

Umowa powierzenia przetwarzania danych osobowych

zawarta dniar pomiędzy:

(zwana dalej „Umową”)

Akademickim Centrum Zdrowia w Mikołowie sp. z o.o., ul. Waryńskiego 2, 43-190 Mikołów
wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000335411,
NIP 6351802538 REGON: 241294970
zwana w dalszej części umowy „**Administratorem danych**” lub „**Administratorem**”
którą reprezentuje:

Katarzyna Muszak – Prezes Zarządu

oraz

Nazwa firmy zewnętrznej

Adres firmy zewnętrznej

zwana w dalszej części umowy „**Podmiotem przetwarzającym**” lub „**Przetwarzającym**”
którą reprezentuje:

Nazwisko i imię – Stanowisko / Nazwisko i imię - Stanowisko

§ 1**Powierzenie przetwarzania danych osobowych**

1. W związku z zawarciem i realizacją umowy głównej:

Nr umowy / data umowy / przedmiot umowy

Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego 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 (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie poleceniem Administratora, jak również 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:

zwykłe / szczególne (pozostawić te, które będą przedmiotem umowy)

pracowników/pacjentów/osób trzecich (jw. lub dopisać inne - jakie)

identyfikacyjne/komunikacyjne/pracownicze/medyczne/finansowe (wymienić jakie np.) - nazwisko i imię (imiona) - data urodzenia - oznaczenie płci - adres miejsca zamieszkania / oddział szpitalny dla każdej kategorii.

2. Powierzone przez Administratora, dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy, o której mowa w § 1 ust 1.
3. Przetwarzanie danych osobowych, o których mowa w ust. 1 przez Podmiot Przetwarzający będzie polegało m.in. na ich:

zbieraniu / utrwalaniu / organizowaniu / porządkowaniu / przechowywaniu / adaptowaniu / modyfikowaniu / pobieraniu / przeglądaniu / wykorzystywaniu / ujawnianiu przez przesłanie / jak również ich dopasowywanie i łączenie (jw. pozostawić te, które będą przedmiotem umowy)

wyłącznie w celu, o którym mowa w ust. 2

4. Zakres danych osobowych wymienionych w ust. 1 jest maksymalnym katalogiem danych , które mogą być przetwarzane w związku z realizacją niniejszej Umowy. W rzeczywistości dane mogą być przekazywane przez Administratora w mniejszym zakresie bez uszczerbku dla postanowień niniejszej Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów

§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 RODO) 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. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr kategorii czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, usuwa wszelkie elektroniczne dane osobowe oraz usuwa ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Jeżeli dane osobowe były przetwarzane w tradycyjnej fizycznej formie, Podmiot przetwarzający zwraca do Administratora wszystkie oryginały dokumentów, o ile dane były przetwarzane w ten sposób oraz niszczy wszystkie kopie dokumentów w sposób uniemożliwiający ich odtworzenie lub odczytanie.
7. 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, jak również umożliwia przeprowadzenie kontroli.

8. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24h.
9. Przetwarzający oświadcza, że nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („EOG”)). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.
10. Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.
11. Planując dokonanie zmian w sposobie przetwarzania danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.
12. Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.
13. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

§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 w formie np. audytu.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego z minimum 7 dniowym uprzedzeniem.
3. Administrator Danych lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe w godzinach pracy Przetwarzającego oraz wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych, systemów IT w których przetwarzane są dane powierzone przez Administratora.
4. Po przeprowadzonym audycie przedstawiciel Administratora lub Administrator Danych sporządza protokół pokontrolny, który podpisują przedstawiciele obu stron.
5. Podmiot przetwarzający, na każdy pisemny wniosek Administratora zobowiązany jest do udzielenia pisemnych informacji dotyczących przetwarzania powierzonych mu danych osobowych w terminie 2 dni roboczych od dnia otrzymania takiego wniosku
6. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
7. 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

Administradora 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, o którym mowa w §5 ust. 1 Umowy musi spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wszelkie działania lub zaniechania podwykonawcy, tym również za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego i Administratora

