Załącznik nr 9

Umowa powierzenia przetwarzania danych osobowych

Zawarta w ..... w dniu ..... pomiędzy:

Zespołem Opieki Zdrowotnej w Świętochłowicach spółka z ograniczoną odpowiedzialnością z siedzibą w Świętochłowicach (kod: 41 – 605), przy ulicy Chorzowskiej nr 38, wpisanym do Krajowego Rejestru Sądowego w Sądzie Rejonowym Katowice – Wschód w Katowicach, Wydział VIII Gospodarczy Krajowego Rejestru Sądowego, nr KRS: 0000426290, Nr NIP: 627-16-69-770, REGON: 000311450

reprezentowanym przez:
Prezesa Zarządu: Anitę Przytocką
Prokurenta: Bogumiłę Wolny
zwaną w dalszej treści umowy **„Administratorem Danych"** (dalej **„Udzielającym Zamówienia")**

a
(Nazwa Firmy, Adres, NIP, REGON)

reprezentowaną przez:

- .....

zwaną dalej **„Podmiotem przetwarzającym"** (dalej **„Przyjmującym Zamówienie")**

łącznie zwani Stronami

Preambuła

Zważywszy, iż Strony zawarły umowę z dnia ..... (dalej „Umowa"), **przedmiotem której jest świadczenie usług w zakresie wykonywania badań laboratoryjnych opisanych szczegółowo w SWKO „Na udzielenie zamówienia na świadczenia zdrowotne w zakresie wykonywania badań laboratoryjnych, mikrobiologicznych, serologii krwi i prowadzenia Banku Krwi w zespole opieki zdrowotnej w Świętochłowicach sp. z o.o. wraz z dzierżawą pomieszczeń laboratorium analitycznego"** Udzielający Zamówienia powierza Przyjmującemu Zamówienie w trybie art. 28 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 dalej jako **„RODO"**, przetwarzanie danych osobowych, których Administratorem Danych jest wyłącznie Udzielający Zamówienie.

§1
Postanowienia podstawowe umowy

1. Udzielający Zamówienie jako Administrator Danych Osobowych, w rozumieniu 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 dalej jako **„RODO"**, w związku z art. 28 RODO powierza Przyjmującemu Zamówienie przetwarzanie danych osobowych w zakresie niezbędnym do realizacji Umowy.
2. Przyjmujący Zamówienie może przetwarzać powierzone dane osobowe jedynie w celu prawidłowej realizacji usług określonych w Umowie oraz w zakresie niezbędnym do prawidłowej realizacji jej przedmiotu.

3. Szczegółowy opis przedmiotu i czasu trwania przetwarzania, charakteru i celu przetwarzania, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą został określony w **Załączniku nr 1** do niniejszej umowy.
4. Przyjmujący Zamówienie ma prawo dalszego powierzenia danych osobowych, o których mowa w niniejszej umowie w zakresie i celu niezbędnym do realizacji przedmiotu Umowy (ogólna zgoda administratora na podpowierzenie danych osobowych). Przyjmujący Zamówienie jest zobowiązany do poinformowania Udzielającego Zamówienia o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających przed faktycznym rozpoczęciem korzystania z usług tych podmiotów, dając tym samym Zleceniodawcy możliwość wyrażenia sprzeciwu wobec takich planowanych zmian, przy czym okres na złożenie sprzeciwu przez Zleceniodawcę wynosi 7 dni od daty powiadomienia Udzielającego Zamówienia przez Przyjmującego Zamówienie o planowanych zmianach dotyczących dodania lub zastąpienia podmiotów przetwarzających.
5. Niezależnie od trybu przewidzianego w ustępie 4 powyżej, Przyjmujący Zamówienie informuje niniejszym Udzielającego Zamówienia, iż korzysta z podwykonawców wskazanych w **Załączniku nr 2.**
6. W przypadku dalszego powierzenia danych osobowych przez Przyjmującego Zamówienie podmiotom przetwarzającym, o których mowa w ust. 4 i 5 powyżej, Przyjmujący Zamówienie zawrze z tymi podmiotami stosowne umowy powierzenia danych uwzględniające obowiązki określone w niniejszej umowie.
7. Przyjmujący Zamówienie zobowiązuje się do wydania imiennych upoważnień do przetwarzania danych osobowych osobom, którym umożliwi dostęp do powierzonych na mocy niniejszej umowy danych osobowych. Jednocześnie Przyjmujący Zamówienie zobowiązuje się zapewnić, że każda osoba przez niego upoważniona do przetwarzania powierzonych danych osobowych zostanie zobowiązana do zachowania w tajemnicy tych danych, a także informacji o stosowanych wobec nich środkach bezpieczeństwa zarówno w trakcie trwania zatrudnienia bądź współpracy, jak i po ustaniu zatrudnienia lub współpracy.

