**Załącznik nr 1 do umowy 32/2023**

**Umowa powierzenia przetwarzania danych osobowych nr 32/2023**

**UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**

zawarta w dniu ....................... w ……………………. pomiędzy:

**Wojewódzkim Szpitalem Zespolonym im. dr. Romana Ostrzyckiego z siedzibą w Koninie, 62-504 Konin, ul. Szpitalna 45,** zarejestrowanym w Sądzie Rejonowym Poznań - Nowe Miasto i Wilda w Poznaniu, IX Wy dział Gospodarczy Krajowego Rejestru Sądowego **(KRS 0000030801, REGON 000311591,** **NIP 665-104-26-75)** zwanym w dalszej części umowy **„Zamawiającym”**, reprezentowanym przez:

........................................................................................................................................................................

........................................................................................................................................................................

Zwaną/ym dalej ***„Administratorem”***,

a

**…………………………,** z siedzibą w ………………. przy ul. ………………………., NIP: ………….., reprezentowanym przez

……….…………………………………………………………….

zwaną/ym dalej ***„Przetwarzającym”***.

***§ 1***

***Definicje***

Administrator i Przetwarzający ustalają następujące znaczenie użytych w niniejszej umowie pojęć:

1. *Umowa powierzenia* – niniejsza umowa;
2. *Umowa główna* – **32/2023**.
3. *RODO* - Rozporządzenie 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 takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119/1 z 4 maja 2016 r.);
4. *Przetwarzanie danych* – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

***§ 2***

***Powierzenie przetwarzania danych osobowych***

1. W związku z realizacją Umowy głównej Administrator, w trybie art. 28 ust. 1 i 3 RODO, powierza Przetwarzającemu przetwarzanie danych osobowych w zakresie i celu określonych w Umowie powierzenia.
2. Przetwarzający może przetwarzać dane osobowe wyłącznie w celu i zakresie przewidzianym w Umowie, co stanowi udokumentowane polecenie w rozumieniu art. 28 ust. 3 lit. a) RODO, oraz zgodnie z innymi udokumentowanymi poleceniami Administratora przekazywanymi przez Administratora droga elektroniczną na adres ………….. lub na piśmie.
3. Administrator oświadcza, że jest administratorem danych osobowych w rozumieniu art. 4 p. 7 RODO.
4. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, krajowymi przepisami dotyczącymi ochrony danych osobowych, RODO oraz innymi przepisami prawa powszechnie obowiązującego chroniącymi prawa osób, których dane dotyczą.
5. Przetwarzający oświadcza, że stosuje środki techniczne i organizacyjne, o których mowa w art. 32 RODO.

**§ 3**

***Zakres i cel przetwarzania powierzonych danych osobowych***

1. Przetwarzający w związku z realizacją Umowy głównej będzie przetwarzał następujące dane osobowe:
2. Personel Administratora: imię i nazwisko,
3. Klienci (pacjenci) Administratora: imię i nazwisko, numer księgi oddziałowej, numer sali, numer łóżka.
4. Powierzone przez Administratora dane osobowe będą przetwarzane przez Przetwarzającego w formie papierowej i elektronicznej. Przetwarzanie danych będzie obejmowało w szczególności operacje takie jak ich: 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.
5. Dane osobowe określone w ust. 1 przetwarzane będą wyłącznie w celu realizacji Umowy głównej.
6. Strony oświadczają, iż współpraca, o której mowa ust. 3 niniejszego paragrafu, odbywa się na terenie Rzeczypospolitej Polskiej – państwie członkowskim Unii Europejskiej. Jakakolwiek relokacja usług w całości lub w części w ramach ww. współpracy powodująca konieczność przekazania przez Przetwarzającego danych osobowych określonych niniejszą umową do państw trzecich lub organizacji międzynarodowej wymaga uprzedniej pisemnej zgody Administratora danych oraz spełnienia konkretnych wymogów określonych w art. 44 i następnych RODO.

***§ 4***

***Sposób wykonania Umowy***

1. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych
2. Przetwarzający zobowiązuje się do zabezpieczenia danych osobowych, o których mowa w §3 ust 1. Umowy powierzenia, poprzez stosowanie odpowiednich środków, o których mowa w art. 32 RODO, w tym w szczególności :
3. uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zobowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualniać te środki w porozumieniu z Administratorem;
4. zobowiązany jest zapewnić by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Administratora w celach i zakresie przewidzianym w Umowie powierzenia;
5. zobowiązany jest prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO, chyba ze Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.

