Załącznik nr 4A

Nr sprawy: ZP/2/2023

Umowa powierzenia przetwarzania danych osobowych
(zwana dalej „Umową"), zawarta pomiędzy:

Szpitalem Miejskim Specjalistycznym im. Gabriela Narutowicza w Krakowie,
31-202 Kraków ul. Prądnicka 35-37, wpisanym do Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla Krakowa- Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000024083, NIP: 945-19-32-621,reprezentowanym przez:

dr n. med. Renata Godyń-Swędzioł - Dyrektora
zwanym dalej „Administratorem",
a
……, reprezentowaną/-ym przez:
…..- …
zwaną/-ym dalej „Przetwarzającym"
zwanymi dalej łącznie „Stronami",
o następującej treści:

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator powierza Przetwarzającemu, w trybie art. 28 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) zwanego dalej RODO, przetwarzanie danych osobowych, na zasadach i w celu określonym w niniejszej Umowie.
2. Niniejsza Umowa o powierzenie przetwarzania danych osobowych (dalej: „Umowa Powierzenia") została zawarta w związku z umową nr ZP/2/2023 **na dostosowanie, modernizację lub dostawę oprogramowania HIS w ramach projektu Małopolski System Informacji Medycznej** – zgodnie z zapisami cytowanej wyżej umowy, (dalej jako: **„Umowa Główna**").
3. Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Przetwarzający oświadcza, że zapewnia stosowanie odpowiednich środków technicznych i organizacyjnych gwarantujących odpowiedni stopnień bezpieczeństwa przetwarzania danych osobowych, odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, zgodnie z art. 32, w związku z art. 28 ust. 3 lit. c RODO, w szczególności Przetwarzający gwarantuje przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo powierzonych danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

§ 2
Zakres i cel przetwarzania danych

1. Administrator powierza Przetwarzającemu do przetwarzania dane osobowe w systemie teleinformatycznym HIS, do których Przetwarzający będzie uzyskiwać dostęp w związku z dostosowaniem, modernizacją lub wdrożeniem oprogramowania HIS, w tym asysty technicznej i usługi serwisowej – w celu realizacji postanowień Umowy Głównej (dalej jako: „dane osobowe") w zakresie określonym niniejszą Umową powierzenia, tj. w szczególności:
   1) dane będące kategorią danych zwykłych:
      a) oznaczenie pacjenta zgodnie z art. 25 pkt. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, pozwalające na ustalenie jego tożsamości: nazwisko i imię (imiona); numer PESEL; datę urodzenia i płeć w przypadku gdy numer PESEL nie został nadany; określenie rodzaju dokumentu potwierdzającego tożsamość obejmującego jego nazwę oraz nazwę kraju,
      w którym został wystawiony; adres miejsca zamieszkania - wpisywany w pierwszej wytworzonej dla tego pacjenta dokumentacji wewnętrznej, adres poczty elektronicznej lub elektronicznej skrzynki podawczej pacjenta, na który ma być przekazana dokumentacja medyczna – w przypadkach udostępniania dokumentacji w sposób, o którym mowa w art. 27 ust. 1 pkt 4 i ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, numer telefonu oraz inne dane osobowe, które mogą być wprowadzane do systemu HIS;
      b) oznaczenie osoby udzielającej świadczeń zdrowotnych oraz kierującej na badanie lub leczenie, zgodnie z § 10 pkt. 3. Rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania: imię (imiona) i nazwisko, tytuł zawodowy, numer prawa wykonywania zawodu, uzyskane specjalizacje, unikalny identyfikator upoważnienia nadany przez Rejestr Asystentów Medycznych, o którym mowa w art. 31b ust. 7 pkt 7 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia – w przypadku osoby upoważnionej, o której mowa w art. 31b ust. 1 tej ustawy oraz inne dane osobowe, które mogą być wprowadzane do systemu HIS;
      c) dane przedstawiciela ustawowego pacjenta oraz dane osób upoważnionych przez pacjenta do uzyskiwania: dokumentacji medycznej, informacji o stanie zdrowia pacjenta, dokumentacji medycznej po śmierci pacjenta - zgodnie z ustawą z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta i rozporządzeniem Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.
      d) dane pracowników Szpitala, osób zatrudnionych na podstawie umów cywilnoprawnych i innych osób upoważnionych do utrzymania Systemu, w którym przetwarzana jest dokumentacja medyczna i zapewnienia bezpieczeństwa tego Systemu: imię i nazwisko, pełniona funkcja lub stanowisko, służbowy adres poczty elektronicznej i służbowy numer telefonu.
   2) Szczególne kategorie danych: informacje dotyczące stanu zdrowia lub stanu funkcjonowania oraz procesu diagnostycznego, leczniczego, pielęgnacyjnego lub rehabilitacji, w tym jednostkowe dane medyczne usługobiorców przetwarzane w systemie informacji, o którym mowa w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, przekazywane lub udostępniane nieodpłatnie przez usługodawców.
2. Na powierzonych do przetwarzania danych będą wykonywane następujące operacje lub zestaw operacji: utrwalanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, dopasowywanie lub łączenie, ograniczanie.
3. Powyższe dane będą przetwarzane na dużą skalę a operacje przetwarzania będą wykonywane systematycznie.

4. Przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją umowy zawartej z Administratorem i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.

§ 3

Obowiązki podmiotu przetwarzającego

1. Przetwarzanie danych osobowych przez Przetwarzającego będzie odbywać się wyłącznie na udokumentowane polecenie Administratora. Za udokumentowane polecenie uznaje się zadania zlecone do wykonywania Przetwarzającemu Umową Główną oraz zadania zlecone przez Administratora w formie pisemnej, w tym elektronicznej (np. zlecenie usunięcia danych).
2. Przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
3. Przetwarzający zobowiązuje się:
   1) dołożyć szczególnej staranności przy przetwarzaniu powierzonych danych osobowych,
   2) nadać upoważnienia do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy,
   3) zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 lit. b Rozporządzenia) przetwarzanych danych, także przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich u Przetwarzającego, jak i po jego ustaniu. Obowiązek zachowania w tajemnicy obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych. W przypadku pacjenta – obowiązek zachowania danych osobowych w tajemnicy rozciąga się także po śmierci pacjenta (art. 24 ust. 3 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta),
   4) zapewnić, aby realizacja umowy powierzenia nie powodowała zakłócenia zadań realizowanych przez Administratora, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych przetwarzanych w systemie teleinformatycznym HIS.
   5) nie później niż z datą podpisania Umowy Głównej dostarczyć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi dla: urządzeń i Systemu informatycznego dostarczonych/obsługiwanych przez Zleceniobiorcę wraz z przepływami danych w Systemie, przy czym dopuszcza się przekazanie powyższego dokumentu w formie elektronicznej na adres poczty elektronicznej Inspektora Ochrony Danych (np. w formacie pdf). Zleceniobiorca zobligowany jest aktualizować ww. opis, adekwatnie do wprowadzanych zmian, przy czym dopuszcza się jego przekazywanie nie rzadziej niż raz na kwartał, do 5-go dnia miesiąca po zakończonym kwartale.
4. Przetwarzający dla zapewnienia, iż spełnia wymagania RODO w zakresie gwarancji zabezpieczenia zobowiązany jest:
   1) przed rozpoczęciem świadczenia usługi uzyskać akceptację Administratora w zakresie spełniania wymagań dotyczących zabezpieczenia przetwarzanych danych w zakresie prawidłowości implementacji tych wymagań w dokumentacji bezpieczeństwa. Akceptacja, o której mowa wyżej nastąpi w oparciu o wypełnioną przez Przetwarzającego „Ankietę dla Podmiotu Przetwarzającego" zgodnie z wzorem stanowiącym załącznik nr 2 do niniejszej Umowy, przy czym:
      a) Ankietę Przetwarzający jest zobowiązany wypełnić i przekazać Administratorowi przed podpisaniem Umowy,
      b) fakt podpisania Umowy przez Administratora jest równoznaczny z akceptacją metod zabezpieczenia przetwarzania danych przez Przetwarzającego, tj. uznanie Przetwarzającego

