Umowa powierzenia przetwarzania danych osobowych nr: …….
zawarta dnia …….. w Sosnowcu pomiędzy:
(zwana dalej „Umową")

Wojewódzkim Szpitalem Specjalistyczny nr 5 im. Św. Barbary w Sosnowcu
41-200 Sosnowiec, Plac Medyków 1, zarejestrowanym w Sądzie Rejonowym w Katowicach Wydział VIII Gospodarczy Krajowego rejestru Sądowego, nr KRS 0000003544, NIP 644-287-67-26,
zwanym w dalszej części umowy **„Administratorem"**
reprezentowanym przez:
……

oraz
……
……
……

zwanym w dalszej części umowy **„Podmiotem przetwarzającym"**
reprezentowanym przez:
……

łącznie zwane **„Stronami"**, a odrębnie **„Stroną"**

§ 1.

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (EU) nr 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 (ogólnego rozporządzenia o ochronie danych), 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 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 następujące rodzaje danych osobowych:
   1) **Dane zwykłe (w tym: imię, nazwisko, adres zamieszkania, PESEL, adres IP, adres e-mail, data urodzenia, numer rachunku bankowego, numery telefonów, NIP, …….)**
   2) **Szczególne kategorie danych (w tym: informacje o stanie zdrowia oraz dotyczące udzielania oraz finansowania świadczeń opieki zdrowotnej, ……)**
   3) **Dane dzieci (w tym: imię, nazwisko, adres zamieszkania, PESEL,data urodzenia, …….)**
   4) **Dane nieustrukturyzowane (kontent o potencjalnej i prawdopodobnej zawartości danych osobowych (wpisy, dokumenty tekstowe, obrazy, nagrania, filmy).**
2. Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:
   1) **klienci administratora,**
   2) **pracownicy Administratora i personel Administratora zatrudniony na innej podstawie niż umowa o pracę,**
   3) **pacjenci Administratora,**
   4) **klienci usługi/produktu Administratora określonych w Umowie Podstawowej,**
   5) **kontrahenci,**
   6) **odbiorcy korespondencji i korespondencji elektronicznej klientów/pacjentów Administratora,**
   7) **……..**

3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy Podstawowej, tj.:
   …… z dnia: **……..…….** nr: **……** w zakresie:
   ……
   ……..
4. Zakres danych osobowych wymienionych powyżej jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa.

§ 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 związanemu 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 ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.
5. Podmiot przetwarzający na żądanie Administratora dostarcza Administratorowi wykaz upoważnionych osób oraz informuje Administratora o cofnięciu upoważnień.
6. 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.
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
8. 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.
9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w czasie nie przekraczającym *24 h*.
   Powiadomienie o stwierdzeniu naruszenia powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.
10. Podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 Rozporządzenia.
11. Podmiot przetwarzający zobowiązany jest do przestrzegania zasad odnoszących się do postępowania w relacjach z dostawcami towarów i usług zewnętrznych, ze szczególnym uwzględnieniem występujących w nich ryzyk oraz zasad zachowania bezpieczeństwa informacji zgodnie z przyjętą przez Administratora „Polityką współpracy z Dostawcami / Wykonawcami w zakresie bezpieczeństwa Informacji" dostępnej na stronie www szpitala (http://www.wss5.pl/rodo).
12. Ze względu na obowiązek powierzenia przetwarzania danych przez Administratora podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniło wymagania rozporządzenia i chroniło prawa osób, których dane dotyczą Podmiot Przetwarzający zobowiązany jest do wypełnienia ankiety bezpieczeństwa danych osobowych *(załącznik nr: 1 - Ankieta bezpieczeństwa danych osobowych)*.

§ 4.

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.

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 pod rygorem nieważności w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy Podstawowej.
3. Zobowiązanie do zachowania poufności trwa przez cały okres obowiązywania Umowy Podstawowej, o której mowa w § 2 punkt 3 powyżej oraz po upływie okresu przedawnienia roszczeń wynikających z Umowy Podstawowej.

§ 5.

Prawo kontroli

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

§ 6.