§2

Postanowienia związane ze stosowaniem wymagań RODO

1. Przyjmujący Zamówienie, jako podmiot przetwarzający powierzone dane osobowe, będzie dążył do wypracowania ze Zleceniodawcą wszelkich niezbędnych rozwiązań, a także do stosowania dodatkowych względem określonych w § 1 obowiązków podmiotu przetwarzającego określonych w art. 28 RODO, w tym w szczególności zobowiązuje się:

a) przetwarzać powierzone dane osobowe wyłącznie na udokumentowane polecenie Udzielającego Zamówienie jako administratora, chyba że obowiązek przetwarzania danych nakładają na Zleceniobiorcę przepisy prawa Unii lub państwa członkowskiego, którym podlega Przyjmujący Zamówienie. W takim wypadku Przyjmujący Zamówienie przed rozpoczęciem przetwarzania danych poinformuje Udzielającego Zamówienia o wiążącym go obowiązku prawnym, o ile dane przepisy prawa nie zabraniają udzielenia takiej informacji z uwagi na ważny interes publiczny;

b) przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego zgodnie z zasadami określonymi w § 1 ust. 4 - 6 niniejszej umowy;

c) biorąc pod uwagę charakter przetwarzania powierzonych danych osobowych, zakres i sposób wsparcia Zleceniodawcy w ramach realizacji Umowy, w miarę możliwości pomagać Zleceniodawcy 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;

d) uwzględniając charakter przetwarzania danych oraz dostępne Przyjmującego Zamówienie informacje, pomagać Udzielającemu Zamówienie w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.

2. Niezależnie od postanowień ustępów poprzedzających Przyjmujący Zamówienie zobowiązuje się wdrożyć wymagane środki techniczne i organizacyjne służące spełnieniu wymagań art. 32 RODO, które będą miały wobec niego zastosowanie jako podmiotu przetwarzającego.
3. Wykaz środków technicznych i organizacyjnych stosowanych przez Zleceniobiorcę na dzień podpisania niniejszej Umowy został określony w **Załączniku nr 3.**

§3

Wzajemna komunikacja

1. Strony wyznaczają swoich przedstawicieli w celu zapewnienia wzajemnej komunikacji w zakresie realizacji przedmiotu niniejszej umowy:

a) po stronie Udzielającego Zamówienie:
Pani Agnieszka Stelmaczonek – Inspektor Ochrony Danych. Kontakt: e-mail: iodo@zoz.net.pl

b) po stronie Przyjmującego Zamówienie:
..... Kontakt: e-mail:....., tel. .....

2. Zmiana osób, o których mowa w ust. 1 nie wymaga zmiany niniejszej umowy i następuje poprzez wzajemne zawiadomienie przez Strony.
3. Przyjmujący Zamówienie zobowiązany jest do zgłaszania do Udzielającego Zamówienie wszelkich przypadków związanych naruszeniami ochrony powierzonych danych osobowych – niezwłocznie, w miarę swoich możliwości w ciągu 48 godzin po stwierdzeniu naruszenia ochrony danych osobowych.
4. Przyjmujący Zamówienie zobowiązuje się do pełnej współpracy z Udzielającym Zamówienie w zakresie realizacji przedmiotu niniejszej umowy, w tym w zakresie komunikacji, o której mowa w ust. 3 oraz do udostępniania Udzielającemu Zamówienie jako administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w niniejszej umowie, w zakresie odnoszącym się do powierzonych na mocy niniejszej umowy danych osobowych. Udostępnienie informacji, o których mowa w zdaniu poprzedzającym następuje na każdorazowe pisemne żądanie Udzielającego Zamówienie w terminie 7 dni roboczych od dnia wpłynięcia żądania do Przyjmującego Zamówienie.