jako tego, który zagwarantował odpowiednie środki techniczne i organizacyjne zapewniające zgodność z RODO procesu przetwarzania danych osobowych powierzonych Umową Główną.

2) w przypadku przetwarzania powierzonych niniejszą umową i Umową Główną danych osobowych poza obszarem UE, dostarczyć poświadczoną kopię dokumentów, które stanowią przesłankę legalności tego działania (np. dokument zawartych standardowych klauzul umownych z podmiotem przetwarzającym działającym na rzecz Przetwarzającego),
3) przynajmniej raz w roku dostarczyć raport z audytu zabezpieczenia środowiska informacyjnego, w którym przetwarzane są powierzone niniejszą umową oraz Umową Główną dane osobowe, przy czym za raport, o którym mowa wyżej Administrator uznaje:
   a) raport z audytu przeprowadzony przez Inspektora Ochrony Danych (wyznaczonego przez Przetwarzającego) lub podmiot zewnętrzny, któremu Przetwarzający zlecił przeprowadzenie przedmiotowego audytu,
   b) raport z audytu certyfikującego, audytu nadzoru, audytu wewnętrznego w zakresie normy PN-EN ISO/IEC 27001 (Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania).

Koszty audytów o których mowa wyżej ponosi Przetwarzający.

5. W miarę możliwości Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
6. Zaleca się by Przetwarzający, przed przystąpieniem do wykonywania kluczowych zmian struktury lub zmian na znacznych ilościach danych objętych umową, powiadomił Administratora o konieczności wykonania kopii bezpieczeństwa danych zgromadzonych na nośnikach informacji stanowiących części składowe lub przynależności obsługiwanego systemu teleinformatycznego. Przetwarzający nie odpowiada za utratę ww. danych podczas wykonywania świadczeń objętych umową, w tym za koszty odtworzenia utraconych danych, z zastrzeżeniem, że powyższe nie dotyczy sytuacji, w której utrata danych nastąpiła z winy Przetwarzającego.
7. Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi (dostępnymi środkami technicznymi umożliwiającymi komunikowanie się na odległość), jednak nie później niż w ciągu 12 godzin od pierwszego spostrzeżenia, w tym dokonuje powiadomienia w formie i zakresie określonych w ust. 8 poniżej.
8. Powiadomienie o naruszeniu ochrony danych osobowych powinno być dokonane drogą elektroniczną na adresy poczty elektronicznej: **iod@narutowicz.krakow.pl** oraz: **inf@narutowicz.krakow.pl** i w szczególności opisywać:
   1) charakter naruszenia, w tym miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) opis możliwych konsekwencji naruszenia,
   3) opis środków zastosowanych lub proponowanych przez Przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym opis działań podjętych w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
9. W celu wykonania obowiązków wynikających z niniejszej Umowy Przetwarzający może przetwarzać także dane znajdujące się w dostarczonych z tytułu Umowy Głównej dokumentach, urządzeniach, oraz w systemach informatycznych m.in. w trybie zdalnej obsługi serwisowej, oraz działań serwisowych w siedzibie Administratora, Przetwarzającego lub Podwykonawcy w zakresie ograniczonym do wypełnienia obowiązków Umowy Głównej.
10. W przypadku dostępu zdalnego do systemu teleinformatycznego, dostęp ten będzie się odbywał w warunkach bezpiecznych, t. j.:

1) transmisja danych będzie zabezpieczona kryptograficznie;
2) dostęp będzie realizowany przy użyciu metod uwierzytelniania;
3) zapewnione zostaną mechanizmy nadzoru realizowanych działań (logowanie czynności i zdarzeń, w tym np. daty i czasu oraz loginu użytkownika serwisującego system wraz z zakresem przeprowadzonych czynności/zmian danych).

