

Umowa powierzenia przetwarzania danych osobowych

UMOWA Nr
/wzór/

zawarta w dniu roku, w Warszawie, pomiędzy:

Wojewódzkim Funduszem Ochrony Środowiska i Gospodarki Wodnej w Warszawie z siedzibą przy ul. Ogrodowej 5/7 w Warszawie (00-893), NIP: 525-20-88-391, REGON: 142 148 155, reprezentowanym przez:

..... – **Prezesa Zarządu**,
zwanym w dalszej części „**Administratorem**”,

.....

a

.....,

z siedzibą w, zarejestrowanym w pod numerem, posiadającym numer NIP: oraz numer REGON:, reprezentowanym przez:

.....,
zwanym w dalszej części „**Podmiotem przetwarzającym**”,
zwanym również „**Stroną**” lub wspólnie „**Stronami**”.

§ 1.

Określenia wymienione w treści niniejszej umowy zostały wyjaśnione w art. 4 Rozporządzenia Parlamentu Europejskiego i Rady 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, zwane dalej RODO).

§ 2.

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 RODO, dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO, Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (zwana dalej Ustawą) oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi prawa.

§ 3.

Zakres i cel przetwarzania danych

1. Powierzone przez Administratora dane będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy nr z dnia w sprawie..... (dalej zwana Umową główną).
2. Kategorie osób: wnioskodawcy/beneficjenci, pełnomocnicy, kandydaci do pracy, pracownicy, stażyści/praktykanci, kontrahenci, kontrolerzy i inne osoby, których dane będą przetwarzane w związku z realizacją Umowy głównej.
3. Rodzaj danych: dane identyfikacyjne, adresowe, kontaktowe, (dane zwykłe, szczególne kategorie danych, dane nieustrukturyzowane) i inne, które będą przetwarzane w związku z realizacją Umowy głównej.

4. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych osobowych: zbierania, utrwalania, wykorzystywania, organizowania, porządkowania, przechowywania, modyfikowania, pobierania, przeglądania, usuwania.
5. Podmiot przetwarzający będzie przetwarzał dane osobowe przez okres obowiązywania Umowy głównej.

§ 4.

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 32 RODO, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych.
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 przetwarzanych danych w tajemnicy (o której mowa w art. 28 ust. 3 pkt b RODO) 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, zwróci Administratorowi wszelkie dane osobowe i/lub usunie wszelkie ich istniejące kopie ze swoich zasobów oraz potwierdzi wykonanie tych czynności stosownym oświadczeniem po zakończeniu obowiązywania Umowy głównej.
6. W miarę możliwości Podmiot przetwarzający będzie pomagał Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz z obowiązków określonych w art. 32-36 RODO (dotyczących zapewnienia bezpieczeństwa danych osobowych, zgłaszania naruszeń ochrony danych osobowych, zawiadomienia osób, których dane dotyczą o naruszeniu ich danych osobowych, dokonania oceny skutków przetwarzania dla ochrony danych osobowych i konsultacji z organem nadzorczym).
7. Podmiot przetwarzający, bez zbędnej zwłoki, nie później jednak niż w ciągu 24 godzin po stwierdzeniu naruszenia, zgłosi Administratorowi każde naruszenie ochrony danych osobowych. Zgłoszenie powinno, oprócz elementów określonych w art. 33 ust. 3 RODO, zawierać informacje umożliwiające Administratorowi określenie czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.
8. Przed zawarciem niniejszej Umowy Podmiot przetwarzający zobowiązany jest przesłać do Administratora uzupełniony i podpisany formularz (oryginał) potwierdzający stosowanie środków organizacyjnych i technicznych w zakresie ochrony danych osobowych. Wzór formularza stanowi załącznik nr 1 do niniejszej umowy.

§ 5.

Prawo audytu lub inspekcji

1. Administrator zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo audytu lub inspekcji, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej umowy.
2. Zawiadomienie o zamiarze przeprowadzenia audytu lub inspekcji powinno być przekazane Podmiotowi przetwarzającemu na co najmniej 3 dni roboczych przed rozpoczęciem czynności.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas audytu lub inspekcji w terminie wskazanym przez Administratora, nie dłuższym niż 5 dni roboczych.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia przez Podmiot przetwarzający obowiązków określonych w art. 28 RODO.

§ 6.

