

Umowa powierzenia przetwarzania danych osobowych do Umowy ...

zawarta w dniu2019 r. w Bydgoszczy, pomiędzy:

Szpitałem Uniwersyteckim nr 2 im. dr J. Biziela w Bydgoszczy (85-168 Bydgoszcz, ul. Ujejskiego 75) wpisanym pod numerem KRS 0000316960 do Rejestru Stowarzyszeń i Innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej Krajowego Rejestru Sądowego (sąd rejestrowy: Sąd Rejonowy w Bydgoszczy-XIII Wydział Gospodarczy Krajowego Rejestru Sądowego), NIP 95-325-82-266

reprezentowanym przez:

Dyrektora dr n. med. Wandę Korzycką- Wilińską

zwanym w treści umowy „Administrator”

a

....

reprezentowanym przez:

.....

zwanym w treści umowy „Przetwarzającym”

(dalej łącznie jako: „**Strony**”)

Mając na uwadze, że:

- 1) Strony zawarły umowę z dnia („**Umowa Podstawowa**”), w związku z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie Danych Osobowych, zwanych dalej także „**Danymi**” w zakresie określonym Umową;
- 2) Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;
- 3) 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 zwanej także **RODO**,

Strony postanowiły zawrzeć Umowę o następującej treści:

1. Opis Przetwarzania

- 1.1. **Przedmiot [art. 28 ust. 3 RODO]** Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.

1.2. **Czas [art. 28 ust. 3 RODO]** Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej oraz po jej zakończeniu przez okres wynikający z powszechnie obowiązujących przepisów prawa.

1.3. **Charakter i cel [art. 28 ust. 3 RODO]** Charakter i cel przetwarzania uzasadnia Umowa Podstawowa.

1.3.1. charakter przetwarzania określony obowiązkami Przetwarzającego określa Umowa Podstawowa,

1.3.2. celem przetwarzania są działania związane z przygotowaniem i realizacją prowadzonych u Administratora badań klinicznych, w zakresie określonym Umową Podstawową

1.4. **Rodzaj danych [art. 28 ust. 3 RODO]** Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („Dane”):

Dane zwykłe i szczególne kategorie danych :

1.4.1. imię i nazwisko pacjenta,

1.4.2. jego numer ewidencyjny PESEL,

1.4.3. jego numery telefonów,

1.4.4. jego adres zamieszkania/nazwa oddziału szpitalnego,

1.4.5. jego data urodzenia,

1.4.6. jego seria i numer dokumentu tożsamości, imiona rodziców, płeć,

1.4.7. numer identyfikacyjny pacjenta,

1.4.8. dane dotyczące zdrowia pacjenta związane z prowadzonymi badaniami

1.4.9. dane osoby upoważnionej (nazwisko, imię, telefon, PESEL, adres) do dostępu do dokumentacji badania,

1.4.10. dane innych osób udzielających świadczeń w imieniu Administratora tj. imię nazwisko, tytuł naukowy

1.5. **Kategorie osób [art. 28 ust. 3 RODO]** Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:

1.5.1 pacjentów Administratora,

1.5.2 osób upoważnionych przez pacjenta,

1.5.3 osób udzielających świadczeń zdrowotnych w imieniu Udzielającego zamówienia.

2. Podpowierzenie

2.1. **Podpowierzenie [art. 28 ust. 2 RODO]** Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („**podpowierzenie**”) w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**”) innym podmiotom przetwarzającym. („**Podprzetwarzający**”), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2.2. **Sprzeciw.** Powierzenie przetwarzania Danych Podprzetwarzającym spoza Listy Zaakceptowanych Podprzetwarzających wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia

wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu w terminie 7 dni od daty zgłoszenia tego faktu przez Przetwarzającego. W razie zgłoszenia uzasadnionego sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem. Zastrzeżenia co do zasadności sprzeciwu i ewentualne jego negatywne konsekwencje Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

2.3. Transfer obowiązków [art. 28 ust. 4 RODO] Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

2.4. Zobowiązanie względem Administratora. Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie 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.

2.5. Zakaz podzlecenia świadczenia głównego [art. 28 ust. 4 RODO] Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

2.6. Podmiot przetwarzający dostarczy Administratorowi **Porozumienie ws podpowierzenia przetwarzania danych osobowych**, w przypadku, jeżeli takie porozumienie zostanie zawarte.

3. Obowiązki Przetwarzającego

Przetwarzający ma następujące obowiązki:

3.1. Udokumentowane polecenia [art. 28 ust. 3 lit. a RODO] Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

3.2. Nieprzetwarzanie poza EOG [art. 28 ust. 3 lit. a RODO] 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 Podprzetwarzających, którzy przekazują Dane poza EOG.

3.3. Poinformowanie o zamiarze przetwarzania poza EOG. [art. 28 ust. 3 lit. a RODO] 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.

3.4. Tajemnica [art. 28 ust. 3 lit. b RODO] Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

3.5. Bezpieczeństwo [art. 28 ust. 3 lit. c RODO] Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony Danych, o których mowa w art. 32 RODO, w zgodzie z dalszymi postanowieniami Umowy.

3.6. Podprzetwarzanie [art. 28 ust. 3 lit. d RODO] Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego).

3.7. Współpraca przy realizacji praw jednostki [art. 28 ust. 3 lit. e RODO] Przetwarzający zobowiązuje się wobec Administratora, w miarę możliwości, do pomocy w odpowiadaniu na żądania osoby,

której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („Prawa jednostki”). Szczegóły obsługi Praw jednostki zostaną uzgodnione pomiędzy Stronami.