***§ 5***

***Obowiązki Przetwarzającego***

1. Przetwarzający zobowiązuje się do ograniczania dostępu do powierzonych danych osobowych wyłącznie do pracowników i osób z nim współpracujących na podstawie umów cywilnoprawnych, którym udzielił upoważnień do przetwarzania danych osobowych.
2. Przetwarzający oświadcza, że zgodnie z art. 28 ust. 3 p. b) RODO zobowiązał osoby upoważnione przez niego do przetwarzania danych osobowych do zachowania w tajemnicy danych osobowych, do których mają lub będą miały dostęp, zarówno w trakcie zatrudniania ich, jak i po jego ustaniu.
3. Przetwarzający, w przypadku wygaśnięcia Umowy głównej oraz rozwiązania Umowy powierzenia, niezwłocznie, ale nie później niż w terminie 7 dni kalendarzowych, według wskazania Administratora zwraca lub usuwa wszelkie dane osobowe, których przetwarzanie zostało mu powierzone oraz usuwa wszelkie ich istniejące kopie, chyba ze prawo Unii Europejskiej lub prawo państwa członkowskiego nakazuje przechowywanie danych osobowych.
4. Mając na uwadze charakter przetwarzania Przetwarzający, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 15-22 RODO.
5. Mając na uwadze charakter przetwarzania oraz dostępne Przetwarzającemu informacje, będzie on pomagał Administratorowi w wywiązaniu się z obowiązków określonych w art. 32-36 RODO.
6. W razie wątpliwości przyjmuje się, że każdorazowe przekazanie Przetwarzającemu danych osobowych w celu wykonania Umowy głównej, stanowi polecenie Administratora do przetwarzania danych zgodnie z Umową powierzenia.
7. W przypadku stwierdzenia naruszenia ochrony danych osobowych, Przetwarzający zobowiązuje się do:
8. przekazania Administratorowi, w formie pisemnej lub elektronicznej, informacji dotyczących stwierdzonego naruszenia, w tym w szczególności informacji, o których mowa w art. 33 ust 3 RODO, w ciągu 24 godzin od stwierdzenia naruszenia;
9. przekazania na żądanie Administratora wszelkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 2 RODO, w ciągu 36 godzin od stwierdzenia naruszenia.
10. Przetwarzający zobowiązuje się stosować się do wskazówek lub zaleceń wydawanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, w szczególności w zakresie stosowania RODO.
11. Przetwarzający niezwłocznie poinformuje Administratora o:
12. wszelkich postępowaniach prowadzonych wobec niego przez organ nadzorczy bądź inny uprawniony organ państwowy, obejmujących dane powierzone przez Administratora;
13. wszelkich kontrolach lub inspekcjach dotyczących przetwarzania powierzonych danych osobowych, w szczególności prowadzonych przez organ nadzorczy;

***§ 6***

***Podpowierzenie***

1. Przetwarzający może powierzyć dalszym podmiotom przetwarzania przekazanych danych wyłącznie w celu wykonania Umowy głównej.
2. O zamiarze podpowierzenia danych osobowych Przetwarzający informuje Administratora wskazując tożsamość (nazwę) podmiotu, któremu ma zamiar podpowierzyć dane oraz zakres danych, charakter, cel i czas trwania podpowierzenia. Jeżeli Administrator w terminie 7 dni od daty zawiadomienia nie wyrazi sprzeciwu, Przetwarzający może podpowierzyć dane.
3. Przetwarzający może podpowierzyć przetwarzanie danych na podstawie pisemnej umowy zawartej z podmiotem mającym przetwarzać podpowierzone dane. Umowa ta powinna określać przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz obowiązki i prawa Administratora.
4. Przetwarzający zobowiąże podmiot mający przetwarzać podpowierzone dane do przestrzegania przepisów prawa dotyczących ochrony danych osobowych w takim samym zakresie jak stanowi Umowa powierzenia. Przetwarzający zagwarantuje Administratorowi w umowie z podmiotem mającym przetwarzać podpowierzone dane możliwość wykonywania prawa kontroli przetwarzania danych u tego podmiotu co najmniej w takim samym zakresie, jaki wynika z Umowy wobec Przetwarzającego.
5. Brak sprzeciwu wobec powierzenia przetwarzania danych przez Przetwarzającego nie oznacza zgody na jeszcze dalsze powierzenie przetwarzania tych danych.
6. Administrator może w każdej chwili sprzeciwić się dalszemu podpowierzaniu w stosunku do jakiegokolwiek podmiotu.
7. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków ochrony danych przez podprzetwarzającego.
8. Przekazanie powierzonych danych do państwa trzeciego może nastąpić wyłącznie na pisemne polecenie Administratora, chyba że Przetwarzający jest zobowiązany do takiego przekazania na mocy prawa Unii Europejskiej lub państwa członkowskiego, któremu podlega Przetwarzający. W takim wypadku przed rozpoczęciem przetwarzania Przetwarzający informuje Administratora o istnieniu tego obowiązku prawnego, o ile prawo nie zabrania udzielenia takiej informacji ze względu na ważny interes publiczny.
9. Przekazanie danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru Gospodarczego może się odbywać wyłącznie na warunkach określonych w art. 44-50 RODO.