11. Przetwarzający zapewnia:
    1) zdolność ciągłego utrzymania poufności, integralności, rozliczalności i dostępności danych osobowych;
    2) zdolność do szybkiego przywrócenia dostępności danych osobowych; w razie incydentu fizycznego lub technicznego.
12. Administrator w celu zapewnienia prawidłowej realizacji Umowy Głównej zapewni Przetwarzającemu dostęp do pomieszczeń, w których zlokalizowane są urządzenia stanowiące części składowe systemu teleinformatycznego HIS, w tym do nośników danych i znajdujących się na nich informacji.
13. Po wygaśnięciu lub wypowiedzeniu Umowy Powierzenia, Przetwarzający adekwatnie do polecenia Administratora usunie powierzone dane osobowe lub niezwłocznie zwróci Szpitalowi wszelkie materiały lub nośniki z danymi, które pozostają w dyspozycji jego i podwykonawców przy czym dane przekazywane w postaci elektronicznej muszą być w powszechnie przyjętym formacie, np. XML. Przetwarzający podejmie stosowne działania, mające na celu wyeliminowanie możliwości dalszego przetwarzania danych, i usunie dane w sposób uniemożliwiający ich odtworzenie z wszelkich posiadanych przez siebie i podwykonawców nośników informacji (w tym również z kopii zapasowych), z zastrzeżeniem ust. 14 niniejszego paragrafu
14. W przypadku, gdy prawo Unii lub prawo państwa członkowskiego nakazują Przetwarzającemu lub jego podwykonawcy przechowywanie danych przez okres wskazany w tych przepisach, Przetwarzający lub jego podwykonawca mają prawo przechowywać dane wyłącznie w zakresie koniecznym do wykonania tego obowiązku prawnego.
15. Przetwarzający zobowiązuje się do niezwłocznego skutecznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzający, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przetwarzającego tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
16. Zapisy w zakresie opisanego w ust. 15 powyżej obowiązku Przetwarzającego winny być zawarte także w umowie powierzenia pomiędzy Przetwarzającym a Jego podwykonawcą.

§ 4
Prawo kontroli

1. Administrator zgodnie z art. 28 ust. 3 lit. h RODO ma prawo kontroli w celu weryfikacji, czy środki zastosowane przez Przetwarzającego przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy Powierzenia.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Przetwarzającego i po Jego uprzednim zawiadomieniu o zamiarze przeprowadzenia czynności kontrolnych w terminie, co najmniej 3 dni kalendarzowych od daty zawiadomienia.
3. Przetwarzający zobowiązuje się do udostępnienia Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO.
4. Przetwarzający zobowiązany jest umożliwić pracownikom Administratora lub podmiotom kontrolującym
   w imieniu Administratora, sprawdzenie pomieszczenia oraz urządzeń, w których przetwarzane są dane

osobowe, jak również udzielić niezbędnych wyjaśnień.

5. Przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni, o ile zalecenia te są zgodne z niniejszą umową i obowiązującymi przepisami prawa.
6. W przypadku, gdy Przetwarzający skorzysta z prawa do dalszego powierzenia przetwarzania danych osobowych innym podmiotom, podwykonawca umożliwi Przetwarzającemu i bezpośrednio Administratorowi przeprowadzenia czynności kontrolnych w celu dokonania oceny spełnienia przez podwykonawcę opisanych w niniejszej umowie obowiązków w zakresie przetwarzania i ochrony powierzonych danych osobowych na zasadach analogicznych do opisanych wyżej. Zapisy w zakresie opisanego wyżej uprawnienia Administratora winny być zawarte w umowie powierzenia pomiędzy Przetwarzającym a Jego podwykonawcą.

