|  |  |
| --- | --- |
| AM\_7\_2020\_103 |  ***Załącznik nr 4****do umowy nr AM/…/2020* |

**Umowa powierzenia przetwarzania danych osobowych**

zawarta dnia: **……….. r.**

**Wojewódzkim Szpitalem im. Św. Ojca Pio w Przemyślu,** z siedzibą w **Przemyślu, ul. Monte Cassino 18, 37-700 Przemyśl (**forma prawna: Samodzielny Publiczny Zakład Opieki Zdrowotnej**),** NIP: 7952066984, REGON: 000314684 wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonym przez Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000057847,

zwanym w dalszej części umowy **„Administratora Danych”**

reprezentowanym przez p. o. Dyrektora Wojewódzkiego Szpitala im. Św. Ojca Pio w Przemyślu – **Barbarę Stawarz**

**a:**

, z siedzibą w , ul. , , wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy w Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: , NIP: , REGON: o kapitale zakładowym w wysokości zł – pokryty w ,

zwanym w dalszej części umowy ,,**Podmiotem Przetwarzającym**”.

reprezentowanym przez:

 –

przy czym każda z nich zwana jest z osobna **„Stroną”,** a łącznie zwane są **„Stronami”.**

**Strony postanowiły, co następuje:**

**P R E A M B U Ł A**

Niniejsza Umowa „Powierzenie przetwarzania danych” (dalej: „**Umowa**”) zostaje zawarta na podstawie art. 28 ust. 4 RODO w związku z zawarciem i realizacją umowy na **Naprawa aparatu RTG z ramieniem C Ziehm Vision** z dnia: **…….. r.** nr **AM/…/2020** – dotyczącej współpracy zawartej przez Strony.

**§ 1**

**DEFINICJE**

Pojęcia użyte w Umowie mają znaczenie określone poniżej, chyba że co innego wynika z kontekstu.

**1. „Administrator danych”** – podmiot, który ustala cele i sposoby przetwarzania danych.

**„Podmiot przetwarzający”** – podmiot, który przetwarza dane osobowe w imieniu Administratora danych i na jego rzecz. Podmiot przetwarzający nie decyduje o środkach i celach przetwarzania danych osobowych.

**2. „Przepisy Dotyczące Ochrony Danych” –** wszystkie przepisy obowiązujące w jakiejkolwiek właściwej jurysdykcji odnoszące się do prywatności albo do używania lub przetwarzania danych dotyczących osób fizycznych, w szczególności:

a). Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu taki danych oraz uchylenia dyrektywy 95/46/WE („**RODO**”);

b). ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000);

c). jakiekolwiek przepisy ratyfikujące, implementujące, adoptujące, uzupełniające albo zastępujące RODO;

d). jakiekolwiek przewodniki lub kodeksy praktyki przyjęte przez organy państwowe lub organy nadzoru dotyczące zgodności postępowania z wyżej wskazanymi przepisami; w każdym wypadku w zakresie obowiązującym, także w przypadku aktualizacji, nowelizacji lub zastąpienia tych przepisów.

**3. „Dane Osobowe”** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; w tym również:

**4. „Dane osobowe dotyczące zdrowia”** – Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE (1); numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

**5. „Przetwarzanie”** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, 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.

**6. „Żądanie osoby, której dane dotyczą”** – żądania osoby, której dane dotyczą, obejmujące jej prawa wynikające z Przepisów Dotyczących Ochrony Danych w zakresie danych jej dotyczących.

**7. „Prawo osoby, której dane dotyczą”** – prawo osoby, której dane dotyczą obejmujące jej prawa wynikające z Przepisów Dotyczących Ochrony Danych w zakresie danych jej dotyczących.

**8. „Organ nadzoru”** – niezależny organ publiczny ustanowiony w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwieniu swobodnego przepływu danych osobowych w Unii Europejskiej.

**9. „Naruszenie Bezpieczeństwa”** – każda utrata, nieautoryzowane lub nielegalne przetwarzanie, zniszczenie, uszkodzenie, zmianę albo nieautoryzowane ujawnienie lub udostępnienie Danych Osobowych, niezależnie czy naruszenie było przypadkowe czy zamierzone.

