**Załacznik nr 3.1 do SWKO**

**Umowa powierzenia przetwarzania danych osobowych – wzór**

**KO/01/19**

zawarta w dniu …..... w Obornikach,

pomiędzy:

**Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Obornikach** z siedzibą w Obornikach, przy ulicy Szpitalnej 2, NIP: **787-18-08-424**, REGON: **000306609**, wpisanym do Rejestru Przedsiębiorców KRS pod numerem 0000014366

reprezentowanym przez: Małgorzatę Ludzkowską – Dyrektora

zwana dalej „**Administratorem**"

oraz

….....

….....

reprezentowaną przez: ……..

znaną dalej „**Podmiotem przetwarzającym**"

łącznie zwanymi „**Stronami**", a każda odrębnie „**Stroną**",

zwana dalej „**Umową**".

**§ 1**

**Przedmiot i czas przetwarzania**

1. W ramach Umowy Administrator powierza Podmiotowi przetwarzającemu (podmiotowi przetwarzającemu) zgodnie z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, czynności związane z przetwarzaniem dalej szczegółowo opisanych danych osobowych wyłącznie w celu realizacji Umowy Głównej.
2. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych wyłącznie w zakresie i celu określonym w niniejszej Umowie. Jakiekolwiek przetwarzanie danych osobowych, o których mowa w Umowie poza tym zakresem i celem będzie działaniem wbrew upoważnieniu Administratora.
3. Administrator oświadcza, że jest Administratorem danych osobowych, które powierza Podmiotowi przetwarzającemu do przetwarzania.
4. Postanowienia niniejszej Umowy powierzenia pozostają w pełni zgodne z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 „RODO").
5. Zgodną wolą Stron jest uregulowanie aktualnych warunków powierzenia przetwarzania danych osobowych. W momencie wejścia w życie niniejszej Umowy jej postanowienia zastępują wszelkie dotychczasowe ustalenia Stron, zawarte w umowie lub umowach powierzenia, sporządzonych w oparciu o art. 31 ustawy z dnia 29.08.1997 r. o ochronie danych osobowych, dotyczące powierzenia przetwarzania danych osobowych, o których mowa w niniejszej Umowie.

**§ 2**

**Charakter i cel przetwarzania danych**

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie powierzonych danych osobowych w poniżej wymienionych celach:

- Aktualizacji nowych wersji i serwisowania programu kompatybilnego z istniejącym systemem RIS/PACS.

2. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy, następujące kategorie danych osobowych:

a) Dane pracowników Administratora:
- imię (imiona) i nazwisko,
- numer PESEL
- numer NIP
– numer telefonu
- adres e-mail
- stanowisko

b) dane pacjentów
- imię (imiona), nazwisko
- numer PESEL,
- data urodzenia
- adres zamieszkania
- wyniki badań i konsultacji
- zakres udzielonych świadczeń zdrowotnych

3. Zakres danych osobowych, które może przetwarzać Podmiot przetwarzający wynika bezpośrednio z zadań i czynności określonych w umowie głównej.

4. Podmiot przetwarzający będzie wykonywał na powierzonych danych następujące operacje:

    - dostęp do danych

5. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w zakresie wskazanym w ust. 1-3 powyżej, w sposób zgodny z treścią Umowy, w celu realizacji Umowy Głównej i jedynie przez czas trwania Umowy, w dalszej części Umowy jako „**Powierzone Dane**”.

**§ 3**

**Oświadczenia stron**

1. Administrator oświadcza, że Powierzone Dane zgromadził zgodnie z obowiązującymi przepisami prawa.

2. Podmiot przetwarzający oświadcza, że dysponuje środkami technicznymi i organizacyjnymi umożliwiającymi prawidłowe przetwarzanie Powierzonych Danych, w zakresie i celu przewidzianym w niniejszej Umowie.

3. Podmiot przetwarzający zobowiązuje się stosować przy przetwarzaniu danych z wykorzystaniem mechanizmów umożliwiających zdalne zarządzanie bezpieczne połączenia VPN.

4. Podmiot przetwarzający oświadcza, że nie przekazuje Powierzonych Danych do państwa trzeciego ani do organizacji międzynarodowej i zobowiązuje się ich nie przekazywać przez cały okres trwania Umowy.

5. Podmiot przetwarzający zobowiązuje się przed rozpoczęciem przetwarzania niezwłocznie poinformować Administratora jeżeli prawo Unii lub prawo państwa członkowskiego, któremu podlega nałoży na niego taki obowiązek prawny, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

**§ 4**

**Zobowiązanie do zachowania tajemnicy**

1. Podmiot przetwarzający zgodnie z art. 28 ust. 3 lit. b RODO zobowiązuje się do zachowania Powierzonych Danych w tajemnicy.

