UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

(zwana dalej „Umową”)

zawarta pomiędzy:

**Samodzielnym Publicznym Zakładem Opieki Zdrowotnej w Węgrowie** z siedzibą w Węgorowie, ul. Kościuszki 15, 07-100 Węgrów, wpisanym do Krajowego Rejestru Sądowego prowadzonego przez ………………………………….. pod numerem …………………….. oraz Rejestru Podmiotów wykonujących Działalność Leczniczą prowadzonego pod numerem …………………………………. posiadającym REGON …………………………, NIP ………………………., zwanym dalej Użytkownikiem, reprezentowanym przez:

**…………………………………………………………..**,

zwanym w w dalszej części Umowy **„Administratorem”** lub **„Administratorem danych”,**

a

…………………………………………………………………………………………………………………………………………………………………..

zwanym w dalszej części Umowy **„Podmiotem przetwarzającym”** lub **„Przetwarzającym”,**

zwanymi dalej łącznie „**Stronami**”, o następującej, zgodnie ustalonej przez Strony, treści:

**§ 1**

**POLECENIE DOKONYWANIA**

**PRZETWARZANIA DANYCH OSOBOWYCH W IMIENIU ADMINISTRATORA**

1. W celu wykonywania umowy – „…………………………………..” (zwanej dalej „**Umową** **podstawową**”), której przedmiotem jest ……………………………………………………………………, **Administrator** powierza **Podmiotowi** **przetwarzającemu** dokonywanie, w imieniu **Administratora**, przetwarzania danych osobowych w zakresie i na zasadach określonych w **Umowie**.
2. **Podmiot** **przetwarzający** uprawniony jest do dokonywania przetwarzania **danych** **osobowych** w imieniu **Administratora** wyłącznie w celu i w sposób określonych w **Umowie**.

**§ 2**

**RODZAJ DANYCH OSOBOWYCH I KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ**

Polecenie dokonywania przetwarzania danych osobowych, będące przedmiotem **Umowy**, obejmuje dane osobowe w następujących kategoriach osób i rodzaju (zwane dalej „**danymi** **osobowymi**”):

Rodzaj danych osobowych i kategorie osób:

1. W oparciu o niniejszą Umowę przetwarzane będą:

a. Dane zwykłe identyfikacyjne i dane kontaktowe, w tym imiona i nazwisko, adres zamieszkania lub pobytu, adres e-mail, data i miejsce urodzenia, numer PESEL, numer NIP, numer telefonu kontaktowego, odział NFZ, adres IP, seria i numer dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, stanowisko służbowe, nazwa użytkownika systemu;

b. Szczególne kategorie danych, w tym informacje dotyczące stanu zdrowia, w tym jednostek chorobowych oraz wykonanych badań, informacje o przyjmowanych lekach, informacje dot. niepełnosprawności.

2. Przetwarzane kategorie osób w celu wykonania Umowy podstawowej:

a. Klienci Administratora (pacjenci, przedstawiciele ustawowi pacjentów, osoby upoważnione przez pacjentów);

b. Pracownicy Administratora (bez względu na podstawę ich zatrudnienia – umowa o pracę, umowa cywilnoprawna, kontrakt, staż) oraz użytkownicy systemu.

**§ 3**

**CZYNNOŚCI PRZETWARZANIA OBJĘTE POWIERZENIEM,**

**CHARAKTER I CELE PRZETWARZANIA DANYCH OSOBOWYCH**

1. **Administrator** powierza **Podmiotowi** **przetwarzającemu** dokonywanie przetwarzania **danych** **osobowych**
w celu wykonywania **Umowy** **podstawowej**.
2. Przetwarzanie danych przez **Podmiot przetwarzający** będzie polegało na ……………………….. na rzecz Administratora danych, na zasadach określonych w Umowie podstawowej.

**§ 4**

**OŚWIADCZENIA PODMIOTU PRZETWARZAJĄCEGO**

* 1. Przetwarzający oświadcza, że zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wszystkie 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 uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej **„Rozporządzenie”**)
	i chroniło prawa osób, których dane dotyczą.
	2. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, Przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający wiążącemu się z przetwarzaniem ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, w szczególności ryzyku naruszenia ochrony Danych Osobowych, o którym mowa w art. 4 pkt 12 oraz art. 32 Rozporządzenia.
	3. Przetwarzający oświadcza, że wszystkie systemy, w których przetwarzane są Dane Osobowe, są zgodne z Rozporządzeniem, w szczególności w zakresie bezpieczeństwa przetwarzania.
	4. Administrator jest uprawniony do wydawania wytycznych w zakresie środków bezpieczeństwa danych osobowych w każdym momencie, a Przetwarzający jest obowiązany uwzględnić je w miarę możliwości.

