykonywaniem której niezbędne będzie przetwarzanie przez Wykonawcę zwanego dalej „Podmiotem przetwarzającym” danych osobowych w imieniu Zamawiającego zwanego dalej „Administratorem danych”, Administrator danych powierza w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania przez Podmiot przetwarzający, na zasadach i w zakresie określonym niniejszą umową („Umowa”).
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane:
 - a) Pracowników PGL Lasy Państwowe w postaci:
Imiona, nazwiska, nazwisko rodowe, dane adresowe, stanowisko służbowe oraz innych danych wynikających min. z zawartych umów i wymogów przepisów prawa

- b) Interesantów i klientów PGL Lasy państwowe w szczególności:
Imion, nazwisk, PESEL, nr dokumentów tożsamości, dane o uprawnieniach do kierowania pojazdów, danych adresowych, numerów telefonów kontaktowych, dane pojazdu, dane o właścicielu pojazdu, dane ubezpieczeniowe oraz innych danych wynikających z wymogów przepisów prawa.
2. Powierzone przez Administratora danych, dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji usług/dostaw, wdrożenia i utrzymania systemu informatycznego pn. System Informatyczny Straży Leśnej (nr postępowania DZ.270.104.2023) do umowy głównej (DZ....)
 3. Rodzaj powierzonych danych obejmuje wszelkie rodzaje danych w tym tzw. szczególne kategorie danych oraz dane osobowe dotyczące wyroków skazujących i czynów zabronionych.
 4. Z uwagi na cel powierzenia danych osobowych, przetwarzanie będzie miało charakter stały i ciągły.
 5. Podmiot przetwarzający w zakresie realizacji celu określonego w ust. 2 jest uprawniony do wykonywania następujących operacji na danych”
 - a) zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, usuwanie i niszczenie.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem danych na osobowych w ramach umowy, usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba, że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Czynności zwrotu, zniszczenia każdorazowo będą udokumentowane przez Podmiot przetwarzający protokołem zniszczenia. Zamawiający poinformuje pisemnie Podmiot przetwarzający o konieczności usunięcia danych osobowych w terminie nie dłuższym niż 7 dni od daty wygaśnięcia/rozwiązania umowy głównej DZ
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki nie później niż 48 godzin od stwierdzenia naruszenia zgłasza je Administratorowi Danych na adres e-mail: iod@zilp.lasy.gov.pl oraz biuro@zilp.lasy.gov.pl. Podmiot przetwarzający zobowiązany jest do zgłoszenia każdego naruszenie Danych

Osobowych powierzonych Umową, którego będzie uczestnikiem zgodnie z art. 33 Rozporządzenia.

8. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych wyłącznie na podstawie niniejszej Umowy lub na podstawie innego udokumentowane polecenia Administratora Danych, za jakie uważa się polecenie przekazane drogą pisemną lub elektroniczną.
9. Podmiot przetwarzający obowiązany jest do wdrożenia takich środków technicznych i organizacyjnych, które umożliwią udostępnienie danych jedynie uprawnionym podmiotom i jednostkom organizacyjnym PGL Lasy Państwowe, a w szczególności, o ile znajduje to zastosowanie, jednostkom nadrzędnym PGL Lasy Państwowe.
10. Administrator danych nie wyraża zgody na użycie narzędzi firm trzecich, z których na co dzień korzysta Podmiot przetwarzający, w szczególności w zakresie korespondencji realizowanej za pomocą e-maila i rozwiązań chmurowych. Tym samym nie wyraża zgody na incydentalne przetwarzanie danych osobowych przez te firmy i ich przedstawicieli. Dane osobowe będą przechowywane na serwerach zlokalizowanych w Unii Europejskiej i nie mogą być przekazane - na podstawie standardowych klauzul ochrony danych - do państwa trzeciego."

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum siedmiodniowym wyprzedzeniem informuje o przystąpieniu do kontroli jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
5. Osoby fizyczne prowadzące działalność gospodarczą, współpracujące z Podmiotem przetwarzającym na podstawie umów cywilno-prawnych są traktowane jak personel Podmiotu przetwarzającego i nie stanowią innych podmiotów – dalszych przetwarzających (podwykonawców) w rozumieniu Rozporządzenia, w odniesieniu do niniejszej Umowy.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

Umowa zostaje zawarta na czas trwania umowy głównej **DZ....** wyłącznie w celu realizacji usług/dostaw, wdrożenia i utrzymania systemu informatycznego pn. System Informatyczny Straży Leśnej (nr postępowania **DZ270.104.2023**). Zawarcie niniejszej umowy ani jego wykonanie nie stanowi i nie będzie stanowić naruszenia żadnych umów zawartych przez Administratora Danych lub Podmiot Przetwarzający.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
 - a) Pomimo zobowiązania 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 Danych;

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba, że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.

2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych.
4. Umowa wchodzi w życie z dniem podpisania przez ostatnią ze Stron, nie później zaś niż przed dniem podjęcia przez Podmiot przetwarzający czynności wymagających przetwarzania danych osobowych w celu realizacji przez Podmiot przetwarzający zadań objętych Umową główną DZ

Załączniki:

1. **załącznik nr 1** – Wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający;
2. **załącznik nr 2** – Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów).

Administrator danych

Podmiot przetwarzający

Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający

PYTANIE	ODPOWIEDŹ
Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy?	
Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia?	
Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	

Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?	
Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji?	
Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany?	
Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?	
Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby?	
Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób?	
Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	
Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka?	

Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	
Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach?	
Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane?	
Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych?	
Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu?	
Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych?	
Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe?	
Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych?	
Gdzie są przechowywane kopie zapasowe?	
Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania?	
Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design?	
Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default?	
Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?	
Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	

Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów)

Przy wykonaniu Umowy Procesor korzysta z usług następujących podprocesorów:

PODPROCESOR	ADRES SIEDZIBY