Dalsze powierzenie danych do przetwarzania

1. Podmiot Przetwarzający może powierzyć konkretne operacje przetwarzania Danych (*„podpowierzenie”*) jedynie w celu wykonania Umowy Podstawowej, w drodze pisemnej umowy podpowierzenia (*„Umowa Podpowierzenia”*) innym podmiotom przetwarzającym (*„Podprzetwarzającym”*) pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora.
2. Lista Podprzetwarzających zaakceptowanych przez Administratora stanowi *załącznik nr 2 do Umowy – Lista Zaakceptowanych Podprzetwarzających*.
3. Zmiana bądź dodanie Podprzetwarzającego wymaga każdorazowo pisemnej zgody Administratora pod rygorem nieważności.
4. Dokonując podpowierzenia, Podmiot Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia.
5. Podmiot Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi pisemne oświadczenie o zobowiązaniu się do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.
6. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy (*„Podprzetwarzającego”*) obowiązków w zakresie ochrony danych.
7. W przypadku dalszego powierzenia przetwarzania danych osobowych Podmiot Przetwarzający zobowiązuje się do zawarcia w umowach z dalszymi podmiotami przetwarzającymi (*„Podprzetwarzającym”*) postanowień, zgodnie z którymi, umowy dalszego przetwarzania będą ulegały automatycznemu rozwiązaniu w chwili zakończenia obowiązywania niniejszej Umowy.
8. Podmiot Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy Podstawowej.

§ 7.

Oświadczenia Stron

1. Administrator oświadcza, że jest Administratorem danych osobowych oraz że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Podmiot Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.
3. Przetwarzający na żądanie administratora danych powinien przedstawić dokumentację potwierdzająca przetwarzanie danych osobowych zgodnie z wymogami RODO, mogą to być między innymi: certyfikat potwierdzający wdrożenie normy PN-EN ISO/IEC 27001, raporty z przeprowadzonych przez niezależne podmioty audytów, dokumentacja potwierdzająca przeprowadzenie szkoleń, dokumentacja potwierdzająca wdrożenie zabezpieczeń technicznych i organizacyjnych.

§ 8.

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 odpowiada za szkody, jakie powstaną po stronie Administratora lub osób trzecich w wyniku niezgodnego z Umową, lub obowiązującymi przepisami prawa, przetwarzania danych osobowych przez Podmiot Przetwarzający.
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 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 Pracowników Urzędu upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 9.

Czas obowiązywania umowy

1. Niniejsza umowa zostaje zawarta na czas trwania Umowy Podstawowej, o której mowa w § 2 pkt 3 powyżej.
2. Rozwiązanie umowy, o której mowa w § 2 pkt 3 powyżej skutkować będzie ustaniem niniejszej Umowy.
3. **Administrator** może rozwiązać umowę, o której mowa w § 2 pkt 3 powyżej ze skutkiem natychmiastowym, bez zachowania okresu wypowiedzenia, gdy **Podmiot przetwarzający** narusza zobowiązania wynikające z niniejszej Umowy.

§ 10.

Rozwiązanie, zmiana umowy

1. Administrator 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 lub Rozporządzeniem;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 11.

Inspektor Ochrony Danych Osobowych

1. Kontakt z Inspektorem Ochrony Danych [IOD] w Wojewódzkim Szpitalem Specjalistyczny nr 5 im. Św. Barbary: **Imię i Nazwisko;** e-mail: **iod@wss5.pl**; telefon: **516 008 944**

2. Kontakt z Inspektorem Ochrony Danych [IOD] w Podmiocie Przetwarzającym lub pełnomocnikiem Podmiotu Przetwarzającego właściwym z uwagi na przedmiot Umowy: **Imię i Nazwisko;** e-mail: ……..…….; telefon: ……..……..

§ 12.

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. Każdorazowo przez pojęcie „dni" rozumie się dni kalendarzowe.
3. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

…… ……

Administrator Podmiot przetwarzający

ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Załącznik nr 1 do umowy powierzenia danych osobowych nr: …… z dnia: …… .