1. Podmiot przetwarzający jest odpowiedzialny za przetwarzanie danych osobowych niezgodnie z treścią umowy, jak również jest odpowiedzialny za przetwarzanie danych osobowych niezgodnie z obowiązującymi przepisami prawa, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym
2. Podmiot przetwarzający zobowiązany jest do zwolnienia Administratora danych z obowiązku zapłaty odszkodowania oraz zadośćuczynią na rzecz osób trzecich wraz z odsetkami ustawowymi za opóźnienie i kosztami procesu oraz administracyjnych kar pieniężnych – w każdym przypadku wyrządzenia szkody majątkowej lub niemajątkowej w wyniku przetwarzania przez Podmiot przetwarzający danych osobowych niezgodnie z treścią niniejszej umowy lub obowiązujących przepisów prawa, jak również w przypadku naruszenia przepisów prawa.
3. 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 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 danych.
4. Administrator zobowiązuje się do wypełniania obowiązków przewidzianych w art. 13 lub art. 14 „RODO” wobec osób fizycznych, których dane osobowe bezpośrednio lub pośrednio zostały pozyskane w związku z realizacją umowy.

§7

Powiadomienie o Naruszeniach Danych Osobowych

1. Podmiot Przetwarzający powiadamia Administratora Danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia oraz umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora Danych o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.
2. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, na adres email: iod@szpital-mikolow.com.pl tak aby umożliwić Administratorowi Danych spełnienie obowiązku powiadomienia organu nadzoru w odpowiednim czasie. Zgłoszenia można dokonać również telefonicznie, jednak w ciągu 48 godzin od zgłoszenia należy wysłać na wyżej wskazany mail wszelkie niezbędne informacje dotyczące naruszenia danych osobowych. Zgłoszenia telefoniczne należy zgłaszać do Inspektora Ochrony Danych pod numerem telefonu 730191446.
3. Zgłoszenie powinno zawierać co najmniej informacje o:
 - a) dacie, czasie trwania oraz lokalizacji naruszenia ochrony danych osobowych;
 - b) charakterze i skali naruszenia, tj. w szczególności o kategoriach i przybliżonej liczbie osób, których dane dotyczą, oraz kategoriach i przybliżonej liczbie wpisów danych osobowych, których dotyczy naruszenie, a w razie możliwości, także wskazania podmiotów danych, których dotyczyło

naruszenie;

- c) systemie informatycznym, w którym wystąpiło naruszenie (jeżeli naruszenie nastąpiło w związku z przetwarzaniem danych w systemie informatycznym);
 - d) przewidywanym czasie potrzebnym do naprawienia szkody spowodowanej naruszeniem;
 - e) charakterze i zakresie danych osobowych objętych naruszeniem;
 - f) możliwych konsekwencjach naruszenia, z uwzględnieniem konsekwencji dla osób, których dane dotyczą;
 - g) środkach podjętych w celu zminimalizowania konsekwencji naruszenia oraz proponowanych działaniach zapobiegawczych i naprawczych;
 - h) danych kontaktowych osoby mogącej udzielić dalszych informacji o naruszeniu.
4. Przetwarzający nie będzie bez wyraźnych instrukcji Administratora powiadamiał o naruszeniu:
- a) osób, których dane dotyczą ani
 - b) organu nadzorczego.

§8

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez okres trwania umowy, o której mowa w § 1 ust. 1
2. W każdym wypadku umowa przestaje wiązać Strony z dniem, z którym przestają być związane postanowieniami umowy, o której mowa w § 1 ust. 1

§9

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
 - 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 danych;
2. Rozwiązanie niniejszej umowy na podstawie § 9 ust. 1 stanowi podstawę do rozwiązania przez Administratora umowy, o której mowa w §1 ust. 1.

§10

Usunięcie Danych

1. Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:
 - a) usunięcia Danych,
 - b) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.
2. Przetwarzający dokona usunięcia Danych po upływie 14 dni od zakończenia Umowy, chyba że Administrator Danych poleci mu to uczynić wcześniej.
3. Po wykonaniu zobowiązania, o którym mowa w § 10, Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich danych.

§11

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.

§12

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

Administrator danych

Podmiot przetwarzający