§ 5

Wsparcie podczas kontroli Urzędu Ochrony Danych Osobowych

1. W ramach wynagrodzenia należnego z tytułu wykonywanej Usługi Przetwarzający zobowiązuje się do wspierania Administratora podczas kontroli Urzędu Ochrony Danych Osobowych. Przetwarzający dostarczy osobie wskazanej przez Administratora pisemnych wyjaśnień, dokumentów, zapisów dotyczących przetwarzania powierzonych danych osobowych – niezwłocznie, ale nie później niż w terminie 2 dni roboczych od skierowania przez Administratora zapytania w formie papierowej lub elektronicznej na adres poczty elektronicznej: iod@narutowicz.krakow.pl oraz: sekretariat@narutowicz.krakow.pl
2. Przetwarzający zobowiązuje się do zapewnienia właściwej współpracy podczas kontroli Administratora poprzez:
    1) udostępnienie dokumentów i zapisów;
    2) umożliwienie wglądu w informacje przechowywane na nośnikach danych i w systemach informatycznych;
    3) umożliwienie osobie wskazanej przez Administratora dokonywania przeglądów stanu systemów służących przetwarzaniu oraz ich zabezpieczeń;
    4) umożliwienie przeprowadzenia testów stosowanych przez Administratora zabezpieczeń;
    5) udzielenie ustnych i pisemnych wyjaśnień.

§ 6

Dalsze powierzenie danych do przetwarzania, odpowiedzialność Przetwarzającego

1. Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych osobowych przez Przetwarzającego dalszym Podprzetwarzającym wyłącznie w zakresie i celu określonym w § 2 niniejszej umowy, z zastrzeżeniem postanowień ust. 2 poniżej.
2. W przypadku, gdy Przetwarzający skorzysta z prawa do dalszego powierzenia przetwarzania danych osobowych innym podmiotom (Podprzetwarzającym), Przetwarzający zobowiązany jest do niezwłocznego przekazania Administratorowi wykazu takich podmiotów – zgodnie z załącznikiem nr 1 do niniejszej umowy.
3. Przetwarzający w okresie obowiązywania Umowy Głównej zobowiązany jest poinformować pisemnie Administratora o wszelkich zamierzonych działaniach dotyczących dodania, zmianach lub zastąpienia innych podmiotów przetwarzających z wyprzedzeniem, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec tych działań. Administrator może wyrazić sprzeciw w formie pisemnej w terminie 5 dni roboczych od powzięcia powyższej informacji od Przetwarzającego.
4. W przypadku, gdy Przetwarzający skorzysta z prawa do dalszego powierzenia przetwarzania danych osobowych innym podmiotom (podwykonawcom), Przetwarzający jest zobowiązany do niezwłocznego przekazania Administratorowi pisemnej informacji zawierającej nazwę podmiotu (podwykonawcy), jego dane rejestrowe oraz na jaki okres i w jakim zakresie nastąpiło dalsze

powierzenie przetwarzania danych osobowych oraz jakimi środkami zachodzić będzie podpowierzenia danych.