2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy Powierzonych Danych, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody

Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania Powierzonych danych gwarantowały zabezpieczenie przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

4. Podmiot przetwarzający zobowiązuje się, iż osoby upoważnione do przetwarzania Powierzonych danych również zobowiążą się do zachowania tych danych w tajemnicy. Lista osób upoważnionych do przetwarzania Powierzonych Danych stanowi Załącznik nr 1 do Umowy. W każdym przypadku zmiany osób upoważnionych do ich przetwarzania Podmiot przetwarzający zobowiązuje się niezwłocznie przekazać Administratorowi aktualną listę osób upoważnionych.

**§ 5**

**Ocena skutków dla ochrony danych oraz konsultacje z organem nadzorczym**

1. Podmiot przetwarzający na żądanie Administratora pomaga mu w zapewnieniu przestrzegania obowiązków, które wynikają z dokonania oceny skutków dla ochrony danych.

2. Jeżeli przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych Podmiot przetwarzający pomaga Administratorowi realizować wytyczne w zakresie uprzednich konsultacji z organem nadzorczym (UODO).

**§ 6**

**Środki zabezpieczające**

1. Podmiot przetwarzający oświadcza, że podejmie środki zabezpieczające, wymagane na mocy art. 32 RODO, zgodnie z art. 28 ust. 3 lit. c RODO.

   Podmiot przetwarzający oświadcza, że uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia zastosowane środki techniczne i organizacyjne, są odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku przetwarzania Powierzonych Danych, tj.

   a) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,

   b) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są zgodnie z obowiązującymi dobrymi praktykami w zakresie ochrony infrastruktury i zasobów teleinformatycznych jak również, że zabezpieczenia te pozostają w zgodzie z wiążącymi przepisami prawa, w tym szczególności szyfruje Powierzone Dane,

   c) stosuje odpowiednie środki techniczne i organizacyjne do zapewnienia przetwarzanym w ramach jego umowy danym ochrony, w szczególności zabezpiecza dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Udokumentowanie realizacji powyższych działań może nastąpić poprzez:

   a) stosowanie zatwierdzonych kodeksów postępowania z uwzględnieniem specyfiki sektora, o których mowa w art. 40 RODO;

   b) uzyskanie certyfikacji na podstawie dopuszczonego postępowania certyfikującego zgodnego z art. 42 RODO.

**§ 7**

**Prowadzenie rejestru czynności**

1. Podmiot przetwarzający zobowiązuje się prowadzić oddzielny rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora dla powierzonych danych w formie elektronicznej, który udostępnia Administratorowi na każde jego żądanie .

2. Podmiot przetwarzający zobowiązuje się współpracować z organem nadzorczym i na jego żądanie udostępniać mu rejestr w celu monitorowania operacji przetwarzania na Powierzonych Danych.

**§ 8**

**Współdziałanie w wykonywaniu praw osób, których dane dotyczą**

1. Podmiot przetwarzający wdroży odpowiednie środki techniczne i organizacyjne, aby móc wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO, w szczególności w zakresie zagwarantowania:
    a. prawa do sprostowania danych,
    b. prawa do usunięcia danych,
    c. prawa do sprzeciwu,
    d. oraz prawa do przenoszenia danych.
2. Podmiot przetwarzający zobowiązuje się do przekazywania Administratorowi żądanych przez podmiot informacji/podejmowania określonych działań niezwłocznie, ale nie później niż w terminie 7 dni od dnia poinformowania Podmiot przetwarzający przez Administratora o wystąpieniu z takim wnioskiem przez podmiot danych, a także zobowiązuje się współpracować z Administratorem w miarę możliwości w celu jego realizacji.

**§ 9**

**Zarejestrowanie i zgłoszenie incydentu**

1. Zgodnie z art. 28 ust. 3 lit. f RODO, Podmiot przetwarzający uczestniczy w realizacji obowiązku Administratora, określonego w art. 33 RODO, w szczególności niezwłocznie, nie później niż w ciągu 24 godzin poinformuje Inspektora Ochrony Danych lub osobę odpowiedzialną za ochronę danych u Administratora o jakichkolwiek przypadkach naruszenia ochrony danych osobowych tzw. incydentach wraz z:
    a. opisem charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazaniem kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
    b. opisem możliwych konsekwencji naruszenia ochrony danych osobowych,
    c. opisem zastosowanych lub proponowanych środków w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
2. W przypadku, gdy ustalenie wszelkich danych dotyczących incydentu będzie niemożliwe w terminie wskazanym w ust. 1 powyżej, Podmiot przetwarzający będzie przekazywał informacje sukcesywnie, w miarę ich pozyskiwania.
3. Podmiot przetwarzający prowadzi bieżącą dokumentację zawierająca opis naruszeń, o których mowa w ust. 1 powyżej. Na żądanie Administratora niezwłocznie, nie później niż w ciągu 24 godzin przekaże kopię prowadzonej dokumentacji.
4. Na żądanie Administratora Podmiot przetwarzający zobowiązuje się udzielić wszelkich informacji dotyczących Przetwarzanych Danych w sytuacji, powzięcia informacji o wystąpieniu incydentu przez Administratora od osoby trzeciej niezwłocznie, nie później niż w ciągu 24 godzin.