**§ 5**

**OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO**

* 1. Przetwarzający obowiązany jest, uwzględniając charakter przetwarzania oraz dostępne mu informacje, czynnie pomagać Administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia, w tym odpowiadać niezwłocznie na zapytania Administratora.
	2. Przetwarzający jest obowiązany, biorąc pod uwagę charakter przetwarzania, pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, inne niż te, o których mowa w ustępie poprzedzającym, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.
	3. **Podmiot** **przetwarzający** zobowiązany jest do:
1. podjęcia przed rozpoczęciem dokonywania przetwarzania **danych** **osobowych** na podstawie **Umowy**
i stosowania przez cały czas trwania przetwarzania **danych** **osobowych** środków organizacyjnych i technicznych zapewniających odpowiedni stopień bezpieczeństwa **danych** **osobowych**;
2. prowadzania wymaganej obowiązującymi przepisami o ochronie danych osobowych dokumentacji ochrony danych, w tym wszelkich polityk, rejestrów;
3. współpracowania, na każde żądanie, z jakimkolwiek organem nadzorczym uprawnionym do kontroli przestrzegania przepisów o ochronie danych w zakresie i sposób określonych przez ten organ;
4. dokumentowania wszelkich naruszeń ochrony **danych osobowych**, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działania zaradcze;
5. zapewnienia by:
* dostęp do **danych** **osobowych** miały wyłącznie osoby upoważnione do tego przez **Podmiot** **przetwarzający**;
* osoby upoważnione do przetwarzania **danych** **osobowych** zobowiązały się na piśmie do zachowania w tajemnicy tych **danych osobowych** oraz sposobów ich zabezpieczenia.
	1. Podmiot przetwarzający zobowiązany jest do wypełnienia „Ankiety bezpieczeństwa dla podmiotów przetwarzających” oraz jej przesłanie na adres e-mail: **iod@spzoz.wegrow.pl** (załącznik do niniejszej Umowy powierzenia przetwarzania danych) oraz przedłożenie jej podpisanego oryginału Administratorowi.

**§ 6**

**OBOWIĄZEK INFORMOWANIA I WSPOMAGANIA ADMINISTRATORA**

1. **Podmiot** **przetwarzający** zobowiązany jest do niezwłocznego poinformowania (nie później niż w ciągu 24 godzin od chwili zaistnienia zdarzenia) **Administratora** [*za pośrednictwem poczty elektronicznej na adres:* ***iod@spzoz.wegrow.pl****]* o:
2. jakimkolwiek postępowaniu lub orzeczeniu dotyczącym **danych** **osobowych**, w tym zwłaszcza ich prawidłowego zabezpieczenia;
3. stwierdzonym przez **Podmiot** **przetwarzający** naruszeniu ochrony danych osobowych, w tym w szczególności **danych** **osobowych** lub zagrożeniu takiego naruszenia wraz ze wskazaniem (opisem):
4. charakteru naruszenia ochrony danych osobowych, w tym kategorii i przybliżonej liczby osób, których dane dotyczą;
5. możliwych konsekwencji naruszenia ochrony danych osobowych;
6. środków zastosowanych lub proponowanych przez **Podmiot** **przetwarzający** w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków;
7. zapowiedzi albo rozpoczęciu przez organ nadzorczy kontroli lub postępowania wyjaśniającego dotyczącego **danych** **osobowych**.
8. **Podmiot** **przetwarzający** zobowiązany jest do wspomagania **Administratora**, w sposób przez niego określony, we wszelkich sprawach dotyczących **danych** **osobowych**, w szczególności poprzez:
9. udzielanie pisemnych wyjaśnień lub informacji**;**
10. udostępnianie dokumentów lub innego rodzaju zapisów**;**
11. umożliwianie:
12. wglądu lub zapisania informacji przechowywanych w systemach informatycznych;
13. dokonywania przeglądów stanu systemów informatycznych;
14. przeprowadzania testów zabezpieczeń systemów informatycznych.
15. Obowiązek, o którym mowa w ust. 2 powyżej dotyczy także wspierania **Administratora** w wywiązywaniu się z obowiązku udzielania osobie, której dane dotyczą informacji na temat przetwarzania jej danych osobowych oraz wszelkich innych obowiązków **Administratora**, wynikających z korzystania przez osobę, której dane dotyczą z przysługujących jej praw zgodnie z obowiązującymi przepisami prawa o ochronie danych osobowych.