§4

Prawo audytu

1. Udzielający Zamówienie zastrzega sobie możliwość skorzystania z prawa kontroli poprzez przeprowadzanie audytu działalności Przyjmującego Zamówienie zgodnie z wymaganiami niniejszej umowy oraz aktualnie obowiązujących przepisów prawa z zakresu ochrony danych osobowych (w tym w szczególności RODO) na zasadach określonych w niniejszym Paragrafie, a Przyjmujący Zamówienie przyjmuje to zobowiązanie.
2. Audyt, o którym mowa w ust. 1 może być przeprowadzany wyłącznie przez pisemnie upoważnionych przez Udzielającego Zamówienie pracowników lub audytorów oraz pod warunkiem pisemnego zobowiązania ich do zachowania w tajemnicy wszelkich informacji uzyskanych w trakcie prowadzonych czynności audytowych.
3. Audyt, o którym mowa w ust. 1 może się odnosić wyłącznie do powierzonych przez Udzielającego Zamówienie danych osobowych i wykorzystywanych do tego narzędzi, infrastruktury i procedur. Sposób przeprowadzenia audytu nie może naruszać innych obszarów działalności Przyjmującego Zamówienie (w tym w zakresie zasad współpracy z innymi podmiotami niż Przyjmującego Zamówienie), m.in. informacji poufnych, zobowiązań umownych, informacji dotyczących współpracy Przyjmującego Zamówienie z innymi podmiotami.
4. Udzielający Zamówienie będzie miał prawo do skorzystania z prawa audytu w siedzibie Przyjmującego Zamówienie lub innej lokalizacji, w której Przyjmujący Zamówienie przetwarza powierzone dane osobowe pod warunkiem wcześniejszego powiadomienia Przyjmującego Zamówienie o planowanym audycie na co najmniej 10 dni roboczych przed planowanym terminem audytu. Informację o planowanym audycie Udzielający Zamówienie przekazuje osobom wskazanym do kontaktu po stronie Przyjmującego Zamówienie o których mowa w § 3 ust. 1 lit. b).

§5

Odpowiedzialność i postanowienia końcowe

1. W ostatnim dniu obowiązywania Umowy, o której mowa w Preambule, w zależności od decyzji Udzielającego Zamówienie powierzone do przetwarzania dane będą podlegały zwrotowi lub zniszczeniu przez Przyjmującego Zamówienie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje dalsze przechowywanie danych osobowych.
2. W przypadku stwierdzenia przez Przyjmującego Zamówienie, iż wydane mu przez Udzielającego Zamówienie polecenia w trybie określonym w § 2 ust. 1 lit. a) oraz § 3 ust. 4 niniejszej umowy stanowią naruszenie przepisów RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych

osobowych, Przyjmującego Zamówienie niezwłocznie poinformuje o tym fakcie Udzielającego Zamówienie.

3. W sprawach nieuregulowanych zastosowanie mają przepisy prawa polskiego właściwe ze względu na naturę postanowień niniejszej umowy oraz RODO (od momentu rozpoczęcia stosowania).
4. Niniejsza umowa powierzenia danych osobowych zostaje zawarta na czas realizacji postanowień Umowy, o której mowa w Preambule i przestaje obowiązywać z chwilą zakończenia jej realizacji lub rozwiązania w trybie w niej określonym.
5. Niezależnie od postanowień ustępu poprzedniego Stronom przysługuje prawo do rozwiązania niniejszej umowy w każdym czasie w przypadku rażącego naruszania jej postanowień.
6. W przypadku wystąpienia sporów między Stronami sądem właściwym do ich rozpatrywania jest sąd właściwy miejscowo dla powoda.
7. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Wykaz załączników:

