**Umowa powierzenia przetwarzania danych osobowych**

**do Umowy z dnia …………………… roku**

zawarta pomiędzy:

Uniwersyteckim Szpitalem Dziecięcym w Krakowie, ul. Wielicka 265, 30-663 Kraków, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej, przez Sąd Rejonowy dla Krakowa - Śródmieścia, XI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000039390, NIP: 6792525795, który reprezentuje:

Prof. Uj. dr hab. Wojciech Cyrul – Dyrektor

zwany dalej („Administratorem” /„Powierzającym”)

a ……………………………………………………………………………

zwaną dalej („Przetwarzającym” / „Procesorem”)

Mając na uwadze, że:

* Strony zawarły umowę w dniu …………………………. roku („**Umowa Podstawowa**”), dotyczącą udzielania świadczeń medycznych przez lekarza specjalistę w …………………………………………….. w związku, z wykonywaniem której konieczne jest powierzenie Procesorowi przez Administratora przetwarzania danych osobowych w zakresie określonym niniejszą Umową;
* Celem niniejszej umowy (dalej **„Umowa”**) jest ustalenie warunków, na jakich Procesor wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;
* Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz. Urz. UE L 119, s. 1) – dalej **RODO**.

Strony postanowiły zawrzeć Umowę o następującej treści:

1. **Przedmiot umowy**
	1. Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Procesorowi przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych. Umowa stanowi umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 28 RODO.
	2. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
	3. Powierzenie przetwarzania Danych Osobowych następuje w celu umożliwienia Procesorowi prawidłowej realizacji szczegółowo opisanych w Umowie Podstawowej.
	4. Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („**Dane Osobowe**”):

**Dane zwykłe:**

1. imię i nazwisko,
2. numer ewidencyjny PESEL,
3. adres e-mail,
4. adres IP,
5. numery telefonów,
6. adres zamieszkania,
7. data urodzenia,
8. NIP,
9. seria i numer dokumentu tożsamości,
10. imiona rodziców,

**Dane szczególnych kategorii i dane karne:** informacje o stanie zdrowia,

1. diagnozy,
2. dane o stopniu niepełnosprawności
3. informacje gromadzone w dokumentacji medycznej,
4. stosowane leczenie,
5. opisy i wyniki badań (co obejmuje zapisane w postaci cyfrowej zdjęcia, filmy, badania obrazowe itp.)
6. dokumentacja medyczna
	1. Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:
7. klientów usług oraz pacjentów Administratora oraz ich opiekunów lub przedstawicieli ustawowych,
8. osób upoważnionych do uzyskiwania informacji o stanie zdrowia pacjentów,
9. osób uzyskujących dostęp do dokumentacji medycznej,

1. **Obowiązki Procesora**
	1. Procesor przetwarza Dane Osobowe wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.
	2. Procesor nie może podpowierzyć przetwarzania danych osobowych innemu podmiotowi .
	3. Procesor zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do nich jest niezbędny dla realizacji Umowy.
	4. Procesor zapewnia, że wszystkie osoby dopuszczone przez niego do przetwarzania Danych Osobowych uzyskały stosowne upoważnienie do ich przetwarzania, określające zakres i cel upoważnienia.
	5. Procesor zapewnia, że wszystkie osoby, które zostały przez niego upoważnione do przetwarzania Danych Osobowych, zostały pisemnie zobowiązane do zachowania Danych Osobowych w tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy. Zobowiązanie do zachowania tajemnicy obejmuje także wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania Danych Osobowych, także po rozwiązaniu Umowy lub upływie okresu na jaki została zawarta.
	6. W przypadku stwierdzenia przez Procesora naruszenia bezpieczeństwa Danych Osobowych, Procesor jest zobowiązany niezwłocznie poinformować o tym Administratora oraz podjąć niezwłocznie wszelkie czynności mające na celu ustalenie szczegółów naruszenia i zabezpieczenie Danych Osobowych przed dalszymi naruszeniami.
	7. Procesor 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 RODO.
	8. Procesor niezwłocznie, nie później jednak niż w ciągu 48 godzin, powiadamia Administratora o każdorazowym otrzymaniu przez niego żądania dostępu do Danych Osobowych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania, pochodzących od osoby której dotyczą Dane Osobowe. Zawiadomienie powinno zostać złożone Administratorowi w formie pisemnej lub elektronicznej, z załączeniem kopii żądania tej osoby.
	9. Procesor współpracuje z Administratorem przy wykonywaniu przez Administratora jego obowiązków, o których mowa w art. 32˗36 RODO
	10. Jeżeli Procesor poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.
	11. Planując dokonanie zmian w sposobie przetwarzania Danych, Procesor 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 Procesora zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Procesora.
	12. Procesor zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru kategorii czynności przetwarzania danych osobowych (wymóg art. 30 RODO). Procesor udostępniania na żądanie Administratora prowadzony rejestr kategorii czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Procesora. Procesor nie może wykorzystywać w celu realizacji Umowy zautomatyzowanego przetwarzania, w tym profilowania, o którym mowa w art. 22 ust. 1 i 4 RODO bez uprzedniej zgody Administratora.
	13. Procesor ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych zgodnie z RODO. Procesor zobowiązuje się do monitorowania stanu przeszkolenia osób upoważnionych oraz aktualizacji prowadzonych szkoleń w zakresie koniecznym do wypełnienia zobowiązań wynikających z Umowy.
2. **Obowiązki Administratora**

Administrator zobowiązany jest współdziałać z Procesorem w wykonaniu Umowy, udzielać Procesorowi wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich obowiązków wynikających z Umowy.