**§ 10**

**Szkolenia**

1. Podmiot przetwarzający zobowiązuje się zapoznać osoby upoważnione do przetwarzana danych osobowych z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych.

**§ 11**

**Kontrola zabezpieczeń**

1. Administrator zastrzega sobie możliwość kontroli sposobu wypełnienia przez Podmiot przetwarzający obowiązków umownych, zgodnie z art. 28 ust. 3 lit. h RODO.

2. Administrator jest uprawniony do żądania udzielania informacji lub wyjaśnień w formie pisemnej, w postaci papierowej lub elektronicznej, dotyczących Powierzonych Danych. Podmiot przetwarzający jest zobligowany udzielić wszelkich niezbędnych informacji dotyczących realizacji postanowień Umowy niezwłocznie, nie później niż 7 dni od dnia otrzymania żądania.
3. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Administratora za przetwarzanie Powierzonych Danych Podmiot przetwarzający zobowiązany jest niezwłocznie podjąć działania w celu ich usunięcia oraz natychmiast poinformować o nich Administratora.
4. Podmiot przetwarzający niezwłocznie informuje Administratora o wszelkich czynnościach, w szczególności kontrolnych i skargowych, prowadzonych przez organ nadzorczy z zakresu Powierzonych Danych.
5. Administrator zastrzega sobie prawo do kontroli zgodności przetwarzania Powierzonych Danych z niniejszą Umową przez Podmiot przetwarzający . Administrator danych powiadomi Podmiot przetwarzający o zamiarze przeprowadzenia przedmiotowej kontroli z wyprzedzeniem, nie krótszym niż 7 dni. Podmiot przetwarzający zobowiązany jest umożliwić Administratorowi danych przeprowadzenie przedmiotowej kontroli, w szczególności poprzez udostępnienie systemów informatycznych, nośników, dokumentacji i pomieszczeń, w zakresie niezbędnym dla kontroli przetwarzania Powierzonych Danych.
6. W przypadku powzięcia przez Administratora wiadomości o rażącym naruszeniu zobowiązań wynikających z przepisów obowiązującego prawa lub Umowy a także incydencie, Podmiot przetwarzający umożliwi Administratorowi przeprowadzenie niezapowiedzianej kontroli.
7. Podmiot przetwarzający jest zobowiązany do zastosowania się do zaleceń pokontrolnych sformułowanych przez Administratora dotyczących zabezpieczenia Powierzonych Danych.

**§ 12**

**Współdziałanie przy kontroli organu nadzorczego**

1. Podmiot przetwarzający zobowiązuje się współdziałać z Administratorem w przypadku wszczęcia przez organ nadzorczy postępowania kontrolnego u Administratora, o ile w zakresie kontroli będą również Powierzone Dane.
2. Na żądanie Administratora Podmiot przetwarzający stawi się w wyznaczonym na przeprowadzenie kontroli miejscu i czasie.

**§ 13**

**Podpowierzenie przetwarzania danych**

1. Podmiot przetwarzający może powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu („Podwykonawcy”), jeśli wynika to z zakresu Umowy Głównej, po uzyskaniu uprzedniej pisemnej zgody Administratora na powierzenie Podwykonawcy dalszego powierzenia przetwarzania danych osobowych w określonym celu i zakresie, wyrażonej w formie pisemnej pod rygorem nieważności. W celu powierzenia przetwarzania danych osobowych przez Podwykonawcę, Podmiot przetwarzający zobowiązany jest zawrzeć z Podwykonawcą pisemną umowę powierzenia przetwarzania danych osobowych o treści i zakresie jak najbardziej zbliżonym do niniejszej Umowy.
2. W przypadku skorzystania z usług Podwykonawcy, Podmiot przetwarzający zobowiązany jest do zapewniania, iż Podwykonawca będzie przetwarzał dane osobowe wyłącznie w celu i zakresie opisanym w umowie zawartej przez Podwykonawcę z Podmiotem przetwarzającym, przy czym cel i zakres przetwarzania nie będzie szerszy niż wynikający z niniejszej Umowy oraz Podwykonawca zobowiązany będzie do zachowania wszelkich wymagań określonych w § 3 ust.2.
3. Podmiot przetwarzający nie może korzystać z Podwykonawców w celu realizacji Umowy Głównej lub niniejszej Umowy w sytuacji, gdy dalsze powierzenie przetwarzania danych osobowych Podwykonawcy będzie wiązało się transferem danych osobowych poza EOG.
4. Administrator będzie mieć prawo bezpośredniego przeprowadzenia kontroli, w tym inspekcji przetwarzania danych osobowych przez dalszy podmiot przetwarzający na takich samych zasadach jak przewidziane w § 13 Umowy.