Podmiot przetwarzający:	
Imię I Nazwisko osoby wypełniającej	
Stanowisko	
Adres e-mail i nr telefonu	

Lp.	Pytanie	Odpowiedź	Uwagi
1	Proszę podać ilość lokalizacji i kraje, w których będą przetwarzane powierzone dane osobowe.		
2	Czy Państwa personel został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
3	Czy personel przetwarzający powierzone dane osobowe w pozostałych krajach został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa?		
4	Czy powierzone dane osobowe będą przekazywane poza EOG? Np. ze względu na lokalizację systemu IT, będą przetwarzane przez osoby zlokalizowane poza EOG lub osoby te będą miały możliwość dostępu do tych danych?		
5	Jeśli tak to w jakim kraju?		
6	Czy w Państwa organizacji przeprowadzane są okresowe audyty zgodności z przepisami ochrony danych osobowych?		
7	Czy w Państwa organizacji przeprowadzane są okresowe audyty bezpieczeństwa IT?		
8	Czy posiadają Państwo wdrożoną politykę bezpieczeństwa przetwarzania danych osobowych zgodną z zasadami RODO?		
9	Czy prowadzą Państwo rejestr czynności przetwarzania, w tym dla procesora, zgodnie z art. 30 RODO?		

10	Czy jesteście Państwo zobowiązani do wyznaczenia IOD, zgodnie z art. 37 RODO?		
11	Jeśli tak, to czy wyznaczono IOD?		
12	Jeśli nie, to czy wyznaczyli Państwo osobę, która będzie odpowiedzialna za zapewnienie zgodności przetwarzania danych z przepisami i bezpieczeństwa danych?		
13	Czy do przetwarzania danych w Państwa organizacji są dopuszczone wyłącznie osoby posiadające upoważnienia?		
14	Czy osoby te zostały zobowiązane do zachowania poufności danych oraz informacji o stosowanych przez Państwa zabezpieczeniach?		
15	Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych?		
16	Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO?		
17	Czy wdrożyli Państwo instrukcję postępowania w przypadku sytuacji naruszenia ochrony danych osobowych?		
18	Jeśli tak, to czy zgodnie z tą instrukcją zdołają Państwo przekazać administratorowi danych informacje o incydencie w ciągu 24 godzin od stwierdzenia naruszenia?		
19	Czy w celu zaplanowania środków bezpieczeństwa przeprowadzono analizę ryzyka?		
20	Czy wdrożyli Państwo system zarządzania bezpieczeństwem informacji np. ISO 27001?		
21	Czy do przetwarzania danych w Państwa pomieszczeniach, stosuje się fizyczne zabezpieczenia przed dostępem osób nieuprawnionych? Proszę krótko opisać jakie np. system kontroli dostępu, drzwi zamykane na klucz, system alarmowy, ochrona fizyczna, monitoring wizyjny.		
22	Czy przetwarzanie danych było już przedmiotem zewnętrznych audytów lub kontroli, np. PUODO w Państwa organizacji?		

23	Jeśli tak, proszę zwięźle opisać wyniki kontroli/ audytów		
24	Czy posiadają Państwo wdrożoną instrukcję zarządzania systemami IT służącymi do przetwarzania danych osobowych lub inne dokumenty wewnętrzne regulujące zasady zarządzania infrastrukturą IT?		
25	Czy Państwa systemy IT zapewniają rozliczalność operacji wykonywanych na danych osobowych, tzn. czy istnieje odnotowują nazwę użytkownika, datę oraz charakter operacji wykonanej na konkretnym rekordzie w bazie?		
26	Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane?		
27	Czy stosują Państwo pseudonimizację i szyfrowanie danych?		
28	Czy podjęli Państwo środki, aby zapewnić zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania?		
29	Czy w Państwa organizacji są stosowane środki służące ochronie systemów IT przed działaniem tzw. złośliwego oprogramowania?		
30	Jeśli tak, to czy podlegają one cyklicznej aktualizacji?		
31	Czy podjęli Państwo środki, aby zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? Np. regularny backup		
32	Czy dostęp do systemów IT wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		
33	Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?		

Lista Zaakceptowanych Podprzetwarzających

Załącznik nr 2 do umowy powierzenia danych osobowych nr: …….. z dnia: …… .

L.p.	Nazwa i dane kontaktowe podmiotu podprzetwarzającego	Dane kontaktowe inspektora ochrony danych	Cel podpowierzenia	Zakres podpowierzenia
1				
2				
3				
4				
5				
6				
7				
8				