1. **Bezpieczeństwo danych**
	1. Procesor oświadcza, że przeprowadził analizę ryzyka przetwarzania powierzonych Danych Osobowych i stosuje się do jej wyników, co do organizacyjnych i technicznych środków ochrony danych.
	2. Przed rozpoczęciem przetwarzania danych osobowych Procesor musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO, a w szczególności: uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Procesor powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualnić te środki w porozumieniu z Administratorem.
	3. Procesor oświadcza, że ocenił czy stopień przyjętego przez niego poziomu bezpieczeństwa Danych Osobowych jest odpowiedni do ryzyka związanego z ich przetwarzaniem. Procesor stosuje się do wyników tej oceny oraz udostępnia Administratorowi wszelkie informacje na ten temat na każde jego żądanie.
	4. Procesor oświadcza, że zobowiązuje się stale monitorować przyjęte środki techniczne oraz organizacyjne pod kątem ich adekwatności oraz zapewnienia zgodności przetwarzania Danych Osobowych z wymaganiami RODO.
2. **Powiadomienie o Naruszeniach Danych Osobowych**
	1. Procesor zobowiązuje się do powiadamia Administratora o każdym podejrzeniu naruszenia ochrony Danych Osobowych w ciągu 24 godzin od jego wykrycia, w tym przekazuje informacje, o których mowa w art. 33 ust. 3 RODO.
	2. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane w formie pisemnej wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.
	3. Procesor przeprowadza wstępną analizę ryzyka naruszenia praw i wolności osób, których dane dotyczą i przekazuje wyniki tej analizy do Administratora w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.
	4. Procesor zobowiązuje się do przekazania Administratorowi – na jego żądanie - wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO w ciągu 48 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.
	5. Każde powiadomienie o stwierdzeniu naruszenia, powinno być przesłane w formie pisemnej wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia.
3. **Nadzór**
	1. Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Procesora o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz wglądu do dokumentacji oraz systemów informatycznych związanych z przetwarzaniem powierzonych Danych Osobowych. Administrator uprawniony jest do żądania od Procesora udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.
	2. Procesor jest zobowiązany do współpracy z Administratorem oraz organem nadzoru w zakresie w jakim postępowanie to dotyczy Danych Osobowych. Procesor jest zobowiązany do niezwłocznego powiadomienia Administratora o wszczęciu postępowania kontrolnego przez organ nadzoru, w zakresie w jakim dotyczy ono Danych Osobowych oraz o wszelkich innych działaniach innych organów, bądź innych zdarzeniach mających wpływ na przetwarzanie powierzonych Danych Osobowych.
	3. Procesor udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO oraz umożliwia mu przeprowadzanie audytów lub inspekcji. Audyt lub inspekcję może w imieniu Administratora przeprowadzić upoważniony przez niego podmiot.
	4. Udostępnianie ww. informacji powinno nastąpić niezwłocznie po otrzymaniu żądania Administratora, nie później jednak niż w terminie 48 godzin, w formie pisemnej lub elektronicznej.
	5. Przetwarzający zobowiązuje się stosować do ewentualnych wskazówek lub zaleceń wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.
4. **Oświadczenia Stron**
	1. Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Procesorowi.
	2. Procesor 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. Na żądanie Administratora Procesor okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe, raporty z audytów, certyfikaty lub inne dowody, iż Procesor zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
5. **Odpowiedzialność**
	1. Procesor odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Procesora lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Procesor odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.
6. **Okres Obowiązywania Umowy Powierzenia**
	1. Umowa obowiązuje od dnia ……………. roku i została zawarta na czas obowiązywania Umowy Podstawowej.
7. **Zakończenie przetwarzania**
	1. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Procesor zobowiązany jest do trwałego usunięcia przetwarzanych Danych Osobowych oraz wszelkich ich kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.
	2. Procesor złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych Osobowych lub w pisemnym oświadczenie o pozostawieniu danych szczegółowo wskaże podstawę prawną nakazującą ich dalsze przechowywanie.
8. **Postanowienia Końcowe**
	1. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.
	2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
	3. Umowa podlega prawu polskiemu oraz RODO.

……………………………………… …………………………………………...

(Podpis i pieczątka Administratora/Powierzającego) (Podpis i pieczątka Przetwarzającego/Procesora)