5. Przekazanie powierzonych danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Przetwarzającego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W przypadku posiadania takiego obowiązku prawnego przez Przetwarzającego, Przetwarzający powiadamia o tym Administratora przed rozpoczęciem przetwarzania o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
6. Powierzenie przetwarzania Danych osobowych innemu podmiotowi nastąpi na podstawie umowy zawartej pomiędzy Przetwarzającym i innym podmiotem, której postanowienia zapewnią ochronę danych osobowych w sposób nie mniejszy niż jest to przewidziane w niniejszej Umowie. Przetwarzający ponosi odpowiedzialność za działania lub zaniechania podmiotów, którym dalej powierzył przetwarzanie Danych osobowych jak za działania własne.
7. Zawarta umowa musi zawierać wszystkie zobowiązania określone w niniejszej umowie oraz precyzować: czas, charakter i cel przetwarzania danych z uwzględnieniem zakresu (lub kategorii) przetwarzanych danych.
8. Administrator ma prawo do nie wyrażenia zgody na dalsze powierzenie wskazanemu przez Przetwarzającemu podwykonawcy w przypadku, gdy Administratorowi znane są okoliczności nie zastosowania przez wskazany podmiot odpowiednich środków technicznych i organizacyjnych mających na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności nie zabezpieczenia ich przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, a także w przypadku, kiedy Administratorowi znane są informacje o naruszeniach ochrony danych osobowych występujących w podmiocie wskazanym przez Przetwarzającego.
9. Przetwarzający odpowiada za szkody wyrządzone wskutek niewykonania lub nienależytego wykonania obowiązków wynikających z Umowy oraz z obowiązujących przepisów, w tym za szkody powstałe w wyniku udostępnienia danych osobowych osobom nieupoważnionym, ich zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów, nieuprawnioną zmianą danych, uszkodzeniem lub zniszczeniem, które nastąpiły z winy Przetwarzającego. Odpowiedzialność ograniczona jest do wysokości szkody rzeczywistej.

§ 7
Obowiązywanie i rozwiązanie Umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas trwania umowy, o której mowa w § 1 ust. 2.
2. Rozwiązanie umowy powierzenia przetwarzania danych ze skutkiem natychmiastowym jest równoznaczne z rozwiązaniem umowy głównej ze skutkiem natychmiastowym.
3. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Przetwarzający:
   1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   2) przetwarza dane osobowe w sposób niezgodny z umową;
   3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez uprzedniej zgody Administratora lub nie poinformował Administratora o przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

§ 8

Zasady zachowania poufności

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora 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. 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.

§ 9

Postanowienia końcowe

1. Administrator i Przetwarzający z tytułu i dla zapewnienia współpracy celem realizacji zapisów Umowy Głównej udostępnią dane osobowe swoich pracowników stronie drugiej w maksymalnym zakresie: imię i nazwisko, tytuł zawodowy, stanowisko, służbowy adres poczty elektronicznej, służbowy numer telefonu.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, RODO oraz przepisów prawa UE i krajowego regulujących prawa osób, których dane są przetwarzane.
4. Wszelkie spory wynikające na tle wykonania niniejszej umowy rozstrzygać będzie sąd powszechny właściwy miejscowo ze względu na siedzibę Administratora.

_____	_____
Administrator (Szpital)	Przetwarzający

Załącznik nr 1
do umowy powierzenia przetwarzania danych osobowych

Lista podmiotów podprzetwarzających

Lp.	Nazwa, adres siedziby podmiotu podprzetwarzającego, dane rejestrowe oraz lokacja fizyczna powierzonego zbioru danych	Charakter i cel powierzenia	Czynności przetwarzania	Kategorie powierzonych danych osobowych	Czas przetwarzania (daty od -do)	Dane kontaktowe Inspektora Ochrony Danych lub wyznaczonej przez podmiot przetwarzający osoby do kontaktu (w przypadku braku wyznaczenia IOD)
1.						
2.						
3.						
4.						

Załącznik nr 2
do Umowy powierzenia przetwarzania danych osobowych

Ankieta dla Podmiotu Przetwarzającego
weryfikująca wdrożone środki techniczne i organizacyjne

w zakresie spełniania minimalnych wymagań gwarantujących przetwarzanie danych osobowych w sposób zgodny z wymaganiami RODO[1]