Załącznik nr 1 - szczegółowy opis przedmiotu i czasu trwania przetwarzania, charakteru i celu przetwarzania, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą.
Załącznik nr 2 - podwykonawcy, którym Przyjmującego Zamówienie powierzył do przetwarzania dane osobowe na podstawie usługi objętej Umową, o której mowa w Preambule.
Załącznik nr 3 - wykaz środków technicznych i organizacyjnych stosowanych przez Przyjmującego Zamówienie (Podmiot przetwarzający) umożliwiający należyte zabezpieczenie danych osobowych.

.....	.....
Udzielający Zamówienia	**Przyjmujący Zamówienie**

Załącznik nr 1 do umowy powierzenia danych osobowych z dnia .....

Charakterystyka danych osobowych powierzonych do przetwarzania

Opis przedmiotu przetwarzania:

Czas trwania przetwarzania:

Przetwarzanie danych odbywa się przez okres trwania Umowy z dnia .....

Charakter przetwarzania:

Stały, w tym z wykorzystaniem systemów informatycznych, przez okres obowiązywania Umowy z dnia .....

Cel przetwarzania:

Wykonywanie obowiązków wynikających z Umowy z dnia .....

Rodzaj danych osobowych objętych przetwarzaniem:

Kategorie osób, których dane dotyczą:

Załącznik nr 2 do umowy powierzenia danych osobowych z dnia .....

Wykaz Podwykonawców, z którymi Przyjmującego Zamówienie (Podmiot przetwarzający) zawarł stosowne umowy powierzenia przetwarzania danych uwzględniające obowiązki określone w niniejszej umowie.

PODWYKONAWCA	ADRES SIEDZIBY

Załącznik nr 3 do umowy powierzenia danych osobowych z dnia .....

Wykaz środków technicznych i organizacyjnych stosowanych przez Przyjmującego Zamówienie (Podmiot przetwarzający) umożliwiający należyte zabezpieczenie danych osobowych.

☐ został wyznaczony inspektor ochrony danych osobowych, nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych, należy podać dane kontaktowe IOD jeśli dotyczy (imię i nazwisko, numer telefonu oraz adres poczty elektronicznej):

.....

☐ do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie w przedmiotowym zakresie,

☐ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

☐ została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych, spełniająca wymagania określone dla środków organizacyjnych, o których mowa w np. 24 ust. 2 RODO. Nazwa i data sporządzenia dokumentu, w tym data ostatniej aktualizacji dokumentu/ów (jeśli dotyczy):

.....

		Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do: ✓ technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania, ✓ opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych, ✓ sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji, ✓ sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji), ✓ sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych.		
1	☐	Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.
2	☐	Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.

3	☐	Zastosowano urządzenia typu UPS, generator prądu i / lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
4	☐	Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej / komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.
5	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
6	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.
7	☐	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.
8	☐	Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
9	☐	Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
10	☐	Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
11	☐	Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
12	☐	Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
13	☐	Zastosowano procedurę oddzwonienia (*callback*) przy transmisji realizowanej za pośrednictwem modemu.
14	☐	Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
15	☐	Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity.
16	☐	Użyto system Firewall do ochrony dostępu do sieci komputerowej.
17	☐	Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
Środki ochrony w ramach narzędzi programowych i baz danych:		

W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.		
1	☐	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2	☐	Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
3	☐	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4	☐	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.
5	☐	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.
6	☐	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
7	☐	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
8	☐	Zastosowano kryptograficzne środki ochrony danych osobowych.
9	☐	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
10	☐	Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
Środki organizacyjne:		
W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do innych środków organizacyjnych zastosowanych przez administratora w celu ochrony danych, takich jak: instrukcje, szkolenia, zobowiązania.		
1	☐	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
2	☐	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
3	☐	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

4	☐	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
5	☐	Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Jeżeli zastosowane zostały dodatkowo inne środki nie wymienione w udostępnionych listach, należy je wyszczególnić poniżej:

.....

.....

.....