

# UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

do umowy NR ...../SPSSZ/2020

zawarta w dniu .....2020 r., pomiędzy:

..... z siedzibą w ul. ...., 00-000 ..... zarejestrowaną w Krajowy Rejestr Sądowy, Rejestr Przedsiębiorców prowadzony przez Sąd Rejonowy dla ....., Wydział Gospodarczy, pod nr KRS ....., Nr NIP ....., Nr Regon ....., Kapitał zakładowy .....,00 PLN, reprezentowaną przez:

1. .... – p. ...., zwanym dalej „Przetwarzającym”

a

Samodzielnym Publicznym Specjalistycznym Szpitalem Zachodnim im. św. Jana Pawła II z siedzibą w Grodzisku Mazowieckim ul. Dalekiej 11, wpisanym do rejestru sądowego Sądu Rejonowego dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000158332, NIP 529-100-47-02, Regon 000311639, zwanym dalej „Administratorem”, reprezentowanym przez:

1. Dyrektora Szpitala Zachodniego - p. Krystynę Płukis  
zwani dalej „Stroną” lub „Stronami”

## § 1

### Przedmiot Umowy

1. Strony oświadczają, że zawarły umowę (zwaną dalej Umową Główną), której realizacja wymaga powierzenia Przetwarzającemu przetwarzania danych osobowych, administrowanych przez Administratora, w tym także szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 Rozporządzenia 2016/679/WE – tj. danych dotyczących zdrowia, przy czym szczegółowe informacje o Umowie Głównej/Umowach Głównych wskazano w poniższej tabeli:

LP	Numer	Data zawarcia	Przedmiot umowy – cel i charakter przetwarzania	Kategoria osób których dane dotyczą – rodzaj powierzonych danych osobowych	Czas przetwarzania	Podpowierzenie
1	...../SPSSZ/2020	00.00.2020	[...]	[...]	24 m-cy od daty zawarcia	nie

2. Administrator potwierdza dotychczasowe powierzenie oraz nadal powierza Przetwarzającemu przetwarzanie danych osobowych uzyskanych przez Przetwarzającego w związku z realizacją w/w Umowy Głównej, w celu i zakresie wskazanym powyżej, a Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe, zgodnie z wymogami i warunkami obowiązujących w tym zakresie przepisów prawnych, w tym z treścią Ogólnego Rozporządzenia o Ochronie Danych 2016/679/WE. Strony oświadczają, że powierzone dane osobowe, będą przetwarzane tylko na terenie Europejskiego Obszaru Gospodarczego (EOG).

3. Przetwarzający 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, obowiązany jest zastosować odpowiednie środki techniczne i organizacyjne, zapewniające stopień ochrony bezpieczeństwa danych osobowych, odpowiadający stopniowi ryzyka naruszenia praw osób których dane dotyczą.

4. Przetwarzający oświadcza, iż dysponuje środkami, doświadczeniem, wiedzą i wykwalifikowanym personelem, co umożliwi mu prawidłowe wykonanie niniejszej Umowy, w tym zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia 2016/679/WE.

5. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w niniejszej umowie oraz Umowie Głównej, a przy ich przetwarzaniu zobowiązany jest stosować środki zabezpieczające, o których mowa w art. 32 Rozporządzenia 2016/679/WE, w szczególności poprzez stosowanie urządzeń zapewniających kontrolę dostępu, pseudonimizację i szyfrowanie danych.

6. W ramach udzielonego powierzenia, Przetwarzający może przetwarzać dane poprzez utrwalanie, zwielokrotnianie, przechowywanie, porządkowanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, usuwanie oraz niszczenie.