**§ 7**

**KORZYSTANIE Z USŁUG INNEGO PODMIOTU PRZETWARZAJĄCEGO**

1. **Administrator** wyraża ogólną zgodę na korzystanie przez **Podmiot** **przetwarzający** z usług innego podmiotu przetwarzającego (zwanego dalej „**Innym** **podmiotem** **przetwarzającym**”) w celu wykonywania w imieniu **Administratora** wszystkich lub wybranych czynności przetwarzania **danych** **osobowych.**
2. **Podmiot przetwarzający** zobowiązany jest do uprzedniego poinformowania **Administratora** o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających – w takim wypadku **Administrator** uprawniony jest do wyrażenia wiążącego sprzeciwu wobec takich zmian.
3. Informacja obejmująca zamierzone zmiany, o których mowa w ust. 2 powyżej, winna zostać przekazana za pośrednictwem poczty elektronicznej na adres: **iod@spzpz.wegrow.pl** i powinna zawierać:
4. imię i nazwisko/nazwę oraz dane kontaktowe **Innego** **podmiotu** **przetwarzającego**;
5. określenie czynności przetwarzania **danych** **osobowych**, w celu wykonywania których **Podmiot** **przetwarzający** będzie korzystać z usług **Innego** **podmiotu** **przetwarzającego**;
6. W przypadku podpowierzenia przetwarzania danych osobowych, podpowierzenie będzie mieć za podstawę umowę, na podstawie której Podwykonawca zobowiąże się do wykonywania tych samych obowiązków, które na mocy niniejszej Umowy powierzenia nałożone są na Przetwarzającego. Umowa będzie podpisana w tej same formie co Umowa powierzenia.
7. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec **Innego** **podmiotu** **przetwarzającego**. Przetwarzający poinformuje Administratora w przypadku rozwiązania umowy podpowierzenia w terminie 7 dni.
8. Przetwarzający zapewni, aby **Inne** **podmioty** **przetwarzające**, którym podpowierzono przetwarzanie danych stosowały co najmniej równorzędny poziom ochrony danych osobowych co Przetwarzający.
9. **Strony** zgodnie postanawiają, że w przypadku gdy **Inny** **podmiot** **przetwarzający** nie wywiąże się ze spoczywających na nim obowiązków ochrony **Danych** **osobowych**, pełna odpowiedzialność wobec **Administratora** za wypełnienie obowiązków **Innego** **podmiotu** **przetwarzającego** spoczywa na **Podmiocie** **przetwarzającym**.

**§ 8**

**PRAWO AUDYTU**

**ORAZ OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO**

1. **Administrator** uprawniony jest do przeprowadzania audytu **Podmiotu** **przetwarzającego** w zakresie zgodności wykonywania przez niego czynności przetwarzania **Danych** **osobowych** z postanowieniami **Umowy** oraz obowiązującymi przepisami o ochronie danych, w szczególności w celu sprawdzenia wykonywania przez **Podmiot** **przetwarzający** ciążących na nim obowiązków.
2. O zamiarze przeprowadzenia audytu **Administrator** zobowiązany jest zawiadomić **Podmiot przetwarzający** z co najmniej 3 dniowym wyprzedzeniem, przy czym w przypadku uzyskania przez **Administratora** informacji o rażącym naruszeniu przez **Podmiot przetwarzający** obowiązków wynikających z **Rozporządzenia** lub **Umowy**, **Administrator** uprawniony jest do przeprowadzenia audytu bez uprzedniego zawiadomienia.
3. **Administrator** ma prawo wskazać osoby upoważnione do przeprowadzenia audytu w jego imieniu.
4. **Administrator** uprawniony jest do przekazania **Podmiotowi przetwarzającemu**, po przeprowadzonym audycie, pisemnych zaleceń i wytycznych wraz z terminem ich realizacji, nie krótszym niż 7 dni. **Podmiot przetwarzający** zobowiązany jest do wykonania sformułowanych zaleceń pokontrolnych, dotyczących w szczególności zabezpieczenia **danych** **osobowych** pod względem technicznym i organizacyjnym oraz sposobu wykonywania czynności ich przetwarzania.

