

Umowa powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych zawarta w dniu DD.MM.RRRR r.
w Opolu pomiędzy:

Regionalnym Centrum Krwiodawstwa i Krwiolecznictwa w Opolu

z siedzibą przy ul. Kośnego 55, 45–372 Opole,

działającym na podstawie wpisu w Krajowym Rejestrze Sądowym pod Nr KRS: 0000009878,

w Sądzie Rejonowym w Opolu, VIII Wydział Gospodarczy

NIP 754-25-54-112, REGON 000292103

zwanym w dalszej części niniejszej umowy „**Administratorem**”

którego reprezentuje:

Dyrektor – Iwona Rajca-Biernacka,

a

XXXXXXXX

z siedzibą XXXXXXXX

NIP / KRS: XXXXXXXX

zwanym w dalszej części niniejszej umowy „**Podmiotem przetwarzającym**”

którego reprezentuje:

XXXXXXXX

dalej również łącznie Strony lub osobno Strona

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z wejściem w życie Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 r. (t.j. Dz. U. z 2019 r. poz. 1781) strony zawierają niniejszą umowę powierzenia przetwarzania danych osobowych zgodną z Art. 28 ustęp 3 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) zwanego dalej „**Rozporządzeniem**”
2. **Administrator** powierza **Podmiotowi przetwarzającemu** przetwarzanie danych osobowych w trybie art. 28 Rozporządzenia
3. **Administrator** oświadcza, że w rozumieniu Rozporządzenia jest „**Administratorem**” danych osobowych, których przetwarzanie powierza Podmiotowi przetwarzającemu.
4. **Administrator** powierza **Podmiotowi przetwarzającemu** przetwarzanie danych osobowych na zasadach określonych w § 2 Umowy. Powierzenie danych osobowych Podmiotowi Przetwarzającemu następuje w celu wykonania umowy zawartej pomiędzy Stronami w dniu ----- roku (dalej jako „Umowa główna”).

4. **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, w szczególności **Podmiot przetwarzający** oświadcza, że stosuje odpowiednie środki bezpieczeństwa techniczne i organizacyjne, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
5. **Podmiot przetwarzający** zobowiązuje się, przy przetwarzaniu powierzonych mu przez Administratora danych osobowych, do ich zabezpieczenia (w szczególności przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) przez podjęcie **środków bezpieczeństwa technicznych i organizacyjnych** zapewniających odpowiedni stopień bezpieczeństwa tj. odpowiadających ryzyku zgodnie z art. 32 Rozporządzenia
6. Środki bezpieczeństwa, o których mowa w ust. 5 powyżej, należy poddawać przeglądom i aktualizacji.
7. W szczególności środki te obejmują wdrożenie i stosowanie przez Administratora odpowiednich **polityk ochrony danych**.
8. Wszelkie informacje uzyskane w związku z wykonywaniem niniejszej umowy, w szczególności informacje o sposobach zabezpieczania danych przez drugą stronę należy zachować w tajemnicy, również po wygaśnięciu niniejszej umowy.
9. Podmiot przetwarzający potwierdza, że posiada wiedzę, że powierzone mu dane osobowe mogą stanowić także tajemnicę przedsiębiorstwa i ich procesowanie wymaga zachowania najwyższej staranności, w tym w zakresie zasad bezpieczeństwa wynikających z obowiązujących przepisów prawa i Umowy głównej.

§ 2

Zakres i cel przetwarzania danych

1. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w następującym zakresie i celu:

cel przetwarzania	Realizacja umowy w zakresie:
przedmiot przetwarzania	Dawcy krwi
czas trwania przetwarzania	Do czasu trwania umowy głównej
charakter przetwarzania	<i>zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, pobieranie, przeglądanie, wykorzystywanie, usuwanie</i>
rodzaj danych osobowych -	<i>Dane zwykłe:</i> <i>Dawca krwi - imię i nazwisko, Pesel, Data urodzenia, płeć, wzrost i waga, nr telefonu, adres zamieszkania i inne identyfikujące dane.</i>

	<i>Dane osobowe specjalnej kategorii art. 9 RODO</i> <i>Dane z wywiadu medycznego, składniki krwi miejsce przechowywania dokumentacji medycznej, dodatkowe informacje medyczne.</i>
kategorie osób, których dane dotyczą	<i>Dane osobowe zwykłe</i> <i>Dane osobowe specjalnej kategorii art. 9 RODO</i>

§ 3

Sposób wykonania niniejszej umowy przez Podmiot przetwarzający

1. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych przez Administratora danych osobowych, a w szczególności:

- a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, które stanowi Umowa Główna oraz dodatkowe polecenia przekazywane na piśmie lub mailowo.
- b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się **pisemnie** do zachowania tajemnicy przed przystąpieniem do przetwarzania danych powierzonych przez Administratora – to pisemne zobowiązanie musi obejmować również zobowiązanie do zachowania tajemnicy po ustaniu zatrudnienia;
- c) podejmuje wszelkie środki wymagane na mocy art. 32 Rozporządzenia;
- d) przestrzega warunków korzystania z usług *innego podmiotu przetwarzającego*, o których mowa w art. 28 ust. 2 i 4 Rozporządzenia oraz warunkami niniejszej umowy;
- e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia;
- f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia;
- g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub **zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie**, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie lub zezwalają na przechowywanie danych osobowych;
- h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora **przeprowadzanie audytów**, w tym inspekcji, i przyczynia się do nich;
- i) niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

2. Podmiot przetwarzający zobowiązuje się prowadzić, w formie pisemnej (w tym elektronicznej), rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zawierający informacje o:
 - a) nazwie oraz danych kontaktowych Podmiotu Przetwarzającego oraz innych podmiotów przetwarzających (w przypadku podpowierzenia danych osobowych)
 - b) nazwie Administratora, a także inspektora ochrony danych, gdy ma to zastosowanie;
 - b) kategoriach przetwarzanych dokonywanych w imieniu Administratora;
 - c) gdy ma to zastosowanie - przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwie tego państwa trzeciego lub organizacji międzynarodowej;
 - d) ogólnym opisie technicznych i organizacyjnych środków bezpieczeństwa, służących do zabezpieczenia powierzonych danych osobowych.

§ 4

Audyty

1. Na podstawie art. 28 ust. 3 pkt h) Rozporządzenia Administrator ma prawo do wykonania kontroli i audytów mających na celu sprawdzenie zgodności przetwarzania przez Podmiot przetwarzający powierzonych mu danych osobowych z wymaganiami niniejszej umowy oraz sprawdzenie sposobów ich zabezpieczania.
2. Administrator jest w każdym momencie upoważniony do przeprowadzenia audytu zgodności przetwarzania danych osobowych przez Podmiot przetwarzający z Umową oraz obowiązującymi przepisami prawa, w szczególności Administrator może przeprowadzić weryfikację zgodności i adekwatności środków technicznych i organizacyjnych zabezpieczających przetwarzanie danych osobowych wdrożonych przez Podmiot przetwarzający.
2. Audyt powinien być zapowiedziany z wyprzedzeniem co najmniej 14 dni kalendarzowych.
3. Audyty będą prowadzone przez Administratora lub audytora upoważnionego przez Administratora w godzinach pracy Podmiotu przetwarzającego.
5. Na zakończenie audytu, audytujący sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron.
6. **Podmiot przetwarzający** może wnieść zastrzeżenia do protokołu w ciągu 10 dni roboczych od daty jego podpisania przez Strony.
7. **Podmiot przetwarzający** zobowiązuje się dostosować do zaleceń poaudytowych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania powierzonych danych osobowych.
8. Koszty związane z przeprowadzeniem audytu ponosi podmiot, który zlecił przeprowadzenie audytu, bez prawa do żądania zwrotu takich kosztów ani zapłaty dodatkowego wynagrodzenia.
9. Administrator lub upoważniony przez niego audytor przed rozpoczęciem audytu będzie zobowiązany do podpisania zobowiązania do zachowania tajemnicy przedsiębiorstwa i tajemnicy dotyczącej danych osobowych oraz sposobów ich zabezpieczania.

§ 5

Odpowiedzialność Podmiotu przetwarzającego

1. W przypadku naruszenia ochrony danych osobowych, przepisów Rozporządzenia lub niniejszej umowy z przyczyn leżących po stronie **Podmiotu przetwarzającego**, w następstwie, czego Administrator, jako administrator powierzonych danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą administracyjną, **Podmiot przetwarzający** zobowiązuje się pokryć Administratorowi poniesione z tego tytułu straty i koszty.
2. **Podmiot przetwarzający** zobowiązuje się odpowiedzieć niezwłocznie (tj. w czasie nie dłuższym niż 72 godziny) i właściwie na każde pytanie Administratora dotyczące przetwarzania powierzonych mu na podstawie niniejszej umowy danych osobowych oraz udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
3. **Podmiot przetwarzający** zobowiązuje się niezwłocznie zawiadomić Administratora o:
 - 1) każdym żądaniu udostępnienia danych osobowych właściwemu organowi publicznemu, chyba, że zakaz zawiadomienia wynika z przepisów prawa,
 - 2) każdym stwierdzeniu lub podejrzeniu naruszenia ochrony danych osobowych (nie później niż w terminie **24 godzin**)
 - 3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
4. Podmiot przetwarzający niezwłocznie informuje Administratora o każdej planowanej kontroli administracyjnej / audytowi ochrony danych oraz o każdej decyzji administracyjnej lub sądowej dotyczącej przetwarzania przez niego danych osobowych powierzonych przez Administratora.

