**umowa powierzenia przetwarzania danych osobowych**

pomiędzy

### Wielkopolskim Centrum Pulmonologii i Torakochirurgii im. E i J Zeylandów Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Poznaniu, ul. Szamarzewskiego 62, zarejestrowanym w KRS pod nr 0000001844, zwanym w dalszej części umowy „Administratorem”, reprezentowanym przez:

### Dyrektor - prof. nadzw. dr hab. med. Aleksandra Barinowa -Wojewódzkiego

a

………………………………

zarejestrowanym w ……………..pod nr ……………………, zwanym w dalszej części umowy „Podmiotem przetwarzającym”, reprezentowanym przez:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **WCPIT** jako Administrator w rozumieniu art. 4 pkt 7) 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) (Dz.Urz.UE z 4 maja 2016 r. seria L 119) – zwanego dalej RODO przekazuje ………………………(nazwa firmy) jako Podmiotowi przetwarzającemu w trybie art. 28 RODO z uwzględnieniem właściwych przepisów ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2016 r. poz. 186 ze zm., dalej UPP) przetwarzanie w jego imieniu danych osobowych (zwane powierzeniem w dalszej części niniejszej Umowy) na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych zgodnie z niniejszą Umową, RODO oraz innym przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie niniejszej Umowy:

🞏 dane osobowe pacjentów w zakresie takich danych jak:

* nazwisko i imię (imiona),
* imiona rodziców,
* data urodzenia,
* adres miejsca zamieszkania( adres do korespondencji),
* numer telefonu
* numer ewidencyjny PESEL,
* rodzaj i numer dokumentu potwierdzającego tożsamość,
* nazwisko i imię przedstawiciela ustawowego oraz adres jego zamieszkania( dot. osób małoletnich, całkowicie ubezwłasnowolnionych lub niezdolnych do świadomego wyrażania zgody,
* opis stanu zdrowia i udzielonych mu świadczeń zdrowotnych, w zakresie określonym przepisami prawa, w tym: Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Ustawy z dnia 27 sierpnia 2004 o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.
* inne informacje lub dane pacjenta, w zakresie niezbędnym do należytego wykonania przedmiotu Umowy, o którym mowa w pkt.1 Umowy, celem wykonania na danych operacji takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

🞏 dane osobowe pracowników/personelu w zakresie takich danych jak:

* nazwisko i imię (imiona),

1. Powierzone Podmiotowi przetwarzającemu do przetwarzania dane osobowe:

🞏 ~~nie obejmują żadnej z kategorii danych wskazanych w art. 9 RODO~~,

🞏 obejmują szczególne kategorie danych wskazanych w art. 9 RODO:

dane dotyczące zdrowia pracowników, klientów,

🞏 obejmują dane osobowe dzieci,

🞏 ~~nie obejmują danych osobowych dzieci~~.

1. Zakres danych osobowych wymienionych w pkt. 4 jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy. W rzeczywistości dane mogą być przekazywane przez Administratora w mniejszym zakresie bez uszczerbku dla postanowień Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa.
2. Realizacja niniejszej Umowy przez Podmiot przetwarzający, w tym przetwarzanie powierzonych danych osobowych winno pozostawać w zgodzie z UPP, w tym nie może powodować zakłócenia udzielania świadczeń zdrowotnych przez Administratora, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej pacjentów Administratora. Podmiot przetwarzający zobowiązany jest do zachowania w tajemnicy informacji związanych z pacjentami Administratora uzyskanych w związku z realizacją Umowy. Zobowiązanie to trwa nadal także po śmierci pacjenta.
3. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, zabezpieczyć je poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa danych odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO. Podmiot przetwarzający jest zobowiązany wykazać Administratorowi wdrożenie tych środków poprzez złożenie oświadczenia zawierającego informacje o:
4. sposobie zapewnienia pseudonimizacji i szyfrowania danych osobowych,
5. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
6. zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
7. prowadzeniu regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
8. Wymogi i oświadczenie wynikające z punktu poprzedzającego mogą być uznane za zrealizowane przez Podmiot przetwarzający, jeżeli Administrator zaakceptuje przedłożony:
9. zatwierdzony kodeks dobrych praktyk w rozumieniu art. 40 RODO oraz oświadczenie o spełnianiu wymogów wynikających z tego kodeksu,
10. certyfikat w rozumieniu art. 42 RODO wydany przez podmiot certyfikujący, kryteria certyfikacji oraz oświadczenie Podmiotu przetwarzającego o dalszej realizacji kryteriów certyfikacji,
11. dokument dobrych praktyk wydany przez organ nadzorczy, Europejską Radę Ochrony Danych Osobowych lub inny organ nadzorczy w rozumieniu art. 51 RODO oraz oświadczenie o spełnieniu wymogów wynikających z dobrych praktyk.
12. Przed dopuszczeniem do przetwarzania powierzonych danych osobowych, nie później jednak niż w terminie 7 dni od podpisania Umowy, Podmiot przetwarzający jest uprawniony i jednocześnie zobowiązany do:
    1. udzielenia pisemnych upoważnień i poleceń do przetwarzania danych osobowych wszystkim osobom, które zostaną przez niego dopuszczone do ich przetwarzania z uwzględnieniem rozwiązań zawartych w niniejszej Umowie,
    2. przeszkolenia osób uczestniczących w operacjach przetwarzania powierzonych danych w zakresie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk podmiotu przetwarzającego w dziedzinie ochrony danych osobowych,
    3. zobowiązania na piśmie do zachowania w tajemnicy, o której mowa w art. 28 ust 3 lit b RODO, przetwarzanych powierzonych danych osobowych i sposobów ich zabezpieczenia, przez osoby, które upoważni do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
13. Podmiot przetwarzający oświadcza, iż ma / nie ma\* powołanego Inspektora Ochrony Danych:

