Załącznik nr 3

Umowa powierzenia przetwarzania danych osobowych
zawarta dnia _____ pomiędzy:
(zwana dalej „Umową")

Uniwersyteckim Szpitalem Klinicznym im. Jana Mikulicza-Radeckiego we Wrocławiu, ul. Borowska 213, 50-556 Wrocław,
zwany w dalszej części umowy **„Administratorem danych" lub „Administratorem"**
reprezentowanym przez: **Beatę Freier - Dyrektora**

a

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

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części RODO) 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, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy dane osobowe pracowników Administratora w postaci: imienia i nazwiska, stanowiska służbowego, numeru telefonu służbowego, służbowego adresu mailowego oraz dane osobowe użytkowników serwisu internetowego w postaci adresu IP.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy głównej z dnia ……. nr …….. .

§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 RODO.
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. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. 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 RODO.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin.
8. Podmiot przetwarzający wypełnia „Ankietę bezpieczeństwa danych osobowych dla podmiotu przetwarzającego” (Załącznik nr 1).

§4
Prawo kontroli

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

§5
Przekazywanie danych do krajów trzecich

1. W przypadku przekazywania danych osobowych do państwa trzeciego (spoza Europejskiego Obszaru Gospodarczego) dodatkowo zastosowanie mają Standardowe Klauzule Umowne (Moduł drugi – przekazywanie danych przez Administratora dla podmiotu przetwarzającego) dotyczące przekazywania danych osobowych do państw trzecich na podstawie przepisów RODO (rozdział V). W przypadku transferu danych do podmiotu przetwarzającego, który posiada siedzibę w USA i który przystąpił do programu “ Ram Ochrony Danych UE-USA” (zgodnie z decyzją KE z 10 lipca 2023 r.) stosowanie Standardowych Klauzul Umownych nie jest konieczne. Stosowanie przedmiotowych klauzul nie jest konieczne również w przypadku transferu danych do tych państw, które zapewniają odpowiedni poziom ochrony danych na podstawie decyzji Komisji Europejskiej.

§6
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 Administratora 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 ust. 1 winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 7

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 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 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 inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§8

Czas obowiązywania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia na czas trwania umowy głównej nr…….. z dnia ……

§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 i RODO;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§10

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.

§11
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 RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla siedziby Administratora danych.
4. Zmiany niniejszej Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.

…….. ……

Administrator danych Podmiot przetwarzający

Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych

ANKIETA BEZPIECZEŃSTWA DANYCH OSOBOWYCH DLA PODMIOTU PRZETWARZAJĄCEGO

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 powierzone dane osobowe będą przetwarzane w postaci anonimowej czy pseudoanonimowej, czy też bez anonimizacji?		
3	Czy Państwa personel został przeszkolony z zasad przetwarzania danych osobowych zgodnych z RODO, w tym zasad bezpieczeństwa przetwarzania?		
4	Czy Państwo korzystają z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez Państwa sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?		
5	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?		
6	Jeśli tak to w jakim kraju?		
7	Czy w Państwa organizacji przeprowadzane są okresowe audyty zgodności z przepisami ochrony danych osobowych?		
8	Czy w Państwa organizacji przeprowadzane są okresowe audyty bezpieczeństwa IT?		
9	Czy posiadają Państwo wdrożoną politykę ochrony danych osobowych zgodną z zasadami RODO?		
10	Czy prowadzą Państwo rejestr czynności przetwarzania, w tym dla procesora rejestr kategorii czynności przetwarzania, zgodnie z art. 30 RODO?		

11	Czy jesteście Państwo zobowiązani do wyznaczenia Inspektora Ochrony Danych, zgodnie z art. 37 RODO?		
12	Jeśli tak, to czy wyznaczono Inspektora Ochrony Danych?		
13	Jeśli nie, to czy wyznaczyli Państwo osobę, która będzie odpowiedzialna za koordynację zapewnienia zgodności przetwarzania danych z przepisami o ochronie danych osobowych		
14	Czy do przetwarzania danych w Państwa organizacji są dopuszczone wyłącznie osoby posiadające upoważnienia?		
15	Czy osoby te zostały zobowiązane do zachowania poufności danych oraz informacji o stosowanych przez Państwa zabezpieczeniach?		
16	Czy korzystają Państwo z usług podwykonawców i podpowierzają lub planują podpowierzyć im przetwarzanie danych przekazanych przez administratora danych?		
17	Jeśli tak, to czy z podwykonawcami zawarto pisemne umowy powierzenia danych odpowiadające wymogom określonym w art. 28 RODO?		
18	Czy wdrożyli Państwo instrukcję postępowania w przypadku sytuacji naruszenia ochrony danych osobowych?		
19	Jeśli tak, to czy zgodnie z tą instrukcją zdołają Państwo przekazać administratorowi danych informacje o incydencie w ciągu 24 godzin od stwierdzenia naruszenia?		
20	Czy w celu zaplanowania środków bezpieczeństwa przetwarzania danych przeprowadzono ocenę skutków dla ochrony danych?		
21	Czy wdrożyli Państwo system zarządzania bezpieczeństwem informacji np. ISO 27001?		
22	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.		
23	Czy przetwarzanie danych było już przedmiotem zewnętrznych audytów lub kontroli, np. UODO w Państwa organizacji?		
24	Jeśli tak, proszę zwięźle opisać wyniki kontroli/ audytów		
25	Czy posiadają Państwo wdrożoną instrukcję zarządzania systemami IT służącymi do przetwarzania danych osobowych lub inne dokumenty wewnętrzne regulujące zasady zarządzania infrastrukturą IT?		

26	Czy Państwa systemy IT zapewniają rozliczalność operacji wykonywanych na danych osobowych, tzn. czy odnotowują nazwę użytkownika, datę oraz charakter operacji wykonanej na konkretnym rekordzie w bazie?		
27	Czy w przypadku przekazywania danych osobowych środkami telekomunikacyjnymi lub na nośnikach zewnętrznych, przekazywane dane są szyfrowane?		
28	Czy stosują Państwo pseudonimizację i szyfrowanie danych?		
29	Czy podjęli Państwo środki, aby zapewnić zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania?		
30	Czy w Państwa organizacji są stosowane środki służące ochronie systemów IT przed działaniem tzw. złośliwego oprogramowania?		
31	Jeśli tak, to czy podlegają one cyklicznej aktualizacji?		
32	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		
33	Czy dostęp do systemów IT wymaga uwierzytelniania użytkownika tj. podania indywidualnego identyfikatora i hasła?		
34	Jeśli tak, to czy zastosowano systemowe mechanizmy wymuszające okresowe zmiany haseł użytkowników?		
35	Czy posiadają Państwo politykę zarządzania kopiami zapasowymi?		

……..

data i czytelny podpis osoby upoważnionej do reprezentacji podmiotu przetwarzającego