5. Wszelkie umowy dalszego przetwarzania danych będą ulegały automatycznemu rozwiązaniu w razie zakończenia obowiązywania niniejszej Umowy, niezależnie od przyczyny. W przypadku uzyskania pisemnej zgody Administratora na dalsze powierzenie danych przez Podmiot przetwarzający , Podmiot przetwarzający ponosi pełną odpowiedzialność za powierzenie Podwykonawcom przetwarzania danych, będących przedmiotem Umowy, z naruszeniem obowiązujących przepisów prawa oraz za wszelkie szkody powstałe z powodu nienależytego przetwarzania danych przez tych Podwykonawców. Podmiot przetwarzający odpowiada za działania i zaniechania Podwykonawców, jak za własne działania i zaniechania.

**§ 14**

**Odpowiedzialność i prawo do odszkodowania**

1. Podmiot przetwarzający jest w pełni odpowiedzialny za udostępnienie lub wykorzystanie Powierzonych Danych niezgodnie z treścią Umowy, a w szczególności za udostępnienie Powierzonych Danych osobom nieupoważnionym.
2. 2.Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy podmiot działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.
3. Administrator oraz Podmiot przetwarzający odpowiadają w stosunku do osób zainteresowanych oraz w stosunku do siebie nawzajem w sposób opisany w art. 82 RODO.
4. W przypadku podniesienia jakichkolwiek roszczeń w rozumieniu art. 82 RODO wobec Administratora przez osobę zainteresowaną Podmiot przetwarzający zobowiązuje się do wspierania Administratora przy obronie przed tymi roszczeniami, na ile będzie to możliwe.
5. 5.W przypadku, w którym Administrator zostanie zobowiązany prawomocną decyzją lub prawomocnym wyrokiem właściwego sądu do zapłaty kary pieniężnej, odszkodowania, zadośćuczynienia lub jakiejkolwiek innej kwoty z tytułu naruszenia przepisów dotyczących ochrony danych osobowych lub w związku ze szkodą lub krzywdą wyrządzoną w związku z naruszeniem przepisów dotyczących ochrony danych osobowych, jeśli takie naruszenie lub szkoda (krzywda) wynikać będą z naruszenia przez Podmiot przetwarzający lub jego Podwykonawcę postanowień Umowy, Podmiot przetwarzający odpowiada względem Administratora w pełnej wysokości, niezależnie od jakichkolwiek ograniczeń odpowiedzialności przewidzianych w Umowie lub Umowie Głównej i zobowiązany jest zwrócić Administratorowi wszelkie koszty poniesione przez Administratora, w tym w szczególności zwrócić kwotę wypłaconego odszkodowania, zadośćuczynienia lub kary pieniężnej.

**§ 15**

**Czas obowiązywania umowy**

1. Umowa obowiązuje na czas obowiązywania Umowy Głównej.
2. Administrator może wypowiedzieć niniejszą Umowę ze skutkiem natychmiastowym w każdym czasie, w szczególności w sytuacji nieprzestrzegania przez Podmiot przetwarzający postanowień Umowy oraz obowiązujących przepisów prawa z zakresu ochrony danych osobowych.
3. Zobowiązanie do zachowania poufności nie wygasa po zakończeniu Umowy i jest nieograniczone w czasie. W przypadku gdyby powyższe zastrzeżenie okazało się nieważne lub bezskuteczne, zobowiązanie do zachowania poufności trwa przez okres 10 lat od dnia wygaśnięcia Umowy Głównej, niezależnie od przyczyny.

**§ 16**

**Zakończenie przetwarzania danych**

Po zakończeniu przetwarzania Powierzonych Danych zgodnie z niniejszą Umową, według wyboru Administratora, Podmiot przetwarzający zobowiązuje się w terminie 7 dni:

1. Zwrócić Powierzone Dane do siedziby Administratora na własny koszt, w sposób wskazany przez Administratora, albo

2. Trwale usunąć Powierzone Dane oraz niezwłocznie przedstawić dowód ich trwałego usunięcia Administratorowi,
3. Zaniechać ich przetwarzania we własnym zakresie, zgodnie z art. 28 ust. 3 lit. g RODO, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania tychże danych osobowych.

**§ 17**

**Postanowienia końcowe**

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. Prawem właściwym dla Umowy jest prawo Rzeczpospolitej Polskiej.
3. Zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Wszelkie spory wynikające z niniejszej Umowy lub powstające w związku z nią będą rozstrzygane przez Sąd Powszechny właściwy dla Administratora.

_____ _____

**/Administrator/** **/Podmiot przetwarzający /**