UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta dnia _____ w Chorzowie pomiędzy

Administratorem danych:	Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Zespołem Szpitali Miejskich Strzelców Bytomskich 11, 41-500 Chorzów NIP: 6271923530, REGON: 271503410, KRS: 0000011939 Reprezentowanym przez **Jerzego Szafranowicza** - dyrektora
Podmiotem Przetwarzającym:	_____ _____ _____ Reprezentowanym przez _____ - _____

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz.UE.L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem"), na zasadach, w zakresie i w celu określonych w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.

§ 2
Zakres i cel przetwarzania danych

1. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy Głównej **(numer, data zawarcia, przedmiot umowy głównej w celu realizacji której następuje powierzenie przetwarzania danych osobowych).**
2. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie niniejszej Umowy dane osobowe następujących kategorii:
   (kategorie danych osobowych, np. imiona i nazwiska, adresy zamieszkania, numery PESEL, informacje o stanie zdrowia itd.).
   dotyczące następujących kategorii osób:
   kategorię osób, których dane dotyczą, np. pracowników administratora, pacjentów administratora, kontrahentów administratora itd.
   stanowiące ☐ **dane osobowe zwykłe;** ☐ **dane osobowe szczególnych kategorii.**
3. Zakres danych osobowych wymienionych w ust. 2 powyżej jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy Głównej. W rzeczywistości dane mogą być przekazywane przez Administratora w mniejszym zakresie bez uszczerbku dla postanowień niniejszej Umowy.
4. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych:
   ☐**utrwalanie,** ☐**organizowanie,** ☐**porządkowanie,** ☐**przechowywanie,** ☐**adaptowanie lub modyfikowanie,** ☐ **pobieranie,** ☐ **przeglądanie,** ☐ **wykorzystywanie,** ☐ **ujawnianie poprzez przesłanie,** ☐ **rozpowszechnianie lub innego rodzaju udostępnianie,** ☐ **dopasowywanie lub łączenie,** ☐ **ograniczanie,** ☐ **usuwanie lub niszczenie**
   które są w minimalnym zakresie niezbędne do realizacji celu, o którym mowa w ust. 2 powyżej.

§ 3
Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z Rozporządzeniem, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Lista środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający stanowi załącznik nr 1 do niniejszej Umowy.
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 osobowe, przy czym będą to wyłącznie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych, a przetwarzanie przez nich danych osobowych objętych Umową jest niezbędne do realizacji celu niniejszej Umowy oraz Umowy Głównej.
4. Podmiot przetwarzający zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby, o których mowa w niniejszym ustępie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
5. Dla zapewnienia prawidłowej realizacji ust. 4 powyżej Podmiot przetwarzający dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora danych.
6. Podmiot przetwarzający pomaga Administratorowi danych w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 Rozporządzenia. Podmiot przetwarzający – w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora danych w terminie 5 dni roboczych od otrzymania wiadomości. Udzielając informacji, Podmiot

przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.

7. W przypadku stwierdzenia jakiegokolwiek naruszenia ochrony danych osobowych Podmiot przetwarzający lub podwykonawca Podmiotu przetwarzającego zgłasza je Administratorowi danych w ciągu 24h od stwierdzenia przez niego wystąpienia naruszenia ochrony danych osobowych.
8. Zgłoszenie o którym mowa w ust. 8 powyżej powinno zawierać co najmniej:
   a) datę i godzinę stwierdzenia naruszenia ochrony danych osobowych,
   b) czas trwania naruszenia ochrony danych osobowych,
   c) opis naruszenia ochrony danych osobowych wraz z opisem sposobu wykrycia,
   d) informację o danych osobowych, których dotyczyło naruszenie,
   e) informację o przyczynie naruszenia ochrony danych osobowych,
   f) informację o osobach, których danych dotyczyło naruszenie wraz z informacją o tym, czy osoby te zostały poinformowane o naruszenie,
   g) opis działań podjętych w związku ze stwierdzonym naruszeniem ochrony danych.

§ 4
Prawo kontroli

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo kontroli, mającej na celu weryfikację, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych będzie realizować prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 5 dniowym uprzedzeniem.
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni.
5. Określone powyżej zasady kontroli Podmiotu przetwarzającego mają zastosowanie do przeprowadzanych przez Administratora danych kontroli podwykonawców Podmiotu przetwarzającego, o których mowa w § 6 ust. 1 niniejszej Umowy.

§ 5
Raportowanie

1. Na wniosek Administratora danych Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z Rozporządzenia.
2. Informacji, o których mowa w ust. 1 powyżej, udziela się w terminie 7 dni od dnia doręczenia wniosku, z zastrzeżeniem ust. 3 poniżej.
3. Jeżeli wniosek, o którym mowa w ust. 1 powyżej, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 12 godzin od doręczenia wniosku.