**§ 2**  
**Prawa i obowiązki Stron**

1. Przetwarzający:

- a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, przy czym za takie udokumentowane polecenia uważa się niniejszą umowę oraz Umowę Główną. W przypadku powierzenia przetwarzania danych w zakresie szerszym niż to wynika z niniejszej umowy oraz Umowy Główniej, Administrator wyda odrębne polecenie i określi zakres, cel oraz przedmiot powierzenia.
- b) zobowiązany jest udostępnić Administratorowi, na każde żądanie, informacji o środkach technicznych i organizacyjnych i dokumentacji dotyczącej tych środków, które stosuje w celu ochrony danych osobowych;
- c) zobowiązany jest stosować się do poleceń Administratora dotyczących przetwarzania powierzonych danych;
- d) zobowiązany jest zapewnić, aby przetwarzanie danych następowało przy pomocy osób, które posiadają odpowiednią wiedzę na temat ochrony danych osobowych oraz które zobowiązały się do zachowania tajemnicy, lub tajemnicę zobowiązane są zachować na podstawie odrębnych przepisów;
- e) zobowiązany jest zapewnić, aby przetwarzanie danych następowało przy pomocy osób, które posiadają pisemne upoważnienie wydane przez Przetwarzającego;
- f) zobowiązany jest prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych;
- g) zobowiązany jest prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora;
- h) zobowiązany jest prowadzić rejestr naruszeń ochrony danych;
- i) zobowiązany jest przechowywać dane osobowe zawarte na elektronicznych nośnikach informacji, w taki sposób, aby dostęp do nich miały jedynie osoby uprawnione, a do danych przetwarzanych w systemach informatycznych osoby, które przeszły pomyślnie proces uwierzytelnienia i autoryzacji;
- j) zobowiązany jest pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 Rozporządzenia 2016/679/WE;
- k) zobowiązany jest pomagać Administratorowi, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 Rozporządzenia 2016/679/WE, w szczególności Przetwarzający zobowiązuje się do poinformowania Administratora o złożonym żądaniu osoby, której dane dotyczą w ciągu 2 dni od dnia otrzymania takiego żądania;
- l) zobowiązany jest do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych Danych Osobowych przez Przetwarzającego, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych Danych Osobowych, skierowanej do Przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących Przetwarzania powierzonych Danych Osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy;
- m) zobowiązany jest niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane mu polecenie stanowi naruszenie Rozporządzenia 2016/679/WE lub innych przepisów o ochronie danych;
- n) Przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z niniejszą umową przetwarzania danych przez Przetwarzającego.
- o) w przypadku niewykonania lub nienależytego wykonania przez Przetwarzającego niniejszej Umowy, Przetwarzający zobowiązuje się do zapłaty odszkodowania Administratorowi lub osobie trzeciej, która zgłosiła takie żądanie do Administratora lub Przetwarzającego.
- p) za naruszenie przez pracowników, zleceniobiorców, współpracowników lub podwykonawców warunków Umowy Powierający odpowiada jak za działania własne.

2. Administrator:

- a) ma prawo dokonywania kontroli i audytów oraz żądania udzielenia przez Przetwarzającego wyjaśnień i informacji o środkach i wszelkich okolicznościach i warunkach przetwarzania przez niego danych osobowych;
- b) uprawniony jest do wydawania Przetwarzającemu wiążących poleceń, dotyczących środków służących zabezpieczeniu danych osobowych;
- c) ma prawo do rozwiązania niniejszej umowy ze skutkiem natychmiastowym oraz rozwiązania Umowy Główniej, jeżeli Przetwarzający nie przestrzega swoich zobowiązań wynikających z niniejszej Umowy, w tym m.in. narusza obowiązujące przepisy prawa dotyczące przetwarzania danych osobowych;

### § 3

#### Naruszenie ochrony danych osobowych

1. W przypadku zdarzenia mogącego skutkować naruszeniem ochrony danych osobowych, Przetwarzający zobowiązany jest do:
  - a) przekazania Administratorowi informacji w terminie 24 godzin od wykrycia zdarzenia, drogą telefoniczną oraz mailową na adres [iod@szpitalzachodni.pl](mailto:iod@szpitalzachodni.pl);
  - b) wyznaczenia osób odpowiedzialnych za podjęcie kroków w celu zbadania przyczyn i skutków zdarzenia i podjęcia działań naprawczych w uzgodnieniu z Administratorem;
  - c) podania wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, o których mowa w art. 34 Rozporządzenia 2016/679/WE w ciągu 24 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych;
  - d) przeprowadzenia analizy skutków naruszenia praw i wolności podmiotów danych i przekazania wyników tej analizy do Administratora, w tym oceny czy konieczne jest zgłoszenie naruszenia do organu nadzorczego, a to w terminie 36 godzin od wykrycia zdarzenia;
  - e) przygotowania w ciągu 48 godzin od wykrycia zdarzenia, informacji wymaganych w zgłoszeniu naruszenia ochrony danych do organu nadzorczego, jeżeli decyzję o dokonaniu zgłoszenia podejmie Administrator;