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania niniejszej umowy, po uzyskaniu przedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania pod warunkiem, że wskazany podmiot daje gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, o których mowa w art. 28 ust. 4 Rozporządzenia, przy zachowaniu zasad i celu określonych w umowie. Podmiot przetwarzający we własnym zakresie reguluje z Podprocesorami materię, o której mowa w zdaniu 1.
3. W terminie 2 dni roboczych od podpisania niniejszej umowy Podmiot przetwarzający prześle Administratorowi za pośrednictwem poczty elektronicznej na adres iod@wfosigw.pl listę Podprocesorów, z którymi będzie współpracował w zakresie realizacji umowy. Administrator ma prawo wniesienia sprzeciwu w ciągu 2 dni roboczych od przekazania listy Podprocesorów biorących udział w przetwarzaniu danych w ramach realizacji umowy.
4. Podmiot przetwarzający (w przypadku zmiany listy Podprocesorów) przekaze Administratorowi niezwłocznie aktualną listę Podprocesorów biorących udział w przetwarzaniu danych w ramach realizacji umowy. Administrator ma prawo wniesienia sprzeciwu w ciągu 2 dni roboczych od przekazania ww. listy.
5. Administrator wnosi sprzeciw, o którym mowa w ust. 3 i 4, drogą elektroniczną na adres, z którego została wysłana do niego lista Podprocesorów. Do czasu upływu terminu na zgłoszenie sprzeciwu przez Administratora Podprocesor nie jest uprawniony do przetwarzania w imieniu i na rzecz Administratora, na zasadach i w celu określonym w niniejszej umowie.
6. Podmiot przetwarzający nie może przekazać powierzonych danych do państwa trzeciego.
7. Podwykonawca, o którym mowa w ust. 1 powyżej, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej umowie.

§ 7.

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
2. 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.
3. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w niniejszej umowie, o jakiegokolwiek 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 Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
4. Podmiot przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków wynikających z niniejszej umowy oraz przepisów z zakresu ochrony danych osobowych.

§ 8.

Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas realizacji Umowy głównej.

§ 9.

Rozwiązanie umowy

ADO może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

- 1) pomimo zobowiązania go do usunięcia istotnych uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
- 2) przetwarza dane osobowe w sposób niezgodny z umową;
- 3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody ADO.

§ 10.

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych dotyczących ADO lub jego kontrahentów, otrzymanych od ADO i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej, w jakich posiadanie wszedł w związku z realizacją niniejszej umowy (dane poufne), także po jej zakończeniu.
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 ADO w innym celu niż wykonanie niniejszej umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa – w takim przypadku Podmiot przetwarzający niezwłocznie poinformuje ADO o planowanym udostępnieniu danych osobowych.

§ 11.

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. W sprawach nieuregulowanych niniejszą umową zastosowanie będą miały przepisy Kodeksu cywilnego, RODO oraz Ustawy o ochronie danych osobowych.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla siedziby ADO.
4. Zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
5. Korespondencja wysyłana przez Strony na adresy siedzib wskazane w niniejszej Umowie, będzie uznana za doręczoną. W razie zmiany adresu siedziby Strony zobowiązują się do wzajemnego, pisemnego powiadomienia o zmianie adresu siedzib, pod rygorem uznania wysłanej korespondencji za doręczoną. Zmiana adresów siedzib nie powoduje zmiany niniejszej Umowy i nie wymaga podpisania aneksu.

Podmiot przetwarzający

Administrator

**Formularz potwierdzający stosowanie środków organizacyjnych i technicznych
w zakresie ochrony danych osobowych**

.....
(nazwa i adres Podmiotu przetwarzającego)
stosuje właściwe środki organizacyjne i techniczne, umożliwiające należyte zabezpieczenie danych osobowych, zgodnie z RODO.

został wyznaczony inspektor ochrony danych osobowych, należy podać dane kontaktowe (imię i nazwisko, numer telefonu oraz adres poczty elektronicznej):

.....
.....
.....

do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie w przedmiotowym zakresie,

prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych, należy ją wyszczególnić poniżej:

.....
.....
.....
.....
.....
.....