.……………………………………………………………………………………………..

<wpisać imię, nazwisko, adres poczty elektronicznej lub numer telefonu kontaktowego>.

W przypadku powołania Inspektora Ochrony Danych, Podmiot przetwarzający oświadcza, że został on zgłoszony organowi nadzorczemu, a w przypadku jego niezgłoszenia na chwilę zawarcia Umowy, Wykonawca oświadcza, że zostanie on zgłoszony najpóźniej do dnia 1 września 2018 roku.

1. Podmiot przetwarzający zobowiązuje się do zwrócenia Administratorowi wszelkich danych osobowych powierzonych przez Administratora w ciągu 7 dni roboczych od dnia rozwiązania lub wygaśnięcia Umowy. Podmiot przetwarzający jest zobowiązany do usunięcia wszelkich istniejących kopii w powyższym terminie, chyba, że prawo Unii lub prawo państwa członkowskiego nakazuje przechowywanie tych danych osobowych. W powyższym terminie Podmiot przetwarzający zobowiązany jest również złożyć Administratorowi pisemne oświadczenie o wykonaniu zobowiązania przewidzianego niniejszym punktem.
2. Podmiot przetwarzający zobowiązuje się do pomocy Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.
3. Podmiot przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje pomaga Administratorowi Danych wywiązywać się z obowiązków określonych w art. 32-36 RODO.
4. Podmiot przetwarzający, w myśl art. 33 ust. 2 RODO, zobowiązany jest bez zbędnej zwłoki, nie później jednak niż w terminie 24 godzin od stwierdzenia naruszenia, zawiadomić Administratora o naruszeniu ochrony danych osobowych, które nastąpiło w Podmiocie przetwarzającym – niezależnie od tego czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie winno zawierać przynajmniej elementy, o których mowa w art. 33 ust. 3 RODO.
5. Niezawiadomienie Administratora w powyższym terminie o wykrytym incydencie skutkuje obowiązkiem zapłaty Administratorowi kary Umownej w wysokości 1 % wartości przedmiotu umowy podstawowej nr EA………….., za każdy przypadek naruszenia w terminie 7 dni od daty doręczenia wezwania do jej zapłaty. Administrator jest uprawniony do dochodzenia odszkodowania przewyższającego wysokość zastrzeżonej kary Umownej na zasadach ogólnych.
6. Administratorowi zgodnie z art. 28 ust. 3 lit. h) RODO przysługuje prawo do kontroli prawidłowości przetwarzania przez Podmiot przetwarzający powierzonych mu danych osobowych a w szczególności realizacji obowiązku zabezpieczenia tych danych. Administrator realizuje przysługujące mu prawo kontroli poprzez:
7. żądanie złożenia pisemnych i ustnych wyjaśnień:

* w przypadku żądania pisemnych wyjaśnień Podmiot przetwarzający zobowiązany jest udzielić odpowiedzi Administratorowi nie później niż w terminie 36 godzin od dostarczenia złożenia żądań,
* w przypadku żądania ustnych wyjaśnień Podmiot przetwarzający zobowiązany jest natychmiast udzielić odpowiedzi Administratorowi, jeżeli pytanie zostało zadane w trakcie normalnych godzin pracy Podmiotu przetwarzającego w dniu roboczym; w przypadku gdy udzielenie odpowiedzi jest utrudnione z uwagi na wymóg sprawdzenia pewnych okoliczności odpowiedź winna nastąpić pisemnie nie później niż w terminie 36 godzin od dostarczenia złożenia żądań,

1. żądania dostarczenia poświadczonej kopii lub skanu dokumentacji dotyczącej przetwarzania danych osobowych przez Podmiot przetwarzający, w szczególności upoważnień do przetwarzania danych osobowych i polityk ochrony danych w zakresie dotyczącym zabezpieczenia danych przetwarzanych w imieniu Administratora – realizacja niniejszego obowiązku winna nastąpić nie później niż w terminie 48 godzin od dostarczenia złożenia żądań,
2. realizację kontroli poprzez przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych, w których przetwarzane są powierzone dane osobowe na następujących zasadach:

* kontrola może nastąpić za uprzednim co najmniej 7 dniowym pisemnym powiadomieniem Podmiotu przetwarzającego o planowanym przeprowadzeniu kontroli,
* powiadomienie winno wskazywać osobę lub osoby ze strony Administratora uprawnione do przeprowadzenia kontroli, dzień roboczy przeprowadzenia kontroli oraz godzinę rozpoczęcia kontroli,
* Podmiot przetwarzający obowiązany jest umożliwić Administratorowi przeprowadzenie kontroli we wskazanym przez Administratora terminie.

1. Podmiot przetwarzający ma obowiązek zastosować się do wskazań Administratora mających na celu usunięcie stwierdzonych uchybień lub poprawę stanu bezpieczeństwa danych osobowych. W przypadku przekazania przez Administratora stosownych uwag Podmiot przetwarzający zobowiązany jest, w terminie 7 dni roboczych od otrzymania zawiadomienia od Administratora, do wskazania Administratorowi sposobu oraz terminu usunięcia uchybień lub poprawy stanu bezpieczeństwa przetwarzania danych osobowych, przy czym termin ten nie może być jednak dłuższym niż 14 dni roboczych.
2. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy i wyłącznie po uzyskaniu przez Podmiot przetwarzający każdorazowej zgody Administratora udzielonej w formie pisemnej pod rygorem nieważności. Podmiot przetwarzający przekazuje Administratorowi dane podmiotów, którym dane mają zostać powierzone.
3. Podmiot przetwarzający zobowiązany jest przedstawić projekt Umowy podpowierzenia przetwarzania danych osobowych Administratorowi przed uzyskaniem jego zgody oraz zapewnić, że treść Umowy podpowierzenia przetwarzania danych będzie zabezpieczać interes Administratora co najmniej na takim poziomie, jak niniejsza Umowa. W szczególności Umowa podpowierzenia przetwarzania danych winna zapewniać, że Podwykonawca spełnia te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie i uprawniać Administratora do bezpośredniego przeprowadzenia pełnej kontroli przetwarzania danych osobowych przez podwykonawcę, któremu Podmiot przetwarzający powierzył dalsze przetwarzanie danych osobowych. Jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków, Podmiot przetwarzający ponosi odpowiedzialność wobec Administratora za takie zachowanie podwykonawcy jak za własne działania lub zaniechania zgodnie z postanowieniami niniejszej Umowy.
4. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora 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 o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
5. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią niniejszej Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
6. 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 jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego w zakresie dotyczącym wyłącznie danych osobowych powierzonych przez Administratora.
7. Podmiot przetwarzający, bez zbędnej zwłoki, zobowiązuje się do poinformowania Administratora o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach dotyczących przetwarzania w Podmiocie przetwarzającym danych osobowych, w szczególności prowadzonych przez organ nadzorczy, w zakresie, w jakim kontrola ta będzie dotyczyć danych osobowych powierzonych przez Administratora.
8. W razie naruszenia przez Podmiot przetwarzający ochrony danych osobowych powierzonych do przetwarzania skutkującego nałożeniem na Administratora administracyjnej kary pieniężnej określonej w art. 83 RODO oraz odszkodowania zasądzonego na rzecz osoby, której dane osobowe dotyczą w trybie art. 82 RODO, Administratorowi przysługuje odszkodowanie od podmiotu przetwarzającego w wysokości nałożonej administracyjnej kary pieniężnej oraz kwoty zasądzonego odszkodowania na rzecz osoby, której dane dotyczą.
9. 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, zwanych dalej danymi poufnymi.
10. 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 w innym celu niż wykonanie postanowień niniejszej Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub niniejszej Umowy.
11. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.
12. Administrator zezwala na zdalny dostęp Podmiotowi przetwarzającemu do systemu informatycznego tylko na żądania zatwierdzone przez **pracownika IT** zgodnie z niniejszymi zasadami:

* Połączenie jest uruchamiane przez **pracownia IT** tylko na czas potrzebny na wykonanie prac serwisowych.
* Zdalny dostęp jest możliwy tylko za pomocą szyfrowanej transmisji za pośrednictwem połączenia VPN lub Tunelu SSH.

1. Dni robocze na potrzeby niniejszej Umowy oznaczają dni tygodnia od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu Cywilnego oraz RODO oraz właściwe przepisy prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Sądem właściwym dla rozpatrzenia sporów wynikłych z niniejszej Umowy będzie sąd właściwy dla siedziby powoda.

Podmiot przetwarzający Administrator (podpis i pieczęć) (podpis i pieczęć)

\* niepotrzebne skreślić