***§ 7***

***Prawo kontroli***

1. Administrator, zgodnie z art. 28 ust. 3 p. h) RODO, jest uprawniony do kontroli przetwarzania powierzonych danych w miejscu prowadzenia działalności i w godzinach pracy Przetwarzającego.
2. Administrator poinformuje Przetwarzającego o planowanej kontroli drogą elektroniczną lub faksem, z przynajmniej 7-dniowym wyprzedzeniem.
3. Przetwarzający zobowiązuje się do usunięcia stwierdzonych w drodze kontroli uchybień w terminie 14 dni od ich przedstawienia Przetwarzającemu przez Administratora.
4. Przetwarzający zobowiązuje się do udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków, o których mowa w art. 28 RODO oraz w Umowie powierzenia oraz umożliwia Administratorowi przeprowadzenie audytów, w tym inspekcji.
5. Przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wskazane mu zalecenia stanowią naruszenie RODO lub innych przepisów o ochronie danych.

***§ 8***

***Odpowiedzialność Przetwarzającego***

1. Przetwarzający ponosi odpowiedzialność w zakresie przewidzianym w obowiązujących przepisach o ochronie danych osobowych, w szczególności RODO. Przetwarzający jest odpowiedzialny za ewentualne udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową powierzenia, RODO lub przepisami krajowymi, a w szczególności za udostępnienie ich osobom nieupoważnionym.
2. W przypadku naruszenia obowiązujących przepisów prawa, w szczególności RODO lub niniejszej Umowy z przyczyn leżących po stronie Przetwarzającego, w następstwie czego Administrator, jako administrator danych osobowych, zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Przetwarzający zobowiązuje się pokryć poniesione przez Administratora z tego tytułu straty.

***§ 9***

***Czas obowiązywania Umowy***

1. Niniejsza Umowa powierzenia zostaje zawarta na czas obowiązywania Umowy głównej.
2. Powierzenie przetwarzania danych osobowych obowiązuje przez cały czas trwania Umowy powierzenia, a także po ustaniu jej obowiązywania – przez okres wymagany przepisami prawa, jeżeli obowiązujące przepisy nakładają taki obowiązek na Przetwarzającego.

***§ 10***

***Warunki wypowiedzenia i rozwiązania Umowy***

1. Administrator ma prawo wypowiedzieć niniejszą Umowę ze skutkiem natychmiastowym w przypadku gdy Przetwarzający:
2. przetwarza dane osobowe w sposób niezgodny z Umową lub RODO, w szczególności wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
3. powierzył przetwarzanie danych osobowych nieupoważnionym podmiotom pomimo sprzeciwu Administratora,
4. nie zaprzestał niewłaściwego przetwarzania danych osobowych w terminie wyznaczonym przez Administratora,
5. w inny rażący sposób nie wywiązuje się z obowiązków wynikających z niniejszej Umowy.

***§ 11***

***Poufność***

1. Przetwarzający zachowa w tajemnicy wszelkie informacje, dane, materiały, dokumenty i dane osobowe otrzymane od Administratora i od współpracujących z nim osób oraz dane uzyskane w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych 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.

 ***§ 12***

***Postanowienia końcowe***

1. Wszelkie zmiany i uzupełnienia niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
2. W przypadku, gdy którekolwiek z postanowień niniejszej Umowy, kilka jej postanowień lub część tych postanowień są lub okażą się bezskuteczne lub nieważne, pozostałe postanowienia niniejszej umowy zachowują swoją pełną moc.
3. Zawiadomienia i oświadczenia dokonywane w formie pisemnej będą doręczane listem poleconym lub za pośrednictwem kuriera na adresy Stron wskazane w komparycji Umowy, chyba że Strona doręczy drugiej Stronie zawiadomienia o zmianie adresu. Strony zobowiązują się wzajemnie do zawiadamiania drugiej strony o każdorazowej zmianie adresu wskazanego w Umowie. Doręczenie pod adres wskazany przez Stronę, w przypadku odesłania zwrotnego przez pocztę lub innego operatora przesyłki wysłanej na podany adres uważa się za skuteczne z upływem trzeciego dnia, licząc od dnia następującego po dniu wysłania, jeżeli przesyłka nie została podjęta przez adresata, bez względu na przyczynę niepodjęcia.
4. Spory wynikłe z tytułu niniejszej Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
6. Załączniki stanowią integralną część umowy.

............................................. .................................................... ***Administrator Przetwarzający***

**Załączniki:**

* + - 1. Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający

**Załącznik nr 1 do umowy PPDO**

**Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający**

|  |  |
| --- | --- |
| **PYTANIE** | **ODPOWIEDŹ** |
| Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |   |
| Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |   |
| Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |   |
| Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? |   |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy? |   |
| Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia? |   |
| Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |   |
| Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |
| Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |

|  |  |
| --- | --- |
| Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji? |   |
| Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany? |   |
| Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych? |   |
| Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby? |   |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób? |   |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników? |   |
| Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka? |   |
| Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladachbez możliwości dostępu do nich osób nieupoważnionych? |  |
| Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach? |  |
| Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane? |  |
| Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych? |  |
| Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu? |  |
| Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych? |  |
| Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe? |  |
| Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |

|  |  |
| --- | --- |
| Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych? |   |
| Gdzie są przechowywane kopie zapasowe? |   |
| Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania? |   |
| Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design? |   |
| Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default? |   |
| Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych? |   |
| Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? |   |