**10. „Ocena Skutków dla Ochrony Danych”** – proces opisujący planowane przetwarzanie, oceniający jego celowość i proporcjonalność oraz służący do określenia i zarządzania ryzykiem dla praw i wolności osób, których dane dotyczą.

**§ 2**

**ZAKRES UMOWY I PODZIAŁ OBOWIĄZKÓW**

1. Administrator danych oświadcza, że jest administratorem danych w rozumieniu RODO.
2. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 RODO zbiór Danych Osobowych do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie oraz Załączniku nr 1 do Umowy.
3. Podmiot przetwarzający zobowiązuje się do przetwarzania Danych Osobowych zgodnie z wytycznymi Administratora danych, Umową oraz Załącznikiem nr 1.
4. Podmiot przetwarzający oświadcza, iż dysponuje odpowiednimi środkami technicznymi i organizacyjnymi, w tym należytymi zabezpieczeniami zapewniającymi przetwarzanie danych osobowych zgodnie z przepisami RODO.

**§ 3**

**POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH**

1. W związku z zawarciem i realizacją Umowy Administrator danych powierza Podmiotowi przetwarzającemu przetwarzanie Danych Osobowych.
2. Administrator danych powierza Podmiotowi przetwarzającemu Dane Osobowe, w zakresie wymienionym w Załączniku nr 1 do Umowy.
3. Zakres Danych Osobowych wymienionych w ust. 1 jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy.
4. Podmiot przetwarzający przyjmuje do wiadomości, że Dane Osobowe zawierają dane wrażliwe i dołoży należytej staranności w celu ochrony i działania zgodnego z Przepisami Dotyczącymi Ochrony Danych.

**§ 4**

**INSTRUKCJE PRZETWARZANIA**

1. Podmiot przetwarzający przetwarza Dane Osobowe wyłącznie w celu wykonania Umowy lub na udokumentowane polecenie Administratora danych, za wyjątkiem przetwarzania, do którego zobowiązują Podmiot przetwarzający odrębne przepisy.
2. Podmiot przetwarzający zapewnia zachowanie w tajemnicy przetwarzanych Danych Osobowych oraz sposobów ich zabezpieczenia przez osoby, które upoważnia do przetwarzania Danych Osobowych, zarówno w trakcie zatrudnienia lub współpracy, jak i po ustaniu zatrudnienia lub współpracy.
3. Biorąc pod uwagę charakter przetwarzania, Podmiot przetwarzający w miarę możliwości pomaga poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na Żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw wskazanych w RODO.
4. Na żądanie Administratora danych, a zawsze w przypadku zakończenia trwania Umowy, Podmiot przetwarzający jest zobowiązany:
5. niezwłocznie zaprzestać przetwarzania Danych Osobowych;
6. w zależności od żądania Administratora danych, bezpiecznie zwrócić Administratorowi danych wszelkie Dane Osobowe posiadane przez Podmiot przetwarzający, zarówno w formie pisemnej, jak i elektronicznej lub innej lub bezpowrotnie usunąć wszelkie kontrolowane lub posiadane Dane Osobowe.

**§ 5**

**PRACOWNICY / WSPÓŁPRACOWNICY PODMIOTU PRZETWARZAJĄCEGO**

1. Podmiot przetwarzający może dopuścić do przetwarzania Danych Osobowych wyłącznie osoby posiadające upoważnienie do przetwarzania Danych Osobowych.
2. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania Danych Osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
3. Podmiot przetwarzający ponosi odpowiedzialność za szkody wyrządzone przez osoby przez niego zatrudnione lub świadczące na jego rzecz usługi na skutek ujawnienia informacji prawnie chronionych, naruszenia Przepisów Dotyczących Ochrony Danych oraz niewłaściwego wykonywania Umowy.

**§ 6**

**OCENA SKUTKÓW DLA OCHRONY DANYCH**

Podmiot przetwarzający zobowiązuje się do rzetelnej pomocy przy realizacji obowiązku Oceny Skutków dla Ochrony Danych, wynikającego z Przepisów Dotyczących Ochrony Danych.