§ 6

Korzystanie przez podmiot przetwarzający z usług *innego podmiotu przetwarzającego* (podpowierzenie)

1. Administrator wyraża zgodę na korzystanie przez Podmiot przetwarzający z usług *innych podmiotów przetwarzających*.
2. Podmiot przetwarzający chcąc skorzystać z usług *innego podmiotu przetwarzającego* ma obowiązek poinformować Administratora z wyprzedzeniem 5 dni roboczych o każdym zamierzonym powierzeniu przetwarzaniu danych. Administrator może wprost sprzeciwić się dalszemu powierzeniu danych osobowych, w terminie 5 Dni Roboczych od otrzymania informacji, o której mowa w zdaniu poprzednim. W przypadku wyrażenia sprzeciwu przez Administratora, w tym terminie Podmiot przetwarzający nie jest uprawniony do zawarcia umowy z dalszym podmiotem przetwarzającym, którego dotyczy sprzeciw.
3. Na inny(e) podmiot(y) przetwarzający(e) nałożone zostają – na mocy Rozporządzenia i niniejszej umowy te same obowiązki ochrony danych jak określone w Rozporządzeniu oraz w niniejszej umowie, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.

4. Jeżeli *inny podmiot przetwarzający* nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na podmiocie przetwarzającym.

§ 7

Czas obowiązywania i warunki wypowiedzenia umowy

1. Niniejsza umowa powierzenia zostaje zawarta na czas nie/określony od dnia **DD.MM.RRRR** (do dnia DD.MM.RRRR) i może być wypowiedziana przez każdą ze stron z zachowaniem ... miesięcznego terminu wypowiedzenia, w formie pisemnej pod rygorem nieważności.
2. Wypowiedzenie niniejszej umowy jest jednoznaczne z wypowiedzeniem umowy w związku z którą powierzono nam dane do przetwarzania.

§ 8

Warunki wypowiedzenia umowy

1. Administrator ma prawo rozwiązać niniejszą umowę ze skutkiem natychmiastowym tj. bez zachowania terminu wypowiedzenia, jeżeli **Podmiot przetwarzający**:
 - 1) przetwarza dane osobowe w sposób niezgodny z niniejszą umową,
 - 2) powierzył przetwarzanie danych osobowych *innemu Podmiotowi przetwarzającemu* bez wcześniejszego poinformowania Administratora,
 - 3) uniemożliwia wykonanie audytu ochrony danych,
 - 4) nie usunął w wyznaczonym terminie uchybień wskazanych podczas audytu ochrony danych,
 - 5) nie odpowiada niezwłocznie tj. w czasie 72 godzin i właściwie na każde pytanie Administratora dotyczące przetwarzania powierzonych mu na podstawie niniejszej umowy danych osobowych
 - 6) nie udostępnia Administratorowi informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 9

Rozwiązanie umowy

1. W przypadku wygaśnięcia / wypowiedzenia niniejszej umowy, nie później niż w terminie do 14 dni kalendarzowych, **Podmiot przetwarzający** zobowiązuje się **zwrócić** wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, oraz **usunąć wszystkie ich istniejące kopie** w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji - chyba że właściwe przepisy prawa krajowego lub unijnego nakazują/zezwalają na przechowywanie tych danych osobowych i potwierdzić powyższe przekazanym Administratorowi protokołem.

2. Usunięcie danych osobowych musi być potwierdzone protokołem z ich usunięcia. Protokół powinien być dostarczony administratorowi w ciągu 7 dni po ich usunięciu.

§ 11

Osoby odpowiedzialne za realizację umowy

1. Ze strony administratora:
 - a) Imię i nazwisko, e-mail, nr telefonu
2. Ze strony podmiotu przetwarzającego:
 - a) Imię i nazwisko, e-mail, nr telefonu

§ 12

Postanowienia Końcowe

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego, Rozporządzenia oraz inne przepisy prawa powszechnie obowiązującego.
4. Spory wynikłe z tytułu niniejszej umowy będzie rozstrzygał Sąd właściwy dla siedziby administratora
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....
za Administratora

.....
za Podmiot przetwarzający