- 3.8. **Wsparcie przy obowiązkach bezpieczeństwa [art. 28 ust. 3 lit. f RODO]** Przetwarzający, uwzględniając charakter przetwarzania oraz odstępnę mu informacje pomaga Administratorowi wywiązać się z obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32–36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).
- 3.9. **Legalność poleceń** Jeżeli Przetwarzający 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). Przetwarzający odpowiada wobec Administratora za szkodę wyrządzoną brakiem informacji, nieprawidłową informacją lub spóźnioną informacją.
- 3.10. **Projektowanie prywatności [art. 25 ust. 1 RODO]** 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.
- 3.11. **Minimalizacja [art. 25 ust. 2 RODO]** Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.
- 3.12. **RCPD [art. 30 ust. 2 RODO]** Przetwarzający zobowiązuje się do prowadzenia rejestru czynności przetwarzania danych osobowych w imieniu administratora, w tym (wymóg art. 30 RODO). Przetwarzający udostępniania na uzasadnione żądanie Administratora, jak również na żądanie właściwych organów nadzoru prowadzony rejestr czynności przetwarzania danych przetwarzającego, w odniesieniu do Administratora z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.
- 3.13. **Profilowanie [art. 22 RODO]** 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.
- 3.14. **Szkolenie personelu** Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

4. Obowiązki Administratora

- 4.1. Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

5. Bezpieczeństwo danych

- 5.1. **Bezpieczeństwo danych osobowych [art. 32 RODO]** Strony przeprowadziły analizę ryzyka przetwarzania Danych, i stosują odpowiednie organizacyjne i techniczne środki ochrony danych zgodnie z art. 32 RODO.

6. Powiadomienie o Naruszeniach Danych Osobowych [art. 33 RODO]

6.1. **Powiadomienie o naruszeniu.** Przetwarzający powiadamia niezwłocznie Administratora, nie później niż 24 od stwierdzenia naruszenia danych o każdym naruszeniu ochrony Danych, informuje Administratora o czynnościach wyjaśniających i o ustaleniach z chwilą ich dokonania. W razie opóźnienia w zgłoszeniu Przetwarzający informuje również o przyczynach opóźnienia. Przetwarzający odpowiada przed Administratorem za negatywne skutki poniesione przez Administratora wskutek opóźnienia w zgłoszeniu.

6.2. **Rozwinięcie.** Powiadomienie o stwierdzeniu naruszenia odpowiadać musi wymogom art. 33 ust. 3 RODO aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.

7. Nadzór

7.1. **Sprawowanie kontroli [art. 28 ust. 3 lit. h RODO]** Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do:

7.1.2 przeprowadzania audytów lub inspekcji, o których Administrator informuje Przetwarzającego, co najmniej z 7 dniowym wyprzedzeniem; Administrator ma prawo kontrolować Przetwarzającego dwa razy w ciągu każdego roku obowiązywania umowy, chyba, że doszło do naruszenia przetwarzania Danych lub podejrzenia takiego naruszenia, Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji;

7.1.3 do żądania od Przetwarzającego udzielania informacji niezbędnych do wykazania spełnienia obowiązków wynikających z RODO i niniejszej umowy, w szczególności dotyczących przebiegu przetwarzania Danych Osobowych,

7.2. **Współpraca przy kontroli. [art. 28 ust. 3 lit. h RODO]** Przetwarzający współpracuje z organem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

8. Oświadczenia Stron

8.2. **Oświadczenie Administratora.** Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

8.3. **Oświadczenie Przetwarzającego [art. 28 ust. 1 RODO].** Przetwarzający oświadcza, że w ramach prowadzonej działalności przetwarzane dane osobowe w zakresie objętym Umową i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

8.4. **Referencje [art. 28 ust. 1 RODO].** Na uzasadnione żądanie Administratora Przetwarzający przekaze Administratorowi stosowne informacje lub dowody, iż Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

9. Odpowiedzialność

9.2. **Odpowiedzialność Przetwarzającego [art. 82 ust. 3 RODO]** Przetwarzający odpowiada za szkody spowodowane swoim działaniem lub zaniechaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

- 9.3. **Odpowiedzialność za Podprzetwarzających [art. 28 ust. 4 RODO]** Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

10. Okres Obowiązywania Umowy Powierzenia [art. 28 ust. 3 RODO]

- 10.1. Umowa została zawarta na czas obowiązywania Umowy Podstawowej.

11. Usunięcie Danych

- 11.2. **Usunięcie danych [art. 28 ust. 3 lit g RODO]** Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:

11.2.1 usunięcia Danych i usunięcia wszelkich ich istniejących kopii,

lub

11.2.2 zwrotu Danych,

chyba, że prawo Unii Europejskiej lub prawo polskie stanowi inaczej, w szczególności z uwagi na terminy przechowywania dokumentacji medycznej i odpowiedzialność solidarną Administratora i Przetwarzającego za udzielone na podstawie Umowy podstawowej świadczenia.

- 11.3. **Karencja.** Przetwarzający dokona usunięcia Danych lub zwrotu Danych w terminie uzgodnionym z Administratorem uwzględniającym normalny czas konieczny na realizację tego obowiązku w normalnym trybie czynności.

12. Postanowienia Końcowe

- 12.1. **Pierwszeństwo.** 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.

- 12.2. **Egzemplarze.** Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

- 12.3. **Właściwość prawa.** Umowa podlega prawu polskiemu oraz RODO.

Administrator

Przetwarzający