**§ 7**

**PRAWO DO INFORMACJI I KONTROLI**

1. Podmiot przetwarzający zobowiązuje się przestrzegać wszelkich rozsądnych i zgodnych z prawem żądań Administratora danych (oraz jego audytorów i ich wewnętrznych lub zewnętrznych reprezentantów) dotyczących dostępu i kontroli do siedziby, systemów, procedur, ewidencji i osób uprawnionych Podmiotu przetwarzającego przetwarzających Dane Osobowe dla umożliwienia Administratora danych kontroli i weryfikacji.
2. Podmiot przetwarzający na każdy pisemny wniosek Administratora danych zobowiązany jest do udzielenia pisemnych informacji dotyczących przetwarzania powierzonych mu Danych Osobowych w terminie 3 dni od dnia otrzymania takiego wniosku, chyba że żądanie wynika z prowadzonej przez Organy nadzoru kontroli lub innego zdarzenia zagrażającego obowiązującym Przepisom Dotyczącym Ochrony Danych – w takim przypadku, żądanie weryfikacji może być dokonane z wyprzedzeniem, Administrator danych zostanie niezwłocznie poinformowany o konieczności pilnego pisemnego udzielenia wyżej wymienionych informacji.
3. Podmiot przetwarzający niezwłocznie informuje Administratora danych o wszelkich postępowaniach, dotyczących danych osobowych, decyzjach administracyjnych lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanej do Podmiotu przetwarzającego, a także o wszelkich planowanych lub trwających kontrolach i inspekcjach dotyczących przetwarzania danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Organ nadzoru.

**§ 8**

**ŚRODKI TECHNICZNE I ORGANIZACYJNE**

1. Podmiot przetwarzający zobowiązuje się do wdrożenia przed przystąpieniem do pierwszej czynności przetwarzania Danych Osobowych, technicznych i organizacyjnych środków, które zapewnią bezpieczeństwo przetwarzania danych osobowych w sposób określony w Przepisach Dotyczących Ochrony Danych. W szczególności, Podmiot przetwarzający powinien zabezpieczyć dane osobowe przed dostępem osób nieupoważnionych, ich usunięciem przez osoby nieupoważnione oraz przed ich uszkodzeniem lub zniszczeniem.
2. Podmiot przetwarzający będzie prowadził rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora danych, zawierający informacje wskazane w art. 30 RODO i na zasadach tam określonych. Procesor zobowiązuje się do udostępniania rejestru na każde żądanie Organu nadzorczego lub Administratora danych, w szczególności poprzez udostępnianie jego aktualnego odpisu w formie wskazanej przez, odpowiednio, Organ nadzorczy lub Administratora danych.
3. Podmiot przetwarzający zobowiązuje się do przestrzegania wszelkich mających zastosowanie przy wykonywaniu niniejszej Umowy wewnętrznych polityk, procedur oraz innych aktów wewnętrznych Administratora danych, w szczególności w zakresie ochrony informacji, przedstawionych mu przez Administratora danych.

**§ 9**

**NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH**

1. Podmiot przetwarzający zobowiązuje się niezwłocznie, nie później niż w terminie 36 godzin, powiadomić Administratora danych o wszelkich przypadkach uzyskania przypadkowego lub nieupoważnionego dostępu do powierzonych danych osobowych lub o innych zdarzeniach mogących mieć wpływ na Naruszenie Bezpieczeństwa.
2. Po stwierdzeniu Naruszenia Bezpieczeństwa, Podmiot przetwarzający zobowiązany jest do powiadomienia Administratora danych, poprzez wystosowanie dokumentu zawiadomienia który powinien zawierać:
3. datę, czas trwania oraz lokalizację Naruszenia Bezpieczeństwa;
4. charakter i skalę Naruszenia Bezpieczeństwa, w szczególności kategorię i przybliżoną liczbę osób, których Naruszenie Bezpieczeństwa dotyczyło, a jeżeli jest to możliwe wskazanie konkretnych osób, których Dane Osobowe zostały naruszone;
5. system informatycznych lub aplikację, w którym doszło do Naruszenia Bezpieczeństwa;
6. przewidywany czas niezbędny do likwidacji szkody spowodowanej Naruszeniem Bezpieczeństwa;
7. możliwe konsekwencje Naruszenia Bezpieczeństwa, w tym konsekwencje Osób, których dane dotyczą;
8. środki podjęte w celu minimalizacji konsekwencji Naruszenia Bezpieczeństwa oraz proponowane działania naprawcze i zapobiegawcze;
9. dane kontaktowe Inspektora Ochrony Danych Osobowych lub osoby, która może udzielić więcej informacji na temat Naruszenia Bezpieczeństwa.
10. Jeżeli Podmiot przetwarzający nie będzie w stanie jednocześnie przedstawić informacji, o których mowa w pkt 2, powinien je przekazać Administratorowi danych niezwłocznie.
11. Do czasu uzyskania instrukcji od Administratora danych Podmiot przetwarzający niezwłocznie podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków Naruszenia Bezpieczeństwa.
12. Podmiot przetwarzający jest zobowiązany do dokumentowania wszelkich Naruszeń Bezpieczeństwa dotyczących Danych Osobowych, w tym okoliczności tego naruszenia, jego skutków oraz podjętych działań zapobiegawczych i naprawczych.