§ 6
Dalsze powierzenie danych do przetwarzania

1. Administrator danych wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania przez podwykonawców Podmiotu przetwarzającego (podpowierzenie), w celu wykonania niniejszej Umowy, przy czym podwykonawcy Podmiotu przetwarzającego powinni spełniać co najmniej te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający niniejszą Umową. Lista podmiotów (podprocesorów) w odniesieniu do których Administrator danych wyraża zgodę na podpowierzenie przetwarzania danych stanowi załącznik nr 2 do niniejszej Umowy.
2. W przypadku zmiany lub dodania innych podwykonawców biorących udział w przetwarzaniu danych powierzonych przez Administratora danych Podmiot przetwarzający informuje o zamierzonych zmianach, dając Administratorowi danych możliwość wyrażenia sprzeciwu wobec takich zmian w terminie 5 dni roboczych od przekazania informacji o zamierzonych zmianach.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora danych, chyba że taki obowiązek nakłada na Podmiot przetwarzający prawo Unii Europejskiej 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.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora danych za niewywiązanie się z obowiązków spoczywających na podwykonawcy, wynikających z niniejszej Umowy.

§ 7
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią niniejszej Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
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 niniejszej Umowie, o jakiejkolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu

dotyczących 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 zostaje zawarta na czas obowiązywania określonej w § 2 ust. 1 Umowy Głównej.
2. Każda ze stron może rozwiązać niniejszą Umowę za uprzednim 1-miesięcznym okresem wypowiedzenia..

§ 9
Osoby odpowiedzialne za realizację umowy

3. Strony wyznaczają następujące osoby odpowiedzialne za realizację niniejszej Umowy:
   a) ze strony Administratora: Grzegorz Koczy, e-mail: iod@zsm.com.pl, tel.: 32 349 92 67
   b) ze strony Podmiotu Przetwarzającego _____, e-mail:_____, tel.: _____

§ 10
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 niniejszą Umową,
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 11
Usunięcie danych po rozwiązaniu Umowy

1. Z chwilą zakończenia obowiązywania niniejszej Umowy Podmiot przetwarzający jest zobowiązany do:
   a) zwrotu danych osobowych powierzonych do przetwarzania w związku z realizacją niniejszej Umowy;
   b) usunięcia wszelkich istniejących kopii danych osobowych powierzonych do przetwarzania w związku z realizacją niniejszej Umowy, chyba że Administrator danych postanowi inaczej lub prawo Unii Europejskiej bądź prawo państwa członkowskiego nakazują dalsze przetwarzanie danych osobowych.
2. Zwrot lub usunięcie przez Podmiot przetwarzający danych osobowych następuje niezwłocznie, jednak nie później niż w terminie 14 dni od dnia zakończenia obowiązywania niniejszej Umowy.
3. Wykonanie obowiązku, o którym mowa w ust. 1 lit. a) powyżej zostanie potwierdzone pisemnym protokołem podpisanym przez przedstawicieli Administratora danych i Podmiotu przetwarzającego.
4. Wykonanie obowiązku, o którym mowa w ust. 1 lit. b) powyżej zostanie potwierdzone pisemnym oświadczeniem złożonym przez Podmiot przetwarzający.

§ 12
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, a także danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie niniejszej Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub treści niniejszej Umowy.

§ 13
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych niniejsza Umową, zastosowanie będą miały odpowiednie przepisy Kodeksu cywilnego oraz Rozporządzenia o którym mowa w § 1 ust. 1, a także innych aktów prawnych.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla siedziby Administratora danych.

§ 14
Załączniki

1. Załącznik nr 1. Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający w celu zapewnienia poufności, integralności i dostępności powierzonych danych osobowych.
2. Załącznik nr 2. Wykaz podprocesorów Podmiotu przetwarzającego.

Administrator danych	**Podmiot Przetwarzający**

Załącznik nr 1. Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający w celu zapewnienia poufności, integralności i dostępności powierzonych danych osobowych.

Lp.	Pytanie	Odpowiedź
1	Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
2	Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
3	Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
4	Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
5	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy?	
6	Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia?	
7	Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	
8	Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?	
9	Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
10	Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji?	
11	Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany?	
12	Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych?	
13	Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby?	
14	Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób?	
15	Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	

16	Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka?	
17	Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	
18	Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach?	
19	Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane?	
20	Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych?	
21	Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu?	
22	Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych?	
23	Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe?	
24	Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
25	Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych?	
26	Gdzie są przechowywane kopie zapasowe?	
27	Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania?	
28	Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design?	
29	Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default?	
30	Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych?	
31	Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	

Załącznik nr 2. Wykaz podprocesorów Podmiotu przetwarzającego

Podmiot przetwarzający będzie zlecał przetwarzanie powierzonych mu danych osobowych następującym podmiotom:

Nazwa podprocesora	Adres siedziby podprocesora