### § 4

#### Termin obowiązywania umowy – usunięcie danych

1. Niniejsza Umowa zostaje zawarta na czas wynikający z czasokresu przetwarzania danych osobowych przez Powierzającego, w tym niniejsza Umowa nie ulega rozwiązaniu mimo rozwiązania Umowy Głównej, jeżeli z przepisów szczególnych, w tym dotyczących przechowywania dokumentacji medycznej wynikają dłuższe okresy, w których dane osobowe nadal będą przetwarzane przez Przetwarzającego.
2. Po zakończeniu przetwarzania danych osobowych, niezależnie od dalszego obowiązywania Umowy Głównej, Przetwarzający zobowiązany jest do usunięcia lub zwrotu Administratorowi wszelkich danych osobowych (w tym również części danych) uzyskanych w związku z realizacją Umowy Głównej, których dalsze przetwarzanie, w tym archiwizowanie nie jest wymagana odrębnymi przepisami prawa.
3. Jeżeli odrębne przepisy tego wymagają, Przetwarzający zobowiązany jest do archiwizacji lub usunięcia danych osobowych zgodnie z tymi przepisami. W zakresie nieuregulowanym w odrębnych przepisach, Przetwarzający zobowiązany jest do usunięcia danych w sposób uniemożliwiający ich odtworzenie. Przed usunięciem danych Przetwarzający uzgodni z Administratorem, które z powierzonych danych podlegać będą zwrotowi, a które usunięciu.

### § 5

#### Postanowienia końcowe

1. Niniejsza umowa wchodzi w życie z dniem jej podpisania.
2. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
3. W sprawach nie uregulowanych niniejszą Umową mają zastosowanie przepisy Rozporządzenia 2016/679/WE, Kodeksu Cywilnego oraz wszelkich innych przepisów krajowych dotyczących ochrony danych osobowych
4. Spory związane z wykonywaniem niniejszej Umowy rozstrzygane będą przez sąd właściwy dla siedziby Administratora.
5. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwa dla Administratora i jeden dla Przetwarzającego.

w imieniu Administratora

w imieniu Przetwarzającego

# Oświadczenie

Działając w imieniu ..... z siedzibą w ul. ...., 00-000 ..... zarejestrowaną w Krajowy Rejestr Sądowy, Rejestr Przedsiębiorców prowadzony przez Sąd Rejonowy dla ....., Wydział Gospodarczy, pod nr KRS ....., Nr NIP ....., Nr Regon ....., Kapitał zakładowy ....., 00 PLN, reprezentowaną przez: Panią/a ..... – reprezentującego ..... na podstawie pełnomocnictwa/umowy z dnia .....2020 r., zwanym dalej „Przetwarzającym”, w związku z podjętym w dniu .....2020r. przetargiem nieograniczonym na usługę ..... dla Szpitala Zachodniego w Grodzisku Mazowieckim i procedurą wyboru kontrahenta niniejszym potwierdzam wdrożenie w ww. podmiocie odpowiednich środków technicznych, organizacyjnych i prawnych gwarantujących, by przetwarzanie spełniało wymogi 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 chroniło prawa osób, których dane dotyczą.

## Wdrożono następujące środki techniczne, organizacyjne i prawne:

zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
przyjętej u potencjalnego kontrahenta polityki bezpieczeństwa danych osobowych i instrukcji bezpieczeństwa systemów informatycznych, w szczególności w zakresie ich przejrzystości oraz zgodności z obowiązującym prawem.
regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych;

.....  
miejsce i data

.....  
imię i nazwisko oraz podpis osoby reprezentującej Kontrahenta