**§ 10**

**USUNIĘCIE I ZWROT DANYCH OSOBOWYCH**

1. Po wygaśnięciu niniejszej Umowy, Podmiot przetwarzający jest zobowiązany – adekwatnie do żądania Administratora danych - do zwrotu Danych Osobowych, w tym wszelkich ich kopii lub do usunięcia wszystkich Danych Osobowych.
2. W przypadku podpowierzenia, Danych Osobowych innemu podmiotowi, Podmiot przetwarzający zobowiązuje się do dopilnowania, aby podmiot ten dopełnił obowiązków z ust. 1.
3. Na żądanie Administratora danych Podmiot przetwarzający zobowiązany jest dostarczyć dokument potwierdzający zastosowanie się do obowiązku zwrotu lub usunięcia Danych Osobowych.
4. Przepisów powyższych nie stosuje się w przypadku, gdy na podstawie odrębnych przepisów Podmiot przetwarzający zobowiązani są do przechowywania Danych Osobowych przez dłuższy czas.
5. W przypadku, gdy odrębne przepisy prawa zobowiązują Podmiot przetwarzający do dalszego przetwarzania Danych Osobowych, Podmiot przetwarzający zawiadamia Administratora danych o takim obowiązku wskazując odpowiednie przepisy prawa.

**§ 11**

**ODPOWIEDZIALNOŚĆ PODMIOTU PRZETWARZAJĄCEGO**

1. Podmiot przetwarzający ponosi odpowiedzialność za przetwarzanie Danych Osobowych niezgodne z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania Danych Osobowych osobom nieupoważnionym.

**§ 12**

**POUFNOŚĆ**

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.
3. Strony zobowiązują się do dołożenia należytej staranności w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych, w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

**§ 13**

**POSTANOWIENIA KOŃCOWE**

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony, nie dłużej jednak niż Umowa lub czynności z niej wynikające związane z gwarancją i rękojmią*.
2. Każdorazowo przez pojęcie „dni” rozumie się dni kalendarzowe.
3. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej.
4. Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym egzemplarzu dla Administratora danych i Podmiotu przetwarzającego.
5. Umowa zawiera 1 załącznik.
6. Sprawy sporne rozstrzygane będą przez Sąd właściwy dla siedziby Administratora danych.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Podmiot przetwarzający Administrator danych

**ZAŁĄCZNIK nr 1**

**DO UMOWY POWIERZENIA PRZETWARZANIA DANYCH**

Przedmiotem Załącznika jest szczegółowe przedstawienie: charakteru i celu przetwarzania, kategorii danych i osób, których dane dotyczą.

1. Przetwarzanie Danych Osobowych przez Podmiot przetwarzający dotyczy **następujących kategorii Osób,** których dane dotyczą:
2. **Dane pacjentów / osób badanych** zapisane w bazie danych aparatu oraz dane pracowników i kontrahentów.
3. Przetwarzanie Danych Osobowych przez Podmiot przetwarzający dotyczy **następujących Danych Osobowych:**
4. Imię i nazwisko;
5. P E S E L;
6. Data urodzenia;
7. Wiek;
8. Adres zameldowania / zamieszkania;
9. Dane dotyczące zdrowia pacjentów / osób badanych;
10. Dane osobowe i kadrowe pracowników;
11. Dane kontrahentów.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Podmiot przetwarzający Administrator danych