| Lp. | TAK/NIE/ NIE DOTYCZY *niepotrzebne skreślić | Zabezpieczenia danych osobowych stosowane u Podmiotu przetwarzającego |
|--|--|--|
| Środki ochrony fizycznej i technicznej danych | | |
| 1 | TAK/NIE/ NIE DOTYCZY | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, objęte są systemem kontroli dostępu. |
| 2 | TAK/NIE/ NIE DOTYCZY | Pomieszczenia, w których przetwarzany jest zbiór danych osobowych, wyposażone są w system alarmowy przeciwwłamaniowy. |
| 3 | TAK/NIE/ NIE DOTYCZY | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych. |
| 4 | TAK/NIE/ NIE DOTYCZY | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony. |
| 5 | TAK/NIE/ NIE DOTYCZY | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony. |
| 6 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej. |
| 7 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C. |

| | | |
|----|-------------------------|---|
| 8 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min |
| 9 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). |
| 10 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie. |
| 11 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie. |
| 12 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej. |
| 13 | TAK/NIE/ NIE DOTYCZY | Pomieszczenie, w którym przetwarzany jest zbiór danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i / lub wolnostojącej gaśnicy. |
| 14 | TAK/NIE/ NIE DOTYCZY | Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową |
| 15 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego. |
| 16 | TAK/NIE/ NIE DOTYCZY | Zbiór danych osobowych przetwarzany jest w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach. |
| 17 | TAK/NIE/ NIE DOTYCZY | Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie. |
| 18 | TAK/NIE/ NIE DOTYCZY | Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie. |
| 19 | TAK/NIE/ NIE DOTYCZY | Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej. |
| 20 | TAK/NIE/ NIE DOTYCZY | Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. |
| 21 | TAK/NIE/ NIE DOTYCZY | Zastosowano urządzenia chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania, jeżeli tak to jakie (proszę wymienić): |
| 22 | TAK/NIE/ NIE DOTYCZY | Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej / komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła. |
| 23 | TAK/NIE/ NIE DOTYCZY | Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. |
| 24 | TAK/NIE/ NIE DOTYCZY | Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN. |

| | | |
|---|-------------------------|--|
| 25 | TAK/NIE/ NIE DOTYCZY | Użyto system Firewall do ochrony dostępu do sieci komputerowej. |
| 26 | TAK/NIE/ NIE DOTYCZY | Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej. |
| 27 | TAK/NIE/ NIE DOTYCZY | Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł. |
| 28 | TAK/NIE/ NIE DOTYCZY | Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych. |
| 29 | TAK/NIE/ NIE DOTYCZY | Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji. |
| 30 | TAK/NIE/ NIE DOTYCZY | Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych. |
| 31 | TAK/NIE/ NIE DOTYCZY | Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu. |
| 32 | TAK/NIE/ NIE DOTYCZY | Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej. |
| 33 | TAK/NIE/ NIE DOTYCZY | Zastosowano środki ochrony przed szkodliwym oprogramowaniem. |
| 34 | TAK/NIE/ NIE DOTYCZY | Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej. |
| 35 | TAK/NIE/ NIE DOTYCZY | Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia. |
| Środki ochrony w ramach narzędzi programowych i baz danych | | |
| 1 | TAK/NIE/ NIE DOTYCZY | Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych. |
| 2 | TAK/NIE/ NIE DOTYCZY | Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych. |
| 3 | TAK/NIE/ NIE DOTYCZY | Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. |
| 4 | TAK/NIE/ NIE DOTYCZY | Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN. |
| 5 | TAK/NIE/ NIE DOTYCZY | Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej. |
| 6 | TAK/NIE/ NIE DOTYCZY | Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego. |
| 7 | TAK/NIE/ NIE DOTYCZY | Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych. |
| 8 | TAK/NIE/ NIE DOTYCZY | Zastosowano kryptograficzne środki ochrony danych osobowych. |

| | | |
|-----------------------------|-------------------------|--|
| 9 | TAK/NIE/ NIE DOTYCZY | Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. |
| 10 | TAK/NIE/ NIE DOTYCZY | Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika. |
| Środki organizacyjne | | |
| 1 | TAK/NIE/ NIE DOTYCZY | 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. |
| 2 | TAK/NIE/ NIE DOTYCZY | Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. |
| 3 | TAK/NIE/ NIE DOTYCZY | Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy. |
| 4 | TAK/NIE/ NIE DOTYCZY | Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. |
| 5 | TAK/NIE/ NIE DOTYCZY | Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. |

Inne środki organizacyjno-techniczne:

.....
Podpis i pieczęć Podmiotu przetwarzającego