**§ 9**

**CZAS TRWANIA PRZETWARZANIA**

1. **Podmiot** **przetwarzający** uprawniony jest do wykonywania czynności przetwarzania w imieniu **Administratora** przez czas obowiązywania **Umowy**.
2. **Umowa** zawarta jest na czas obowiązywania **Umowy** **podstawowej**, przy czym rozwiązanie, wypowiedzenie lub wygaśnięcie **Umowy** **podstawowej** powoduje jednoczesne odpowiednio rozwiązanie, wypowiedzenie lub wygaśnięcie **Umowy** bez konieczności składania przez **Strony** dodatkowych oświadczeń w tym zakresie, chyba że **Strony** postanowią inaczej, z zastrzeżeniem postanowień poniższych.
3. **Administrator** jest uprawniony do wypowiedzenia **Umowy** ze skutkiem natychmiastowym w przypadku:
4. dokonywania przez **Podmiot** **przetwarzający** przetwarzania **danych** **osobowych** w celu lub w sposób inny niż określony w **Umowie**;
5. korzystania przez **Podmiot** **przetwarzający**, w celu wykonywania w imieniu **Administratora** wszystkich lub wybranych czynności przetwarzania **Danych** **osobowych**, z usług **Innego** **podmiotu** **przetwarzającego** bez zgody **Administratora** lub wbrew sprzeciwowi **Administratora.**
6. **Strony** zgodnie postanawiają, że wypowiedzenie **Umowy** w przypadkach określonych w ust. 3 powyżej powoduje jednoczesne wypowiedzenie **Umowy** **podstawowej** z winy **Podmiotu przetwarzającego** bez konieczności składania dodatkowych oświadczeń, chyba że co innego wynika z oświadczenia o wypowiedzeniu **Umowy** złożonego przez **Administratora**.

**§ 10**

**POSTĘPOWANIE Z DANYM OSOBOWYMI**

**PO ZAKOŃCZENIU ICH PRZETWARZANIA**

1. W przypadku posiadania przez **Podmiot przetwarzający** danych osobowych lub ich kopii,po zakończeniu przetwarzania **danych** **osobowych**, niezależnie od sposobu lub przyczyny, **Podmiot** **przetwarzający** zobowiązany jest, na swój koszt i ryzyko, do:
2. niezwłocznego zwrócenia **danych** **osobowych** **Administratorowi** i następnie usunięcia wszelkich istniejących ich kopii;

lub

1. niezwłocznego usunięcia **danych** **osobowych**

według wyboru **Administratora**.

1. **Dane** **osobowe** lub ich kopie powinny zostać usunięte przez **Podmiot** **przetwarzający** w terminie 14 (słownie: czternastu) dni od dnia zakończenia przetwarzania na podstawie **Umowy**.
2. **Podmiot** **przetwarzający** zobowiązany jest do przekazania **Administratorowi** w terminie 7 (słownie: siedmiu) dni od dnia usunięcia **danych** **osobowych**, protokołu usunięcia **danych** **osobowych**.

**§ 11**

**PRAWO WŁAŚCIWE, JURYSDYKCJA SĄDÓW POLSKICH**

**ORAZ UMOWA PROGORACYJNA**

1. **Strony** zgodnie postanawiają, że **Umowa** podlega prawu polskiemu.
2. Spory o charakterze sprawy cywilnej mogące wyniknąć na tle realizacji **Umowy, Strony** poddają jurysdykcji sądów polskich, zaś w zakresie właściwości miejscowej właściwemu rzeczowo sądowi powszechnemu dla powoda.

**§ 12**

**POSTANOWIENIA KOŃCOWE**

1. Ilekroć w **Umowie** przewidziane jest uprawnienie lub obowiązek zawiadomienia drugiej **Strony**, zawiadomienie, aby mogło zostać uznane za skuteczne, powinno być wysłane listem poleconym.
2. Wszelkie zmiany **Umowy** wymagają zachowania formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych **Umową** w zakresie przetwarzania **danych** **osobowych** zastosowanie mają obowiązujące przepisy prawa o ochronie danych osobowych.
4. **Umowa** została sporządzona w formie elektronicznej i podpisana przez każdą ze **Stron** kwalifikowanym podpisem elektronicznym.
5. Datą zawarcia niniejszej Umowy jest data złożenia oświadczenia woli o jej zawarciu przez ostatnią ze **Stron**.

|  |  |
| --- | --- |
| **ADMINISTRATOR:** | **PODMIOT PRZETWARZAJĄCY:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(podpis)* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(podpis)* |