L.p	Element zabezpieczenia {komentarz}	Do wypełnienia przez Podmiot Przetwarzający	
		Opis zastosowania elementu zabezpieczenia {oczekiwana konwencja wpisu: TAK/NIE: opis odnoszący się do pytania[2]}	**Komentarz/uzasadnienie odstąpienia od elementu zabezpieczenia**
1.	Czy Podmiot wyznaczył i poprawnie zgłosił IOD[3] do organu nadzorczego[4]? {jeśli tak: proszę podać kontakt do IOD}		
2.	Jakie formalne kompetencje posiada IOD do pełnienia swej funkcji? {proszę podać kierunkowe kursy, szkolenia, w tym organizowane przez Podmiot przetwarzający – wraz z datami uczestnictwa}		
3.	W jaki sposób Podmiot zapewnił IOD: a) bezzwłoczne włączanie do spraw związanych z przetwarzaniem danych osobowych b) niezależność i wsparcie w działaniach {proszę podać konkretne zapisy z poli-tyk/procedur/pełnomocnictw/decyzji itp.}		
4.	Czy podmiot wyznaczył osobę zastępującą IOD/zespół wspierający pracę IOD? {proszę opisać sposób realizacji zadania}		
5.	Czy Podmiot opracował, wdrożył i stosuje Politykę Bezpieczeństwa oraz procedury, instrukcje, rejestry normujące zasady przetwarzania danych osobowych? {proszę wskazać z nazwy wdrożone dokumenty wraz z krótkim opisem normowanego przez nie zakresu.}		
6.	Czy Podmiot wdrożył powszechnie uznane rozwiązania zabezpieczenia? {proszę wskazać wdrożone rozwiązania, w tym np.: normy ISO z grup: ISO 27000, 29000 i 31000; Stosowane zatwierdzone kodeksy postępowania, o których mowa w art. 40 RODO (jeżeli dotyczy), lub zatwierdzone mechanizmy certyfikacji, o którym mowa wart. 42 RODO}		
7.	Czy Podmiot wdrożył i testuje mechanizmy obsługi incydentów? {proszę o odpowiedź: tak/nie/w trakcie[5]}		
8.	Czy Podmiot wdrożył i testuje plany ciągłości działania? {proszę o odpowiedź: tak/nie/w trakcie[6]}		
9.	Czy podmiot będzie przetwarzał powierzone dane w systemach informatycznych? {Jeżeli tak, proszę wskazać dla każdego z systemów (oprócz identyfikującej system nazwy): a) zakres przetwarzanych danych; b) lokację fizyczną i logiczną systemu i danych; c) przepływy danych między komponentami systemu z uwzględnieniem puli/zakresu przesyłanych danych; d) sposób zabezpieczenia dla każdego z komponentów systemu (np. szyfrowanie,		

[1] Rozporządzenie 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).
[2] W wymaganych przypadkach w formie załącznika do niniejszej ankiety.
[3] Inspektor Ochrony Danych – vide art. 37-29 RODO. Poprawne zgłoszenie – vide: Rozdział 2 ustawy z 10 maja 2018 o ochronie danych osobowych.
[4] Vide art. 4 pkt 21 RODO.
[5] Wymagany krótki komentarz, jeżeli wdrożone rozwiązanie nie jest kompletne.
[6] Wymagany krótki komentarz, jeżeli wdrożone rozwiązanie nie jest kompletne.

L.p	Element zabezpieczenia {komentarz}	Do wypełnienia przez Podmiot Przetwarzający	
		Opis zastosowania elementu zabezpieczenia {oczekiwana konwencja wpisu: TAK/NIE: opis odnoszący się do pytania[2]}	Komentarz/uzasadnienie odstąpienia od elementu zabezpieczenia
	pseudonimizacja, uwierzytelnianie dostępu, zasady dotyczące tworzenia i zarządzania kopiami bezpieczeństwa, monitorowanie/logi z działań; e) czy stosuje się walidację / weryfikację integralności / autentyczności danych; f) ogólny opis sposobu separacji danych Administratora od innych danych w systemie (danych innych Administratorów); g) ogólny opis sposobu usuwania /aktualizacji danych na wniosek Administratora[7]; h) czy stosuje się rozdział środowiska testowego od produkcyjnego; i) sposób serwisowania z uwzględnieniem dostępu firm serwisujących i ich dostępu do danych; j) grupy funkcyjne osób mających dostęp do systemu / zasady przydzielania dostępu; k) inne istotne zastosowane środki zabezpieczenia technicznego, fizycznego i organizacyjnego.} {zaleca się możliwie syntetyczny opis, a w zakresie prezentacji przepływów zalecaną formą jest diagram. W systemach informatycznych należy uwzględnić również zabezpieczenia poczty elektronicznej[8].}		
10.	W przypadku zgody Administratora i chęci Podmiotu na podpowierzenie przetwarzania danych: • W jakim zakresie Podmiot chce podpowierzyć przetwarzanie tych danych? • W jaki sposób u podwykonawcy nadzorowany jest proces ochrony i zabezpieczenia danych? • Czy w ramach podpowierzenia dane opuszczą EOG, a jeśli tak, to do jakiego kraju trafią dane oraz jakie będą stosowane mechanizmy zabezpieczenia?		
11.	Czy Podmiot prowadzi okresowe audyty zgodności przetwarzania danych osobowych z wymaganiami RODO? {Jeżeli tak, proszę wskazać stosowaną(e) metodę(y), w tym standardy}		
12.	Czy Podmiot prowadził szacowanie ryzyka /ocenę skutków przetwarzania dla zadań, które przyjmuje do realizacji w ramach powierzenia przetwarzania we własnym środowisku? {Jeżeli tak, proszę wskazać wyniki tych działań, w tym informację o zidentyfikowanych ryzykach}		
13.	Czy w przeszłości były przeprowadzone kontrole przez organ(y) nadzorczy(e)? Jeśli tak, to jaka była tego przyczyna? {proszę o odpowiedź: tak/nie, wraz z ewentualnym, krótkim opisem przyczyny}		
14.	W jaki sposób osoby mające dostęp do danych osobowych zostały zapoznane z przepisami dotyczącymi ochrony danych osobowych i zobowiązane do ich przestrzegania?		

[7] Chodzi o retencję danych.

[8] W tym np. sposobu uzgadniania metod szyfrowania i przekazania haseł.

L.p	Element zabezpieczenia {komentarz}	Do wypełnienia przez Podmiot Przetwarzający	
		Opis zastosowania elementu zabezpieczenia **{oczekiwana konwencja wpisu:** **TAK/NIE: opis odnoszący się do pytania[2]}**	**Komentarz/uzasadnienie odstąpienia od elementu zabezpieczenia**
15.	Czy osoby mające dostęp do danych osobowych zostały zobowiązane do zachowania przetwarzanych danych w tajemnicy (w tym również po ustaniu zatrudnienia/współpracy)?		
16.	Jakie są zasady nadawania i dokumento-wania dostępu do: • przetwarzania danych osobowych? • systemów informatycznych?		
17.	Jakie zasady regulują dostęp do stref i pomieszczeń w których przetwarzane będą powierzone Podmiotowi dane przez Administratora? Jakie techniczne rozwiązania są stosowane do kontroli ruchu osobowego i materiałowego (w zakresie zasobów zawierających ww. dane)? {Należy rozróżnić pomieszczenia zwykłe od specjalnych typu serwerownia oraz uwzględnić poszczególne fizyczne lokacje własne i w podmiotach świadczących usługi podpowierzenia}		
18.	W jaki sposób przesyłane są nośniki za-wierające dane osobowe? {Dotyczy zarówno przesyłanych nośników informatycznych jak też dokumentów w formie papierowej. Proszę o uwzględnienie -jeżeli zastosowano w działaniu- różnic między operatorem a operatorem wyznaczonym}		
19.	Czy Podmiot przetwarza dane wielu Administratorów? {Jeśli tak, to jakie mechanizmy zostały wdrożone by zabezpieczyć te procesy?}		

.....

podpis i pieczęć osoby reprezentującej Przetwarzającego